Ameaças cibernéticas: 2021 em retrospectiva

pwc

Conteúdo

Introdução

O *ransomware* consolidou sua posição como principal ameaça de segurança cibernética enfrentada por organizações em todas as regiões e segmentos de indústria, com ímpeto e impacto maiores ao longo de 2021.

A PwC atende mais de 200 mil clientes em 156 países. Usamos nossa posição estratégica como uma das maiores e mais globais redes de serviços profissionais para fornecer um dos serviços de inteligência de ameaças mais globais para nossos clientes. Nossa pesquisa respalda todos os nossos serviços de segurança e é usada por organizações dos setores público e privado em todo o mundo para proteger redes, fornecer informações situacionais e fundamentar estratégias. Este relatório anual documenta as tendências gerais e temáticas que observamos em 2021 e é parte de nossa contribuição para ajudar a construir uma sociedade digital segura.

Programas de afiliados e esquemas de *Ransomware-as-a-Service* (RaaS) fomentaram um crescimento ainda maior da ameaça representada pelo crime cibernético, e seu impacto oculto no cotidiano ficou mais evidente uma vez que escolas, instituições filantrópicas, serviços públicos e a infraestrutura essencial foram mais afetados por ataques indiscriminados. Esses esquemas simplificaram os canais de "prejudicar para lucrar" – oferecendo incentivos financeiros, acordos baseados em reputação e até mesmo fornecendo aos operadores recursos como manuais de invasão passo a passo. Ao mesmo tempo, os esquemas de *ransomware* continuaram a fortalecer os laços mutualistas com o ecossistema do crime cibernético que os cerca, incluindo sistemas de distribuição de *malware* (como TrickBot, IcedID e QakBot), fóruns clandestinos que facilitam o recrutamento de afiliados de *ransomware* e mercados de AaaS (*Access-as-a-Service*).

Enquanto 2020 foi dominado pela pandemia de covid-19, sua disseminação pelo mundo e seu impacto no ciberespaço, uma grande tendência em 2021 foi a proliferação de recursos cibernéticos. As vulnerabilidades de dia zero retomaram seu lugar como uma das principais preocupações discutidas nas conversas sobre segurança cibernética, com questões em torno de sua pesquisa, divulgação e exploração atraindo maior interesse público. Elas surgiram especialmente em relação a ataques indiscriminados e aspectos de segurança nacional, enquanto agentes de ameaças com todas as motivações e recursos se apressavam em explorar vulnerabilidades de alto perfil, como ProxyLogon e Log4Shell. O abuso de *exploits* de dia zero também está relacionado a dois outros fenômenos: o impacto dos *quartermasters* digitais no cenário de ameaças cibernéticas (incluindo o dos *quartermasters* comerciais) e a atividade de vigilância contra alvos civis.

As operações de coleta de inteligência, em sua maioria, permaneceram alinhadas a eventos geopolíticos. No entanto, em 2021, mais do que em qualquer outro ano, identificamos grupos de atividades novos e em ascensão que perseguem objetivos alinhados aos interesses estratégicos de países específicos, como agentes de ameaças provavelmente oriundos de países nos quais não havíamos observado atividade cibernética ofensiva anteriormente.

As análises neste relatório foram conduzidas pela prática de PwC Threat Intelligence, que é distribuída entre Alemanha, Austrália, Brasil, Estados Unidos, Holanda, Itália, Reino Unido e Suécia. Elas se baseiam em nossos conjuntos de dados internos de inteligência sobre ataques cibernéticos de uma ampla variedade de agentes de ameaças. Essa inteligência é obtida em trabalhos de resposta a incidentes da PwC em todo o mundo e em nossos serviços gerenciados de caça a ameaças, bem como em informações publicamente disponíveis.

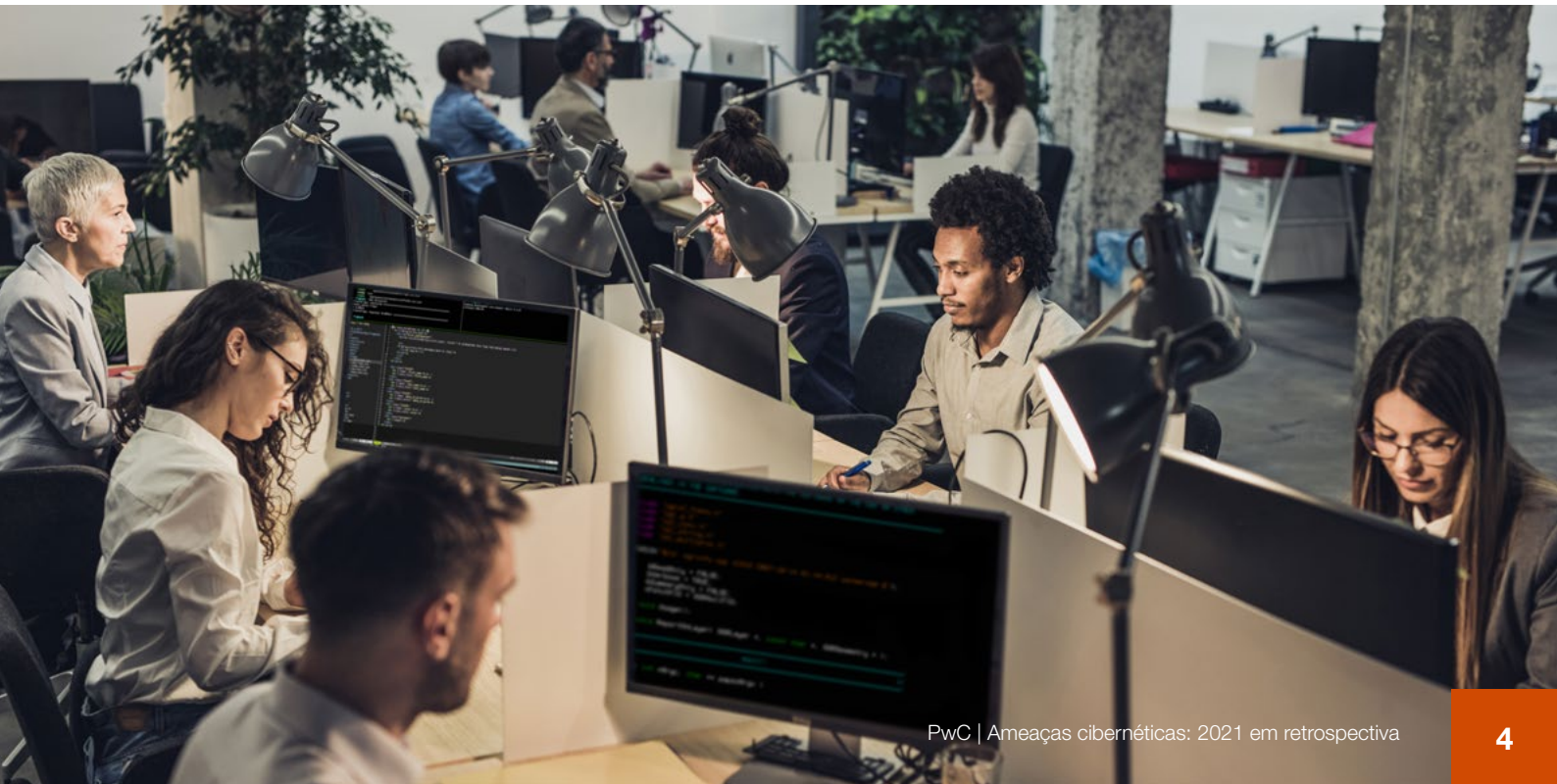
01 |

Tempestade perfeita: dia zero, *quartermasters* e vigilância

Ano do dia zero (0-Day)

As vulnerabilidades de dia zero – e, especialmente, sua pesquisa e divulgação – têm sido um tema de interesse sempre presente na comunidade de segurança cibernética. Em 2021, vários eventos de grande repercussão, inclusive operações altamente direcionadas e exploração em massa de vulnerabilidades, trouxeram esse tópico mais uma vez ao primeiro plano das discussões estratégicas e táticas e aos olhos do público.

Em vez de tratar de ataques de dia zero como uma ameaça intransponível, fornecemos nesta seção o contexto estratégico desse fenômeno.



Uma visão estratégica do cenário do dia zero

As discussões sobre o dia zero geralmente giram em torno da dificuldade de evitá-lo, com base na percepção de que pode ser ainda mais difícil se defender. Em 2021, vimos a cobertura desse tema se generalizar, juntamente com outros tópicos de grande repercussão, como ataques a cadeias de suprimentos (após o incidente da SolarWinds) e *ransomware* (após ataques a entidades como Colonial Pipeline). O ano de 2021 também registrou o maior número de *exploits* de dia zero divulgadas em um único ano,[1] quase o dobro dos números de 2020. As razões por trás desse aumento são sutis e provavelmente resultam de uma combinação de fatores, como:

- **Um elemento mais evidente de segurança nacional**: embora vulnerabilidades de dia zero tenham sido exploradas por anos, em 2021 houve várias demonstrações políticas de "diplomacia de dia zero"; isto é, discussões sobre seu uso no nível da segurança nacional. Como exemplo, a coalizão recém-eleita na Alemanha fez uma declaração política sobre o embargo da compra governamental de vulnerabilidades de dia zero, citando sua "relação altamente problemática com a segurança de TI e os direitos civis".[2] A Administração do Ciberespaço da China (CAC) anunciou novas leis em torno da divulgação de vulnerabilidades domésticas.[3] A nova lei também se aplica aos fornecedores, que devem garantir a mitigação de quaisquer vulnerabilidades em tempo hábil e sua pronta divulgação aos clientes, juntamente com as correções, e estimula as organizações privadas a estabelecer programas de recompensas por *bugs* para incentivar financeiramente a pesquisa de vulnerabilidades.
- **O mercado de *exploits* de dia zero se expandiu:** nos últimos anos, vem crescendo o número de *players* que operam no espaço de pesquisa de vulnerabilidades, entre pesquisadores de segurança individuais, negociadores criminosos de *exploits* dia zero e empresas de espionagem privada, como Hacking Team, FinFisher, NSO Group e Candiru. Negociadores de *exploits* e organizações do setor privado, especialmente, estão entre os *players* de mais destaque no que diz respeito ao desenvolvimento e negociação de *exploits* de dia zero.
- **Mais incentivos do que nunca:** existem hoje cada vez mais caminhos para pesquisadores de vulnerabilidades competirem e ganharem recompensas financeiras por seu trabalho de desenvolvimento de *exploits*. Eles podem ser legítimos, como a Copa Tianfu e o Pwn2Own, ou ilegítimos, caso de concursos de pesquisa ofensiva lançados em fóruns da *dark web* em russo.[4] Com essa atividade firmemente enraizada no mundo da segurança ofensiva, os defensores tiveram que responder, dedicando recursos ao seu próprio trabalho de desenvolvimento de *exploits* para fins de identificação e divulgação, como no Projeto Zero do Google.[5]
- **Um enfoque renovado na infecção de terceiros:** agentes de ameaças com diversas motivações começaram a visar organizações envolvidas em cadeias de suprimentos, muitas vezes permitindo o acesso a vários alvos ao mesmo tempo. Isso levou ao investimento de recursos em pesquisa de vulnerabilidades de tecnologias corporativas amplamente utilizadas, como servidores de e-mail ou *software* de gerenciamento de conhecimento. Naturalmente, isso aumentou a quantidade de *exploits* de dia zero descobertos e, com a divulgação deles (mesmo de forma responsável e acompanhada de correções e avisos do fornecedor), da quantidade de tentativas de explorar essas vulnerabilidades.

Em última análise, evitar ataques de dia zero não é uma questão trivial para desenvolvedores e fornecedores de software, muito menos para sua base de clientes. No entanto, clientes e defensores não devem subestimar as capacidades e medidas que podem ser implementadas com foco na detecção e resposta a comportamentos e atividades pós-*exploits*. Além de uma higiene de segurança central robusta, uma função sólida de detecção e resposta pode fazer a diferença no impacto que os novos ataques de dia zero podem ter nas organizações.

1. "2021 has broken the record for zero-day hacking attacks", MIT Technology Review: Patrick Howell O'Neill. https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/ (23/9/2021)
2. "New German government coalition promises not to buy exploits", Recorded Future, https://therecord.media/new-german-government-coalition-promises-not-to-buy-exploits/ (8/12/2021)
3. Full (vulnerability) disclosure", PwC Threat Intelligence, CTO-SIB-20210810-01A
4. "Play evil games, win evil prizes", PwC Threat Intelligence, CTO-SIB-20210625-01A
5. Google, "Project Zero", https://googleprojectzero.blogspot.com

Visão geral da atividade de *quartermaster*

A maneira como os agentes de ameaças adquirem e fornecem ferramentas pode afetar não apenas a atribuição de responsabilidades, mas, o que é mais importante, seus recursos e a capacidade de buscar novos grupos para alvejar. O conceito de *quartermaster* (ou intendente) digital não é novo quando se trata de operações cibernéticas, mas continua cada vez mais relevante. Os intendentes têm sido tradicionalmente associados ao fornecimento de tecnologia para unidades militares. Consequentemente, os intendentes digitais são mais frequentemente considerados no contexto de agentes de ameaças persistentes avançadas (APT, na sigla em inglês) que conseguem acesso a recursos compartilhados apenas entre um grupo seleto de agentes de ameaças ou obtêm ferramentas de uma entidade central encarregada de distribuí-las e permitir seu uso.

No entanto, a PwC também define como "intendentes comerciais" as empresas que vendem soluções de segurança ofensivas, como *spyware*, *exploits* de dia zero e recursos relacionados, para entidades que operam. Enquanto os intendentes tradicionais geralmente fornecem ferramentas apenas para os agentes de ameaças de seu próprio país, os clientes dos intendentes comerciais podem estar localizados em vários países.

Quartermasters de APT

Embora nem sempre seja possível provar, a hipótese de que vários grupos de APT operam ou são financiados pelo mesmo *quartermaster* digital não pode ser descartada para vários conjuntos de agentes de ameaças. Em 2021, continuamos a observar esse fenômeno, seja por meio de observações de capacidade compartilhada (*malware*, técnicas, *exploits* etc.), seja por sobreposições de infraestrutura (tanto pelos mesmos padrões observados em C2s quanto pela reutilização de domínios/IPs por outros agentes de ameaças).

Shadows e Proxies: agentes de ameaças com sede na China compartilham ferramentas

O compartilhamento contínuo de ferramentas e técnicas é um tema recorrente entre os agentes de ameaças baseados na China. Embora nem todos os agentes de ameaças naquele país compartilhem ferramentas entre si e nem todos tenham acesso às mesmas ferramentas, os acordos de *quartermasters* (abordados em detalhes em uma seção mais à frente) continuam a complicar a atribuição de responsabilidades pelos ataques. Por exemplo, as mesmas famílias de *malware* (como PlugX, PoisonIvy, ShadowPad, Quarian e o *backdoor* Winnti) são usadas por vários agentes de ameaças na China e, como foi muito divulgado em 2021 com os incidentes do ProxyLogon, alguns agentes de ameaças também compartilham *exploits*.

Percebemos que, embora não se tenha observado que todos esses agentes de ameaças tenham tido acesso às ferramentas compartilhadas detalhadas a seguir, elas são os principais exemplos da dinâmica descrita nesta seção.

ShadowPad e Scatterbee

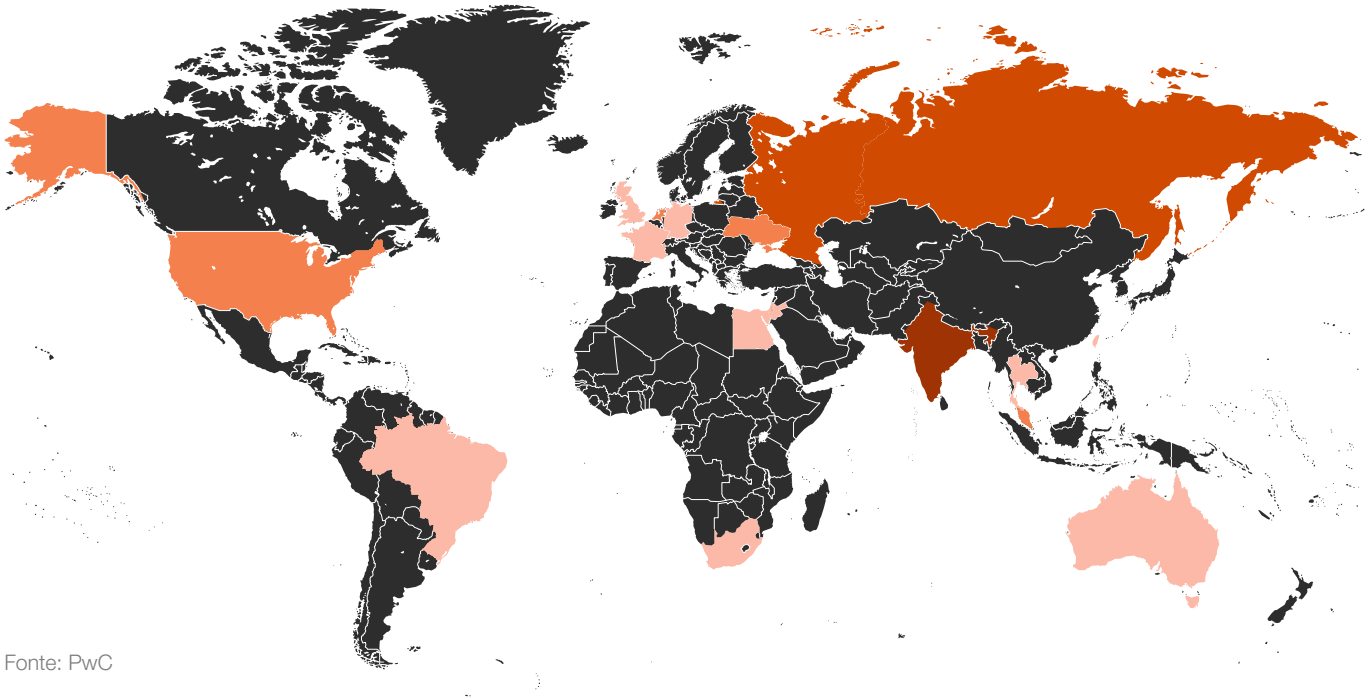
O ShadowPad é um *backdoor* modular que permite a um agente de ameaças personalizar a funcionalidade fornecida em um implante. Cada amostra do ShadowPad que vimos tem um módulo raiz projetado para orquestrar o próximo conjunto de módulos, incluindo um módulo de plug-ins que pode ser personalizado dependendo da funcionalidade que o agente de ameaças requer. Os plug-ins podem habilitar recursos como comunicações C2 sobre HTTP ou TCP, registro de teclas, coleta de captura de tela, mapeamento de portas e coleta de informações do sistema, entre outros.[6]

Ao monitorar amostras "padrão" do ShadowPad em 2021, identificamos e analisamos uma nova variante, que chamamos de ScatterBee: amostras do ShadowPad que foram ofuscadas com o uso de uma técnica personalizada.[7] Provavelmente para minimizar a detecção nas redes das vítimas, o mecanismo de empacotamento ScatterBee implementa ofuscação de fluxo de controle, codificação de *string*, resoluções de API dinâmicas, várias técnicas antianálise, bem como decodificação/descriptografia de *shellcode*. Avaliamos que um ou mais usuários do ShadowPad têm acesso ao ScatterBee e provavelmente distribuíram algumas dessas cargas maliciosas por meio de ataques *watering hole* em sites usados para fornecer arquivos de atualização do Adobe Flash. Avaliamos que a maioria das cargas úteis do ScatterBee pode ser diretamente vinculada ao agente de ameaças que rastreamos como Red Dev 10 (também conhecido como Earth Lusca) e foi usada para atingir organizações nos setores aeroespacial e de defesa.

Avaliamos que o ShadowPad é muito provavelmente usado por pelo menos 11 agentes de ameaças baseados na China.[8] Nossa análise em subconjuntos específicos da infraestrutura do ShadowPad nos permitiu identificar um amplo conjunto de vítimas, desde entidades sediadas na Índia nos setores de telecomunicações e petróleo e gás até unidades de organizações humanitárias internacionais no Leste Asiático.

6. "Shining a light on ShadowPad usage throughout 2019", PwC Threat Intelligence, CTO-TIB-20200213-01A
7. "Chasing Shadows", PwC Threat Intelligence, CTO-TIB-20211021-01A
8. "My, My, MySSL tracking C2 infrastructure through certificate reuse", PwC Threat Intelligence, CTO-TIB-20210226-01B

Figura 1: Distribuição geográfica das vítimas do ShadowPad observadas até dezembro de 2021



Fonte: PwC

O Exchange como alvo: ProxyLogon

No início de 2021, o Red Dev 13 (também conhecido como HAFNIUM) começou a explorar vulnerabilidades no Microsoft Exchange, o que ficou conhecido coletivamente como ProxyLogon.[9] [10] [11] Em março de 2021 (perto, mas antes da primeira divulgação pública dessas campanhas), vários agentes de ameaças na China começaram a explorar as mesmas vulnerabilidades, em grande escala, em contraste a ataques precisos.

Como já destacamos, não é incomum que esses agentes de ameaças compartilhem ferramentas. No entanto, o rápido compartilhamento desses *exploits* antes da correção das vulnerabilidades do Microsoft Exchange foi sem precedentes.

Desenvolvedores no Irã trabalhando em vários APTs

Os agentes de ameaças são normalmente identificados pelos recursos, infraestrutura, alvos e TTPs (táticas, técnicas e procedimentos) gerais que exibem. No entanto, desenvolvedores ou operadores por trás de campanhas que trabalham com vários agentes de ameaças podem confundir a análise e a atribuição de responsabilidades.

Esse pode ser o caso de agentes de ameaças com sede no Irã. Por exemplo, ao pesquisar as campanhas de *phishing* do Yellow Liderc[12] (também conhecido como Tortoiseshell, TA456), identificamos um conjunto de documentos PDFs maliciosos direcionados ao setor de ensino superior. Esse alvo normalmente não se alinhava com o Yellow Liderc, mas corresponde ao do Yellow Garuda (também conhecido como Charming Kitten, APT35, PHOSPHORUS, TA453 e ITG18). Já havíamos observado sobreposições de infraestrutura entre esses dois agentes de ameaças, o que levantou a hipótese de que o Yellow Liderc seja uma ramificação do Yellow Garuda.[13] Com base em várias semelhanças entre esses agentes de ameaças, avaliamos que há uma probabilidade realista de que um operador tenha estendido sua atuação ou transitado entre os dois em 2021.

9. "HAFNIUM exploiting Exchange vulnerabilities", PwC Threat Intelligence, CTO-QRT-20210303-01A
10. "HAFNIUM targeting Exchange Servers with 0-day exploits", Microsoft, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ (2/3/2021)
11. "Operation Exchange Marauder: Active Exploitation of Multiple 0-day Microsoft Exchange Vulnerabilities", Volexity: Josh Grunzweig, Matthew Meltzer, Sean Koessel, Steven Adair, Thomas Lancaster, https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-0-day-vulnerabilities/ (2/3/2021)
12. "Eat, Sleep, Liderc, Repeat", PwC Threat Intelligence, CTO-TIB-20210730-01A
13. "Caught in a .NET", PwC Threat Intelligence, CTO-TIB-20210211-02A

Quartermasters comerciais

Os *quartermasters* comerciais diferem das empresas definidas como *hackers* de aluguel (*hack-for-hire* em inglês), como CyberRoot e BellTroX.[14] Empresas que atuam como *hackers* de aluguel são encarregadas de fazer a invasão real em nome de um cliente pagante, enquanto os *quartermasters* comerciais oferecem apenas ferramentas pagas pelo cliente, que são usadas pelo próprio cliente para fazer a invasão. Os primeiros exemplos de *quartermasters* comerciais incluem o Hacking Team e o FinFisher, que se viram no centro de um grande escândalo e mudaram de nome ou faliram. Apesar da queda de atividade dessas empresas, a PwC continua a observar os agentes de ameaças, principalmente os que executam operações de vigilância aproveitando os *quartermasters* comerciais e seus recursos.[15]

A atenção recente do público a *quartermasters* comerciais como o NSO Group e o Candiru forneceram insights sobre uma indústria relativamente secreta e crescente, que tem implicações para profissionais de segurança cibernética e vítimas em potencial, como:

- dificuldade em responsabilizar agentes de ameaças que, de outra forma, não seriam capazes de conduzir operações tão sofisticadas;
- capacitação rápida de um país para atingir o setor público e privado com *malware* avançado, como uma empresa, órgão governamental ou seu pessoal; e
- potencial abuso dessas ferramentas para atingir jornalistas, ativistas e a sociedade civil.

Além disso, as ferramentas produzidas por *quartermasters* comerciais são quase certamente usadas contra uma ampla gama de alvos, que também podem incluir funcionários de governos e executivos do setor privado, atraindo a atenção de organizações que talvez não imaginem que esses tipos de agentes de ameaças se encaixam em seu perfil de ameaça.

14. "Cyber Threats 2020: A Year in Retrospect", PwC Threat Intelligence
15. "A closer look at commercial quartermasters", PwC Threat Intelligence, CTO-SIB-20210906-01A

Um olhar sempre atento: vigilância e sociedade civil

Seja armada pela ascensão de negociadores de *exploits* e fornecedores de *software* de vigilância, aprimorada por acordos de *quartermaster* ou realizada por grupos patrocinados por nações, a vigilância de alvos civis representa uma ameaça significativa a uma sociedade digital segura para todos. Minorias, ativistas dos direitos civis, dissidentes, políticos e jornalistas, além da sociedade civil em geral, costumam cair na mira de atividades de espionagem patrocinadas por nações. Os alvos na sociedade civil geralmente incluem também ONGs, movimentos sociais, coalizões e organizações religiosas que podem compartilhar interesses comuns.

Embora a atividade de vigilância geralmente se concentre em uma pessoa de interesse, às vezes se descobre que as organizações associadas a esses indivíduos são vítimas, pois a organização é considerada um trampolim de acesso ao alvo pretendido. Esse fator é útil para contextualizar as ameaças à sociedade civil como um problema comum.

Ampliando a vigilância: de *hacker* de aluguel a *quartermaster* comercial

Candiru

Em julho de 2021, o Citizen Lab,[16] a Microsoft,[17] e o Google[18] expuseram em graus variados um *quartermaster* comercial chamado Candiru, que rastreamos como Gray Mazzikim (também conhecido como SOURGUM). Segundo a Microsoft, o *spyware* do agente teria sido implantado contra mais de cem vítimas. Vários domínios associados a campanhas que rastreamos em 2021 indicaram um claro ataque a ativistas de direitos humanos e jornalistas; outros se alinharam mais com os interesses estratégicos de uma nação, como exportações de energia ou organizações governamentais. O *spyware* vendido por Gray Mazzikim é altamente sofisticado e pode infectar e monitorar iPhones, Androids, Macs, PCs e contas na nuvem.[19] Quando um alvo é infectado com o *spyware*, o operador pode extrair os dados privados da vítima de vários aplicativos e contas, incluindo Gmail, Skype, Telegram e Facebook, além de capturar o histórico de navegação e as senhas.[20] O agente da ameaça também pode conseguir ligar a webcam e o microfone do alvo ou fazer capturas de tela.

Como o Candiru é fornecedor de vários agentes de ameaças em todo o mundo, a complexidade e a escala desses ataques são bastante extensas. Nos esforços para maximizar a cobertura dessas ameaças e categorizá-las, a PwC rastreia o Candiru como Gray Mazzikim e seus clientes, que atualmente consistem em pelo menos quatro agentes de ameaças diferentes, em separado quando possível.[21] Há uma ampla variedade de alvos, mas com um foco distinto na Europa e no Oriente Médio.

16. Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus", Citizen Lab, https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/ (15/7/2021)
17. "Protecting customers from a private-sector offensive actor using 0-day exploits and DevilsTongue malware", Microsoft, https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/ (15/7/2021)
18. "How we protect users from 0-day attacks", Google, https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/ (14/7/2021)
19. "Another commercial quartermaster", PwC Threat Intelligence, CTO-TIB-20210806-02A
20. "Another commercial quartermaster", PwC Threat Intelligence, CTO-TIB-20210806-02A
21. "A closer look at commercial quartermasters", PwC Threat Intelligence, CTO-SIB-20210906-01A

NSO Group

O NSO Group, que a PwC monitora como Gray Anqa, foi fundado em 2010. A empresa é mais conhecida pelo *spyware* chamado Pegasus, mas também oferece uma série de outros produtos, incluindo software de geolocalização para telefones celulares e sistemas de análise de dados. Seus principais serviços e ofertas de produtos são voltados para dispositivos e redes móveis. O Pegasus é conhecido por infectar as versões mais recentes de sistemas operacionais populares de celulares por meio de *exploits* de dia zero e clique zero, incluindo um dos *exploits* mais sofisticados já documentados, conhecido como FORCEDENTRY.[22] [23]

O NSO ganhou as manchetes em várias ocasiões por vender seu *spyware* Pegasus para nações que acabaram abusando das ferramentas para espionar a sociedade civil.

As semelhanças reconhecíveis entre Gray Anqa e Gray Mazzikim são muitas: tipo semelhante de empresa, operação no mesmo país, recrutamento nas mesmas bases de talentos e clientela semelhante. Em ambos os casos, as capacidades ofensivas prontamente disponíveis para compra põem em evidência uma indústria que permite ao consumidor usar ferramentas sofisticadas que também foram abusadas para perpetrar ataques à sociedade civil em escala internacional.

Puxando a tomada: reação aos *quartermasters* comerciais

Em 2021, os *quartermasters* comerciais capturaram as atenções do público e dos tribunais em vários países. Por exemplo, várias empresas de tecnologia dos EUA estão processando fornecedores comerciais de *spyware* em nome de sua base de clientes e, em alguns casos, buscando restringir o acesso dos réus ao hardware e software das empresas. Também em 2021 observamos a primeira ação de grande repercussão contra *quartermasters* comerciais em nível nacional: o Departamento de Comércio dos EUA colocou o NSO Group e o Candiru em sua lista de entidades, citando o risco significativo de eles agirem "contrariamente à segurança nacional ou aos interesses de política externa dos Estados Unidos".[24]

Uma primeira consequência de tal ação foi, por exemplo, a decisão do governo israelense de restringir em dois terços a lista de países para os quais as empresas de segurança israelenses podem vender ferramentas de *hacking* ofensivas e de vigilância. Conforme já destacado, notamos que os *quartermasters* comerciais operam em vários países, com vários negociadores ativos na Europa,[25] [26] e nos EUA.[27]

A provável existência duradoura de *quartermasters* comerciais traz um novo conjunto de desafios. É relativamente fácil para um país comprar ferramentas ofensivas personalizadas e altamente sofisticadas que elevam suas capacidades às de uma ameaça persistente avançada. A alta sofisticação dos *quartermasters* comerciais, além de seus orçamentos para pesquisa e desenvolvimento, também pressupõe sua capacidade de se reequipar, mantendo altos padrões de segurança operacional, o que permite aos usuários finais continuar operando mesmo após a exposição pública.

22. "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild", CitizenLab: Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, Ron Deibert, https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/ (13/9/2021)
23. "A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution", Google Project Zerolan Beer & Samuel Groß, https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html (15/12/2021)
24. "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities", United States Commerce Department, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list (3/11/2021)
25. "You Only Click Twice: FinFisher's Global Proliferation", CitizenLab: Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ (13/3/2013)
26. "FinSpy: Unseen Findings", Kaspersky, https://securelist.com/finspy-unseen-findings/104322/ (28/9/2021)
27. "Exclusive: An American Company Fears Its Windows Hacks Helped India Spy On China And Pakistan", Forbes: Thomas Bewster, https://www.forbes.com/sites/thomasbrewster/2021/09/17/exodus-american-tech-helped-india-spy-on-china/?sh=13286ba07009 (17/9/2021)

Vigilantes persistentes avançados: atividade de vigilância APT

Red Dev Redemption

O Red Dev 3 (também conhecido como DeepCliff ou RedAlpha) é um agente de ameaças ativo desde pelo menos 2015. Ele foi exposto pela primeira vez em código aberto em 2018 pelo CitizenLab em um ataque a uma comunidade específica.[28] Ao longo de 2021, observamos que o Red Dev 3 configurou centenas de domínios para hospedar páginas de *phishing* de credenciais destinadas a diversos grupos de alvos em escala internacional.[29]

A convenção de nomenclatura de domínio do Red Dev 3 imita provedores de serviços de e-mail bastante usados, e o agente da ameaça também pode falsificar portais de login para os serviços de e-mail específicos das organizações visadas.[30]

O Red Dev 3 também visava ou falsificava serviços, como meios de comunicação populares entre comunidades de diáspora e dissidentes; ONGs com foco em refugiados, direitos civis e humanos, como a Anistia Internacional; e *think tanks* e institutos de formulação de políticas.

Desde abril de 2021, observamos uma ampliação do foco dos ataques do agente de ameaças, passando da sociedade civil para entidades governamentais, incluindo ministérios de relações exteriores em pelo menos cinco países, bem como várias organizações governamentais e políticas em todo o mundo.[31] No entanto, o agente de ameaças também continuou a atacar aberta e persistentemente cidadãos e comunidades vulneráveis em relação a temas políticos e sociais sensíveis.

As novas artimanhas do Red Nue

O Red Nue, ativo desde pelo menos 2017, é conhecido pelo uso do *backdoor* multiplataforma LootRAT, também chamado de ReverseWindow.[32] O LootRAT tem variantes para Windows[33] e Macintosh[34] (relatada em código aberto como Demsty), além de uma variante para Android conhecida como SpyDealer.[35] O Red Nue também usa outro *backdoor*[36] do Windows conhecido como WinDealer[37] desde pelo menos 2019. Na época, ele foi implantado em alvos como parte de uma campanha de *watering hole* em um site de notícias chinês para a comunidade da diáspora chinesa.

Em 2021, observamos que o agente de ameaças continua a iterar no LootRAT, implantando uma variante Linux do *backdoor*.[38] A nova amostra do *backdoor* teve a seção de comentários do binário removida, provavelmente em uma tentativa de tornar a análise e o entendimento sobre o agente de ameaças mais difícil. Todas as vítimas que observamos nessa campanha estavam na Ásia e incluíam uma empresa de tecnologia que fornece software de simulação.

28. "Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community", CitizenLab: Masashi Crete-Nishihata, Jakub Dalek, Etienne Maynier, John Scott-Railton, https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/ (30/1/2018)
29. "Red Dev Redemption", PwC Threat Intelligence, CTO-TIB-20210202-01A
30. "Red Dev Redemption 2", PwC Threat Intelligence, CTO-TIB-20210223-01A
31. "Red Dev Redemption 3", PwC Threat Intelligence, CTO-TIB-20210401-01A
32. "'LuoYu': The eavesdropper sneaking in multiple platforms", Team T5: Leon & Shui, https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf (28/1/2021)
33. "Red Dev 7 gets a Nue name", PwC Threat Intelligence, CTO-TIB-20201016-01A
34. "APT trends report Q2 2017", Kaspersky, https://securelist.com/apt-trends-report-q2-2017/79332/ (8/8/2017)
35. "LootRAT deals four of a kind", PwC Threat Intelligence, CTO-TIB-20200130-02A
36. "Threats under the Spotlight: February 2021", PwC Threat Intelligence, CTO-TUS-20210317-01A
37. "Malware WinDealer used by LuoYu Attack Group", JPCERT: Yuma Masubuchi, https://blogs.jpcert.or.jp/en/2021/10/windealer.html#1 (26/10/2021)
38. "Threats under the Spotlight: April 2021", PwC Threat Intelligence, CTO-TUS-20210511-01A

“A alta sofisticação dos *quartermasters* comerciais, além de seus orçamentos para pesquisa e desenvolvimento, também pressupõe sua capacidade de se reequipar, mantendo altos padrões de segurança operacional, o que permite aos usuários finais continuar operando mesmo após a exposição pública.”

Partes da Ásia aparecem fortemente na vitimologia do Red Nue. Esse agente de ameaças tem como alvo indivíduos e universidades com a variante Demsty MacOS do LootRat. Por exemplo, o SpyDealer (a versão Android do LootRAT) tem a capacidade de roubar informações de mais de 40 aplicativos de comunicações móveis, incluindo WeChat, Facebook, WhatsApp, Skype, Sina Weibo, Tencent Weibo e Oupeng Browser, muitos dos quais são amplamente utilizados na China.

O White Dev 75 ataca o Oriente Médio e o Norte da África

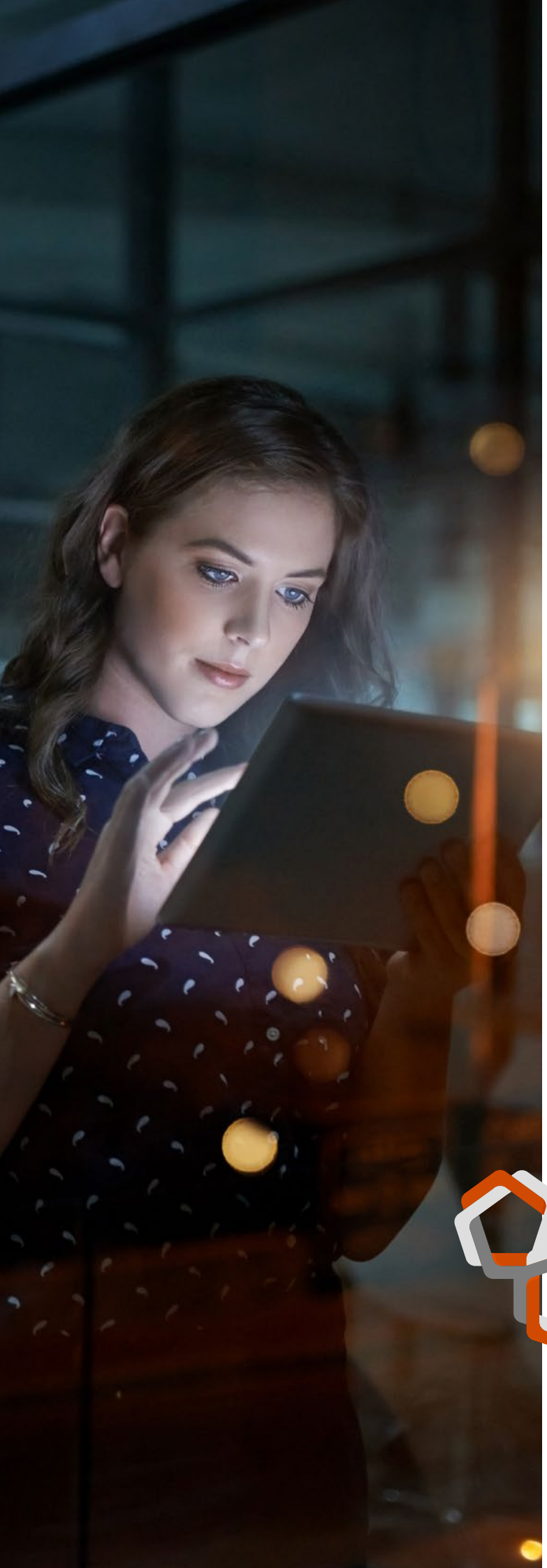
O White Dev 75 está ativo desde pelo menos 2015, e a PwC identificou que esse agente de ameaças é motivado provavelmente por espionagem. Suas vítimas são sobretudo membros da sociedade civil, que devem estar sendo visados em relação a temas políticos. O White Dev 75 se mantém altamente eficaz em comprometer contas de e-mail de jornalistas, dissidentes e indivíduos com atuação política localizados em todo o Oriente Médio e Norte da África. [39] [40] [41]

Entre pelo menos abril e outubro de 2021, o White Dev 75 registrou dezenas de novos domínios de *phishing* que se alinham com táticas e procedimentos anteriores observados em suas campanhas, incluindo um que se faz passar pelo Ministério das Relações Exteriores (MRE) de um país do Oriente Médio. O White Dev 75 é especialmente eficaz devido à sua capacidade de burlar o MRE e tirar partido de técnicas convincentes de engenharia social. Os e-mails de *phishing* que o White Dev 75 costuma usar são alertas de segurança falsos de comportamento anormal de login. O agente da ameaça também foi observado abusando do OAuth para burlar o MRE e senhas.[42] O OAuth é um aplicativo comum para autenticar serviços de terceiros sem a necessidade de compartilhar senhas. Os TTPs observados do White Dev 75 não são muito avançados, mas demonstram persistência e inteligência em suas técnicas de espionagem para executar essas táticas contra a sociedade civil.

+40

apps dos quais o SpyDealer (a versão Android do LootRAT) pode roubar informações

39. “White Dev 75, like shooting phish in a barrel”, PwC Threat Intelligence, CTO-TIB-20210303-01A
40. “New White Dev 75 infrastructure”, PwC Threat Intelligence, CTO-TIB-20211015-01A
41. “When Best Practice Isn’t Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users”, Amnesty, https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/ (19/12/2018)
42. “Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa”, Amnesty International, https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/ (16/8/2019)



Vigilância doméstica do Yellow Garuda

O Yellow Garuda (também conhecido como Charming Kitten, PHOSPHORUS, ITG18) é um agente de ameaças versátil com base no Irã que está ativo desde pelo menos 2012. Ele foi muito ativo ao longo de 2021, realizando uma série de atividades com capacidade de vigilância.

Encontramos evidências de que o Yellow Garuda realizou uma campanha de vigilância doméstica direcionada para extrair dados da conta do Telegram de uma vítima.[43] Isso incluiu a exfiltração de mensagens, arquivos de mídia, detalhes de associações a grupos e contatos da vítima. Entre setembro e outubro de 2021, o agente de ameaças comprometeu pelo menos seis vítimas no Irã, de acordo com dados obtidos pela PwC, além de cópias da ferramenta de "captura" personalizada do agente, que foi usada para exfiltrar os dados das contas das vítimas. Também descobrimos um relatório operacional escrito pelo próprio agente de ameaças sobre a vigilância de uma sétima vítima doméstica. Os dados dessa vítima eram mais extensos e provavelmente resultado de exfiltração via *malware* móvel.

A adição de *malware* móvel no conjunto de ferramentas do Yellow Garuda foi relatada em código aberto[44] e se correlaciona com nossa própria análise de uma amostra de *malware* do Android com vários links para a infraestrutura conhecida do Yellow Garuda no início de 2021.[45] Essa amostra foi mascarada como o aplicativo de mensagens WhatsApp e incluiu a capacidade de gravar áudio e vídeo, tirar fotos, acessar contatos, dados de localização e SMS e iniciar chamadas. Sua funcionalidade e base de código eram semelhantes a uma amostra mais antiga de *malware* para Android de 2018. Ela teria sido usada para atingir cidadãos iranianos, o que indica que o Yellow Garuda provavelmente dispõe desse recurso há algum tempo.

43. "Yellow Garuda's VIP Telegram tool", PwC Threat Intelligence, CTO-TIB-20220110-01A
44. UNC788: IRAN'S DECADE OF CREDENTIAL HARVESTING AND SURVEILLANCE OPERATIONS, VB2021 localhost, https://vblocalhost.com/uploads/VB2021-Haeghebaert.pdf (Outubro/2021)
45. "A fresh bouquet of malware", PwC Threat Intelligence, CTO-TIB-20210511-02A

02 |

Crime cibernético

Ransomware

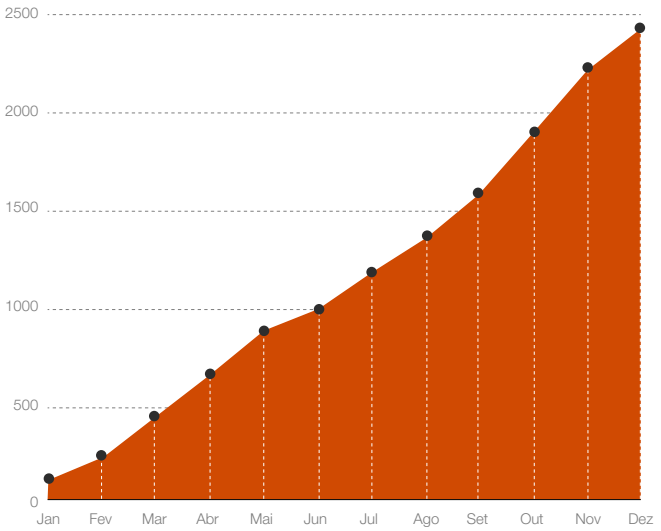
O *ransomware* continuou sendo a ameaça cibernética mais importante enfrentada pela maioria das organizações em 2021. Os fatores que levam à tendência atual continuam aplicáveis, e muitos foram ampliados de acordo com as seguintes observações:

- O número de agentes de ameaças envolvidos em operações de *ransomware* aumentou, graças à proeminência crescente dos acordos de *Ransomware-as-a-Service* (RaaS) e esquemas de afiliados;
- O ritmo e a frequência dos ataques divulgados publicamente quase dobraram; e
- O vazamento de dados roubados, ou a ameaça de vazá-los, tornou-se um procedimento padrão para a maioria dos agentes de ameaças de grande repercussão, adicionando riscos de privacidade, regulatórios e de reputação à crise nos negócios causada pela criptografia de dados.

A esmagadora maioria dos incidentes de *ransomware* teve motivação financeira. Um conjunto limitado de ataques provavelmente teve motivação política e intenções destrutivas.

Em 2020, aproximadamente 1.300 vítimas de *ransomware* tiveram seus dados expostos em sites de vazamento. O número quase dobrou em 2021, com 2.435 vítimas expostas.

Figura 2: Total acumulado de vazamentos de *ransomware* em 2021

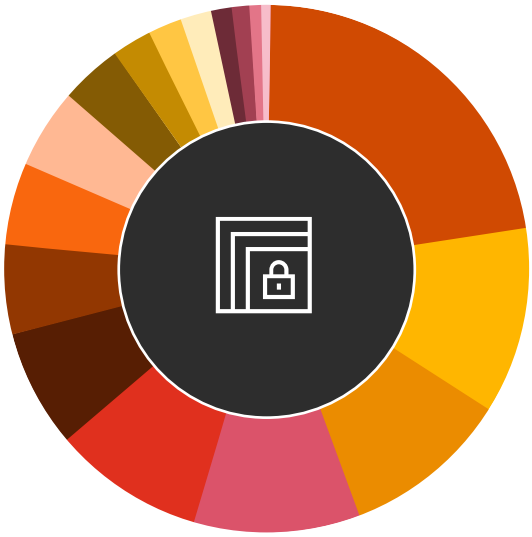


Fonte: PwC

2.435

vítimas foram expostas em sites de vazamento, quase o dobro do número de exposições de 2020

Figura 3: Incidentes de *ransomware* no primeiro trimestre de 2021

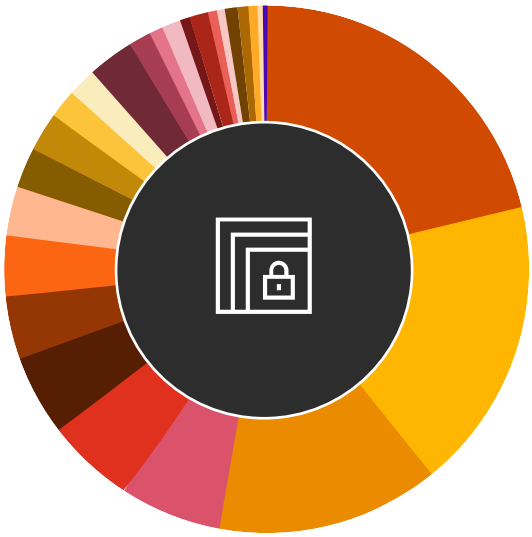


Fonte: PwC

O número de agentes de ameaças envolvidos em operações de *ransomware* oscilou, com alguns elementos de destaque fazendo pausas, se desligando completamente ou ressurgindo sob uma nova "marca" após um período de inatividade, conforme detalhado nas seções a seguir. Por exemplo, no primeiro trimestre de 2021, a PwC observou que 17 agentes de ameaças vazaram dados sobre aproximadamente 440 vítimas, mas 65% desses ataques foram atribuídos apenas a cinco agentes:

- White Onibi (também conhecido como Conti) – 23%
- White Dev 70 (também conhecido como Avaddon) – 12%
- White Apep (também conhecido como DarkSide) – 10%
- White Ursia (também conhecido como Sodinokibi, REvil) – 10%
- Blue Lelantos (também conhecido como DoppelPaymer) – 10%

Figura 4: Incidentes de *ransomware* no segundo trimestre de 2021



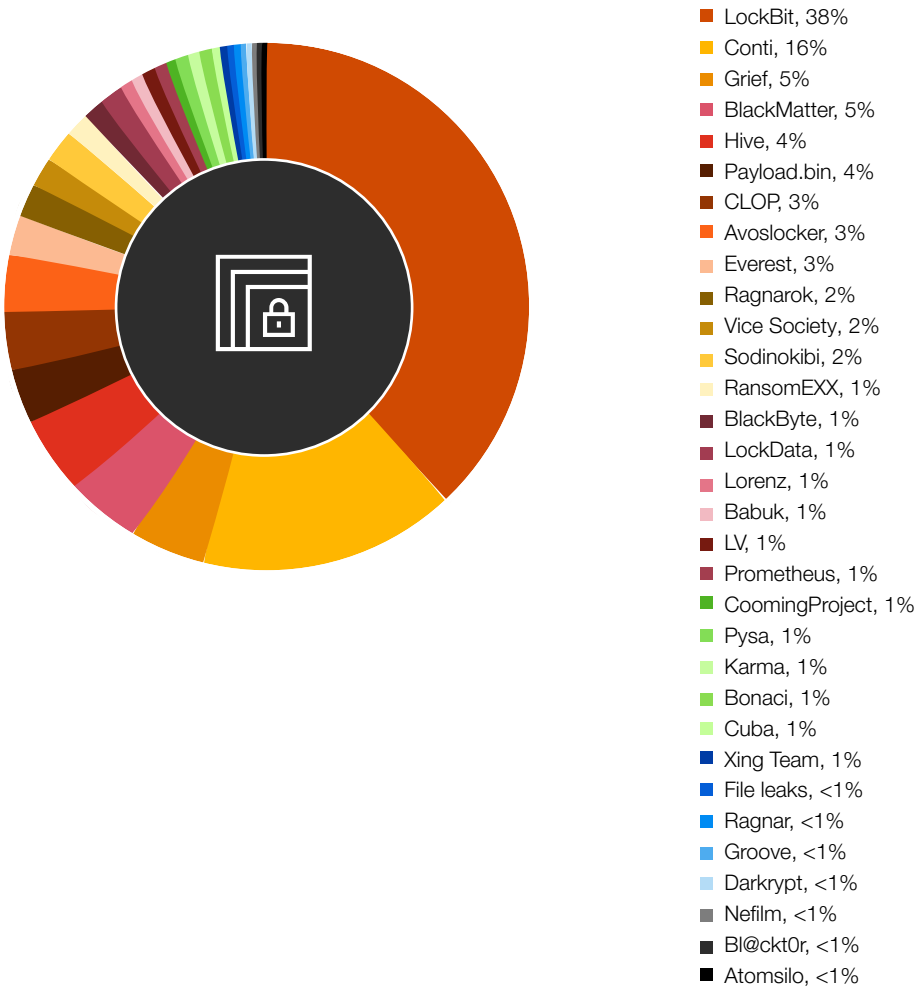
Fonte: PwC

No segundo trimestre de 2021, o número de agentes de ameaças observados em operações de *ransomware* aumentou para 27, e o número correspondente de vítimas foi superior a 500. No entanto, a atividade foi novamente dominada por um pequeno número de famílias de *ransomware*, com aproximadamente 60% dos incidentes atribuíveis apenas a quatro operações:

- Conti – 22%
- Avaddon – 18%
- REvil – 13%
- DarkSide – 6%

Avaliamos que a significativa redução nas operações do DoppelPaymer no segundo trimestre de 2021 se deveu provavelmente ao fato de o agente de ameaças ter renomeado suas operações antes de introduzir a variante de *ransomware* conhecida como “Grief”.

Figura 5: Incidentes de *ransomware* no terceiro trimestre de 2021



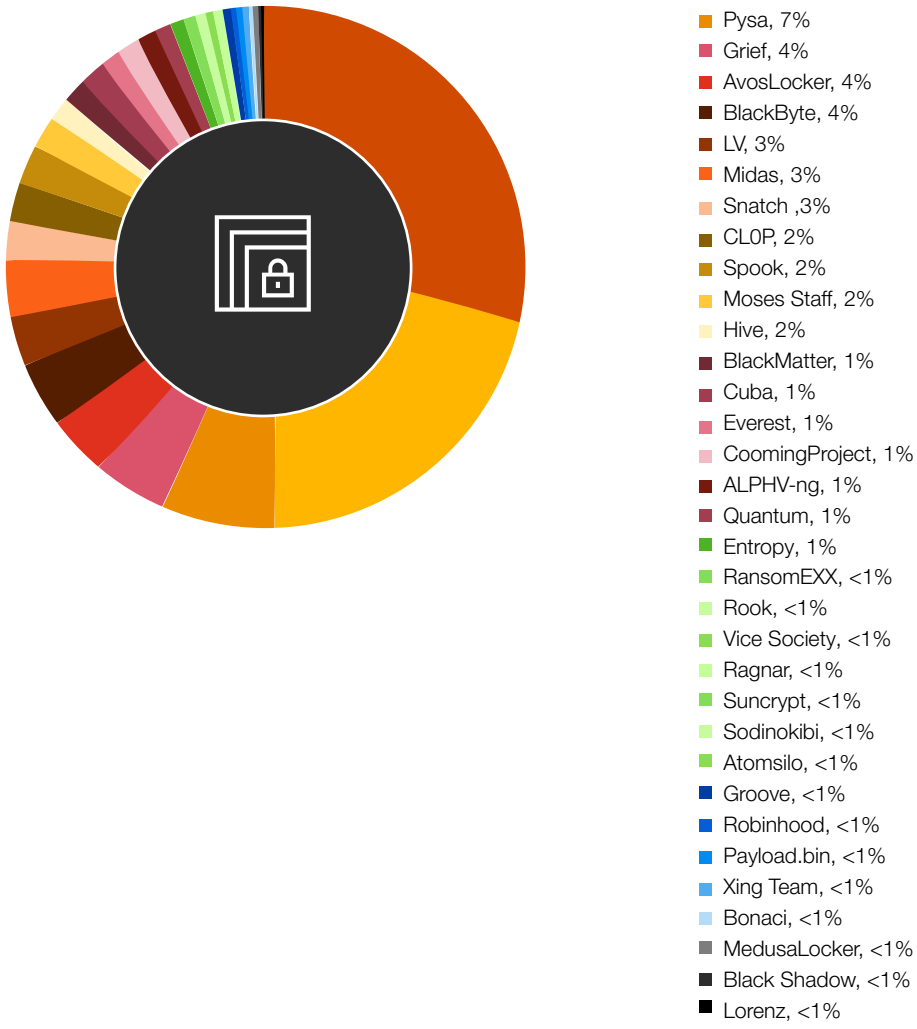
Fonte: PwC

No terceiro trimestre de 2021, mudanças significativas no mercado de *ransomware* começaram a produzir efeito. Elas foram causadas pela expulsão de programas afiliados de seus principais sites de recrutamento e pela dissolução voluntária de algumas operações após ataques de grande repercussão. No entanto, o evento de mais impacto no mercado de *ransomware* durante esse período foi o ressurgimento do White Janus (também conhecido como LockBit), em julho de 2021, como LockBit 2.0. O programa de afiliados original do LockBit ficou inativo no fim de 2020 e ressurgiu apenas em julho de 2021, no fórum criminal RAMP, enquanto o White Janus reformulava seu *ransomware*.[46]

O agente de ameaças rapidamente estabeleceu uma operação de ritmo acelerado, respondendo por quase 40% dos incidentes observados no terceiro trimestre. Isso resultou provavelmente da atração de afiliados de outros esquemas de *ransomware* fechados no fim do segundo trimestre ou início do terceiro. No total, 32 agentes de ameaças vazaram dados de quase 600 vítimas no terceiro trimestre, com 64% dos incidentes novamente atribuíveis a apenas quatro operações de *ransomware*:

- LockBit – 38%
- Conti – 16%
- BlackMatter – 5%
- Grief – 5%

Figura 6: Incidentes de *ransomware* no quarto trimestre de 2021



Fonte: PwC

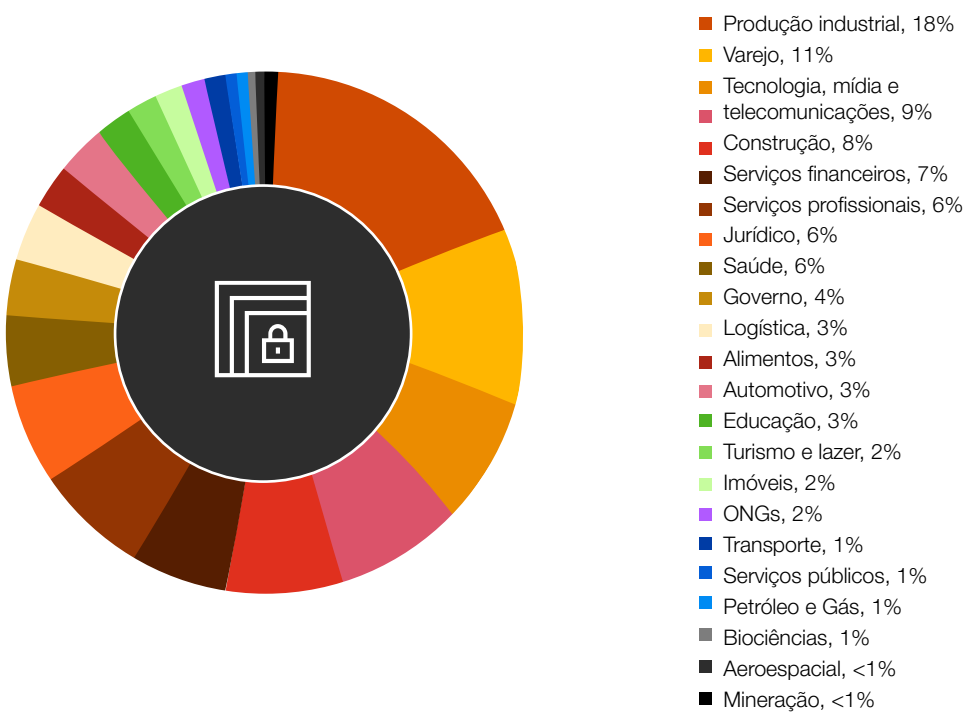
46. "Lockbit 2.0", PwC Threat Intelligence, CTO-TIB-20211027-02A

No quarto trimestre de 2021, o ritmo dos ataques aumentou, com aproximadamente 850 vítimas adicionadas à contagem de incidentes observados. Assim como no trimestre anterior, o número de agentes de ameaças vazando dados cresceu mais uma vez, com 35 sites de vazamento ativos durante o período. LockBit e Conti continuaram dominando, e 64% dos incidentes observados foram atribuídos apenas a cinco atores:

- LockBit – 29%
- Conti – 21%
- White Thalia (também conhecido como Pysa) – 6%
- Grief – 4%
- White Caerus (também conhecido como AvosLocker) – 4%

Um pico na atividade observada do Pysa foi resultado de um influxo de vazamentos de dados em 10 de novembro, causado mais provavelmente pela atualização do site de vazamentos do agente de ameaças, negligenciado, do que pelo aumento nas operações do Pysa no período específico.

Figura 7: Incidentes de *ransomware* por setor em 2021



Fonte: PwC

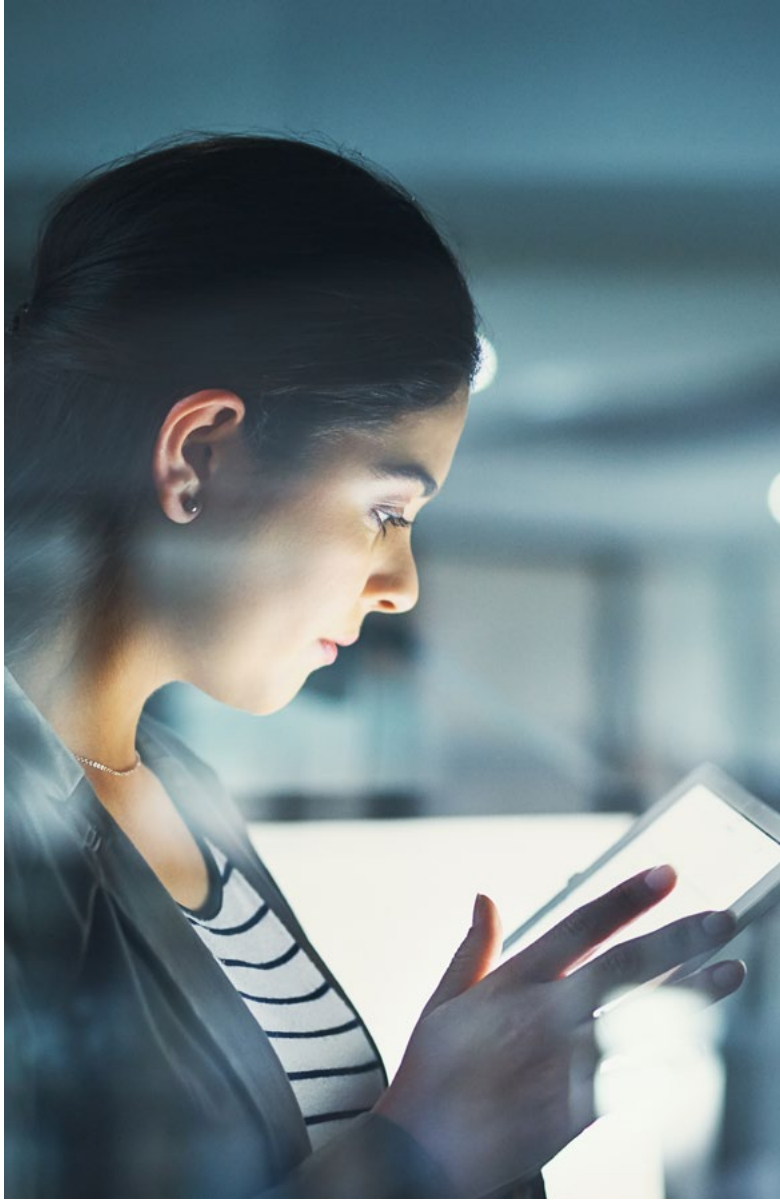
Detalhamento setorial

As operações de *ransomware* são em grande medida indiferentes ao setor econômico das organizações, embora desde que a pandemia começou, muitos agentes de ameaças tenham feito declarações públicas – as quais não mantiveram por completo – de que evitariam atacar hospitais ou outras instalações de saúde. Quando os agentes de ameaças especificaram objetivos de ataque, seu foco foi puramente no tamanho da organização (número de *endpoints*), sua localização geográfica (com ênfase em Canadá, União Europeia, Estados Unidos e Reino Unido) e sua receita.[47] Como em 2020, poucos setores ficaram imunes a violações, mas alguns sofreram ataques com mais frequência do que outros. Os seis principais setores responderam por 60% de todos os incidentes observados:

- Produção industrial – 18%
- Varejo e consumo – 11%
- Tecnologia – 9%
- Construção – 8%
- Serviços financeiros – 7%
- Serviços profissionais – 6%

Os mesmos seis principais setores foram responsáveis por 66% dos incidentes de *ransomware* em 2020.

Não tivemos evidências de que esses setores sejam especificamente visados por agentes de ameaças. No entanto, sem considerar o setor de saúde, esses seis setores coincidem com os seis principais segmentos de indústria por receita nos Estados Unidos.[48] Para alguns dos agentes de ameaças mais ativos – por exemplo, o White Onibi – a receita das vítimas é um fator importante para decidir sobre prosseguir com a atividade de exploração após conseguir acesso inicial. Isso pode ter alguma influência sobre a distribuição das vítimas por setor.



60%

de todos os incidentes observados abrangem seis setores (produção industrial, varejo e consumo, tecnologia, construção, serviços financeiros e serviços profissionais)

47. CTO-TIB-20211209-01A - Nothing else BlackMatters, CTO-TIB-20210827-01A - How to be a ransomware operator
48. "Economy of the United States by sector", Wikipedia, https://en.wikipedia.org/wiki/Economy_of_the_United_States_by_sector

Estudo de caso de resposta a incidentes:

HSE

O sistema de saúde pública da República da Irlanda – *Health Service Executive* (HSE) – encomendou à PwC um relatório sobre um ataque de Conti que interrompeu seus sistemas de TI em maio de 2021. O HSE publicou esse relatório em 10 de dezembro de 2021, estabelecendo uma das primeiras instâncias globais de "divulgação completa" após esse tipo de incidente.[49]

Em 14 de maio de 2021, o *ransomware* Conti foi ativado em mais de 3.500 estações de trabalho e 2.800 servidores do HSE, causando perturbações generalizadas e prolongadas nos serviços de saúde na Irlanda. Algumas unidades de saúde foram incapazes de acessar os dados de pacientes ou agendar consultas por meio de sistemas eletrônicos. As origens do ataque remontam a março de 2021, quando um usuário abriu um anexo malicioso entregue por e-mail. Houve um intervalo significativo entre o acesso inicial à rede e a atividade pós-exploração. Isso resultou provavelmente do fato de o comprometimento inicial ter sido causado por uma operação de acesso como serviço (AaaS, na sigla em inglês), antes que o Conti assumisse o controle do *endpoint* comprometido para avançar no ataque.

O Conti é um sistema de *ransomware* "operado por humanos", implantado com a execução manual de comandos em lote – em vez de um *malware* que se propaga automaticamente por uma rede – criptografando indiscriminadamente qualquer infraestrutura que encontra. A operação do Conti seguiu TTPs conhecidos associados ao agente da ameaça, como a implantação do Cobalt Strike para facilitar o movimento lateral e a elevação de privilégios dentro da rede; o uso de outras ferramentas, como o Mimikatz, para identificar e violar contas e sistemas no nível de administrador, principalmente do Active Directory; e a exfiltração de dados antes da criptografia de arquivos. O impacto do ataque poderia ter sido muito maior se o Conti tivesse sido ativado em sistemas médicos e nos principais ativos de TI da vítima. Muitos dos fatores que contribuíram para a escala e o impacto do incidente não são exclusivos do HSE. O relatório destaca as lições que todas as organizações precisam considerar ao se preparar para um ataque cibernético semelhante e para garantir que poderão mitigar e se recuperar de um evento como esses.

49. https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html

Programas de afiliados

Os programas de afiliados continuaram a ser um motor por trás da escala e do ritmo das operações de *ransomware* em 2021. Esses programas geralmente oferecem acesso a uma gama específica de *ransomware* com base em participação nos lucros. Nesse esquema, um agente principal de ameaças, como White Ursia, é responsável por desenvolver e gerenciar *malware*. Ele fornece acesso a seus afiliados, cujo papel é realizar ataques. Os valores extorquidos das vítimas são divididos entre os operadores de *ransomware* e seus afiliados em acordos prévios de participação nos lucros. Isso permite que agentes de ameaças com habilidades de invasão e exploração de redes tenham acesso a recursos de *ransomware* e monetização que não poderiam desenvolver facilmente, o que reduz as barreiras de entrada.

Muitas das operações de *ransomware* mais prolíficas, como DarkSide, REvil e LockBit, abriram esquemas de afiliados de *ransomware*; outros, como Conti, recrutaram "pentesters" sem especificar seus objetivos finais. Os programas de afiliados foram promovidos principalmente em fóruns criminais de língua russa, como Exploit e XSS. Como o número e a qualidade dos afiliados eram um fator determinante na receita gerada por muitas operações de *ransomware*, a competição entre esquemas rivais se intensificou. Agentes de ameaças reforçaram seu perfil ao:

- depositar grandes somas de criptomoedas em suas contas do fórum, para demonstrar o sucesso financeiro de seu esquema;
- realizar entrevistas promovendo o sucesso e a receita de suas operações, muitas das quais atraíram cobertura positiva nos fóruns criminais onde recrutaram afiliados;
- postar links para reportagens sobre suas operações;
- oferecer acordos competitivos de participação nos lucros aos seus recrutas; e
- alegar superioridade técnica sobre seus concorrentes.

Figura 8: Anúncio de recrutamento de afiliados do DarkSide

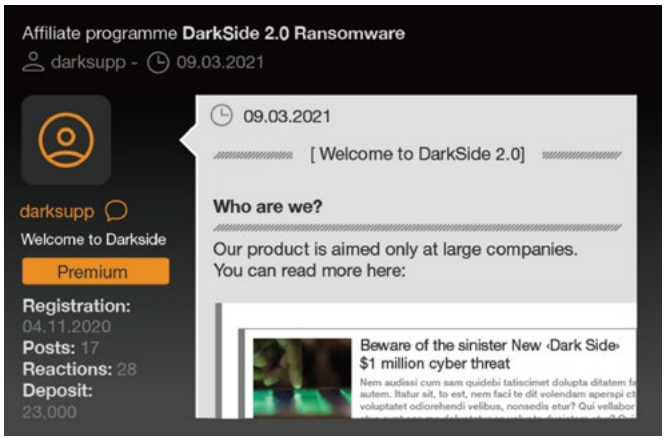


Figura 9: REvil

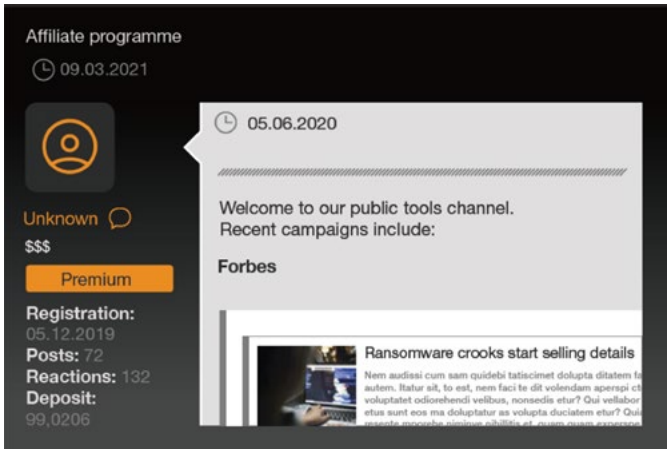


Figura 10: Anúncio do LockBit 2.0 alegando desempenho técnico superior em relação aos esquemas rivais

Encryption speed comparative table for some ransomware - 02.08.2021

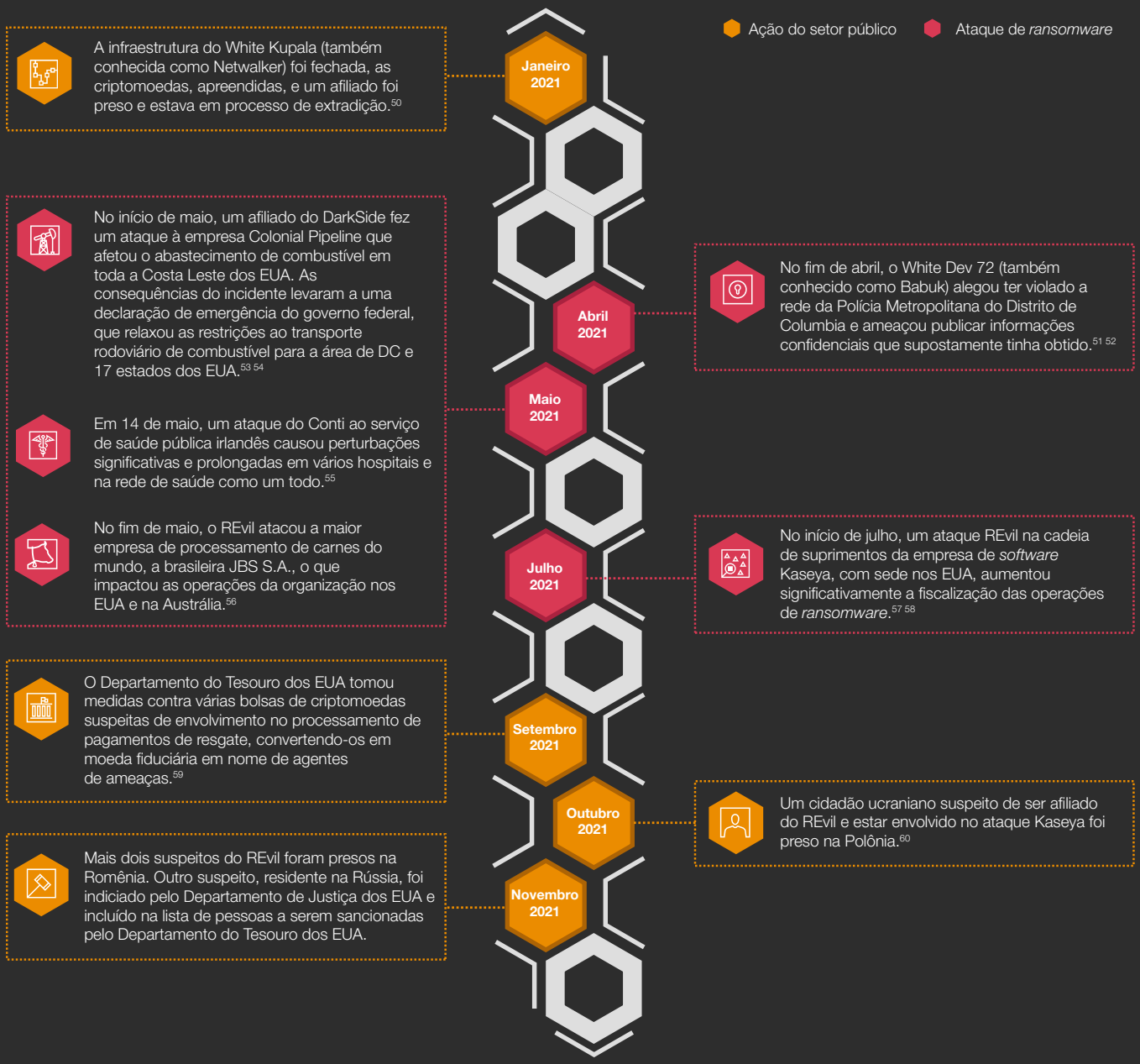
PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109909
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797

Um tema político: resposta legal e regulatória

Uma série de incidentes que afetaram principalmente organizações dos EUA no primeiro semestre de 2021 elevou significativamente o perfil do *ransomware*:

Figura 11: Linha do tempo de ataques de *ransomware* de grande repercussão e ação do setor público



50. "Department of Justice Launches Global Action Against NetWalker Ransomware", US Department of Justice, https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware, 27th January 2021
51. "Babuk - A new kid on the block", PwC Threat Intelligence, CTO-TIB-20210201-02A
52. "Ransomware gang leaks data from Metropolitan Police Department", BleepingComputer: Sergiu Glatan, https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-from-metropolitan-police-department/ (11/5/2021)
53. "DarkSide", PwC Threat Intelligence, CTO-QRT-20210512-01A
54. "Hackers Breached Colonial Pipeline Using Compromised Password", Bloomberg: William Turton, Kartikay Mehrotra, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password (4/6/2021)
55. "Ransomware Attack on Health Sector - UPDATE 2021-05-16", Ireland National Cybersecurity Centre, https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf (16/5/2021)
56. "JBS: Cyber-attack hits world's largest meat supplier", BBC, https://www.bbc.co.uk/news/world-us-canada-57318965 (2/6/2021)
57. "Kaseya supply chain compromise", PwC Threat Intelligence, CTO-QRT-20210703-01A
58. "Important Notice August 4th, 2021", Kaseya, https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-August-4th-2021 (4/8/2021)
59. "Treasury Takes Robust Actions to Counter Ransomware", US Department of Treasury, https://home.treasury.gov/news/press-releases/jy0364, 21/9/2021
60. "Ukrainian Arrested and Charged with Ransomware Attack on Kaseya", US Department of Justice, https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya, 8/11/2021

Expulsão em massa de esquemas de afiliados

O aumento do foco e da pressão sobre os sistemas de *ransomware*, especialmente em consequência do incidente da Colonial Pipeline, teve impacto imediato nos esquemas de afiliados. Em 14 de maio, os administradores do fórum criminal XSS excluíram postagens relacionadas a:

- recrutamento de esquema de afiliados;
- o aluguel de *ransomware*; e
- a venda de *software* de *locker* (*ransomware*).

Os administradores citaram várias razões para suas ações, mas uma questão-chave foi o fato de o *ransomware* ter se tornado "perigoso e tóxico… e estar sendo associado a geopolítica e ataques patrocinados por países". O outro fórum principal onde os esquemas de afiliados estavam operando, o Exploit, também seguiu o exemplo, citando razões semelhantes para sua própria proibição.[61]

A proibição de esquemas de afiliados não resultou na expulsão de agentes de ameaças de *ransomware* dos próprios fóruns, embora alguns tenham se retirado. Por exemplo, o White Ursia anunciou que fecharia seu esquema de afiliados REvil e o "tornaria privado". Depois, cancelou completamente suas participações no fórum. O White Apep anunciou que encerraria a operação de *ransomware* DarkSide e liberou chaves de descriptografia para o *malware*.[62] Outros, no entanto, como o White Janus (também conhecido como LockBit), mantiveram sua participação e simplesmente transferiram as atividades de recrutamento de afiliados para seu site de vazamento.

Figura 12: Administração do XSS proíbe atividades de *ransomware* no site

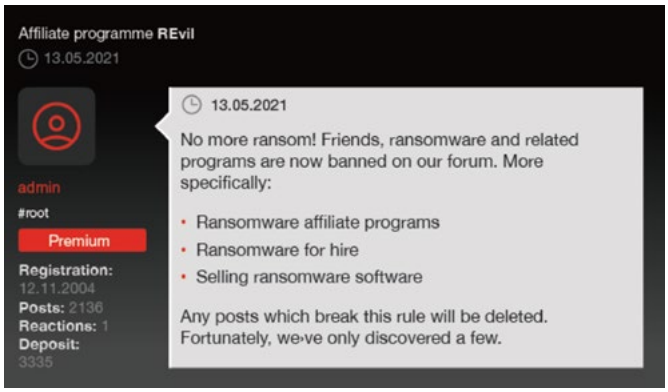


Figura 13: Administração do Exploit faz o mesmo

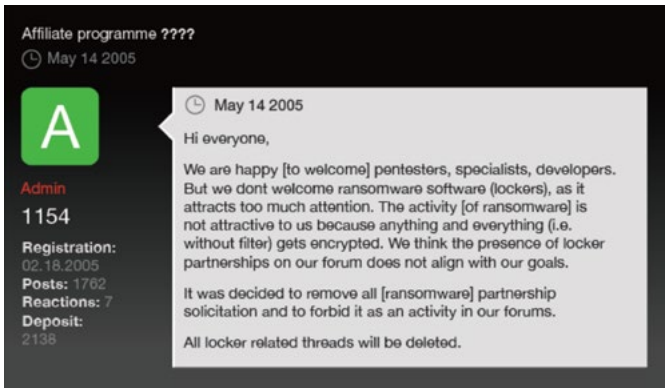
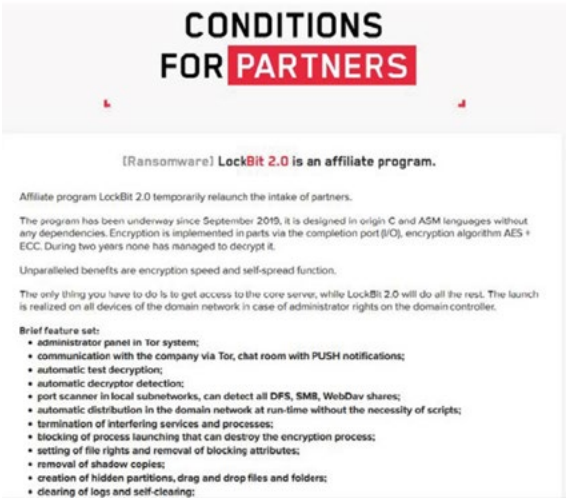


Figura 14: Anúncio de recrutamento de afiliados no site de vazamento do White Janus



61. "Ransomware gets more ban for its buck", PwC Threat Intelligence, CTO-SIB-20210525-01A
62. "DarkSide", PwC Threat Intelligence, CTO-QRT-20210512-01A

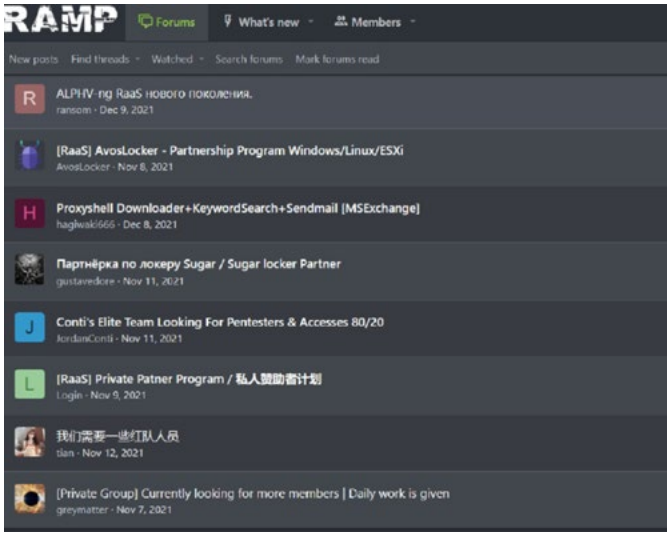
Embora os esquemas abertos de recrutamento de afiliados tenham sido alvo da proibição, o recrutamento de “pentesters” continuou sem grandes perturbações, com anúncios nas seções de pesquisa de trabalho ou freelance do Exploit e do XSS não afetados em grande medida. Os anúncios não declaravam abertamente que o recrutamento estava sendo feito para operações de *ransomware*, mas as especificações de trabalho para muitos dos cargos vagos tinham semelhanças com campanhas anteriores de recrutamento de esquemas de afiliados.

Figura 15: Anúncio de recrutamento de Pentester por agente de ameaça não identificado

Surge o RAMP

Em resposta às proibições do fórum para recrutamento de afiliados, em meados de julho foi criado um fórum criminoso que alegava atender especificamente às necessidades de operações de *ransomware* e programas afiliados. O site operava no início a partir do endereço da *dark web* usado antes pelo White Dev 72 (também conhecido como Babuk) para seu site de vazamento e se chamava RAMP, possivelmente em referência a um site da *dark web* anterior, em russo, envolvido na venda de drogas. O fórum tem uma seção especificamente dedicada a esquemas RaaS, além de anúncios de recrutamento de pentesters e acesso a redes corporativas. Entre os esquemas de *ransomware* conhecidos atualmente ativos no RAMP estão Conti, AvosLocker e BlackCat.

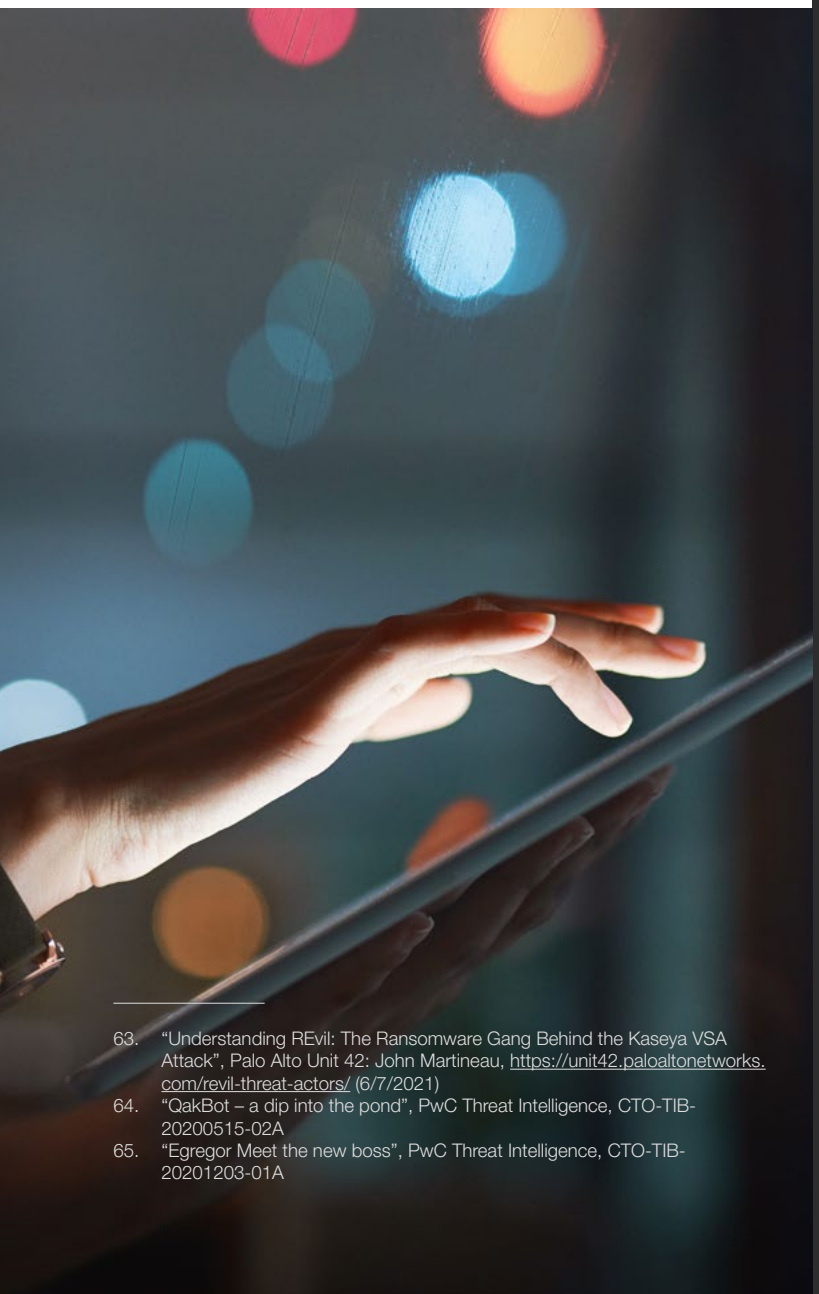
Figura 16: Anúncios de recrutamento de afiliados no fórum RAMP



Mudanças de marca no *ransomware*

Como outra consequência provável do aumento da pressão legal e política, observamos em 2021 um dos movimentos mais intensos de mudança de marca no *ransomware* nos últimos anos. Essas iniciativas têm três benefícios principais:

- permitir que os agentes de ameaças de crimes cibernéticos consagrados "reinicializem" seus programas após um revés (por exemplo, após a descoberta de uma falha na rotina de criptografia de seu *ransomware* resultar na publicação de um "descriptografador" para o *malware*);
- esconder-se ou reduzir a atenção sobre um grupo específico após uma quantidade significativa de atividades ou campanhas e,
- impedir ou atrasar a atribuição de ataques, quando o agente da ameaça perceber que isso representa uma vantagem operacional.



63. "Understanding REvil: The Ransomware Gang Behind the Kaseya VSA Attack", Palo Alto Unit 42: John Martineau, https://unit42.paloaltonetworks.com/revil-threat-actors/ (6/7/2021)
64. "QakBot – a dip into the pond", PwC Threat Intelligence, CTO-TIB-20200515-02A
65. "Egregor Meet the new boss", PwC Threat Intelligence, CTO-TIB-20201203-01A

Estudo de caso de resposta a incidentes:

HSE

Em fevereiro de 2021, a equipe de resposta a incidentes da PwC respondeu a um ataque de Sodinokibi/REvil a uma organização francesa do setor agrícola. A invasão começou em meados de janeiro, quando um anexo malicioso, entregue aos funcionários da empresa por meio de um e-mail de *phishing*, instalou o QakBot na estação de trabalho da vítima.

Após obter acesso, o agente da ameaça implantou o Cobalt Strike para fortalecer sua presença no ambiente da vítima. Ele também começou a acessar as credenciais LSASS, usando o Windows Remote Desktop Protocol (RDP) para se mover lateralmente pela rede. O agente da ameaça usou uma combinação de trabalhos BITS, PowerShell e interação de linha de comando para instalar e executar cargas úteis e rastrear identidades digitais da rede. O RClone, software de código aberto usado para gerenciar conteúdo em sistemas de armazenamento em nuvem, foi usado para exfiltrar dados dos armazenamentos da vítima no local e em nuvem, antes que o *ransomware* fosse detonado.

Embora o agente da ameaça tenha implantado o *ransomware* Sodinokibi/REvil, sua maneira de operar no ambiente da vítima se assemelhava mais às técnicas adotadas por afiliados de outro programa de *ransomware* que a PwC rastreia como White Samyaza (também conhecido como Egregor ou Prolock). Por exemplo, embora o QakBot também tenha sido observado como fonte de infecções pelo REvil,[63] ele está mais fortemente associado a operações do White Samyaza.[64] A ferramenta de linha de comando RClone costuma ser usada, embora não exclusivamente, pelos operadores Egregor/Prolock, em especial com a renomeação do utilitário como "svchost.exe" para se integrar ao ambiente da vítima.[65] Além disso, os arquivos de *ransomware* observados durante a resposta ao incidente foram rotulados com o nome da vítima. Esse esquema de nomenclatura é uma característica exclusiva do *ransomware* Egregor e normalmente não é observado no *ransomware* Sodinokibi/REvil (cujos arquivos geralmente são nomeados de acordo com um esquema de nomenclatura aleatório).

Com base nos dados que examinamos, acreditamos ser altamente provável que um afiliado do White Samyaza tenha se transferido para o White Ursia e implantado o Sodinokibi/REvil usando TTPs geralmente observados em afiliados do White Samyaza.

Blue Lelantos

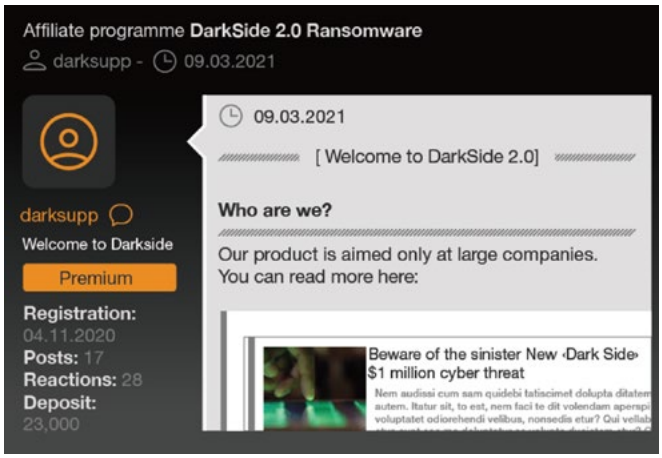
Em dezembro de 2019, membros do grupo criminoso russo Evil Corp (rastreado pela PwC como Blue Lelantos) foram indiciados pelas autoridades dos EUA e designados para sanções.[66] As operações do Evil Corp continuaram ao longo de 2020, mas as mudanças nas suas operações se tornaram aparentes no fim do ano e cada vez mais perceptíveis no início de 2021. As detecções do WastedLocker,[67] um dos principais sistemas de *ransomware* do Evil Corp, praticamente desapareceram no fim de 2020. No entanto, a operação do WastedLocker continuou ao longo de 2021, por meio de uma sucessão de mudanças de nome. Os pedidos de resgate do WastedLocker começaram a aparecer como *ransomware* Hades no fim de 2020; Phoenix Cryptolocker em março de 2021; Payloadbin em junho; e Macaw em outubro.[68]

Da mesma forma, a DoppelPaymer,[69] operação de "dupla extorsão" do Evil Corp de grande destaque na mídia, encerrou suas operações em maio, com a última vítima adicionada ao site de vazamento naquele mês. Em junho, surgiu um novo *ransomware* autodenominado Grief ou PayorGrief, que logo começou a postar dados de vítimas em seu site de vazamento. A análise de amostras do Grief revelou fortes semelhanças de código com o DoppelPaymer. A principal diferença é o uso da criptomoeda Monero pelo Grief para pagamentos de resgate. Avaliamos que o Grief é mais um exercício de *rebranding* do Evil Corp, e é improvável que seja o último.[70]

Embora não tenhamos comprovação direta dos motivos dos exercícios sucessivos de *rebranding* feitos pelo Evil Corp em 2021, avaliamos como altamente provável que eles sejam resultado da designação do grupo como entidade sancionada pelas autoridades dos EUA:

- Como na maior parte das operações de *ransomware*, a maioria das vítimas está nos EUA;
- Uma organização que faça ou facilite um pagamento de resgate a uma entidade sancionada poderia violar as sanções dos EUA e, portanto, estaria menos propensa a pagar;
- O *rebranding* do WastedLocker e do DoppelPaymer tornou mais difícil, pelo menos no curto prazo, atribuir um incidente de *ransomware* a uma entidade sancionada; e
- Reformular o código existente, em vez de escrever novas variantes de *ransomware* do zero, reduz os custos de oportunidade do Evil Corp e o tempo necessário para manter suas operações de *ransomware*.

Figura 17: Postagem de anúncio "Bem-vindo ao Darkside 2.0"



66. "Rezident evil: Dridex indictments", PwC Threat Intelligence, CTO-SIB-20200102-01A
67. "WastedLocker – EvilCorp's new smoking gun", PwC Threat Intelligence, CTO-TIB-20200730-01A
68. "New World, New Macaw", PwC Threat Intelligence, CTO-QRT-20211117-01A
69. "A new DoppelPaymer", PwC Threat Intelligence, CTO-TIB-20200710-01A
70. "Causing more Grief", PwC Threat Intelligence, CTO-TIB-20211028-01A

White Apep

O DarkSide (também conhecido como BlackMatter), que a PwC monitora como White Apep, está em operação desde pelo menos agosto de 2020 e já havia passado por dois movimentos de *rebranding* até o fim de 2021. O primeiro veio em janeiro de 2021, dois meses após o lançamento do programa de afiliados do DarkSide, quando a empresa de segurança Bitdefender desenvolveu e lançou publicamente uma ferramenta de descriptografia[71] para que as vítimas do DarkSide recuperassem seus arquivos. As operações do White Apep foram interrompidas, provavelmente para que o agente da ameaça se reorganizasse, e só foram retomadas em 9 de março de 2021 sob a nova marca DarkSide 2.0. O retorno foi acompanhado pelo relançamento do seu programa de afiliados e apresentou uma versão atualizada do *ransomware*, criada para evitar a descriptografia pelas ferramentas existentes.[72]

Foi após esse primeiro *rebranding* que um dos afiliados do DarkSide executou um dos incidentes mais prejudiciais observados em 2021, o ataque bem-sucedido à empresa americana Colonial Pipeline em 7 de maio. O ataque levou à paralisação das operações em um oleoduto de quase 9 mil quilômetros de extensão usado para fornecer quase metade do combustível da Costa Leste dos EUA. O foco crescente do governo americano no DarkSide e o desmantelamento subsequente da infraestrutura levaram o agente de ameaças a anunciar, em meados de maio, que encerraria suas operações.[73]

O segundo *rebranding* do White Apep veio no fim de julho, na forma de um novo sistema RaaS denominado BlackMatter. O novo *ransomware* compartilhava partes de seu código com o DarkSide 2.0. Isso incluía rotinas de código que implementavam elevação de privilégios, identificação de identidade das vítimas e recursos de rede.[74]

A pressão crescente da repressão ao crime levou o White Apep mais uma vez a anunciar sua saída da cena do *ransomware* em novembro de 2021. A decisão foi logo seguida pelo anúncio de uma recompensa de US$ 10 milhões do Departamento de Justiça dos EUA por qualquer informação sobre o grupo.[75] No fim de 2021, as operações do White Apep permaneciam inativas. No entanto, dado o número de transformações que o *ransomware* e as operações gerais do White Apep sofreram, avaliamos que há uma probabilidade realista de que essa interrupção das operações represente uma chance de permanecer fora do radar, apenas para ressurgir com mais uma nova marca. Há indícios circunstanciais de que o ALPHV-ng (também conhecido como BlackCat), que atualmente é monitorado pela PwC como White Dev 101, é mais uma nova marca. O esquema de afiliados do agente de ameaças foi lançado no RAMP em 9 de dezembro de 2021, e a equipe de resposta a incidentes da PwC respondeu a vários incidentes do BlackCat conduzidos por um afiliado específico que antes fazia parte do esquema BlackMatter.

71. "Darkside Ransomware Decryption Tool", Bitdefender, https://www.bitdefender.com/blog/labs/darkside-ransomware-decryption-tool/ (11/1/2021)
72. "Darkside", PwC Threat Intelligence, CTO-QRT-20210512-01A
73. "DarkSide, Blamed for Gas Pipeline Attack, Says It is Shutting Down" New York Times, https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html (14/5/2021)
74. "Nothing else BlackMatters", PwC Threat Intelligence, CTO-TIB-20211209-01A
75. "Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice", US Department of State, https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/ (4/11/2021)

White Ursia

O White Ursia foi um dos agentes de ameaças de *ransomware* mais ativos no primeiro semestre de 2021. A face pública de sua operação, usando as identidades on-line UNKN e "Unknown" no Exploit e XSS, respectivamente, teve grande repercussão, com a realização de entrevistas e a promoção do programa de afiliados do REvil. É provável que a pressão crescente sobre o White Ursia, com o agente se vendo alvo de vigilância maior após os ataques da Kaseya e do JBS, tenha dado início a seu primeiro movimento off-line em 2021. O UNKN já havia anunciado a decisão de "desaparecer" após a expulsão de programas afiliados de XSS e Exploit em maio. O "Happy Blog" do White Ursia, site de vazamento usado para publicar dados de vítimas, passou a ficar off-line em meados de julho, assim como sua infraestrutura de pagamento de resgates. As operações do REvil foram interrompidas, e o "UNKN" não postou mais comentários sobre XSS ou Exploit após 4 de julho. O desligamento da infraestrutura de pagamento do REvil e o sumiço do UNKN mancharam a reputação do agente de ameaças.

Em setembro, novas personas on-line – "REvil" no Exploit e "0_neday" no XSS – anunciaram, após o sumiço do "UNKN", ter conseguido restaurar as operações do REvil a partir de backups. O White Ursia retomou as operações e postou dados sobre seis vítimas entre 10 de setembro e 14 de outubro, antes que o site fosse derrubado de novo, desta vez provavelmente para sempre. O '0_neday' alegou ter perdido o controle da infraestrutura do REvil após um ataque cibernético suspeito que teve como alvo o agente de ameaças pessoalmente e decidiu ficar na surdina. Em 14 de janeiro de 2022, o Serviço Federal de Segurança (FSB) da Rússia anunciou a detenção de 14 suspeitos e buscas em 25 locais relacionados a uma investigação sobre a operação REvil.[76] Embora pelo menos algumas das prisões tenham ocorrido no início de 2022, é bastante provável que elementos da operação REvil tenham sido desbaratados pelas autoridades russas antes da ação realizada em janeiro de 2022. Vários agentes de ameaças criminosos no XSS especularam que o sumiço do UNKN em julho e o fim subsequente de suas comunicações foi resultado da ação do FSB. No entanto, é impossível confirmar essas alegações.

Comprometimento da cadeia de suprimentos: o novo normal

Ataques à cadeia de suprimentos têm sido uma fórmula testada e comprovada usada por vários agentes de ameaças. Embora sejam tradicionalmente associados a agentes de ameaças patrocinados por nações, os agentes com motivação financeira também foram bem-sucedidos em explorá-los. No início de 2021, o White Austaras (também conhecido como TA505), que controla o *ransomware* CL0P, conseguiu expor a ameaças várias organizações que usavam o software de transferência de arquivos legado Accellion FTA. O White Austaras exfiltrou dados de pelo menos 25 vítimas e exigiu um resgate para não os expor no site de vazamento do CL0P.[77] [78]

Em julho de 2021, o White Ursia colocou em risco várias organizações que eram clientes do Kaseya, uma empresa americana especializada em software de gerenciamento de redes e TI, ao manipular o software VSA da empresa para fornecer cargas maliciosas. O ataque alcançou uma escala muito maior do que o incidente Accellion, com 1.400 organizações afetadas pelo *ransomware* REvil/Sodinokibi.[79]

76. "Moscow court arrests all REvil ransomware hackers detained after FBI request to Russia", TASS, https://tass.com/russia/1388649 (15/1/2022)
77. "Exploitation of Accellion File Transfer Appliance", Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/uscert/ncas/alerts/aa21-055a, 24/2/2021
78. "Accellion Provides Update to FTA Security Incident Following Mandiant's Preliminary Findings", Accellion, https://www.globenewswire.com/news-release/2021/02/22/2179666/0/en/Accellion-Provides-Update-to-FTA-Security-Incident-Following-Mandiant-s-Preliminary-Findings.html (22/2/2021)
79. "Kaseya supply chain compromise", PwC Threat Intelligence, CTO-QRT-20210703-01A

Distribuição e acesso

Sistemas de distribuição

Os sistemas de distribuição de *malware* se mostraram um complemento vital dos arsenais de agentes de ameaças de *ransomware*. Trata-se de softwares projetados especificamente para abrigar cargas maliciosas, que são posteriormente descartadas pelo agente de ameaças para conseguir acesso a um sistema ou rede. Em 2021, com *players* estabelecidos e novos participantes ativos no mercado de distribuição de *malware*, os agentes de ameaças cibernéticas puderam alternar entre várias opções e identificar a mais confiável para suas operações.

Emotet

O Emotet, que a PwC monitora como White Taranis, é um dos sistemas de distribuição de *malware* mais antigos e proeminentes. No início de 2021, houve uma operação internacional, chamada LadyBird, de desmantelamento da infraestrutura de *botnets* do Emotet. Com mais de 700 dispositivos usados para os sistemas C2 do Emotet apreendidos, além de prisões feitas na Ucrânia,[80] [81] foi possível impedir que o agente de ameaças realizasse suas campanhas de *spam* malicioso e *spear phishing* durante quase todo o ano.

No entanto, em meados de novembro, a PwC observou o Trickbot, o *trojan* bancário operado pelo grupo que a PwC monitora como White Magician, distribuindo binários Emotet maliciosos para máquinas Trickbot infectadas e executando-os na memória. Essa provavelmente foi uma tentativa de ajudar a restaurar a infraestrutura de comando e controle do Emotet. Essa técnica está alinhada com atividades semelhantes associadas ao White Taranis, onde o Emotet foi usado como um meio para ajudar a distribuir binários do Trickbot após uma derrubada semelhante do Trickbot em outubro de 2020.

Além da distribuição de binários Emotet e do retorno de sua infraestrutura de comando e controle, também observamos a entrada em operação de dois novos servidores de *botnets* de distribuição de spam, Epoch 4 e Epoch 5. Eles foram adicionados a outros três servidores de *botnet*, Epoch 1, Epoch 2 e Epoch 3, usados antes pelo White Taranis para infectar máquinas. Outras atualizações também foram observadas nos recursos de criptografia do Emotet, que são usados para criptografar o tráfego de rede, e em seus protocolos de comunicação.[82] Essas inclusões no arsenal do Emotet destacam os recursos significativos aos quais o White Taranis tem acesso e a ameaça contínua que ele representa para as organizações.

A ausência do Emotet durante a maior parte de 2021 forçou uma parcela importante de sua base de clientes a procurar outras formas de distribuir *malware*. Em 2021, sistemas de distribuição de *malware*, como Buerloader, Bazar, SquirrelWaffle e IcedID, aumentaram sua atividade fortemente, o que talvez tenha sido consequência da lacuna que o Emotet deixou após seu desmantelamento.

IcedID turbinado

O agente de ameaças que a PwC monitora como White Khione está por trás do sistema de distribuição de *malware* IcedID (também conhecido como Bokbot), que está associado a sistemas de *ransomware* de grande repercussão, como Conti e Sodinokibi/REvil. Identificado pela primeira vez em 2017, o IcedID foi originalmente desenvolvido como um *trojan* bancário, capaz de roubar informações financeiras. No entanto, como outros *trojans* bancários, o IcedID foi depois reconfigurado como um *malware* modular projetado para fornecer acesso remoto a redes, o que depois seria vendido a outros usuários como parte do modelo *Access as a Service*.[83] Em 2021, o IcedID reforçou sua capacidade na ausência do Emotet, provando ser um dos mais robustos sistemas de distribuição de *malware*. Sua principal funcionalidade está nas consistentes campanhas de *spam*, que são usadas para iniciar a cadeia de infecção. Entre seus outros recursos, destacam-se a execução remota de código e injeção no navegador da Web, para que o IcedID execute ataques do tipo *person-in-the-middle* com o objetivo de extrair informações financeiras. No entanto, o IcedID é normalmente usado para implantar cargas úteis do próximo estágio, como Cobalt Strike.

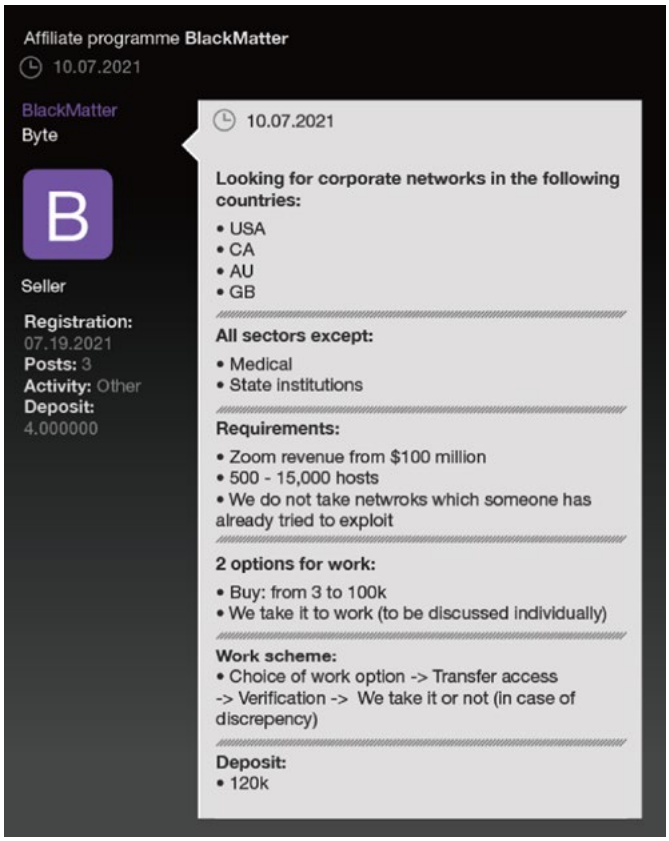
80. "Emotet is back", PwC Threat Intelligence, CTO-QRT-20211116-01A
81. "World's most dangerous malware Emotet disrupted through global action", Europol, https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action (18/11/2021)
82. "How the new Emotet differs from previous versions", Intel 471, "https://intel471.com/blog/emotet-returns-december-2021", 9/12/2021
83. "Colder than IcedID", PwC Threat Intelligence, CTO-TIB-20210511-01A

Access as a Service (AaaS)

Os sistemas de distribuição, como Emotet e IcedID, sempre foram a opção de acesso inicial para muitos agentes de ameaças cibernéticas. No entanto, sua disponibilidade e acessibilidade talvez não sejam confiáveis. Alguns sistemas são forçados a ficar *off-line*, enquanto outros exigem um relacionamento de longa data para acessar os serviços de distribuição de *malware*. Isso deu margem para o crescimento do mercado de *Access as a Service* (AaaS) em 2021. Esses mercados permitem a compra e venda de acesso a *hosts* comprometidos de uma ampla variedade de organizações e setores, geralmente na forma de acesso RDP e VPN, bem como *webshells*. Vários fóruns criminais em russo, como Exploit e XSS, e mercados dedicados, como Odin e MagBo, são usados para anunciar listagens de acesso.[84]

Um fator principal por trás do aumento do AaaS é a menor barreira de entrada que ele oferece para novos agentes de ameaças. O AaaS elimina a necessidade de realizar invasões complexas ou campanhas de *phishing* generalizadas para coletar credenciais. Com o AaaS, a intrusão inicial já foi concluída, o que permite ao comprador fazer a transição direta para a atividade pós-exploração e a implantação de *ransomware*. Em 2021, vimos vários agentes de ameaças de *ransomware* ou seus afiliados usarem AaaS como meio de acesso inicial, incluindo o White Janus (também conhecido como Lockbit 2.0) e o White Apep (também conhecido como BlackMatter ou DarkSide).

Figura 18: O White Apep busca acesso a redes corporativas no fórum Exploit



84. "AaaS you like it", PwC Threat Intelligence, CTO-SIB-202108802-01A

03 |

Atividade regional

Nesta seção, descrevemos campanhas realizadas pelos agentes de ameaças que, segundo nossa avaliação, estão baseados em regiões geográficas específicas. Elas incluem desde operações de coleta de inteligência (em apoio a objetivos políticos e/ou estratégicos nacionais) até atividades com motivação financeira: direcionadas e oportunistas. Como em 2020, continuamos a enxergar o cenário de ameaças cibernéticas alinhado às circunstâncias geopolíticas, com eventos no mundo real influenciando igualmente operações motivadas por espionagem e sabotagem.

Ásia-Pacífico

Impulso de sobrevivência

Na Coreia do Norte, uma peça central da doutrina política de Kim Jong-un é o desenvolvimento contínuo da força nuclear do país, acompanhado de um enfoque nas finanças nacionais. De modo geral, as operações cibernéticas têm sido provavelmente um dos principais meios de o Estado norte-coreano conter o impacto das sanções internacionais e alcançar seus objetivos estratégicos. A criptomoeda, em especial, é uma fonte crucial de renda para o regime da Coreia do Norte, com vários agentes de ameaças no país visando organizações e indivíduos envolvidos com criptomoedas, principalmente bolsas de criptomoedas, desde 2017.[85]

Os mais novos agentes de ameaças da Coreia do Norte

Ao longo de 2021, observamos dois grupos principais de atividade que, em nossa avaliação, muito provavelmente eram conduzidos por agentes de ameaças da Coreia do Norte. Eles visavam entidades que lidam com criptomoedas e o setor financeiro em escala internacional. Inicialmente, monitoramos esses dois grupos em separado, respectivamente como Black Alicanto (também conhecido como Dangerous Password, LeeryTurtle, CryptoMimic, CryptoCore e Operation SnatchCrypto)[86] [87] e Black Dev 2 (também conhecido como Operation Gold Hunting, Operation SnatchCrypto). Por sobreposições em termos de recursos, infraestrutura e vitimologia, acabamos por avaliar que Black Alianto e Black Dev 2 provavelmente são o mesmo agente de ameaças da Coreia do Norte. Avaliamos ainda que esse agente de ameaças é muito provavelmente uma evolução do subgrupo Bluenoroff com motivações financeiras do Black Artemis (também conhecido como Lazarus Group ou HIDDEN COBRA).

A seguir, apresentamos o Black Alicanto e o Black Dev 2 individualmente para fornecer uma visão geral dos diferentes TTPs que associamos aos dois grupos de atividade.

Black Alicanto

O Black Alicanto tem motivação financeira e está ativo desde pelo menos 2018, alvejando organizações e entidades de criptomoedas no setor de serviços financeiros. Embora esse agente de ameaças geralmente usasse como iscas documentos maliciosos relacionados a promoções ou bônus para empregados para induzir alvos a abrir a carga útil, observamos que, entre setembro e dezembro de 2021, o Black Alicanto usou como iscas documentos com descrições de cargos em empresas nos setores de finanças e criptomoedas, como Goldman Sachs, J.P. Morgan, Commerz AG, SALT Lending e Blockchain Intelligence Group.[88]

O Black Alicanto inicialmente envia e-mails de *spear phishing* aos alvos com arquivos compactados anexados. Eles normalmente contêm documentos de extensão dupla (arquivos .LNK disfarçados como documentos do Word ou PDF) ou documentos de isca e arquivos .LNK maliciosos chamados Password.txt.lnk, ambos protegidos por senha. Os arquivos de link exploram os links encurtados de URL do Bit.ly para levar o alvo a baixar *scripts* maliciosos de domínios registrados pelo agente de ameaças. O Black Alicanto tem o cuidado de garantir que apenas alvos reais, e não pesquisadores de segurança, recebam suas cargas úteis. Ele implementa manualmente cargas úteis de estágio posterior apenas para esses alvos.

Uma dessas cargas é o msoRAT,[89] [90] um *trojan* de acesso remoto (RAT, na sigla em inglês) que o Black Alicanto implanta manualmente nos sistemas das vítimas em que tem interesse. O msoRAT é uma evolução de um *backdoor* usado há anos pelo BlueNoroff.[91] [92]

85. "Report of the Panel of Experts established pursuant to resolution 1874 (2009)", United Nations Security Council, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf (30/8/2019)
86. "All LNKs lead back to Black Dev 1 Part 1", PwC Threat Intelligence, CTO-TIB-20210408-01A
87. "All LNKs lead back to Black Dev 1 Part 2", PwC Threat Intelligence, CTO-TIB-20210525-01A
88. "Who is Black Alicanto hiring", PwC Threat Intelligence, CTO-TIB-20210913-01A
89. "All LNKs lead back to Black Dev 1 Part 1", PwC Threat Intelligence, CTO-TIB-20210408-01A
90. "Unveiling the Cryptomimic", NTT Security: Hajime Takai, Shogo Hayashi, Rintaro Koike, https://vb2020.vblocalhost.com/uploads/VB2020-Takai-etal.pdf (2020)
91. "Lazarus Group Campaign Targets Cryptocurrency Vertical", F-Secure, https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf (18/8/2020)
92. "Attributing Attacks Against Crypto Exchanges to LAZARUS – North Korea", ClearSky, https://www.clearskysec.com/wp-content/uploads/2021/05/CryptoCore-Lazarus-Clearsky.pdf (Maio, 2021)

Black Dev 2

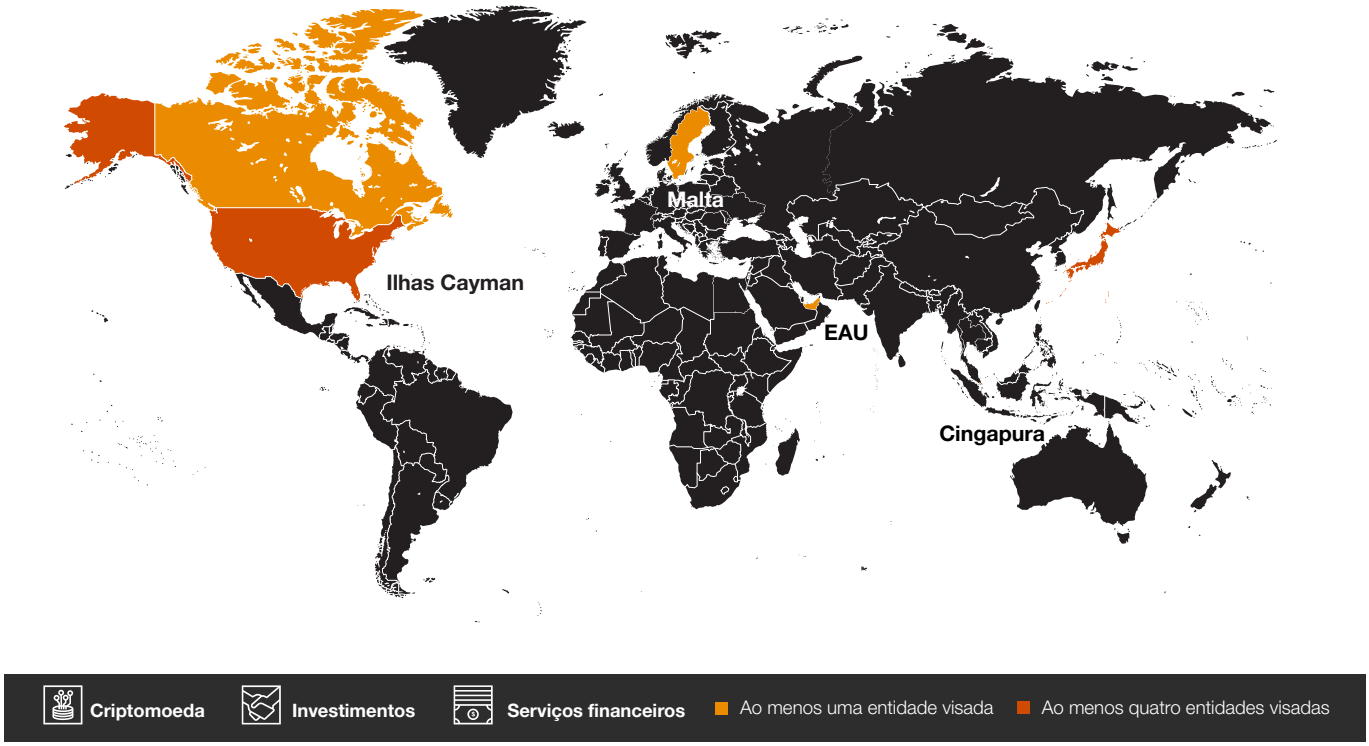
Desde pelo menos agosto de 2020, monitoramos um grupo de atividade que chamamos inicialmente de Black Dev 2.[93] Ele visava principalmente entidades no segmento de criptomoedas e tecnologia financeira (fintech), bem como empresas de *venture capital* (VC), sobretudo aquelas que financiam empreendimentos relacionados a criptomoedas e tecnologia.

As invasões que associamos ao Black Dev 2 normalmente envolviam documentos de isca com temas sobre uma apresentação de capital de risco ou corporativa ou sobre acordos de confidencialidade. Os documentos de isca continham um modelo remoto malicioso de um domínio registrado por um agente de ameaças. As macros do modelo remoto baixariam uma carga útil adicional – em geral, um *backdoor* malicioso e uma biblioteca de link dinâmico (DLL) de perfis de vítimas – a ser injetada em outro processo em execução.

Ao verificar os horários de criação e última modificação de documentos maliciosos criados pelo Black Dev 2, identificamos um padrão correspondente ao de um dia de trabalho médio, começando por volta das 8h e terminando por volta das 18h, com um intervalo de almoço de uma ou duas horas no meio, correspondendo ao fuso horário GMT+9, que inclui a Coreia do Norte.

Também observamos que o Black Dev 2 usou uma família de *malware* que provavelmente é uma variante do msoRAT, em infraestrutura sobreposta a outros servidores msoRAT C2 usados pelo Black Alicanto.[94] Com base na semelhança de configuração da infraestrutura e das cadeias de invasão adotadas pelo Black Dev 2 e pelo Black Alicanto, e sua vitimologia comum, avaliamos que provavelmente o Black Dev 2 e o Black Alicanto sejam o mesmo agente de ameaças sediado na Coreia do Norte e uma evolução do Bluenoroff.

Figura 19: Distribuição geográfica das entidades visadas pelo Black Dev 2



Fonte: PwC

93. "Capital injection", PwC Threat Intelligence, CTO-TIB-20210630-03A
94. "Bitcoin is silver, compromise is gold: Emerging North Korea-based threat actors on the hunt for cryptocurrency", PwC: Sveva Vittoria Scenarelli, https://www.youtube.com/watch?v=BOZecjABjSk

Missões complementares

Além da obrigação de continuar gerando fundos para o regime, os agentes de ameaças sediados na Coreia do Norte mantiveram a perseguição de metas alinhadas com os objetivos estratégicos norte-coreanos.

Black Banshee

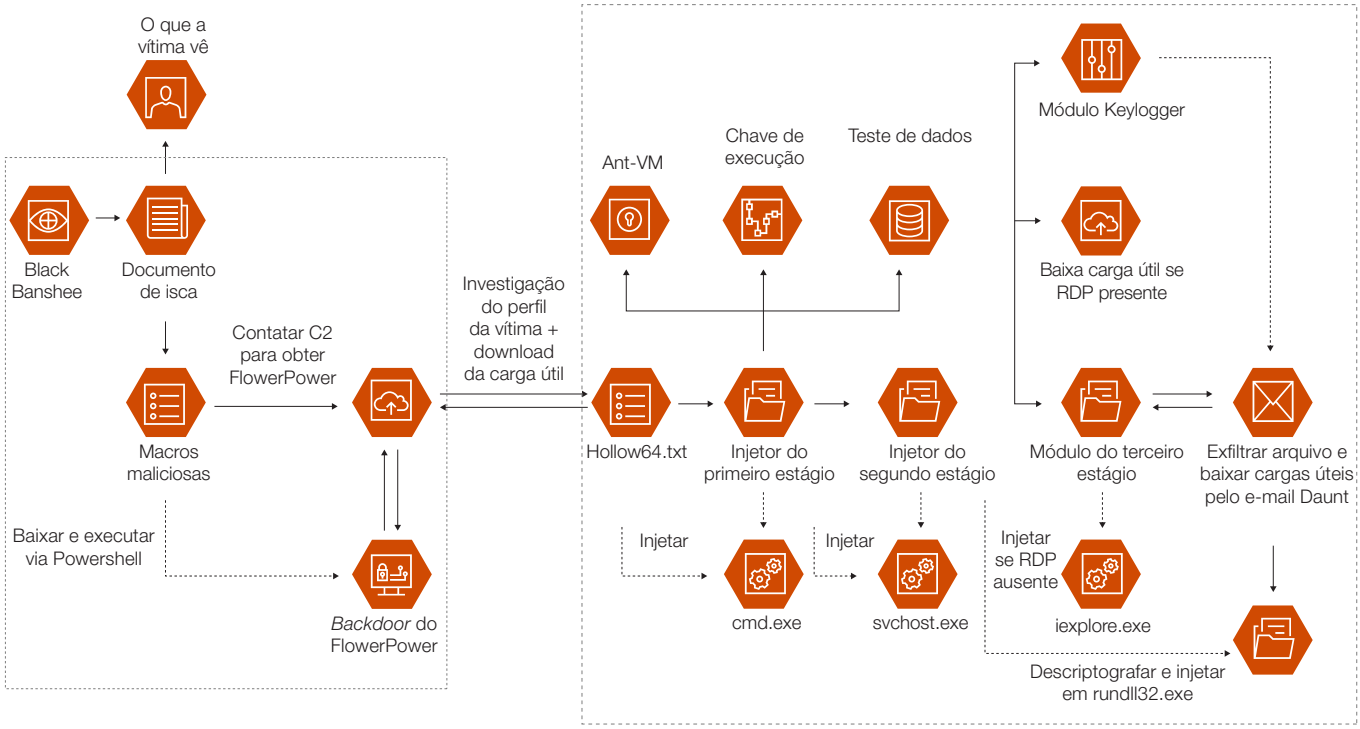
Em 2021, os principais setores de interesse do Black Banshee (também conhecido como Kimsuky ou Velvet Chollima) permaneceram alinhados com seus alvos históricos e incluíram:

- governo e setor público;
- diplomacia e política, incluindo *think tanks*;
- academia (com atenção especial à pesquisa nuclear e política internacional);
- defesa e espaço aéreo;
- energia nuclear; e,
- sociedade civil e grupos específicos, como jornalistas, ONGs e grupos religiosos ativos em relação à Coreia do Norte.

Atualização do BravePrince

Em 2021, observamos que o Black Banshee manteve seu foco principalmente nessas prioridades e reorganizou as ferramentas de seu arsenal para perseguir seus objetivos regionais. Por exemplo, o Black Banshee desenvolveu uma versão atualizada de seu *backdoor* BravePrince e o usou para atingir vítimas sul-coreanas.[95] O *backdoor* BravePrince atua na investigação de perfis de vítimas, *keylogger* e ladrão de informações, exfiltrando dados de vítimas pelo serviço de e-mail sul-coreano Daum. O *backdoor* também consegue exfiltrar arquivos específicos de interesse do Black Banshee, sugerindo não apenas que o operador interage diretamente com o implante, mas também que o agente da ameaça implanta o *backdoor* especificamente para alvos de interesse. A campanha se concentrou em entidades sul-coreanas. Seu provável objetivo era obter informações diplomáticas, políticas e militares sobre o posicionamento da Coreia do Sul em relação à Coreia do Norte, China, Rússia e aos Estados Unidos. Uma atualização sobre essa campanha publicada em novembro de 2021[96] também detalhou o ataque a materiais aeroespaciais e de defesa, bem como pesquisas científicas em campos específicos, como combustível de aviação.

Figura 20: Etapas de uma cadeia de intrusão Black Banshee envolvendo o *backdoor* BravePrince



95. "The Banshee, The Flower, The Dragon and Prince", PwC Threat Intelligence, CTO-TIB-20210508-01A
96. "North Korean attackers use malicious blogs to deliver malware to high-profile South Korean targets", Cisco Talos: Jung soo An, Asheer Malhotra, Kendall McKay, https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html (10/11/2021)

Política nuclear para BabySharks

O Black Banshee também continuou a executar campanhas do BabyShark durante a maior parte do ano,[97] mantendo seu antigo foco em temas nucleares, políticos e diplomáticos. Identificamos e notificamos pelo menos oito vítimas que o Black Banshee havia atacado desde agosto de 2021. Entre elas, estão figuras diplomáticas; analistas seniores (atuais ou antigos) de *think tanks* centrados na região Ásia-Pacífico; acadêmicos experientes com especialização em história, política e defesa da região Ásia-Pacífico; e funcionários de ONGs com atuação na península coreana. Esses ataques também estão alinhados com campanhas anteriores operadas pelo Black Banshee desde pelo menos o fim de 2018, quando observamos pela primeira vez o agente de ameaças começar a visar indivíduos que trabalham em organizações supranacionais, como as Nações Unidas.

Black Artemis

O Black Artemis (também conhecido como HIDDEN COBRA ou Lazarus Group) continuou visando fortemente os setores aeroespacial e de defesa como parte de uma campanha que monitoramos como ShowState.[98] A campanha se manteve em 2021, apoiando-se em documentos de engenharia social e *spear phishing* sobre oportunidades de emprego no segmento aeroespacial e de defesa, expandindo-se para incluir empresas de engenharia e manufatura.[99]

Em 2021, uma campanha diferente do Black Artemis teve como alvo entidades sul-coreanas e envolveu documentos maliciosos com macros usadas para obter acesso inicial. No entanto, nesse conjunto de intrusões, as macros lançavam no disco uma imagem PNG contendo dados maliciosos em formato compactado, dificultando a detecção estática por software antivírus. A macro convertia a imagem PNG em um arquivo BMP e a executava via mshta.exe. A carga executável incorporada, uma família de *malware* que chamamos de PaintJob,[100] tem semelhanças com a rotina de criptografia usada pelo Dtrack, um conhecido RAT que atribuímos ao subgrupo do Black Artemis conhecido como Andariel.

O Black Artemis também visou persistentemente pesquisadores de vulnerabilidades e segurança ofensiva ao longo do ano passado. Em janeiro de 2021, Google[101] e Microsoft[102] relataram a ocorrência de uma campanha de engenharia social que durou meses e que tinha como base perfis do Twitter que se passavam por pesquisadores de segurança, bem como contas de LinkedIn, Telegram, Discord e Keybase. O Black Artemis abordava os alvos sob o falso pretexto de colaborar em um projeto de pesquisa de vulnerabilidades. Em seguida, enviava a eles um projeto do Visual Studio com *backdoor* com código malicioso executando o *dropper* Comebacker, que acabava levando à instalação do *backdoor* Klackring.

O agente de ameaças também mantinha um blog de segurança que funcionava como um *watering hole* e direcionava a ele os pesquisadores de segurança visados durante a conversa. Quando os alvos visitavam o site, um *exploit* de dia zero do Chrome levava à instalação de um serviço malicioso em sua máquina, juntamente com um *backdoor* na memória. O Black Artemis podia então explorar o acesso aos sistemas de pesquisa de segurança para identificar e roubar pesquisas de segurança ofensivas de seu interesse.

Um esforço paralelo do Black Artemis incluiu ataques específicos a pesquisadores chineses de segurança ofensiva com documentos de isca maliciosos em língua chinesa.[103] Tentativas de colocar em risco pesquisadores de segurança também envolveram uma versão *trojan* do IDA Pro[104] – software de *disassembling* amplamente utilizado em pesquisas de segurança cibernética, sobretudo na análise de vulnerabilidades e no desenvolvimento de *exploits*.

97. "Nuclear Policy For BabySharks", PwC Threat Intelligence, CTO-TIB-20211014-01A
98. "Cyber Threats 2020: A Year in Retrospect", PwC Threat Intelligence (2020)
99. "Your dream job awaits - just please enable editing", PwC Threat Intelligence, CTO-TIB-20210916-01A
100. "Paint me like one of your BMP files", PwC Threat Intelligence, CTO-TIB-20210428-01A
101. "New campaign targeting security researchers", Google, https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/ (25/1/2021)
102. "ZINC attacks against security researchers", Microsoft, https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/ (28/1/2021)
103. "North Korean Hackers Caught Snooping on China's Cyber Squad", The Daily Beast: Shannon Vavra, https://www.thedailybeast.com/north-korean-hackers-caught-snooping-on-chinas-cyber-squad (22/11/2021)
104. @ESETresearch, Twitter, https://twitter.com/ESETresearch/status/1458438155149922312?s=20 (10/11/2021)

Um ano de atividade dos agentes de ameaças na China

Planejamento

Continuamos a observar atividade significativa de agentes de ameaças na China. Alguns desses agentes, como o Red Djinn, estão se concentrando em segmentos específicos, como semicondutores, inteligência artificial, saúde (o que inclui pesquisa genética e biotecnologia), computação quântica e exploração espacial, marítima e polar.[105] Outros, como o Red Kelpie estão conduzindo (e em alguns casos permitindo que outros conduzam) ataques muito mais abrangentes.

Além dos objetivos estratégicos econômicos, também continuamos a observar atividades contra o setor público motivadas por espionagem; o Red Vulture (também conhecido como Ke3chang, APT15, APT25, NICKEL) e o Red Keres (também conhecido como APT31, ZIRCONIUM) são exemplos conhecidos desse tipo de foco de segmentação.

Red Djinn

O agente de ameaças baseado na China que rastreamos como Red Djinn (também chamado de BlackTech, Mobwork, Palmerworm) permaneceu ativo em 2021, usando ferramentas conhecidas (como PLEAD e TSCookie) e novas (como Consock, FlagPro e SpiderRAT).

No início de 2021, observamos uma série de campanhas do Red Djinn usando famílias de *malware* conhecidas como PLEAD e TSCookie, incluindo variantes Linux de ambos os *backdoors* para ampliar a variedade de sistemas que poderiam ser alvos de ataques. Essas campanhas foram direcionadas para organizações sediadas em partes da Ásia e incluíram uma empresa de TI e telecomunicações. O agente de ameaças registrou domínios com temas sobre tecnologias de nuvem e VPN, e as famílias de *malware* continham IDs de campanha que indicavam como provável alvo os setores de produção industrial e engenharia.

New Djinn

Embora o Red Djinn tenha histórica e consistentemente se concentrado em atingir as maiores economias da Ásia, também já observamos alvos mais abrangentes desse agente de ameaças. Por exemplo, ele tinha como alvo uma subsidiária internacional de um provedor de serviços gerenciados (MSP, na sigla em inglês) para realizar um ataque de *island-hopping* para se mover lateralmente para a rede principal do MSP.

Por meio do rastreamento do Consock,[106] [107] uma variante personalizada do Gh0stRAT associada ao Red Djinn (também conhecido como Gh0stTimes), conseguimos identificar o controlador do *malware*.

Figura 21: Times.exe, o controlador do *malware* Consock do Red Djinn

Figura 22: o Times.exe foi originalmente projetado para sistemas em idioma chinês

105. "China's 5-year plan has 7 technology targets' watch for responses", S&P Global, https://www.spglobal.com/marketintelligence/en/newsinsights/latest-news-headlines/china-s-5-year-plan-has-7-technology-targets-watch-for-responses-63161384 (15/3/2021)
106. "BlackTechs ELF-esteem", PwC Threat Intelligence, CTO-TIB-20210329-01A
107. "BlackTech's Gh0st", PwC Threat Intelligence, CTO-TIB-20201113-01A

Também descobrimos iscas de *spear phishing* usadas pelo agente de ameaças para distribuir o Consock e uma nova família de *malware* que chamamos de Flagpro. Avaliamos que o Red Djinn provavelmente usou o Flagpro[108] no ataque à subsidiária de um provedor de serviços de TI japonês e desenvolvedor de *software* que opera no leste e sul da Ásia.

Em nossa análise dessa campanha, identificamos uma série de *scripts* de exploração que muito provavelmente foram usados pelo Red Djinn em suas operações. Metadados revelaram que alguns deles provavelmente foram retirados ou adaptados de bancos de dados abertos de vulnerabilidades, como o Seebug. Eles foram acompanhados de pastas contendo dados que sugeriam que o Red Djinn estava realizando reconhecimento de sistemas vulneráveis em escala internacional. Além disso, identificamos o código de exploração para os dispositivos Citrix e Mikrotik que pareciam ainda estar em desenvolvimento.[109] Também identificamos atividade do Red Djinn desde março de 2021, explorando as vulnerabilidades do ProxyLogon, após sua divulgação inicial, para implantar um novo *backdoor* que chamamos de SpiderRAT.[110] [111]

Red Vulture

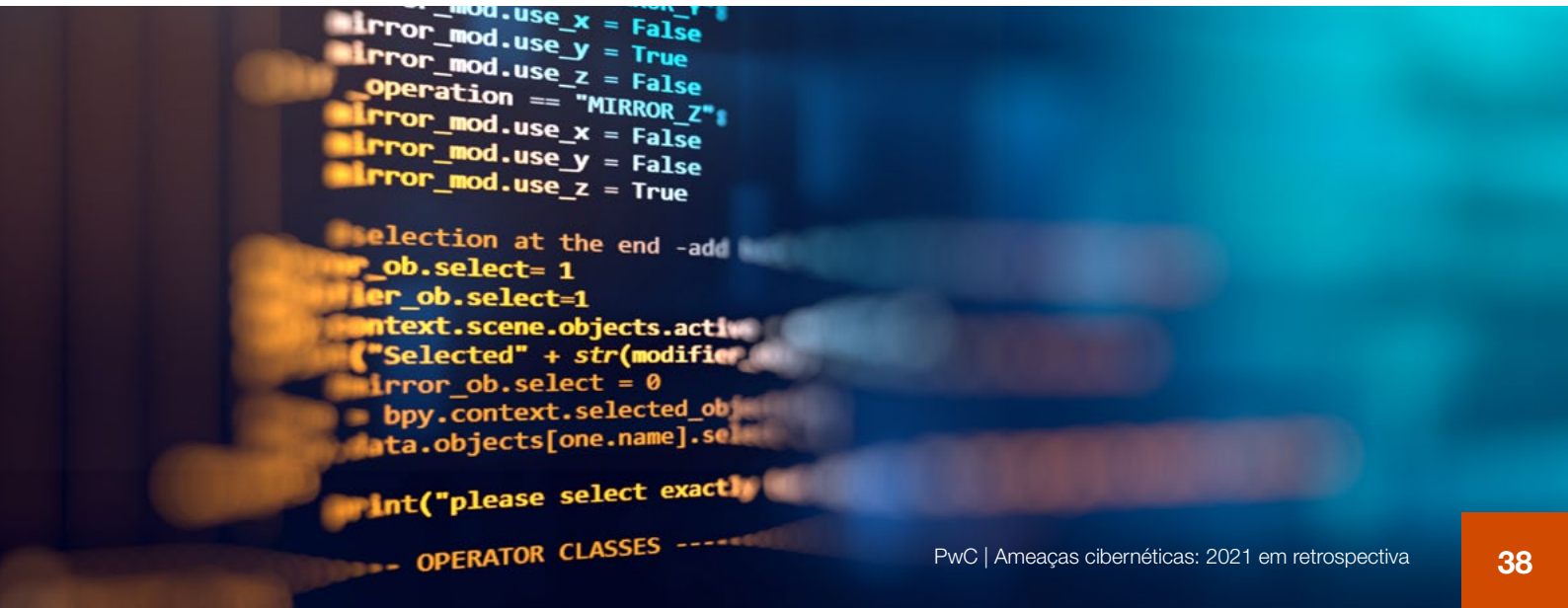
O Red Vulture aumentou seu ritmo operacional ao longo de 2021. Observamos o Red Vulture realizando reconhecimentos regulares em várias organizações ao longo do ano, nos seguintes setores:

- Governo;
- Aeroespacial e defesa;
- Educação; e
- ONGs.

Esse reconhecimento consistiu principalmente na navegação feita pelo agente de ameaças nos sites e serviços de perímetro das organizações visadas (por exemplo, VPN e e-mail). Há evidências de que o agente está fazendo verificação em massa de vulnerabilidades na infraestrutura voltada para o público.[112] O sucesso do Red Vulture em atingir vítimas em 2021 se deveu, em geral, ao uso abundante de explorações contra sistemas de autenticação de perímetro (por exemplo, VPNs).

O reconhecimento observado foi direcionado ao ataque de ministérios de Relações Exteriores, com foco na Europa e América do Sul.[113] [114] [115]

108. "Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors", Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt (29/9/2020)
109. "Red Djinn's red flags", PwC Threat Intelligence, CTO-TIB-20210903-02B
110. "Back to Black(Tech): an analysis of recent BlackTech and an open directory full of exploits", PwC: Sveva Vittoria Scenarelli, Adam Prescott, https://vblocalhost.com/conference/presentations/back-to-blacktech-an-analysis-of-recent-blacktech-operations-and-an-open-directory-full-of-exploits/ (7/10/2021)
111. "Red Djinns spider web", PwC Threat Intelligence, CTO-TIB-20211202-01A
112. "NICKEL targeting government organizations across Latin America and Europe", Microsoft, https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/ (6/12/2021)
113. "Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity", US CISA, https://us-cert.cisa.gov/ncas/alerts/aa20-258a (24/10/2020)
114. "A committee of vultures", PwC Threat Intelligence, CTO-SIB-20210722-01A
115. "Okrum and Ketrican: An Overview of Recent Ke3chang Group Activity", ESET, Julho/2019, https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf



Red Keres

No início de 2021, o Escritório Federal Alemão para a Proteção da Constituição (BfV) informou sobre o ataque do Red Keres a instituições, incluindo "ministérios e autoridades, organizações políticas e fundações" em toda a Europa.[116]

Analisando a infraestrutura do Red Keres divulgada pelo BfV, também identificamos evidências sugerindo que o agente de ameaças provavelmente comprometeu e estava acessando diretamente o servidor de e-mail do Ministério das Relações Exteriores de um governo do Sudeste Asiático entre pelo menos dezembro de 2020 e fevereiro de 2021.[117] Na mesma época aproximadamente, observamos atividade semelhante envolvendo o servidor de e-mail do Ministério da Defesa de um governo diferente do Sudeste Asiático.

No fim de 2021, a Agência Nacional de Segurança de Sistemas de Informação (ANSSI) da França divulgou um relatório detalhado sobre os TTPs do Red Keres. O relatório detalhou a configuração da infraestrutura de anonimização em várias camadas do agente de ameaças, envolvendo mais de mil roteadores do tipo SOHO (sigla em inglês para pequenos escritórios/*home office*), uma técnica em que vários outros agentes de ameaças da China investiram ao longo de 2021, segundo observações da PwC. O relatório também destacou as muitas diferentes técnicas que o Red Keres utiliza ao tentar ter acesso a uma vítima, variando de *spear phishing*, força bruta de senha e abuso de credenciais válidas, até a exploração de vulnerabilidades como ProxyLogon ou em produtos de VPN (rede virtual privada).

Red Kelpie

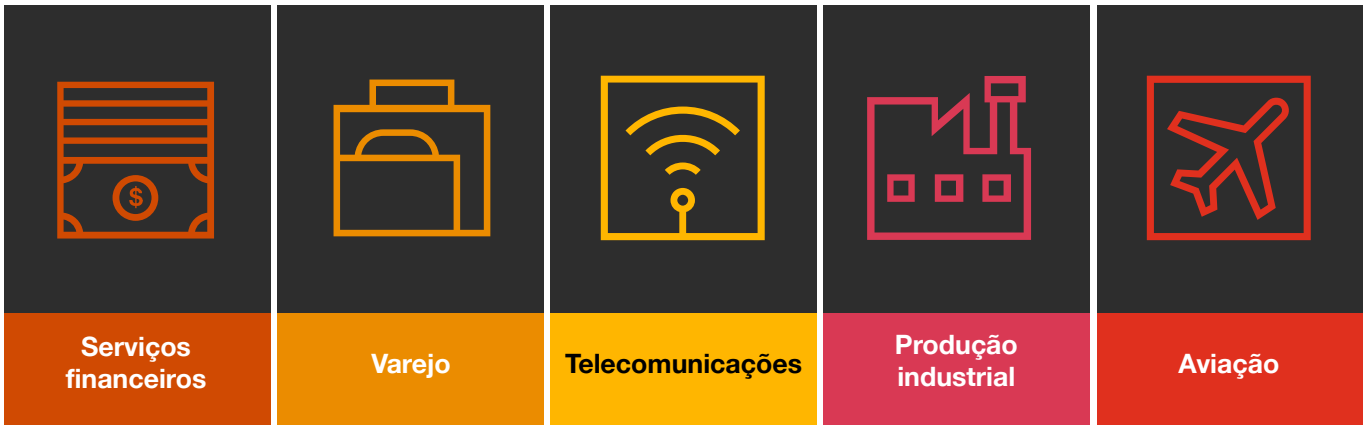
O agente de ameaças que monitoramos como Red Kelpie (que tem sobreposições com o APT41 e o BARIUM) conta com uma ampla variedade de famílias de *malware*, incluindo ShadowPad e CROSSWALK, além de ferramentas comuns, como Cobalt Strike. Ele é diversificado em relação a seus alvos, que englobam vários setores estrategicamente importantes.

ChaChaLoader

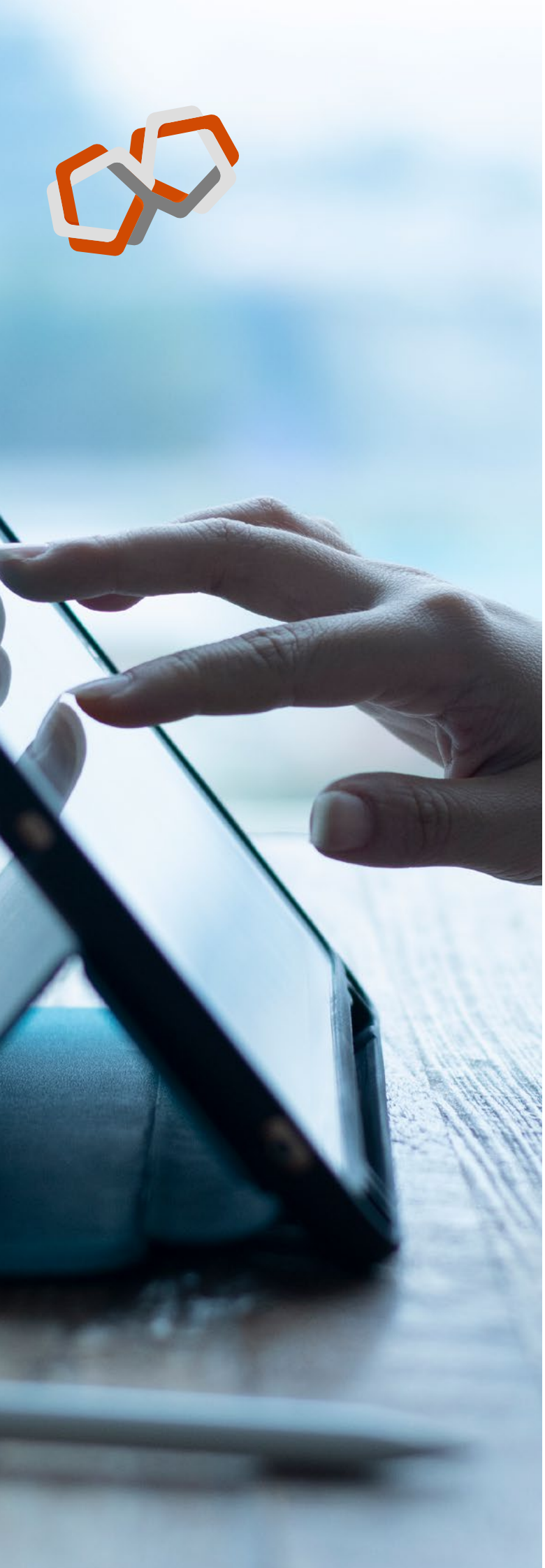
Em 2021, o Red Kelpie conduziu uma série de campanhas usando seu conhecido *loader* Motnug e uma provável evolução chamada ChaChaLoader. Motnug e ChaChaLoader foram usados para carregar o Cobalt Strike e, em alguns casos raros, um *backdoor* recém-observado que foi chamado de SIDEWALK em código aberto e que é uma provável evolução do *backdoor* CROSSWALK.[118] É plausível que os poucos casos em que o SIDEWALK foi implantado no lugar do CobaltStrike foram de alvos de alto valor.

Essas campanhas visavam uma gama de setores, incluindo serviços financeiros, varejo, telecomunicações, produção industrial e aviação.

Figura 23: alvos do Red Kelpie em 2021



116. "BfV Cyber-Brief Nr. 01/2021 - Bedrohung deutscher Stellen durch Cyberangriffe der Gruppierung APT31", Bundesamt für Verfassungsschutz, https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-cyberabwehr/broschuere-2021-01-bfv-cyber-brief-2021-01 (18/1/2021)
117. "Red Keres flows into South East Asia", PwC Threat Intelligence, CTO-TIB-20210211-01A
118. "Learning to ChaCha with Red Kelpie", PwC Threat Intelligence, CTO-TIB-20210624-02A



Vulnerabilidade do Confluence

Em anos anteriores, o Red Kelpie explorou em massa vulnerabilidades na infraestrutura voltada para o público para obter acesso inicial, uma tática que também observamos em 2021. Notamos especialmente o Red Kelpie explorar a vulnerabilidade de execução de código Atlassian Confluence CVE-2021-26084 para suprimir um *script* em lote e um DLL usados para carregar e executar o Cobalt Strike.[119] O Red Kelpie foi observado anteriormente usando *exploits* de vulnerabilidades no software Citrix/Cisco para implantar *scripts* em características muito semelhantes, que também são conhecidos por carregar e executar o Cobalt Strike.[120]

Ativo, mesmo após indiciamento

Em setembro de 2020, o Departamento de Justiça dos EUA indiciou sete indivíduos da Ásia alegando que eles eram *hackers* e que as invasões que eles conduziram eram conhecidas em código aberto como APT41, BARIUM, Winnti, entre outros nomes.[121]

Apesar desses indiciamentos, a atividade do Red Kelpie continuou ao longo de 2021. Talvez o maior custo para o Red Kelpie do indiciamento tenha sido a apreensão de contas, servidores e domínios utilizados pelo agente de ameaças, o que o forçou a alterar em parte seu ritmo operacional. Monitoramos novos conjuntos de infraestrutura usados por esse agente de ameaças no fim de 2020/2021, mas ainda observamos sobreposições com infraestrutura associada mais antiga atribuída ao APT41/BARIUM. Os indiciamentos de vários dos operadores por trás das campanhas não parecem ter tido qualquer impacto geral significativo nas operações do agente de ameaças.

119. "Active exploitation of CVE-2021-26084", PwC Threat Intelligence, CTO-QRT-20210906-01A
120. "This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits", Mandiant, https://www.mandiant.com/resources/apt41-initiates-globalintrusion-campaign-using-multiple-exploits (25/3/2020)
121. "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally", US Department of Justice, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer (16/9/2020)

Estudo de caso de resposta a incidentes:

A variante FUNRUN do Red Dev

A PwC respondeu a uma invasão em um *think tank* executada por um agente de ameaças da China, que identificamos como Red Dev 14.[122] Usando os *exploits* do ProxyLogon, o agente de ameaças lançou um *webshell* em um servidor Exchange local. Inicialmente, o agente tentou algum reconhecimento por meio do *webshell* (que consiste principalmente na coleta de informações do sistema, como nomes de usuários e processos em execução) e executou comandos para esvaziar a memória do LSASS a fim de obter credenciais por meio de binários *living-off-the-land*. O agente de ameaças utilizou uma variante de *backdoor* chamada FUNRUN para lançar o ProcDump a fim de esvaziar a memória LSASS, além de lançar o Mimikatz no disco.

Depois de obter as credenciais, o agente de ameaças se moveu lateralmente na rede por meio de compartilhamentos remotos SMB, instalando o *backdoor* FUNRUN em *hosts* adicionais. O agente também executou comandos para procurar outros *webshells* no servidor Exchange. Isso provavelmente foi feito para testar se o servidor Exchange já havia sido comprometido (provavelmente pelo ProxyLogon), o que informaria o Red Dev 14 se outro agente de ameaças também estava presente no sistema. Isso talvez afetasse o modo como ele atingiria seus objetivos.

Do ponto de vista de atribuição, observamos antes o *backdoor* FUNRUN ser usado pelo agente de ameaças da China que monitoramos como Red Pegasus (também conhecido como APT9).[123] No entanto, muito tempo se passou entre o momento em que o Red Pegasus foi observado pela última vez usando esse *backdoor* (durante 2014 e 2015) e a atividade do FUNRUN que detectamos em 2021. Com base nessa questão, no fato de que o mecanismo de carregamento era diferente para esse *backdoor* em comparação com o uso do Red Pegasus e que não havia sobreposições de infraestrutura com o Red Pegasus, decidimos monitorar essa atividade sob o novo nome Red Dev 14.

O Red Dev 14 comprometeu vítimas em vários locais como parte dessa campanha, principalmente do setor agrícola.

122. "Introducing Red Dev 14", PwC Threat Intelligence, CTO-TIB-20210412-01A

Agentes de ameaças na China atacam telecomunicações

Os ataques ao setor de telecomunicações continuam sendo um objetivo para vários agentes de ameaças da China. As empresas desse setor têm uma gama de informações de alto valor, como dados de provedores de telecomunicações sobre seus clientes (que, dependendo do provedor, podem ser metadados sobre conexões a sites ou registros de chamadas). Essa informação pode ser explorada por agentes de ameaças para fins de vigilância ou para coletar informações tradicionais sobre as atividades de alvos específicos.

Por exemplo, conforme mencionado antes, continuamos a ver ataques de Red Kelpie ao setor de telecomunicações,[124] além da ferramenta compartilhada ShadowPad ser usada para violar provedores de telecomunicações.[125] Apoiamos uma investigação de resposta a incidentes para um provedor de telecomunicações no Sudeste Asiático, onde observamos uma variante do *backdoor* Evora ser usada pelo agente de ameaças Red Salamander (também conhecido como LotusBlossom), da China.[126]

Algumas coisas mudam e outras permanecem iguais para os agentes de ameaças na Índia

Nossas investigações sobre as operações dos agentes de ameaças na Índia revelaram um foco estreito em países de relevância estratégica para a Índia, especialmente em seus vizinhos próximos, China e Paquistão. Quase todos os agentes de ameaças de espionagem baseados na Índia que monitoramos usam documentos de isca relacionados a políticas ou temas políticos de países-alvo ou a assuntos militares e de defesa.

Orange Kala (Donot)

O ritmo operacional e o foco dos ataques do Orange Kala (também conhecido como Donot) em 2021 foram semelhantes ao do ano anterior, com pouca variação nos TTPs. Em pelo menos um caso, o agente de ameaças usou um documento de isca relacionado à tecnologia de mísseis.[127] Esse tema de isca não era novo para o Orange Kala, pois o conteúdo de vários outros documentos de isca, desde pelo menos novembro de 2020, foi retirado de notícias e periódicos voltados para tecnologia de defesa antimísseis. No entanto, enquanto a maioria dos documentos de isca anteriores sobre esse tema estavam relacionados aos Estados Unidos, essa campanha foi a primeira em que a PwC observou o Orange Kala com foco na tecnologia de mísseis da Ásia-Pacífico. Tanto nessa campanha quanto ao longo do ano, o Orange Kala usou fortemente a ferramenta de *Malware-as-a-Service* (MaaS) WarzoneRAT.

123. Mandiant, “Advanced Persistent Threat Groups”, https://www.mandiant.com/resources/apt-groups
124. Mandiant, “Advanced Persistent Threat Groups”, https://www.mandiant.com/resources/apt-groups
125. “ShadowPad not a dead cert”, PwC Threat Intelligence, CTO-TIB-20211116-02A
126. “Inside a Red toolbox”, PwC Threat Intelligence, CTO-TIB-20210518-01A
127. “Orange Kala enters the Warzone”, PwC Threat Intelligence, CTO-TIB-20210112-01A

Estudo de caso:

Ataques do Red Menshen a provedores de telecomunicações

Ao longo de 2021, monitoramos e respondemos a várias invasões atribuídas a um agente de ameaças baseado na China que chamamos de Red Menshen.[128] Esse agente foi observado tentando invadir provedores de telecomunicações no Oriente Médio e na Ásia, bem como entidades governamentais, de educação e de logística usando um *backdoor* personalizado que chamamos de BPFDoor. Esse *backdoor* é compatível com vários protocolos para comunicação com um C2, incluindo TCP, UDP e ICMP. Isso possibilita ao agente vários mecanismos para interagir com o implante.

Nossa pesquisa mostrou que esse agente de ameaças usa várias ferramentas em sua fase de pós-exploração. Isso abrange variantes personalizadas da ferramenta compartilhada Mangzamel (incluindo variantes de Golang), variantes personalizadas de Gh0st e ferramentas de código aberto como Mimikatz e Metasploit para apoiar sua movimentação lateral em sistemas Windows.[129] [130] Também identificamos que o agente de ameaças envia comandos às vítimas do BPFDoor por meio de servidores privados virtuais (VPSs, na sigla em inglês) hospedados em um provedor conhecido. Esses VPSs, por sua vez, são administrados via roteadores comprometidos em Taiwan, que o agente de ameaças usa como túneis VPN.

As atividades do Red Menshen que observamos ocorreram entre segunda e sexta-feira (nenhuma foi observada nos fins de semana), e a maioria das comunicações se realizou entre 1:00 e 10:00 UTC.[131] Esse padrão sugere uma janela de atividade consistente de 8 a 9 horas para o agente, com uma probabilidade realista de alinhamento com o horário de trabalho local.

128. "Compromising Eurasian Telecoms justforfun", PwC Threat Intelligence, CTO-TIB-20210709-01A
129. "A Window into Red Dev 18", PwC Threat Intelligence, CTO-TIB-20210831-02A
130. "Of Gh0sts and Golang", PwC Threat Intelligence, CTO-TIB-20211011-01A
131. "Red Dev 18 Further Developments", PwC Threat Intelligence, CTO-QRT-20210727-01A

Em uma campanha, o agente de ameaças implantou o WarzoneRAT utilizando uma DLL maliciosa que acabou por decodificar e executar uma longa linha de comando codificada em um *script* em lote.[132] Alguns documentos de isca usados nessa campanha, e carregados em um scanner antivírus on-line dos Emirados Árabes Unidos, tinham como tema novos navios da marinha iraniana, e outros tratavam de exercícios navais multinacionais organizados pelo Paquistão, sugerindo o provável interesse do agente de ameaças em temas militares.

Compartilhar é cuidar

Ao longo do ano, observamos vários cruzamentos de TTPs entre Orange Kala e outros agentes de ameaças da Índia que ainda estamos investigando. Eles podem indicar maior interconexão entre os agentes de ameaças da Índia do que se pensava antes. Em fevereiro de 2021, monitoramos uma campanha envolvendo[133] um modelo de arquivo RTF malicioso com links para as operações Orange Kala e Orange Dev 1 (ou CONFUCIUS) em 2020.[134] Os links também foram identificados em uma campanha de 2017 direcionada ao Paquistão e conhecida como Operação Shaheen.[135] A atividade de 2021 se concentrou em temas militares e de defesa, usando documentos de isca com referência a propostas de defesa e, em um caso, à Marinha Real Tailandesa. O Orange Kala e o Orange Dev 1 são conhecidos por terem visado os setores de defesa e governo no passado. A campanha de 2021 usou técnicas diferentes de atividades semelhantes relatadas em 2020,[136] adicionando uma camada extra à cadeia de ataque, com os documentos RTF iniciais baixando um segundo RTF na máquina da vítima e usando esse segundo RTF como um *downloader* de uma DLL maliciosa.

Em junho de 2021, observamos uma campanha do Orange Athos (também conhecido como Patchwork) envolvendo *scripts* VBA que eram usados pelo Orange Kala em 2019.[137] As macros VBA eram surpreendentemente semelhantes nas atividades de 2019 e 2021 – até nomes de variáveis exclusivos. Isso sugere, com probabilidade realista, que eles não eram produto de um construtor de macros, mas macros criadas sob medida por um agente de ameaças e reaproveitadas por outro. Embora o documento malicioso tenha sido modelado com base na biografia de um indivíduo paquistanês retirada do Scribd.com, o agente alterou o texto original para afirmar que o pai do indivíduo trabalhou para a Comissão de Pesquisa Espacial e Alta Atmosfera (Suparco), a agência espacial do Paquistão. O documento foi usado para distribuir às vítimas o *backdoor* BADNEWS, um item antigo no arsenal do Orange Athos. Outros relatórios de código aberto[138] [139] abordaram no início do ano mais documentos de isca maliciosos com temas relacionados à Suparco. Esses documentos distribuíram aos alvos o WarzoneRAT e foram atribuídos ao agente de ameaças Orange Dev 1 da Índia.

Essas campanhas apresentam ao menos um mínimo de ferramentas compartilhadas ou de adaptação cruzada de ferramentas simples entre os agentes de ameaças localizados na Índia. No entanto, observamos isso apenas no nível de vetores de acesso inicial. Os agentes de ameaças localizados na Índia ainda apresentam uma ampla diferença de opções de *backdoors* em estágios posteriores.

132. "Batch scripts back alright", PwC Threat Intelligence, CTO-TIB-20210223-02A
133. "Orange Kala or Orange Dev 1 - you decide", PwC Threat Intelligence, CTO-TIB-20210520-01A
134. "BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps", Blackberry Cylance, https://www.blackberry.com/us/en/forms/enterprise/bahamut-report (October 2020)
135. "The White Company: Inside the Operation Shaheen Espionage Campaign", Cylance, https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf (18/3/2021)
136. "BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps", Blackberry Cylance, https://www.blackberry.com/us/en/forms/enterprise/bahamut-report (Outubro/2020)
137. "Sharing is Caring", PwC Threat Intelligence, CTO-TIB-20210818-01A
138. "Confucius APT deploys Warzone RAT", Uptycs: Abhijit Mohanta, Ashwin Vamshi, https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat (12/1/2021)
139. "Warzone RAT – Beware of the Trojan malware stealing data triggering from various Office documents", Quickheal: Ayush Puri, https://blogs.quickheal.com/warzonerat-beware-of-the-trojan-malware-stealing-data-triggering-from-various-office-documents/ (1/7/2021)

Orange Athos (Patchwork)

O Orange Athos (também conhecido como Patchwork) continuou a fazer uso intenso do *backdoor* BADNEWS (também conhecido como BozokRAT) em diferentes campanhas em 2021. Houve apenas pequenas alterações na base de código do *malware* desde que ele foi relatado pela primeira vez em código aberto em 2016.[140]

O agente de ameaças manteve seu foco anterior[141] em alvos chineses e paquistaneses. Em uma campanha que observamos em abril de 2021, o agente usou um documento de isca relacionado à cooperação militar entre a China e o Paquistão.[142] O documento era um arquivo .docx malicioso que explorava a CVE-2017-0261, uma vulnerabilidade *Use-After-Free* (UAF) especificamente para imagens *postscript* encapsuladas (EPS). Essa é uma técnica que observamos o agente de ameaças empregar de modo consistente em várias campanhas de 2020 envolvendo ferramentas, técnicas e procedimentos (TTPs) quase idênticos, cada um com foco em alvos localizados na China.

Entre as invasões separadas, uma[143] apresentou como isca um falso formulário do Conselho Federal de Receita do Paquistão, pedindo aos funcionários dos departamentos do governo federal paquistanês que inserissem seus dados pessoais para se qualificarem a receber um pacote especial de isenção tributária. Quando as vítimas abriam o RTF, a mesma vulnerabilidade mencionada acima (CVE-2017-0261) levava à instalação do *backdoor* BADNEWS. Com a exploração contínua dessa vulnerabilidade específica e o uso de ferramentas bem documentadas em código aberto, esse parece ser outro agente de ameaças que persistirá com TTPs testados e comprovados.

Orange Yali (BITTER)

Ao longo de 2021, identificamos vários sites se passando por empresas paquistanesas legítimas que, acreditamos, foram provavelmente criadas e mantidas pelo agente de ameaças Orange Yali, localizado na Índia (também conhecido como BITTER) desde 2020. Os sites, que normalmente têm pouco ou nenhum conteúdo ou espaço reservado para texto, foram usados para preparar cargas úteis do *backdoor* "rkftl", às vezes empacotado como um instalador MSI, bem como utilitários, como o cliente SSH e Telnet PuTTY. O Orange Yali também continuou a usar a família de *malware* conhecida como ArtraDownloader e introduziu o uso de arquivos CHM (HTML compilado) em uma campanha direcionada especificamente a entidades chinesas.[144] [145] Vários relatórios também indicaram que o Orange Yali usou pelo menos dois *exploits*[146] [147] ao longo de 2021, ambos provavelmente adquiridos de um negociador de *exploits*, e não desenvolvidos internamente pelo agente de ameaças.[148] Isso indica que pelo menos um agente de ameaças motivado por espionagem e localizado na Índia tem recursos para acessar o mercado privado de dia zero, algo que não havíamos observado antes com agentes de ameaças ativos na região.

140. "Monsoon – Analysis of an APT campaign", Forcepoint, https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysisreport.pdf
141. "Cyber Threats 2020: A Year in Retrospect", PwC Threat Intelligence
142. "Orange Athos has BADNEWS for its adversaries", PwC Threat Intelligence, CTO-TIB-20210204
143. "Threats under the Spotlight October 2021", PwC Threat Intelligence, CTO-TUS-20211118-01A
144. "Orange Yali continues to set up shop in Pakistan", PwC Threat Intelligence, CTO-TIB-20210527-02A
145. "Operation Magichm": CHM file release and subsequent operation of BITTER-organization", QiAnXin, https://ti.qianxin.com/blog/articles/%22operationmagichm%22:CHM-file-release-and-subsequent-operation-of-BITTER-organization/ (15th March 2021)
146. "Windows kernel 0-day exploit (CVE-2021-1732) is used by BITTER APT in targeted attack", DBAPPSecurity, https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/ windows-kernel-0-day-exploit-is-used-by-bitter-apt-in-targeted-attack/ (10/2/2021)
147. "0-day vulnerability in Desktop Window Manager (CVE-2021-28310) used in the wild", Kaspersky: Boris Larin, Costin Raiu, Brian Bartholomew, https://securelist.com/0-day-vulnerability-in-desktop-window-manager-cve-2021-28310-used-in-the-wild/101898/ (13/4/2021)
148. "APT trends report Q2 2021", Kaspersky, https://securelist.com/apt-trends-report-q2-2021/103517/ (29/7/2021)

A espionagem não compensa: atividades de agentes de ameaças no Paquistão

Ao longo de 2021, o Green Havildar (também conhecido como APT36, Transparent Tribe, Gorgon Group) continuou operando de acordo com seu provável objetivo principal de coletar inteligência (inclusive visando os setores militar, governamental e público em geral, sobretudo na Índia). Esse agente de ameaças usa *spear phishing* básico para acesso inicial, com documentos de isca variando de currículos pessoais até programas de conferências, com várias amostras relacionadas a militares e defesa.[149]

O Green Havildar é conhecido por usar o CrimsonRAT, que ele continuou a operar por meio de um modelo construtor: o RAT dispõe de um amplo conjunto de recursos de vigilância e exfiltração, um modelo de ofuscação de código consistente e flexibilidade para que o agente de ameaças altere as portas pelas quais a atividade C2 é conduzida. Entre abril e julho de 2021, o Team Cymru publicou relatórios expondo a configuração da infraestrutura C2 do Green Havildar, incluindo o gerenciamento que o agente de ameaças fez dela por RDP.[150] [151]

Em 2021, observamos um aumento na atividade das operações do Green Havildar com motivação financeira e focadas em crimes cibernéticos (relatadas em código aberto como Gorgon Group, também conhecido como Aggah, MasterMana). Como em 2020, a maioria das campanhas de *spam* do Gorgon Group envolveu documentos de iscas do PowerPoint e links do OneDrive, fornecendo RATs comuns como AgentTesla, Remcos e Quasar. Além disso, observamos o uso de dois injetores comuns diferentes, RunPE e HCrypt, pelo agente de ameaças.

Embora o Gorgon Group também seja conhecido por hospedar *scripts* maliciosos de vários estágios em sites públicos de colagem, como Pastebin e Blogspot, monitoramos uma série de campanhas que usavam contas no The Internet Archive para fins semelhantes. Em agosto de 2021, foi divulgado que o Gorgon Group estava usando sites comprometidos para produzir cargas maliciosas de próximo estágio e distribuir Warzone RAT no lugar de sites de colagem, em um esforço para evitar a detecção e remoção de seus recursos orquestrados.[153]

Enquanto as operações de coleta de inteligência do Green Havildar se concentram principalmente na Índia e ocasionalmente em países vizinhos, como o Afeganistão,[154] a atividade do Gorgon Group tem um alcance internacional não necessariamente limitado a aspectos políticos. Por exemplo, a partir de abril de 2021, monitoramos uma campanha do Gorgon Group direcionada a organizações na Holanda e na Coreia do Sul,[155] inclusive no setor manufatureiro (um alvo frequente desse agente de ameaças). Em contraste com o Green Havildar, o Gorgon Group tem alvos relativamente indiscriminados, e não observamos que ele tenha implementado nenhum recurso personalizado.

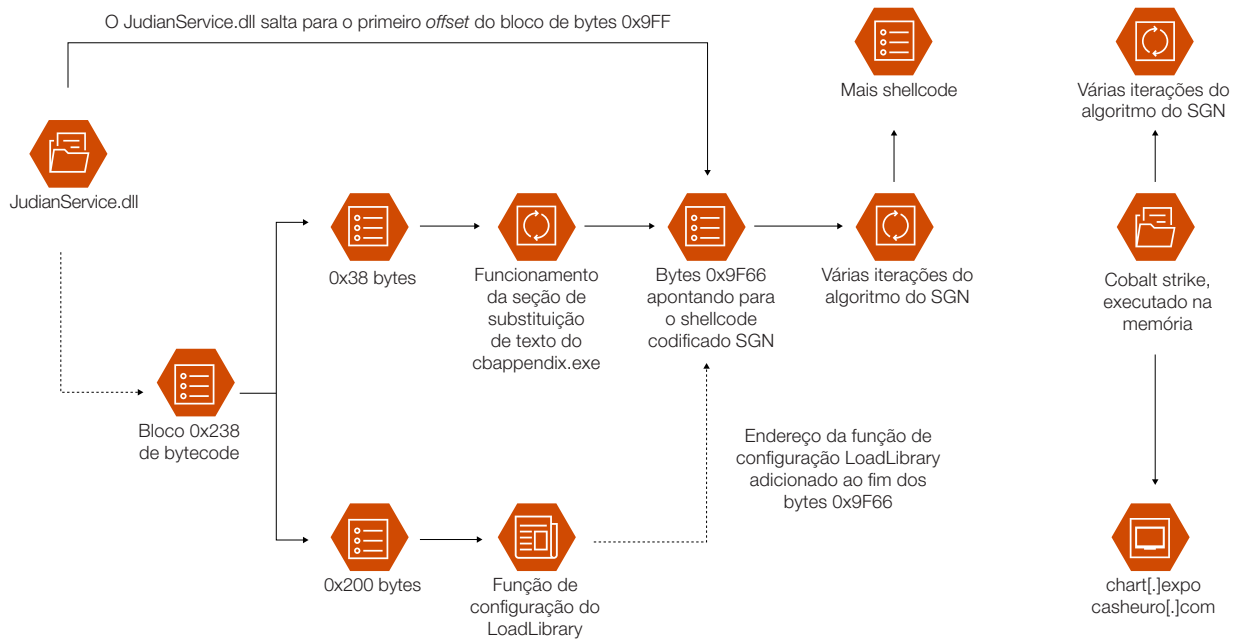
149. "CrimsonRAT - Green Havildars premium export", PwC Threat Intelligence, CTO-TIB-20210310-02A
150. "Transparent Tribe APT Infrastructure Mapping Part 1: A High-Level Study of CrimsonRAT Infrastructure October 2020 – March 2021", Team Cymru: Joshua Picolet, https://team-cymru.com/blog/2021/04/16/transparent-tribe-apt-infrastructure-mapping/ (16/4/2021)
151. "Transparent Tribe APT Infrastructure Mapping Part 2: A Deeper Dive into the Identification of CrimsonRAT Infrastructure October 2020 – June 2021", Team Cymru: Joshua Picolet, https://team-cymru.com/blog/2021/07/02/transparent-tribe-apt-infrastructure-mapping-2/ (2/7/2021)
152. "Aggah Using Compromised Websites to Target Businesses Across Asia, Including Taiwan Manufacturing Industry", Anomali, https://www.anomali.com/blog/aggahusing-compromised-websites-to-target-businesses-across-asia-including-taiwan-manufacturing-industry (12/8/2021)
153. "Cyber Threats 2020: A Year in Retrospect", PwC Threat Intelligence
154. "Threats under the Spotlight - December 2020", PwC Cyber Threat Intelligence, CTO-TUS-20210111-01A
155. "Not Enough Mana to Conduct that Operation", PwC Threat Intelligence, CTO-TIB-20210630-02A

(Nem) tudo está tranquilo no front do Scarlet: atividade do agente de ameaças no Vietnã

Depois que o Facebook atribuiu publicamente o Scarlet Ioke (também conhecido como Ocean Lotus, APT32) em dezembro de 2020 ao CyberOne Group, uma empresa de TI com sede no Vietnã, observamos uma redução drástica no ritmo operacional desse agente de ameaças – pelo menos no que diz respeito a campanhas conhecidas e em andamento. Por outro lado, as empresas chinesas de segurança cibernética continuaram observando ataques de Scarlet Ioke na China no ano passado, o que é coerente com o antigo foco do agente de ameaças. Por exemplo, o Sangfor[156] fez relatos em março sobre a atividade do Scarlet Ioke usando um *loader* geralmente chamado de "DgBase.dll". O *backdoor* de Linux RotaJakiro,[157] que também está equipado com a funcionalidade *botnet*, foi igualmente atribuído em código aberto ao Scarlet Ioke, com base em sobreposições de código entre o RotaJakiro e o *backdoor* OceanLotus.

Entre o fim de 2020 e setembro de 2021, observamos uma campanha[158] envolvendo *loaders* de DLL para Cobalt Strike e MetaSploit que usavam várias camadas de codificação Shikata Ga Nai para evitar sua detecção. Em alguns casos, as cargas úteis do Cobalt Strike usaram o serviço web Glitch para conduzir a atividade de C2.

Figura 24: Uma cadeia de ataque suspeita de Scarlet Ioke carregando CobaltStrike Beacon na memória



156. APT, Sangfor, https://mp.weixin.qq.com/s/WnKc0JbjA5_IsjPFSzFoYA (31/3/2021)
157. "RotaJakiro: A long live secret backdoor with 0 VT detection", 360 Netlab, https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/ (28/4/2021)
158. "Youre not Shikata Ga Nai believe this", PwC Threat Intelligence, CTO-TIB-20211102-02A

Em pelo menos um caso, a DLL foi carregada por um binário legítimo de Kingsoft, um software predominantemente usado em países cujo idioma é o mandarim chinês. Além disso, muitas das amostras de Cobalt Strike que identificamos estavam disfarçadas como o serviço QQ da Tencent ou como o mecanismo de busca chinês Sogou, uma tática consistente com o Scarlet Ioke. Essa evidência sugere, com probabilidade realista, que os binários tinham como objetivo atingir vítimas que falam chinês. Com base nos TTPs e nos ataques que observamos nessa campanha, avaliamos que há uma probabilidade realista de que ela tenha sido conduzida pelo Scarlet Ioke. Entre os fatores que contradizem essa avaliação destacam-se a falta de vínculos diretos com atividades anteriores do Scarlet Ioke e o uso de ferramentas típicas de teste de penetração que também poderiam fazer parte de um exercício doméstico da equipe vermelha.

Em última análise, os agentes de ameaças respondem de maneira diferente à divulgação e atribuição. Alguns, como Red Kelpie e Yellow Garuda, podem continuar operando sem alterar seus TTPs, enquanto outros podem mudar de ferramentas e técnicas ou até mesmo sofrer uma reestruturação radical. Com base nas observações, avaliamos como improvável que o Scarlet Ioke tenha parado de operar. Na verdade, consideramos provável que o agente de ameaças esteja se reequipando e reorganizando, com planos de ampliar sua atividade em novas campanhas.

Os agentes de ameaças respondem de maneira diferente à divulgação pública de suas atividades. Alguns, como Red Kelpie e Yellow Garuda, podem manter as operações sem alterar seus TTPs, enquanto outros (possivelmente também o Scarlet Ioke) podem mudar de ferramentas e técnicas ou até mesmo sofrer uma reestruturação radical.

Oriente Médio

Atividade de ameaças no Irã

A mudança de face das operações de sabotagem

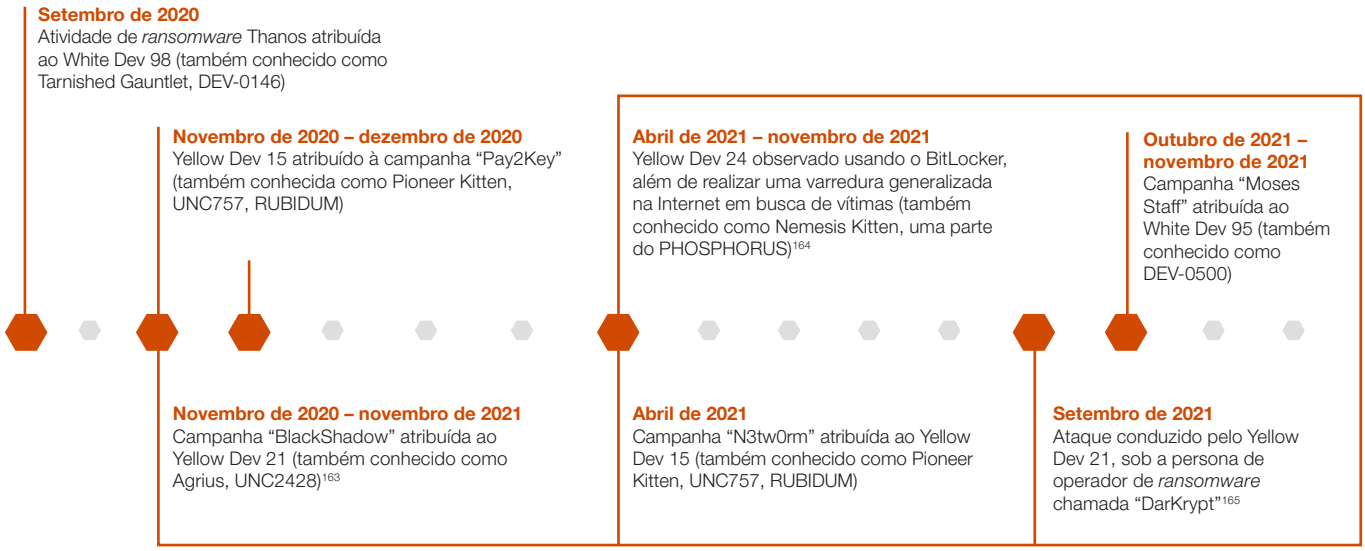
Os agentes de ameaças localizados no Irã têm um longo histórico de ataques de sabotagem para destruir e desestabilizar as organizações das vítimas. Esses ataques colocam os agentes de ameaça em evidência, o que geralmente leva à imputação de responsabilidades e ao escrutínio de suas operações pelos setores público e privado. Em uma tentativa de reduzir a atenção indesejada, os agentes de ameaças do Irã geralmente culpam coletivos hacktivistas ou se apresentam dessa forma, uma tática que continua a ser adotada por suspeitos de ameaças do Irã, como o White Dev 95 (conhecido também como Moses Staff).[159]

Observado pela primeira vez no fim de 2020 e ganhando destaque em 2021, registramos agentes de ameaças localizados no Irã ampliando táticas de motivação falsa, como atividades de Pay2Key e N3tw0rm do Yellow Dev 15 para utilizar *ransomware* para sabotagem em vez de ganho financeiro.[160] Em conjunto com comportamentos hacktivistas, isso pode funcionar para semear confusão sobre a verdadeira natureza e as intenções de um agente de ameaças.

Agentes de ameaças localizados no Irã, como Yellow Dev 15 e Yellow Dev 21, disfarçaram-se também de criminosos cibernéticos, em vez de hacktivistas, em algumas campanhas de sabotagem, nas quais também fingiram extorquir suas vítimas.[161] Em uma ocasião, o Yellow Dev 21 ameaçou vender os dados de uma vítima a terceiros se um pagamento não fosse feito.[162]

A PwC observou que os seguintes suspeitos de ameaças no Irã, com diferentes níveis de confiança, utilizam o *ransomware* em suas campanhas:

Figura 25



159. "Whose campaign is it anyway", PwC Threat Intelligence, CTO-TIB-20211121-01A
160. "Ransomware or sabotage, that is the question", PwC Threat Intelligence, CTO-SIB-20210927-01A
161. "Ransomware or sabotage, that is the question", PwC Threat Intelligence, CTO-SIB-20210927-01A
162. "Whose campaign is it anyway", PwC Threat Intelligence, CTO-TIB-20211121-01A
163. "New Version Of Apostle Ransomware Reemerges In Targeted Attack On Higher Education", SentinelOne, https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/#:~:text=New%20Version%20Of%20Apostle%20Ransomware%20Reemerges%20In%20Targeted%20Attack%20On%20Higher%20Education,-Amitai%20Ben%20Shushan&text=SentinelLabs%20has%20been%20tracking%20the,destructive%20attacks%20starting%20December%202020. (30/9/2021)
164. "Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021", Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/ (16/11/2021)
165. "Sharp dressed threat actor", PwC Threat Intelligence, CTO-TIB-20211222-02A

Estudo de caso

N3tw0rm

No final de abril de 2021, a variante de *ransomware* N3tw0rm surgiu visando vítimas israelenses nos setores de varejo, logística, ONGs e construção. A análise técnica posterior revelou semelhanças entre o N3tw0rm e outra variante de *ransomware* chamada Pay2Key. A variante é controlada pelo Yellow Dev 15 e não há registro do fornecimento de chaves de descriptografia (em dezembro de 2021, a carteira bitcoin listada no pedido de resgate N3tw0rm permaneceu vazia, uma indicação de que nenhuma vítima pagou o resgate). As motivações por trás dos ataques parecem ter relação com sabotagem e não com ganhos financeiros.[166]

Estudo de caso

Moses Staff

A partir de setembro de 2021, um agente de ameaças autodenominado Moses Staff (Cajado de Moisés) iniciou uma campanha destrutiva de "bloqueio e vazamento" contra organizações israelenses. Monitoramos o agente da ameaça por trás dessa campanha como White Dev 95. A maioria das vítimas observadas no fim de 2021 eram organizações israelenses com uma presença comercial não adequada à declaração de missão do agente de ameaças de expor vários crimes supostamente cometidos pelo governo israelense. Elas também abrangem uma gama diversificada de setores: jurídico, logística, varejo, serviços públicos, serviços profissionais, transporte, construção, manufatura e serviços financeiros. Essa vitimologia sugere que os alvos provavelmente foram escolhidos de forma oportunista, com o foco apenas em Israel como localidade, e não em expor qualquer suposto delito.

O White Dev 95 também apresentou várias semelhanças com diferentes campanhas com foco em Israel ocorridas em 2021 e atribuídas a agentes de ameaças localizados no Irã. Eles buscaram especificamente a atenção do público na tentativa de impulsionar suas atividades. Para alcançar esse efeito, o White Dev 95 opera várias plataformas digitais para vazar dados das vítimas, além de interagir diretamente com elas pelo Twitter. Um dos principais diferenciais entre a campanha Moses Staff e operações semelhantes de agentes de ameaças do Irã é que o White Dev 95 pula a fase de extorsão de seus ataques, preferindo vazar dados roubados sem aviso prévio. Isso provavelmente aumenta a confusão causada às vítimas, maximizando o elemento destrutivo da campanha.

166. "Pay2Key to N3tw0rm", PwC Threat Intelligence, CTO-TIB-20210513-01A

Você não consegue ensinar novos TTPs a um antigo agente de ameaças

A maioria dos agentes de ameaças com sede no Irã que monitoramos surgiu com novos tipos de ferramentas no ano passado, mas contando com técnicas já testadas e comprovadas. Os agentes de ameaças do Irã costumam ser conhecidos pelo uso de ferramentas de código aberto, principalmente as de segurança ofensiva, além de campanhas de engenharia social.

Ferramentas de código aberto

O Yellow Nix (também conhecido como Static Kitten, MERCURY, MuddyWater) usou ferramentas comerciais de administração remota de forma sistemática ao longo de 2021 – entre elas, ConnectWise Control (também conhecido como ScreenConnect) e Remote Utilities – para ter acesso inicial às vítimas.[167] Também observamos o Yellow Nix usando documentos habilitados para o Microsoft Office, inclusive como um mecanismo de distribuição do ConnectWise Control.[168]

Tanto o Yellow Dev 24[169] quanto o Yellow Dev 15[170] usaram a ferramenta FRP de código aberto. Ela permite que um sistema forneça acesso à rede a sistemas controlados por agentes de ameaças localizados fora da rede da vítima. Da mesma forma, o Yellow Orc (também conhecido como APT 33, Refined Kitten, Stonedrill) usa o PoshC2, um *framework* C2 de código aberto usado para pós-exploração e movimento lateral. Em 2021, observamos uma nova atividade de Yellow Orc, que incorporou uma estrutura semelhante de C2 disponível publicamente.[171]

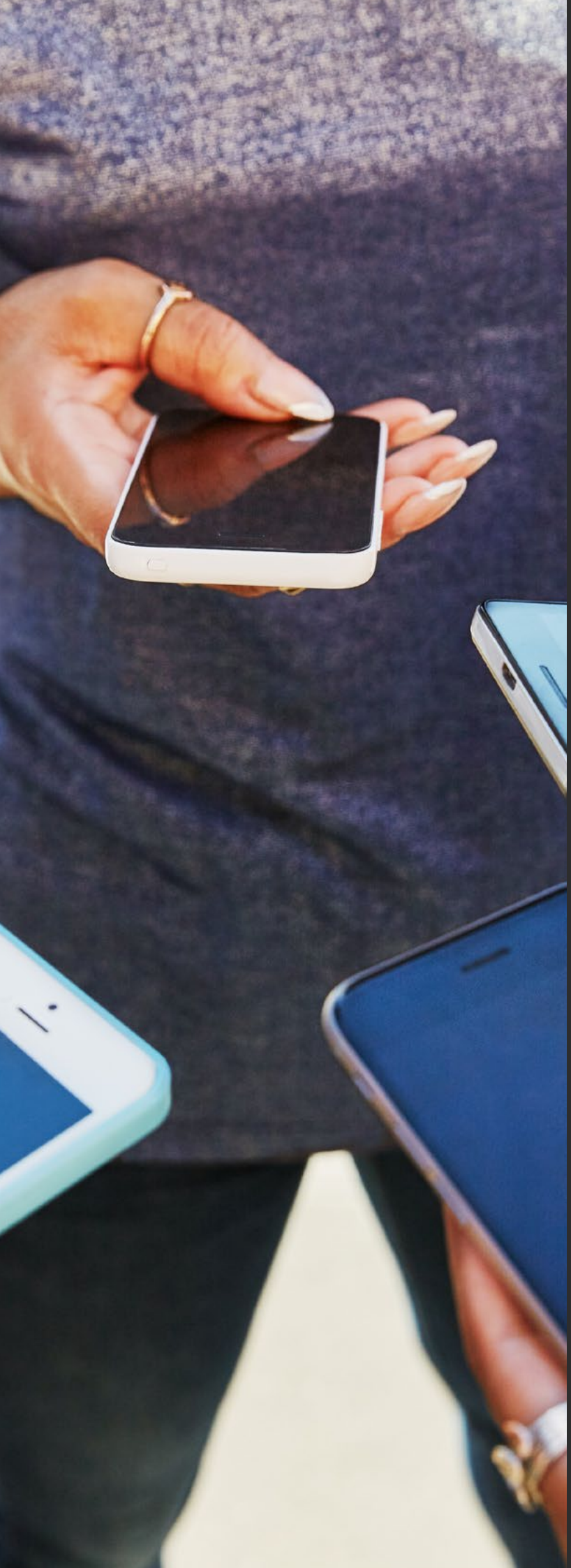
Engenharia social

Um denominador comum entre muitos agentes de ameaças do Irã é usar iscas de *phishing* com temas de emprego ou recrutamento, contando com plataformas de mídia social para se comunicar diretamente com os alvos e estabelecer uma relação de confiança. Em vários casos periféricos, técnicas de *phishing* e engenharia social ignoraram a autenticação multifator (MFA, na sigla em inglês). No entanto, segundo nossas observações, a MFA continua sendo altamente eficaz em frustrar a maioria dos ataques.[172]

O Yellow Maero (também conhecido como APT34, OilRig, COBALT GYPSY) tem um longo histórico de engenharia social. Em janeiro de 2021, observamos que ele usou um folheto de recrutamento com a marca de um provedor de serviços de TI legítimo sediado nos EUA e anunciou várias funções de TI, negócios e engenharia disponíveis no Oriente Médio. O documento de isca provavelmente é legítimo, embora tenha sido deturpado pelo agente da ameaça.

Em julho, o agente de ameaças que monitoramos como Yellow Orc (também conhecido como APT33, Elfin) realizou uma campanha envolvendo iscas de emprego e um site falso de busca de vagas para cargos no Oriente Médio,[173] principalmente com foco nos seguintes setores: petróleo e gás, químico, energia, biociências, manufatura, mineração, infraestrutura e governo.[174] O conteúdo de diretórios abertos também mostra que o agente de ameaça provavelmente começou o ano visando os EUA por meio de arquivos HTA maliciosos. Ao mesmo tempo, conduziu uma operação aproveitando um *malware* disfarçado de um painel de casos de covid-19 da Organização Mundial da Saúde (OMS).[175] O diretório aberto mostrou que o Yellow Orc provavelmente também usou imagens de uma pessoa do sexo feminino para fazer engenharia social com seus alvos.[176] As imagens se assemelham a relatórios de código aberto sobre a persona "Marcella Flores" operada pelo agente de ameaças que monitoramos como Yellow Liderc.[177] O Yellow Orc tem usado táticas de engenharia social com temas de emprego desde pelo menos 2017.

167. "Missed connections", PwC Threat Intelligence, CTO-TIB-20210216-01A
168. "A blast from the past", PwC Threat Intelligence, CTO-TIB-20210622-01A
169. "Scanning the internet for vulnerabilities", PwC Threat Intelligence, CTO-TIB-20211118-01A
170. "The mysteries of Pay2Key", PwC Threat Intelligence CTO-SIB-20210113-01A
171. "The [redacted] sheds light on a campaign", PwC Threat Intelligence, CTO-TIB-20210712-01A
172. "White Dev 75, like shooting phish in a barrel", PwC Threat Intelligence, CTO-TIB-20210303-01A
173. "Yellow Maeros Art Attack", PwC Threat Intelligence, CTO-TIB-20210226-02A
174. "New job, same malware", PwC Threat Intelligence, CTO-TIB-20210806-01A
175. "The [redacted] sheds light on a campaign, PwC Threat Intelligence, CTO-TIB-20210712-01A
176. "The [redacted] sheds light on a campaign, PwC Threat Intelligence, CTO-TIB-20210712-01A
177. "I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona", Proofpoint, https://www.proofpoint.com/us/blog/threat-insight/iknew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media (28/7/2021)



O Yellow Liderc (também conhecido como Tortoiseshell e TA456)[178] e um agente de ameaças estreitamente relacionado que monitoramos como Yellow Dev 13 continuaram a usar o LinkedIn e o Facebook para engenharia social ao longo de 2021, mantendo uma rede de empresas e personas de recrutamento falsas.[179] [180] Tanto a Microsoft quanto a Meta documentaram o processo persistente, mas paciente, do Yellow Liderc de usar as mídias sociais, geralmente durante vários meses entre a conexão inicial com o alvo e a distribuição de conteúdo malicioso.[181] [182]

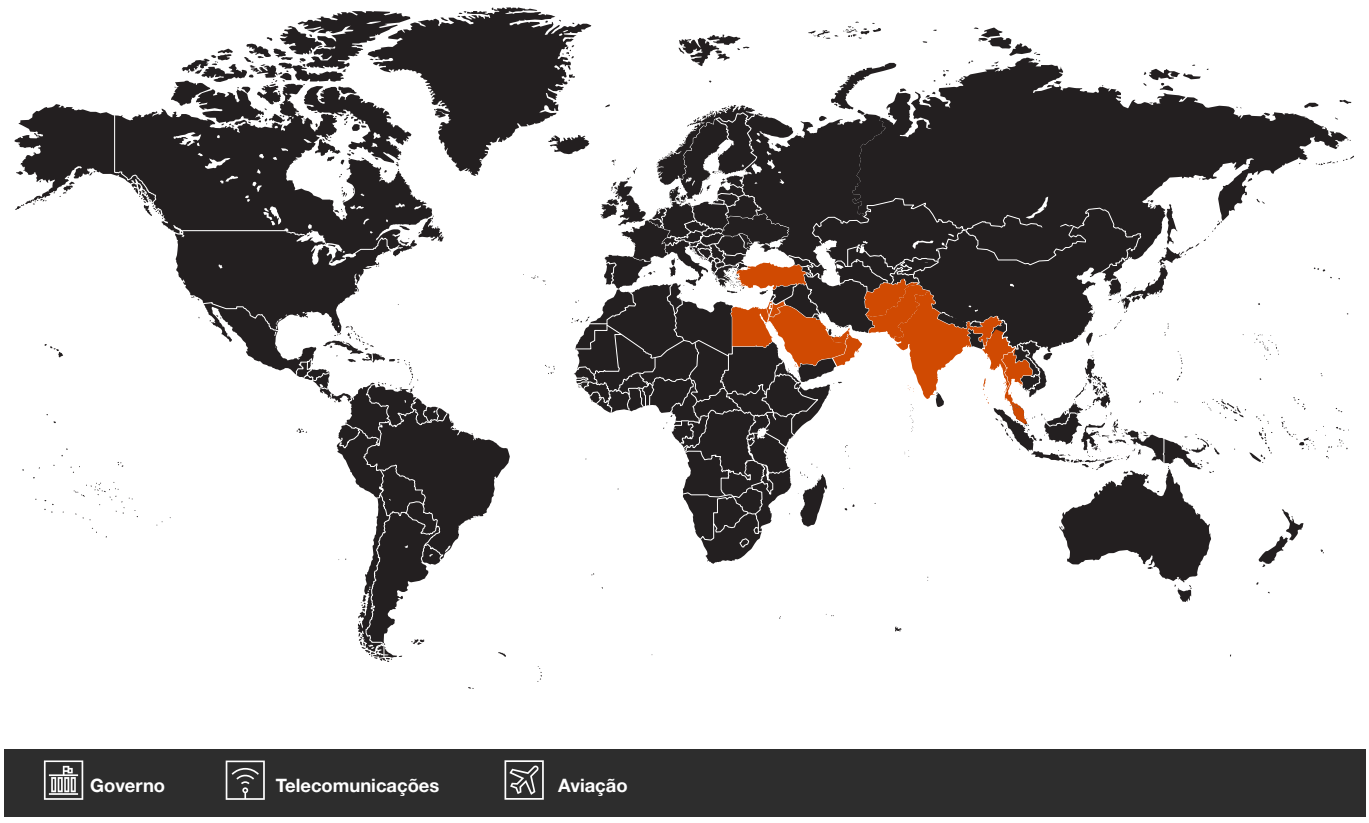
178. "Of course I'm real....", PwC Threat Intelligence, CTO-SIB-20210818-01A
179. "Eat, Sleep, Liderc, Repeat", PwC Threat Intelligence, CTO-TIB-20210730-01A
180. "Iran-based threat actor responses to rising geopolitical tensions", PwC Threat Intelligence, CTO-SIB-20200108-01A
181. "Taking Action Against Hackers in Iran", Meta, https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/ (15/7/2021)
182. "Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021", Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021 (16/11/2021)

Yellow Nix

O Yellow Nix continuou a ampliar seus horizontes além das regiões geográficas vizinhas ao Irã. Após um ano movimentado em 2020, quando ele atacou a Europa em várias campanhas, vimos esse agente de ameaças, em setembro de 2021, desviar sua atenção para o Sudeste Asiático. Os ataques aos setores de governo, aviação e telecomunicações na Malásia, especialmente, seguiram-se a conversas de cooperação econômica entre autoridades iranianas e malaias.[183] Esse costuma ser o caso do Yellow Nix, com sua atividade muitas vezes refletindo de perto os investimentos políticos e comerciais do Irã. O Yellow Nix também pareceu demonstrar um interesse maior pelo setor de aviação.

Em setembro de 2020, os Estados Unidos sancionaram pessoas relacionadas ao Yellow Mimas, um agente de ameaças conhecido por visar setores globais de aviação e telecomunicações para monitorar os movimentos dos viajantes. Desde então, os analistas da PwC não observaram a atividade do Yellow Mimas, e ele também esteve ausente nos relatórios de ameaças de código aberto. Ainda não está claro se o Yellow Mimas entrou em um período de inatividade, mas o aumento do Yellow Nix em visar e atuar contra organizações de aviação demonstra que seu objetivo de obter inteligência desse setor provavelmente está sendo cumprido, embora ainda não esteja claro em que medida o Yellow Nix consegue isso. A vitimologia recente do Yellow Nix também reflete a do Yellow Mimas e indica que o Yellow Nix pode estar envolvido na vigilância de indivíduos relevantes.[184]

Figura 26: Locais e setores atacados pelo Yellow Nix



Fonte: PwC

183. "Yellow Nix shifts south east", PwC Threat Intelligence, CTO-TIB-20211015-03A
184. "Yellow Nix has a complaint", PwC Threat Intelligence, CTO-TIB-20211216-02A

Yellow Dev 9

Relatado pela primeira vez por fontes abertas em 2019, o Yellow Dev 9 motivado por espionagem (também conhecido como Lyceum ou Siamese Kitten) compartilha semelhanças em sua vitimologia, infraestrutura e ferramentas com outro agente de ameaças do Irã que monitoramos como Yellow Maero. O Yellow Dev 9 continuou ativo em 2021, quando atacou os setores de telecomunicações e aviação africanos, fazendo engenharia social com alvos no LinkedIn e hospedando seu *malware* temático de recrutamento em domínios disfarçados de empresas de tecnologia da informação.[185] Apesar de vários pesquisadores de segurança divulgarem relatórios públicos sobre o Yellow Dev 9, o agente de ameaças continuou a desenvolver novas variantes de *malware*, chamadas *backdoors* "Milan" e "Shark", que usam conectividade de rede HTTP e DNS. A infraestrutura do Yellow Dev 9 tem um padrão específico, em que o agente de ameaças registrou domínios de comando e controle (C2) sistematicamente com nomes relacionados a DNS, "update" e CDN durante 2021.[186] O Yellow Dev 9 é conhecido por reutilizar sua infraestrutura histórica de campanhas anteriores.[187]

Yellow Garuda

Um dos agentes de ameaças mais ativos e amplamente relatados no ano passado foi o Yellow Garuda (também conhecido como Charming Kitten, PHOSPHORUS e ITG18). Esse agente é altamente capaz e persistente, tendo aumentado seu ritmo operacional em 2021 e mantido uma extensa rede de infraestrutura de *phishing*. As campanhas do Yellow Garuda variam de simples *phishing* de credenciais[188] à violação de sites legítimos,[189] implantação de *malware* móvel,[190] uso de *bots* do Telegram para identificar informações dos dispositivos das vítimas[191] e esforços redobrados de engenharia social.

Essas operações se traduzem em ataques generalizados a vítimas em todo o mundo e em vários setores. A vitimologia ao longo de 2021 incluiu conjuntos de alvos internos no Irã e em países vizinhos em todo o Oriente Médio, além de alvos típicos nos EUA e na Europa.

185. "New Iranian Espionage Campaign By "Siamesekitten" – Lyceum", ClearSky, https://www.clearskysec.com/siamesekitten (17/8/2021)
186. "Finding Yellow Dev 9, PwC Threat Intelligence, CTO-TIB-20211028-02A
187. "Lyceum calling", PwC Threat Intelligence, CTO-TIB-20200605-01A
188. "Get your shine on Yellow Garuda", PwC Threat Intelligence, CTO-TIB-20210514-01A
189. "Only if your invited", PwC Threat Intelligence, CTO-QRT-20210907-01A
190. "A fresh bouquet of malware", PwC Threat Intelligence, CTO-TIB-20210511-02A
191. "Charming Kittens Telegram bot", PwC Threat Intelligence, CTO-TIB-20210909-01A

Yellow Dev 19

Um agente de ameaças localizado no Irã que a PwC monitora como Yellow Dev 19 foi observado atacando sites relacionados à eleição presidencial dos Estados Unidos em 2020, no que o governo dos EUA avalia ser uma tentativa de influenciar e interferir na eleição.[192] Avaliamos em maio de 2021 que o Yellow Dev 19 provavelmente estava muito vinculado ao setor educacional iraniano, especificamente representado por um estudante ou membro do corpo docente, o que é apoiado por uma acusação de novembro de 2021 dos EUA, que aponta dois indivíduos com idades entre 23 e 26 anos.[193] Também identificamos que o Yellow Dev 19 provavelmente está interessado em atingir entidades governamentais da Arábia Saudita.[194]

De acordo com a acusação do governo dos EUA, a empresa supostamente responsável por liderar a tentativa de campanha é a Emennet Pasargad, que atua apoiando o governo iraniano.[195] Os analistas da PwC também observaram sobreposições entre essa empresa, e membros sancionados do seu conselho, e o Yellow Liderc.[196] A PwC avalia que a Emennet Pasargad e/ou seu pessoal provavelmente estão envolvidos em outras operações, como *ransomware* para fins de sabotagem, e estão bastante alinhados com o Exército dos Guardiães da Revolução Islâmica.

Yellow Dev 24

De pelo menos abril a novembro de 2021, a PwC observou dispositivos de varredura em massa do Yellow Dev 24 (também conhecido como Nemesis Kitten, parte do PHOSPHORUS) voltados para a Internet, inclusive dispositivos Fortinet e servidores Microsoft Exchange.[197] Em alguns casos, o Yellow Dev 24 implantou *ransomware* posteriormente via BitLocker, contando com ferramentas de código aberto e técnicas de *living-off-the-land*. O Yellow Dev 24 é um dos vários agentes de ameaças com origem no Irã que estão usando *ransomware* para fins de sabotagem, ao mesmo tempo que são capazes de realizar atividades de espionagem. O Yellow Dev 24 também é oportunista em sua seleção de alvos, o que torna esse agente de ameaças relevante para um público global.[198]

As vítimas dessa campanha eram geograficamente dispersas e incluíam organizações nos EUA, Austrália, Emirados Árabes Unidos e África do Sul.[199] O agente de ameaças supostamente comprometeu quase mil dispositivos em pouco mais de seis meses.[200] Uma atividade um pouco mais direcionada (embora ainda oportunista) ocorreu por meio de pulverização de senhas de empresas de tecnologia de defesa dos EUA e de Israel, portos de entrada no Golfo Pérsico e empresas globais de transporte marítimo com presença comercial no Oriente Médio.[201]

192. "Alert (AA20-304A) Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data", US CISA, https://us-cert.cisa.gov/ncas/alerts/aa20-304a
193. "Learning on the job with Yellow Dev 19", PwC Threat Intelligence, CTO-TIB-20201118-02A
194. "Learning on the job with Yellow Dev 19", PwC Threat Intelligence, CTO-TIB-20201118-02A
195. "Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election", United States Department of the Treasury, https://home.treasury.gov/news/press-releases/jy0494 (18/11/2021)
196. "New leaks and possible IRGC links", PwC Threat Intelligence, CTO-SIB-20210809-01A
197. "Scanning the internet for vulnerabilities", PwC Threat Intelligence, CTO-TIB-20211118-01A
198. "Scanning the internet for vulnerabilities", PwC Threat Intelligence, CTO-TIB-20211118-01A
199. "Scanning the internet for vulnerabilities", PwC Threat Intelligence, CTO-TIB-20211118-01A
200. "Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021", Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021 (16/11/2021)
201. "Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021", Microsoft, https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021 (16/11/2021)

Atividade de ameaças em todo o Oriente Médio

Teal Dev 2

O agente de ameaças turco Teal Dev 2 (também conhecido como StrongPity) continuou a implantar seu conhecido *backdoor* StrongPity ao longo de 2021, embora, de acordo com nossas observações, essa atividade tenha diminuído no segundo semestre do ano. Foram revelados novos TTPs do Teal Dev 2, com relatórios de código aberto mostrando links de infraestrutura entre o StrongPity e o *malware* Android. Esses links não eram conhecidos como parte do conjunto de ferramentas do agente de ameaças, mas provavelmente têm sido usados desde pelo menos 2019.[202] Com base nessas observações, avaliamos que o uso aparentemente moderado de ferramentas e técnicas específicas do Teal Dev 2 talvez as tenha feito passar despercebidas por vários anos, o que é um provável sinal de campanhas altamente direcionadas.

Grey Karkadann

O Gray Karkadann (também conhecido como Arid Viper, APT-C-23 e parte do Gaza Cybergang) continuou usando técnicas testadas e comprovadas para atacar entidades no Oriente Médio, com forte ênfase na política palestina e nas relações Palestina-Israel. Ao longo de 2021, isso incluiu o uso contínuo do Micropsia,[203] seu *malware* para Windows, que normalmente é acompanhado por documentos de isca alinhados com seus principais temas de ataque. Também observamos o desenvolvimento contínuo de seu *malware* para dispositivos móveis, que é distribuído por meio de lojas de aplicativos de terceiros ou sites controlados por agentes de ameaças. Relatórios de código aberto observam que o arsenal do Gray Karkadann agora inclui *malware* para iOS, além de seus implantes Android conhecidos.[204] O *malware* móvel do agente de ameaças contém ampla funcionalidade de vigilância e camuflagem, muitas vezes disfarçada de aplicativos legítimos.[205]

White Dev 21

Em maio de 2021, observamos um conjunto de atividades direcionadas a pessoas de idioma árabe com interesse em assuntos do Oriente Médio.[206] As atividades começaram pelo menos em 2019 e envolveram o uso de documentos com macros habilitadas e conteúdo sobre uma ampla gama de notícias e temas relacionados à Palestina, ao Líbano e ao Iraque. Isso indica que o agente de ameaças provavelmente visou várias vítimas separadas durante essa campanha. O relatório de código aberto vinculou a atividade a um agente de ameaças conhecido como WIRTE e enfatizou o ataque a várias organizações de destaque entre entidades governamentais e diplomáticas, escritórios de advocacia e instituições financeiras, o que torna o agente uma preocupação para uma ampla variedade de setores.[207] De acordo com nossas observações, o WIRTE compartilha sobreposições de infraestrutura com o White Dev 21, um agente de ameaças que observamos em 2019 usando iscas com temas de eleições e relações diplomáticas relacionados à política egípcia e palestina. Avaliamos que ele seja provavelmente um desdobramento do Gaza Cybergang.[208] [209]

202. "StrongPity APT Group Deploys Android Malware for the First Time", Trend Micro, https://www.trendmicro.com/en_us/research/21/g/strongpity-apt-group-deploysandroid-malware-for-the-first-time.html (21/7/2021)
203. "Threats under the Spotlight November 2021", PwC Threat Intelligence, CTO-TUS-20211203-01A
204. "Taking Action Against Arid Viper", Facebook, https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf (April 2021)
205. "Hiding in plain sight", PwC Threat Intelligence, CTO-TIB-20211126-01A
206. "Phishing in the Middle East", PwC Threat Intelligence, CTO-TIB-20210629-02A
207. "WIRTE's campaign in the Middle East "living off the land" since at least 2019", Kaspersky, https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-theland-since-at-least-2019/105044/ (29/11/2021)
208. "Elections in Palestine – on the campaign trail", PwC Threat Intelligence, CTO-TIB-20191216-02A
209. "There's a (Houdini)RAT in the Embassy", PwC Threat Intelligence, CTO-TIB-20191112-01A

Europa e antiga União Soviética

Agentes de ameaças localizados na Rússia continuaram suas operações cibernéticas em 2021, buscando acessar informações confidenciais ou sensíveis. Isso incluiu ataques a ministérios de governos em toda a Europa e países vizinhos à Rússia. Vimos o interesse especial do agente de ameaças Blue Athena (também conhecido como Sofacy) no setor de mineração e recursos naturais na Ásia Central.

Também continuamos a ver ataques sistemáticos a entidades na Ucrânia pelo agente de ameaças russo Blue Otso. Monitoramos a atividade do Blue Otso em ataques a entidades no leste da Ucrânia, pouco antes de o Serviço de Segurança Ucraniano (SBU) desmascarar vários supostos operadores do Blue Otso em novembro de 2021.

Além dos agentes de ameaças localizados na Rússia, nossa pesquisa também incluiu o monitoramento de outras atividades maliciosas. O White Tur é um exemplo de um agente de ameaças ainda não atribuído, cujo interesse se concentrou em setores e locais muito específicos. Em outros lugares, o agente de ameaças Rose Matsil, localizado na Geórgia, foi observado em associação com ataques a organizações médicas na Rússia em 2021.

Blue Dev 5 – um *phisher* 'nobre'

O agente de ameaças de origem russa Blue Dev 5 (também conhecido como NOBELIUM,[210] NobleBaron) foi um dos mais prolíficos e tecnicamente sofisticados que monitoramos em 2021. O Blue Dev 5 demonstrou novas técnicas e competência cuidadosa, incluindo a violação de ambientes de nuvem da Microsoft e exploração de relacionamentos de confiança entre organizações.

O Blue Dev 5 teve êxito na violação de vários revendedores de nuvem e MSPs, aproveitando relações de confiança na nuvem mantidas por essas organizações com seus clientes para violar os ambientes de nuvem dos clientes e explorar o acesso fornecido aos MSPs a fim de penetrar as redes de seus clientes. Depois de ter acesso às organizações que ataca, o Blue Dev 5 procura ter acesso persistente, camuflado e de longo prazo às instâncias do Azure AD e do Microsoft 365, incluindo contas privilegiadas e dados confidenciais. O Blue Dev 5 demonstrou altos níveis de segurança operacional e tomou medidas para evitar detecções e tornar mais difícil para as organizações que são vítimas de seus ataques investigarem atividades suspeitas (por exemplo, fazer login em contas comprometidas nessas organizações a partir de endereços IP residenciais).

No momento, não podemos vincular definitivamente o Blue Dev 5 ao agente de ameaças por trás dos ataques da cadeia de suprimentos da SolarWinds que monitoramos como Blue Nova.[211] [212] No entanto, observamos uma sobreposição relevante nas técnicas usadas pelos dois, inclusive nas técnicas para executar ataques sofisticados baseados em identidade contra ambientes de nuvem da Microsoft. Também observamos que tanto o Blue Dev 5 quanto o Blue Nova[213] se aproveitam das relações de confiança de terceiros para ter acesso aos ambientes de TI das organizações.

210. Obs.: não agrupamos a atividade do Blue Dev 5 com o mesmo agente de ameaça que conduziu a atividade SolarWinds (que monitoramos como Blue Nova) devido a diferenças nos TTPs observados.
211. O NCSC do Reino Unido avaliou como alta a probabilidade de que esse agente seja o Serviço de Inteligência Estrangeira da Rússia (SVR).
212. "UK and US call out Russia for SolarWinds compromise", NCSC, https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise (15/4/2021)
213. O Blue Nova atacou o Mimecast para ter acesso às chaves usadas para autenticar contas de serviço nos servidores de e-mail das vítimas, além de atacar o software desenvolvido pela SolarWinds.

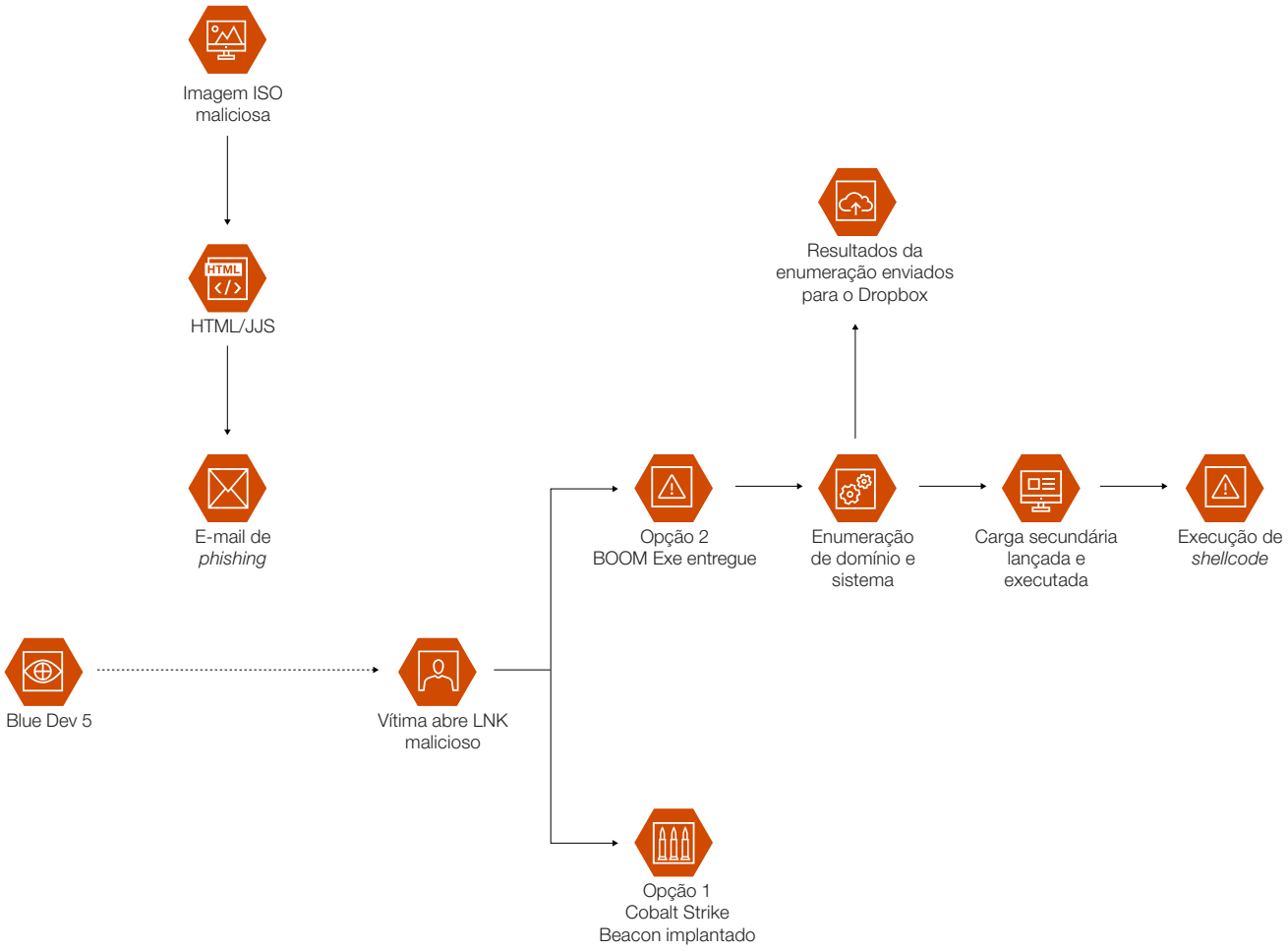
As organizações preocupadas com a ameaça do Blue Dev 5 devem tomar medidas para:

- implementar uma estratégia robusta de acesso privilegiado que inclua o uso de práticas de administração seguras e restrições rigorosas em torno do uso de acesso privilegiado;
- monitorar os logs do Azure AD e do Microsoft 365 em busca de técnicas usadas para comprometer e abusar de contas privilegiadas, técnicas de persistência e eventos globais raros; e
- auditar regularmente as configurações e relações de confiança da nuvem (Azure AD, Microsoft 365 e Azure).

O Blue Dev 5 também foi observado usando outras técnicas conhecidas para ter acesso aos ambientes das organizações, incluindo pulverização de senha e uso de credenciais comprometidas.

O Blue Dev 5 atraiu bastante atenção em maio de 2021, quando realizou uma campanha de *phishing* disfarçada de USAID, para distribuir o *malware* Cobalt Strike Beacon empacotado com um *loader* personalizado. Extraímos a seguinte visão dessa atividade:

Figura 27: Uma cadeia de intrusão Blue Dev 5 envolvendo exfiltração do Dropbox

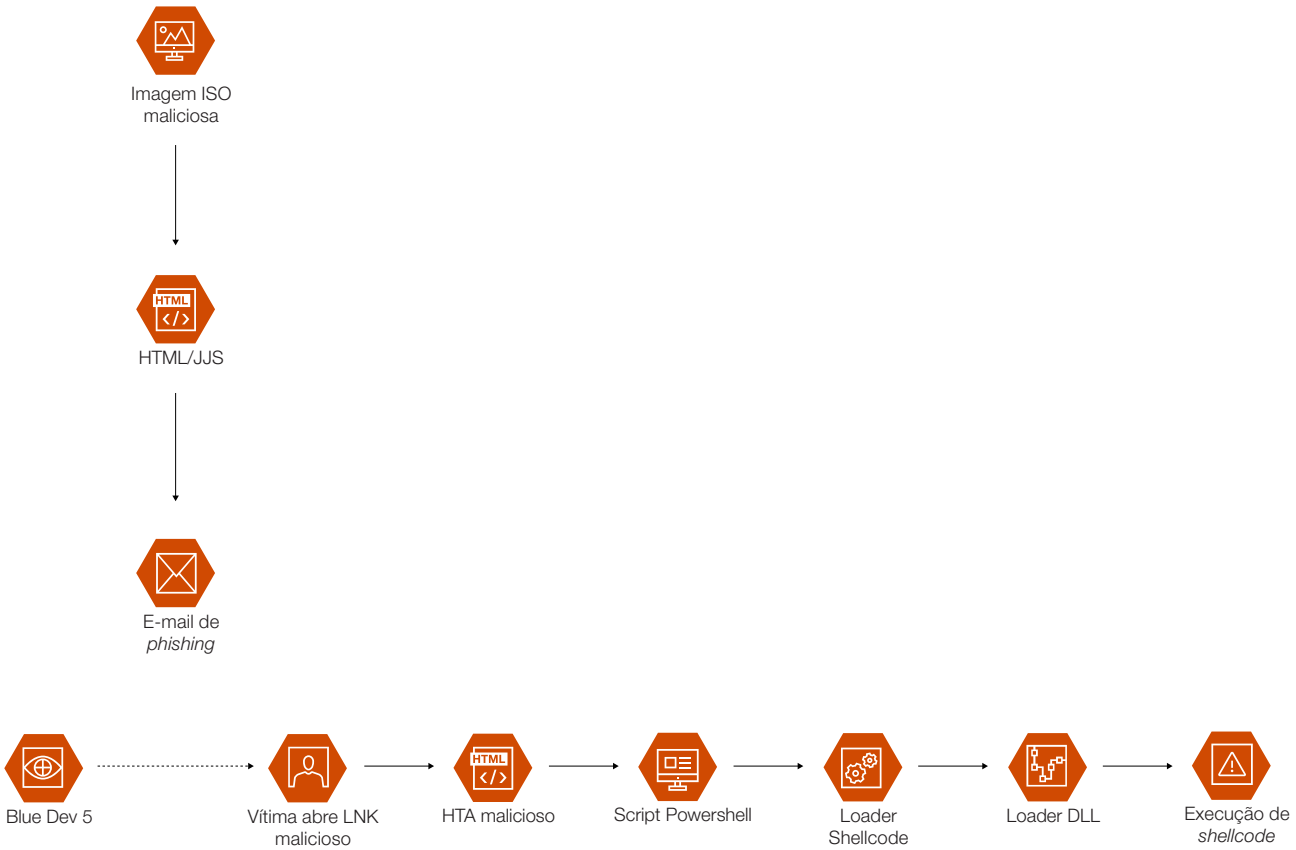


Há evidências de que os anexos HTML do primeiro estágio foram abertos por funcionários de várias embaixadas em toda a Europa,[214] o que dá uma visão do amplo ataque realizado por esse agente de ameaças. Algumas cargas úteis usadas pelo Blue Dev 5 parecem ter sido mais direcionadas: uma observada em março de 2021[215] buscou variáveis de ambiente relacionadas ao Ministério das Relações Exteriores de um país do Leste Europeu; outra se passou por uma atualização de um sistema de gerenciamento de documentos do governo ucraniano.[216]

Ao monitorar a infraestrutura do Blue Dev 5, também observamos que seus TTPs se tornam mais complexos. Por exemplo, em uma isca HTML que provavelmente foi criada em novembro de 2021, o agente de ameaças adicionou vários outros estágios entre a isca HTML inicial e a carga útil do Cobalt Strike Beacon entregue aos alvos. Nesse e em outro caso que identificamos, o documento de isca pretendia notificar a vítima de que uma embaixada foi fechada devido à covid-19.

Avaliamos como altamente provável que o Blue Dev 5 continue ativo ao longo do próximo ano e que seus TTPs continuem a evoluir ao longo do tempo para escapar melhor da detecção.

Figura 28: uma variante de uma cadeia de intrusão de acesso inicial do Blue Dev 5



214. "Blue Dev 5 - The Roots of Targeting", PwC Threat Intelligence, CTO-TIB-20210608-01A
215. "Blue Dev 5 - Mysteries of Foreign Affairs", PwC Threat Intelligence, CTO-TIB-20210527-01A
216. "NobleBaron | New Poisoned Installers Could Be Used In Supply Chain Attacks", Volexity, https://www.sentinelone.com/labs/noblebaron-new-poisoned-installerscould-be-used-in-supply-chain-attacks/ (1/6/2021)

Foco nos Bálcãs: White Tur

Em janeiro de 2021, a PwC observou um domínio de *phishing* dirigido aos militares sérvios.[217] Logo depois, identificamos infraestrutura adicional relacionada que mostrava ataques em andamento a organizações governamentais e de defesa da Sérvia e da República Srpska desde pelo menos 2017. Estamos monitorando essa atividade em associação com um agente de ameaças que chamamos de White Tur. A República Srpska é uma das duas entidades federais da Bósnia-Herzegovina. A atividade ocorreu em um cenário estratégico complexo, pois a região dos Bálcãs tem uma história diversificada, mas conturbada. Os ataques à Sérvia e à República Srpska são de especial interesse, pois, nos últimos meses, há apelos cada vez mais fortes por parte de alguns grupos para que a República Srpska ganhe mais autonomia ou se separe por completo.[218]

A infraestrutura adicional revelou atividades anteriores que o Ministério do Interior da República Srpska divulgou em abril de 2020:[219] uma campanha de *spear phishing* com uma mensagem atribuída ao primeiro-ministro da República Srpska que levava a um arquivo HTA malicioso responsável pela execução do código PowerShell de um domínio C2. Identificamos esse domínio como conectado ao domínio de *phishing* militar sérvio.

O monitoramento da infraestrutura relacionada ao longo do ano identificou ataques a organizações de pesquisa e desenvolvimento sérvias estreitamente vinculadas às forças armadas e de defesa.[220] Em setembro de 2021, o White Tur realizou uma violação estratégica em um site para hospedar documentos e arquivos usados como armas com temas de defesa e sobre a República Srpska.[221] Antes disso, os arquivos do White Tur usados como armas eram hospedados em uma infraestrutura dedicada registrada pelo agente de ameaças. Em termos de recursos, observamos o White Tur empregar documentos com macros usadas como armas que levam a um *backdoor* JScript. Como alternativa, o White Tur implantou um *backdoor* do Windows, empacotado em um arquivo usado como arma contendo o projeto de código aberto OpenHardwareMonitor, que utilizava objetos de transferência de bits COM para enviar informações de volta ao C2.

De modo geral, avaliamos que o White Tur provavelmente é um agente de ameaças motivado por espionagem e está vinculado a uma nação. Com base em tensões regionais, vários possíveis candidatos estão envolvidos nessa atividade, tanto dentro quanto fora dos Bálcãs. No momento, não temos evidências técnicas suficientes para fazer uma avaliação altamente confiável dos possíveis apoiadores do White Tur. No entanto, avaliamos que provavelmente os Bálcãs continuarão sendo uma região de interesse para agentes de ameaças de várias origens e motivações, entre eles o White Tur. Exploramos mais o White Tur em **nosso blog**.

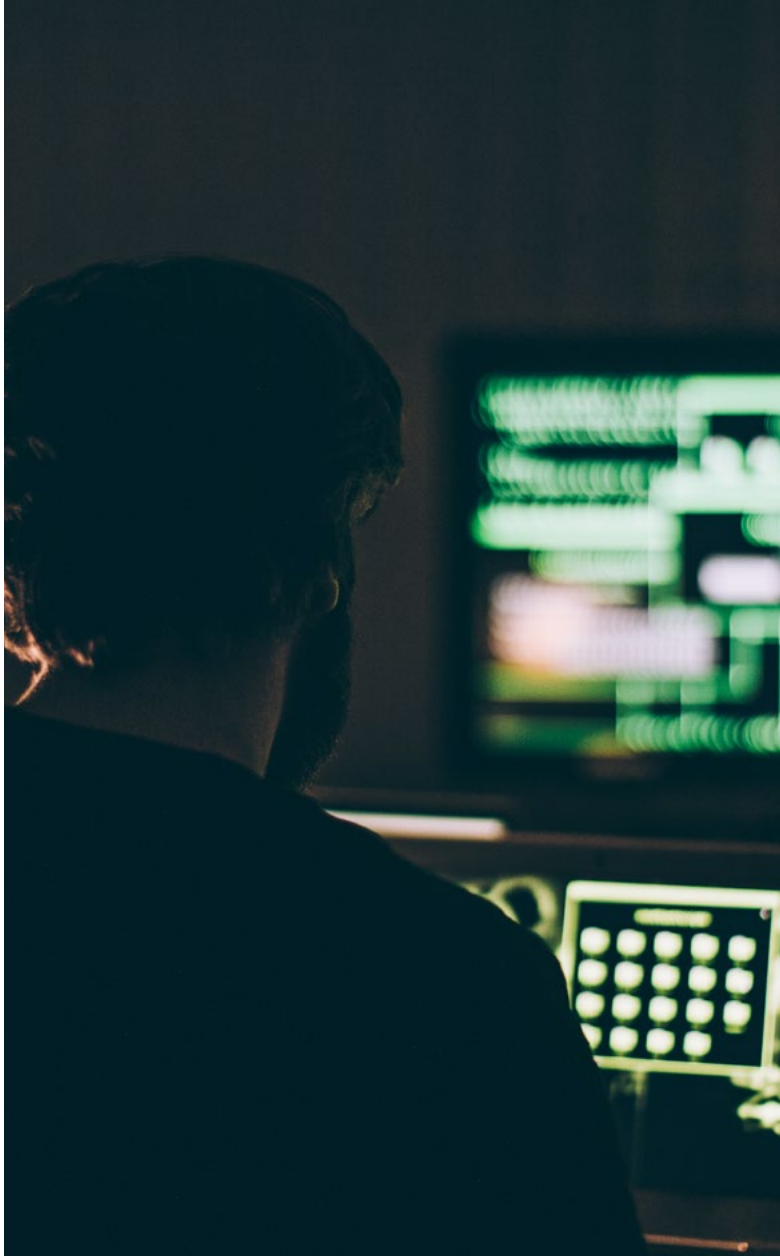
217. "(Darth) Vladars under attack Part 1", PwC Threat Intelligence, CTO-TIB-20210310-01A
218. "Bosnia is in danger of breaking up, warns top international official", The Guardian, https://www.theguardian.com/world/2021/nov/02/bosnia-is-in-danger-of-breakingup-warns-eus-top-official-in-the-state (2/11/2021)
219. "MINISTARSTVO UNUTRAŠNJIH POSLOVA REPUBLIKE SRPSKE", Republika Srpska Ministry of Interior, https://mup.vladars.net/lat/index.php?vijest=vtk&id=23325&vrsta=aktuelnosti (24/4/2020)
220. "(Darth) Vladars under attack Part 2", PwC Threat Intelligence, CTO-TIB-20210423-01A
221. "(Darth) Vladars under attack Part 3", PwC Threat Intelligence, CTO-TIB-20210903-01A

Alienação: Blue Odin

O Blue Odin (também conhecido como CloudAtlas) é um agente de ameaças conhecido por tomar como alvo uma variedade de organizações na Rússia e regiões da Ucrânia anexadas à Rússia usando documentos maliciosos. Ele também controla de perto as cargas úteis que esses documentos distribuem para aumentar a dificuldade que os pesquisadores têm de rastreá-lo.

Em 2021, observamos várias novas facetas na atividade do Blue Odin, desde erros de segurança operacional (OPSEC) até novos TTPs. Em um caso, um documento malicioso usado para atacar o Ministério da Defesa de um país da Europa Central continha links embutidos para um serviço de tradução on-line, que parece ter sido usado para traduzir a fonte do conteúdo da isca do inglês original para o ucraniano. Isso sugere que o operador responsável por preparar o documento pode ter o ucraniano como como idioma nativo.

Outra observação foi o uso do Responder pelo Blue Odin no início de 2021. O Responder é uma ferramenta de código aberto usada para realizar ataques de autenticação forçada SMB. Nesse tipo de ataque, o sistema da vítima tenta se autenticar em um servidor controlado pelo agente da ameaça usando NTLM. Isso permite que o agente da ameaça capture *hashes* de desafio. Mais tarde, esses *hashes* podem sofrer ataques de força bruta *off-line* para recuperar a senha da vítima. O documento malicioso em questão provavelmente visava indivíduos associados a entidades diplomáticas e de relações exteriores. Ele continha caminhos UNC para imagens em servidores controlados por agentes de ameaças que resultaram no ataque de autenticação forçada descrito acima. Curiosamente, um dos endereços IP embutidos no documento provavelmente era um erro de digitação: o IP especificado não parecia estar hospedando um servidor Responder, mas sim um endereço IP com uma única diferença de caractere. Isso representa uma ruptura com relação às técnicas anteriores usadas nos documentos maliciosos do agente de ameaças, que geralmente usavam links de modelo remoto. Em outros aspectos, a atividade do Blue Odin permaneceu muito semelhante à observada anteriormente: como um documento malicioso detectado em dezembro de 2021.[222]



Ele buscou um modelo remoto contendo uma exploração do Equation Editor que baixa e executa um HTA e, por sua vez, implanta uma variante do VBSshower. Essa cadeia é muito semelhante à cadeia de exploração documentada pela Kaspersky em 2019.[223]

Com base na atividade que observamos, avaliamos que há uma probabilidade realista de que os alvos do Blue Odin estejam alinhados com as prioridades estratégicas ucranianas, e não russas. Por exemplo, a atividade do Blue Odin dentro das fronteiras da Ucrânia parece se concentrar principalmente nas regiões autoproclamadas separatistas no leste da Ucrânia e na Crimeia. Também observamos o Blue Odin visando organizações russas, inclusive nos setores de energia e governo.[224]

222. "Hunting Blue Odin Servers", PwC Threat Intelligence, CTO-TIB-20211215-01A
223. "Recent Cloud Atlas activity" Kaspersky, https://securelist.com/recent-cloud-atlas-activity/92016/ (12/8/2019)
224. "Exploring Blue Odin", PwC Threat Intelligence, CTO-TIB-20210308-01A

O Blue Otso em uma montanha-russa

O Blue Otso (também conhecido como Gamaredon, Armageddon) experimentou grandes sucessos e reveses em 2021, desde amplas violações de sistemas sensíveis até a exposição pelo Serviço de Segurança da Ucrânia.

Em fevereiro, o Centro Nacional de Coordenação de Segurança Cibernética da Ucrânia informou que o Blue Otso havia comprometido os sistemas de gerenciamento de documentos do governo ucraniano conhecidos como SEI EB[225] e ASKOD.[226] Embora os indicadores iniciais de comprometimento fossem escassos, identificamos um conjunto de arquivos que provavelmente foi carregado em um varredor on-line para vários antivírus por um indivíduo ou por indivíduos envolvidos na resposta a incidentes relacionados a um único servidor ASKOD.[227] Esses arquivos incluíam várias ferramentas de *malware* Otso, como scripts de download, ferramentas de exfiltração, um cliente VNC e um script usado para adicionar referências de modelo remoto a documentos do Microsoft Word, que estão de acordo com as avaliações feitas pelo NCCC. Esses arquivos também incluíam carimbos de data/hora de modificação, que avaliamos como provavelmente precisos para os horários de implantação ou modificação na máquina da vítima. Esses carimbos de data/hora sugerem que o agente de ameaças provavelmente teve acesso à vítima desde pelo menos 5 de fevereiro de 2021, várias semanas antes da divulgação do incidente.

As operações do Blue Otso também enfrentaram perturbações consideráveis em 2021. O primeiro exemplo relevante foi divulgado pelo Serviço de Segurança da Ucrânia (SBU) em abril, com a prisão de uma pessoa em conexão com um indivíduo que enviou mensagens para os números pessoais de funcionários do SBU.[228] Essas mensagens continham um link para um site que mais tarde identificamos como murders-dkr[.]ru, que, por sua vez, continha um link para um arquivo supostamente contendo listas de funcionários da SBU pelos quais uma das entidades separatistas oferecia recompensas. Esse foi o primeiro indicador disponível em código aberto de que o Blue Otso, antes considerado um agente de ameaças baseado na Rússia, pode muito bem ser apoiado por atividades de regiões não ocupadas dentro da Ucrânia.

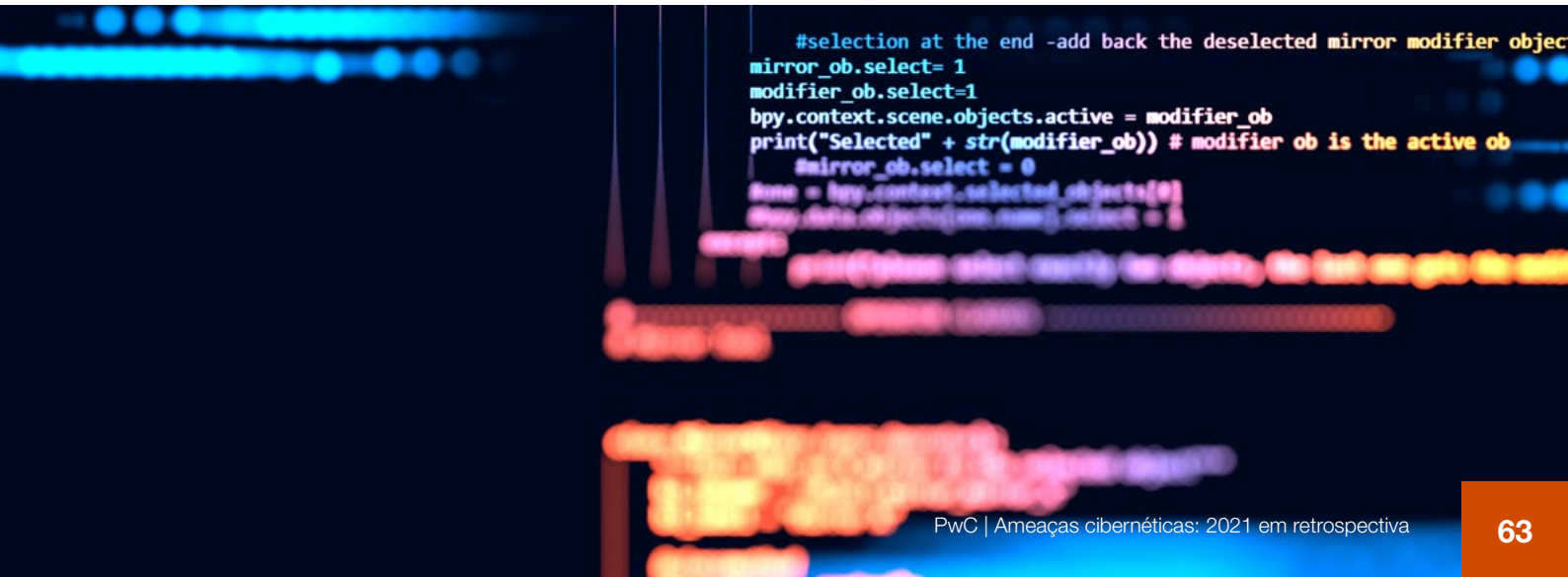
Isso foi expandido em novembro de 2021, quando o SBU divulgou as identidades de vários operadores do Blue Otso e alegou que a atividade do agente da ameaça está vinculada a uma unidade do FSB da Rússia com sede na Crimeia.[229] [230] Essa unidade é subordinada supostamente ao 18º Centro do FSB, também conhecido como Centro de Segurança da Informação, uma unidade que já foi associada a violações de dados pelo Departamento de Justiça dos EUA. Segundo relatos,[231] o SBU sugeriu pela primeira vez o envolvimento do 18º Centro em 2015, quando também sugeriu o envolvimento do 16º Centro do FSB, mais conhecido por sua associação com o Blue Python (também chamado Turla ou Snake). Nossa análise[232] revelou que esse anúncio ocorreu em meio a relatos da expansão militar russa perto da fronteira com a Ucrânia após exercícios militares de grande escala, antes da guerra na Ucrânia.

225. "The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies", NCCC, https://www.rnbo.gov.ua/en/Diialnist/4823.html (24/2/2021)
226. "The NCCC at the NSDC of Ukraine has updated information on cyberattacks on the document management system of state bodies", NCCC, https://www.rnbo.gov. ua/en/Diialnist/4824.html (25/2/2021)
227. "Inside the ASKOD Compromise", PwC Threat Intelligence, CTO-TIB-20210319-01A
228. "SBU finds hacker hunting for personal information of employees", Security Service of Ukraine, https://ssu.gov.ua/en/novyny/sbu-vyiavyla-khakera-yakyi-poliuvav-napersonalni-dani-spivrobitnykiv-sluzhby (23/4/2021)
229. "SSU identifies FSB hackers responsible for over 5,000 cyber attacks against Ukraine", Security Service of Ukraine, https://ssu.gov.ua/en/novyny/sbu-vstanovylakhakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy (4/11/2021)
230. "Ukraine discloses identity of Gamaredon members, links it to Russia's FSB", The Record: Catalin Cimpanu, https://therecord.media/ukraine-discloses-identity-ofgamaredon-members-links-it-to-russias-fsb/ (4/11/2021)
231. "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare", Looking Glass Cyber, https://web.archive.org/web/20190921173500/https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf (28/4/2015)
232. "Blue Otsos Armageddon", PwC Threat Intelligence, CTO-SIB-20211210-01

04 |

Novos agentes de ameaças em destaque

Nesta seção, destacamos os agentes de ameaças cibernéticas específicos que descobrimos em 2021. Isso não significa que eles não estivessem ativos antes. No entanto, à medida que expandimos continuamente nosso monitoramento e identificamos novos agentes de ameaças em função de nossa visibilidade e nossa coleta, consideramos valioso fornecer cobertura neste relatório para agentes de ameaças menos conhecidos e que ainda estamos buscando compreender totalmente. Os agentes de ameaças que descrevemos a seguir foram incluídos porque exibiram atividades relevantes, seja em termos de recursos, alvos, vínculos com outros agentes de ameaças ou do tipo de operações que realizam.



Red Dev 17

Em 2021, começamos a monitorar uma série de invasões sob o nome Red Dev 17 que avaliamos terem sido conduzidas provavelmente por um agente de ameaças localizado na China. Nossa análise sugere que o Red Dev 17 está ativo desde pelo menos 2017.

Os alvos observados do Red Dev 17 estão principalmente na Índia e incluem os militares indianos, uma empresa multinacional de tecnologia localizada na Índia e uma empresa estatal de energia. Avaliamos como altamente provável que o agente da ameaça por trás das invasões associadas ao Red Dev 17 também seja responsável pela campanha conhecida em código aberto como Operation NightScout.

O Red Dev 17 é um usuário do modelo 8.t de conversão de documentos em armamentos (também conhecido como RoyalRoad) e abusa de utilitários benignos, como os binários Logitech ou Windows Defender, para instalar e executar variantes Chinoxy ou PoisonIvy nos sistemas das vítimas.

Identificamos vínculos de capacidade e infraestrutura entre o Red Dev 17 e o agente de ameaças que chamamos de Red Hariasa (também conhecido como FunnyDream APT), além de sobreposições de infraestrutura com o Red Wendigo (também conhecido como Icefog ou RedFoxtrot) e com servidores ShadowPad C2. No momento, não temos evidências suficientes para vincular diretamente o Red Dev 17 a qualquer um desses agentes de ameaças. No entanto, avaliamos com probabilidade realista que o Red Dev 17 opere dentro de um cluster de agentes de ameaças que compartilham ferramentas e infraestrutura, além de enfoque marcado em alvos no Sudeste Asiático e na Ásia Central.

Blue Dev 6

Em outubro de 2021, observamos vários documentos convertidos em armas que usavam *workers* da Cloudflare como canal C2. Avaliamos que essa atividade provavelmente foi conduzida pelo Blue Dev 6 (também conhecido como ReconHellCat), um agente de ameaças divulgado pela QuoIntelligence em agosto de 2020.[233] Os documentos usavam modelos e macros remotas para executar uma carga útil baixada de um C2 de um *worker* da Cloudflare. A carga útil, que foi fortemente ofuscada, tinha várias semelhanças com o *malware* BlackSoul (também conhecido como BlackWater), incluindo código usado para iterar nas pastas do navegador e fazer a autenticação durante a comunicação C2. As campanhas que analisamos visavam uma série de setores, como energia, defesa e governo, além de uma organização humanitária internacional.

Yellow Dev 23

Monitoramos um novo *cluster* de atividades com foco nos setores de telecomunicações e TI como Yellow Dev 23 (também conhecido como MalKamak ou DEV-0270). Fontes abertas divulgaram esse agente de ameaças no fim de 2021 e descreveram uma campanha fortemente concentrada em Israel, especificamente nos setores de TI e telecomunicações.[234] [235] Além dos relatórios de código aberto, observamos o agente de ameaças fazendo *typosquatting* (sequestro de domínios) entre fevereiro e julho para usurpar conexões de login do Facebook e do Office365. Várias das amostras de *malware* atribuídas em código aberto a esse agente de ameaças têm sobreposições com outro agente de ameaças localizado no Irã que monitoramos como Yellow Liderc, conhecido por atacar o setor de TI no Oriente Médio.[236]

233. "ReconHellcat Uses NIST Theme as Lure To Deliver New BlackSoul Malware", QuoIntelligence, https://quointelligence.eu/2021/01/reconhellcat-uses-nist-theme-aslure-to-deliver-new-blacksoul-malware/ (6/1/2021)
234. "Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms", Cybereason, https://www.cybereason.com/blog/operation-ghostshell-novel-rattargets-global-aerospace-and-telecoms-firms (6/10/2021)
235. "Iran-linked DEV-0343 targeting defense, GIS, and maritime sectors", Microsoft, https://www.microsoft.com/security/blog/2021/10/11/iran-linked-dev-0343-targetingdefense-gis-and-maritime-sectors/ (11/10/2021)
236. "Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks", Symantec, https://symantec-enterprise-blogs.security.com/blogs/threatintelligence/tortoiseshell-apt-supply-chain (18/9/2019)

Estudo de caso de resposta a incidentes:

White Dev 89 chamando

Em 2021, apoiamos uma investigação de resposta a incidentes em uma organização de saúde envolvendo um agente de ameaças que chamamos de White Dev 89. Esse agente foi observado realizando ataques oportunistas, provavelmente usando campanhas de publicidade maliciosa, para fornecer aplicativos trojanizados de Zoom, AnyDesk e Windscribe para suas vítimas. Eles instalariam os aplicativos legítimos, mas implantariam e executariam um script mal-intencionado do PowerShell (provavelmente uma versão modificada de um agente do PowerShellEmpire). Esse acesso permitiu que o agente de ameaças realizasse reconhecimento básico no sistema infectado.[237]

Depois que o White Dev 89 identificou o perfil de uma máquina comprometida, observamos que ele lançava um script PowerShell adicional para implantar o Cobalt Strike Beacon. Isso deu início a mais atividades, como a movimentação lateral via SMB para outros sistemas na rede. Entre outras técnicas de movimentação lateral usadas pelo White Dev 89, estão o comprometimento de contas com privilégios elevados, a execução de ferramentas como ADFind e BloodHound para mapear a rede de destino e o uso de 7-ZIP e SubInAcl durante a pós-exploração.

Embora os objetivos finais desse agente de ameaças não sejam claros, encontramos conexões com outras campanhas conhecidas. Em especial, vimos sobreposições com a infraestrutura usada antes em campanhas do QakBot, o que nos leva a supor que o White Dev 89 é o mesmo agente de ameaças por trás do QakBot ou já usou o QakBot para acesso inicial.

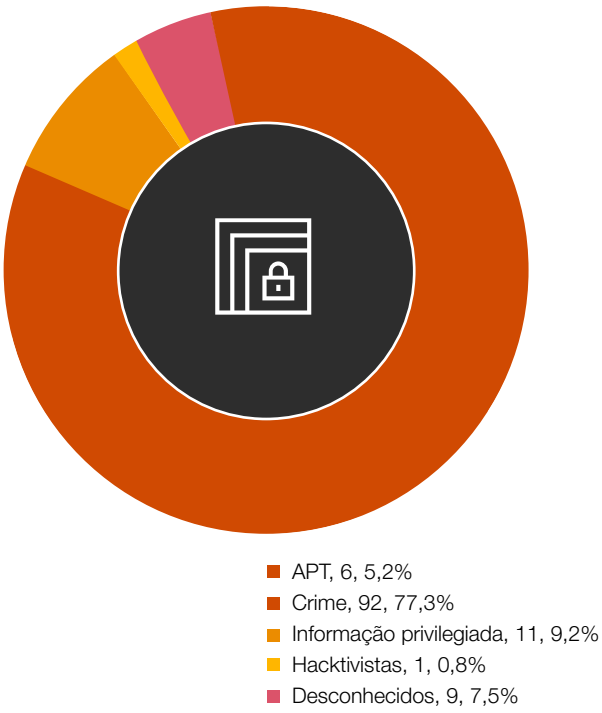
237. "A Zoom call with White Dev 89", PwC Threat Intelligence

Estatística de resposta a incidentes da PwC

Figura 29: casos de *ransomware* na resposta a incidentes por setor, 2021

Fonte: PwC

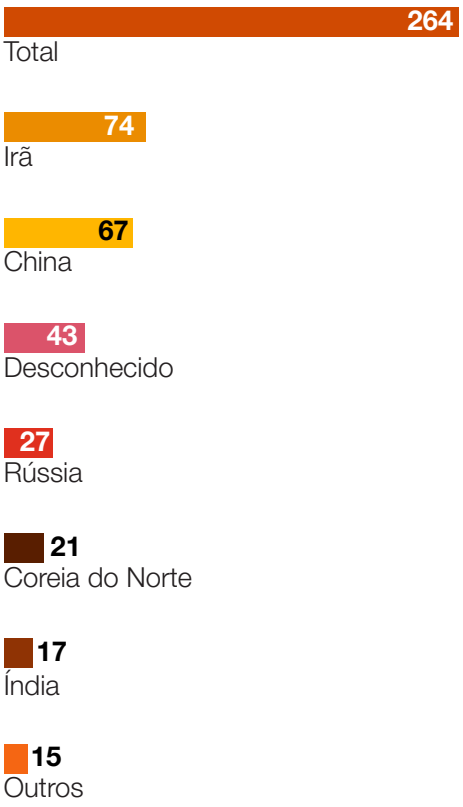
Figura 30: Incidentes por tipo, 2021



Fonte: PwC

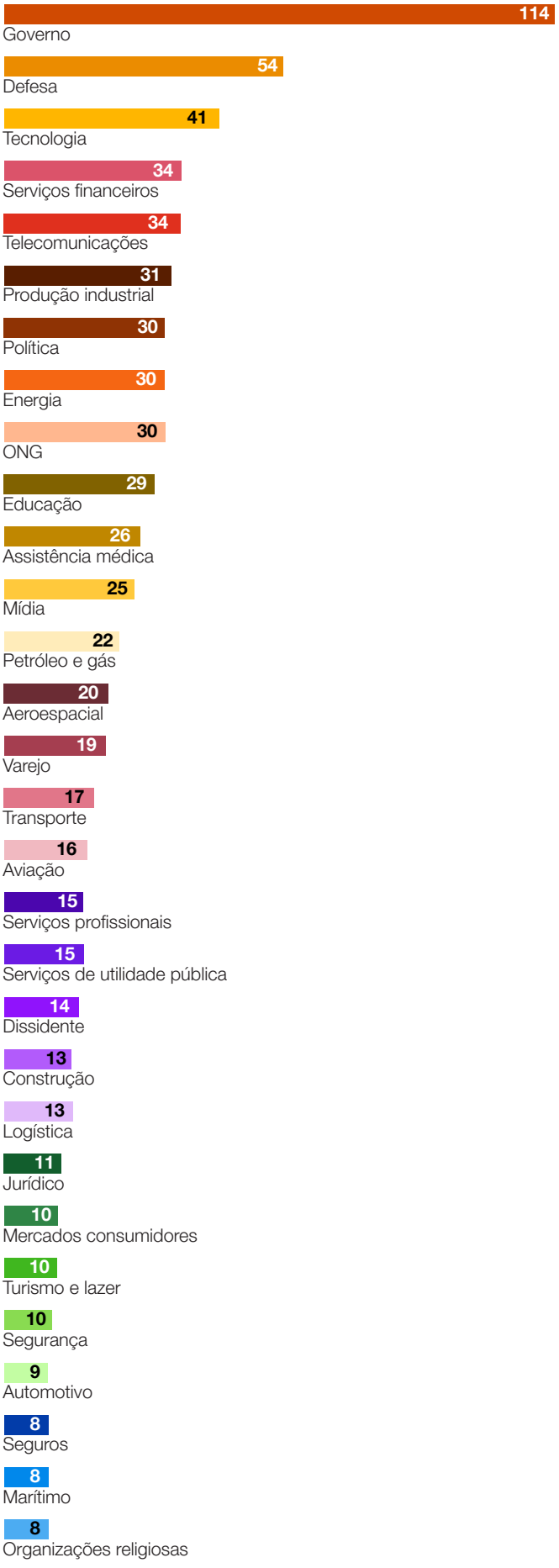
Estatísticas dos informes da PwC Threat Intelligence

Figura 31: Informes por local do agente de ameaças, 2021



Fonte: PwC

Figura 32: Informes por setor, 2021



Fonte: PwC

05 |

Segmentos em destaque

Nesta seção, destacamos as principais ameaças cibernéticas observadas em 2021 em vários setores.

Telecomunicações

2021 foi marcado pela continuação do interesse dos agentes de ameaças motivados por espionagem no setor de telecomunicações, provavelmente para fins de coleta de informações confidenciais, como observamos em anos anteriores.[238] Estimamos que mais de 80 empresas de telecomunicações foram comprometidas por agentes de ameaças localizados em dois países.

Conforme mencionado antes neste relatório, o Red Menshen (antigo Red Dev 18) implantou seu *malware* sob medida BPFDoor em várias organizações na região Ásia-Pacífico, inclusive em provedores de telecomunicações de vários países.[239]

A PwC observou outros agentes de ameaças da China visando o setor de telecomunicações, como o ataque do Red Kelpie (também conhecido como APT41) com seu loader *malware* Motnug a um provedor do Paquistão.[240] Essa mesma vítima também parece ter sido atacada pelo agente de ameaças iraniano Yellow Mora:[241] no início de 2021, a PwC analisou uma campanha do Yellow Mora (também conhecida como Greenbug) no setor de telecomunicações no sul da Ásia.[242] Nossa análise mostrou que o Yellow Mora provavelmente passou um longo período no ambiente da vítima, o que confirma relatos públicos de como esse agente opera.[243] Em uma atividade semelhante, o Yellow Nix (também chamado Static Kitten, MERCURY ou MuddyWater) teve como alvo um grande número de organizações de telecomunicações no Oriente Médio, Sul da Ásia, Sudeste da Ásia e Ásia Central, começando em janeiro e continuando ao longo do ano.[244] A PwC avalia que o objetivo desses ataques talvez seja, pelo menos em parte, vigiar e monitorar indivíduos, o que se alinha com o histórico de ataques a esse setor por grupos estreitamente associados como o Yellow Mimas.[245]

O setor também não escapou de operações de *ransomware*. O novo *ransomware* Macaw do Blue Lelantos, por exemplo, foi implantado em uma empresa de telecomunicações sediada nos EUA, enquanto o White Janus e o White Apep – dois dos operadores de *ransomware* mais ativos de 2021 – também atacaram várias organizações do setor com o *ransomware* Lockbit 2.0 e o Darkside/BlackMatter, respectivamente. Em geral, várias empresas estatais de telecomunicações, bem como provedores privados conhecidos de telecomunicações, foram vítimas de *ransomware* no ano passado, como a Corporación Nacional de Telecomunicaciones do Equador, a Schepisi Communications e a MasMovil, da Espanha.

238. "Cyber Threats 2020: A Year in Retrospect", PwC Threat Intelligence
239. "Compromising Eurasian Telecoms, justforfun", PwC Threat Intelligence, CTO-TIB-20210709-01A
240. "Learning to ChaCha with Red Kelpie", PwC Threat Intelligence, CTO-TIB-20210624-02A
241. "Yellow Mora is listening", PwC Threat Intelligence, CTO-TIB-20210426-01A
242. "Yellow Mora is listening", PwC Threat Intelligence, CTO-TIB-20210426-01A
243. "Sophisticated Espionage Group Turns Attention to Telecom Providers in South Asia", Symantec, https://symantec-enterprise-blogs.security.com/blogs/threatintelligence/greenbug-espionage-telco-south-asia (19/5/2020)
244. "Yellow Nix working overtime remotely", PwC Threat Intelligence, CTO-TIB-20210309-01A
245. "Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry", US Department of the Treasury, https://home.treasury.gov/news/press-releases/sm1127 (17/9/2020)

Tecnologia

Tecnologias inovadoras são valiosas para os que procuram replicar produtos e serviços, e os agentes de ameaças continuam interessados em propriedade intelectual. As próprias empresas de tecnologia podem ser alvo de ataques à cadeia de suprimentos e do tipo island hopping, principalmente quando fornecem serviços aos clientes (inclusive de TI e segurança cibernética). Em 2021, várias companhias aéreas (como as que participam da One Star Alliance e outras da Ásia-Pacífico) foram comprometidas por uma violação inicial de seus fornecedores compartilhados de tecnologia de comunicação: SITA.[246] A análise de código aberto[247] desse conjunto de invasões apontou para o Red Kelpie como o provável autor. Também observamos tentativas do Red Djinn com tipos semelhantes de intrusões, visando subsidiárias estrangeiras de empresas japonesas provavelmente para se mover lateralmente e entrar na rede principal do alvo.

Agentes de ameaças foram observados usando nomes de empresas de tecnologia em certificados SSL associados à sua infraestrutura maliciosa, como alguns localizados na China, onde a infraestrutura ShadowPad C2 foi identificada disfarçada de NVIDIA Corporation.[248] Também observamos amostras de *malware* HyperBro assinadas com um certificado pertencente a uma empresa de aplicativos móveis. Embora evidências sugiram que o *malware* HyperBro possa ser compartilhado entre vários agentes de ameaças localizados na China, seu usuário original é o Red Phoenix (também conhecido como APT27, Emissary Panda e Lucky Mouse). Observamos que o Red Phoenix continua atacando especificamente o setor de tecnologia e identificamos que ele comprometeu pelo menos uma empresa de tecnologia sediada nos EUA.

Ataques contra o setor de tecnologia também foram iniciados por criminosos cibernéticos. A Acer foi comprometida pelo *ransomware* REvil em duas ocasiões. Na segunda, a empresa recebeu um pedido de resgate de US$ 50 milhões, um dos mais altos conhecidos até o momento.[249]

Finalmente, empresas de tecnologia israelenses também foram alvo de atenção indesejada (supostamente uma campanha “hacktivista”) do White Dev 95, que avaliamos ser, muito provavelmente, um agente motivado por sabotagem por trás de uma operação de informações contra Israel. Em vez de buscar a extorsão, o agente da ameaça criptografa as redes de suas vítimas e imediatamente passa a vazar dados roubados – atividade que tem as características de operações de “bloqueio e vazamento”.

246. “Global Cyber Bulletin - June 2021”, PwC Threat Intelligence, CTO-GCB-20210706-01A
247. “Big airline heist: APT41 likely behind a third-party attack on Air India”, Group-IB: Nikita Rostovev, https://blog.group-ib.com/colunmtk_apt41 (10/6/2021)
248. “ShadowPad not a dead cert”, PwC Threat Intelligence, CTO-TIB-20211116-02A
249. “Acer confirms second cyber attack in 2021”, ZDNet: Jonathan Greig, https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/ (14/10/2021)

Serviços financeiros

As organizações do setor de serviços financeiros continuaram sendo alvos valiosos para os agentes de ameaças cibernéticas. Ao longo de mais de três meses de listagem nos mercados criminais RaidForums, XSS e Exploit, as instituições de serviços financeiros foram classificadas entre os três principais setores mais afetados. Elas registraram um preço mais alto em relação a outros setores impactados, sem dúvida devido ao fato de as listagens de serviços financeiros atraírem mais os compradores em termos de ganhos financeiros potenciais.

Grupos já estabelecidos de crime organizado podem visar especificamente instituições financeiras devido à expectativa de grandes pagamentos de resgate. Por exemplo, no início de 2021, a seguradora americana CNA foi comprometida quando os funcionários executaram uma atualização falsa do navegador. A instituição supostamente acabou pagando um resgate de US$ 40 milhões. Em maio de 2021, os operadores do *ransomware* Avaddon vazaram dados pertencentes a divisões do Grupo AXA com sede na Ásia (incluindo dados pessoais de clientes) contendo registros médicos confidenciais. Eles também ameaçaram os sites da AXA com um ataque de negação de serviço (DDoS, na sigla em inglês) se um resgate não fosse pago. Mais recentemente, no fim de novembro de 2021, observamos uma campanha de MirrorBlast provavelmente conduzida pelo White Austaras, envolvendo e-mails de spam que sugerem ataques a companhias de seguros no Canadá e na França, bem como várias empresas de gestão de ativos e patrimônio com sede nos EUA e em Hong Kong.[250]

Agentes situados na Coreia do Norte continuaram a representar uma ameaça grave para as instituições de serviços financeiros em geral, desde empresas de investimento e capital de risco até *exchanges* de criptomoedas (ou qualquer outra organização que lida com criptomoedas). Uma acusação do Departamento de Justiça dos EUA de fevereiro de 2021 contra cidadãos norte-coreanos (supostamente integrantes do Black Artemis) afirma que o agente de ameaças roubou US$ 11,8 milhões de uma instituição financeira de Nova York usando aplicativos trojanizados de negociação de criptomoeda.[251] O Black Alicanto e o Black Dev 2 têm atacado sistematicamente instituições financeiras, muitas vezes enviando e-mails de *spear phishing* para os alvos, bem como usando documentos de isca relacionados a criptomoedas ou que fingem ser propostas legítimas de *joint venture*.

250. "Well its been a MirrorBlast", PwC Threat Intelligence, CTO-TIB-20211025-01A
251. "Billion Dollar Baby", PwC Threat Intelligence, CTO-SIB-20210322-01A

Varejo

Em 2021, os operadores de *ransomware* continuaram a visar o setor de varejo, explorando a necessidade dos varejistas de manter o tempo de atividade operacional sem interrupções e, assim, pressionando suas vítimas a pagar o resgate rapidamente. Com a rápida digitização do setor, os agentes de *ransomware* conseguem paralisar sistemas de pagamento de pontos de extremidade, o que leva à perda de receitas e pressiona ainda mais a organização a atender ao pedido de resgate.

Das variantes de *ransomware* observadas atacando o setor de varejo, o Conti, operado pelo agente de ameaças White Onibi, foi a mais ativa. Esse *ransomware* foi usado com sucesso para atingir varejistas que vendem desde roupas a joias com pedidos de pagamento de resgates de alto valor ou o roubo de informações confidenciais e exclusivas,[252] [253] [254] que o White Onibi leiloou em 2021.[255]

Outros operadores de *ransomware* também visaram o setor de varejo. Como parte do ataque à cadeia de suprimentos contra o Kaseya, o *ransomware* Sodinokibi infectou a rede da Visma Esscom, fornecedora de TI. Como resultado da infecção da Visma Esscom, mais de 500 lojas da rede de supermercados Coop em toda a Suécia tiveram que fechar, pois seus sistemas de pagamento foram desconectados.[256] Em outro exemplo, em dezembro de 2021, um incidente de *ransomware* que afetou o varejista SPAR deixou 330 lojas do Reino Unido *off-line* por – em alguns casos – vários dias. Esses incidentes são apenas alguns dos inúmeros que afetaram o setor de varejo em 2021 e ameaçaram a operação normal dos negócios.[257] [258] [259] [260]

Nossa análise das listagens em mercados criminais mostrou que, embora a maioria das listagens de empresas de varejo contivesse dados de consumidores, várias (sobretudo no fórum Exploit) prometiam aos compradores a capacidade de redirecionar pagamentos com cartão em sites de comércio eletrônico. Para as marcas que operam no espaço de comércio eletrônico, também vale lembrar que estão em andamento operações de clonagem de cartão de crédito conhecidas como "Magecart".[261] O National Cyber Security Centre (NCSC) do Reino Unido notificou mais de 4 mil pequenos e médios varejistas antes da Black Friday que eles estavam usando portais de pagamento comprometidos em suas plataformas de comércio eletrônico Magento.

252. "Conti ransomware rakes in over $25 million in just four months", Acronis, https://www.acronis.com/en-us/cyber-protection-center/posts/conti-ransomware-rakes-inover-25-million-in-just-four-months/ (23/11/2021)
253. "Retailer Fat Face Pays $2 Million Ransom to Conti Gang", Bank Info Security, https://www.bankinfosecurity.com/retailer-fat-face-pays-2-million-ransom-to-contigang-a-16277 (26/3/2021)
254. "Graff multinational jeweller hit by Conti gang. Data of its rich clients are at risk, including Trump and Beckham", Security Affairs, https://securityaffairs.co/ wordpress/123980/cyber-crime/conti-ransomware-graff-jeweller.html (31/10/2021)
255. "Conti Ransom Gang Starts Selling Access to Victims", Krebs on Security, https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/ (25/10/2021)
256. "Coop supermarket closes 500 stores after Kaseya ransomware attack", Bleeping Computer, https://www.bleepingcomputer.com/news/security/coop-supermarketcloses-500-stores-after-kaseya-ransomware-attack/ (3/7/2021)
257. "Hundreds of SPAR stores forced to shut following a major cyber incident", Teiss, https://www.teiss.co.uk/spar-supermarket-cyber-incident/ (13/12/2021)
258. "NCSC statement on cyber incident affecting Spar stores", NCSC, https://www.ncsc.gov.uk/news/spar-stores-incident (10/12/2021)
259. "Canadian retailer Home Hardware hit by ransomware", ITWorld Canada, https://www.itworldcanada.com/article/canadian-retailer-home-hardware-hit-byransomware/445416 (2/4/2021)
260. "Office Depot parent expects over $20M loss due to malware attack", Retail Dive, https://www.retaildive.com/news/office-depot-parent-expects-over-20m-loss-dueto-malware-attack/597544/ (30/3/2021)
261. "The many tentacles of Magecart Group 8", Malwarebytes: Jérôme Segura, https://blog.malwarebytes.com/threat-intelligence/2021/09/the-many-tentacles-ofmagecart-group-8/ (13/9/2021)

Estudo de caso de resposta a incidentes:

DarkSide: do acesso inicial ao pedido de resgate em quatro horas

Em abril de 2021, as equipes de resposta a incidentes da PwC de vários países apoiaram um cliente de varejo global que foi vítima de um ataque de *ransomware* executado pelo DarkSide (monitorado pela PwC como White Apep).

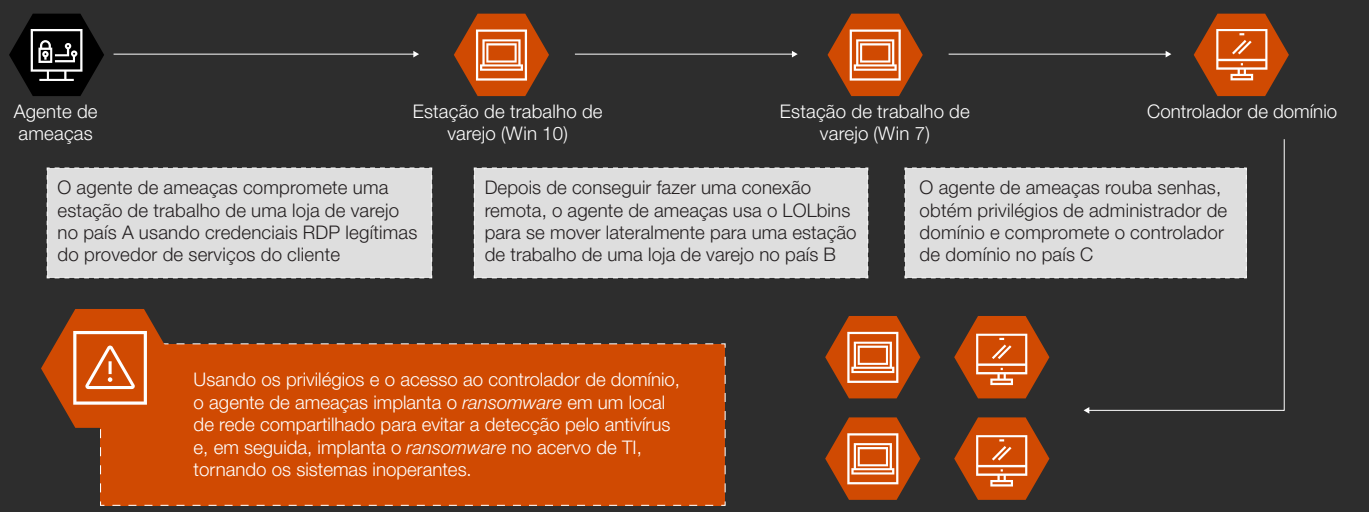
A análise do incidente permitiu identificar que o agente de ameaças usou uma ferramenta de acesso remoto conhecida como LogMeIn para ter acesso ao acervo de TI do cliente. Essa ferramenta foi usada com fins legítimos por um dos provedores de serviços de TI da organização para permitir o acesso remoto para manutenção de estações de trabalho de lojas de varejo e sistemas de suporte. Na invasão inicial, foi usada uma funcionalidade do *software* LogMeIn que permite a usuários com credenciais válidas acessar remotamente um sistema sem precisar interagir com nenhum empregado do cliente.

Depois de comprometer o cliente de lojas de varejo no país A, o agente de ameaças baixou as ferramentas de administração, usando-as para realizar reconhecimento interno na rede do cliente. Ao mesmo tempo, ele elevou seus privilégios para uma conta administrativa padrão usada em todo o domínio por meio do despejo de memória LSASS. Com os privilégios elevados, o agente de ameaças migrou para sistemas no país B que estavam no fim do ciclo de vida e sem receber atualizações.

O agente de ameaças então usou as credenciais coletadas desses sistemas para criar um usuário administrador de domínio, gerando e armazenando a senha da conta em uma conta do LastPass pertencente ao agente de ameaças.

Depois de comprometer o controlador de domínio, o agente de ameaças criou uma tarefa agendada e a implantou em todos os computadores na infraestrutura de TI do cliente, ordenando que eles baixassem e executassem o *ransomware*. O tempo desde o comprometimento inicial até a implantação do *ransomware* foi de aproximadamente quatro horas. Enquanto o operador de *ransomware* exigia um resgate de US$ 12 milhões, o cliente conseguiu estabelecer processos de negócios manuais para manter a organização operacional durante os esforços de resposta e recuperação de incidentes que duraram três semanas.

Figura 33: DarkSide – Do acesso inicial ao pedido de resgate em quatro horas



Estudo de caso de resposta a incidentes:

ShinyHunters: caça ao tesouro

Em dezembro de 2021, a PwC respondeu a um incidente em um cliente de varejo localizado na Índia que observou um aumento no uso de recursos de sistema em sua infraestrutura de nuvem e, em seguida, recebeu um e-mail com um pedido de resgate do agente de ameaças cibernéticas que monitoramos como White Dev 100 (também conhecido como ShinyHunters).

A análise revelou que o agente de ameaças teve acesso à rede usando uma chave comprometida de acesso à nuvem pertencente a um ex-integrante da diretoria executiva da organização. O agente de ameaças usou as credenciais comprometidas para ter acesso via console da Web à infraestrutura do cliente. Ele não conseguiu acessar nenhuma das instâncias e passou a executar comandos de reconhecimento para mapear a rede.

O agente de ameaças conseguiu criar instâncias e chaves SSH, acabando por injetá-las no armazenamento de chaves SSH autorizadas. Essas ações, combinadas com as modificações no grupo de segurança, permitiram que o agente da ameaça usasse SSH livremente no ambiente do cliente. Além disso, ele acessou vários diretórios .ssh e copiou chaves SSH privadas disponíveis para dar suporte à sua movimentação lateral. À medida que se movia pela rede, o agente de ameaças identificou sistemas de interesse, inclusive instâncias de teste e automação que ele explorou para expandir seu acesso. Durante esse período, o agente de ameaças manteve acesso a várias janelas de terminal no ambiente comprometido. A análise da atividade não permitiu identificar se havia vários operadores trabalhando ou um único indivíduo.

Produção industrial

Para organizações do setor de produção industrial, qualquer ataque que possa afetar a disponibilidade ou integridade de sistemas infectados representa um risco crítico. Esses ataques causam inatividade operacional, lentidão na produção e na distribuição, o que resulta em perda de receita e em altos custos de remediação que aumentam as dificuldades de retorno ao serviço. Há também problemas indiretos, como atrasos nos prazos de produção, violação de contratos com fornecedores e danos à reputação. O setor enfrenta cada vez mais ataques relevantes e direcionados, que vão desde a venda de dados confidenciais por empregados descontentes para concorrentes até ataques de *ransomware* conduzidos por grupos sofisticados do crime organizado.

Os operadores das campanhas do *ransomware* BlackMatter atacaram o setor de produção industrial mais do que qualquer outro entre janeiro e maio de 2021, em uma série de eventos sofisticados que renderam mais de 17,5 milhões de libras em pagamentos de bitcoin.[262] O Lockbit 2.0 também apresentou um foco no segmento de produção industrial: 21% dos dados de sites de vazamento entre janeiro e setembro de 2021 pertenciam a vítimas do setor.

Os ataques de comprometimento de e-mail corporativo (BEC, na sigla em inglês) continuam sendo uma ameaça substancial para todos os setores, incluindo o de produção industrial. Em 2021, a PwC observou uma campanha provavelmente associada ao Bronze Dev 2 (também conhecido como SilverTerrier), situado na Nigéria, com foco em organizações do setor. E-mails de *spear phishing* eram enviados com um anexo malicioso disfarçado de documento de orçamento urgente, que distribuía a ferramenta de acesso remoto (RAT, na sigla em inglês) AgentTesla.

A espionagem continua predominando no setor de produção industrial e atrai historicamente muito interesse de agentes de ameaças de coleta de inteligência devido a associação deles com clientes dos setores de defesa e espaço aéreo. De modo mais amplo, o investimento em tecnologia em todo o setor provavelmente aumentará esse interesse. Em abril de 2021, o Black Artemis distribuiu para empresas do setor documentos de isca convertidos em armas e disfarçados como candidaturas de emprego para implantar cargas maliciosas na rede da vítima.[263] O impacto de um ataque de espionagem bem-sucedido pode resultar na perda de competitividade em mercados internacionais já pressionados e em sanções regulatórias se os dados pessoais forem acessados em uma invasão.

262. "Nothing else BlackMatters", PwC Threat Intelligence, CTO-TIB-20211209-01A
263. "Your dream job awaits, just please enable editing", PwC Threat Intelligence, CTO-TIB-20210916-01A

Multinacional do setor de produção industrial enfrenta o LockBit

Em março de 2021, a PwC respondeu a um incidente de *ransomware* que afetou uma multinacional do setor de produção industrial. No caso, um operador do LockBit executou o *ransomware* em servidores e estações de trabalho em dez países.

A análise e investigação do incidente mostrou que o agente de ameaças começou a coletar informações sobre o cliente e preparar o ataque no quarto trimestre de 2020. Depois de conseguir acesso inicial, o agente usou o serviço de hospedagem de arquivos MEGA para baixar *malware* e realizou pesquisas na web para entender a localização e a natureza dos sistemas infectados. Em seguida, o agente baixou e executou ferramentas de varredura de rede (Softperfect Network Scanner) e se movimentou lateralmente usando contas comprometidas com o suporte de ferramentas populares (como o Mimikatz).

Ao longo dos meses seguintes, o agente de ameaças violou um controlador de domínio nos Estados Unidos, mudou-se para outro servidor nos EUA e, em março de 2021, usou um controlador de domínio no Japão para distribuir o *ransomware*.

Nos momentos finais do ataque, o agente de ameaças interagiu com a solução *antimalware* do cliente para garantir que o *ransomware* não fosse parado e, por fim, distribuiu e executou o *ransomware*. Embora o ataque tenha causado danos significativos à organização da vítima, não houve evidências claras de exfiltração de dados.

06 | Conclusão

Em 2021, o cenário de ameaças cibernéticas continuou a registrar um aumento no número de agentes de ameaças com todos os níveis de habilidade e motivações.

Nos últimos anos, o *ransomware* se mantém como a ameaça mais difundida e com impacto mais imediato para organizações de todos os portes e setores no mundo. Os desenvolvedores de *ransomware* continuam a expandir seus esquemas de afiliados em tamanho, receita e recursos. Os ataques à cadeia de suprimentos agora se tornaram parte do "novo normal" no cenário de ameaças cibernéticas, incorporados pelos agentes de ameaças cibernéticas em suas estratégias para alcançar o máximo impacto.

Ao mesmo tempo, ameaças diferentes em uma sociedade digital segura ganharam evidência com a importância e o impacto dos *quartermasters* digitais: as tradicionalmente vinculadas a operações patrocinadas por nações e as que envolvem negociadores comerciais do setor privado que fornecem a uma ampla gama de clientes ferramentas e recursos de ponta para a realização de ataques.

Todas essas ameaças culminaram na renovação do foco em vulnerabilidades de dia zero – com vários exemplos de operações direcionadas e ataques em grande escala, além de incentivos financeiros e estratégicos crescentes à atividade de pesquisa e desenvolvimento de *exploits*.

Avaliamos que, em 2022, continuaremos vendo os temas que surgiram ou se mantiveram em 2021, como *ransomware* e seu ecossistema criminoso, a importância dos negociadores de vulnerabilidades e ferramentas e as consequências das vulnerabilidades recém-descobertas que afetam vítimas despreparadas. Diante de vulnerabilidades e incidentes que ganham as manchetes dos jornais, a segurança cibernética se torna cada vez mais presente aos olhos do público. É mais importante do que nunca que os defensores continuem colaborando, compartilhando informações e apoiando as organizações e a sociedade. O foco deve ser em medidas de prevenção e detecção, além de planos de mitigação e resposta a incidentes eficazes em conter os agentes de ameaças.

PwC Cybersecurity

Para mais informações sobre as ameaças detalhadas neste relatório, entre em contato conosco pelo e-mail br_cyberintelligence@pwc.com.

A PwC é reconhecida mundialmente por analistas setoriais como líder em segurança cibernética, uma firma capaz de atuar globalmente e apresentar soluções para os desafios de segurança e risco que seus clientes enfrentam. Apoiamos nossos serviços de assessoria e estratégia em segurança no nível do conselho na experiência e no conhecimento adquiridos nas linhas de frente de nossos serviços especializados em defesa cibernética, como Defesa Cibernética Gerenciada, Red Teaming, resposta a incidentes e inteligência de ameaças.

Temos como diferencial nossa capacidade de combinar pensamento estratégico, fortes capacidades técnicas e realização de projetos complexos com excelência no atendimento ao cliente. Nossa expertise única em matéria de segurança e pesquisa, conhecimento técnico e compreensão dos riscos cibernéticos ajudam os clientes a obter a clareza necessária para se adaptar com confiança a um cenário de novos desafios e oportunidades.

Reunimos uma equipe de especialistas com experiência em gerenciamento de segurança, detecção e monitoramento de ameaças, inteligência de ameaças, consultoria e arquitetura de segurança, mudanças comportamentais e assessoria jurídica e regulatória em nossos esforços para ajudar nossos clientes a proteger o que é mais importante para eles.

Somos especializados em fornecer serviços que ajudam os clientes a resistir, detectar e responder a ataques cibernéticos avançados. Isso inclui eventos de crise, como violações de dados, ataques de *ransomware*, espionagem econômica e invasões direcionadas, incluindo aquelas comumente chamadas de ameaças persistentes avançadas (APTs).

Nossa pesquisa de inteligência de ameaças apoia todos os nossos serviços de segurança e é usada por organizações do setor público e privado em todo o mundo para proteger redes, conhecer o entorno de atuação e apoiar estratégias.

pwc

www.pwc.com.br

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil