Ameaças cibernéticas:
2023 em retrospectiva

pwc

Conteúdo

Sumário executivo

Em nossa 6ª retrospectiva anual, a equipe de inteligência de ameaças da PwC apresenta insights de pesquisas conduzidas ao longo de 2023, com base tanto na coleta direta quanto na parceria estreita com as equipes globais de resposta a incidentes e segurança da PwC.

O objetivo deste relatório é apresentar as ameaças cibernéticas, técnicas e possíveis alvos dos atacantes, a fim de capacitar organizações e indivíduos a se defenderem. Embora não abordemos diretamente o impacto dos ataques cibernéticos que pesquisamos, o ano de 2023 serviu para enfatizar o crescente custo humano resultante das atividades cibernéticas maliciosas. Seja direta ou indiretamente, ou como resultado de conflitos mais amplos que abrangem o domínio cibernético, o impacto de ataques cibernéticos sobre vidas, meios de subsistência e direitos humanos está aumentando. Essa realidade preocupante serve como motivação para todos os envolvidos na defesa cibernética e como um lembrete da importância do nosso trabalho.

2023 foi um ano de exploração de vulnerabilidades críticas, com uma grande variedade de agentes de ameaças persistentes avançadas (APT, na sigla em inglês) e criminosos cibernéticos se aproveitando delas para obter acesso inicial a sistemas ou redes.

Um destaque especial foi o ataque a aplicações de transferência de arquivos pelo grupo de *ransomware* CL0P, o que permitiu ao agente da ameaça acessar uma quantidade significativa de dados sensíveis. Esses dados foram usados para extorquir organizações, elevando expressivamente ao longo do ano o número de vítimas registradas nos sites de vazamento de *ransomware*, que superaram os observados nos anos anteriores por uma margem significativa.

Com a continuação dos conflitos globais e o início de outros, todos os setores e países envolvidos testemunharam atividades de agentes de ameaças relacionadas. Na guerra na Ucrânia, as campanhas cibernéticas passaram de ações focadas em sabotagem para esforços de espionagem mais convencionais.

No início do conflito entre Israel e Hamas, a atividade desses agentes resultou em frequentes ataques de sabotagem.[1] Em ambos os contextos, o hacktivismo foi evidente, resultando em ataques de negação de serviço e campanhas de vazamento de dados.

Violações na cadeia de suprimentos continuaram sendo uma ameaça importante para as organizações, com agentes de ameaças baseados na Coreia do Norte conduzindo vários ataques desse tipo ao longo de 2023. Embora esses incidentes não tenham tido tanto impacto quanto alguns realizados em anos anteriores, eles destacam o amplo acesso que os agentes de ameaças podem conseguir. Também servem como alerta sobre a capacidade de evolução desses agentes.

Apesar do uso de ferramentas, técnicas e procedimentos (TTPs, na sigla em inglês) conhecidos entre os principais agentes de APTs em países como China, Rússia, Irã e Coreia do Norte, muitos deles demonstraram uma sofisticação crescente em suas próprias áreas.

Cibercriminosos demonstraram que, mesmo com várias operações realizadas por forças de segurança e indústrias, o ecossistema de *ransomware* como serviço manteve sua eficiência, permitindo a realização de campanhas escaláveis contra organizações.

[1] PwC Threat Intelligence, CTO-QRT-20231205-01A - Yellow Dev 35 targets Unitronics PLCs in sabotage attacks against critical infrastructure.

Vários agentes de ameaças baseados na China se concentraram exclusivamente no uso de ferramentas nativas (*living off the land*), enquanto outros intensificaram a exploração de dispositivos periféricos. Agentes de ameaças baseados na Rússia refinaram vetores de infecção inicial e famílias de *malware*, aproveitando-se de vulnerabilidades críticas sempre que possível.

No Irã, eles utilizaram diversas identidades falsas para encobrir campanhas de sabotagem. Enquanto isso, na Coreia do Norte, em meio a violações variadas na cadeia de suprimentos, agentes de ameaças testaram novos vetores de infecção e ferramentas para atingir seus objetivos.

Cibercriminosos demonstraram que, mesmo com várias operações realizadas por forças de segurança e indústrias, o ecossistema de *ransomware* como serviço manteve sua eficiência, permitindo a realização de campanhas escaláveis contra organizações.

A vasta gama disponível de sistemas para distribuição de *malware* e ferramentas de roubo de credenciais permitiu que afiliados rapidamente desenvolvessem competências para comprometer sistemas, realizar movimentos laterais e criptografar/extrair dados para extorquir as vítimas. Em 2023, a ameaça do crime cibernético, abrangendo tanto as operações de *ransomware* quanto a violação de e-mail corporativo, continuou tendo o mesmo impacto de antes.

De modo geral, a retrospectiva de 2023 da PwC destaca a importância contínua de compreender o cenário de ameaças cibernéticas em constante evolução e os agentes de ameaças que nele operam.

Tendências

- Os dados de sites de vazamento de *ransomware* superaram muito os dos anos anteriores.
- A exploração de vulnerabilidades críticas em infraestruturas públicas aumentou, com um recorde de vulnerabilidades divulgadas este ano.[2]
- A exfiltração e extorsão de dados se tornaram mais focadas para os agentes de ameaças de *ransomware*, com alguns grupos optando por abandonar completamente a criptografia.
- O hacktivismo relacionado a conflitos geopolíticos continuou, indicando que essa prática pode estar se tornando usual.
- A inteligência artificial, apesar de algumas experimentações realizadas por agentes de ameaças, não apresentou impacto marcante.
- O *phishing* direcionado evoluiu significativamente, deixando de priorizar documentos com macros para buscar uma gama mais ampla de métodos de infecção.

[2] '2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is', Qualys, https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one (19/12/2023)

Quem somos

A PwC atende mais de 200 mil clientes em 152 países. Utilizamos nosso ponto de vista privilegiado como uma das maiores redes internacionais de serviços profissionais para prestar serviços de inteligência de ameaças globais, personalizados e fornecidos localmente aos nossos clientes.

Nossa pesquisa é a base de nossos serviços de segurança e é utilizada por organizações dos setores público e privado em todo o mundo para proteger redes, fornecer consciência situacional e apoiar a formulação de estratégias.

A área de inteligência de ameaças da PwC integra nossas capacidades de detecção com pesquisas especializadas em ameaças e esforços proativos para identificar problemas emergentes. Essa abordagem nos permite descobrir e eliminar lacunas em nossa detecção de atividades maliciosas, aprimorar nosso entendimento sobre as ameaças e incorporar inteligência prática em nossos relatórios.

Nossa equipe de inteligência de ameaças é composta por especialistas de diversos países, como Austrália, Alemanha, Estados Unidos, Itália, Noruega, Suécia, Reino Unido e República Tcheca.

Gostaríamos também de reconhecer as contribuições e insights das equipes de resposta a incidentes das firmas-membro da PwC, especialmente da Alemanha, Áustria, Brasil, Europa Central e Oriental, Hong Kong, Irlanda, Japão, Noruega e Reino Unido.

Vulnerabilidades em aplicações acessíveis ao público

Principal insight: em 2023, observou-se um aumento significativo na exploração de vulnerabilidades em aplicações acessíveis ao público, realizada tanto por grupos de ameaças persistentes avançadas (APTs, na sigla em inglês) quanto por organizações cibercriminosas. Embora muitas dessas vulnerabilidades sejam usadas principalmente para acesso inicial, notou-se uma tendência crescente de ataques direcionados a aplicações de transferência de arquivos para roubar os dados armazenados.

A descoberta de vulnerabilidades em aplicações e sistemas operacionais cada vez mais complexos continua crescendo: houve um número recorde de vulnerabilidades identificadas em 2023.[3] Os agentes de ameaças continuam a investir tempo e dinheiro na pesquisa e compra de *exploits* (tanto para descoberta quanto para aproveitamento de *exploits* conhecidos, mesmo quando existem correções disponíveis).

[3] '2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is', Qualys, https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one (19/12/2023)

Esses esforços visam alcançar diversos objetivos contra alvos específicos, especialmente para obter acesso inicial a redes. Em 2023, várias ondas globais de incidentes foram desencadeadas pela exploração de vulnerabilidades críticas em uma série de aplicações voltadas ao público, como:

- VMWare ESXi;[4] [5]
- Fortra GoAnywhere;[6]
- Progress MOVEit;[7] [8]
- Citrix NetScaler;[9]
- Microsoft Outlook;[10] [11]
- Cisco ASA SSL VPN;[12]
- Cisco IOS XE;[13]
- Progress WS_FTP;[14]
- Atlassian Confluence;[15] [16]
- SysAid;[17] e
- Barracuda Email Security Gateway Appliance.[18]

[4] PwC Threat Intelligence, CTO-QRT-20230204-01A - Widespread ESXi Exploitation

[5] PwC Threat Intelligence, CTO-TIB-20230217-01A - ESXiArgs Followup

[6] PwC Threat Intelligence, CTO-TIB-20230216-01A - Exploitation of GoAnywhere Vulnerability

[7] PwC Threat Intelligence, CTO-QRT-20230601-01A - MOVEit Critical Vulnerability

[8] PwC Threat Intelligence, CTO-QRT-20230607-02A - White Austaras puts MOVEit breach victims on notice

[9] PwC Threat Intelligence, CTO-VRB-20231114-01A - October Vulnerability Research Bulletin

[10] PwC Threat Intelligence, CTO-QRT-20230316-01A - CVE-2023-23397

[11] PwC Threat Intelligence, CTO-TIB-20230921-03A - Ongoing exploitation of CVE-2023-23397

[12] PwC Threat Intelligence, CTO-QRT-20230911-01A - CVE-2023-20269 ongoing exploitation

[13] PwC Threat Intelligence, CTO-QRT-20231017-01A - Active exploitation of Cisco IOS XE

[14] PwC Threat Intelligence, CTO-QRT-20231004-01A - Active exploitation of WS_FTP

[15] PwC Threat Intelligence, CTO-QRT-20231005-01A - Active exploitation of Confluence vulnerability

[16] PwC Threat Intelligence, CTO-QRT-20231108-01A - Cerber *ransomware* leverages CVE-2023-22518

[17] PwC Threat Intelligence, CTO-QRT-20231109-01A - CL0P *exploits* CVE-2023-47246

[18] PwC Threat Intelligence, CTO-VRB-20230612-01A - May Vulnerability Research Bulletin

A exploração dessas vulnerabilidades permitiu que agentes de ameaças motivados por espionagem e cibercrime tivessem acesso inicial a uma variedade de dispositivos e comprometessem uma quantidade significativa de organizações em todo o mundo. Em alguns casos, isso permite que o agente da ameaça tome medidas imediatas em relação aos seus objetivos, como o roubo de dados associados ao próprio aplicativo.

Em outros, a exploração é apenas a primeira etapa de uma intrusão, dando ao agente da ameaça acesso para avançar ainda mais na rede e estabelecer uma base de operações na periferia, a partir da qual ele pode resistir a atividades tradicionais de contenção ou erradicação.

Independentemente da motivação do agente da ameaça, a exploração dessas vulnerabilidades, especialmente se feita como um *zero-day*, pode levar a campanhas generalizadas e difíceis de detectar, que muitas vezes exigem das equipes de segurança a identificação de novas fontes de *logs* para uma rápida análise histórica.

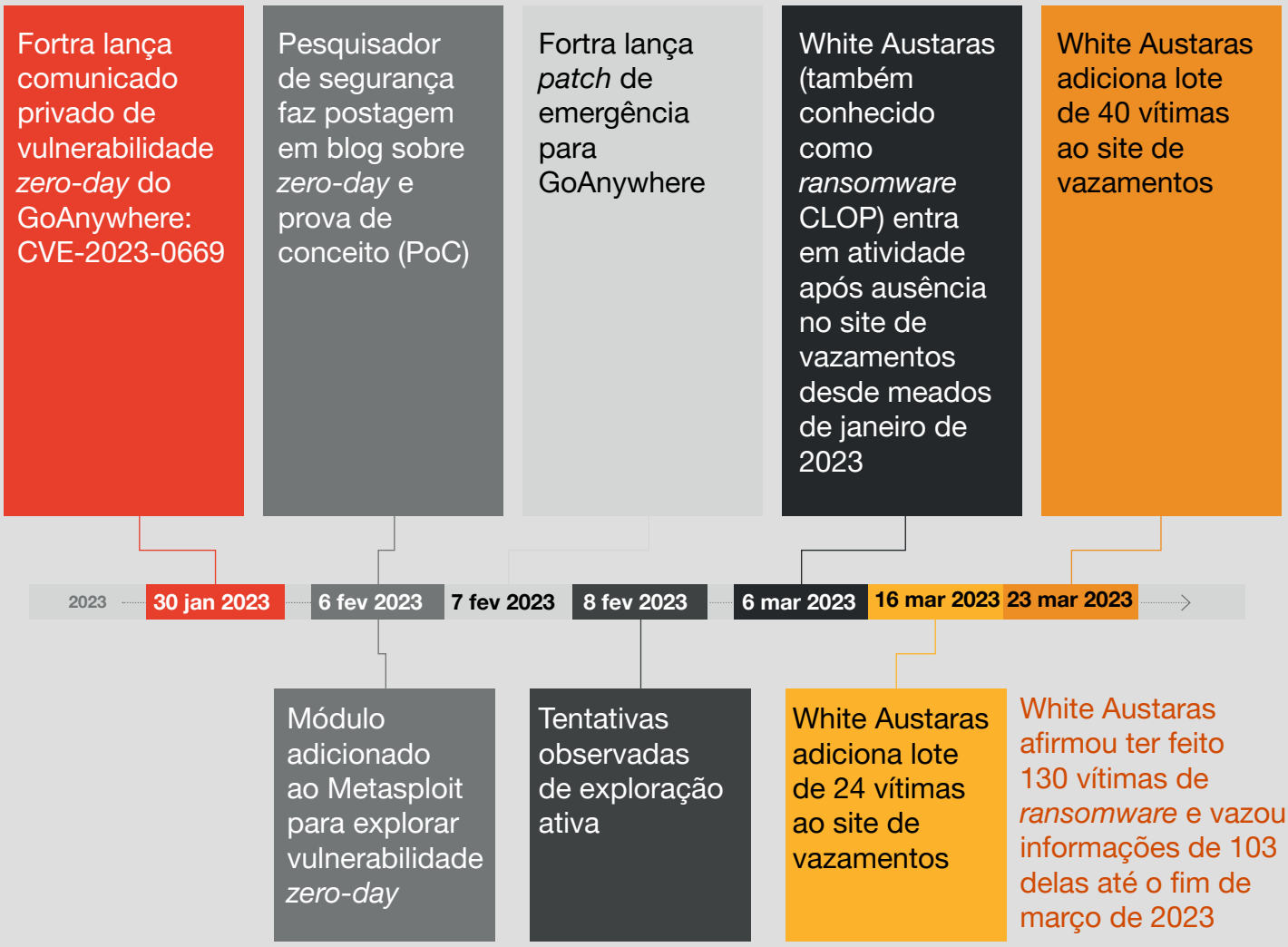
Os agentes de ameaça continuam a explorar vulnerabilidades em categorias de aplicativos como clientes de e-mail ou VPN. Destacamos alguns exemplos específicos e tendências nas próximas seções.

Independentemente da motivação do agente da ameaça, a exploração dessas vulnerabilidades, especialmente se feita como um *zero-day,* pode levar a campanhas generalizadas e difíceis de detectar, que muitas vezes exigem das equipes de segurança a identificação de novas fontes de *logs* para uma rápida análise histórica.

Vulnerabilidades em soluções de transferência de arquivos

A atividade do White Austaras (também conhecido como CL0P, Lace Tempest, TA505 e FIN11) foi destaque entre os eventos cibernéticos críticos de 2023. Conhecido por campanhas de *ransomware* mais tradicionais, o agente de ameaças adotou uma abordagem diferente ao longo do ano, optando por atacar soluções de transferência de arquivos voltadas ao público nas organizações.

Isso incluiu o ataque a servidores Fortra GoAnywhere para explorar a CVE-2023-0669 e implantar seu *backdoor* chamado Truebot,[19] ou explorar a CVE-2023-47246 em SysAid para instalar o GraceWire (também conhecido como FlawedGrace e BARBWIRE).[20] Em ambos os cenários, o acesso obtido permitiria a exfiltração de dados, que poderiam ser usados depois para exigir pagamentos em troca da não divulgação das informações.



[19] PwC Threat Intelligence, CTO-TIB-20230216-01A - Exploitation of GoAnywhere Vulnerability

[20] PwC Threat Intelligence, CTO-QRT-20231109-01A - CL0P *exploits* CVE-2023-47246

A exploração ativa da CVE-2023-34362, uma vulnerabilidade crítica na solução de transferência de arquivos MOVEit da Progress, foi especialmente relevante nas operações do White Austaras.[21] O impacto geral desse incidente foi sem precedentes, com mais de 250 organizações listadas em sites de vazamento de *ransomware* e sugestões de que o número total de entidades afetadas estava na casa dos milhares.[22]

Em comparação com os incidentes envolvendo GoAnywhere e SysAid, o White Austaras demonstrou planejamento nas campanhas com o MOVEit. Em vez de implantar *malware*s personalizados como Truebot ou GraceWire, o agente de ameaças introduziu uma *webshell* personalizada para interagir com o servidor comprometido.[23] Essa *webshell* tinha capacidade para listar arquivos no servidor e exfiltrá-los, permitindo uma exfiltração de dados eficiente e em massa pelos servidores MOVEit.

Essas três campanhas revelam uma mudança no ritmo das operações de alguns grupos de *ransomware*. Em cada uma delas, o agente de ameaças não foi observado implantando *ransomware*: ele se concentrou exclusivamente na exfiltração de dados. Talvez, com mais tempo, o agente de ameaças poderia ter tentado criptografar arquivos além de roubá-los.

No entanto, há uma probabilidade realista de que o White Austaras perceba que se concentrar na extorsão de dados, em vez de interromper as atividades comerciais com *ransomware*, pode ser igualmente eficaz. Além disso, criptografar soluções de transferência de arquivos pode não ser tão efetivo quanto realizar um ataque de *ransomware* em toda a organização, o que provavelmente contribuiu para a decisão do agente de ameaças de não seguir esse caminho.

Previsão: em 2024, esperamos que mais agentes de ameaças de crimes cibernéticos deixem de lado a utilização tradicional de *ransomware* e se concentrem na extorsão de dados.

[21] 'MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)', Progress, https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 (31/05/2023)

[22] KonBriefing, 'MOVEit hack victim list', https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html

[23] PwC Threat Intelligence, CTO-QRT-20230601-01A - MOVEit Critical Vulnerability

Cisco IOS XE

Uma das vulnerabilidades críticas mais exploradas em 2023 foi a CVE-2023-20198 em dispositivos Cisco IOS XE.[24] [25] Nos incidentes, um agente de ameaças não identificado (que monitoramos como White Dev 163) explorou várias vulnerabilidades para criar contas válidas e implantar *backdoors* para acesso persistente.

Nossa pesquisa indicou níveis de infecção similares aos detalhados pela Shadowserver,[26] ou seja, entre 40 mil e 50 mil dispositivos foram infectados em outubro de 2023, de um total de cerca de 72 mil instâncias vulneráveis.

Essa exploração generalizada levou o mesmo agente de ameaças a introduzir uma nova versão do *backdoor*, provavelmente em resposta à intensa vigilância e ampla divulgação sobre a implantação inicial.[27]

Em geral, houve pouca atividade subsequente relatada usando esses *backdoors*. Várias hipóteses foram propostas, como a exploração em massa para mascarar o comprometimento direcionado de um grupo menor de vítimas, ou uma tentativa de cooptar dispositivos para se tornarem parte de um *botnet* futuro.

Esse incidente, contudo, ressaltou a capacidade de resposta rápida de um agente de ameaças diante de uma divulgação, desde a exploração massiva inicial até a reinstalação dos *backdoors*. Portanto, as organizações precisam agir rapidamente para instalar correções, mitigar problemas e corrigir os softwares vulneráveis, além de mobilizar equipes de resposta a incidentes quando necessário.

Quanto maior o número de dispositivos expostos à internet mantidos por uma organização, maior a probabilidade de enfrentarem eventos cibernéticos críticos, especialmente com o aumento do interesse dos agentes de ameaças nesses sistemas.

---

[25] PwC Threat Intelligence, CTO-QRT-20231017-01A - Active exploitation of Cisco IOS XE

[26] Shadowserver, 'General statistics', https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=other&d1=2023-10-15&d2=2023-10-23&source=compromised_website&source=compromised_website6&tag=device-implant%2B&style=stacked

[27] '*Backdoor* Implanted on Hacked Cisco Devices Modified to Evade Detection', The Hacker News, https://thehackernews.com/2023/10/*backdoor*-implant-on-hacked-cisco.html (24/10/2024)

Tecnologia operacional

Muitas organizações que se enquadram no âmbito da infraestrutura nacional crítica (INC) têm grandes instalações de tecnologia operacional (TO) devido à natureza de seus negócios. Embora não seja algo exclusivo para INC, existem vários agentes de ameaças com um interesse permanente em atacar entidades relacionadas, seja para reconhecimento, coleta de inteligência, atividades disruptivas ou destrutivas.

Esses ataques muitas vezes se alinham com os interesses de algumas nações e com a dinâmica geopolítica. Isso faz com que, na parte mais extrema da escala, as capacidades cibernéticas ofensivas sejam usadas como um vetor alternativo à guerra tradicional, provavelmente numa tentativa de degradar ou destruir serviços críticos.[28]

Entre

40 a 50 mil

dispositivos foram infectados ao longo de outubro de 2023 em aproximadamente 72 mil instâncias vulneráveis.

Em 2023, foi divulgado um conjunto de vulnerabilidades de execução remota de código em TO na SDK CODESYS V3, utilizada por muitas organizações para desenvolver controladores lógicos programáveis (PLCs, na sigla em inglês),[29] [30] e nos módulos de comunicação da Rockwell Automation.[31] [32]

---

[28] PwC Threat Intelligence, CTO-SIB-20230105-01A - The OT threat landscape

[29] PwC Threat Intelligence, CTO-QRT-20230811-01A - Disclosed CODESYS Vulnerabilities

[30] 'Multiple high severity vulnerabilities in CODESYS V3 SDK could lead to RCE or DoS ', Microsoft, https://www.microsoft.com/en-us/security/blog/2023/08/10/multiple-high-severity-vulnerabilities-in-codesys-v3-sdk-could-leadto-rce-or-dos/ (10/8/2023)

[31] PwC Threat Intelligence, CTO-TIB-20230717-01A - OT - Rockwell Automation Vulnerabilities

[32] 'Rockwell Automation Select Communication Modules', CISA, https://www.cisa.gov/news-events/ics-advisories/icsa-23-193-01 (12/7/2023)

No último caso, a empresa fornecedora de soluções de segurança ICS/OT, Dragos, mencionou que uma “APT não identificada” tinha capacidade de explorar essas vulnerabilidades da Rockwell Automation, mas que não houve nenhuma exploração ativa conhecida antes da divulgação.[33]

Na época em que essas vulnerabilidades foram divulgadas, observamos muitas instâncias dessas tecnologias expostas na internet. Embora não tenha ocorrido exploração conhecida em nenhum desses casos, isso representa uma ampla superfície de ataque para agentes de ameaças motivados a comprometer e/ou interromper dispositivos de TO.

33 ‘Dragos Enabled Defense Against APT *Exploits* for Rockwell Automation ControlLogix’, Dragos, https://www.dragos.com/blog/mitigating-cves-impacting-rockwell-automation-controllogix-firmware/ (12/7/2023)

Atividade cibernética em torno de conflitos

Principal insight: com a continuação de guerras e o surgimento de outros conflitos, os agentes de ameaças mudaram o ritmo de suas operações relacionadas a eles. Esses agentes deixaram de usar *wipers* para adotar técnicas mais convencionais de espionagem. O hacktivismo permaneceu constante ao longo do ano, com campanhas de sabotagem registradas no último trimestre de 2023.

Em 2023, observamos a continuação de conflitos existentes e a rápida escalada de novos. Em grandes conflitos, atividades cibernéticas relacionadas são quase inevitáveis. Elas envolvem tanto os países participantes quanto organizações com qualquer nível de envolvimento.

Além das atividades de espionagem, existe também a possibilidade de ações cibernéticas, como operações de *hack-and-leak* e campanhas de desinformação, que se manterão relevantes ao longo de 2024, graças à realização de pelo menos 64 eleições nacionais importantes, abrangendo quase metade da população mundial.

A tecnologia continua a desempenhar um papel de destaque na guerra,[34] tanto por meio de soluções emergentes, como drones, quanto pelo emprego de tecnologias de uso duplo como GPS, satélites e smartphones. Os smartphones especialmente, por proporcionarem às tropas acesso a uma quantidade maior de dados e aplicações diretamente nas linhas de frente, também têm sido objeto de rastreamento por geolocalização, o que possibilita o direcionamento cinético das tropas.[35] [36]

[34] PwC Threat Intelligence, CTO-SIB-20231121-01A - The evolving nature of technology in warfare

[35] 'Ukraine war: Mobile networks being weaponised to target troops on both sides of conflict', Sky News, https://news.sky.com/story/ukrainewar-mobile-networks-beingweaponised-to-target-troops-on-both-sides-of-conflict-12577595 (4/1/2023)

[36] 'Russian blame game breaks out after Moscow says its own troops' cell phone use caused Makiivka strike', CNN, https://edition.cnn.com/2023/01/04/europe/makiivka-strike-russia-cell-phone-reaction-intl/index.html (5/1/2023)

A guerra na Ucrânia

O impacto da invasão russa da Ucrânia continuou sendo sentido ao longo de 2023, tanto no cenário físico e militar quanto do ponto de vista cibernético.

No início do ano, apresentamos um panorama retrospectivo dos ataques cibernéticos associados à invasão e ao conflito durante seu primeiro ano,[37] ressaltando o uso de vulnerabilidades *zero-day* e programas *wipers* por agentes de ameaças russos, assim como uma visão geral sobre campanhas de hacktivismo.

Contudo, ao longo de 2023, os agentes de ameaças cibernéticas baseados na Rússia focaram menos em ataques de sabotagem com *wipers* e mais em operações convencionais de espionagem contra organizações. Um exemplo foram as campanhas conduzidas pelo agente de ameaças baseado na Rússia, Blue Dev 8, provavelmente motivado por espionagem, utilizando temas como o UKR net, um portal de internet popular na Ucrânia.[38]

[37] PwC Threat Intelligence, CTO-TIB-20230428-01A - Ukraine One Year On

[38] PwC Threat Intelligence, CTO-TIB-20230214-01A - Blue Dev 8s interest in Ukrainian regions

A opção estratégica por organizações ucranianas como alvos continuou sendo uma prioridade para diversos agentes de ameaças. No primeiro semestre de 2023, além do foco geral em empresas ucranianas,[39] detectamos que o agente de ameaças White Dev 140 estava mirando especificamente um fabricante envolvido no mercado interno de negociação de grãos da Ucrânia.[40]

A exportação de grãos da Ucrânia se tornou altamente contenciosa desde o início da invasão, considerando o papel do país como um dos principais produtores de grãos do mundo e após a Rússia impor um bloqueio às exportações marítimas ucranianas.

No primeiro semestre de 2023, além do foco em empresas ucranianas de modo geral, detectamos que o agente de ameaças White Dev 140 estava mirando especificamente um fabricante envolvido no mercado interno de negociação de grãos da Ucrânia.

Avaliamos como quase certo que a coleta tradicional de inteligência persistirá durante o conflito, e é improvável que ocorra uma retomada generalizada do uso de *wipers* (ainda que não possamos excluir totalmente sua aplicação quando puderem servir a objetivos militares).

[39] PwC Threat Intelligence, CTO-TIB-20230302-01A - White Dev 140 the persistent presence targeting Ukraine

[40] PwC Threat Intelligence, CTO-SRT-20230530-01A - Engrained targeting in Ukraine

O conflito Israel/Hamas

Os ataques terroristas do Hamas contra Israel, em 7 de outubro de 2023, deram início a mais um capítulo desse conflito, intensificando as tensões geopolíticas e a atividade de ameaças cibernéticas, provocando sofrimento humano devastador e aumentando os desafios de segurança para quem vive na região.

Essa guerra, assim como a invasão da Ucrânia e outros conflitos ao redor do mundo, tem sido acompanhada por uma intensa atividade cibernética. Alguns agentes de ameaças têm explorado guerras, catástrofes, crises humanitárias e outros desafios para alcançar seus objetivos.

Para alguns, sua missão está entrelaçada com atividades no domínio físico. Outros buscam simplesmente tirar proveito das manchetes. A exploração é variada, incluindo agentes de ameaças que criam temas como parte de campanhas de *phishing* contra grupos específicos, aproveitando-se de que esses alvos estariam mais propensos a cair nas armadilhas dos agentes de ameaças porque estão emocionalmente envolvidos ou são diretamente afetados pelo problema em questão.

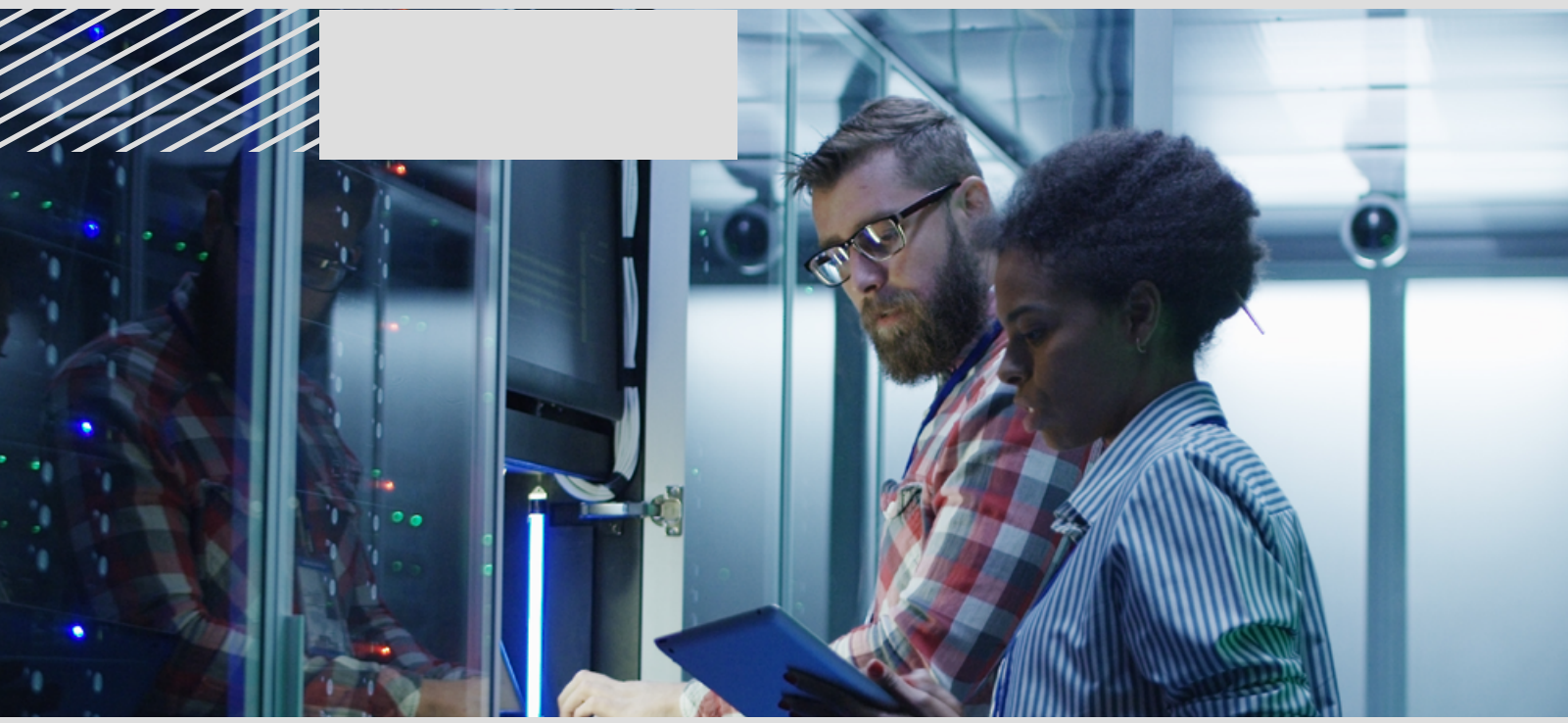
Consideramos esses e outros fatores ao realizar nossas análises e ao contextualizar a atividade de ameaça, a vitimologia observada e o impacto dessa atividade em uma escala mais ampla.

Essa guerra, assim como a invasão da Ucrânia e outros conflitos ao redor do mundo, tem sido acompanhada por uma intensa atividade cibernética. Alguns agentes de ameaças têm explorado guerras, catástrofes, crises humanitárias e outros desafios para alcançar seus objetivos.

Após os ataques de outubro de 2023 contra Israel, e a subsequente invasão israelense de Gaza, a atividade cibernética relacionada ao conflito se intensificou imediatamente.[41] No início, vários grupos hacktivistas demonstraram a intenção de se envolver – por exemplo, o Anonymous Sudan e o Killnet reivindicaram responsabilidade por ataques de negação de serviço contra organizações em Israel.

Um grupo conhecido como Threatsec disse ter visado e derrubado o maior provedor de serviço de internet em Gaza, o Alfanet. Em alguns casos, as alegações de invasões por hacktivistas incluíram vítimas de ataques anteriores. Isso sugere que algumas das "vitórias" anunciadas no contexto do conflito são, na verdade, violações antigas que foram recicladas.

No início do conflito, a partir de 7 de outubro de 2023, não registramos um aumento imediato nas ações de agentes de ameaças baseados no Irã contra Israel. De acordo com nossas observações, demorou cerca de uma a duas semanas para que qualquer atividade relacionada fosse detectável.



Por exemplo, uma versão para Windows da ferramenta de limpeza de disco BiBi Wiper, utilizada pelo Yellow Dev 31 (também conhecido como DEV-0842) contra organizações israelenses, tinha um carimbo de compilação de 21 de outubro de 2023.[42]

[42] 'BiBi Wiper Used in the Israel-Hamas War Now Runs on Windows', Blackberry, https://blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows (10/11/2023)

Observamos ainda que o Yellow Dev 19 (também conhecido como Vice Leaker, Cotton Sandstorm e Emennet Pasargad) começou a varrer câmeras de segurança, sistemas CCTV e servidores do Protocolo de Streaming em Tempo Real (RTSP, na sigla em inglês) em Israel na segunda metade de outubro de 2023.[43]

Foi publicamente atribuída ao Yellow Nix (também conhecido como MuddyWater e Mango Sandstorm) a criação de um aplicativo falso RedAlert em 12 de outubro de 2023, imitando um aplicativo israelense usado para alertar sobre ataques de foguetes.[44] [45] Esse atraso nas atividades maliciosas indica que os agentes de ameaças baseados no Irã agiram de forma reativa, e não proativa, ao conflito.

Esperamos que a atividade cibernética continue durante o conflito, especialmente por parte de grupos baseados nos territórios palestinos, como o Grey Karkadann (também conhecido como AridViper, APT-C-23, Desert Falcon),[46] Grey Hades (também conhecido como Gaza Hacking Team, Molerats e Gaza Cybergang)[47] e Beige Rukh (também conhecido como SysJoker e Storm-1133).[48]

---

[43] PwC Threat Intelligence, CTO-TIB-20231207-01A - The IRGC and its alter egos in 2023

[44] 'Malicious "RedAlert - Rocket Alerts" application targets Israeli phone calls, SMS, and user information', Cloudflare, https://blog.cloudflare.com/malicious-redalert-rocket-alerts-application-targets-israeli-phone-calls-sms-and-userinformation/ (14/10/2023)

[45] @likethecoins, X, https://x.com/likethecoins/status/1722654860586156423 (9/11/2023)

[46] 'Arid Viper | APT's Nest of SpyC23 *Malware* Continues to Target Android Devices', SentinelOne, https://www.sentinelone.com/labs/arid-viper-apts-nest-of-spyc23-*malware*-continues-to-target-android-devices/ (6/11/2023)

[47] 'Pro-Palestinian hacking group evolves tactics amid war', CyberScoop, https://cyberscoop.com/gaza-hamas-israelcyber-hacking-espionage/ (14/11/2023)

[48] 'Israel-Hamas War Spotlight: Shaking the Rust Off SysJoker', Check Point, https://research.checkpoint.com/2023/israel-hamas-war-spotlight-shaking-the-rust-off-sysjoker/ (23/11/2023)

Estudo de caso

Hacktivismo

Durante o ano de 2023, observamos agentes hacktivistas direcionando ataques a organizações envolvidas de alguma forma nos conflitos em curso. Sejam governos que ofereciam suporte a determinados países ou empresas do setor privado, fornecendo recursos para um dos lados do conflito, os hacktivistas empregaram ataques de negação de serviço para interromper temporária e publicamente o funcionamento das infraestruturas utilizadas por esses alvos.

Ao longo do ano, monitoramos a atividade de DDoS do grupo hacktivista NoName057(16) (que identificamos como White Dev 149).[49] Com sua ferramenta chamada DDosia, o grupo distribui aplicativos de DDoS que podem ser executados por voluntários. Esses aplicativos coletam listas de alvos definidas pelo NoName057(16) e, em seguida, realizam ataques de negação de serviço contra esses alvos.

O agente de ameaças visou principalmente organizações na Europa, mas também observamos alvos na América do Norte, no Japão e na Austrália. As campanhas do NoName057(16) coincidiram, em alguns casos, com eventos e mudanças geopolíticas importantes, como as visitas do presidente ucraniano Volodymyr Zelenskyy a outros países, atividades náuticas na Europa e as eleições parlamentares na Polônia.[50]

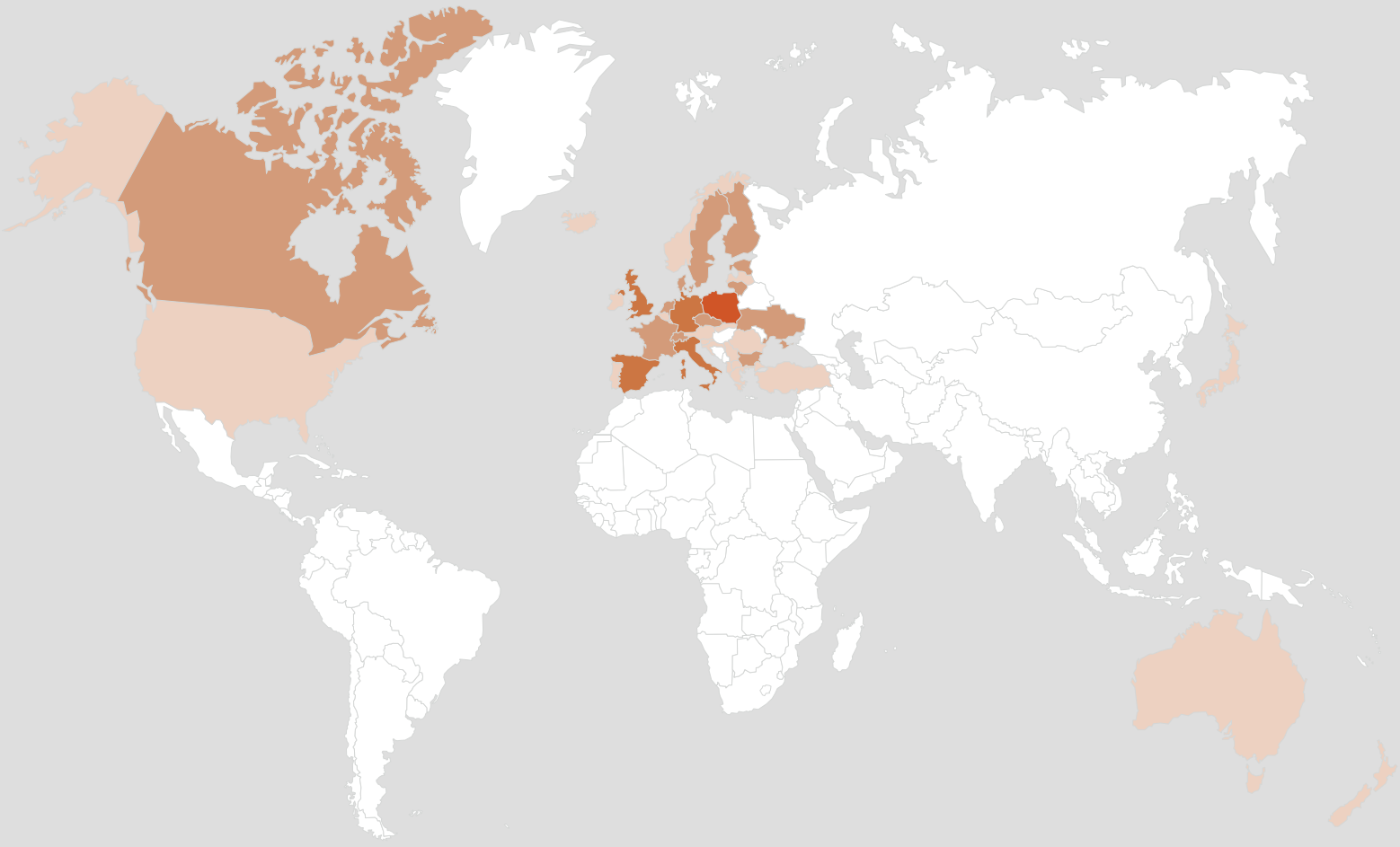
[49] PwC Threat Intelligence, CTO-TIB-20231124-01A - I have NoName, and I must scream

[50] PwC Threat Intelligence, CTO-SIB-20240104-01A - NoName is taking names

Compreender eventos geopolíticos pode, entre outros fatores, ajudar a contextualizar a análise de inteligência de ameaças segundo a perspectiva de uma organização específica. Publicamos um artigo sobre a importância da inteligência estratégica de ameaças.

0 148

Número de organizações que foram alvo do White Dev 149 em 2023



Violações na cadeia de suprimentos

Principal insight: em 2023, ocorreram diversas violações de alto impacto na cadeia de suprimentos, sendo que várias das mais importantes foram realizadas por agentes de ameaças baseados na Coreia do Norte. As organizações precisam responder rapidamente a esses incidentes para impedir ações subsequentes de agentes mal-intencionados.

Embora esses tipos de ataques não sejam novidade, muitas outras violações[51] ocorreram desde a campanha mais proeminente e sofisticada dos últimos tempos: a que atingiu a cadeia de suprimentos da SolarWinds em 2021.[52] Violações em cadeia de suprimentos podem ocorrer de várias maneiras, conforme mostra a figura a seguir.

Elas podem incluir desde a violação de software utilizado pelas organizações até o comprometimento de um terceiro confiável, que usa ferramentas para conduzir atividades maliciosas diretamente, como foi o caso da violação na cadeia de suprimentos da Kaseya, em meados de 2021. O ataque resultou na implantação do *ransomware* Sodinokibi/REvil em organizações que utilizavam o software da Kaseya.[53]

Formas de ataques à cadeia de suprimentos

[51] PwC Threat Intelligence, CTO-SIB-20230419-01A - One breach to rule them all

[52] 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST *Backdoor*', Mandiant, https://www.mandiant.com/resources/blog/evasive-attacker-leveragessolarwinds-supply-chain-compromises-with-sunburst-*backdoor* (13/12/2023)

[53] PwC Threat Intelligence, CTO-QRT-20210703-01A - Kaseya supply chain compromise

Cadeias de desenvolvimento de software e plataformas de implantação também se tornaram alvos recentes de violações na cadeia de suprimentos. Em janeiro de 2023, a plataforma de integração e distribuição de software CircleCI divulgou detalhes de um incidente que havia começado no fim de dezembro de 2022.[54]

Um agente de ameaças não identificado inicialmente violou a máquina de um engenheiro da CircleCI e implantou um *malware* para sequestrar uma sessão válida de SSO, roubar *cookies* válidos e elevar privilégios para acessar partes do ambiente de produção da CircleCI.

O agente da ameaça conseguiu, então, acessar e exfiltrar informações de clientes, incluindo variáveis de ambiente, *tokens* e chaves para sistemas dos clientes. Embora os dados tivessem sido criptografados durante o armazenamento, o relatório da CircleCI indicou que o agente da ameaça provavelmente conseguiu obter as chaves de criptografia da memória, de*script*ografar os dados e, posteriormente, acessar o ambiente de clientes específicos da CircleCI.

Em 2023, houve um aumento significativo na frequência de ataques à cadeia de suprimentos por agentes de ameaças baseados na Coreia do Norte. Embora esses agentes já tivessem visado várias etapas da cadeia de suprimentos em anos anteriores, como o ataque realizado em 2021 contra uma solução letã de monitoramento de ativos de TI para distribuir cargas maliciosas a um *think-tank* sul-coreano,[55] diversos incidentes em 2023 ganharam destaque.[56]

Em 2023

houve um aumento significativo na frequência de ataques à cadeia de suprimentos por agentes de ameaças baseados na Coreia do Norte.

[54] 'CircleCI incident report for January 4, 2023 security incident', CircleCI, https://circleci.com/blog/jan-4-2023-incident-report/ (12/1/2023)

[55] 'Lazarus Attackers Turn to the IT Supply Chain', Threatpost, https://threatpost.com/lazarus-apt-it-supplychain/175772/ (26/10/2021)

[56] PwC Threat Intelligence, CTO-SIB-20231024-01A - DPRK Supply Chain Attacks

2020

WIZVERA VeraPort

O grupo Black Artemis (também conhecido como Lazarus Group ou HIDDEN COBRA) explorou o utilitário de gerenciamento de segurança VeraPort da WIZVERA, amplamente usado na Coreia do Sul, para baixar um *malware* assinado digitalmente nos sistemas das vítimas a partir de servidores comprometidos.

2021

Empresa de TI da Letônia

O subgrupo Diamond Sleet do Black Artemis (também conhecido como Labyrinth Chollima, ZINC e TEMP.Hermit) invadiu um fornecedor letão de software de monitoramento de ativos de TI, provavelmente com o objetivo de alcançar os clientes finais.

2022-Mar/2023

X_Trader e 3CX

O ataque à cadeia de suprimentos do Black Artemis contra a 3CX – no qual uma atualização trojanizada distribuiu um *downloader* inicial nos sistemas das vítimas – teve origem na violação do software X_Trader da Trading Technologies.

Jul/2023

JumpCloud

O Black Artemis primeiro violou a JumpCloud, depois executou *scripts* maliciosos nos sistemas dos clientes por meio do *framework* de comandos da empresa para baixar e executar cargas maliciosas adicionais.

Ago/2023

Campanha VMConnect

O Black Artemis criou pacotes maliciosos PyPI e npm imitando o software VMConnect e outros pacotes voltados para criptomoedas. Esses pacotes continham código malicioso que decodificava uma carga útil nos sistemas das vítimas.

Out/2023

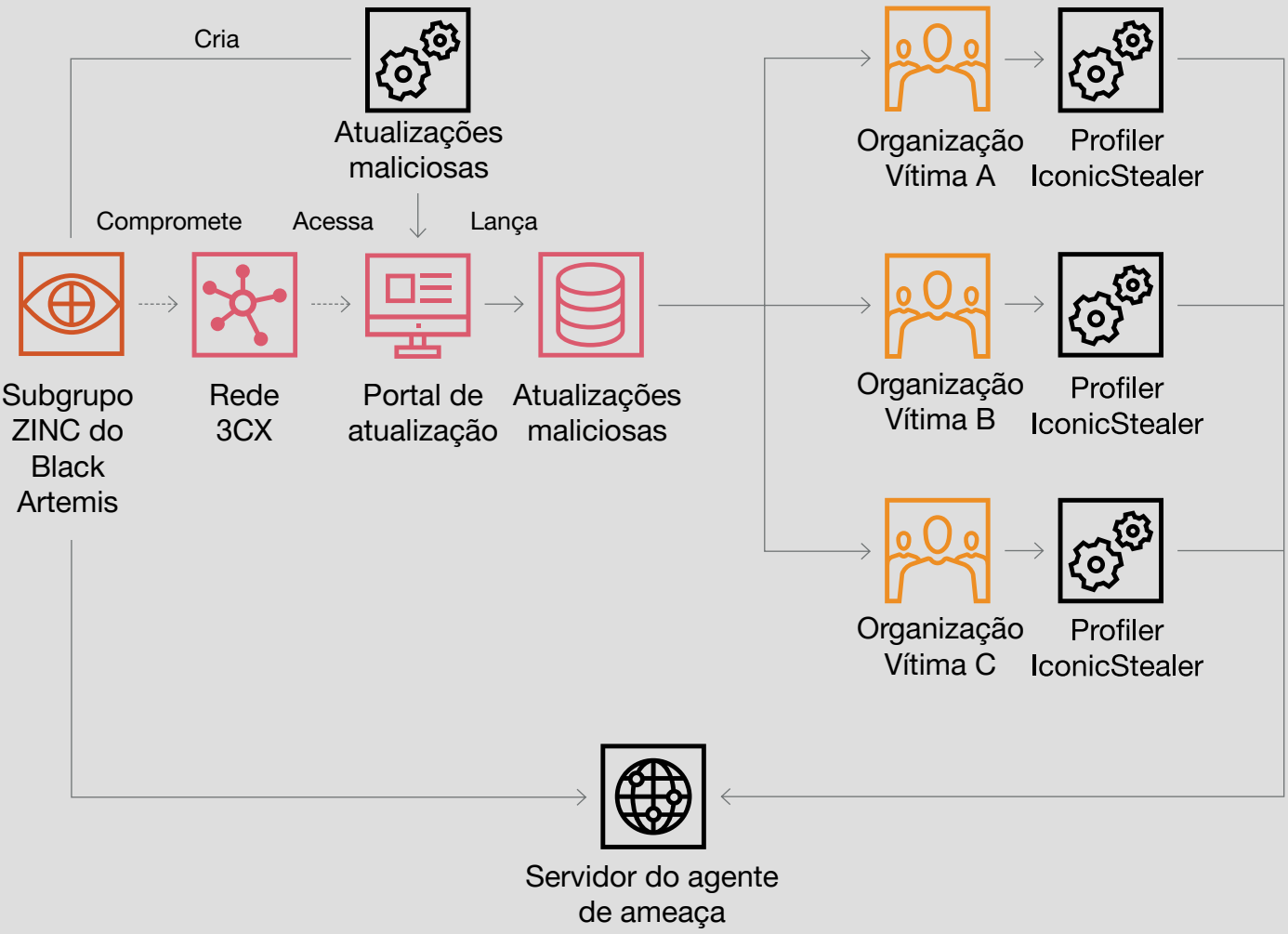
CyberLink

O subgrupo Diamond Sleet do Black Artemis usou um atualizador trojanizado da CyberLink (hospedado na infraestrutura da CyberLink) para instalar um *backdoor* personalizado, que chamamos de BlueMantis.

X_Trader e 3CX

Em janeiro de 2023, componentes da solução de videoconferência desenvolvida pela 3CX foram violados por um agente de ameaças baseado na Coreia do Norte, que a PwC chama de Black Artemis (também conhecido como Lazarus Group e HIDDEN COBRA).[57]

Tanto as versões para Windows quanto para macOS do 3CXDesktopApp foram modificadas para executar um *malware* de roubo de informações conhecido como IconicStealer. Algumas organizações vítimas do ataque (provavelmente apenas no setor de criptomoedas)[58] também tiveram um *backdoor* conhecido como Gopuram implantado por meio da aplicação trojanizada da 3CX para atividades subsequentes.[59]



[57] PwC Threat Intelligence, CTO-QRT-20230330-01A - 3CX Supply Chain Compromise

[58] 'Not just an infostealer: Gopuram *backdoor* deployed through 3CX supply chain attack', Kaspersky, https://securelist.com/gopuram-*backdoor*-deployed-through-3cx-supplychain-attack/109344/ (3/4/2023)

[59] PwC Threat Intelligence, CTO-TIB-20230414-02A - 3CX Supply Chain Compromise Followup

Pesquisas subsequentes de terceiros revelaram que a violação da cadeia de suprimentos da 3CX foi facilitada por um ataque anterior à cadeia de suprimentos, envolvendo software trojanizado da Trading Technologies.[60] Esse ataque provavelmente foi realizado por um subgrupo do Black Artemis conhecido como AppleJeus (também denominado Citrine Sleet), com base em capacidades semelhantes.

Um "ataque duplo à cadeia de suprimentos" não é algo comumente observado e demonstra alto grau de persistência e planejamento, ou pelo menos a capacidade do agente de ameaças de aproveitar oportunidades de violação, com o provável objetivo de atingir organizações de criptomoedas para ganho financeiro.

[60] '3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible', Mandiant, https://www.mandiant.com/resources/blog/3cx-software-supply-chaincompromise (20/4/2023)

Agentes de ameaças baseados na Coreia do Norte cometem outras violações da cadeia de suprimentos

Vários outros ataques à cadeia de suprimentos foram atribuídos a agentes de ameaças baseados na Coreia do Norte em 2023. Em junho, a JumpCloud, provedora de SaaS para gestão de dispositivos e identidades, foi afetada por um ataque à cadeia de suprimentos atribuído a um subgrupo do Black Artemis chamado TraderTraitor.[61]

O acesso inicial foi garantido pela engenharia social bem-sucedida realizada contra um engenheiro da JumpCloud, o que levou à alteração de um fluxo de trabalho para disseminar *malware* aos clientes da JumpCloud. Estima-se que cinco organizações tenham sido atingidas por esse incidente, que aparenta ter sido uma campanha direcionada.

Além disso, desde pelo menos julho de 2023, pesquisadores observaram uma campanha chamada VMConnect, que realizava engenharia social em alvos com convites para colaborar em projetos específicos de desenvolvimento de software nas áreas de *blockchain*, criptomoeda, apostas on-line e segurança cibernética.[62]

---

[61] 'JumpCloud Intrusion | Attacker Infrastructure Links Compromise to North Korean APT Activity', SentinelOne, https://www.sentinelone.com/labs/jumpcloud-intrusion-attacker-infrastructure-links-compromise-to-north-korean-aptactivity/ (20/7/2023)

[62] 'Security alert: social engineering campaign targets technology industry employees', GitHub, https://github.blog/2023-07-18-security-alert-social-engineering-campaign-targets-technology-industry-employees/ (18/7/2023)

O agente da ameaça, que também foi avaliado como provavelmente sendo o TraderTraitor,[63] usou uma combinação de pacotes maliciosos npm e Python incorporados nesses projetos para infectar os usuários finais.

3CX

Agente de ameaça:	Black Artemis – subgrupo AppleJeus
Alvo avaliado:	Organizações verticais de criptomoeda
Vetor de ataque:	Fornecedor de software comprometido e atualizações trojanizadas

JumpCloud

Agente de ameaça:	Black Artemis – subgrupo TraderTraitor
Alvo avaliado:	Organizações verticais de criptomoeda
Vetor de ataque:	Fornecedor de SaaS comprometido e fluxos de trabalho sequestrados

VMConnect

Agente de ameaça:	Black Artemis – subgrupo TraderTraitor
Alvo avaliado:	Organizações verticais de criptomoeda
Vetor de ataque:	Pacotes npm trojanizados disseminados para acesso inicial

Finalmente, em novembro de 2023, a Microsoft revelou uma violação da cadeia de suprimentos que ocorria desde o mês anterior pelo menos e foi atribuído ao subgrupo Black Artemis ZINC (também conhecido como Diamond Sleet, Labyrinth Chollima e TEMP.Hermit).[64]

Como parte desse ataque, o agente de ameaças trojanizou um binário de atualização da CyberLink, uma empresa de software de reconhecimento facial e multimídia. Esse binário modificado foi hospedado na infraestrutura comprometida da CyberLink para ser baixado pelas vítimas. Em seguida, o atualizador trojanizado descarregaria um *backdoor* básico de reconhecimento, que chamamos de “BlueMantis”, nos sistemas infectados, visando inicialmente traçar o perfil das vítimas a fim de selecionar alvos para ações futuras.[65]

---

[63] ‘JumpCloud Intrusion | Attacker Infrastructure Links Compromise to North Korean APT Activity’, SentinelOne, https://www.sentinelone.com/labs/jumpcloud-intrusion-attacker-infrastructure-links-compromise-to-north-korean-aptactivity/(20/7/2023)

[64] ‘Diamond Sleet supply chain compromise distributes a modified CyberLink installer’, Microsoft, https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modifiedcyberlink-installer/ (22/11/2023)

[65] PwC Threat Intelligence, CTO-QRT-20231124-01A - Black Artemis CyberLink supply chain compromise

Embora todas as violações da cadeia de suprimentos cometidas por agentes de ameaças baseados na Coreia do Norte descritas antes tenham visado principalmente organizações do setor de criptomoedas, elas enfatizam o impacto que esses incidentes podem causar de modo geral.

O acesso às organizações poderia ter sido muito mais amplo se as intrusões não tivessem sido descobertas mais cedo, o que ofereceria uma seleção de alvos além das organizações de criptomoedas, conforme desejado. Assim como a exploração de uma vulnerabilidade *zero-day*, há pouco ou nenhum aviso de que um ataque à cadeia de suprimentos está acontecendo, com muitos casos sendo detectados apenas após outras ações já terem sido realizadas pelo agente da ameaça.

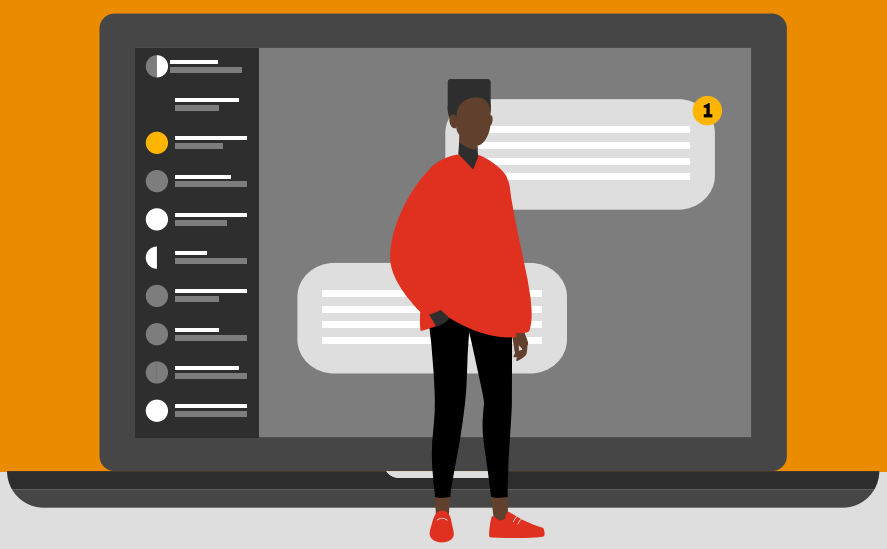
No geral, esses incidentes revelam um aumento na sofisticação das atividades dos agentes de ameaças baseados na Coreia do Norte. Conforme o acesso inicial às organizações se torna mais complexo devido a mudanças estratégicas nas políticas, como a desativação padrão de macros, e a segurança dos e-mails se fortalece, eles são forçados a buscar abordagens alternativas. Isso pode explicar por que esses agentes estão voltando sua atenção agora para outros pontos de entrada nas organizações.

Devido ao sucesso desses ataques em 2023 e aos desafios de se defender contra eles, prevê-se que os agentes de ameaças norte-coreanos possam continuar visando as cadeias de suprimentos em 2024.

Violações da cadeia de suprimentos cometidas por agentes de ameaças baseados na Coreia do Norte: o acesso às organizações poderia ter sido muito mais amplo se as intrusões não tivessem sido descobertas mais cedo, o que ofereceria uma seleção de alvos além das organizações de criptomoedas, conforme desejado.

Inteligência artificial

Principal insight: como os agentes de ameaças estão experimentando a IA para apoiar suas operações, seu uso não teve impacto significativo ao longo de 2023.



Após a apresentação das capacidades do ChatGPT no fim de 2022, surgiram especulações sobre a possibilidade de agentes de ameaças explorarem a IA no futuro. As observações iniciais, baseadas em pesquisas de fontes restritas e públicas, indicam que eles ainda estão na fase inicial de experimentação com diversos modelos de IA. No entanto, espera-se que, com o tempo, esse uso aumente em uma ampla variedade de campanhas.[66]

O uso mais impactante da IA por agentes de ameaças em 2023 ocorreu em violações de e-mail empresarial (BEC, na sigla em inglês). Com a criação de ferramentas como WormGPT[67] e as dicas gerais compartilhadas em fóruns na *dark web* para "desbloquear" as proteções de outras ferramentas de IA, os agentes de ameaças de BEC agora têm uma abordagem muito mais escalável para conduzir suas campanhas.

Seja pedindo que uma ferramenta de IA generativa crie iscas de *phishing* mais eficazes ou escreva um *malware* básico para o operador, a IA tem o potencial de reduzir ainda mais as barreiras de entrada para os agentes de ameaça.

---

[66] 'Threat Actors are Interested in Generative AI, but Use Remains Limited', Mandiant, https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited (17/8/2023)

[67] 'WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks', SlashNext, https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launchbusiness-email-compromise-attacks/ (13/7/2023)

Outro exemplo do emprego de IA foi a continuação do uso de imagens de personas geradas por IA pelo Yellow Dev 13 (também conhecido como Smoke Sandstorm e TA455) como parte de suas campanhas de *phishing*.[68] No entanto, essa abordagem não foi atualizada para usar modelos de IA mais novos disponíveis. Ela se concentrou mais na reutilização de personas criadas previamente.

No futuro, será mais difícil saber como diferentes tipos de agentes de ameaças estão explorando indevidamente a IA generativa. Observar agentes criminosos discutindo abordagens em fóruns ou observar operações de influência que utilizam personas geradas por IA pode fornecer bons insights, mas muitos usarão essas tecnologias de maneira discreta como parte de suas operações.

Da mesma forma, há um esforço considerável sendo dedicado à pesquisa de IA na perspectiva de defesa, visando aprimorar tarefas como a detecção de indicadores de comprometimento, revisão de códigos de segurança e desenvolvimento de *playbooks* para gerenciamento de incidentes.[69] Independentemente de quem use a IA generativa, a validação dos resultados continuará sendo um grande desafio no futuro previsível.

[68] PwC Threat Intelligence, CTO-TIB-20230811-01A - Relunching A Career with Yellow Dev 13

[69] PwC Threat Intelligence, CTO-SIB-20230310-01A - A primer into artificial intelligence

Atividade de agentes de ameaças baseados na China

Principal insight: agentes de ameaças baseados na China continuam a mirar globalmente diversos setores. Eles compartilham ferramentas entre si, mas têm adotado novas estratégias, como a utilização intensiva de recursos locais (*live off the land*) e o emprego de redes de *proxies* ocultas, para dificultar a detecção e atribuição de suas atividades.

Setores visados: aeroespacial, construção civil, defesa, educação, entretenimento, governamental, institutos de pesquisa (*think tanks*), logística, marítimo, mídia, mineração, organizações não governamentais (ONGs), política, produção industrial, saúde, serviços financeiros, serviços públicos, tecnologia, telecomunicações, transporte e varejo.

Países visados: Afeganistão, África do Sul, Alemanha, Argélia, Austrália, Brasil, Butão, Camboja, Coreia do Sul, Egito, Emirados Árabes Unidos, Espanha, Estados Unidos, Filipinas, França, Geórgia, Hungria, Índia, Indonésia, Irã, Irlanda, Itália, Japão, Jordânia, Macau, Mianmar, Nepal, Noruega, Paquistão, Polônia, Quênia, República Democrática do Congo, Republika Srpska, Romênia, Ruanda, Rússia, Sérvia, Sri Lanka, Suíça, Tailândia, Taiwan, Timor-Leste, Turcomenistão, Reino Unido, Uzbequistão, Zimbábue.

[70] 'How China Is Remaking the Belt and Road', The Diplomat, https://thediplomat.com/2023/10/how-china-isremaking-the-belt-and-road/ (19/10/2023)

Em outubro de 2023, durante o Fórum do Cinturão e Rota, que marcou o décimo aniversário da iniciativa, a China reiterou suas prioridades de alta tecnologia. Liderado pelo presidente Xi Jinping, o evento sinalizou uma mudança de enfoque, passando de grandes projetos de infraestrutura para iniciativas compactas e tecnologicamente avançadas, como finanças digitais, comércio eletrônico e projetos de sustentabilidade verde e azul.[70]

Essa mudança de direção deve levar a um ajuste nas estratégias dos agentes de ameaças baseados na China, com maior ênfase em tecnologias-chave e setores correlatos.[71]

A ampla gama de setores e países-alvo de agentes de ameaças baseados na China em 2023 ilustrou claramente a competência e os recursos abundantes que eles possuem. Durante o ano, nossa investigação expôs o rápido desenvolvimento desses grupos, desde o refinamento de estratégias preexistentes até a criação de novas.

Por exemplo, nossa pesquisa contínua sobre o agente de ameaças baseado na China Red Moros (também conhecido como GALLIUM, Granite Typhoon e Alloy Taurus) revelou seu foco em entidades na Europa, África e Ásia, utilizando ferramentas personalizadas já estabelecidas, como BlackMould,[72] [73] PingPull e Zapto.[74] [75]

---

[70] 'How China Is Remaking the Belt and Road', The Diplomat, https://thediplomat.com/2023/10/how-china-isremaking-the-belt-and-road/ (19/10/2023)

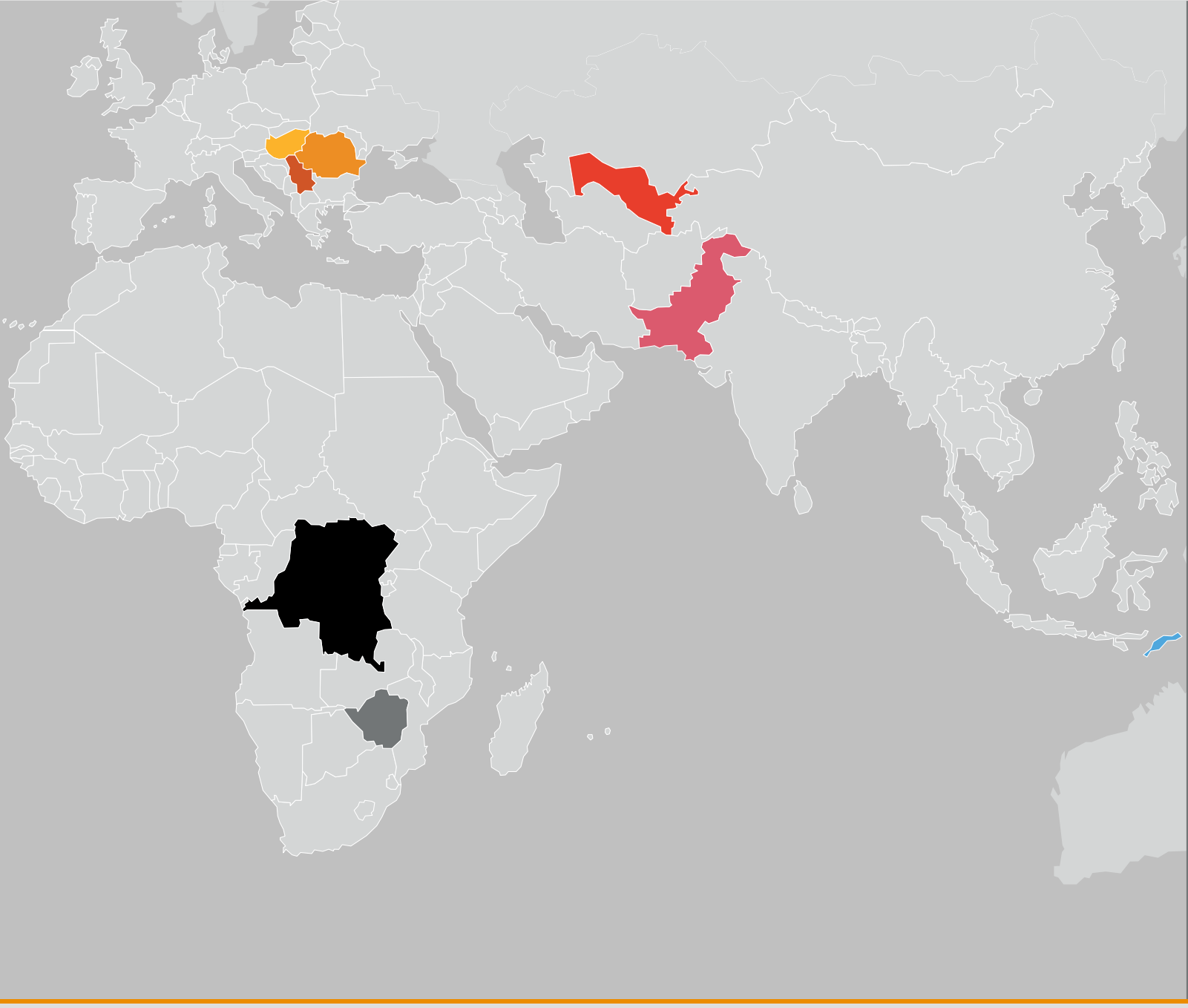
[71] PwC Threat Intelligence, CTO-SIB-20231201-01A - Belt and Road, and China's long-term strategy

[72] PwC Threat Intelligence, CTO-TIB-20230526-01A - Breaking the Mould

[73] 'GALLIUM: Targeting global telecom', Microsoft, https://www.microsoft.com/en-us/security/blog/2019/12/12/gallium-targeting-global-telecom/ (12/12/2019)

[74] PwC Threat Intelligence, CTO-TIB-20230912-01A - Red Moros runs riot

[75] 'Chinese Alloy Taurus Updates PingPull *Malware*', Palo Alto, https://unit42.paloaltonetworks.com/alloy-taurus/ (26/4/2023)



País: Hungria
Setor: governo

País: Romênia
Setor: telecomunicações

País: Sérvia
Setor: governo

País: Uzbequistão
Setor: telecomunicações

País: Paquistão
Setor: telecomunicações

País: Timor-Leste
Setor: telecomunicações

País: Zimbábue
Setor: telecomunicações

País: República Democrática do Congo
Setor: governo

Em time que está ganhando não se mexe

Em 2023, alguns agentes de ameaças baseados na China continuaram a usar ferramentas estabelecidas, provavelmente como continuação de acordos vigentes de *quartermaster*. O ShadowPad, um *backdoor* modular usado por pelo menos dez desses agentes, seguiu sendo amplamente utilizado, recorrendo a certificados SSL/TLS falsificados de renomadas empresas de tecnologia para servidores de comando e controle.[76]

Além disso, continuamos monitorando as atividades do Red Dev 32, que é provavelmente um escritório regional do agente de ameaças Red Scylla (conhecido também como CHROMIUM, Charcoal Typhoon, ControlX e Aquatic Panda), e seu uso do *backdoor* ShadowPad.[77]

Empregado há mais de uma década, o PlugX é outra ferramenta compartilhada entre os agentes de ameaças baseados na China. O Red Lich (também conhecido como Mustang Panda, BRONZE PRESIDENT, TANTALUM, TA416, RedDelta e Basin) continuou a usar sua variante do PlugX para atingir entidades governamentais em toda a Europa, adotando iscas temáticas de diplomacia ou política.[78]

Também continuamos observando esses agentes utilizando o *framework* comercial C2 Cobalt Strike. Em especial, observamos o Red Dev 50 empregar tanto as versões padrão do Cobalt Strike quanto uma variante personalizada e uma combinação de carregador em uma intrusão.[79]

O ShadowPad, um *backdoor* modular usado por pelo menos dez agentes de ameaças baseados na China, seguiu sendo amplamente utilizado, recorrendo a certificados SSL/TLS falsificados de renomadas empresas de tecnologia para servidores de comando e controle.

76 PwC Threat Intelligence, CTO-TIB-20230202-01A - ShadowPad flatters to deceive

77 PwC Threat Intelligence, CTO-TIB-20230124-01A - Red Dev 32 - Additional Infrastructure

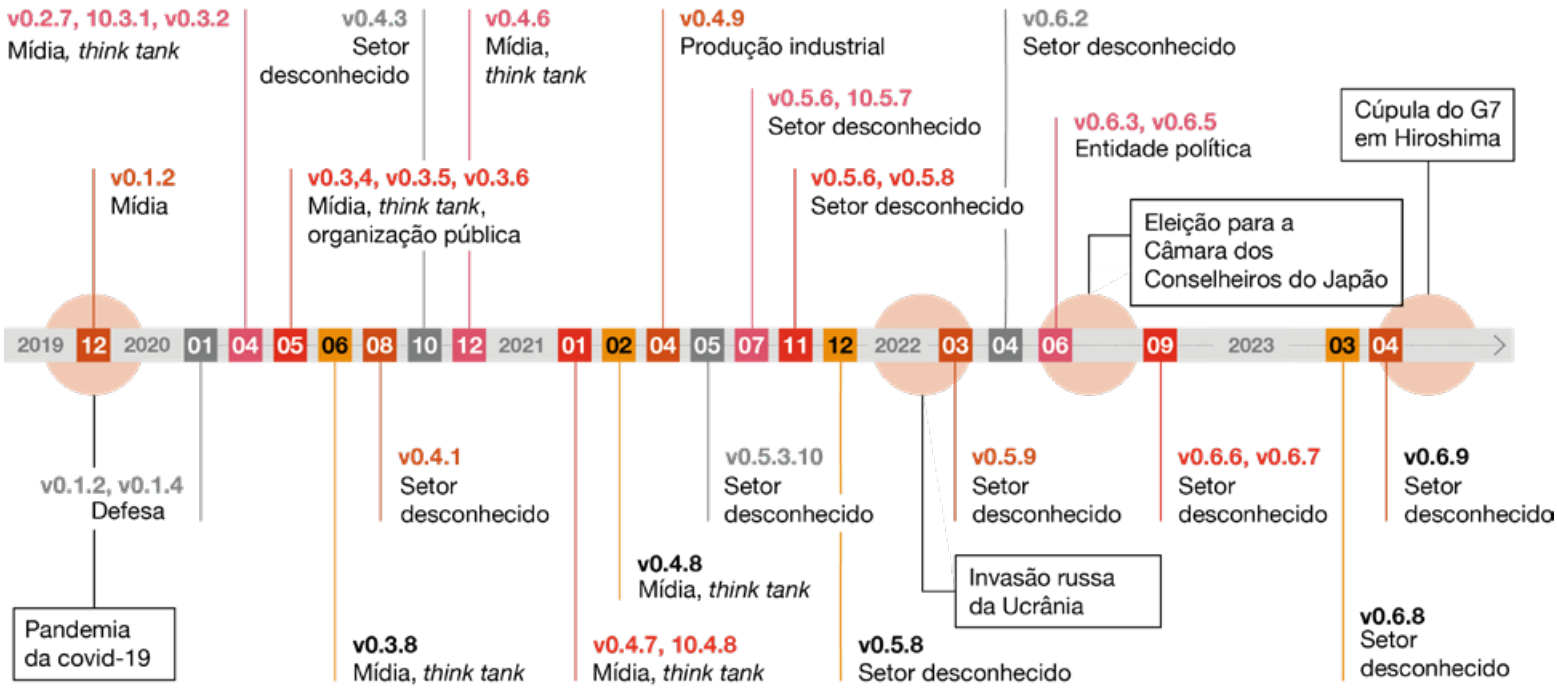
78 PwC Threat Intelligence, CTO-TIB-20230526-02A - Red Lichs PlugX Diplomacy

79 PwC Threat Intelligence, CTO-TIB-20230623-01A - Once, twice, three times AES

Artefatos deixados em amostras de *malware* também podem oferecer insights sobre o desenvolvimento de ferramentas específicas ao longo do tempo. Estamos monitorando a ferramenta de acesso remoto LODEINFO há vários anos. Ela provavelmente é usada pelo Red Apollo (também conhecido como APT10, Stone Panda e Cicada) para atacar entidades no Japão.[80] [81]

Com o tempo, a LODEINFO incorporou mais capacidades para permitir o acesso a um sistema infectado, como gerenciar arquivos, executar comandos, capturar telas e coletar registros de teclas. Algumas variantes até têm a opção de criptografar arquivos.[82]

Como parte dessa pesquisa, catalogamos as versões conhecidas de LODEINFO (baseadas em sua configuração interna) ao longo do tempo e relacionamos essas versões a campanhas específicas e setores visados, como ilustrado na figura a seguir.



[80] PwC Threat Intelligence, CTO-QRT-20230329-01A - LODEINFO activity targeting Japan

[81] PwC Threat Intelligence, CTO-TIB-20230718-02A - How LODEINFO has evolved over time

[82] 'APT10: Tracking down LODEINFO 2022, part II', Kaspersky, https://securelist.com/apt10-tracking-down-lodeinfo-2022-part-ii/107745/ (31/10/2023)

Estudo de caso

KEYPLUG

Um exemplo de um *backdoor* comum entre agentes de ameaças baseados na China é o KEYPLUG. A família de *malware*, que foi detalhada publicamente pela primeira vez em 2022, mas é provavelmente usada desde 2017,[83] é um *backdoor* em C++ para Windows e Linux.

Ela é capaz de operar com vários protocolos de rede, incluindo padrões como HTTP, TCP, UDP, mas também Websockets sobre TLS e MsQuic, além de ter suporte para uma gama de *plugins* para variantes do Windows.

Ao monitorar diferentes amostras e tipos de infraestrutura usados para operar o KEYPLUG, atribuímos atividades e alvos a vários agentes de ameaças baseados na China.[84] Por exemplo, observou-se que o Red Dev 39 provavelmente mirava organizações no Sudeste Asiático, além de usar um instalador do navegador Mozilla modificado para entregar o KEYPLUG.

O Red Dev 40 parece ter comprometido entidades no Paquistão, Afeganistão, Nepal e Sri Lanka. Também observamos tráfego provável do Red Dev 54 saindo de entidades governamentais africanas.[85]

83 'Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments', Mandiant, https://www.mandiant.com/resources/blog/apt41-us-state-governments (8/3/2022)

84 PwC Threat Intelligence, CTO-TIB-20230127-01A - KEYPLUG-ing away

85 PwC Threat Intelligence, CTO-TIB-20230921-01A - Red Dev 54 Flaxing its infrastructure

Baseando-se na infraestrutura observada dos usuários de KEYPLUG, notamos o uso do Cobalt Strike em diferentes formatos, como o Red Dev 48 utilizando o Geacon (uma implementação do Beacon do Cobalt Strike escrita em Golang)[86] ou o Red Dev 54 usando o CrossC2 (outra implementação do Beacon do Cobalt Strike para expandir o uso para macOS e Linux).

Os usuários de KEYPLUG também foram observados empregando o *scanner* de vulnerabilidades Acunetix, assim como a VPN SoftEther, ambos características comuns de agentes de ameaças baseados na China, como o Red Dev 32[87] e o Red Moros.[88] Prevemos uma alta probabilidade de uso do KEYPLUG em 2024, à medida que mais agentes o integrarem em suas ferramentas.

Uma pesquisa conjunta da nossa equipe, da SentinelOne e da Microsoft destaca o KEYPLUG, seu uso pelo Red Dev 40/STORM-0866 e suas conexões com o Sandman APT. Confira: https://www.sentinelone.com/labs/sandman-apt-china-based-adversaries-embrace-lua/

[86] PwC Threat Intelligence, CTO-TIB-20230615-01A - Red Dev 48s KEYPLUG scholarship

[87] PwC Threat Intelligence, CTO-TIB-20230124-01A - Red Dev 32 - Additional Infrastructure

[88] PwC Threat Intelligence, CTO-TIB-20230912-01A - Red Moros runs riot

Mudança de estratégia

Embora o *malware* personalizado, compartilhado e comercial ainda seja amplamente utilizado, agentes de ameaças baseados na China têm se adaptado ao uso de TTPs alternativos como parte de suas atividades de intrusão. Em maio de 2023, a Microsoft divulgou atividades de um agente de ameaças que ela identifica como Volt Typhoon (que monitoramos sob o nome de Red Dev 49).[89] [90]

O relatório detalha um agente de ameaças utilizando técnicas de exploração para acesso inicial, seguido por uma série de técnicas de *living off the land* para movimentação lateral e coleta de dados. O relatório também destaca os riscos de agentes de ameaças visando infraestruturas críticas nos EUA para reconhecimento, com possíveis objetivos futuros de sabotagem e ataques desestabilizadores.

Para acesso inicial, observamos a tendência de agentes de ameaças baseados na China dependerem mais fortemente da exploração de dispositivos de borda. Relatórios públicos, como os da CISA, destacaram de que forma agentes de ameaças como o Red Djinn (também conhecido como BlackTech, Palmerworm, Huapi e COBALT) violaram roteadores (no caso, via *firmware*) para ter acesso inicial e manter acesso persistente a uma rede.[91]

Por exemplo, observamos o Red Vulture (também conhecido como APT15/APT25, Nylon Typhoon e NICKEL) violando dispositivos Fortinet de organizações governamentais para acesso inicial.[92]

---

[89] 'Volt Typhoon targets US critical infrastructure with living-off-the-land techniques', Microsoft, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-landtechniques/ (24/5/2023)

[90] PwC Threat Intelligence, CTO-QRT-20230525-01A - Volt Typhoon

[91] 'ZuoRAT Hijacks SOHO Routers To Silently Stalk Networks', Lumen, https://blog.lumen.com/zuorat-hijacks-sohorouters-to-silently-stalk-networks/ (28/6/2022)

[92] PwC Threat Intelligence, CTO-TIB-20231219-01A - The TRIAD Cluster

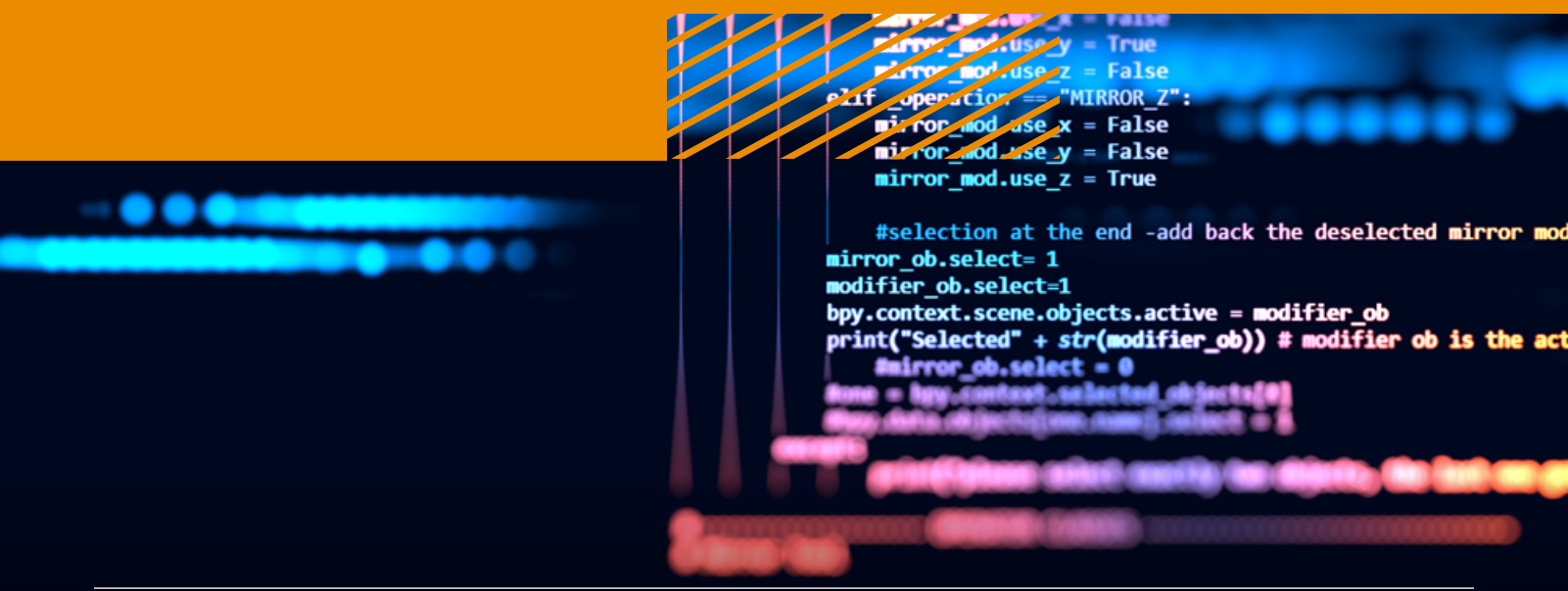
Atualização sobre redes de proxy

Em nosso relatório Ameaças cibernéticas: 2022 em retrospectiva, destacamos uma rede comercial de *proxy* encoberta usada por agentes de ameaças baseados na China e que chamamos de RedRelay.

As redes de *proxy* são usadas para diversos fins, inclusive anonimização para reconhecimento, varredura ativa de organizações, tentativas de exploração de vulnerabilidades em infraestruturas expostas ao público e, às vezes, como parte da administração de servidores de comando e controle ou para encaminhar tráfego desses servidores para servidores de *back-end*.

Ao longo de 2023, informamos sobre várias outras redes de *proxy* que monitoramos, além do uso atribuído a agentes de ameaças específicos, como Red Lumo (que opera o ZuoRAT)[93] e Red Vulture, que fez uso extensivo de outra rede de *proxy* além do RedRelay em 2023.[94] Essas redes realizaram atividades, como:

- reconhecimento de organizações na América do Norte, Europa, África e Ásia;
- ataques a tecnologias específicas, como Fortinet, Asus, Ivanti e Citrix;
- varredura de roteadores, câmeras IP, entre outros; e
- interação com infraestruturas de comando e controle, como ShadowPad e PlugX C2s.



[93] 'ZuoRAT Hijacks SOHO Routers To Silently Stalk Networks', Lumen, https://blog.lumen.com/zuorat-hijacks-sohorouters-to-silently-stalk-networks/ (28/6/2022)

[94] PwC Threat Intelligence, CTO-TIB-20231123-01A - Red Vultures Proxy Menagerie

O uso dessas redes por agentes de ameaças baseados na China pode ser desafiador para os defensores de redes, tanto no que diz respeito à identificação de indicadores técnicos quanto à atribuição de responsabilidade. Isso ocorre porque parte das redes de *proxy* pode ser formada por dispositivos comprometidos, como *botnets*, o que faz com que certos indicadores de comprometimento sejam temporários e difíceis de rastrear.

Além disso, o fato de diversas ameaças utilizarem as mesmas redes de *proxy* pode ocultar as reais intenções de atividades específicas, tornando necessário, em alguns casos, avaliar o comportamento da rede como um todo para compreender as ameaças e suas origens de forma mais precisa.

Ao longo de 2023, informamos sobre várias outras redes de *proxy* que monitoramos, além do uso atribuído a agentes de ameaças específicos, como Red Lumo (que opera o ZuoRAT) e Red Vulture, que fez uso extensivo de outra rede de *proxy* além do RedRelay em 2023.

Em resumo, observamos uma proliferação contínua das capacidades das redes de *proxy*, acompanhada por uma crescente diversidade de redes, usuários e fornecedores conhecidos. É altamente provável que vários agentes de ameaças baseados na China estejam atuando como facilitadores na distribuição de acesso a essas redes, permitindo sua rápida utilização conforme necessário.

Com base nessa análise, consideramos muito provável que a adoção de redes de *proxy* continue a se expandir em 2024 e nos anos seguintes, com um número cada vez maior de redes sustentando uma parcela crescente do cenário de agentes de ameaças baseados na China.

Atividade de agentes de ameaças baseados na Rússia

Principal insight: agentes de ameaças baseados na Rússia exibiram a maioria dos mesmos TTPs observados em anos anteriores, mas adaptaram suas abordagens para executar campanhas mais eficazes, especialmente utilizando explorações de vulnerabilidades críticas para obter acesso inicial e aprimorando vetores de infecção inicial e famílias de *malware*. Embora a espionagem tenha sido a principal motivação, também foram observados, ao longo de 2023, alguns agentes de ameaças com motivações duplas.

Setores visados: aviação, defesa, energia, governo, logística, marítimo, militar, petróleo e gás, serviços profissionais, tecnologia, transporte.

Países visados: Albânia, Alemanha, Eslováquia, Grécia, Itália, Jordânia, Noruega, Polônia, Portugal, República Tcheca, Romênia, Turquia, Ucrânia.

Em 2023, ocorreram importantes atribuições públicas relacionadas a agentes de ameaças baseados na Rússia. O NCSC do Reino Unido, em colaboração com parceiros internacionais, divulgou informações sobre o grupo russo conhecido como Star Blizzard, vinculando suas atividades ao Centro 18 do Serviço Federal de Segurança (FSB) da Rússia.

Essas ações incluíram tentativas de interferir na política e democracia do Reino Unido.[95] Além disso, a CISA, trabalhando em conjunto com outros órgãos, detalhou as atividades atribuídas ao Serviço de Inteligência Estrangeira Russo, especialmente ao grupo APT29, que explorou em massa vulnerabilidades no JetBrains TeamCity para obter acesso inicial.[96]

[95] 'UK and allies expose Russian intelligence services for cyber campaign of attempted political interference', NCSC, https://www.ncsc.gov.uk/news/uk-and-allies-expose-cyber-campaign-attempted-political-interference (7/12/2023)

[96] 'Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally', CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a (13/12/2023)

Além das atividades direcionadas à Ucrânia, conforme já mencionado, observamos vários agentes de ameaças baseados na Rússia operando em outras regiões em 2023. Entre eles, destacaram-se grupos prolíficos, como o Blue Otso (também conhecido como Grupo Gamaredon), que utilizou cadeias de infecção variadas,[97] experimentando uma série de linguagens de *script* para obter acesso inicial, como PowerShell, VBScript e LNKs.

Além disso, campanhas adicionais do Blue Dev 5 (também conhecido como NOBELIUM, Midnight Blizzard e BlueBravo), tiveram como alvo embaixadas por toda a Europa.[98] Em especial, o Blue Dev 5 usou diferentes abordagens em suas campanhas de *phishing*, como mostra a figura a seguir.

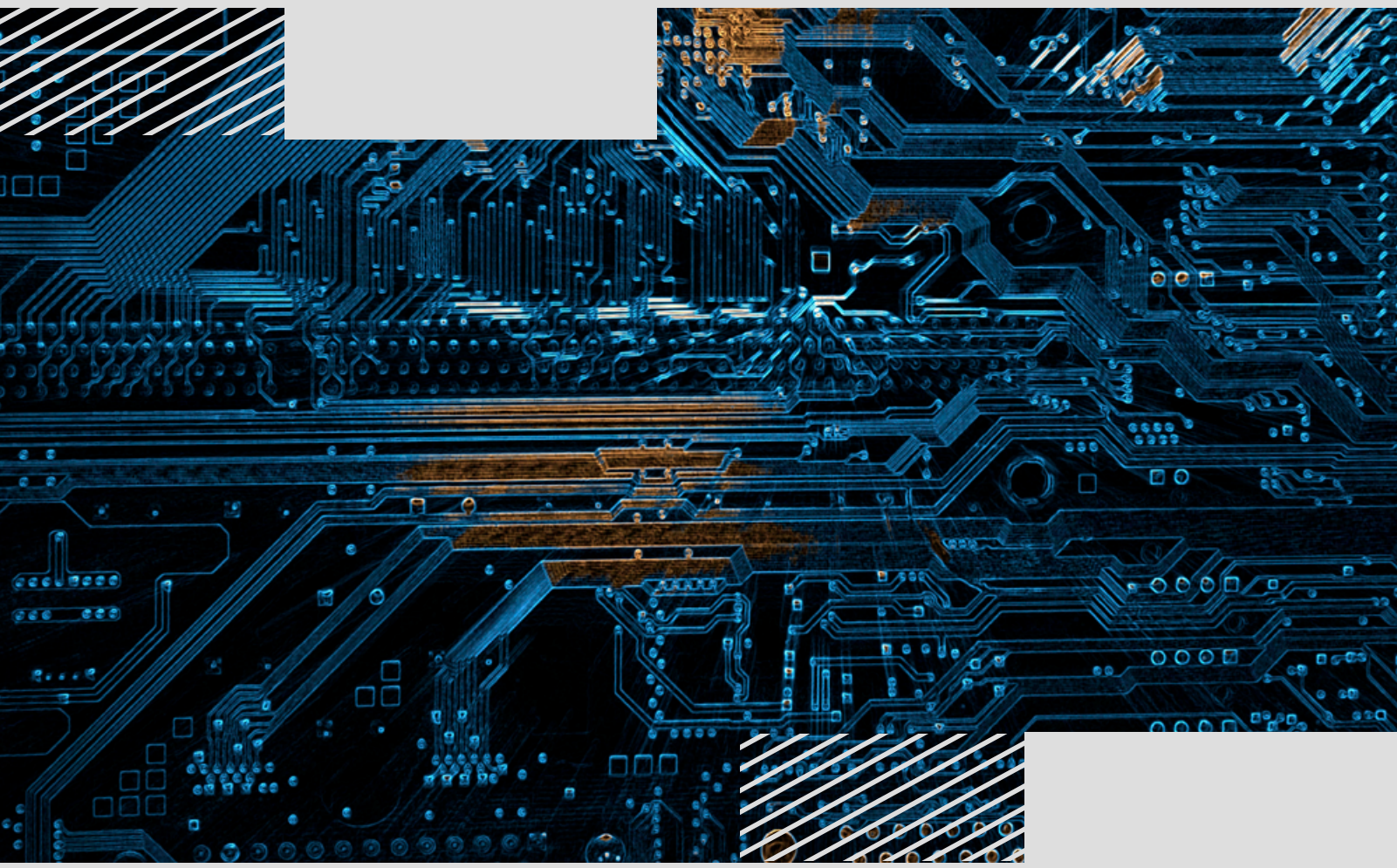
[97] PwC Threat Intelligence, CTO-TIB-20230116-01A - Blue Otsos diverse infection chains

[98] PwC Threat Intelligence, CTO-TIB-20230906-01A - An invitation to compromise

Houve algumas mudanças nos padrões de atividade de agentes de ameaças baseados na Rússia ao longo do ano. Por exemplo, o Blue Dev 11 (também conhecido como Tropical Scorpius, STORM-0968 e Void Rabisu) é um agente de ameaças com motivações duplas, inicialmente conhecido por disseminar o *ransomware* Cuba, mas que gradualmente passou a usar o *backdoor* RomCom para fins de espionagem.[99]

Além disso, continuamos a monitorar a infraestrutura do Blue Callisto (também conhecido como Callisto Group, SEABORGIUM e Star Blizzard) e observamos sobreposições com *stagers* do Cobalt Strike, o que indica que o Blue Callisto pode estar usando o Cobalt Strike.

Também há uma probabilidade realista de que outro agente de ameaças baseado na Rússia esteja utilizando essa infraestrutura para o Cobalt Strike (notamos algumas sobreposições de infraestrutura entre o Blue Dev 11 e o Blue Callisto no uso de um mesmo servidor).[100]



[99] PwC Threat Intelligence, CTO-TIB-20230210-01A - Blue Dev 11s ROMCOM isn't all love

[100] PwC Threat Intelligence, CTO-TIB-20230322-01A - Blue Callisto 2023 tracking update

Estudo de caso

Blue Athena

O Blue Athena (também conhecido como APT28, Sofacy e Fancy Bear) continuou sendo um agente de ameaças muito ativo, com base na Rússia, ao longo de 2023. Uma das principais campanhas descobertas foi a exploração da CVE-2023-23397 como um *zero-day*.[101]

Trata-se de uma vulnerabilidade crítica no Outlook que pode ser usada para roubar *hashes* NTLM por meio de um e-mail malicioso, assim que o Blue Athena é recebido e processado pelo cliente do Outlook.[102] A análise revelou que a exploração dessa vulnerabilidade estava ocorrendo desde pelo menos o início de 2022,[103] mas continuou ao longo de 2023.[104]

Uma característica marcante dessas campanhas foi o uso de roteadores Ubiquiti comprometidos para coletar credenciais roubadas, o que permitiu a identificação de atividades relacionadas ao Blue Athena.

Esses roteadores foram utilizados tanto para executar o Responder, capturando credenciais vazadas por meio da vulnerabilidade CVE-2023-23397,[105] quanto para realizar campanhas tradicionais de *phishing* de credenciais.[106] Os alvos eram diversos, abrangendo regiões geográficas (como Ucrânia, Turquia e Polônia) e setores variados, incluindo governo, petróleo e gás, defesa e logística.

[101] 'Guidance for investigating attacks using CVE-2023-23397', Microsoft, https://www.microsoft.com/en-us/security/blog/2023/03/24/guidancefor-investigating-attacks-using-cve-2023-23397/ (24/3/2023)

[102] PwC Threat Intelligence, CTO-QRT-20230316-01A - CVE-2023-23397

[103] PwC Threat Intelligence, CTO-TIB-20230517-01A - Blue Athena 2023 update

[104] PwC Threat Intelligence, CTO-TIB-20230921-03A - Ongoing exploitation of CVE-2023-23397

[105] GitHub, 'Responder/MultiRelay', https://github.com/lgandx/Responder

[106] PwC Threat Intelligence, CTO-TIB-20230517-01A - Blue Athena 2023 update

Outras atividades do Blue Athena também mostraram avanços em suas capacidades. Por exemplo, observamos o agente de ameaças usando um golpe de *phishing* com tema do Yahoo, falsificando um documento que sugere atividade suspeita na conta da vítima.[107]

Ao clicar no botão de redefinição de senha, o usuário seria alvo de um ataque de *browse*r-dentro-do-*browser* (BitB, na sigla em inglês) para coletar credenciais. Um ataque BitB cria uma janela *pop-up* que parece ser o próprio navegador (com um URL aparentemente legítimo), mas que, na verdade, é uma página web renderizada pelo atacante dentro de uma janela do navegador existente.

[107] PwC Threat Intelligence, CTO-TIB-20230629-01A - Blue Athena targeting Iranian diplomacy

Atividade de agentes de ameaças baseados no Irã

Principal insight: ferramentas de monitoramento e gerenciamento remoto, *malware* personalizado e *phishing* de credenciais continuam sendo as principais abordagens dos agentes de ameaças baseados no Irã. Em campanhas de sabotagem, eles tentaram usar várias identidades para disfarçar operações de *hack-and-leak*, nas quais informações são hackeadas e vazadas.

Setores visados: aeroespacial, defesa, dissidentes, educação, energia, governo, jurídico, logística, mídia, marítimo, ONG, petróleo e gás, político, produção industrial, saúde, segurança, serviços financeiros, serviços profissionais, serviços públicos, tecnologia, *think tanks*, transporte, transporte marítimo, turismo.

Países visados: Afeganistão, Albânia, Argentina, Arábia Saudita, Áustria, Azerbaijão, Bahrein, Catar, Cazaquistão, Coreia do Sul, Dinamarca, Egito, Estados Unidos, Iraque, Israel, Itália, Iêmen, Jordânia, Kuwait, Suécia, Turquia, Uruguai.

Ao longo de 2023, monitoramos e relatamos diversas atividades de agentes de ameaças baseados no Irã, abrangendo tanto grupos de intrusão bem estabelecidos quanto novos. A análise das atividades ao longo do ano revela uma tendência clara: a continuidade do uso de táticas eficazes em invasões e o aprimoramento de TTPs que precisam ser atualizados para garantir o sucesso das operações.

Por exemplo, o Yellow Nix (também conhecido como MuddyWater e Mango Sandstorm) continuou a usar ferramentas de monitoramento e gerenciamento remoto (RMM), com foco especial na ferramenta SimpleHelp RMM.

A aplicação dessas ferramentas permite que os agentes de ameaças reduzam custos com o emprego de uma solução pronta para uso, que pode permitir o acesso inicial, manter persistência e estabelecer comando e controle no ambiente visado.

Essas campanhas tinham diferentes alvos geográficos (com base em instaladores suspeitos observados e na análise da infraestrutura), provavelmente envolvendo entidades governamentais no Oriente Médio.[108]

O Yellow Garuda (conhecido como Charming Kitten, Mint Sandstorm, APT42 e ITG18) também continuou a usar páginas falsas de *login* do Google Meet no Google Sites, além de iscas em PDF que imitavam organizações de mídia ocidentais e *think tanks*.[109]

Os agentes de ameaças baseados no Irã continuaram a desenvolver novas ferramentas para suas campanhas. Por exemplo:

- o Yellow Dev 13 continuou a usar seu carregador de *malware* personalizado C5 (capaz de carregar PowerShell a partir de uma chave de registro);[110]
- o *backdoor* personalizado Mango, do Yellow Dev 9 (também conhecido como Lyceum e Storm-0133), utilizou um site violado de recrutamento israelense para comando e controle, além de usar o *backdoor* NotifyTray para atacar uma entidade governamental israelense;[111] [112] e
- o Yellow Maero (também conhecido como APT34, OilRig e Hazel Sandstorm) utilizou seu *backdoor* personalizado iDoor para provavelmente fazer vítimas no Iêmen.[113]

[108] PwC Threat Intelligence, CTO-TIB-20230207-01A - Yellow Nix simply wants to help

[109] PwC Threat Intelligence, CTO-TIB-20230512-01A - Pleased to Meet you, Hope you catch my creds

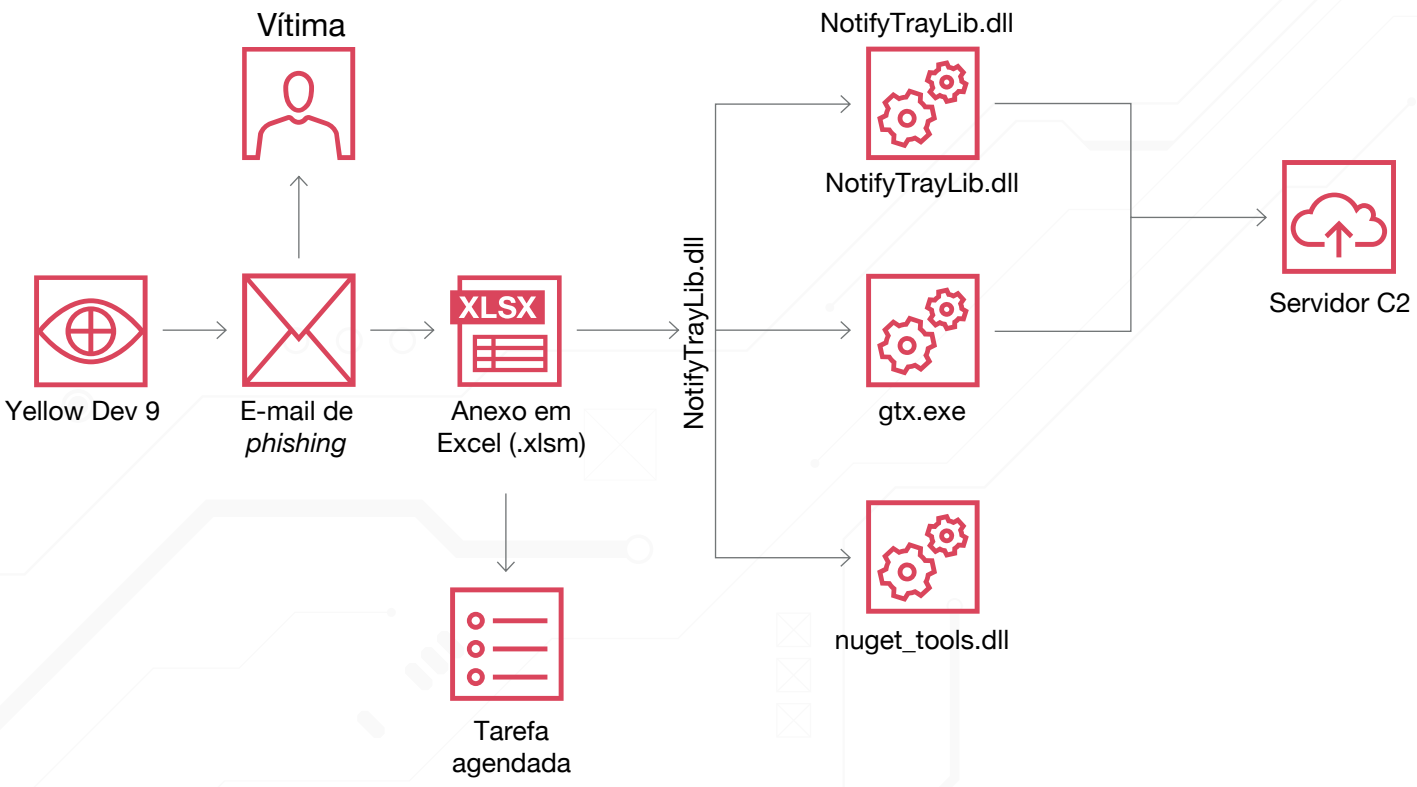
[110] PwC Threat Intelligence, CTO-TIB-20230811-01A - Relunching A Career with Yellow Dev 13

[111] PwC Threat Intelligence, CTO-TIB-20230607-01A - Mango obscuro

[112] PwC Threat Intelligence, CTO-TIB-20230623-02A - Reading with Lyceum

[113] PwC Threat Intelligence, CTO-TIB-20230713-01A - Listening at the iDoor

Em conjunto com outros pesquisadores,[114] também observamos o Yellow Garuda experimentando *malware* para macOS em 2023, o que destaca sua capacidade de ampliar seu escopo de ataques a *endpoints*.



Apesar do uso de *malware* personalizado, também observamos o emprego de ferramentas de código aberto. Por exemplo, com base nos caminhos de depuração (PDB) compartilhados, conseguimos agrupar o uso do iDoor pelo Yellow Maero e o do *framework* Covenant C2, provavelmente direcionados ao setor de serviços de TI na Jordânia e na Arábia Saudita (com base nos domínios falsificados e pacotes de idioma utilizados nas campanhas).[115] [116]

Além de suas ferramentas RMM, o Yellow Nix também utilizou ferramentas de código aberto ao longo de 2023 (e em anos anteriores), como a ferramenta de *proxy* Venom,[117] a ferramenta de tunelamento Ligolo[118] e a ferramenta de extração de credenciais LsassSilentProcessExit.[119] [120]

---

[114] 'Welcome to New York: Exploring TA453's Foray into LNKs and Mac *Malware*', Proofpoint, https://www.proofpoint.com/uk/blog/threat-insight/welcome-new-york-exploring-ta453s-foray-lnks-and-mac-*malware* (6/7/2023)

[115] PwC Threat Intelligence, CTO-TIB-20230713-01A - Listening at the iDoor

[116] GitHub, 'Covenant', https://github.com/cobbr/Covenant

[117] GitHub, 'Venom - A Multi-hop *Proxy* for Penetration Testers', https://github.com/Dliv3/Venom

[118] GitHub, 'Ligolo-ng : Tunneling like a VPN', https://github.com/nicocha30/ligolo-ng

[119] GitHub, 'LsassSilentProcessExit', https://github.com/deepinstinct/LsassSilentProcessExit

[120] PwC Threat Intelligence, CTO-TIB-20230207-01A - Yellow Nix simply wants to help

Agentes de ameaças baseados no Irã costumam usar personas para mascarar sua influência e operações de sabotagem. Monitoramos dois agentes de ameaças ao longo de 2023 que corresponderam a várias personas: Yellow Dev 19 (também conhecido como Vice Leaker, Cotton Sandstorm e Emennet Pasargad) e Yellow Dev 33 (também conhecido como Marigold Sandstorm e Cobalt Sapling).[121]

A motivação desses agentes de ameaças geralmente é relacionada à sabotagem, com ênfase em operações de *hack-and-leak*, mas eles também conduzem campanhas de baixo impacto, como desfigurações de sites ou ataques DDoS.

É altamente provável que eles também usem dados exfiltrados para fins de espionagem antes de vazar os dados on-line. O vazamento de dados provavelmente visa influenciar ou amplificar suas mensagens quanto a percepções, comportamentos ou decisões para promover interesses e objetivos estratégicos iranianos.

Agentes de ameaças baseados no Irã costumam usar personas para mascarar sua influência e suas operações de sabotagem.

Tabela 1 – Uma visão geral das personas usadas pelo Yellow Dev 19 e Yellow Dev 33 e nossa avaliação de cada uma delas em relação ao agente de ameaças

Ativo em 2023	Persona usada	Agente de ameaça	Avaliação de confiança*
Março	Moses Staff	Yellow Dev 33	Alta
Agosto	Anzu Team	Yellow Dev 19	Alta
Setembro	Yooz E Cybery	Yellow Dev 33	Média
Outubro	Moses Staff	Yellow Dev 33	Alta
Novembro	Cyber Toufan	Yellow Dev 19	Baixa
Novembro	Abraham's Ax	Yellow Dev 33	Alta

* Veja o Apêndice A – Metodologia.

[121] PwC Threat Intelligence, CTO-TIB-20231207-01A - The IRGC and its alter egos in 2023

Ambos os agentes de ameaças foram observados visando organizações em Israel, Bahrein, Suécia e Dinamarca em 2023. Por exemplo, o Moses Staff esteve ativo em vários momentos ao longo de 2023, postando dados de entidades israelenses e ameaçando fazer ataques destrutivos. Além disso, em novembro de 2023, uma persona que usava o nome Cyber Toufan divulgou em um fórum subterrâneo que estava vazando dados de uma empresa de segurança israelense.

Além das campanhas de destruição mencionadas anteriormente em relação ao conflito Israel/Hamas, foram observadas outras campanhas focadas em sabotagem. O Yellow Dev 35 (também conhecido como Cyber Av3ngers e Soldiers of Solomon), muito provavelmente parte do Corpo da Guarda Revolucionária Islâmica do Irã (IRGC, na sigla em inglês),[122] [123] visou infraestruturas críticas utilizando controladores lógicos programáveis da série Unitronics Vision, acessíveis pela internet.

Eles vandalizaram esses sistemas e reivindicaram a implantação de *ransomware*.[124] Os principais alvos foram serviços de fornecimento de água nos EUA, mas vários setores em Israel, como energia, transporte marítimo e logística, também foram alvos desse agente de ameaças.

[122] 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities', CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a (1/12/2023)

[123] Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure', U.S. DEPARTMENT OF THE TREASURY, https://home.treasury.gov/news/press-releases/jy2072 (2/2/2024)

[124] PwC Threat Intelligence, CTO-QRT-20231205-01A - Yellow Dev 35 targets Unitronics PLCs in sabotage attacks against critical infrastructure

Estudo de caso

Yellow Liderc

O agente de ameaças baseado no Irã Yellow Liderc (também conhecido como Imperial Kitten, Tortoiseshell, TA456 e Crimson Sandstorm) é outro alinhado ao IRGC que permaneceu ativo durante todo o ano de 2023. Em relação às suas TTPs habituais de comprometimento estratégico de websites, houve uma atualização em 2023 na maneira como os domínios são usados em páginas da web comprometidas.

De forma específica, o agente de ameaças deixou de usar domínios relacionados ao jQuery ou redes de entrega de conteúdo (CDNs), passando a adotar domínios que estão diretamente relacionados ao próprio site infectado,[125] assim como à ferramenta de insights sobre experiência do produto, Hotjar.[126]

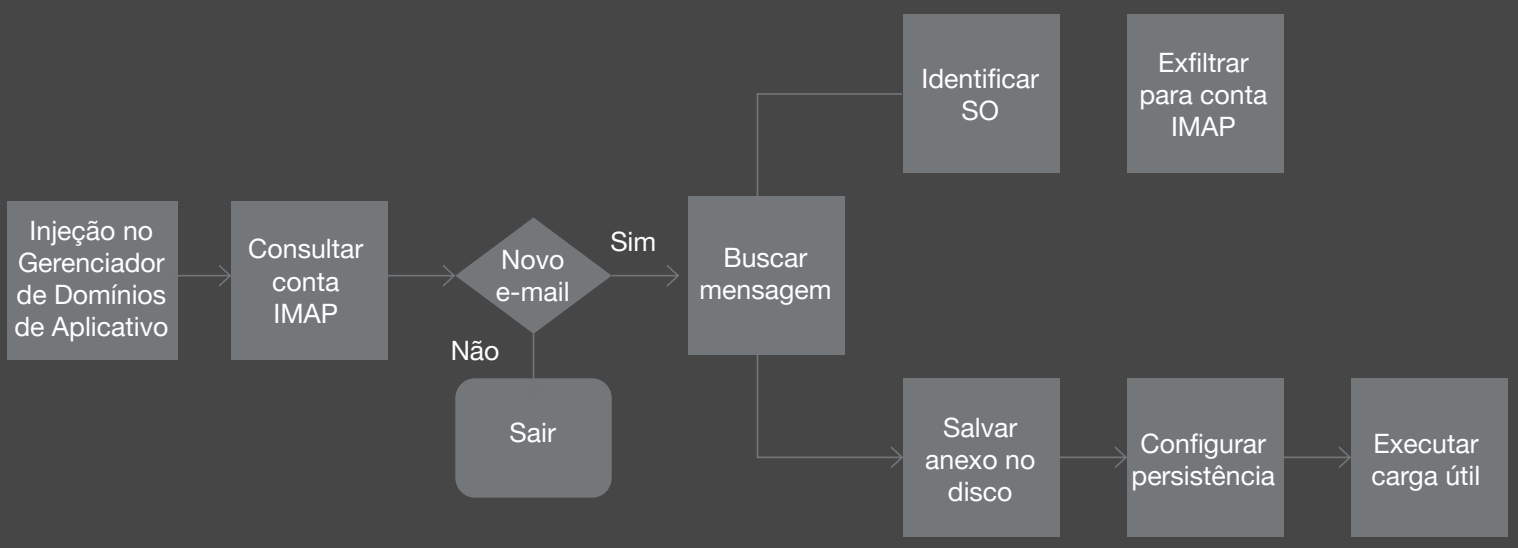
Uma campanha observada em 2023 destacou que o Yellow Liderc havia violado o site de uma organização marítima e logística da América do Sul com Java*Script* malicioso embutido para traçar o perfil dos visitantes do site. Avaliamos que a motivação provável desse comprometimento foi a relação de longa data da organização com uma empresa de transporte e logística de Israel. Historicamente, o Yellow Liderc se concentra em alvos de Israel.

[125] PwC Threat Intelligence, CTO-QRT-20230418-01A - Yellow Liderc strikes again

[126] PwC Threat Intelligence, CTO-QRT-20230815-01A - Yellow Lidercs recent *script* activity

Observamos uma nova ferramenta utilizada pelo Yellow Liderc, conhecida como IMAPLoader, que avaliamos ser provavelmente uma substituição para um implante IMAP baseado em Python que foi usado em 2021 e 2022.[127] Essa família de *malware* funciona como um *downloader*, possibilitando que um agente de ameaças obtenha informações sobre um sistema infectado e baixe etapas subsequentes utilizando o protocolo IMAP e contas de e-mail sob seu controle.

Para mais análises sobre o Yellow Liderc, consulte nosso blog de outubro de 2023.



[127] PwC Threat Intelligence, CTO-TIB-20231024-01A - Yellow Liderc ships its *scripts* and delivers IMAPLoader *malware*

Atividade de agentes de ameaças baseados na Coreia do Norte

Principal insight: agentes de ameaças baseados na Coreia do Norte continuam a mirar os mesmos setores esperados, incluindo criptomoedas e organizações não governamentais. Novos TTPs foram identificados para alcançar esses alvos, como versões de *malwares* já conhecidos para macOS e experimentações com novas técnicas de acesso inicial.

Setores visados: educação, energia, governo, mídia, ONGs, serviços financeiros, tecnologia.

Países visados: China, Cingapura, Coreia do Sul, Estados Unidos, Israel, Japão, Malta, Reino Unido, Tailândia, Vietnã.

[128] PwC Threat Intelligence, CTO-TIB-20230210-02A - Dont call m

Além de realizar ataques à cadeia de suprimentos destacados anteriormente, os agentes de ameaças baseados na Coreia do Norte continuaram suas atividades com um ritmo intenso e direcionado. No entanto, a maior parte dessas iniciativas seguiu padrões semelhantes aos que documentamos no passado.

O Black Alicanto (também conhecido como DangerousPassword, LeeryTurtle, CryptoMimic, CryptoCore, Operation SnatchCrypto, Bluenoroff e APT38) continuou a mirar organizações que operam no setor de criptomoedas e no espaço Web3, desde corretoras até empresas de finanças descentralizadas (DeFi).

Além de manter o uso de arquivos LNK, o Black Alicanto inovou ao utilizar HTML compilado (CHM), instaladores de software da Microsoft (MSI) e arquivos de Disco Rígido Virtual (VHD, na sigla em inglês) como métodos de acesso inicial durante 2022 e 2023.[128]

O grupo também persistiu no uso de e-mail e redes sociais, incluindo LinkedIn, em suas estratégias de engenharia social, geralmente se apresentando como fornecedores de informações sobre oportunidades de investimento e financiamento ou atuando como recrutadores.[129]

No fim de 2022 e ao longo de 2023, o Black Alicanto ampliou seu arsenal com *malware*s destinados a sistemas macOS, exemplificado pelo uso da ferramenta conhecida como RustBucket em fontes abertas.[130] Projetamos que o Black Alicanto continuará a explorar novas famílias de *malware* para macOS ao longo de 2024.

As estimativas anuais sobre o valor roubado em criptomoedas por agentes de ameaças ligados à Coreia do Norte continuam a crescer, com relatórios apontando que, entre 2017 e 2023, o montante total chega a 1,7 bilhão de dólares.[131]

---

128 PwC Threat Intelligence, CTO-TIB-20230210-02A - Dont call my name, Alicanto

129 PwC Threat Intelligence, CTO-TIB-20230731-01A - Keeping up with Black Alicanto infrastructure

130 ‘BlueNoroff APT group targets macOS with ‘RustBucket’ *Malware*’, Jamf, https://www.jamf.com/blog/bluenoroffapt-targets-macos-rustbucket-*malware*/ (21/4/2023)

131 ‘North Korean Hackers Stole $600 Million in Crypto in 2023’, TRM, https://www.trmlabs.com/post/north-korean-hackers-stole-600-million-in-crypto-in-2023 (5/1/2024)

Os lucros gerados por essas operações provavelmente continuam a financiar o regime norte-coreano, incluindo seu programa de mísseis, o qual, segundo autoridades dos EUA, é custeado em aproximadamente 50% por ataques cibernéticos e roubos de criptomoedas conduzidos por esses agentes.[132] Prevemos que o foco da Coreia do Norte em criptomoedas continuará ao longo de 2024.

O Black Banshee (também conhecido como Kimsuky, APT43, THALLIUM e Emerald Sleet) continuou a se passar por *think tanks*, organizações não governamentais (ONGs) e meios de comunicação, com o objetivo de realizar ataques de *phishing* contra indivíduos em *think tanks*, institutos de formulação de políticas e organizações próximas ao governo, para coletar credenciais de contas de e-mail ou implantar *malware*.

As atividades do Black Banshee provavelmente estão alinhadas com seu objetivo de longo prazo de reunir informações sobre questões diplomáticas e políticas nos países visados, incluindo sanções internacionais, políticas nucleares e cooperação (sobretudo militar) de outros países com a Coreia do Sul.[133]

Também observamos que o Black Shoggoth (conhecido ainda como APT37, Reaper e Ricochet Chollima) continuou a empregar o ROKRAT – utilizando, por exemplo, documentos falsificados que simulavam um acordo entre uma empresa líbia do setor de petróleo, gás e energia e uma empresa sul-coreana que a financiava.[134]

Fizemos uma apresentação na conferência SANS CyberThreat sobre as atividades do Black Alicanto: https://sansorg.egnyte.com/dl/3P3HxFiNgL

[132] 'Half of North Korean missile program funded by cyberattacks and crypto theft, White House says', CNN, https://edition.cnn.com/2023/05/10/politics/northkorean-missile-program-cyberattacks/index.html (10/5/2023)

[133] PwC Threat Intelligence, CTO-TIB-20230503-01A - Black Banshees requests for comment

[134] PwC Threat Intelligence, CTO-TUS-20230228-01A - Threats under the Spotlight January 2023

Estudo de caso

Andariel

No fim de outubro de 2023, observamos o grupo Andariel (também conhecido como Onyx Sleet, PLUTONIUM, Silent Chollima, Stonefly e Clasiopa), que monitoramos como um subgrupo do agente de ameaças norte-coreano Black Artemis (conhecido ainda como Lazarus Group e HIDDEN COBRA), direcionando ataques a sistemas Citrix expostos à internet.[135]

O grupo realizou sequestro de sessões, provavelmente explorando a vulnerabilidade CVE-2023-4966 (também conhecida como CitrixBleed) e baixou o carregador TomCryptor para a ferramenta de *proxy* personalizada HazyLoad. Outras análises nos levaram a identificar uma ferramenta de tunelamento, chamada COUNTERCALL, usada em conjunto com o HazyLoad.

Os TTPs que observamos nessas intrusões estão alinhados com o *modus operandi* já estabelecido do Andariel. Desde pelo menos 2021, o grupo costuma explorar infraestruturas expostas à internet para obter acesso inicial, como nos casos de Log4Shell e da vulnerabilidade CVE-2023-42793 em instâncias do JetBrains TeamCity.[136] [137]

[135] PwC Threat Intelligence, CTO-TIB-20231219-02A - Andariel CitrixBleed and HazyLoad

[136] 'Operation Blacksmith: Lazarus targets organizations worldwide using novel Telegram-based *malware* written in DLang', Cisco, https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/ (11/12/2023)

[137] 'Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability', Microsoft, https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/ (18/10/2023)

Além disso, o uso de ferramentas de *proxy*, que destacamos em um estudo de caso no relatório “Ameaças cibernéticas 2022: um ano em retrospectiva”,[138] é uma prática comum. Enquanto alguns agentes de ameaças estão adotando o uso mais amplo de binários *living off the land* e reduzindo o uso de *malware* personalizado em suas campanhas, o Andariel demonstra que alguns grupos, especialmente os norte-coreanos, continuam a desenvolver seus próprios implantes para intrusões.

1,7 bilhão de dólares

A estimativa anual sobre o valor roubado em criptomoedas por agentes de ameaças norte-coreanos continua a crescer, com relatórios apontando que, entre 2017 e 2023, o montante total chega a 1,7 bilhão de dólares.

[138] PwC Threat Intelligence, CTO-YIR-20230403-01A - PwC Cyber Threats 2022 A Year in Retrospect

Atividade de agentes de ameaças motivados por crimes

Principal insight: a atividade de *ransomware* permanece intensa, com o número de vítimas em sites de vazamento superando significativamente os anos anteriores. A colaboração contínua entre operadores e afiliados tem acelerado o desenvolvimento de capacidades para criptografar e exfiltrar dados. O uso persistente de sistemas de entrega de *malware* e *stealers* (ferramentas de roubo de informações) sustenta essas táticas, mesmo com a repressão das autoridades. As violações de e-mails corporativos também continuam sendo altamente impactantes, embora recebam menos atenção que as operações de *ransomware*.

O cibercrime se manteve como uma ameaça universal, afetando a maioria dos países e setores com base em diversas técnicas, todas com o objetivo comum de monetizar o acesso a organizações e seus dados.

O ecossistema de *ransomware* como serviço (RaaS) incentiva agentes de ameaças a otimizar as operações de acesso a organizações, desde o acesso inicial (por meio de famílias de *malware* de cibercrime ou utilizando *logs* de ferramentas de roubo de credenciais para entrar em contas legítimas) até a implantação do *ransomware* por afiliados.

A extorsão de dados por meio de sites de vazamento é o principal objetivo dos afiliados de *ransomware*, com alguns optando por pular a fase de criptografia de dados, conforme destacado antes, na seção sobre a exploração de soluções de transferência de arquivos.

Para aumentar o impacto desses vazamentos, alguns grupos de *ransomware* buscam divulgá-los ao máximo, como no caso em que o agente da ameaça relatou a violação diretamente à Comissão de Valores Mobiliários dos EUA (SEC).[139] Mais detalhes sobre o tema na nossa visão sobre as regras de divulgação da SEC, além dos benefícios da inteligência de ameaças para ajudar a cumprir essas regras.

3.735

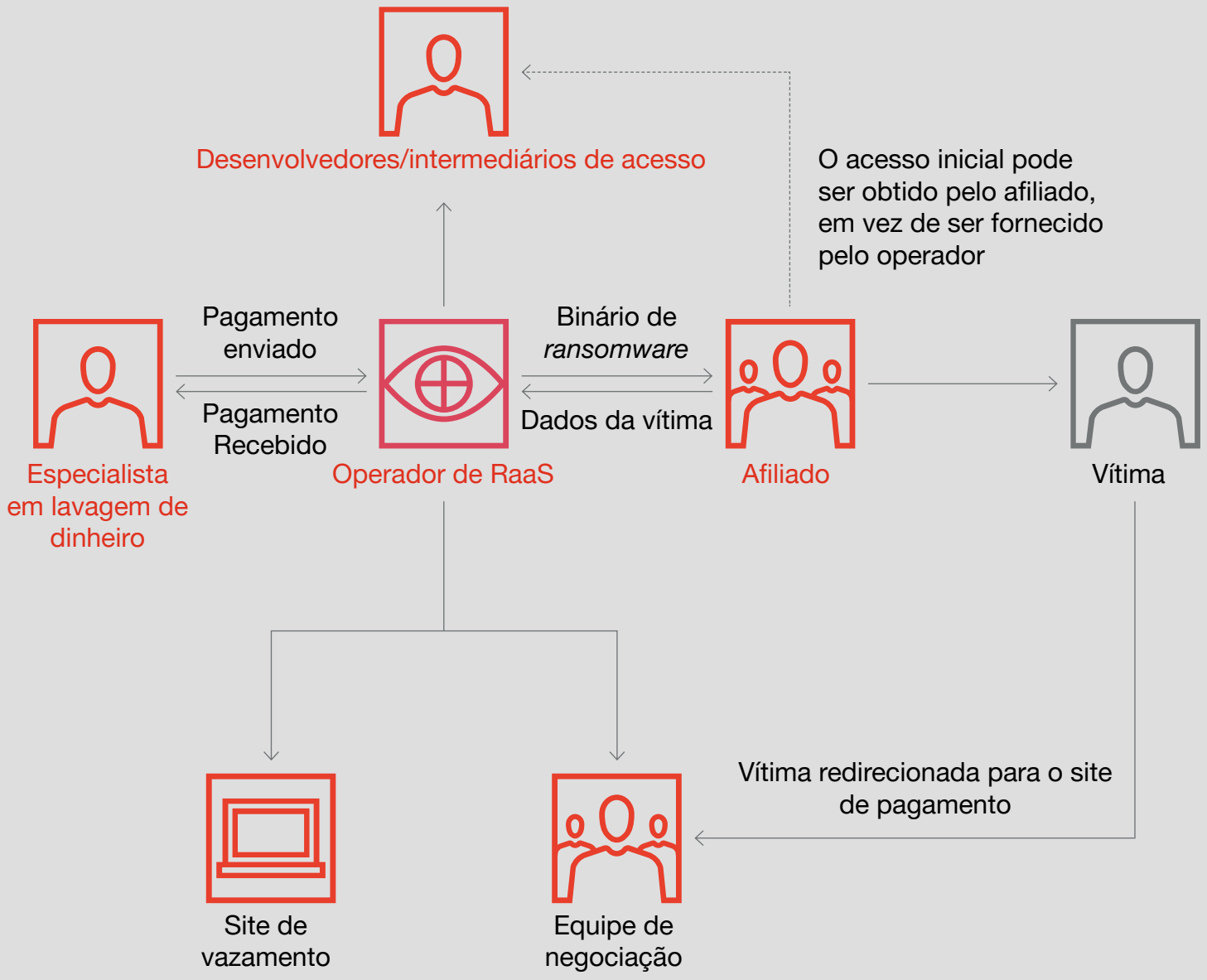
vítimas de *ransomware* em sites de vazamento foram observadas por nós em 2023. Esse é o maior número registrado em um único ano desde que começamos a monitorar esses dados, em 2019.

Além disso, a ameaça persistente representada por agentes de comprometimento de e-mail empresarial (BEC) afeta organizações globalmente e continua a superar o *ransomware* como a forma de cibercrime mais impactante em termos de perdas diretas, principalmente devido à baixa barreira de entrada e à fácil disponibilidade de recursos na internet aberta para facilitar esse tipo de operação.

[139] '*Ransomware* Group Files SEC Complaint Over Victim's Failure to Disclose Data Breach', SecurityWeek, https://www.securityweek.com/*ransomware*-group-files-sec-complaint-over-victims-failure-to-disclose-data-breach/ (16/11/2023)

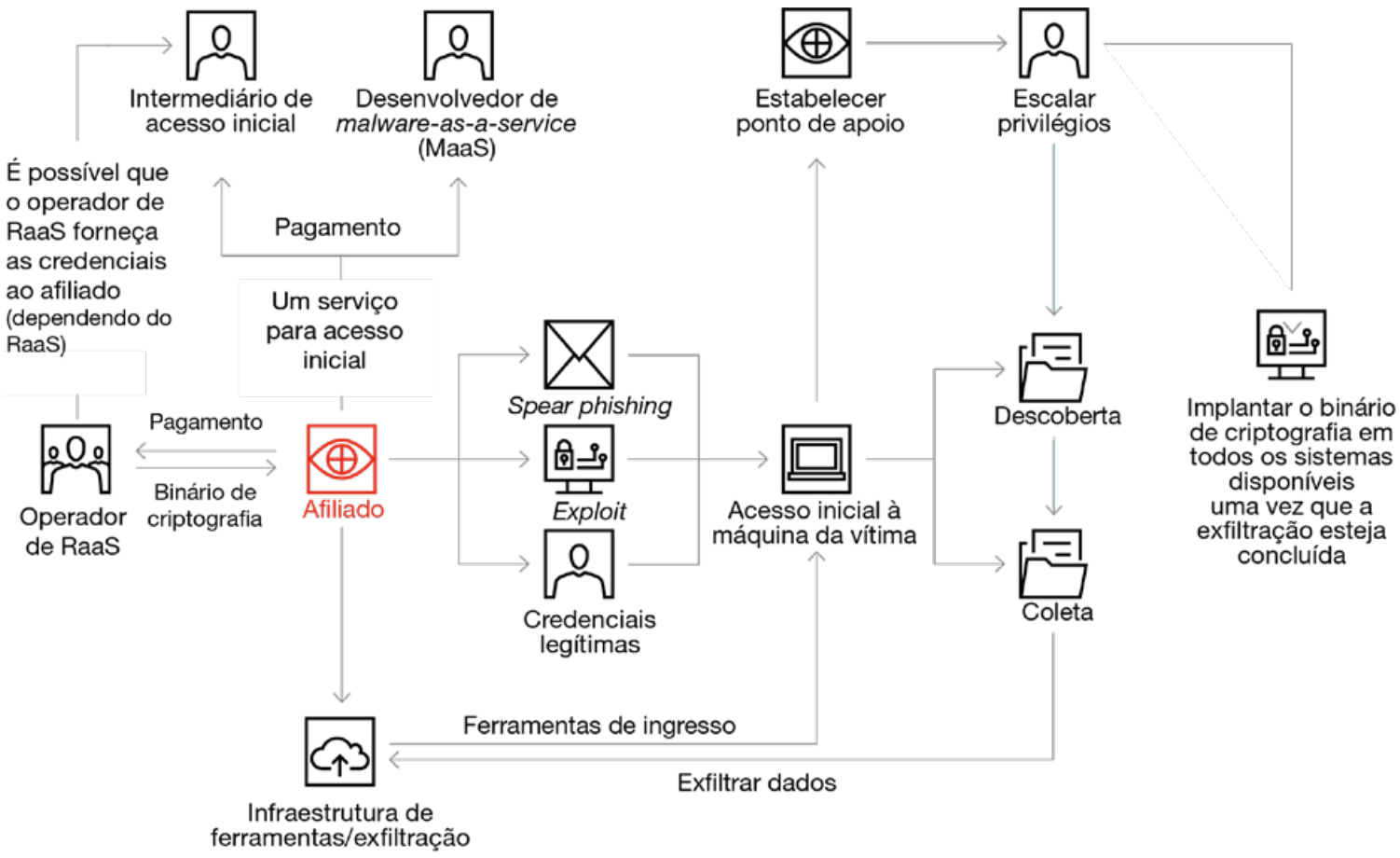
Ransomware-as-a-service

O ecossistema de RaaS (*ransomware* como serviço) é formado por programas de afiliados, que podem ser visualizados de forma aproximada na figura a seguir.[140]



[140] PwC Threat Intelligence, CTO-SIB-20231025-01A - Affiliates in the *ransomware* ecosystem Part 1

Essa segmentação das campanhas de *ransomware* permitiu que os ataques escalassem rapidamente, aumentando o número de grupos envolvidos. Com isso, os operadores dos programas podem se concentrar na "marca" e no desenvolvimento do *ransomware* (criando capacidades, como o *ransomware* ESXi),[141] enquanto a responsabilidade pela intrusão é delegada aos afiliados. A figura anterior pode ser reformulada em torno do afiliado de *ransomware*, conforme mostrado a seguir.

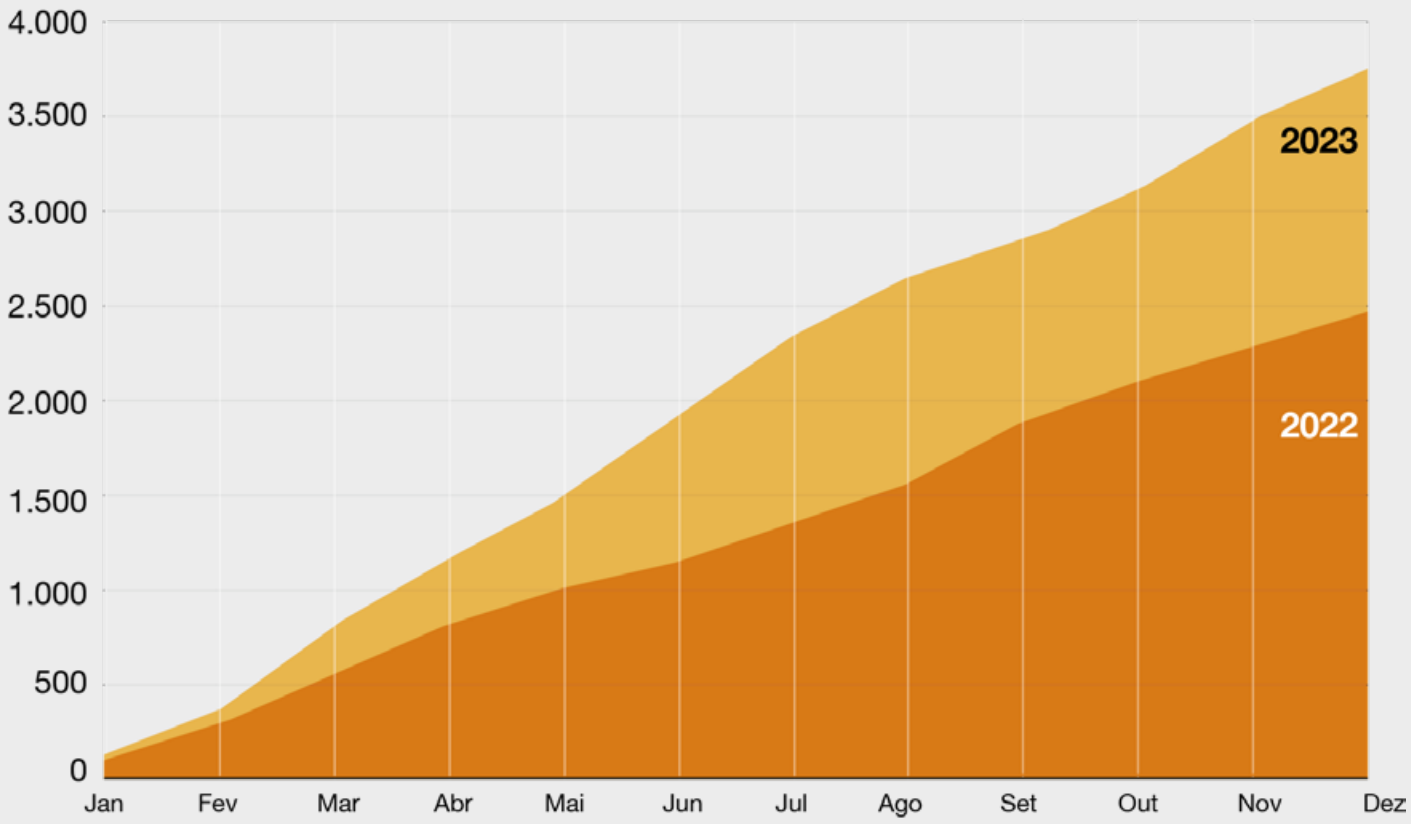


Em nosso relatório "Ameaças cibernéticas 2022: um ano em retrospectiva", avaliamos que os dados de sites de vazamento de *ransomware* de 2021 e 2022 (que apresentaram volumes semelhantes) representavam um "pico" dessa atividade. No entanto, essa previsão foi infelizmente refutada, já que o número total de vítimas em sites de vazamento de *ransomware* em 2023 superou o de 2022 já em agosto, quatro meses antes do fim do ano.[142]

[141] PwC Threat Intelligence, CTO-TIB-20230316-01A - ESXi don't think were in Windows anymore

[142] PwC Threat Intelligence, CTO-SRT-20230927-01A - *Ransomware* report for August 2023

Número de vítimas em 2022 x 2023



As campanhas do White Austaras (também conhecido como CL0P, Lace Tempest, FIN11 e TA505) com foco nas vulnerabilidades do GoAnywhere e MOVEit inflaram os números totais de sites de vazamento, acrescentando centenas de novas organizações à contagem geral de vítimas.

Uma explicação parcial para o aumento significativo em relação aos anos anteriores pode estar nas diversas campanhas direcionadas a soluções de transferência de arquivos gerenciados.

As campanhas do White Austaras (também conhecido como CL0P, Lace Tempest, FIN11 e TA505) com foco nas vulnerabilidades do GoAnywhere e MOVEit inflaram os números totais de sites de vazamento, acrescentando centenas de novas organizações à contagem geral de vítimas.[143]

No entanto, mesmo sem considerar esses incidentes, 2023 foi marcado por um crescimento da atividade de *ransomware*, evidenciando um ecossistema cada vez mais eficiente.

[143] PwC Threat Intelligence, CTO-SIB-20230821-01A - The audacity of White Austaras

Estudo de caso

Starfraud

O cibercriminoso conhecido como White Dev 146 (que também atende por Starfraud, 0ktapus, Scatter Swine, Scattered Spider e UNC3944) tem sido notório por realizar campanhas de *phishing* de credenciais. Desde junho de 2022, ele é suspeito de estar por trás de uma onda de ataques e violações direcionadas a diversos provedores de autenticação e empresas de tecnologia, afetando centenas de organizações de diferentes segmentos no setor privado.[144]

Um dos marcos dessas campanhas é o emprego de páginas de *login* fraudulentas, que imitam as interfaces de plataformas como Okta, Azure e Duo. Esse método visa capturar credenciais e senhas temporárias (OTPs) dos funcionários das empresas visadas.

[144] PwC Threat Intelligence, CTO-TIB-20230307-01A - The long reach of credential *phishing*

Indústria	Organizações simuladas
Telecomunicações	T-Mobile, AT&T, Verizon, Rogers, Telus, Lycamobile, Comcast, Sprint, Syniverse, Cricket Wireless
Tecnologia	Twilio, Okta, Cloudflare, Yahoo, Mailchimp, Intuit, Infosys, Mailgun, Twitter, SendGrid, Evernote, Gemini, HubSpot, Wipro, DXC Technology, Cognizant, ServiceNow
Experiência do cliente	Sitel, Transcom, Sykes, iQor, Qualfon, Sprint, Medallia, Teleperformance, TTEC, TaskUs, Sutherland Global, Sinch, Klaviyo, CGS, Afni, Alorica, Arise, Atento, Concentrix, Ibex, Startek, Working Solutions
Serviços profissionais	Accenture, Manpower Group
Mídia e entretenimento	Epic Games, Riot Games
Criptomoeda	Binance, Blockfi, Kucoin, Coinbase
Seguros	Asurion, Assurant
Turísmo e lazer	MGM Resorts
Varejo	Best Buy

Em setembro de 2023, o Starfraud ganhou as manchetes por seu envolvimento na violação da MGM Resorts.[145] Nesse ataque, ele simulou a identidade de um funcionário da MGM e utilizou suas credenciais para persuadir o suporte técnico de TI a redefinir o MFA da conta do empregado.

Com esse acesso, foi possível entrar nos sistemas do Okta e do Azure, estabelecendo um acesso contínuo e, por fim, implantar o *ransomware* ALPHV. O incidente teve grande repercussão, pois a queda dos sistemas resultou em problemas de acesso aos quartos dos hotéis e interrupções em serviços digitais.

[145] PwC Threat Intelligence, CTO-SIB-20231025-02A - Disruptors in the cyber criminal space

Sistemas de distribuição de *malware*

Além de algumas das explorações de vulnerabilidades críticas destacadas, afiliados de *ransomware* continuaram a usar sistemas de distribuição de *malware* como método de acesso inicial às redes. Essas famílias de *malware* (mais conhecidas como "*trojans* bancários") permitem que criminosos cibernéticos façam um perfil inicial do sistema infectado e, se desejarem, implantem ferramentas adicionais para atacar a rede.

Ao longo de 2023, alguns sistemas de distribuição foram observados de forma consistente. É o caso do Emotet da Blue Cronus (também conhecido como Grupo Conti), que emergiu de um período de inatividade para retomar plenamente suas operações.[146]

Algumas perturbações modificaram o cenário de ameaças. Por exemplo, uma ação coordenada de forças internacionais de segurança, denominada "Operação Duck Hunt", resultou na desinstalação forçada do botnet Qakbot de centenas de milhares de dispositivos, cessando efetivamente suas operações.[147]

Na sequência, a Blue Cronus adotou o sistema de entrega Pikabot,[148] utilizando uma combinação de cadeias de infecção para sua implantação, conforme ilustrado na figura a seguir.

Esperam-se mais perturbações causadas por sistemas de distribuição de *malware* em 2024. Os efeitos dessas ações demoram a se manifestar, com vários casos observados de ressurgimento dos *botnets* afetados.

Por exemplo, observaram-se campanhas de distribuição do Qakbot no fim de 2023, apesar de sua desativação no começo do ano.[149] Em meio a tudo isso, a adoção de variantes como Pikabot e DarkGate continuará em 2024,[150] evidenciando a natureza constantemente mutável dos agentes de ameaças no cibercrime.

---

[146] PwC Threat Intelligence, CTO-QRT-20230317-01A - Emotet recommences full scale operations

[147] PwC Threat Intelligence, CTO-QRT-20230830-01A - Qakbot is (not) ok

[148] PwC Threat Intelligence, CTO-QRT-20231114-01A - Pikabot picking up steam 149 PwC Threat Intelligence, CTO-QRT-20231218-01A - Qakbot back to hack

Ladrões de informação

Em uma época em que os agentes de ameaças obtêm acesso inicial a redes utilizando uma variedade de métodos complexos, como a exploração de vulnerabilidades em aplicações expostas ao público ou as cadeias de infecção mais recentes empregadas em ataques de *spear phishing*, uma abordagem mais simples se destaca: explorar a identidade alheia.

Como já foi destacado, o Starfraud usou esse recurso com grande eficácia em suas campanhas. No entanto, esse não foi o único agente de ameaças a fazê-lo. No ano passado, surgiram diversos novos tipos de *infostealers* (ladrões de informação), tanto baseados em atualizações de versões existentes quanto em variantes inéditas.

Esses programas são desenvolvidos para capturar credenciais de acesso a serviços on-line, dados de preenchimento automático, *cookies* armazenados em navegadores e detalhes de carteiras de criptomoedas. Entre eles, incluem-se:

- Redline[151]
- Vidar[152]
- Rhadamanthys[153]
- Mystic[154]
- Raccoon[155]

Assim como o RaaS, esses ladrões podem ser oferecidos como parte de plataformas de *malware* como serviço (MaaS). Isso permite que os usuários tenham acesso a diferentes níveis de funcionalidades e a um painel de controle no qual é possível visualizar as informações coletadas pelos ladrões.

[151] PwC Threat Intelligence, CTO-SIB-20230224-01A - We can steal it for you wholesale

[152] PwC Threat Intelligence, CTO-TIB-20230113-01A - Vidar Stealer

[153] PwC Threat Intelligence, CTO-TIB-20230228-01A - Rhadamanthys Stealer

[154] PwC Threat Intelligence, CTO-TIB-20230801-01A - Demystifying Mystic Stealer

[155] PwC Threat Intelligence, CTO-TIB-20231108-01A - Analysing *malware* with the wrapper still on

A prevalência desses ladrões de informações representa um problema sério para as organizações, pois as credenciais costumam ser reutilizadas em contas pessoais e corporativas.

Assim, mesmo que os pontos de acesso estejam protegidos contra todos os ladrões de credenciais dentro de uma organização, pode ser que o comprometimento de uma conta pessoal de um funcionário seja suficiente para permitir o *login* bem-sucedido de um agente de ameaça.

Isso destaca a importância de não apenas defender os dispositivos dentro de uma rede, mas também as identidades dos funcionários. Uma abordagem é monitorar *logs* de ladrões de credenciais ou bancos de dados de violações em busca de endereços de e-mail de funcionários, para identificar de forma proativa credenciais que possam estar comprometidas.

O sucesso desses ladrões de informações geralmente decorre de configurações inadequadas ou da falta de autenticação multifatorial na organização visada. Outro fator crítico é a proteção insuficiente de contas de alto valor, como as contas PAM, que muitas vezes não são adequadamente defendidas por métodos mais robustos, como as chaves de segurança FIDO2.[156]

[156] PwC Threat Intelligence, CTO-TIB-20230307-01A - The long reach of credential *phishing*

Comprometimento de e-mail empresarial

As organizações enfrentam uma série de ameaças de agentes sofisticados, mas uma das mais comuns globalmente é o comprometimento de e-mail empresarial (BEC), que pode ser até mais frequente que o próprio *ransomware* como serviço.[157] O uso generalizado de e-mails pelas empresas abre inúmeras possibilidades para campanhas oportunistas de BEC.

Normalmente, esses ataques envolvem a falsificação da identidade de empresas legítimas ou executivos para induzir funcionários a revelar informações sigilosas, transferir fundos ou comprar cartões-presente. Os responsáveis por esses ataques têm grande especialização em engenharia social e em obter acesso a contas de e-mail.

Aproximadamente 13% das atividades da equipe de resposta a incidentes da PwC foram dedicadas a violações de e-mail empresarial. A equipe da PwC Hong Kong observou várias campanhas do tipo *adversary-in-the-middle* (AiTM), empregando ferramentas como Evil QR, EvilProxy e Evilginx para roubar credenciais e *tokens* de sessão e acessar contas.[158] [159]

Outros incidentes também evidenciaram o uso de *credential stuffing* para acesso inicial de agentes de ameaças de BEC, explorando a reutilização de credenciais entre contas pessoais e empresariais.[160]

13%

das atividades da equipe de resposta a incidentes da PwC aproximadamente foram dedicadas a violações de e-mail empresarial.

---

[157] PwC Threat Intelligence, CTO-SIB-20230620-01A - Everybody wants to rule the inbox

[158] 'Watch Out for the Adversary-in-the-Middle: WhatsApp QR Code Hijacking Targets Hong Kong and Macau Consumers', Dark Lab, https://blog.darklab.hk/2023/10/26/watch-out-for-the-adversary-in-the-middle-whatsappqr-code-hijacking-targets-hong-kong-and-macau-consumers/ (26/10/2023)

[159] 'Watch Out for the Adversary-in-the-Middle: Multi-Stage AiTM *Phishing* and Business Email Compromise Campaign', Dark Lab, https://blog.darklab.hk/2023/11/01/watch-out-for-the-adversary-in-the-middle-multi-stageaitm-*phishing*-and-business-email-compromise-campaign/ (1/11/2023)

[160] PwC Threat Intelligence, CTO-TUS-20230324-01A - Threats Under the Spotlight February 2023

Outras atividades relevantes

Além das campanhas de agentes de ameaças esperadas (especialmente as de APTs comuns e grupos voltados para atividades criminosas), há sempre outros agrupamentos de atividades desses agentes que podem não ser atribuídos ou que não se enquadram claramente nas principais categorias discutidas antes.

Por exemplo, os agentes de ameaças contratados para realizar ataques continuaram ativos em 2023. Observamos algumas campanhas direcionadas ao setor de criptomoedas, com sobreposições de baixa confiança com o grupo White Dev 48 (também conhecido como DeathStalker).[161] Além disso, artigos de fontes abertas detalharam outras campanhas de mercenários cibernéticos e ataques sob encomenda em 2023.[162]

Atividades supostamente atribuídas a agentes de ameaças ocidentais também foram discutidas em 2023. Na mesma época em que a Kaspersky revelou a campanha Operação Triangulação – na qual seus pesquisadores foram alvo de implantes telefônicos em uma complexa cadeia de infecção com várias etapas – o FSB russo afirmou ter "desvendado uma operação de inteligência dos serviços especiais americanos utilizando dispositivos móveis da Apple".[163]

Também foi sugerido que a Agência de Segurança Nacional (NSA, na sigla em inglês) trabalhava em estreita colaboração com a Apple, porém nenhuma prova foi apresentada para sustentar essas afirmações. Em um relato separado, a empresa de segurança chinesa 360 Intelligence Centre indicou que a NSA continuava a utilizar uma ferramenta chamada SecondDate,[164] que havia sido divulgada nos vazamentos do ShadowBrokers.[165]

Apesar de se afirmar que a SecondDate ainda era usada e que tinha como alvo uma universidade chinesa, nenhuma evidência foi apresentada para corroborar essas declarações.

---

[161] PwC Threat Intelligence, CTO-QRT-20230607-01A - Shortcut to compromise

[162] 'Active Lycantrox infrastructure illumination', Sekoia, https://blog.sekoia.io/active-lycantrox-infrastructureillumination/ (2/10/2023)

[163] 'Russia says US hacked thousands of Apple phones in spy plot', Reuters, https://www.reuters.com/technology/russias-fsb-says-us-nsa-penetrated-thousands-apple-phones-spy-plot-2023-06-01/ (2/6/2023)

[164] '新证据!网攻西工大的神秘黑客身份被锁定，"间谍软件"是关键!', CoreSec360, https://mp.weixin.qq.com/s/yxV9AIMrasGiaSj5gi9LSg (14/9/2023)

[165] 'Hacking the hackers: everything you need to know about Shadow Brokers' attack on the NSA', Wired, https://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers (18/4/2017)

Agentes de ameaças vinculados à Turquia

Embora uma parte significativa das atividades de agentes de ameaças monitoradas seja associada a grupos criminosos ou às principais regiões conhecidas por ameaças persistentes avançadas, como China, Rússia, Coreia do Norte e Irã, a PwC observou uma diversidade de outros agentes no cenário de ameaças, alguns dos quais apresentaram TTPs inovadores.

Por exemplo, grupos turcos nem sempre são prioridade nas estratégias de segurança das organizações, mas em 2023 se observou uma variedade significativa de atividades por parte desses agentes. O coletivo hacktivista Teal Kayra (conhecido também como Türk Hack Tim ou Turk Hack Team) realizou ataques DDoS contra a Suécia e a Dinamarca como retaliação a episódios de queima de exemplares do Alcorão,[166] e o Teal Kurma (também conhecido como Sea Turtle) usou infraestrutura para simular ONGs e organizações midiáticas que servem ao público do Oriente Médio.[167]

Mais informações sobre o Teal Kurma podem ser encontradas em nosso blog.

[166] PwC Threat Intelligence, CTO-SIB-20230216-01A - Teal Kayras Cyber Army

[167] PwC Threat Intelligence, CTO-TIB-20231204-01A - The Tortoise and The Malwahare

Atividade de agentes de ameaças baseados no Líbano

No início do conflito entre Israel e Hamas, a PwC registrou atividades do agente de ameaças baseado no Líbano Aqua Dev 1 (também chamado de POLONIUM e Plaid Rain). Esse agente, conhecido por suas conexões com outros grupos afiliados ao Ministério da Inteligência e Segurança do Irã (MOIS)[168] e por sua aliança com o Hezbollah,[169] iniciou uma nova campanha em resposta ao conflito.

A campanha de *phishing* provavelmente distribuiu *malware* por meio de um site falso que se passava por uma plataforma de localização de israelenses desaparecidos. Além disso, observou-se que o agente de ameaças realizou varreduras em dispositivos Fortinet em Israel, a fim de explorá-los para obter acesso.[170] Embora o Aqua Dev 1 já fosse conhecido por visar Israel antes do conflito, essa campanha ressalta a natureza reativa dos agentes de ameaças motivados por eventos geopolíticos.

[168] 'Exposing POLONIUM activity and infrastructure targeting Israeli organizations', Microsoft, https://www.microsoft.com/en-us/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/ (2nd June 2022)

[169] PwC Threat Intelligence, CTO-QRT-20231016-01A - Aqua Dev 1 continues to focus on Israel

Spyware

O *spyware* comercial continuou a representar uma ameaça para diferentes organizações e indivíduos ao longo de 2023.[171] Foram publicados vários estudos relevantes sobre fornecedores de *spyware*, com alguns detalhes sobre seus clientes. Essas campanhas geralmente exploram vulnerabilidades de zero clique e um clique, além de vulnerabilidades já conhecidas, para atingir e infectar dispositivos móveis.

O Pegasus, desenvolvido pela empresa de tecnologia israelense NSO Group, que monitoramos como Grey Anqa, é um produto de *spyware* consolidado destinado a dispositivos Android e iOS. Anteriormente, o Pegasus era usado para monitorar ativistas, dissidentes, jornalistas, políticos, líderes governamentais e executivos do setor privado.[172]

Em 2023, investigações do Citizen Lab revelaram que o *spyware* também mirou um jornalista russo residente na Alemanha,[173] além de um funcionário de uma organização da sociedade civil com sede em Washington, DC e presença internacional.[174] A última campanha utilizou uma cadeia de *exploits* denominada BLASTPASS, que dependia de vulnerabilidades presentes na biblioteca libwebp, comumente usada para analisar imagens WebP.[175]

O *spyware* comercial continuou a representar uma ameaça para diferentes organizações e indivíduos ao longo de 2023. Foram publicados vários estudos relevantes sobre fornecedores de *spyware*, com alguns detalhes sobre seus clientes.

[171] PwC Threat Intelligence, CTO-SIB-20231201-02A - *Spyware* among us

[172] 'On the list: Ten prime ministers, three presidents and a king', Washington Post, https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-*spyware*/ (20/7/2021)

[173] 'Exiled Russian journalist hacked using NSO Group *spyware*', Guardian, https://www.theguardian.com/technology/2023/sep/13/exiled-russian-journalist-galina-timchenko-reportedly-hacked-using-nso-group-*spyware* (13/9/2023)

[174] 'BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild', Citizen Lab, https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/ (7/9/2023)

[175] PwC Threat Intelligence, CTO-QRT-20230928-01A - Critical WebP Vulnerability

Em outubro de 2023, a Anistia Internacional lançou um extenso relatório sobre o *spyware* Predagente, em parceria com o European Investigative Collaborations (EIC), contando com contribuições jornalísticas dos veículos Mediapart e Der Spiegel. Conhecido como Predagente Files, o relatório detalha o *spyware* Predagente, seu desenvolvedor – a empresa de tecnologia Cytrox AD, da Macedônia do Norte – e suas conexões com o fornecedor de *spyware* irlandês Intellexa.[176]

Uma investigação realizada em setembro de 2023 pelo Citizen Lab e pelo Google revelou que o ex-deputado egípcio Ahmed Eltantawy foi alvo de tentativas de instalação do *spyware* Predagente. Os ataques utilizaram links maliciosos enviados por SMS e WhatsApp, logo após Eltantawy anunciar que concorreria à Presidência do Egito em 2024.[177]

Em março de 2023, a administração Biden emitiu uma ordem executiva que proíbe agências governamentais dos EUA de utilizar *spyware* comercial.[178] Além disso, ao longo do ano, outros fornecedores de *spyware* comercial foram adicionados às listas de entidades sancionadas.[179]

No entanto, ainda não existe uma regulamentação global mais abrangente sobre *spyware*, o que dificulta o controle efetivo de sua disseminação. À medida que as tensões globais se intensificarem devido a conflitos existentes e novos, as capacidades de *spyware* enfrentarão cada vez mais escrutínio público, especialmente os produtos de *spyware* usados por entidades governamentais.

---

[176] 'Who are Intellexa, the Irish *spyware* company placed on a US 'blacklist'?', The Irish Times, https://www.irishtimes.com/technology/2023/07/19/who-are-intellexa-the-irish-spyware-company-placed-on-a-us-blacklist/ (19/7/2023)

[177] 'PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator *Spyware* After Announcing Presidential Ambitions', Citizen Lab, https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-withpredator-spyware-after-announcing-presidential-ambitions/ (22/9/2023)

[178] 'FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial *Spyware* that Poses Risks to National Security', The White House, https://www.whitehouse.gov/briefing-room/statementsreleases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-ofcommercial-spyware-that-poses-risks-to-national-security/ (27/3/2023)

[179] 'US adds *spyware* developers Intellexa, Cytrox to blacklist', SC Media, https://www.scmagazine.com/brief/us-addsspyware-developers-intellexa-cytrox-to-blacklist (19/7/2023)

Mudanças nos TTPs de acesso inicial

Após alguns atrasos, a Microsoft concluiu no início de 2023 a implementação do bloqueio padrão de macros em documentos baixados da internet.[180] Documentos habilitados para macros eram amplamente utilizados para obter acesso inicial aos sistemas Windows corporativos por meio de *spear phishing*.

Essa alteração obrigou os agentes de ameaças a buscar novas técnicas. Embora a adaptação aos novos vetores de infecção possa ser desafiadora para as organizações, essa mudança também pode proporcionar melhores oportunidades de detecção de comportamentos maliciosos, além de forçar os agentes de ameaças a investir em novos métodos para alcançar seus objetivos.

Entre o fim de 2022 e início de 2023, observou-se um aumento no uso de arquivos OneNote em campanhas de *phishing*.[181] Esse formato de arquivo permitia a inclusão de outros arquivos que, quando ativados com um duplo clique pelo usuário, seriam executados. Dessa forma, os *payloads* poderiam conter links de atalho do Windows (LNKs), *scripts* em lote, aplicações HTML (HTAs) ou até mesmo arquivos executáveis.

Em setembro de 2023, investigações do Citizen Lab e do Google revelaram que o ex-deputado egípcio Ahmed Eltantawy foi alvo de tentativas de instalação do *spyware* Predagente. Os ataques utilizaram links maliciosos enviados por SMS e WhatsApp, logo após Eltantawy anunciar que concorreria à Presidência do Egito em 2024.

[180] Microsoft, 'Macros from the internet are blocked by default in Office', https://learn.microsoft.com/en-us/deployoffice/security/internet-macrosblocked

[181] PwC Threat Intelligence, CTO-TIB-20230208-01A - There can only be OneNote

Embora essa técnica tenha ganhado popularidade inicialmente entre os sistemas de distribuição dos cibercriminosos (como o QakBot), a Microsoft foi rápida em lançar atualizações para bloquear a inserção de arquivos com extensões perigosas em documentos OneNote.[182] Isso fez com que a técnica tivesse vida curta, forçando os agentes de ameaças a se adaptarem mais uma vez.

Um método alternativo de acesso inicial que ganhou destaque no início de 2023 foi o malvertising. Trata-se de uma variante da técnica de comprometimento *drive-by* que envolve a compra de anúncios na internet, impulsionados por envenenamento de otimização de mecanismos de busca (SEO) para redirecionar as vítimas a páginas que simulam ser sites legítimos de download de aplicativos famosos.[183]

Observou-se a distribuição de várias famílias de *malware* por esse método, entre elas os ladrões de credenciais Redline e Rhadamanthys, *frameworks* comerciais de C2 como o Cobalt Strike, e sistemas de distribuição de *malware* como o IcedID.

Esse vetor de acesso inicial é mais oportunista em comparação com outros tipos de campanhas e não facilita a realização de ataques direcionados. No entanto, quando o objetivo é um comprometimento amplo e indiscriminado, o *malvertising* pode ser uma estratégia eficaz para atingir esse propósito.

Por fim, outro formato de arquivo que já foi usado no passado, mas que recentemente ganhou certa popularidade, é o Compiled HTML Help (CHM). Esses arquivos podem conter *scripts* que são executados quando abertos pelo usuário, como Java*Script* codificado (JSE), que observamos ser usado pelo White Dev 157 para atacar organizações de serviços financeiros na Coreia do Sul.[184]

Esperamos que os agentes de ameaças continuem a experimentar novas técnicas de acesso inicial, mas também acreditamos que eles se fixarão em algumas abordagens quando houver um histórico comprovado de sucesso. Dessa forma, algumas dessas abordagens provavelmente se tornarão mais consistentes.

---

[182] Microsoft, 'OneNote blocks embedded files that have dangerous extensions', https://learn.microsoft.com/en-us/deployoffice/security/onenote-extension-block

[183] PwC Threat Intelligence, CTO-TIB-20230130-01A - *Malvertising* primer

[184] PwC Threat Intelligence, CTO-TIB-20230815-01A - Unique CHM files with a history

A Microsoft foi rápida em lançar atualizações para bloquear a inserção de arquivos com extensões perigosas em documentos OneNote. Isso fez com que a técnica tivesse vida curta, forçando os agentes de ameaças a se adaptarem mais uma vez.

Apêndices

Apêndice A – Metodologia

Durante todo o ano, interagimos com clientes, *stakeholders* e especialistas do setor de segurança para validar e aperfeiçoar nossas necessidades de inteligência. Transformamos nossa visibilidade única, ferramentas personalizadas, expertise técnica e nossas análises em inteligência prática e útil para nossos clientes.

Este relatório apresenta uma seleção das análises que elaboramos ao longo de 2023. Além de nossos recursos próprios e do acesso a ferramentas comerciais e de código aberto, trabalhamos em estreita colaboração com as firmas do network PwC em situações de resposta a incidentes e em outras atividades.

Linguagem estimativa

As interpretações da linguagem estimativa ou probabilística (como “provavelmente” ou “quase certamente”) variam muito. Para prevenir mal-entendidos, empregamos termos qualitativos específicos neste relatório ao mencionar expressões de probabilidade e ao realizar avaliações de confiança, quando aplicável. Salvo indicação em contrário, nossas análises não se baseiam em métodos estatísticos.

Expressões de probabilidade

Termo qualitativo	Linguagem de probabilidade associada
Remoto ou muito improvável	Menos de 10%
Improvável ou pouco provável	10-25%
Probabilidade realista	26-50%
Provável ou provavelmente	51-75%
Altamente provável ou muito provável	76-90%
Quase certo	Mais de 90%

Níveis de confiança

Nível	Descrição
Baixo	As fontes de informação eram limitadas e havia muitas lacunas que impediam análises adicionais.
Médio	A(s) fonte(s) de informação estava(m) disponível(is) com confiabilidade média (por exemplo, acesso indireto à informação), embora houvesse lacunas que impediam análises adicionais.
Alto	A(s) fonte(s) de informação estava(m) disponível(is) com alta confiabilidade (por exemplo, acesso direto à informação) e/ou oferecia(m) graus de corroboração, possibilitando uma análise minuciosa.

Apêndice B – Referência de agentes de ameaças

A seguir, são apresentados todos os agentes de ameaças mencionados neste relatório, incluindo o nome atribuído pela PwC, apelidos conhecidos e as motivações avaliadas para cada agente.

Embora um dos nomes de agentes de ameaças utilizados pela equipe de inteligência de ameaças da PwC possa corresponder a apelidos de outros agentes conhecidos, isso não significa necessariamente uma correlação direta de 1:1 entre os nomes. Nossas atividades de monitoramento, agrupamento e atribuição são baseadas em nossa visibilidade.

Agente de ameaça	**Apelidos**	**Motivação**
Aqua Dev 1	POLONIUM, Plaid Rain	Espionagem
Black Alicanto	DangerousPassword, LeeryTurtle, CryptoMimic, CryptoCore, Operation SnatchCrypt, Blueelf, APT38, Sapphire Sleet	Crime cibernético
Black Artemis	Lazarus Group, HIDDEN COBRA	Espionagem, Crime cibernético
Black Banshee	Kimsuky, APT43, THALLIUM, Emerald Sleet	Espionagem
Black Shoggoth	APT37, Reaper, Ricochet Chollima	Espionagem
Blue Athena	APT28, Sofacy, Fancy Bear	Espionagem
Blue Callisto	Callisto Group, SEABORGIUM	Espionagem
Blue Cronus	Conti Group	Crime cibernético
Blue Dev 5	NOBELIUM, Midnight Blizzard, BlueBravo	Espionagem
Blue Dev 8	n/a	Espionagem
Blue Dev 11	Tropical Scorpius, STORM-0968, Void Rabisu	Crime cibernético, Espionagem
Blue Otso	Gamedragon Group	Espionagem
Grey Anqu	NSO Group	Espionagem
Grey Hades	Gaza Hacking Team, Molerats, Gaza Cybergang	Espionagem
Grey Karkadann	AridViper, APT-C-23, Desert Falcon	Espionagem
Red Dev 5	Oro0lxy, Ufo0lxy, DarkShadow	Espionagem
Red Dev 32	n/a	Espionagem
Red Dev 39	n/a	Espionagem
Red Dev 40	STORM-0866	Espionagem
Red Dev 43	n/a	Espionagem
Red Dev 48	n/a	Espionagem
Red Dev 49	Volt Typhoon	Espionagem
Red Dev 50	n/a	Espionagem
Red Dev 54	Flax Typhoon	Espionagem

Agente de ameaça	Apelidos	Motivação
Red Djinn	BlackTech, Palmerworm, Huapi, COBALT	Espionagem
Red Lich	Mustang Panda, BRONZE PRESIDENT, TANTALUM, T416, RedDelta, Basin	Espionagem
Red Lumo	n/a	Espionagem
Red Moros	GALLIUM, Granite Typhoon, Alloy Taurus	Espionagem
Red Relay	n/a	Espionagem
Red Scylla	CHROMIUM, Charcoal Typhoon, ControlX, Aquatic Panda, Earth Lusca	Espionagem
Red Vulture	APT25, Nylon Typhoon, NICKEL	Espionagem
Teal Kayra	Türk Hack Tim, Türk Hack Team	Hacktivismo
Teal Kurma	Sea Turtle	Espionagem
White Austaras	CLOP, Lace Tempest, TA505, FIN11	Espionagem
Beige Rukh	SysJoker, Storm-1133	Espionagem
White Dev 48	DeathStalker	Espionagem
White Dev 140	White Dev 140	Crime cibernético
White Dev 146	Oktapus, Scatter Swine, Scattered Spider, UNC3944	Crime cibernético
White Dev 149	NoName057(16)	Hacktivismo
White Dev 163	n/a	Desconhecido
White Dev 165	Cerber	Crime cibernético
White Janus	LockBit	Crime cibernético
White Lilith	Akira	Crime cibernético
Yellow Dev 9	Lyceum, Storm-0133	Espionagem
Yellow Dev 13	Smoke Sandstorm, TA455	Espionagem
Yellow Dev 19	Vice Leaker, Cotton Sandstorm, Emennet Pasargad	Espionagem, sabotagem
Yellow Dev 31	Storm-0842, DEV-0842	Sabotagem
Yellow Dev 33	Marigold Sandstorm, Cobalt Sapling	Sabotagem, hacktivismo
Yellow Dev 35	Cyber Av3ngers, Soldiers of Solomon	Sabotagem
Yellow Garuda	Charming Kitten, Mint Sandstorm, APT42, ITG18	Espionagem
Yellow Liderc	Imperial Kitten, Tortoiseshell, TA56, Crimson Sandstorm	Espionagem
Yellow Maestro	APT34, OilRig, Hazel Sandstorm	Espionagem
Yellow Nix	MuddyWater, Mango Sandstorm	Espionagem

Contatos

Eduardo Batista
Sócio e líder de Cibersegurança e Privacidade
eduardo.batista@pwc.com

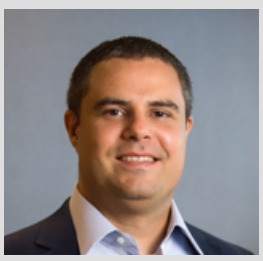
Fernando Mitre
Sócio
fernando.mitre@pwc.com

Joana Mendes
Sócia
joana.mendes@pwc.com

Larissa Escobar
Sócia
larissa.escobar@pwc.com

Magnus Santos
Sócio
magnus.santos@pwc.com

Maressa Juricic
Sócia
maressa.juricic@pwc.com



Rafael Cortes
Sócio
cortes.rafael@pwc.com

pwc

Acesse o site:

www.pwc.com.br

Siga a PwC nas redes sociais: