Ameaças cibernéticas: 2022 em retrospectiva

Sumário Executivo

pwc

Sumário Executivo

O cenário de ameaças cibernéticas ao longo de 2022 refletiu os eventos e as tensões geopolíticas do mundo real, com grande parte do ano sob o impacto da invasão da Ucrânia pela Rússia. A vulnerabilidade Log4Shell provocou um início de ano bem caótico e evidenciou a importância da colaboração da indústria de defesa e as empresas, bem como da criticidade de corrigir e compreender os softwares amplamente utilizados.

A Log4Shell foi um caso extremo em termos de vulnerabilidades divulgadas em 2022, à medida que os criminosos continuaram a fazer uso delas, com códigos maliciosos (*exploits*) e ferramentas bem conhecidas (como o Cobalt Strike) para conduzir seus ataques. No entanto, ao longo de 2022, também vimos esses agentes variando em motivação e sofisticação ao empregar ferramentas e estruturas mais elaboradas, além de terem modificado suas estratégias para superar as práticas de segurança implementadas pelos profissionais de cibersegurança. Adicionalmente, os agentes das ameaças cibernéticas visaram cada vez mais os ambientes em nuvem e as capacidades de identificação e acesso privilegiado.

À medida que a invasão russa escalou para uma guerra de grandes proporções, a Ucrânia ao lado de governos e organizações de cibersegurança ao redor do globo rastrearam e responderam a uma série de esforços de sabotagem implementados por criminosos baseados na Rússia, tais como múltiplas variantes de *wiperware* (códigos maliciosos que visam apagar os drivers ou a memória de computadores).[1, 2, 3] Esses ataques foram amplamente contidos dentro da zona de conflito imediato, isto é, na Ucrânia e nos territórios anexados pelos russos e assim não tiveram o mesmo nível de impacto que se verificou em 2015 e 2016, quando outros criminosos baseados na Rússia se voltaram às redes de energia elétrica ucranianas. Se, por um lado, vários agentes de ameaça cibernéticas motivados por espionagem reagiram a partir das notáveis mudanças nas operações de *phishing* e *targeting*; por outro lado, a própria guerra fez com que alguns cibercriminosos e hacktivistas (por exemplo, Blue Kurama, mais conhecido como Killnet) reagissem e respondessem em suas operações e declarações públicas, manifestando-se pró-Ucrânia ou pró-Rússia e visando entidades governamentais e do setor privado percebidas como de oposição no contexto da guerra.

---

[1] 'ESET Research apresenta junto com um representante do governo ucraniano o Industroyer2 na Black Hat USA, ESET, https://www.eset.com/int/about/newsroom/press-releases/events/eset-research-jointly-presents-industroyer2 -at-black-hat-usa-with-ukrainian-government-representativ/ (25 de agosto de 2022)

[2] 'NCSC aconselha organizações a agir após o ataque da Rússia à Ucrânia', UK National Cyber Security Centre (NCSC), https://www.ncsc.gov.uk/news/organizations-urged-to-bolster-defences (18 de março de 2022)

[3] 'Alerta AA22-110A - Ameaças cibernéticas criminosas e patrocinadas pelo estado russo à infraestrutura crítica', Agência de Cibersegurança e Infraestrutura dos EUA (CISA), https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (20 de abril de 2022)

Além da guerra na Ucrânia, o cenário de ameaças cibernéticas em 2022 viu a persistente otimização e sofisticação de operações de ameaça chinesas, ainda que seus alvos não tenham mudado significativamente em relação a anos anteriores. Esses criminosos empregaram ainda mais técnicas de ofuscação como serviço (*obfuscation-as-a-service*), tais como redes de *proxy* (RedRelay, por exemplo) e o compartilhamento de *malware*s, códigos maliciosos (*exploits*) e conjuntos de ferramentas (como ShadowPad e ScanBox). O agente de ameaças mais proeminente e prolífico a fazer isso foi o Red Scylla (também conhecido como CHROMIUM, ControlX, Earth Lusca, Aquatic Panda), que visou pelo menos 70 organizações em todo o mundo. Outros agentes realizaram operações sofisticadas que afetaram várias regiões, com alguns deles continuando a focar no setor de telecomunicações.

Agentes de ameaça baseados no Irã continuaram a ocupar as manchetes em 2022 graças a seu envolvimento em ataques de sabotagem contra o governo albanês, manifestantes e dissidentes, além de ataques setoriais que se voltaram a organizações, principalmente no Oriente Médio, na Europa e nos Estados Unidos – atividades que, com frequência, alinhavam-se com as prioridades do regime iraniano. Já os agentes da Coreia do Norte duplicaram os roubos de dinheiro a partir de *targeting* a serviços financeiros, criptomoedas e organizações de finanças descentralizadas (DeFi).

De modo geral, as ameaças persistentes avançadas (APT, na sigla em inglês), que analisamos em 2022, pareceram ter se padronizado em grande medida a *targetings* observados anteriormente. A despeito do esforço de algumas regiões da comunidade internacional para isolar economicamente seus países, alguns agentes fizeram avanços significativos em suas operações. Embora presumamos que ações no Ocidente também tenham ocorrido em 2022, não foram identificadas evidências adequadas dessas atividades e, portanto, elas não são abordadas extensivamente neste relatório.

O ecossistema de crime cibernético apresentou avanços na sofisticação de ataques em alguns casos, bem como novos desenvolvimentos que desafiaram as organizações em todo o mundo. Considerando que o *ransomware* permaneceu para muitos como a principal preocupação, vimos sim indícios de um potencial reagrupamento ou recalibração entre alguns agentes mais prolíficos e proeminentes desse tipo de software malicioso. Assim, 2022 terminou com um número quase idêntico de vítimas de vazamentos de sites em comparação com 2021.

Um dos agentes de ameaça mais preocupantes em 2022 foi o White Dev 111 (também conhecido como LAPSUS$ Group), que realizou uma série de operações *smash-and-grab* e *hack-and-leak* contra seus alvos. Muitos ataques usaram engenharia social e outras táticas para exaurir as medidas de segurança e os usuários das organizações que se tornaram vítimas dessas estratégias. As fraudes cibernéticas também se mostraram em crescimento exponencial em 2022, sublinhando ainda mais a tendência dos agentes de ameaça de atuarem na comoditização de acessos, *exploits* e ferramentas e na redução das barreiras à entrada para uma gama ainda maior de criminosos.

Sobre nós

A PwC tem mais de 200.000 clientes em 152 países. Usamos nossa posição privilegiada como uma das maiores redes de serviços profissionais do mundo para oferecer serviços de inteligência contra ameaças globais, oferecendo resultados customizados e entregues localmente a nossos clientes. Nossos estudos embasam nossos serviços de segurança e são usados por organizações dos setores público e privado em todo o mundo para proteger redes, fornecer conscientização situacional e informar estratégias.

PwC Threat Intelligence combina nossas capacidades de detecção com pesquisas focadas em ameaças, bem como esforços proativos para antecipar questões emergentes, criando oportunidades para identificar e conter possíveis lacunas em nosso expertise, enriquecer nosso conhecimento sobre o tema e oferecer inteligência acionável em nossos relatórios. Nossa equipe de Threat Intelligence é composta por membros espalhados por todo o mundo, incluindo Austrália, Alemanha, Brasil, Itália, Países Baixos, Noruega, Suécia, Reino Unido e Estados Unidos. Neste relatório, fornecemos numerosos exemplos que aprimoraram nossa inteligência de ameaças e fundamentaram estratégias cibernéticas resilientes.

[4] Por favor, veja o Apêndice D – Índice de Defesa para um guia rápido com todo o conteúdo de detecção neste relatório.

Conteúdo

Conteúdo de detecção

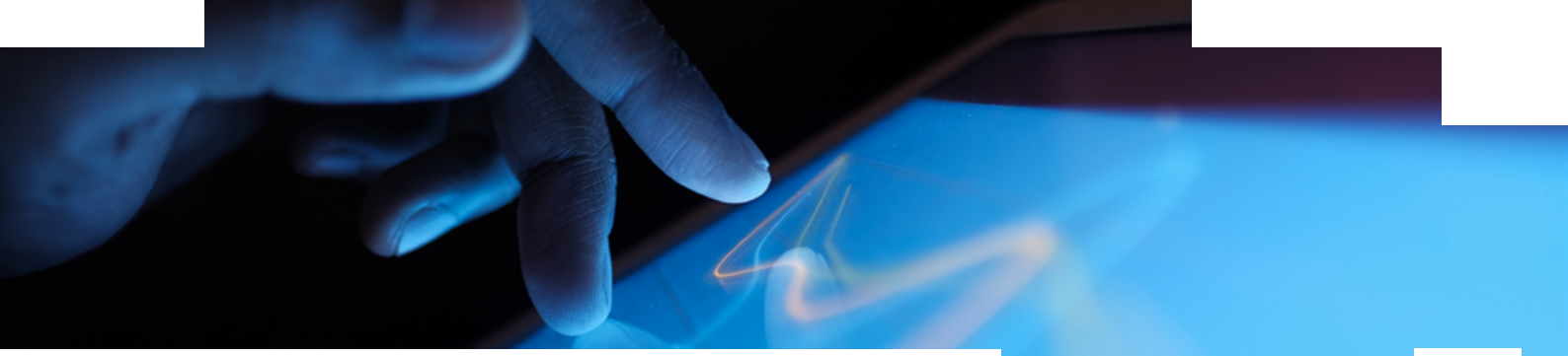
Insights sobre resposta a incidentes

Mais informações à sua disposição

Insights de firmas da PwC

Principais conclusões

Insight sobre ameaças



Principais eventos de 2022

Janeiro

Efeitos da Log4Shell persistem após sua revelação em dezembro de 2021 (pág. 6)

Fevereiro

Começa a invasão russa da Ucrânia (pág. 8)

Março

Vazamentos de conversas internas do grupo Blue Cronus (conhecido como Conti) (pág. 45)

Abril

Surge o White Dev 115 (também conhecido como BlackBasta), vinculado ao Blue Cronus (pág. 46)

Maio

ScanBox mira com iscas temáticas as eleições australianas (pág. 25)

Junho

Red Dev 32 muda do PlugX para o ShadowPad, juntando-se a outros agentes de ameaça (pág. 22)

Julho

Ferramenta de red teaming Brute Ratel ganha tração em fóruns de criminosos cibernéticos (pág. 53)

Agosto

Black Alicanto diversifica suas iscas ao usar programas de instalação de softwares da Microsoft (pág. 32)

Setembro

Notável aumento no número de vítimas de vazamentos de *ransomware* em 2022 (pág. 42)

Outubro

Yellow Dev 32 lança *malware* de celular contra manifestantes no Irã (pág. 29)

Novembro

Diminuição de vazamentos de *ransomware*, em oposição ao mesmo período de anos anteriores (pág. 42)

Dezembro

Blue Callisto faz *phishing* em mais organizações que apoiam a Ucrânia (pág. 15)

O efeito da Log4Shell

Ao se tornar pública em dezembro de 2021, a vulnerabilidade crítica conhecida como Log4Shell (CVE- 2021-44228) – presente em determinadas versões[5] do programa Apache Log4j – provocou um início de ano caótico para empresas no mundo todo.[6] A natureza onipresente do Apache Log4j fez com que entidades do mais diversos setores e países precisassem de uma resposta mais rápida. Tal urgência foi exacerbada ainda mais por uma prova de princípio disponível gratuitamente logo após a vulnerabilidade ter se tornado conhecida, fornecendo instruções de como explorá-la e permitindo qualquer tipo de invasor executar códigos remotamente em um sistema afetado.

Empresas se esforçaram para descobrir instâncias da Log4j em seus ambientes e a Apache trabalhou para desenvolver um patch, enquanto os agentes de ameaça começaram a aproveitar essa oportunidade logo após sua divulgação.[7]

Detectando o uso da Log4Shell

Uma simples e ampla opção para detecção é inspecionar todo o tráfego de entrada aos servidores expostos em busca desta sequência de caracteres ${jndi: ou considerar algumas técnicas comuns de evasão ao procurar por ${ seguido de jndi.

No fim de dezembro de 2021, a Apache lançou diversas atualizações para resolver a Log4Shell. A comunidade internacional de segurança e várias agências governamentais também informaram quais versões do software continham correções, bem como quais programas ainda precisavam de atenção. [8,9] Este esforço coletivo provavelmente fez a diferença para controlar o caos. No entanto, os agentes de ameaça ainda conseguiram explorar a Log4Shell ao longo de 2022, bem como as vulnerabilidades Log4j associadas CVE-2021-45046 e CVE-2021-45105, descobertas assim que as primeiras tentativas de remediação foram realizadas.

---

[5] Nota: Quando descoberta originalmente, a Log4Shell impactou as versões da Apache Log4j 2.0-beta9 e 2.14.1, e lançamentos subsequentes geraram vulnerabilidades adicionais, corrigidas pela versão 2.17.0. Fonte: 'Alert AA21-356A - Mitigating Log4Shell and Other Log4j-Related Vulnerabilities', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa21- 356a (23 de dezembro de 2021)

[6] CTO-QRT-20211210-01A - Varredura ativa do CVE-2021-44228

[7] 'Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation', Microsoft, https://www.microsoft.com/en-us/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/ (11 de dezembro de 2021)

[8] 'Apache Log4j Vulnerability Guidance', CISA, https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance (dezembro de 2021)

[9] 'Alert: Apache Log4j vulnerabilities', NCSC, https://www.ncsc.gov.uk/news/apache-log4j-vulnerability (10 de dezembro de 2021)

[10] 'Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation', Microsoft, https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021- 44228-log4j-2-exploitation/ (11 de dezembro de 2021)

[11] Nota: Documentamos um exemplo em CTO-TIB-20221007-01A - Yellow Nix com um novo truque de acesso, juntamente com scripts PowerShell.

Desde que a Log4Shell veio a público, dezenas de agentes de espionagem e ameaças com motivação financeira exploraram a vulnerabilidade em vários setores.[10] Por exemplo, em 2002, oito meses após a Log4Shell ter se tornado pública, a Yellow Nix (também conhecida como MuddyWater, MERCURY)[11] a explorou no SysAid, produto de suporte e gerenciamento de TI, para acessar empresas em Israel, de acordo com um relatório da Microsoft.[12] Enquanto casos de Log4j não mitigados ainda são explorados, o uso da Log4Shell é provavelmente tão prevalente quanto o de outras vulnerabilidades[13] de 2022, incluindo a `CVE-2022- 41040` e a `CVE-2022-41082`, geralmente conhecidas como ProxyNotShell.[14]

Por mais que várias vulnerabilidades tenham sido descobertas em 2022, foi a Log4Shell que atingiu o pico de criticidade devido à natureza onipresente do programa Apache Log4j, aos desafios de identificação dos sistemas impactados e à persistência dos agentes de ameaça na busca por sistemas vulneráveis e por aqueles que não foram atualizados ou corrigidos. O impacto da Log4Shell provavelmente teria sido muito pior se não fosse pela forte resposta dos defensores e pelos esforços coletivos da comunidade internacional de segurança.

[12] 'MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations', Microsoft, https://www.microsoft.com/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched- systems-to-target-israeli-organizations/ (25 de agosto de 2022)
[13] 'Alert AA22-117A - 2021 Top Routinely Exploited Vulnerabilities', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-117a (27 de abril de 2022)
[14] CTO-QRT-20221003-01A - ProxyNotShell

A invasão da Ucrânia pela Rússia

Em 24 de fevereiro de 2022, a Rússia invadiu a Ucrânia e atacou a infraestrutura do país com ataques aéreos e mísseis[15]. A invasão se deu após meses de uma retórica cada vez mais agressiva por parte do governo russo, além de anos de violação da integridade territorial ucraniana – incluindo a anexação da península da Crimeia pela Rússia em 2014 e a separação efetiva das regiões de Luhansk e Donetsk, autoproclamadas russas e apoiadas por Moscou, no leste da Ucrânia. A invasão também preparou o terreno para movimentações geopolíticas mais amplas ao longo do ano, com novos países a solicitar adesão à Organização do Tratado do Atlântico Norte (OTAN).[16]

A Ucrânia tem sido, na última década, alvo frequente dos agentes de ameaças baseados na Rússia, haja vista, por exemplo, os vários ataques cibernéticos contra a sua rede elétrica em 2015 e 2016.[17] Os ataques do NotPetya do Blue Echidna (também conhecido como Sandworm) foram inicialmente considerados um *ransomware* voltado a um aplicativo ucraniano de gestão financeira. No entanto, o NotPetya se revelou um *wiperware* destrutivo com consequências devastadoras para empresas que usavam o software alvo além das fronteiras do país europeu.

Os ucranianos ficaram sobrecarregados pelas lembranças do NotPetya quando os *wipers* baseados na Rússia começaram a se propagar em janeiro de 2022 e persistiram nos primeiros meses da invasão, ainda que seu impacto tenha sido contido e muito mais limitado do que o esperado devido aos esforços da Ucrânia, de outros governos e de parceiros da indústria de segurança.[18] Os agentes de ameaça baseados na Rússia se concentraram, particularmente, no Ministério da Defesa ucraniano e no PrivatBank, o maior banco comercial do país, nos primeiros dias da guerra.[19] Temeu-se uma grande atividade cibernética fora da zona de conflito, como visto com o NotPetya, mas isso não se aconteceu até o final de 2022.

[15] CTO-SIB-20220224-01A - Tensions escalate into invasion
[16] CTO-SIB-20221102-01A - NATO expansion - Finland and Sweden's changing cyber threat landscape
[17] CTO-SIB-20220127-01A - Russia and Ukraine: on the brink
[18] 'ESET Research jointly presents Industroyer2 at Black Hat USA with Ukrainian government representative', ESET, https://www.eset.com/int/about/newsroom/press-releases/events/eset-research-jointly-presents- industroyer2-at-black-hat-usa-with-ukrainian-government-representativ/ (25 de agosto de 2022)
[19] 'Ukraine defence ministry website, banks, knocked offline', Reuters, https://www.reuters.com/world/europe/ukraine-reports-cyber-attack-defence-ministry-website-banks-tass-2022-02-15/ (15 de fevereiro de 2022)

JANEIRO DE 2022

Rússia prende 14 pessoas associadas com o White Ursia (pág. 16)
Análise do *wiper* WhisperGate, que associamos ao Blue Dev 7 (pág. 12)
Análise das atividades de *phishing* do Blue Otso (pág. 16)
BlueKurama surge como DDOS-for-hire (pág. 19)
Análise de e-mails com ameaças de bomba enviados aos serviços de segurança da Ucrânia (pág. 11)

FEVEREIRO DE 2022

Começa a invasão da Ucrânia pela Rússia (pág. 9)
Ataque à rede de satélites Viasat (pág. 11)
Análise do *wiper* Hermetic (pág. 12)
Cibercriminosos tomam partido ou projetam neutralidade (pág. 16)
Sanções contra a Rússia: instituições financeiras são excluídas do SWIFT (pág. 10)

MARÇO DE 2022

Análise dos *wipers* CaddyWiper e ControlZero (pág. 12-13)
Análise das operações de *phishing* Blue Callisto e Blue Dev 4 (pág. 15-16)
Vazamentos dos chats internos do Blue Cronus (pág. 17, 45)

ABRIL DE 2022

Análise do StarWiper (pág. 13)
Descoberta da variante Industroyer usada junto com o CaddyWiper pelo Blue Echidna e das variantes CaddyWiper executadas pelo Blue Athena (pág. 11)
Análise da infraestrutura do Blue Callisto (pág. 15)

MEADOS DE 2022

Análise do RAT Dark Crystal (pág. 18)
Blue Kurama continua os ataques DDoS (pág. 19)
Blue Kurama é supostamente atacado por Grey Ares (pág. 19)

FIM DE 2022

Blue Kurama continua os ataques DDoS (pág. 19)
Prossegue a atividade de *phishing* do Blue Otso (pág. 16)
Operações do Blue Lelantos permaneceram desativadas (pág. 17)

De modo geral, observamos que os agentes de ameaças baseados na Rússia concentraram suas operações de sabotagem na zona de conflito imediato, com poucas exceções que afetaram entidades fora da Ucrânia. No entanto, ações mais amplas de *phishing* visaram vários países e empresas em todo o mundo e, em alguns casos, usaram como iscas o tema da guerra no país europeu.

Nas seções seguintes, detalhamos eventos e tendências de destaque relacionados aos agentes de ameaça cibernéticas e suas atividades antes e durante a guerra, tais como operações de sabotagem, *phishing* e interseções com agentes e técnicas de ameaça cibernética criminosa.

O impacto das operações dos agentes de ameaça havia sido antecipado, uma vez que várias agências governamentais publicaram avisos de mitigação que se contrapuseram amplamente às principais ferramentas, técnicas e procedimentos (TTPs) de agentes como o Blue Athena (também conhecido como APT28, FANCY BEAR) e o Blue Kitsune (ou APT29, COZY BEAR), bem como forneceram indicadores sobre eles.[20], [21] O setor privado também contribuiu para esses esforços. As empresas Mandiant[22] e Dragos[23], por exemplo, demonstraram um apoio coletivo aos defensores ao expor as capacidades destrutivas direcionadas aos sistemas de tecnologia operacional (OT).

Sanções e respostas do Ocidente

As respostas do Ocidente à invasão da Ucrânia pela Rússia incluíram uma série de sanções e desaprovação do público em geral. Tais medidas resultaram em repercussões econômicas importantes para a Rússia, com várias delas sendo impostas a empresas e até mesmo indivíduos, como o próprio presidente Vladimir Putin e outros políticos e funcionários do alto escalão russo. Imediatamente após o início da invasão, um conjunto de instituições financeiras russas foi excluído da rede SWIFT – o principal sistema de mensagens de pagamento do mundo.[24, 25] Países-membros da União Europeia, Reino Unido, Estados Unidos e outras nações impuseram novas sanções à Rússia com restrições à cadeia global de suprimentos e outras ações, ao passo que várias marcas estrangeiras optaram por pausar ou retirar operações do país por questões éticas e pela preocupação com a opinião pública.[26]

Por alguns setores estratégicos, essas restrições impactaram a habilidade da Rússia de acessar componentes e tecnologias-chave e, desde então, o país começou a procurar alternativas, com substituições e acesso a cadeias de suprimento ilícitas. À medida que o país prolonga a guerra e se torna cada vez mais isolado, avaliamos que os agentes de ameaça de espionagem baseados na Rússia provavelmente mudarão os objetivos para apoiar as suas capacidades de produção doméstica por meio de espionagem econômica, bem como retaliar organizações e países que expressaram solidariedade à Ucrânia.[27]

Na seção Olhando em frente, mais adiante neste relatório, exploramos como estes cenários podem se materializar e suas possíveis consequências para certos setores e países.

[20] 'NCSC advises organisations to act following Russia's attack on Ukraine', NCSC, https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences (18 de março de 2022)
[21] 'Alert AA22-110A - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (20 de abril de 2022)
[22] 'INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems', Mandiant, https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool (13 de abril de 2022)
[23] 'PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems', Dragos, https://hub.dragos.com/whitepaper/chernovite-pipedream (13 de abril de 2022)
[24] 'Joint Statement on Further Restrictive Economic Measures', The White House, https://www.whitehouse.gov/briefing-room/statements- releases/2022/02/26/joint-statement-on-further-restrictive- economic-measures/ (26 de fevereiro de 2022)
[25] CTO-SIB-20220228-01A - Implications of isolation
[26] CTO-SIB-20220825-01A - Sanctions and sectoral impact
[27] CTO-SIB-20220825-01A - Sanctions and sectoral impact

Operações de sabotagem e sobreposições

Operações de sabotagem foram observadas durante a guerra russa na Ucrânia, desde atividades de informação até ações destrutivas destinadas a interromper as comunicações e os sistemas ucranianos. O ataque à rede de satélites Viasat em fevereiro de 2022, atribuído à Rússia e que coincidiu com o início da guerra, é um exemplo notável de agentes de ameaça cibernéticas a apoiar taticamente operações cinéticas (militares) com ações estratégicas de longo prazo.[28, 29, 30, 31]

Pouco antes da invasão, no final de janeiro e início de fevereiro de 2022, analisamos e-mails com ameaças de bomba aos serviços de segurança ucranianos, que vinham provavelmente de agentes de ameaça baseados na Rússia com o intuito de interromper as atividades cotidianas na Ucrânia.[32] Desde o final de fevereiro de 2022, essas operações de informação se ampliaram e passaram a promover narrativas pró-Rússia ou pró-Ucrânia em uma variedade de canais, principalmente nas redes sociais.[33] Desde então, essas operações foram habilitadas por ciberataques e outras atividades on-line coincidiram com um ressurgimento do hacktivismo.

Wipers

Vários agentes de ameaça baseados na Rússia lançaram *malware*s contra entidades ucranianas à medida que a guerra persistia.[34] A partir de nossa análise e de pesquisas publicadas pela indústria de segurança, encontramos exemplos de sobreposições de código e potenciais indicadores de compartilhamento entre diversos agentes de ameaça da Rússia. Por exemplo, pesquisadores identificaram, em abril de 2022, atividades atribuídas a um criminoso que estávamos monitorando chamado Blue Echidna. Elas apontavam para uma variante do *malware* Industroyer que era usada junto com uma amostra do CaddyWiper para atacar uma fornecedora de energia ucraniana[35, 36]. Já pesquisadores da Mandiant indicaram que o agente identificado como Blue Athena executou variantes do CaddyWiper contra organizações do país.[37] Como as prioridades estratégicas do governo russo são ofensivas contra a Ucrânia, o potencial de que esses agentes compartilhem ou cruzem *malware*s e capacidades entre si não é surpreendente, por mais que existam conflitos históricos e competição interna entre serviços de segurança e inteligência.

---

[28] CTO-WTU-20220513-01A - Ukraine Weekly Report
[29] 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union', Conselho Europeu, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber- operations-against-ukraine-declaration-by-the-high- representative-on-behalf-of-the-european-union/ (10 de maio de 2022)
[30] 'Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion', Governo do Reino Unido, https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine- invasion (10 de maio de 2022)
[31] 'Attribution of Russia's Malicious Cyber Activity Against Ukraine', Departamento de Estado dos Estados Unidos, https://www.state.gov/attribution-of-russias- malicious-cyber-activity-against-ukraine/ (10 de maio de 2022)
[32] CTO-QRT-20220224-01A - Wiping and disruption in Ukraine
[33] CTO-WTU-20220311-01A - Ukraine Weekly Report
[34] 'Wipermania: An All You Can Wipe Buffet', Trellix, https://www.trellix.com/en- us/about/newsroom/stories/research/wipermania-an-all-you-can-wipe-buffet.html (15 de novembro de 2022)
[35] 'Industroyer2: Industroyer reloaded', ESET, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer- reloaded/ (12 de abril de 2022)
[36] CTO-WTU-20220414-01A - Ukraine Weekly Report
[37] 'GRU: Rise of the (Telegram) Mini0ns', Mandiant, https://www.mandiant.com/resources/blog/gru-rise-telegram- minions (23 de setembro de 2022)

Com base em nossa visibilidade e coleta, analisamos os seguintes *wipers:*

O wiper WhisperGate

Antes da invasão da Ucrânia, em um relatório de 15 de janeiro de 2022, a Microsoft destacou uma família de *malware* que rastreou como WhisperGate,[38] o qual nós associamos ao Blue Dev 7. Ele combina várias etapas de ataque, consistindo em reescrever o Registro Mestre de Inicialização (MBR, na sigla em inglês) e a corrupção de arquivos.[39] Quando o WhisperGate foi descoberto pela primeira vez, seu comportamento e design sugeriram que se tratava de um *ransomware*. No entanto, ao contrário das motivações financeiras normais, o processo de destruição dele é irreversível. Isso indica uma intenção de sabotagem em vez de apenas extorsão. Além disso, seus principais alvos foram organizações governamentais ucranianas e ao menos uma empresa de tecnologia conhecida por fornecer serviços a esse governo.

O wiper Hermetic

Ao mesmo tempo em que começava a invasão russa, analisamos o *wiper* Hermetic a partir de relatórios públicos. Este *malware* tentou se infiltrar na infraestrutura ucraniana. Se tivesse sido bem-sucedido, teriam limpado as partições das máquinas infectadas, tornando-as inoperáveis. O código solta um arquivo de partição EaseUS para realizar essas atividades, mas também pode apagar arquivos usando a *interface* de programação de aplicativos (API) do Windows.[40]

CaddyWiper

Em março de 2022, pesquisadores da área de segurança descobriram o CaddyWiper rodando em alguns ambientes na Ucrânia.[41] O *wiper* limpava arquivos e eventualmente o disco rígido de todas as unidades mapeadas no sistema afetado, caso ele não fosse o controlador de domínio primário. Avaliamos que o agente de ameaças por trás dele provavelmente manipulou o *rich header* para encobrir sua identificação digital original de desenvolvimento.[42] Outros pesquisadores vincularam o CaddyWiper ao agente de ameaças que identificamos como Blue Echidna, conhecido por manipular *rich headers* de Executável Portátil (PE), por exemplo, no *Olympic Destroyer*.[43]

---

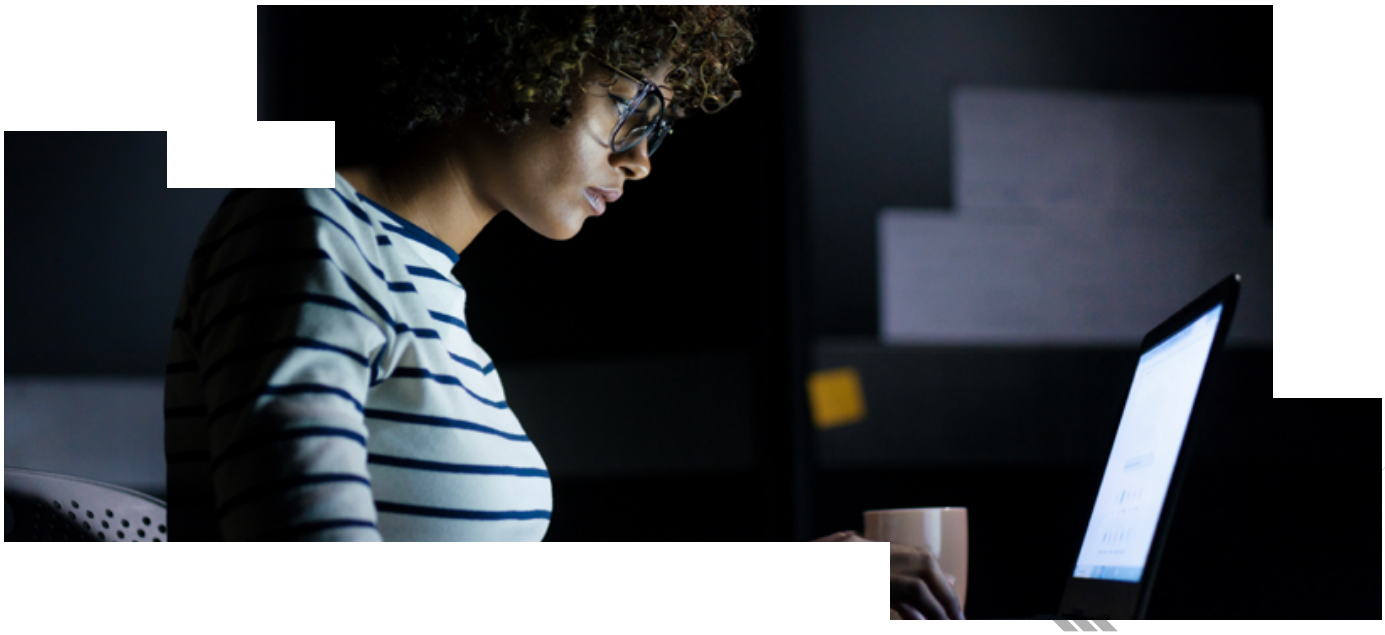
[38] 'Destructive malware targeting Ukrainian organizations', Microsoft, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (15 de janeiro de 2022)
[39] CTO-TIB-20220121-01A - The WhisperGate Wiper
[40] CTO-QRT-20220224-01A - Wiping and disruption in Ukraine
[41] @ESETResearch, Twitter, https://twitter.com/esetresearch/status/1503436420886712321 (14 de março de 2022)
[42] CTO-QRT-20220315-03A - CaddyWiper hits Ukraine
[43] 'The devil's in the rich header', Kaspersky, https://securelist.com/the-devils-in-the-rich-header/84348/ (8 de março de 2018)

O wiper ControlZero

Nomeamos, em março de 2022, um quarto *wiper* como ControlZero (também conhecido como DoubleZero)[44] pelo seu uso da API NtFsControlFile para limpar arquivos. Avaliamos que o *malware* foi provavelmente usado para eventos disruptivos em redes ucranianas. Além disso, ele removeu chaves do registro do sistema afetado, que solicitou uma reinicialização devido à modificação de recursos importantes.[45] Com base em nossas observações, o ControlZero foi o primeiro *wiper* em 2022 a fazer isso para causar interrupções futuras.

StarWiper

Em abril de 2022, analisamos outro *wiper* ao qual nos referimos como Star*Wiper* (também conhecido como ACIDRAIN),[46] que parecia ter como alvos dispositivos móveis em vez de *desktops* devido ao seu microprocessador sem arquitetura de estágios de *pipeline* interligados (MIPS). Fizemos uma correlação deste *wiper* com a invasão da Ucrânia pela Rússia, devido ao uso de um nome de arquivo que referenciava um insulto em língua russa contra ucranianos étnicos. Se o Star*Wiper* fosse realmente do arsenal de *wipers* implantados por agentes de ameaças baseados na Rússia contra o seu país vizinho, ele representaria uma mudança no padrão de *malware*s destrutivos, visando dispositivos móveis em vez daqueles observados anteriormente que visam *desktops*.[47]



[44] 'CERT-UA#4243 - Кібератака на українські підприємства з використанням програми-деструктора DoubleZero', Equipe de Resposta a Emergências Informáticas da Ucrânia (CERT-UA), https://cert.gov.ua/article/38088 (22 de março de 2022)
[45] CTO-QRT-20220222-02A - ControlZero added to the wiper list
[46] 'AcidRain | A Modern Wiper Rains Down on Europe', Sentinel One, https://www.sentinelone.com/labs/acidrain-a- modem-wiper-rains-down-on-europe/ (31 de março de 2022)
[47] CTO-TIB-20220405-01A - StarWiper

Wipers que analisamos (MITRE ATT&CK)

Identificamos cinco *wipers* referentes à invasão russa da Ucrânia – WhisperGate, Hermetic, CaddyWiper, ControlZero e StarWiper –, e mapeamos as táticas (círculo interno) bem como as técnicas (círculo externo) por eles empregadas neste *framework* MITRE ATT&CK.

No círculo abaixo, é possível visualizar nossa cobertura referente à identificação das táticas e técnicas – endereçadas por meio dos relatórios de inteligência e das regras de detecção. Cada cor representa uma tática e sua respectiva técnica. Em cada rótulo, há um número de regras relevantes e/ou nossos relatórios. As cinco técnicas cinza escuro indicam onde não temos uma boa cobertura. Mapear todas as que foram usadas pelas ameaças, e suas visualizações, pode ajudar os defensores a identificar lacunas e fraquezas. Isso pode ser usado junto com a avaliação de risco da organização para priorizar o *backlog* de detecção.

Operações de *phishing*

Agentes de ameaças baseados na Rússia usaram várias operações de *phishing* para atacar organizações e outras entidades ucranianas antes e durante a guerra. Embora essas atividades tenham se concentrado em alvos do governo e militares da Ucrânia, ficou claro que eles também miraram algo mais amplo em suas operações, com algumas se tornando públicas. Esses agentes baseados na Rússia responderam rapidamente a essas divulgações, demonstrando sua capacidade de se adaptar e sustentar operações eficazes, apesar de organizações de segurança comerciais e governamentais estarem ativamente em seu encalço. Em março de 2022, um dia após a divulgação do Google TAG[48] sobre a infraestrutura associada ao agente de ameaças que nós identificamos como o Blue Athena, ele criou domínios de *phishing*, reutilizando códigos copiados de sites anteriores.[49]

Outro exemplo de *phishing* de um agente de ameaças baseado na Rússia, o Blue Callisto (também conhecido como Callisto Group) atacou uma empresa de correio e logística ucraniana, que estava ajudando seu país para além das operações comerciais. Ele também pôs em andamento campanhas de coleta de credenciais contra organizações da Europa e dos Estados Unidos, destacando seu portfólio operacional dinâmico provavelmente a pedido de Moscou.[50] Já em dezembro de 2022, identificamos evidências de que o Blue Callisto mirou seus ataques a organizações que apoiam a Ucrânia, desde aquelas que fornecem ajuda humanitária ao país até as que investigam as ações da Rússia.[51]

Rastreando a infraestrutura do Blue Callisto

Em abril de 2022, analisamos os domínios do Blue Callisto (ou Callisto Group) e descobrimos um padrão comum de infraestrutura, o que, mais tarde, revelou uma extensa infraestrutura de rede. Em nossa avaliação, esse agente de ameaças estava provavelmente a utilizando para conduzir uma campanha de *phishing* com o tema da guerra na Ucrânia.[52] Já em setembro daquele ano, identificamos outras técnicas de rastreamento para o Blue Callisto e seu interesse em laboratórios dos Estados Unidos.[53]

Leia mais sobre o Blue Callisto em um dos nossos posts no blog de 2022

Em nossa análise sobre o Blue Dev 4 (também conhecido como Ghostwriter, UNC1151), encontramos um documento do Word possivelmente associado a ele, já que o nome do arquivo fazia uma referência a Ghostwriter. Além disso, ele continha uma lista de nomes e e-mails de pessoas e organizações ligadas ao exército ucraniano. Avaliamos então que ela provavelmente continha alvos de interesse do Blue Dev 4, por exemplo, o dono de um site de uma loja de uniformes, equipamentos e acessórios militares ucranianos; a Unidade Militar A1965, a saber, as forças navais ucranianas que estão na região de Zaporizhzhia; diversos pesquisadores ligados a institutos de defesa da Ucrânia; e um reservista ucraniano que mora na região de Vinnytsia.[54] O ataque que creditamos ao Blue Dev 4 revelou uma combinação de abordagens, desde ações amplas e oportunistas com várias vítimas até esforços persistentes para comprometer alvos de interesse específicos.

[48] 'An update on the threat landscape', Google TAG, https://blog.google/threat-analysis-group/update-threat- landscape-ukraine/ (7 de março de 2022)
[49] CTO-TIB-20220411-01A - Blue Athena 2022 phishing part 2
[50] CTO-SIB-20220908-01A - Ukraine Threat Update - agosto de 2022
[51] CTO-SRT-20221213-01A - Blue Callisto targets Ukraine-linked organisations
[52] CTO-TIB-20220511-01A - Tracking Callisto infrastructure
[53] CTO-TIB-20220913-02A - Blue Callisto still phishing
[54] CTO-QRT-20220303-01A - Blue Dev 4 phishing operations in 2022

Estudamos também as atividades de *phishing* do Blue Otso (também conhecido como Gamaredon Group), verificadas em janeiro de 2022. À medida que aumentavam as tensões entre Rússia e Ucrânia antes da invasão, o Blue Otso usou iscas temáticas da cidade de Sievierodonetsk e da região da Crimeia em documentos usados como armas nas operações de *spear-phishing,* levando a arquivos auto-extraíveis e binários UltraVNC. Tanto Sievierodonetsk quanto a Crimeia têm forte significado geopolítico. A primeira é uma cidade estrategicamente localizada em Luhansk, mas fora do território separatista apoiado pela Rússia, conhecido como LPR (*Luhansk People's Republic*). Já a segunda região está sob anexação desde 2014.[55] No final de 2022, o Blue Otso voltou a registrar domínios usando um email que atribuímos a ele pela primeira vez em 2020. Eles eram relacionados ao tema do Serviço Especial de Comunicações do Estado da Ucrânia. No entanto, estavam em um formato diferente do que se viu anteriormente. Em 2022, o Blue Otso registrou domínios provavelmente por meio de um processo automatizado, usando listas de palavras sem tema específico.[56] Também é provável que ele tenha mantido, separadamente, *clusters* de atividade controlados manualmente, além dos automatizados. A sua gestão de infraestrutura se diversificou em 2022 e se tornou mais dinâmica do que nos anos anteriores, e seus domínios C2 (comando e controle) mudaram diariamente para se traduzir em novos endereços IP.

Unindo-se para se proteger do crime cibernético

A guerra na Ucrânia colocou sob nova perspectiva os criminosos cibernéticos do Leste Europeu, sobre como eles responderiam à guerra e especialmente a quem eles seriam leais. Antes da invasão, em meados de janeiro de 2022, o governo russo anunciou a prisão de 14 pessoas que supostamente estariam associadas ao White Ursia – o agente da ameaça à frente do *ransomware* conhecido como REvil ou Sodinokibi. Isso fez com que alguns criminosos reconsiderassem seus alvos, à medida que um dos presos também foi considerado responsável pelo ataque *ransomware* de maio de 2021 contra a empresa Colonial Pipeline, dos EUA, o qual tinha sido atribuído ao White Apep (também conhecido como Darkside e BlackMatter).[57] Após a ofensiva da Rússia contra seu país vizinho, em fevereiro de 2022, os criminosos ficaram mais preocupados com sanções que pudessem afetar sua capacidade de extorquir, lavar e sacar fundos de atividades ilícitas[58]. Porém, de modo geral, o crime prosseguiu normalmente.

[55] CTO-TIB-20220203-01A - Blue Otso retains Ukraine interest
[56] 'ACTNIUM targets Ukrainian organizations', Microsoft, https://www.microsoft.com/en- us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/ (4th February 2022) 57 CTO-SIB-20220211-01A - White Ursia, from Unknown to under the bus
[57] CTO-SIB-20220211-01A - White Ursia, from Unknown to under the bus
[58] CTO-SIB-20220915-02A - Tales from the crypto

Sanções que efetivamente restringem organizações criminosas de alto perfil

Em 2021, o Blue Lelantos (também conhecido como Evil Corp) – agente de ameaças responsável pelo *trojan* bancário Dridex e pelos sistemas de *ransomware* BitPaymer, DoppelPaymer, Grief e Wasted Locker – realizou diversas tentativas de fazer um *rebranding* em suas operações. Isso depois de ter sido colocado na lista negra (*blacklisted*) de seguradoras e negociadores especializados nesse tipo de software em resposta a ações aplicadas pelos EUA. Com a necessidade de mudanças radicais em suas operações em 2022, concluímos, a partir das seguintes observações, que o esforço de *rebranding* falhou:

- Outrora um pilar do arsenal da Evil Corp, a atividade do Dridex diminuiu.
- Não observamos novas ações de *rebranding* em variantes de *ransomware* do Blue Lelantos em 2022.
- Outros pesquisadores da área de segurança relataram esforços por parte de elementos do Blue Lelantos para se inscreverem em esquemas rivais de *ransomware*.[59]

Ainda que tenha sido um notório grupo dedicado ao crime cibernético, o encerramento das operações do Blue Lelantos em 2022 demonstrou que, ao menos neste caso, sanções e remoções[60] são ferramentas efetivas para interromper de forma significativa esses crimes.

Em fevereiro de 2022, o *ransomware* Conti, operado pelo Blue Cronus, declarou seu apoio à invasão da Ucrânia e ameaçou, por meio de textos postados diretamente em um site vazado, que iria atacar infraestruturas críticas de países que se voltassem contra a Rússia. Já outros agentes de ameaça, como o White Janus (também conhecido como LockBit) e o White Dev101 (também chamado de ALPHV-ng e BlackCat), enfatizaram que suas motivações eram puramente financeiras e expressaram neutralidade em relação à guerra.[61] Independentemente de suas posições ideológicas, nossa análise revela que agentes baseados na Rússia de *ransomware* provavelmente estão em posição de serem cooptados ou coagidos por Moscou a conduzir operações em apoio ao país.

[59] 'To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions', Mandiant, https://www.mandiant.com/resources/blog/unc2165-shifts-to-evade-sanctions (junho de 2022)
[60] 'Ameaças Cibernéticas: 2021 em Retrospectiva', PwC Threat Intelligence https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/Retrospectiva-Cyber-22.pdf (julho de 2022)

Atividade do *Trojan* de Acesso Remoto (RAT) Dark Crystal na Ucrânia

Desde a invasão da Ucrânia, vários agentes de ameaça motivados por dinheiro e espionagem têm explorado a questão da guerra para atingir as vítimas. Um ataque em particular resultou na execução do Dark Crystal RAT, um *trojan* de acesso remoto (RAT), normalmente observado em operações motivadas por interesses financeiros. Avaliamos que um arquivo Excel malicioso associado a esse ataque – que continha macros e informações referentes ao Serviço de Emergência do Estado da Ucrânia – foi provavelmente usado para atingir uma entidade ligada ao governo de Kiev[62]. O agente que implantou o Dark Crystal RAT mais tarde retornou com outra isca com tema da Ucrânia relacionada a colaboradores baseados na Rússia, que foi usada como arma para executar o WarZone RAT, outra variante de *malware* frequentemente associada a motivações financeiras.

Detectando o *Dark Crystal RAT*

Identificadores de Recursos Universais (URIs, na sigla em inglês)

```
\.php\?type= ds_setdata& ds_setdata_user=[a-f0-9]{40}&
ds_setdata_ext=[a-f0- 9]{32}& ds_setdata_data=

\.php\?type= ds_getdata& ds_getdata_user=[a-f0-9]{40}&
ds_getdata_ext=[a-f0- 9]{32}& ds_getdata_key=[a-f0-9]
{32}$
```

COMSurrogate

O Dark Crystal RAT inicia a tarefa COMSurrogate quando o usuário faz login com privilégios elevados
(MITRE ATT&CK T1053.005 - Scheduled Task/Job: Scheduled Task).[63]

Também executa um comando powershell codificado em b64, que aciona as seguintes detecções
(MITRE ATT&CK T1140 - Deobfuscate/Decode Files or Information e T1059.001 - Command and Scripting Interpreter: PowerShell):

```
[0934]-[evasion]-[m]-powershell_executing_base64_
encoded_commands [0942]-[execution]-[m]-powershell_with_
abbreviated_noprofile_switch
[0931]-[execution]-[m]-powershell_with_abbreviated_
executionpolicy_bypass_switch
```

[62] CTO-TIB-20220616-01A - Opaque Dark Crystal RAT activity in Ukraine
[63] CTO-TIB-20220616-01A - Opaque Dark Crystal RAT activity in Ukraine

À medida que os criminosos motivados financeiramente evitavam ou mergulhavam em narrativas sobre a guerra, vinham à tona outros interlocutores e agentes inspirados no hacktivismo – o que adicionava ainda mais complexidade às operações pró-Rússia ou pró-Ucrânia. Um exemplo é o surgimento de contas hacktivistas autodeclaradas pró-Ucrânia, que se ligavam ao coletivo Anonymous. Estes foram casos que rastreamos como Grey Ares, IT Army of Ukraine[64] e Network Battalion[65] (também conhecido como NB65).[65] O Killnet, coletivo hacktivista pró-Rússia que rastreamos como Blue Kurama[66], ganhou notoriedade por seus múltiplos ataques DDoS (negação distribuída de serviço) contra infraestruturas críticas da Lituânia[67], importantes instituições públicas e privadas da Noruega[67], sites do Parlamento da Letônia e de órgãos públicos da Estônia[68]. Foram notáveis as operações do Blue Kurama em 2022, pois seus alvos abrangeram organizações públicas e privadas críticas de ações da Rússia[69], localizadas fora da zona de conflito imediato. No entanto, descobrimos que a eficácia das campanhas do Blue Kurama, embora amplamente divulgadas, era geralmente de baixa em comparação com outros tipos de ataques cibernéticos.[69]

O alarde do Blue Kurama

O Blue Kurama (também conhecido como Killnet) é apenas um exemplo dos grupos de *hackers* patrióticos, que surgiram durante a guerra e demonstraram apoio tanto a interesses pró-Rússia quanto pró-Ucrânia. No caso do Blue Kurama, em particular, seu alinhamento era de apoio aos russos.[70] Esse agente de ameaças se envolveu principalmente em ataques DDoS contra alvos ucranianos e organizações públicas e privadas, com destaque para aquelas ligadas a infraestruturas críticas e de defesa, de países cujas ações eram tidas como contrárias aos interesses de Moscou (por exemplo, Romênia,[71] Itália,[72] Lituânia, Noruega[73] e Estados Unidos[74]). O grupo se formou inicialmente, em janeiro de 2022, como uma capacidade de DDoS-*for-hire* e foi fundado por uma pessoa que tinha o apelido on-line de `Killmilk`, que afirmava ser um cidadão da Rússia baseado naquele mesmo país. À medida que o Blue Kurama mudou seu modelo *for-hire* para a realização de ataques, ele passou a facilitar suas operações e seus recrutamentos principalmente nos canais de Telegram de língua russa. Em vários fóruns públicos, foi relatado que ele realizou ataques DDoS usando *botnets* Mirai em 2022. Porém, em maio daquele ano, foi a sua vez de se ver no lado receptor de supostos ataques lançados pelo Grey Ares (também conhecido como Anonymous).[75]

Os ataques do Blue Kurama, ainda que bem-sucedidos, foram em sua maioria de curta duração e não resultaram em um impacto significativo ou sustentado. No entanto, a natureza potencialmente disruptiva e destrutiva deles serve como alerta para uma tendência de proliferação no hacktivismo, à medida que a guerra continue ou que outros conflitos surjam.

---

[64] CTO-SIB-20220301-01A - Cyber criminal and hacktivist response
[65] CTO-SIB-202220707-01A - Ukraine Threat Update – junho de 2022
[66] CTO-TIB-20221208-02A - Not cool Killnet
[67] CTO-SIB-202220707-01A - Ukraine Threat Update – junho de 2022
[68] CTO-SIB-20220908-01A - Ukraine Threat Update – agosto de 2022
[69] CTO-TIB-20221208-02A - Not cool Killnet
[70] CTO-TIB-20221208-02A - Not cool Killnet
[71] CTO-WTU-20220505-01A - Ukraine Weekly Report
[72] CTO-WTU-20220513-01A - Ukraine Weekly Report
[73] CTO-SIB-20220707-01A - Ukraine Threat Update – junho de 2022
[74] CTO-SIB-20220804-01A - Ukraine Threat Update – julho de 2022
[75] CTO-WTU-20220526-01A - Ukraine Weekly Report

Agentes baseados na China otimizam suas operações

Ao longo do ano, os agentes de ameaça continuaram a se unir em torno de redes, infraestruturas e capacidades compartilhadas. Como resultado, as operações se tornaram, com frequência, mais simplificadas, abrangentes e tecnicamente sofisticadas do que as observadas anteriormente. Se, por um lado, essa é uma tendência que temos analisado há anos; [76, 77] houve em 2022, por outro lado, um aumento expressivo do compartilhamento de *exploits* e ferramentas, incluindo redes *proxy* de ofuscação como serviço. Nossa avaliação dos padrões de alvo desses agentes apontou ainda operações de segmentação específicas por país, bem como um foco contínuo na cadeia de suprimentos digital e em acordos de alta tecnologia, principalmente em organizações do setor de telecomunicações.

Ainda que os alvos não sejam novos, agentes de ameaça baseados na China estão otimizando cada vez mais suas operações e alavancando recursos *proxy* compartilhados, além de desafiar métodos convencionais de atribuição, de resposta a incidentes e de avaliação de danos.

Além disso, desde o final de 2021, identificamos inúmeros casos envolvendo múltiplos agentes de ameaça tentando ofuscar cargas úteis de implante, provavelmente empregados para evitar detecção e frustrar análises. Destacadamente, o Red Lich (também conhecido como Mustang Panda, Temp.Hex ou TA416) usou ofuscação baseada em LLVM, tanto em seu carregador quanto na carga útil interna do PlugX, em campanhas que miravam entidades na Europa. Embora o uso do LLVM e dessas técnicas não seja algo exatamente novo, isso só havia sido aplicado antes em componentes do carregador e não na própria carga útil.

A evolução dessas estratégias traz desafios adicionais para as tentativas de identificar e fazer engenharia reversa em cenários de ameaças novas e desconhecidas que, de outra forma, seriam detectáveis por meio de assinaturas YARA ou revisão manual usando ferramentas estáticas e dinâmicas. Ao adicionar essa camada extra de proteção em ferramentas personalizadas e sob medida, os agentes que realizam os ataques aumentam a longevidade de suas campanhas mesmo em face das melhorias no lado defensivo.

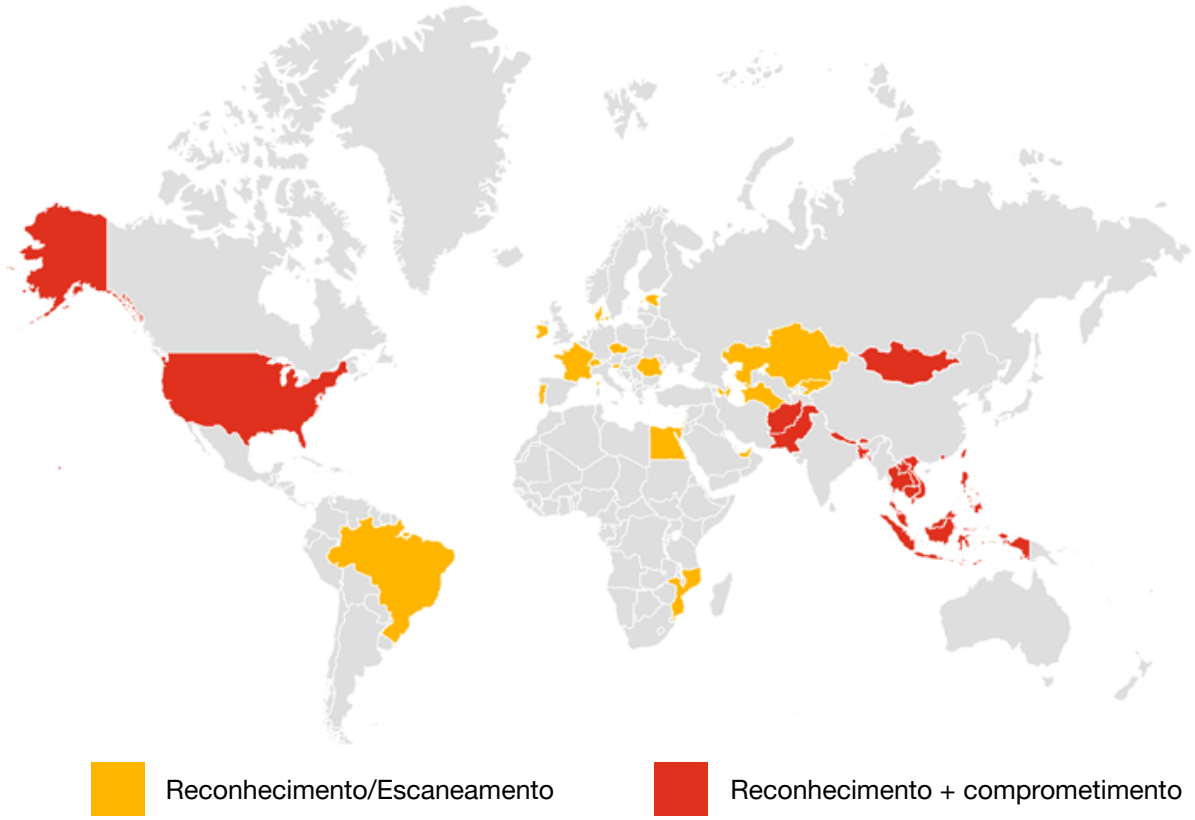
Esperamos que essa tendência de ofuscação e proteção de cargas úteis persista e se aprimore no nível operacional – com agentes de ameaça empregando ofuscação em implantes personalizados, bem como no nível do desenvolvedor – e no qual o *malware* fornecido é prontamente embalado ou ofuscado por um quartel-mestre.

[76] 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence, https://www.pwc.co.uk/cyber- security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf (17 de dezembro de 2020)
[77] 'Ameaças Cibernéticas: 2021 em Retrospectiva', PwC Threat Intelligence https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/Retrospectiva-Cyber-22.pdf (julho de 2022)

Red Scylla, uma ameaça global ligada ao Winnti

Em agosto de 2022, atribuímos ao Red Scylla (também conhecido como CHROMIUM, ControlX, Earth Lusca e Aquatic Panda) a atividade anteriormente rastreada como Red Dev 10,[78] em grande parte devido ao fato de termos identificado um conjunto distinto de infraestrutura e técnicas.[79] Sem dúvida, o Red Scylla foi o agente de ameaças chinês mais proeminente e prolífico em 2022. Já que ele tem o mundo todo como alvo, é sofisticado e tem um ritmo operacional otimizado, é considerado como o mais ativo agente de ameaças da China.

Ataques do Red Scylla em 2022



Pudemos observar o Red Scylla procurando vulnerabilidades, usando a ferramenta de código aberto Acunetix[80] e implantando um amplo conjunto de ferramentas pós-comprometimento que incluíam tanto *backdoors* personalizados quanto ferramentas comumente compartilhadas entre esses agentes de ameaça, tais como o ShadowPad e o PlugX. Desde 2021, temos encontrado o Red Scylla como um usuário do ShadowPad[81], principalmente por meio de um método de ofuscação personalizado que apelidamos de ScatterBee[82], que usa um fluxo de controle, *guardrails* de execução e patching em tempo de execução para obstruir a análise forense. O Red Scylla se voltou a organizações globais de vários setores, tendo avançado rapidamente das atividades de reconhecimento para obter acesso às redes das vítimas e implantar *malware* no início das invasões em uma tentativa de ampliar sua presença nos ambientes afetados.

[78] Veja o Apêndice B – Threat actor reference for more information about our naming convention.
[79] CTO-TIB-20220825-01A - Red Scylla: A Winnti-Linked Global Threat
[80] CTO-TIB-20220621-01A - Red Dev 10 - Acunetix Scanning
[81] 'Chasing Shadows: A deep dive into the latest obfuscation methods being used by ShadowPad', PwC Threat Intelligence, https://www.pwc.co.uk/issues/cyber-security-services/research/chasing-shadows.html (8 de dezembro de 2021)
[82] CTO-TIB-20211021-01A - Chasing shadows

O Red Scylla não foi o único a implantar ShadowPad no último ano já que, durante 2022, ele foi usado por agentes de ameaça que já tínhamos associado a essa família de *malware*, bem como por *clusters* de atividade recém-identificados. Durante o rastreamento da infraestrutura C2 do ShadowPad, encontramos um novo *cluster* baseado na gestão associada, que rastreamos como Red Dev 32.[83] Acreditamos que esse agente provavelmente mudou do PlugX para o ShadowPad em junho, administrando a infraestrutura que oferecia certificados SSL falsos da Microsoft. Mais tarde, em 2022, identificamos evidências de sobreposição entre o Red Dev 32 e o Red Scylla, com caixas de retransmissão operacional (ORBs) do segundo sendo usadas para testar atividades com um C2 ShadowPad do primeiro. Em nossa avaliação, é altamente provável que esses dois agentes de ameaça compartilhem algum tipo de relacionamento organizacional. Em outubro de 2022, vinculamos ainda mais a infraestrutura ShadowPad ao Red Dev 14, em que vários hosts C2 ShadowPad estavam oferecendo um certificado autoassinado roubado que, originalmente, pertencia a uma entidade governamental do Oriente Médio.[84]

Defendendo-se das semelhanças TTP

Dadas as semelhanças de TTP entre os agentes de ameaça baseados na China, um bom conselho aos defensores seria monitorar arquivos LNK com alvos e linhas de comando suplementares (MITRE ATT&CK T1204.002 - User Execution: Malicious File). Além disso, embora as aplicações sequestradas variem, o carregamento lateral de bibliotecas de links dinâmicos (T1574.002 - Hijack Execution Flow: DLL Side-Loading) continua a ser uma técnica consistente nas cadeias de infecção desses agentes.

RedRelay, uma rede *proxy* compartilhada

Ao longo do ano, continuamos a pesquisar uma rede *proxy* usada por diversos agentes de ameaça, que tínhamos identificado um ano antes e a qual nos referimos como RedRelay. Eles tinham começado a se mover para redes *proxy* compartilhadas nos últimos anos. Avaliamos que essas redes supostamente secretas são provavelmente operadas em um arranjo de quartel-mestre, por meio do qual ferramentas são provisionadas, vendidas e compartilhadas por uma entidade pública ou privada. As características da rede *proxy* – como o *proxy multihop* e a facilitação da comunicação via canais criptografados – desafiam os métodos tradicionais de pesquisa para análise e atribuição. Tais redes são também construídas por meio da combinação de centenas de servidores privados virtuais (VPNs, na sigla em inglês) operados por agentes com dispositivos comprometidos.

Avaliamos, por exemplo, a utilização do RedRelay pelo Red Vulture (também conhecido como APT15, APT25 e Ke3chang). Este último usou um *cluster* específico da infraestrutura do RedRelay ao longo de 2021 e no início do ano seguinte. Então, em março de 2022, ele o desativou e reconstruiu antes de retomar suas atividades de reconhecimento e exploração contra governos europeus, instituições pan-europeias e organizações internacionais. Essa mudança evidenciou as medidas proativas de segurança operacional (OPSEC) do Red Vulture e espelhou mudanças mais amplas nos métodos de gerenciamento da infraestrutura RedRelay, que observamos em fevereiro de 2022.[85]

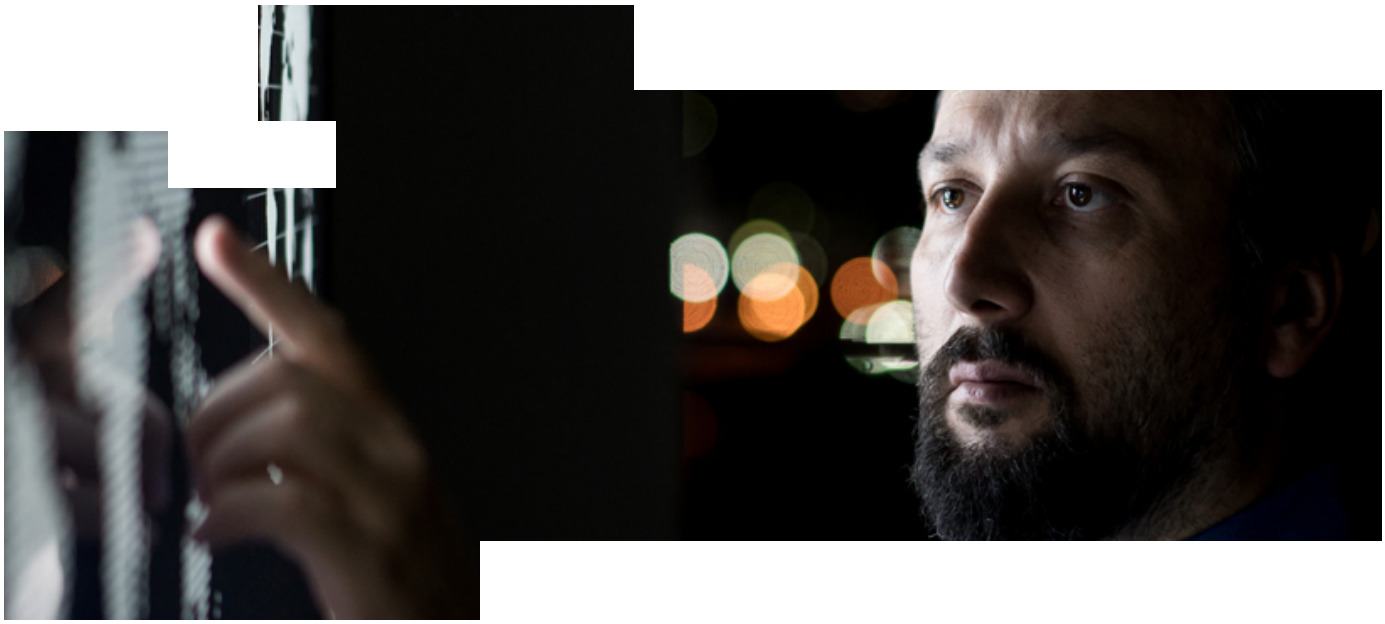
[83] CTO-TIB-20220913-01A - Red Dev 32
[84] CTO-TIB-20221005-01A - Not to worry; I have a certificate of authority
[85] CTO-TIB-20220523-02A - Rampant Reconnaissance Redux

Avaliamos, por exemplo, a utilização do RedRelay pelo Red Vulture (também conhecido como APT15, APT25 e Ke3chang). Este último usou um *cluster* específico da infraestrutura do RedRelay ao longo de 2021 e no início do ano seguinte. Então, em março de 2022, ele o desativou e reconstruiu esse *cluster* antes de retomar suas atividades de reconhecimento e exploração contra governos europeus, instituições pan-europeias e organizações internacionais. Essa mudança evidenciou as medidas proativas de segurança operacional (OPSEC) do Red Vulture e espelhou mudanças mais amplas nos métodos de gerenciamento da infraestrutura RedRelay, que observamos em fevereiro de 2022.[85]

Ataques a países específicos

Em janeiro de 2022, analisamos a comunicação de *malware* com domínios do tipo C2, o qual atribuímos ao Red Orthrus (também conhecido como Keyboy, TA428 e Tropic Trooper). Destacamos que essa variante, em particular, era uma versão 64 bits do RAT, conhecido em código aberto como nccTrojan.[86] As iscas temáticas dos domínios C2, presentes nessas amostras, pareciam imitar organizações dentro dos setores de defesa e manufatura russos. Adicionalmente, mudanças na infraestrutura conhecida por abrigar domínios de nccTrojan evidenciaram novos cruzamentos entre domínios temáticos russos e a infraestrutura do Red Orthrus. Em algum momento, todos eles estavam hospedados em um endereço IP da Rússia e avaliamos que o agente da ameaça provavelmente fez isso intencionalmente para fazer com que o tráfego C2 parecesse inócuo para o alvo.[87] Essas atividades provavelmente indicavam coleta de inteligência à medida que as forças russas se mobilizavam antes da invasão à Ucrânia.

O Red Phoenix (também chamado de APT27, Emissary Panda e LuckyMouse) seguiu como um ameaça ativa e sempre presente no decorrer de 2022. Em janeiro, o Escritório Federal para a Proteção da Constituição da Alemanha (BfV, na sigla em alemão) postou em seu blog[88] detalhes técnicos sobre as operações deste agente de ameaças, evidenciando ainda que o Red Phoenix tinha se voltado contra empresas alemãs. Ao rastrear a infraestrutura e os *malware*s associados às famílias antigas e personalizadas HyperBro e FOCUSFJORD[89] atribuídas ao Red Phoenix, descobrimos que a imensa maioria das operações em 2022 tinham mirado organizações da região do Mar da China Meridional.



[86] 'China-linked TA428 Continues to Target Russia and Mongolia IT Companies', Recorded Future, https://www.recordedfuture.com/china-linked-ta428-threat-group (17 de março de 2021)
[87] CTO-QRT-20220315-01A - Red Orthrus targets Russia
[88] 'Cyber attack campaign against German commercial companies', BfV, https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2022/2022-01-26-cyberbrief.html (26 de janeiro de 2022)
[89] 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence, https://www.pwc.co.uk/cyber- security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf (17 de dezembro de 2020)

Red Phoenix no centro das atenções

HyperBro
Há muito tempo, o *backdoor* HyperBro é associado ao Red Phoenix (também conhecido como APT27, Emissary Panda e LuckyMouse). Esse agente de ameaças usa binários legítimos para fazer um *side-load* de DLLs maliciosos e, assim, instalar o HyperBro nas máquinas das vítimas – técnica empregada pelo Red Phoenix desde 2015. Um indicador do *malware* HyperBro é a presença de um certificado assinado da Cheetah Mobile Inc. – uma empresa chinesa de internet móvel. Além de obter uma resposta consistente, a infraestrutura C2 também invariavelmente hospeda um certificado SSL com a hash SHA-1 `44b9d089cf734d2478165a8539b23aed51887f7d` na porta 443. Dados históricos de varredura on-line sugerem que servidores HyperBro ativos compartilharam essas características desde pelo menos junho de 2019.[90]

FOCUSFJORD
Foram identificadas novas amostras FOCUSFJORD em 2022 que continham o esperado código exclusivo de ofuscação Shikata Ga Nai, em que os *timestamps* remontam a junho. Todos os domínios C2 associados a essas amostras recentes seguiram a tendência de conter o domínio superior (TLD) `.me`.

Outras ferramentas

Além de tudo isso, relatórios em código aberto em agosto de 2022 detalharam como o MiMi – um aplicativo chinês de mensagens instantâneas – foi usado para recuperar variantes ELF e Mac do backdoor rshell junto com links para o Red Phoenix.[91] Desde então, identificamos novas amostras do *malware* rshell. Avaliamos, assim, que em alguns casos o Red Phoenix provavelmente gerenciou a infraestrutura associada com base nas sobreposições com a C2 HyperBro[92.] Também encontramos um servidor C2 HyperBro hospedando simultaneamente um certificado Cobalt Strike, enquanto outro hospedava o Fast Reverse Proxy (FRP).[93]

Ainda em janeiro de 2002, começamos a rastrear uma significativa mudança de *targeting* em uma campanha que avaliamos ser muito provavelmente do Red Lich (também chamado de Mustang Panda, Temp.Hex e TA416), que particularmente tinha como alvos entidades governamentais e diplomáticas europeias, ao passo que, desde 2020, o Red Lich focava em um campo bem mais amplo de atuação – desde organizações não-governamentais (ONGs) até entidades de governo no Sul e Leste da Ásia, além de outros alvos espalhados pelo mundo. Na primeira fase da campanha europeia, desde pelo menos janeiro de 2022 até o final de março, o Red Lich usou arquivos RAR ou ZIP, cujos títulos usavam temas relevantes de assuntos europeus, de países específicos da Europa Central e da guerra russa na Ucrânia.

[90] CTO-TIB-20221102-01A - Rising from the hashes
[91] 'LuckyMouse uses a backdoored Electron app to target MacOS', Sekoia, https://blog.sekoia.io/luckymouse-uses-a-backdoored-electron-app-to-target-macos/ (12th August 2022)
[92] CTO-TIB-20221102-01A - Rising from the hashes
[93] CTO-TIB-20221102-01A - Rising from the hashes

Esses arquivos continham um executável legítimo que baixaria um documento falso para ser mostrado à vítima e um carregador Trident para PlugX, um executável benigno, para um DLL malicioso a ser carregado lateralmente, além de uma amostra PlugX codificada em um recurso DAT.[94] Entre o final de março e outubro de 2022, o Red Lich atualizou suas TTPs no contexto do seu *targeting* a entidades europeias, provavelmente numa tentativa de evitar a detecção e possivelmente em resposta à divulgação pública da campanha.[95] O agente de ameaças passou a usar arquivos compactados com arquivos LNK maliciosos que fariam o carregador Trident executar o PlugX nas máquinas das vítimas. Na segunda fase dessa campanha, o Red Lich adicionou novas medidas de ofuscação e anti-análise ao seu *malware* – incluindo o nivelamento do fluxo de controle LLVM. Ao longo dela, o Red Lich se voltou principalmente a entidades governamentais do leste e centro da Europa envolvidas em assuntos externos, bem como embaixadas e entidades supranacionais sediadas na Bélgica.

Em mais um exemplo da capacidade compartilhada entre os agentes de ameaças, que é usada em operações de alto perfil, analisamos, com a empresa Proofpoint[96], uma campanha de espionagem do ScanBox que ocorreu de abril a junho de 2022. O ScanBox é um *framework* de reconhecimento e exploração da web compartilhado unicamente entre agentes baseados na China, que tem sido usado esporadicamente desde pelo menos 2014. A campanha de 2022 teve alcance internacional, mas com foco em organizações da região da Ásia-Pacífico, entidades governamentais e de mídia australianas, além de empresas e países com ações na região do Mar da China Meridional, incluindo fabricantes globais de indústrias pesadas. Atribuímos essa campanha em particular ao Red Ladon (também conhecido como TA423, APT40 e Leviathan). Ele, que já havia usado o ScanBox em 2018, criou iscas em torno de eleições nacionais, tanto nas campanhas daquele ano quanto nas de 2022, e colocou no ar sites de notícias maliciosos para atrair alvos. Na campanha de 2022, o Red Ladon transpôs literalmente manchetes acerca da eleição australiana de maio de um veículo jornalístico do Reino Unido para um site controlado pelo Red Ladon, que se passava por um veículo de mídia australiano.[97]

Saiba mais sobre o Red Dev 26 em nossa conversa do Virus Bulletin 2022

[94] CTO-QRT-20220302-01A - Red Lich eyes Europe
[95] 'Mustang Panda's Hodur: Old tricks, new Korplug variant', ESET, https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/ (23 de março de 2022)
[96] 'Rising Tide: Chasing the Currents of Espionage in the South China Sea', Proofpoint, https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea (30 de agosto de 2022)
[97] CTO-TIB-20220829-01A - Rising Tide

Foco persistente nas telecomunicações

Embora tenhamos identificado casos de agentes de ameaças visando provedores de telecomunicações por vários anos, nossa pesquisa revelou que o foco contra este setor em 2022 foram os esforços de otimização.[98]

As implicações das invasões em provedores de telecomunicações não podem ser exageradas: essas atividades prejudicam comunicações seguras entre países, empresas e governos e ameaçam normas diplomáticas, sociais e comerciais em todo o mundo.

Em agosto de 2022, atribuímos o Red Moros ao agente de ameaças que anteriormente rastreamos como Red Dev 4 (também conhecido como GALLIUM). Isso aconteceu após termos identificado TTPs, atividades de reconhecimento e infraestrutura, além de comunicações C2 distintas. Ao longo do ano, o Red Moros se voltou de forma agressiva contra provedores de telecomunicações e entidades governamentais em todo o planeta, bem como várias instituições acadêmicas. O que conseguimos observar das suas atividades revelou o uso do software VPN de código aberto SoftEther, tanto ofensivamente quanto como parte da configuração de sua infraestrutura. Também identificamos variantes de uma família de *malware* em código aberto conhecida como PingPull, que avaliamos ser provavelmente uma versão evoluída do *malware* China Chopper.[99]

Leia mais sobre essas ameaças em nossa sinopse da palestra TROOPERS22

Surgido inicialmente em 2021,[100] o Red Menshen permaneceu ativo em 2022 com seu alvo nos setores de telecomunicações e logística. Apesar da divulgação pública de uma das famílias de *malware* mais comumente usadas, a BPFDoor, e de uma remoção aparentemente coordenada de várias infecções de longa duração em agosto, continuamos a observar o Red Menshen acessando sistemas tanto de velhas vítimas quanto de novos alvos.[101]

---

[98] 'U/OO/160405-22: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices', US government, https://media.defense.gov/2022/Jun/07/2003013376/-1/- 1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF (7 de junho de 2022)

[99] CTO-TIB-20220823-02A - Red Moros' Reconnaissance

[100] "Ameaças Cibernéticas: 2021 em Retrospectiva', PwC Threat Intelligence https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/Retrospectiva-Cyber-22.pdf (julho de 2022)

[101] 'Tinker Telco Soldier Spy', PwC Threat Intelligence, https://troopers.de/troopers22/talks/7cv8pz/ (29 de junho de 2022)

Desafios internos e externos do Irã

Em 2022, agentes de ameaças baseados no Irã continuaram a realizar ataques de espionagem contra alvos no Oriente Médio, Europa e América do Norte e, em alguns casos, intensificaram ações destrutivas por meio de *wipers, ransomwares* e hack-and-leak.

Verificamos ainda uma ampliação do foco desses agentes em novos alvos regionais e domésticos, provavelmente em decorrência de falhas da contrainteligência, da agitação doméstica e de uma necessidade de operações de retaliação.

Sanções e fatores que facilitam as operações cibernéticas

Grande parte da resposta do Ocidente às transgressões do Irã em 2022 envolveu sanções adicionais impostas ao regime. O país foi confrontado com medidas punitivas dos EUA[102] por suas atividades ilícitas em quatro áreas principais: seu envolvimento em redes de evasão de sanções para promover vendas de produtos petroquímicos; a comercialização de veículos aéreos não tripulados (UAVs) e armas para a Rússia para uso na guerra; repressão a manifestantes e dissidentes políticos, censura na internet e abusos contra os direitos humanos; e operações cibernéticas agressivas. À medida que o Irã lutava contra um continuado isolamento econômico e diplomático, seus agentes de ameaças atacavam setores e regiões com conexões diretas e tangenciais às sanções e repreensões formais ao regime. Em alguns casos, nossa análise das operações cibernéticas iranianas em 2022 foi baseada nas sanções dos EUA a serem impostas às mesmas entidades que estudamos, tais como o Najee Technology e a Ravin Academy.

Em setembro de 2022, a SECNERD, conhecida oficialmente como Najee Technology, foi incluída na lista de entidades afiliadas ao Corpo da Guarda Revolucionária Islâmica (IRGC) do Irã sancionadas pelo governo americano por seu papel em atividades de *ransomware*.[103] No início do ano, tínhamos começado a rastrear a infraestrutura associada com a SECNERD, um site em língua farsi que se propunha a fornecer recursos de segurança cibernética.[104] Descobrimos sobreposições diretas de infraestrutura entre a SECNERD e o Yellow Dev 24 (também conhecido como DEV-0270 e Nemesis Kitten). Seguimos, na sequência, um rastro corporativo conectando entidades por trás da SECNERD, o que apontava para associações com organizações governamentais iranianas, como o IRGC, a Execução da Ordem do Imam Khomeini (EIKO) e outras sancionadas.[105]

---

[102] 'Iran Sanctions', US Department of State, https://www.state.gov/iran-sanctions/ (23 de novembro de 2022)
[103] 'Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity', US Department of the Treasury, https://home.treasury.gov/news/press-releases/jy0948 (14 de setembro de 2022)
[104] http://secnerd[.]ir, WayBackMachine (Archive), https://web.archive.org/web/20220223151704/http://secnerd.ir (6 de abril de 2022)
[105] CTO-TIB-20220517-01A - Get some better OPSEC nerd

Em outubro de 2022, o governo dos EUA respondeu às operações cibernéticas do Irã e à repressão do governo contra as pessoas que se manifestavam no país. Foram alvos de sanções diversos cidadãos iranianos, agências de inteligência e até mesmo ONGs, como a Ravin Academy.[106] Esta última foi fundada em novembro de 2019, logo após uma série de vazamentos que expôs a ligação de seus cofundadores com o Ministério da Inteligência e Segurança (MOIS) do Irã. Nossa análise da Ravin Academy revelou ainda ligações com o Yellow Nix, além de conexões profissionais com a Yellow Maero (também conhecido como APT34).[107]

Leia mais sobre o Yellow Nix nos posts de nosso blog de 2022

Ataques de sabotagem

Em julho de 2022, vários agentes de ameaça alinhados ao MOIS foram identificados ao conduzir ataques de sabotagem nos sistemas do governo albanês,[108] os quais envolveram reconhecimento e pré-posicionamento antes do uso de *wipers* e *ransonware.*[109] Acreditamos que os ataques foram quase certamente motivados pelo fato de a Albânia abrigar o grupo iraniano Mujahedin-e-Khalq (MEK). A deterioração diplomática entre a Albânia e o Irã foi significativa, com o primeiro cortando as relações formais com o segundo. O governo albanês chegou até a pensar em invocar o Artigo Cinco do Tratado da OTAN, mas, ao final, optou por não escalar ainda mais o conflito com Teerã. Encontramos paralelos entre essas ações e aquelas de janeiro de 2022 contra uma organização sediada nos EUA por sua conexão com o MEK,[110] cumpridas pelo agente de ameaças alinhado ao IRGC, o qual identificamos como o Yellow Dev 19 (também conhecido como Emennet Pasargad).[111]

Nos seus ataques à Albânia, os agentes de ameaça baseados no Irã[112] permaneceram nos sistemas do governo albanês por até 14 meses, o que aponta para um longo pré-posicionamento antes de perpetrar seus efeitos destrutivos. A operação demonstrou um grau de persistência e evidenciou a tendência de os agentes baseados no Irã empregarem tanto ataques de espionagem quanto de sabotagem contra seus alvos. Esses agentes obtiveram acesso inicial ao explorar um servidor SharePoint desatualizado. Em seguida, soltaram *webshells,* fizeram um movimento lateral com a área de trabalho remota do programa AnyDesk e escalaram privilégios usando grupos de funções integrados para o Microsoft Exchange. Eles então aproveitaram essas permissões de função para vazar e-mails usando uma ferramenta sob medida pouco antes de desativar as defesas do endpoint e implantar *wipers* e *ransomware.*[113]

---

[106] 'Treasury Sanctions Iranian Officials and Entities Responsible for Ongoing Crackdown on Protests and Internet Censorship', Departamento do Tesouro dos EUA, https://home.treasury.gov/news/press-releases/jy1048 (26 de outubro de 2022)
[107] CTO-SIB-20220121-01A - Advanced persistent teacher
[108] Nota: Microsoft analisa vários agentes de ameaças baseados no Irã que participaram deste ataque em quatro grupos diferentes de atividade que associamos ao Yellow Maero (também conhecido como APT34), ao Yellow Dev 9 (também conhecido como Lyceum, Hexane) e ao Yellow Dev 31 (também conhecido como DEV-0842). Fonte: 'Microsoft investigates Iranian attacks against the Albanian government', Microsoft, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against- the-albanian-government/ (8 de setembro de 2022)
[109] 'Alert AA22-264A - Iranian State Actors Conduct Cyber Operations Against the Government of Albania', Agência de Segurança Cibernética e Infraestrutura dos EUA, https://www.cisa.gov/uscert/ncas/alerts/aa22-264a (21 de setembro de 2022)
[110] 'PIN 20221020-001 - Iranian Cyber Group Emennet Pasargad Conducting Hack-and-Leak Operations Using False-Flag Persons', Agência Federal de Investigação dos EUA (FBI), https://www.ic3.gov/Media/News/2022/221020.pdf (20 de outubro de 2022)
[111] 'Ameaças Cibernéticas: 2021 em Retrospectiva', PwC Threat Intelligence https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/Retrospectiva-Cyber-22.pdf (julho de 2022)
[112] Nota: Microsoft analisa vários agentes de ameaças baseados no Irã que participaram deste ataque em quatro grupos diferentes de atividade que associamos ao Yellow Maero (também conhecido como APT34), ao Yellow Dev 9 (também conhecido como Lyceum, Hexane) e ao Yellow Dev 31 (também conhecido como DEV-0842). Fonte: 'Microsoft investigates Iranian attacks against the Albanian government', Microsoft, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against- the-albanian-government/ (8 de setembro de 2022)
[113] CTO-TIB-20220916-01A – Iran-based APTs attack Albania

Agentes de ameaça baseados no Irã também continuaram suas operações do tipo *hack-and-leak* ou *lock-and-leak* contra outras organizações – como se viu antes, em 2021, quando o criminoso conhecido como Moses Staff realizou operações lock-and-leak contra diversos setores em Israel.[114] No segundo semestre de 2022, surgiu um agente de ameaças bastante semelhante chamado Abraham's Ax, que alardeava ter obtido acesso aos sistemas do Ministério do Interior da Arábia Saudita e postou mensagens anti-Ocidente e anti-Israel nas redes sociais.[115] O *modus operandi* de ambos era quase idêntico e, inclusive, encontramos sobreposições de infraestrutura da rede a apontar que os dois agentes são, de fato, bem alinhados.[116]

Alvos domésticos e contra dissidentes

Nossa pesquisa ao longo do ano apontou ainda uma tendência persistente de agentes baseados no Irã, como o Yellow Garuda (também conhecido como Charming Kitten, APT42 e PHOSPHORUS), de mirarem alvos dentro do próprio país e contra dissidentes do governo local. O Yellow Garuda atacou pessoas que falavam farsi, provavelmente dentro do Irã, mas com possibilidade de ter acontecido também no exterior, com foco especial em estudantes, ativistas e supostos militantes. Analisamos sobreposições de atividades que se passaram entre setembro de 2021 e junho de 2022, com o Yellow Garuda "armando" documentos da Microsoft com `CVE-2021-40444` e `CVE-2022-30190`. Com base nos tempos de compilação, esse agente foi capaz de operacionalizar esses *exploits* em uma semana após sua revelação pública. Com isso, houve pouco tempo para que os defensores criassem medidas eficazes de detecção e mitigação.[117]

Em meio aos protestos no Irã em 2022 desencadeados pela morte, em setembro, de Mahsa Amini, uma mulher curda iraniana que foi presa por violar leis sobre o uso do *hijab*,[118] o foco dos agentes de ameaça do país continuou a ser doméstico, com alvos em ativistas, dissidentes e manifestantes. Mesmo com a eclosão de protestos generalizados, esses agentes conseguiram mirar aquelas prioridades permanentes do regime de Teerã, como, por exemplo, organizações do próprio governo e nos setores de defesa, telecomunicações e energia.[119] Ao mesmo tempo, o aparato de vigilância do Irã não perdeu seu foco interno, inclusive por meio de capacitadores de terceiros e *malware* implantado em dispositivos móveis de civis.[120] O Yellow Dev 32 foi um dos grupos que miraram alvos internos a fazer uso de um *malware* para Android chamado L3MON nos celulares dos manifestantes em outubro de 2022. [121]

---

[114] 'Ameaças Cibernéticas: 2021 em Retrospectiva', PwC Threat Intelligence https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/Retrospectiva-Cyber-22.pdf (julho de 2022)
[115] 'Abraham's Ax Likely Linked to Moses Staff', Secureworks, https://www.secureworks.com/blog/abrahams-ax- likely-linked-to-moses-staff (26 de janeiro de 2023)
[116] 'Iranian Hacking Group Abraham's Ax claims hack on Saudi Ministry of Interior', Cyberwarzone, https://cyberwarzone.com/abraham-ax-saudi-ministry-interior-cyberattack/ (novembro de 2022)
[117] CTO-TIB-20220728-01A - Bye Follina
[118] 'UN rights chief says 'full-fledged' crisis underway in Iran amid crackdown on protesters', CNN, https://www.cnn.com/2022/11/24/middleeast/iran-protests-un-human-rights-council-intl/index.html (24 de novembro de 2022)
[119] 'Alert AA22-055A - 'Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-055a (24 de fevereiro de 2022)
[120] CTO-TIB-20221206-01A - A sour L3MON and a FurBall
[121] CTO-TIB-20221206-01A - A sour L3MON and a FurBall

Tendências setoriais e regionais

Outra tendência relacionada aos agentes de ameaça do Irã verificada ao longo de 2022 foi seu pesado *targeting* aos setores críticos da indústria naval, logística, transporte marítimo e infraestrutura na Europa e no Oriente Médio. Desde maio de 2022, o Yellow Liderc (também conhecido como Tortoiseshell e CURIUM) inseriu JavaScript em sites verdadeiros dos setores naval, transporte marítimo e logística.[122] O *script* conseguia identificar os visitantes desses portais, capturando a localização do usuário, informações do dispositivo e dados de data ehora das visitas. Concomitantemente, o agente de ameaças registrava domínios ciberocupados por erro de digitação (*typosquatted*) se passando por sites infectados com *scripts* maliciosos. Em nossa avaliação, muito provavelmente o Yellow Liderc usou esses domínios *typosquatted* junto com dados biométricos de usuários para lançar ataques *spear phishing* personalizados. Parte dessa atividade se alinhava com um *targeting* similar reportado em fonte aberta, que detalhou como esse agente atacava empresas transportadoras em Israel entre 2020 e 2022.[123] Avaliamos ainda que grande parte dessa atividade provavelmente estava relacionada a apreensões de navios petroleiros identificados (*flagged*) por transportar petróleo cru iraniano, como foi o caso da embarcação apreendida no Mediterrâneo a pedido do governo dos EUA em maio de 2022.[124]

No início de 2022, identificamos casos do Yellow Garuda usando iscas que abrangiam uma variedade de temas, como as ambições nucleares da Turquia e os portos dos EUA. Consideramos a possibilidade de que esse agente tenha feito isso de olho em alvos no Oriente Médio em geral e que a atividade pode não ter sido indicativa de uma campanha direcionada especificamente a organizações do setor de energia. Pelo menos um documento com uma isca sobre um porto dos EUA foi provavelmente direcionado, já que seu formato consistia em uma carta com um destinatário nomeado.[125]

Por meio da nossa análise de infraestrutura associada divulgada publicamente em fonte aberta em janeiro de 2022[126], vimos também que o Yellow Garuda continuou a mirar jornalistas, *think tanks* e pesquisadores por meio de TTPs parecidos com os vistos em 2019. Atribuímos tal estrutura a esse criminoso e identificamos domínios que se passavam (*spoofing*) por veículos de mídia e *think tanks* dos EUA, Israel e dos Emirados Árabes Unidos. Após análise adicional, verificamos que os indivíduos e as entidades visadas eram, de fato, especialistas reconhecidos de – ou normalmente envolvidos em – política externa do Oriente Médio, negociações nucleares e outros interesses estratégicos relevantes para o regime de Teerã. Identificamos ainda domínios que faziam *spoofing* de contas do Google e da Microsoft, junto com novos alvos domésticos com a vitimologia típica do Yellow Garuda.[127]

Leia mais sobre o Yellow Garuda nos posts de nosso blog de 2022

[122] CTO-TIB-20221208-01A - Yellow Liderc ships its scripts
[123] 'Suspected Iranian Actor Targeting Israeli Shipping, Healthcare, Government and Energy Sectors', Mandiant, https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping (17 de agosto de 2022)
[124] 'Iranian oil tanker's cargo seized in Greece after US request', AP News, https://apnews.com/article/russia- ukraine-politics-united-states-68af0db11c5c03e89049da0629ef4d85 (26 de maio de 2022)
[125] CTO-TIB-20220308-01A - Charming Kitten's Turkish delight
[126] 'Shady Network of Fake Mossad Job Sites Targets Iranian Spies', The Daily Beast, https://www.thedailybeast.com/shady-network-of-fake- mossad-job-sites-target-iranian-spies (24 de janeiro de 2022)
[127] CTO-TIB-20220302-01A - A busy bird that Yellow Garuda

Agentes de ameaça baseados no Irã continuaram a visar organizações de Israel em 2022. Por exemplo, analisamos uma conta do GitHub associada ao Yellow Nix e, em seguida, identificamos um *script* dentro do repositório da conta contendo um endereço IP C2. Atribuímos a infraestrutura ao Yellow Nix e avaliamos que provavelmente ela tenha sida usado para atacar organizações israelenses e turcas.[128] Em outro exemplo, em novembro de 2022, o Yellow Nix se voltou para várias companhias de seguros israelenses usando uma ferramenta comercial de administração remota chamada Syncro.[129]

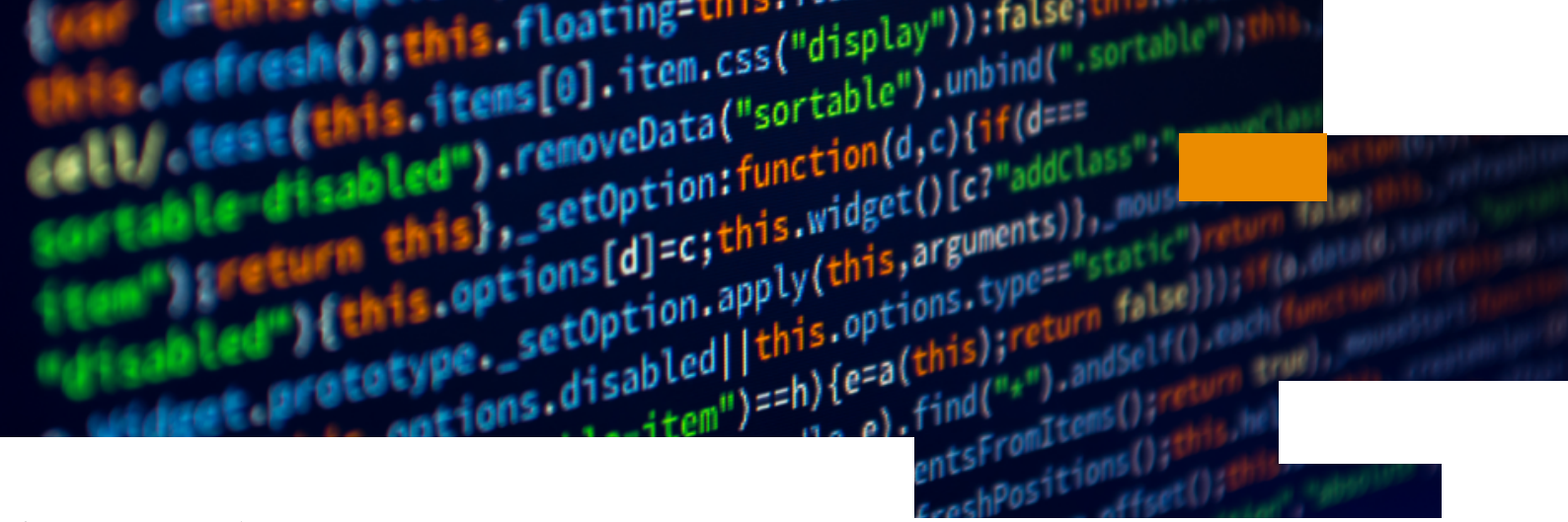
Case de resposta a incidentes envolvendo o Yellow Liderc

No início de 2022, lideramos os mais amplos esforços de respostas a incidentes da PwC envolvendo uma empresa de engenharia e manufatura europeia que tinha sido atacada pelo Yellow Liderc (também conhecido como Tortoiseshell e TA456). A partir de nossa análise baseada nas amostras executáveis fornecidas pela vítima, descobrimos que o agente de ameaças empregava ferramentas e técnicas avançadas. Observamos que essas mudanças provavelmente indicam que o Yellow Liderc está tentando aprimorar sua segurança operacional para evitar detecção e persistir nas redes das vítimas.

Estudamos a funcionalidade de três *scripts* Python ofuscados com PyArmor – uma ferramenta disponível em código aberto para esse exato propósito – e o tráfego de rede entre a vítima e o servidor do Yellow Liderc. Encontramos comunicações C2 desde janeiro de 2022 e que continuaram por um período de pelo menos quatro meses. As amostras, que estavam altamente disfarçadas, comunicavam-se por meio de um protocolo de mensagens seguro para caixas de e-mail dedicadas. Tudo isso era indício de que o Yellow Liderc estava aprimorando sua segurança operacional.[130]

Por mais que, muitas vezes, descubramos agentes de ameaças baseados no Irã justamente por conta de sua segurança operacional deficiente e uso de infraestrutura e ferramentas bem conhecidas, este incidente destaca a importância de não os subestimar nem duvidar de sua capacidade de evoluir para além de comportamentos e limites avaliados. Nosso profundo conhecimento das motivações dos agentes de ameaças e suas táticas nos permitiu priorizar os esforços de resposta a incidentes e fornecer um contexto substancial para a vítima se preparar para o futuro.

[128] CTO-TIB-20220210-01A - Smooth Operator
[129] CTO-TIB-20221206-02A - Let's Syncro up with Yellow Nix
[130] CTO-TIB-20220628-02A - Three varieties of Liderc



Outros estudos de caso regionais

Nesta seção, fornecemos uma amostra de outros agentes de ameaça com variados níveis de sofisticação e motivação.

Assim como em anos anteriores, a atividade dos agentes de ameaças acompanhou os eventos do mundo real e refletiu as circunstâncias geopolíticas, que, em muitos casos, pareciam se relacionar com as prioridades e os objetivos estratégicos nacionais e políticos dos países.

Operações secretas por dinheiro

Nosso estudo das atividades de agentes de ameaças baseados na Coreia do Norte em 2022 reforçou conhecidas tendências, táticas, técnicas, procedimentos e vitimologia já vistos em anos anteriores, tais como ataques a organizações do setor de serviços financeiros e empresas de criptomoedas.[131] Observamos ainda ataques motivados por dinheiro em vários outros setores. Com base nos padrões de *targeting* que vimos em 2022, avaliamos que esses agentes provavelmente continuaram a perpetrar ações de roubo financeiro em nome do governo.

Voltamos a verificar acelerado ritmo operacional nos grupos que agem por motivação financeira como Black Alicanto (também conhecido como COPERNICIUM, DangerousPassword, CryptoMimic, CryptoCore e Operation SnatchCrypto) e Black Dev 2 (também conhecido como Operation Gold Hunting e Operation SnatchCrypto). Eles se voltaram para criptomoedas, além de empresas de capital de risco e startups. Concluímos que o Black Dev 2 está provavelmente ligado ao Black Alicanto e que, desde 2021, os dois têm visado vítimas com iscas temáticas de emprego e oportunidades para levantar capital de risco no espaço das criptomoedas.[132] Entre meados e final de 2022, o Black Alicanto usou instaladores de software da Microsoft (MSIs) para obter acesso inicial e instalação nos sistemas das vítimas, ao contrário do seu uso tradicional de arquivos LNK maliciosos.

Já o Black Artemis (também conhecido como Lazarus Group, Hidden Cobra e ZINC) também esteve bastante ativo, rodando múltiplas campanhas ao longo do ano. Esse agente prosseguiu com sua campanha conhecida como “Operation Dream Job” e “Operation Interception”, que rastreamos como ShowState, usando a família de *malware* conhecida como BLINDINGCAN. [133] Ele continuou a usar implantes de *malware* como o BLINDINGCAN e o DTrack, utilizados ao menos desde 2018 e 2014, respectivamente. Isso mostra que o criminoso prefere desenvolver seu código existente em vez de abandoná-lo, além de adicionar novas ferramentas ao seu arsenal.

[131] CTO-SIB-20220915-02A - Tales from the crypto
[132] CTO-TUS-20220616-01A - Threats under the Spotlight – maio de 2022
[133] CTO-TIB-20220812-01A - Black Artemis’ dream job hunt

O Black Artemis também manteve seu *targeting* com finalidade de espionagem contra entidades militares e de defesa, tendo desenvolvido melhorias expressivas em seu conjunto de ferramentas e introduzido famílias de *malware* como YamaBot e MagicRAT. Relatórios da indústria que alertavam para o fato de esse agente ter se voltado contra empresas do setor de energia[134, 135] ganharam notoriedade e complementaram nossa visão acerca de outros aspectos de sua atividade.

A PwC Coreia do Sul foi alertada, no segundo semestre de 2022, sobre o agente de ameaças de *ransomware* autodenominado GWISIN – que significa fantasma em coreano – e que tinha como alvos apenas organizações nacionais. Aparentemente, esse criminoso tem um profundo conhecimento da Coreia, de seus sistemas de segurança, além de suas certificações de segurança e legislações. O GWISIN empregou técnicas de evasão defensiva, fiel ao seu nome, em combinação com vulnerabilidades na web e *web shells* usados para enviar comandos e copiar dados das vítimas.

Observando o Orange

Agentes de ameaças baseados na Índia mantiveram um ritmo operacional relativamente alto em 2022, empregando TTPs conhecidas desde 2021. Observamos forte direcionamento dos ataques a entidades de defesa e governamentais do Paquistão com um *malware* semelhante ao utilizado em anos anteriores. Porém, vimos também muitos alvos novos e notáveis, além de novas TTPs. Ao que tudo indica, diversos agentes de ameaças, como o Orange Yali (também conhecido como BITTER)[136] e o Orange Kala (também conhecido como DONOT), ampliaram seus alvos para incluir organizações sediadas em outros países da região. Já o Orange Chandi (também conhecido como SideWinder) mudou o processo de ataque de suas TTPs de longa data, usados em 2020 e 2021.

Embora 2022 tenha fornecido evidências de novo *targeting* alinhado a eventos políticos na região[137], os agentes baseados na Índia principalmente mudaram as ferramentas usadas em seus processos de ataque em vez de implementar técnicas mais sofisticadas. Em diversos casos, como se viu em 2021,[138] eles continuaram a fazer uso de RATs comuns em suas campanhas.

---

[134] 'Stonefly North Korea-linked Spying Operation Continues to Hit High-value Targets', Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage (27 de abril de 2022)
[135] 'DTrack activity targeting Europe and Latin America', Kaspersky, https://securelist.com/dtrack-targeting-europe- latin-america/107798/ (15 de novembro de 2022)
[136] CTO-TUS-20221027-01A - Threats under the Spotlight - setembro 2022
[137] CTO-SIB-20220915-01A - APAC-origin forecast - Q2 2022 developments
[138] CTO-TIB-20210112-01A - Orange Kala enters the Warzone

Talentos não precisam se candidatar: ameaças persistentes e avançadas usam iscas com ofertas de emprego

À medida que a COVID-19 levava um crescente número de trabalhadores a repensar suas carreiras, os agentes de ameaças não perderam a oportunidade de explorar esse assunto em 2022 para satisfazer seus objetivos estratégicos de ganhar dinheiro e fazer espionagem. Agentes baseados na Coreia do Norte e no Irã foram, particularmente, ousados em atingir empregados de empresas de alto perfil. Para tanto, usaram engenharia social para abordar funcionários por e-mail e pelas redes sociais para construir relacionamento antes de tentar obter acesso às redes empresariais.[139]

- **Agentes de ameaças baseados na Coreia do Norte e campanhas com motivação financeira**

  A oferta de emprego é um velho pretexto desses criminosos. Durante uma campanha assim em 2022, o Black Artemis (também conhecido como Lazarus Group, HiddenCobra e ZINC) criou diversas personas de rede social, passando-se, inclusive, por profissionais de recrutamento e recursos humanos de grandes empresas. O Black Artemis também desenvolveu sites fingindo ser reconhecidas firmas de recrutamento. Esses portais, no entanto, estavam armados com *exploits* de navegador que implantavam *malware* nos computadores de suas vítimas.

  Em um outro método, após fazer contato com as pessoas via LinkedIn, WhatsApp ou e-mail, o agente de ameaça tentava convencê-las a abrir documentos com códigos maliciosos nos sistemas que usavam para trabalhar. Uma vez abertos, a injeção de modelo remoto ou macros maliciosos baixavam implantes de *malware* nas redes das organizações. Desde pelo menos julho de 2022, o Black Artemis mudou de estratégia para fazer com que seus alvos executassem arquivos EXE[140] ou ISO[141] contidos em arquivos compactados, sob o pretexto de que continham descrições de cargos abertos em grandes empresas de tecnologia ou avaliações de candidatos. Em outro exemplo, desde agosto de 2022 ao menos, o Black Alicanto (também chamado de COPERNICIUM, DangerousPassword, CryptoMimic, CryptoCore e Operation SnatchCrypto) usou arquivos MSI com iscas maliciosas em campanhas semelhantes, provavelmente em uma tentativa de diversificar suas técnicas iniciais.

- **Agente de ameaças iraniano faz campanha para espionar**

  Também o Yellow Dev 13 (conhecido ainda como BOHRIUM e TA455) se passou por recrutadores de empresas reais ou fictícias em várias mídias sociais, como LinkedIn, Facebook, Instagram e Twitter, apesar das remoções realizadas pela Meta[142] e pela Microsoft.[143] Esse agente de ameaças usou ainda uma variedade de fotografias geradas por inteligência artificial (IA) para criar suas personas e fingiu ser por pelo menos um indivíduo real em suas operações.

[139] 'Talent Need Not Apply Tradecraft and Objectives of Job-themed APT Social Engineering', PwC Threat Intelligence, https://i.blackhat.com/USA-22/Thursday/US-22-Wikoff-Talent-Need-Not-Apply.pdf (11 de agosto de 2022)
[140] CTO-TIB-20220812-01A - Black Artemis' dream job hunt
[141] 'It's Time to PuTTY! DPRK Job Opportunity Phishing via WhatsApp', Mandiant, https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing (14 de setembro de 2022)
[142] 'Meta Quarterly Adversarial Threat Report: Q1 2022', Meta, https://about.fb.com/wp- content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf (abril de 2022)
[143] 'Microsoft Corporation, A Washington corporation, Plaintiff, v. John Does 1-2, Controlling a computer network and thereby injuring plaintiff and its customers: Ex Parte temporary restraining order and order to show cause re preliminary injunction', Microsoft, https://news.microsoft.com/wp-content/uploads/prod/sites/358/2022/06/Doc.-No.- 16-Ex-parte-TRO-SEALED.pdf (27th May 2022)

O Yellow Dev 13 também administrou pelo menos dois sites de empresas falsas de recrutamento chamadas ApplyTalents e CareersFinders,[144] supostamente britânicas, e que compartilhavam os mesmos profissionais e contatos de e-mail falsos. Em pelo menos um caso, o ator de ameaça desenvolveu um executável malicioso que simulava uma plataforma de avaliação completa para candidatos a emprego, com testes de aptidão e uma função de suporte via chat ao vivo. Tal plataforma se conectaria, em segundo plano, ao domínio ApplyTalents. Ainda que esta exigisse que os usuários inserissem credenciais provavelmente fornecidas pelo agente de ameaça para evitar o escrutínio de pesquisadores, acreditamos que Yellow Dev 13 estava provavelmente tentando comprometer indivíduos ou organizações para fins de espionagem.

Saiba mais sobre a palestra Talentos Não Precisam se Candidatar no BlackHat USA 2022

Wirting sobre o White Dev 21

O White Dev 21 (também conhecido como WIRTE) permaneceu mirando vítimas ao longo de todo o Oriente Médio, tais como a Jordânia, a Palestina, a Síria e o Líbano. Um *cluster* de atividade em particular revelou, em setembro de 2022, que o White Dev 21 dependia fortemente de iscas temáticas ligadas à geopolítica, apoiando-se em questões tais como o Conselho de Cooperação do Golfo e informações sobre organizações governamentais e serviços financeiros do mundo árabe. O agente de ameaça demonstrou uma habilidade persistente de atingir setores e entidades-chave na região.[145]

Um desenvolvimento in-Tur-essante

Fizemos uma postagem em blog, em janeiro de 2022, a respeito de um agente de ameaça que identificamos como White Tur, o qual vinha atacando organizações dos Balcãs desde pelo menos 2017 e ao longo de 2021. Após nossa publicação,[146] ele seguiu ativo e continuou a visar empresas na região com temas relacionados à Bósnia-Herzegovina e à Sérvia. Identificamos ainda uma série de *scripts* HTML Application (HTA), criados entre janeiro e abril de 2022, e que sinalizam uma mudança nas TTPs do White Tur. Nesta série de *scripts* HTA, ele usava o protocolo WebDAV para transferir uma carga útil (*payload*) maliciosa nas máquinas de suas vítimas.[147]

Saiba mais sobre o White Tur em um de nossos posts de 20022 e na palestra 'Agente de Ameaça de In-Tur-Esse' no SANS CTI Summit 2022

[144] CTO-TIB-20220121-02A - Talent need not apply to this career finder
[145] CTO-TUS-20221027-01A - Threats under the Spotlight – setembro de 2022
[146] 'Threat actor of in-Tur-est', PwC Threat Intelligence, https://www.pwc.com/gx/en/issues/cybersecurity/cyber- threat-intelligence/threat-actor-of-in-tur-est.html (27 de janeiro de 2022)
[147] CTO-TIB-20221012-03A - White Tur's WebDAV adventures

Mais sobre as TTPs do White Tur

Os arquivos HTA são interpretados pelo `mshta.exe`, um bem conhecido binário live-off-the-land (ou LOLBin), que é muito usado pelos agentes de ameaças. Como esses arquivos oferecem a oportunidade de lançar *scripts* em HTML sem muitas das restrições de um navegador, são bastante usados por invasores para executar *scripts* maliciosos em JavaScript e VBScript. Os mecanismos de detecção deveriam estar focados no processo `mshta.exe`, descobrindo, por exemplo, quando ele chama um arquivo HTA, a partir de um local remoto ou grava arquivos com determinadas extensões no disco rígido.

Como White Tur copia executáveis no disco usando o protocolo WebDAV, eles são colocados na pasta para "Inicializar" para garantir sua execução persistente É desafiador monitorar todos os arquivos gravados nessa pasta em um ambiente empresarial. Contudo, dada a frequência de seu uso pelos criminosos, é preciso que os mecanismos de detecção estejam operantes para identificar criações suspeitas de arquivos. A lógica de detecção baseada em atividade anômala ou arquivos globalmente únicos em diretório provavelmente revelará esse tipo de atividade – embora esse tipo de análise não esteja disponível para todas as ferramentas de detecção. Um bom ponto de partida é monitorar LOLBins ou executáveis que, geralmente, usam bastante a gravação de arquivos

O que está acontecendo com o White Dev 140?

Um de nossos projetos de pesquisa em 2022 apontou um padrão de comportamento desconcertante que atribuímos ao White Dev 140. O interesse dele abrangia entidades ucranianas – semelhante ao que vimos com agentes baseados na Rússia. Contudo, o White Dev 140 também possuía outros interesses fora da Ucrânia, o que confundiu nossas avaliações iniciais sobre suas motivações. Esses incluíam:[148]

- Exportadores de alimentos, supermercados e varejistas;
- Organizações governamentais regionais, como o governo de Dnipro e do distrito de Piatykhatky;
- Energoatom, a agência nuclear ucraniana;
- Uma empresa do setor de gás;
- Fábricas de metais e de equipamentos eletrônicos; e,
- Empresas de logística e de entregas particulares.

Exemplos de indicadores das atividades do White Dev 140 que identificamos em 2022:

```
https[:]//product808[.]godaddysites[.]com/purchase-order
https[:]//support-domaill[.]godaddysites[.]com/ukr
https[:]//shipping8[.]godaddysites[.]com/dhl
https[:]//servicesagreement[.]godaddysites[.]com/update
https[:]//support-ukr[.]godaddysites[.]com/log-in
```

[148] CTO-TIB-20221209-02A - Phishing trips to Ukraine

Identificamos a atividade de *spear phishing* do White Dev 140 pela primeira vez em maio de 2022, quando ele se voltou contra um revendedor ucraniano de software que também fornecia licenças para este governo.[149] O e-mail de *spear phishing* continha o tema de rede UKR[.]– um popular portal de internet usado na Ucrânia para e-mail. A mensagem continha um PDF anexado com a seguinte mensagem, em ucraniano, que pode ser traduzida aproximadamente assim:

```
Querido usuário,
Essa é uma mensagem muito importante. Nossos registros mostram
que sua conta não foi atualizada Nota: se você não verificar sua
conta, ela será desativada em breve

Essa atualização é necessária imediatamente após o recebimento
dessa mensagem
Atenciosamente
Equipe do e-mail @UKR
```

As TTPs da atividade de *spear phishing* na época eram semelhantes às usadas pelo BlueAthena, que estava conduzindo uma ampla campanha de *phishing,* com as seguintes táticas:[150,151]

- Anexo em PDF com link de *phishing*, usando temas UKR[.]net;
- Uso de provedores de hospedagem gratuitos;
- *Targeting*; e
- Conteúdos de e-mail.

Os e-mails de *spear phishing* possuíam um anexo em PDF com um link de *phishing* para a URL:

```
https[:]//ukrverifikaciyaakkaunta[.]godaddysites[.]com/privacy-
policy
```

Em outubro de 2022, outro e-mail de *spear phishing* do White Dev 140 visou um domínio ucraniano. O e-mail trazia temas da empresa DHL, mas com uma URL da Deutsche Post que era usada como link de *phishing*. A URL era a seguinte:

```
https[:]//deutschepost[.]godaddysites[.]com/login
```

Ao analisar os dados técnicos associados ao e-mail de *spear phishing*, vimos semelhanças com as páginas de *phishing* de maio e outubro de 2022, analisadas anteriormente.

[149] CTO-QRT-20220601-01A - More phishing attempts against Ukraine
[150] CTO-QRT-20220326-01A - Blue Athena Phishing Part 1
[151] 'Update on cyber activity in Eastern Europe', Google, https://blog.google/threat-analysis-group/update-on-cyber- activity-in-eastern-europe/ (3 de maio de 2022)

A partir da amostra adicional, encontramos um padrão consistente que nos permite identificar outras páginas de *phishing.*

Uma resposta personalizada?

Em setembro de 2022, o Centro Nacional de Emergência de Vírus de Computador da China (CVERC) informou que a Agência de Segurança Nacional dos EUA (NSA), destacadamente a sua divisão de Operações de Acesso Personalizado (TAO), havia atacado uma universidade chinesa por meio de um conjunto de ferramentas[152]. Algumas delas compartilhavam nomes com ferramentas que haviam sido vazadas anteriormente por uma pessoa e um grupo – ambos conhecidos como Shadow Brokers[153]. O relatório de setembro de 2022 não incluiu índices, prazos ou outras características dessas atividades.

Insights da PwC Brasil

A PwC Brasil analisou em 2022 criminosos brasileiros que usavam uma interface web comercial chamada Data Broker Panels. Existente há pelo menos cinco anos, ela possibilita a busca de informações sensíveis sobre cidadãos brasileiros. Eles tiveram a proeza de vender acesso por assinatura a esses painéis, geralmente em planos mensais, permitindo, assim, que outros agentes explorassem as informações para ataques de engenharia social e fraudes.

[152] 'Chinese reports uncover details of cyber attacks by U.S. security agency', Xinhua, https://english.news.cn/20220913/71f9b72993614795b4d8ff554c99ef9b/c.html (13 de setembro de 2022)
[153] 'Shadow Brokers leaks show U.S. spies successfully hacked Russian, Iranian targets', CyberScoop, https://www.cyberscoop.com/nsa-shadow-brokers-leaks-iran-russia-optimusprime-stoicsurgeon/ (18 de abril de 2017)

Mudanças no ecossistema de crimes cibernéticos

Avanços notáveis no ecossistema de crimes cibernéticos surgiram em 2022, com agentes de segurança engajados em operações de *hack-and-leak* semelhantes à versão digital de roubos do tipo *smash-and-grab* combinados com a prática de *big game hunting*. Isso significa que esses agentes estavam atrás de alvos de alto perfil ou percebidos como de alto valor, enquanto tentavam ganhar manchetes e notoriedade.

As mudanças nesse ecossistema foram em grande parte apoiadas por uma corrente subjacente e contínua de agentes de ameaças motivados por dinheiro, que capitalizaram ataques oportunistas e exploratórios envolvendo roubo, extorsão e fraude, com operações de *ransomware* dominando o mercado.

Esses agentes foram ainda mais descarados em 2022 nas tentativas de pressionar as vítimas de extorsão e recrutar informantes. Avaliamos que essa tendência provavelmente se tornará proeminente no próximo ano, à medida que os agentes fragmentam cada vez mais as "marcas" de *ransomware*, competem por recursos e se veem obrigados a responder ao aumento das defesas e da resiliência nas organizações. Ante as intersecções do crime cibernético e os agentes de ameaça do Leste Europeu, abordamos anteriormente neste relatório desenvolvimentos específicos referentes à guerra na Ucrânia - Invasão russa da Ucrânia: Unindo-se para se proteger do crime cibernético.

Avanços do *ransomware*

Foi-se o tempo em que o *ransomware* podia ser considerado um disruptor. Ao longo dos últimos anos, ele se tornou uma ameaça consistentemente dominante para as organizações. Essa prevalência se deve em grande parte às operações de *Ransomware-as-a-Service* (RaaS) – modelo de perpetuação que detalhamos em nosso relatório **Ameaças Cibernéticas: 2021 em Retrospectiva**[154].

Em 2022, o número de vítimas em sites de vazamento se estabilizou em comparação com 2021. Avaliamos que esse nível de atividade deve permanecer consistente em 2023. No entanto, é improvável que o número de "marcas" distintas de *ransomware* represente um indicador relevante do cenário de ameaças, uma vez que tem sido prática comum os grupos mudarem rapidamente e se reformularem.

[154] 'Ameaças Cibernéticas: 2021 em Retrospectiva', PwC Threat Intelligence https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/Retrospectiva-Cyber-22.pdf (julho de 2022)

Seguindo em frente, avaliamos que os dados mais relevantes para acompanhar a atividade de *ransomware* serão os vistos nas TTPs (táticas, técnicas e procedimentos) compartilhadas entre os agentes de ameaças.

TTPs observadas em uma típica operação *Ransomware-as-a-Service* (RaaS)

Acesso Inicial

- Compre credenciais válidas
- Faça campanhas de *phishing*
- Explore vulnerabilidades **Ex: Log4Shell**

Comprometa contas privilegiadas explorando problemas comuns de higiene de TI/AD

Mova-se lateralmente e estabeleça pontos de apoio com ferramentas de segurança ofensiva comuns

Vaze dados sensíveis para a infraestrutura operada pelo atacante

Implante *ransomware* o mais amplamente possível para obter o impacto máximo

Escalação de privilégios	Reconhecimento de Movimento Lateral	Vazamento de Dados	Criptografar arquivos
Valide contas	Cobalt Strike	Compressão de arquivos WinRAR	
Mimikatz	ADFind	Ferramentas personalizadas ExMatter StealBit	
Rubeus	Bloodhound	Utilitários de transferência de arquivos Megasync NGrok FTP WebDAV PuTTY Secure Copy (PSCP)	
LSASS	PsExec	Via C2	
Explore vulnerabilidades	RDP		
Políticas de grupo	Facilitador RDP		

Análise de sites de vazamento

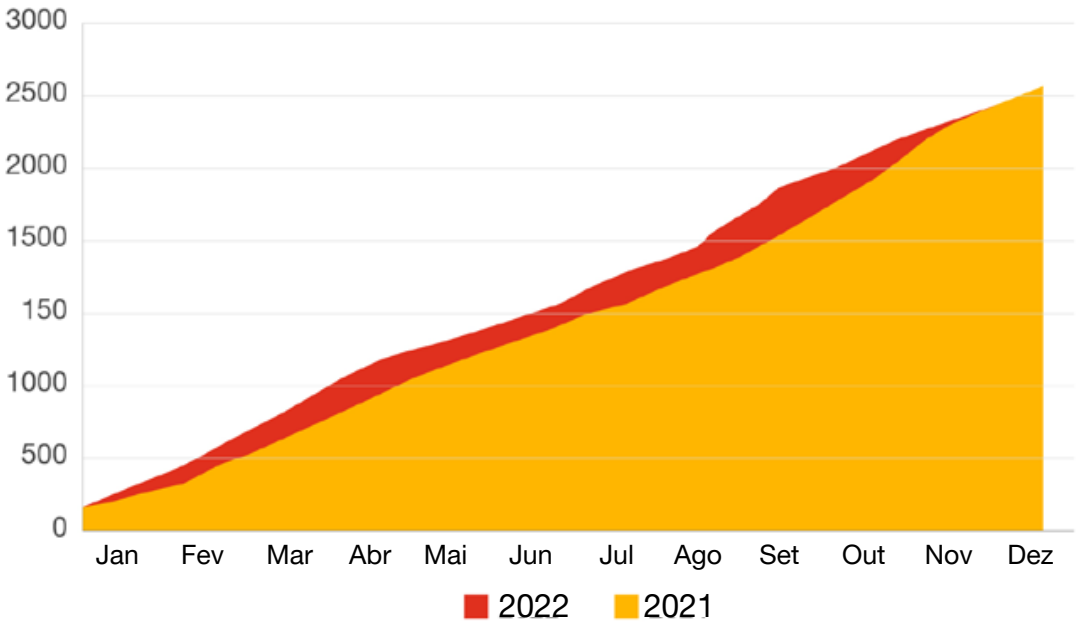
Em 2022, conforme nosso rastreamento, houve um total de 2.462 vítimas postadas em sites de vazamento de *ransomware* – número ligeiramente menor (menos de 1%) que as 2.471 verificadas no ano anterior e quase o dobro das 1.330 de 2020. Em resumo, ainda que tenha havido um aumento progressivo no total de vítimas dos sites de vazamento de *ransomware* de 2020 a 2021, o número pareceu se estabilizar entre 2021 e 2022.

Avaliamos, portanto, que o número de vítimas de sites de vazamento tenha provavelmente atingido seu "ponto alto" em 2021 e 2022. Em 2022, houve ainda desafios significativos para o ecossistema de *ransomware*, como a guerra na Ucrânia, ações legais contra os agentes de ameaças, a volatilidade das criptomoedas, vazamentos internos e conflitos que acabaram por fragmentar grupos de *ransomware* proeminentes.[155]

Atividade de sites de vazamento versus atividades da ameaça *ransomware*

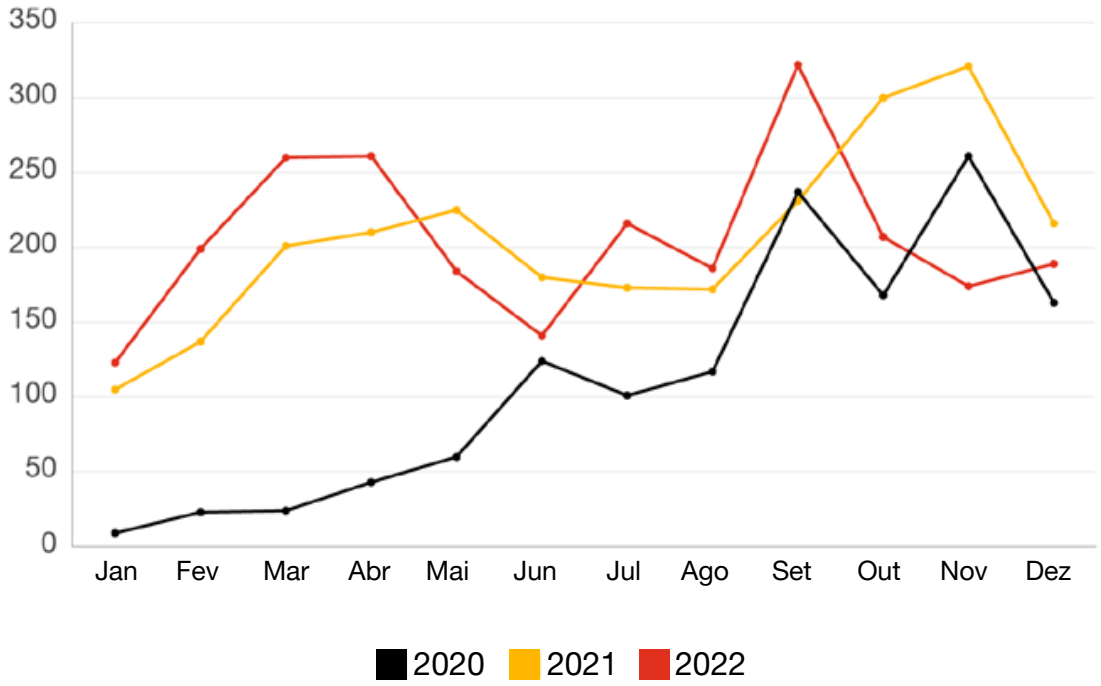
Quando rastreamos a atividade dos sites de vazamento, temos uma boa visão do quadro geral da ameaça ***ransomware.*** No entanto, continuamos a buscar outras vias de análise, dado que esses sites não fornecem uma imagem completa do problema, especialmente em relação aos agentes de ameaças que operam fora dos sites e às vítimas que não são postadas ou divulgadas publicamente.

Número de vítimas de sites de vazamento postadas no decorrer do ano (2021-2022)



[155] CTO-SRT-20230118-01A - Ransomware report for December 2022

Número de vítimas de sites de vazamento postadas mês a mês (2020 – 2022)



Classificamos os ataques *ransomware* como oportunistas e habilitados por operações de infecção generalizadas e indiscriminadas. Porém, é também verdade que observamos, em 2022, vários setores que tiveram mais vítimas em sites de vazamento do que outros. Os cinco com o maior número de vítimas postadas nesses portais foram os de manufatura (15%), construção civil (10%), serviços profissionais (9%), tecnologia (8%) e varejo (8%).

Entre as possíveis explicações para isso estão o alto custo percebido do tempo de inatividade operacional desses setores, bem como o nível comparativamente menor de regulamentações de segurança da informação a eles impostas. Além disso, os ataques de *ransomware* impactaram também, de modo significativo, empresas ligadas a outros segmentos em 2022, tais como o governamental, de telecomunicações, transportes, energia e educação.

White Janus com a maior parte

Analisamos a atividade dos sites de vazamento, em 2022, que apontou que o White Janus (também conhecido como LockBit) dominou numericamente ao longo de todo o período. Ele rapidamente ultrapassou o ritmo de 2021 do Blue Cronus, o qual havia liderado o grupo de *ransomware* em atividade no ano anterior. Em junho de 2022, o White Janus anunciou seu programa LockBit 3.0 RaaS, que impulsionou ainda mais suas operações e ritmo de vazamento na segunda metade do ano. Avaliamos que ele provavelmente passou grande parte daquele mês testando o LockBit 3.0 beta. Assim, não por acaso, houve queda acentuada nas vítimas postadas em seu site de vazamento ante ao verificado na primeira metade de 2022.[156] Até o final de dezembro, o White Janus postou um total de 907 vítimas em seu site para todo o ano de 2022, contra as 460 vítimas que havia postado em 2021.[157]

[156] CTO-QRT-20220804-03A - White Janus changes the Locks
[157] CTO-SRT-20230118-01A - Ransomware report for December 2022

Quando o LockBit 3.0 foi liberado pela primeira vez em junho, identificamos sobreposições na base de código com um *malware* usado anteriormente como principal binário de *ransomware* da agora extinta operação BlackMatter RaaS. Ao estudar essas sobreposições, encontradas inicialmente nas funções de abertura, concluímos que o LockBit 3.0 era quase idêntico ao BlackMatter, como, por exemplo, nas verificações de idioma para códigos de países específicos, na implementação de criptografia e na técnicas anti-análise.[158] As sobreposições técnicas eram tantas que nós, juntamente com outros pesquisadores, avaliamos que a semelhança é provavelmente resultado da aquisição do código-fonte do BlackMatter pelo White Janus[159] – o que acabou sendo confirmado pelo porta-voz do White Janus em uma entrevista de julho de 2022[160].

BlackMatter como BlackCat

O White Janus (também conhecido como LockBit) não foi o único agente de ameaça com capacidades sobrepostas ao BlackMatter em 2022. Em dezembro de 2021, surgiu o agente *ransomware* ALPHV-ng, cujo logotipo fez com que muita gente o batizasse como BlackCat. Começamos a rastreá-lo como White Dev 101 e rapidamente encontramos conexões com o BlackMatter.[161] Com base nas expressivas sobreposições de código entre os binários BlackMatter e White Dev 101, avaliamos que os desenvolvedores do primeiro provavelmente evoluíram suas operações para estabelecer a marca ALPHV-ng após o encerramento de suas operações em novembro de 2021.[162] Se, por um lado, o White Janus dominou a atividade de sites de vazamento de *ransomware* com um número desproporcionalmente maior de vítimas (907) ao longo de 2022, o White Dev 101 vazou o segundo maior número (228), seguido pelo Blue Cronus (também conhecido como Conti) (177) e pelo White Dev 115 (também conhecido como BlackBasta) (139).[163]

[158] CTO-TIB-20220916-02A - LockBit evolves…sort of
[159] 'LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities', Trend Micro, https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant-- lockbit-3-.html (25 de julho de 2022)
[160] 'RHC interviews LockBit 3.0. "The main thing is not to start a nuclear war"', Red Hot Cyber, https://www.redhotcyber.com/en/post/rhc-interviews-lockbit-3-0-the-main-thing-is-not-to-start-a-nuclear-war/ (26 de julho de 2022)
[161] CTO-TIB-20220121-03A - White Dev 101 does not Rust on its laurels
[162] 'The R Word: Retelling the Recent Rise and Resurgence of Resilient Ransomware-as-a-Service Operators', PwC Threat Intelligence, https://www.youtube.com/watch?v=pZ3tyhL61rI (2 de agosto de 2022)

Após o lançamento do LockBit 3.0, em setembro de 2022, o White Janus sofreu um revés envolvendo um "suposto *insider* descontente", que vazou o construtor para o LockBit Black, o criptografador 3.0 do White Janus.[164] Ao testarmos o construtor independentemente, confirmamos que ele gerou binários LockBit 3.0 funcionais e decodificadores válidos, e que os binários acionaram nossas regras de detecção tanto para LockBit 3.0 quanto para BlackMatter[165]. A disponibilidade do construtor LockBit 3.0 certamente reduziu as barreiras à entrada para agentes de ameaças menos sofisticados estreantes no *ransomware* ou que buscavam mais amplamente evitar atribuições. A partir de outubro de 2022, vimos um declínio no ritmo das operações do White Janus – provavelmente uma consequência do vazamento do construtor LockBit 3.0.

Em 2022, notamos também um padrão em que indivíduos experientes, habilidosos e bem-sucedidos passaram das operações RaaS, em processo de dissolução, para outras oportunidades no ecossistema de crimes cibernéticos.

A maturação desse processo nos últimos anos resultou no desenvolvimento de um modelo semelhante ao empresarial, em que pessoas levaram consigo seu conhecimento e *expertise,* enquanto mudavam entre as operações RaaS. Sua influência ficou clara à medida que os grupos *ransomware* surgiam, fragmentavam-se e passavam por processos de *rebranding*. O lançamento do LockBit 3.0 não seguiu esse padrão, o que avaliamos ser provavelmente um indício de uma mudança emergente no modelo RaaS, por meio da qual tecnologias e bases de código são reaproveitadas ou adquiridas de imediato.[166]

Uma defesa eficaz contra ameaças de *ransomware* em constante evolução requer uma abordagem dupla. As empresas têm de utilizar estruturas de prontidão para detectar *ransomware* e, assim, construir uma estratégia que seja independente de ameaças específicas. Ao mesmo tempo, elas precisam formatar um entendimento dos precursores e bases de código subjacentes, que alimentam as ameaças já conhecidas, criando oportunidades para simplificar a detecção e mitigação

Uma profissionalização nada bem-vinda dos programas RaaS

Diversos agentes de ameaças de *ransomware* profissionalizaram ainda mais seus programas RaaS em 2022, apontando que esse cenário supersaturado fez com que eles empregassem novas táticas para superar seus concorrentes, enquanto encontravam novas formas de coagir e extorquir suas vítimas, as quais, por sua vez, também conseguiram aprimorar sobremaneira suas respostas e medidas de segurança.

[164] 'LockBit ransomware builder leaked online by "angry developer"', Bleeping Computer, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-builder-leaked-online-by-angry-developer-/ (21 de setembro de 2022)
[165] CTO-SRT-20221019-01A - Ransomware report for September 2022
[166] CTO-TIB-20220916-02A - LockBit evolves

Programa de recompensa por bugs e bancos de dados pesquisáveis

Em setembro de 2022, o White Janus (também conhecido como LockBit) anunciou o primeiro pagamento de seu programa de recompensa por *bugs*, supostamente no valor de 50.000 dólares. O *bug* descoberto teria permitido a descriptografia de arquivos criptografados pelo *ransomware* do agente de ameaça[167]. Até meados daquele ano, tanto o White Janus quanto o White Dev 101 (também conhecido como ALPHV-ng e BlackCat) adicionaram funcionalidades de pesquisa a seus sites de vazamento, permitindo que visitantes pesquisassem dados de suas vítimas.[168]

Táticas de alta pressão nas negociações de ransomware

Analisamos as comunicações vazadas atribuídas ao grupo de *ransomware* Conti, que revelou operações maduras e de alta pressão em que o agente de ameaça lucrou em cima das comunicações diretas com suas vítimas ou seus representantes nas negociações. Esses vazamentos também contribuíram para nosso entendimento sobre a estabilidade das operações de *ransomware* atribuídas ao agente que rastreamos como Blue Cronus, Conti e Emotet. Identificamos táticas usadas contra as vítimas, entre as quais:

- Funcionários do Conti frequentemente fazem referência a uma contagem regressiva associada com o agendamento do vazamento de dados das vítimas;
- Eles fornecem "provas" de suas invasões por meio de postagens ocultas em blogs contendo informações das vítimas e configurações de diretórios de arquivos;
- Eles oferecem descontos para as vítimas que pagam resgates rapidamente e sem negociação;
- Eles estimam o valor dos dados roubados e os custos de remediação em comparação com o total solicitado na forma de pagamento de resgate e compartilham-a com suas vítimas; e
- Eles ameaçam contatar os clientes, sócios e investidores de suas vítimas.[169]

Operações e atualizações do Blue Cronus

Em 25 de fevereiro de 2022, um dia após a invasão da Ucrânia pela Rússia, o Blue Cronus – agente de ameaça por trás do grupo de *ransomware* Conti, que havia sido anteriormente rastreado como White Onibi – soltou notas públicas em apoio às ações russas. Em seguida, entre 27 de fevereiro e 2 de março, uma conta no Twitter divulgou uma série de dados internos associados às operações do Blue Cronus, revelando detalhes sem precedentes e maquinações internas por meio de mais de 100.000 mensagens trocadas arquivadas em aplicativo, que remontavam a junho de 2020. Após examinar suas comunicações e operações, descobrimos que o White Magician (também conhecido como TrickBot, Bazar e Anchor), o White Onibi (também conhecido como Conti e Ryuk) e o White Taranis (também conhecido como Emotet) eram essencialmente partes componentes da mesma organização criminosa, que designamos como Blue Cronus em março de 2022.[170]

[167] CTO-SRT-20221019-01A - Ransomware report for September 2022
[168] 'Experts concerned about ransomware groups creating searchable databases of victim data', Recorded Future, https://therecord.media/experts-concerned-about-ransomware-groups-creating-searchable-databases-of-victim- data/ (14 de julho de 2022)
[169] CTO-SIB-20220324-01A - Negotiation tactics and internal dynamics
[170] CTO-QRT-2022-20220315-02A - In the leak midwinter

As revelações e posteriores análises sobre as operações do Blue Cronus não o desaceleraram, apesar de uma aparente e gradual retirada de cena e dissolução da marca Conti. Em abril de 2022, o BlackBasta – agente de ameaça de *ransomware* que rastreamos como White Dev 115 – iniciou operações com posts na língua russa nos fóruns de cibercriminosos como Exploit e XSS. Além de o Blue Cronus usar o Qakbot como mecanismo de entrega, o White Dev 115 também utilizou consistentemente esse *malware* para obter acesso inicial às redes de suas vítimas. Desde então, acreditamos que é altamente provável que o White Dev 115 faça parte do portfólio de variantes de *ransomware* da Blue Cronus.[171]

Precursores em análise

Os cibercriminosos se mantiveram na posição de ser alguns dos agentes de ameaça mais ágeis e em constante evolução, especialmente ao responder a práticas aprimoradas de segurança implementadas em toda a indústria, e isso se refletiu na atividade precursora observada em 2022.

Uma forte tendência do ano passado pode ser vista na resposta que alguns criminosos cibernéticos deram à implementação, em julho de 2022, da política da Microsoft para bloquear macros por padrão em documentos do MS Office baixados da Internet,[172] o que será detalhado mais à frente na seção – Insights e tendências dos ataques: sem macros, sem problemas? Os agentes de ameaças por trás do Bumblebee (Blue Cronus), do IcedID (White Khione) e do Qakbot (White Horoja) desenvolveram soluções alternativas para contornar as mudanças implementadas pela *big tech*, resultando em processos de ataque mais personalizados e sofisticados. Eles envolvem múltiplos estágios que usam uma combinação de arquivos ISO e LNK para instalar e executar seus carregadores de *malware* nas máquinas das vítimas.[173]

Bumblebee

No primeiro semestre de 2022, surgiu o carregador inicial de *malware* conhecido como Bumblebee, desenvolvido pelo Blue Cronus para substituir o TrickBot e o BazarLoader. Ele rapidamente se tornou uma ferramenta altamente eficaz usada em ataques de *ransomware*, com técnicas avançadas anti-virtualização e capacidade de entregar kits pós-exploração como o Metasploit ou Cobalt Strike. O Bumblebee é quase exclusivamente entregue por meio de ataques de *phishing,* muitas vezes em *threads* de e-mails e mensagens sequestrados para parecerem mais legítimos às vítimas, disfarçando-se como faturas, convites para reunião e outros documentos destinados a obter respostas. Os e-mails ainda têm "senhas pessoais" para os seus alvos, atraindo-os a abrir um arquivo ZIP malicioso protegido por senha ou um arquivo ISO. Quando a vítima abre o tal arquivo malicioso, o Bumblebee é carregado em sua máquina por meio de um arquivo LNK.[174]

IcedID

O IcedID é um *trojan* bancário transformado em um sistema de entrega de *malware* que atribuímos ao White Khione. Ele é usado por diversos agentes de ameaça como ponto inicial de entrada em um sistema ou rede de determinada vítima. Em 2022, após a implementação do bloqueio padrão de macros pela Microsoft, o White Khione atualizou o IcedID para que se afastasse das maliciosas planilhas Excel com macros em favor de arquivos ISO. Eles foram combinados com a popular campanha de *phishing "Fake Legal Threat"* do White Khione, que tem sido usada direto para entregar suas cargas úteis.

---

[171] CTO-SIB-20221222-01A - Blue Cronus and Black Basta
[172] 'Macros from the internet will be blocked by default in Office', Microsoft, https://learn.microsoft.com/en- us/deployoffice/security/internet-macros-blocked (11 de outubro de 2022)
[173] CTO-TIB-20221014-01A - ISO-lemnly swear, that we are up to no good
[174] CTO-TIB-20220729-02A - New Queen of the APIary

Qakbot

O Qakbot (também conhecido como Qbot ou Pinkslipbot) é controlado pelo agente de ameaça que rastreamos como White Horoja e está em operação desde 2007. Nascido como um *trojan* bancário, ele começou a evoluir em 2021 para um kit completo de ferramentas modulares para *malware*, ostentando capacidades de carregador, um empacotador personalizado, salvaguardas *anti-sandbox* e técnicas *anti-debug*. Ainda que o Qakbot continue a ser entregue por meio de ataques de *phishing* que aproveitam iscas de todo tipo, ele se afastou do uso de arquivos Office habilitados para macros para ser incorporado dentro de MSIs maliciosos e embalados em arquivos ZIP protegidos por senha.[175]

Reativação do White Taranis pelo Blue Cronus

O White Taranis (também conhecido como Emotet) ressurgiu no final de 2021 após ser reativado pelo Blue Cronus. No primeiro semestre de 2022, suas operações prosseguiram em ritmo constante, com breves pausas para implementar atualizações em sua infraestrutura C2, seu motor de spam e suas capacidades de reconhecimento de sistema.[176] O Blue Cronus também reviveu algumas funcionalidades antigas, incluindo seu mecanismo de roubo de credenciais de pagamento por cartão de crédito.[177] Assim como outros membros do grupo em torno do Blue Cronus, o encerramento da operação de *ransomware* Conti não teve impacto imediato nas campanhas do White Taranis. Contudo, em meados de julho, suas operações pararam abruptamente e continuaram inativas até o início de novembro. Foi então que as campanhas foram retomadas com força total, com cargas úteis na forma de documentos maliciosos da Microsoft que continham macros para baixar e executar um binário White Taranis nas máquinas das vítimas.

Depois que a Microsoft mudou o seu padrão para macros, o Blue Cronus procurou contornar essa proteção instruindo os destinatários a copiar anexos maliciosos para sua pasta *"Templates"* e abrir documentos a partir desse local. Essa ação removia o recurso de segurança Mark of the Web (MotW) do documento malicioso e, uma vez aberto, o arquivo não abriria mais na Visualização Protegida, permitindo assim que macros fossem executadas e instalassem o binário Emotet.[178] Ainda resta saber se o agente persistirá com essa técnica ou mudará para os métodos usados pelo Blue Cronus para entrega do Bumblebee e do IcedID.

[175] CTO-TIB-20220525-01A - Duck, Duck, Bot: Qakbot evolves!
[176] CTO-TIB-20221104-01A - More modules, More Problems
[177] CTO-QRT-20220728-01A - You can't keep a good botnet down
[178] CTO-QRT-20221103-01A - Emotet resumes operations

Métodos de detecção para técnicas comuns vistas nas campanhas Bumblebee, Qakbot e IceID

Ao usar carregadores, esses agentes de ameaça convergiram para um caminho de ataque eficaz com pequenas variações a cada campanha. Independentemente delas, esses caminhos têm pontos em comum (nós interseccionados). Justamente neles que podemos construir detecções e identificar evidências de uma possível atividade maliciosa.

Temos visto os agentes ofertando links do Microsoft OneDrive ou do Google Drive para persuadir usuários a realizar downloads de arquivos compactados. Essa estratégia se mostra eficaz porque esses domínios são permitidos na maioria das organizações. Como alternativa, eles usam uma técnica chamada contrabando HTML, que se dá quando um arquivo HTML malicioso é entregue a um usuário com uma solicitação *(prompt)* para que seja aberto. O arquivo em questão contém uma carga útil embutida e ofuscada e, usando JavaScript, o navegador o monta e o grava na máquina do usuário. Com um registro de um usuário a receber um anexo de e-mail de um único arquivo HTML, uma detecção encadeada pode ser construída com base na subsequente execução do HTML por um navegador, onde o arquivo se origina do diretório de downloads do usuário.

Como mencionado anteriormente, arquivos protegidos por senha são populares entre os agentes de ameaça. Se uma empresa analisa suas ferramentas de arquivamento e extrai parâmetros da linha de comando associados à descriptografia, detecções informativas podem ser construídas para um usuário que esteja descompactando um arquivo criptografado no disco. Tais arquivos frequentemente conterão um ISO, que, uma vez montado, apresenta atalho com argumentos de lançamento para executar uma carga útil. O uso de cargas DLL tem também crescido em popularidade, e assim os agentes de ameaça procuram abusar dos binários do sistema como o `rundll32.exe` para executar carga útil. Ações de detecção que procurem por um `rundll32.exe` carregando uma DLL em uma unidade que não seja a C:\ são geralmente robustas. Diante disso, os invasores tentam enviar uma cópia legítima do `rundll32.exe` para realizar a mesma ação. Para detectá-la, as organizações podem buscar sua execução fora do diretório System32 ou, caso tenha sido renomeado, construir detecções para argumentos da linha de comando que são exclusivos do binário com a ausência do nome do processo.

Após a execução, verificamos cargas úteis a tentar desativar rapidamente os recursos do Windows Defender e adicionar exclusões para si mesmas. Em resposta a esses padrões de comportamento, foram criadas assinaturas para as alterações de registro que essas cargas maliciosas fazem no sistema para impor mudanças de configuração.

Hackers, fraudadores e ladrões

Da mesma forma que os criminosos cibernéticos realizaram mudanças rápidas para enfrentar as configurações padrão de macros da Microsoft em 2022, outros agentes de ameaça se mostraram ágeis em suas táticas para evitar a autenticação multifator (MFA). À medida que eles encontravam cada vez mais essas proteções, aumentou a demanda por capacidades de desvio da MFA, com táticas de fadiga, ladrões de credenciais modificados e ofertas aprimoradas de *phishing* como Serviço (PHaaS).

Agentes de ameaças com outras motivações tentaram igualmente escapar da MFA, o que será detalhado mais adiante – Insights e tendências dos ataques: mais MFA, mais evasão.

O LAPSUS$ em julgamento

O grupo de extorsão e ladrão de dados que rastreamos como White Dev 111 (também conhecido como LAPSUS$ Group) ganhou notoriedade internacional graças aos vários ataques de alto perfil que perpetrou contra grandes organizações, como a Samsung, NVIDIA e Microsoft, e também por reivindicações de violações da Okta, Uber e Rockstar. Para isso[179], ele utilizou engenharia social, fadiga MFA e outros ataques que exploram o elemento humano e fazem uso de táticas de *smash-and-grab*. O agente de ameaça surgiu pela primeira vez em dezembro de 2021, após ter comprometido com sucesso o Ministério da Saúde do Brasil,[180] alegando ter roubado 50 TB de dados. Por meio de um canal no Telegram, o White Dev 111 anunciou suas vítimas e postou anúncios de recrutamento para "funcionários/*insiders*" em várias grandes empresas de tecnologia, jogos e telecomunicações solicitando acesso aos seus logins "VPN ou Citrix".[181]

Por mais que vários países tenham prendido adolescentes supostamente afiliados às operações do White Dev 111, [182, 183, 184] as TTPs e motivações dele ainda preocupam organizações em todo o mundo.

Mentirosos, trapaceiros e ladrões

*Malware*s que roubam credenciais prosperaram na economia informal, com sistemas como RedLine,[185] Raccoon[186] e Vidar[187] dominando o mercado. Isso se deu em grande parte porque os desenvolvedores dos ladrões de informações (também conhecidos como *infostealers)* ajustaram suas ferramentas em meio a um salto no número de empresas implementando MFA para proteger seus ambientes.

---

[179] CTO-QRT-20220920-01A - Uber and Rockstar breaches
[180] 'Brazil health ministry website hit by hackers, vaccination data targets', Reuters, https://www.reuters.com/technology/brazils-health-ministry-website-hit-by-hacker-attack-systems-down-2021-12-10/ (10 de dezembro de 2022)
[181] CTO-TIB-20220406-01A - LAPSUS$ Group has entered the chat
[182] 'Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal', BBC News, https://www.bbc.com/news/technology-60864283 (24 de março de 2022)
[183] 'UK police arrest teenager suspected of Uber, GTA 6 hacks', TechCrunch, https://techcrunch.com/2022/09/26/london-police-arrest-uber-rockstar/ (26 de setembro de 2022)
[184] 'PF prende brasileiro suspeito de integrar organização criminosa internacional', Ministério da Justiça e Segurança Pública, https://www.gov.br/pf/pt-br/assuntos/noticias/2022/10/pf-prende-brasileiro-suspeito-de-integrar-organizacao-criminosa-internacional (19 de outubro de 2022)
[185] CTO-TIB-20220209-01A - The Rise of RedLine
[186] CTO-TIB-20220914-02A - Raccoon Stealer 2.0
[187] CTO-TIB-20230113-01A - Vidar Stealer

Ao longo do ano, um número cada vez maior de desenvolvedores de *malwares* que roubam credenciais se aprimoraram ou adicionaram novas capacidades para roubar *cookies* de sessão, o que, em certas circunstâncias, facilitou a evasão da MFA.

Em março, o Raccoon Stealer cessou repentinamente suas operações após os desenvolvedores desse *malware* relatarem que seu líder havia sido morto na Ucrânia durante a invasão russa.[188] Em meados de 2022, eles garantiram à sua base criminosa de clientes que, apesar do enorme contratempo, continuariam a trabalhar no desenvolvimento de uma nova versão do Raccoon Stealer com capacidades aprimoradas. Em outubro, entretanto, o governo dos EUA anunciou que o desenvolvedor líder, um cidadão ucraniano, não tinha sido morto na Ucrânia, mas sim preso pela polícia holandesa em março. Washington acrescentou que a infraestrutura do agente de ameaça havia sido, posteriormente, desmantelada em uma força tarefa de agências de aplicação de leis internacionais, obrigando os desenvolvedores a reiniciar e relançar suas operações.[189]

Phishing com dinamite

Os criminosos cibernéticos continuaram a confiar em táticas de *phishing* testadas e comprovadas, que consistiam em mensagens inteligentes e na dependência da autenticação de fator único. Forçados a se adaptar, vários atores de ameaças aproveitaram serviços gratuitos destinados em grande medida a profissionais de segurança, como o Glitch e o Gophish, que fornecem tanto a infraestrutura quanto as ferramentas para criar e distribuir e-mails de *phishing*, além de desenvolver *landing pages*. Os criminosos envolvidos em ataques de *phishing* também continuaram a demonstrar pouca reserva em se passar por agências governamentais ou de aplicação da lei. Um deles chegou ao ponto de usar a prisão de outro golpista conhecido, o Ramon Abbas (ou `HushPuppi`), para se passar pelo Escritório de Vítimas de Crimes do Departamento de Justiça dos EUA em tentativas adicionais de atacar novos alvos e roubar suas informações financeiras particulares.[190]

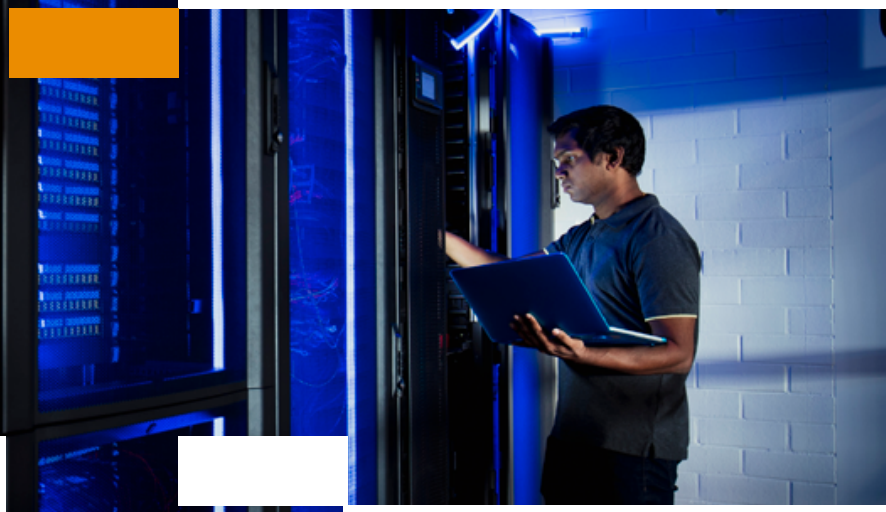
Não apenas uma falha

Criar e manter infraestrutura para realizar ataques de *phishing* é uma operação cara e trabalhosa – e deve ser especialmente frustrante para os agentes de ameaças quando a deles é derrubada por provedores de hospedagem ou bloqueada por navegadores da web. Por isso, eles buscam plataformas e serviços gratuitos que sejam fáceis de operar. O Glitch foi uma dessas plataformas gratuitas de desenvolvimento de software baseada em nuvem que foi usada por criminosos para comprometer e-mails comerciais (BEC) da África Ocidental. Ela tem um plano gratuito que permite aos usuários rapidamente implantar *webapps* públicos com o nome de um host que ela mesma fornece. Os agentes combinaram então o Glitch com um kit de *phishing* mais antigo conhecido como LogoKit para criar páginas de login de webmail falsas e assim capturar credenciais de usuários, que foram, por sua vez, usadas depois para obter acesso às redes das vítimas.[191]

[188] CTO-TIB-20220914-02A - Raccoon Stealer Returns
[189] 'United States of America v. Mark Sokolovsky', US Department of Justice, https://www.justice.gov/usao- wdtx/page/file/1546626/download (26 de setembro de 2022)
[190] 'Nigerian Man Sentenced to Over 11 Years in Federal Prison for Conspiring to Launder Tens of Millions of Dollars from Online Scams', US Department of Justice, https://www.justice.gov/usao-cdca/pr/nigerian-man- sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions (7 de novembro de 2022)
[191] CTO-SIB-20220811-01A - A glitch in the BEC system

Embora não seja particularmente novo, o PHaaS segue como um modelo viável e um recurso útil para os criminosos cibernéticos. Em 2022, um grande número de novos provedores foi visto oferecendo recursos e funcionalidades em demanda, incluindo kits de ferramentas EvilProxy, Caffeine e Robin Banks. O EvilProxy, por exemplo, surgiu em meados do ano como um "adversário no meio" (AitM) entre as vítimas de *phishing* e os portais de login empresarial, e como provedor de uma interface gráfica de usuário (GUI) para personalizar e automatizar as entregas em campanhas de *phishing* – tudo isso por uma reduzida taxa de uso. Assim, o EvilProxy facilita tanto as capacidades de roubo de credenciais e cookies quanto a de contornar a MFA. Não por acaso, ele anunciou sua capacidade de comprometer portais de login de empresas gigantescas, como Google, Microsoft e Linkedin, além de outros serviços.

A funcionalidade *point-and-click* do EvilProxy é um produto em um crescente mercado no ecossistema dos crimes cibernéticos, o que encoraja o desenvolvimento de capacidades sob demanda e baseadas na cobrança de taxas. Além disso, ela reduz ainda mais as barreiras à entrada para que uma ampla gama de agentes de ameaças busque se engajar em ataques.



Insights e tendências dos ataques

Novas tecnologias e vulnerabilidades comuns permearam a dinâmica entre invasores e defensores em 2022 – cada um buscando uma vantagem e destacando a necessidade de defesa. Agentes de ameaças usaram cada vez mais ferramentas e estruturas aprimoradas em seus ataques, além de modificarem suas TTPs para superar as práticas de segurança adotadas pelos defensores. Eles também combinaram essas mudanças com o uso contínuo de métodos testados e comprovados, como explorar instâncias expostas do protocolo de área de trabalho remota (RDP) e sistemas ainda não protegidos com MFA.

Ferramentas e *frameworks*

Vários exemplos de ferramentas e *frameworks* foram discutidos e rastreados em toda a indústria. Observamos ainda um entendimento maior sobre como eles são usados por red teams legítimas e abusadas por invasores mal-intencionados.

No que diz respeito aos defensores, esses *frameworks* oferecem desafios por conta de sua rápida evolução. No entanto, também trazem oportunidades de detecção. Em alguns casos, uma vez que o defensor detecta o uso de um *framework* em particular, outros também podem fazê-lo com a mesma abordagem ou uma semelhante.

Embora alguns *frameworks* tenham ganhado notoriedade em toda a indústria, o Cobalt Strike se manteve como o mais utilizado pós-exploração, adotado por uma ampla variedade de agentes de ameaças. Detectar isoladamente o uso de um *framework* específico continuará, provavelmente, a ser um desafio aos defensores e deverá se tornar mais difícil nos próximos anos.

Detectando o Cobalt Strike

As configurações padrão do Cobalt Strike são bem conhecidas e fáceis de detectar. Por exemplo, o DNS C2 padrão usa ".stage." no nome de domínio. A seguinte regra de detecção de rede procura pelo formato padrão, que normalmente começa com uma consulta por "aaa.stage".*

Rede

```
alert dns any any -> any any (msg:"[PwC] Generic -
CobaltStrike - DNS query for
.stage."; \
    dns_query; content:".stage."; \
    pcre:"/^[a-z]{3}\.stage\.[0-9]+\.(?:[a-z0-9-
    ]+\.)+[a-z]{2,4}$/"; \ classtype:domain-c2; \
    metadata:copyright,Copyright PwC Threat
    Intelligence 2017; metadata:tlp green; \
    metadata:confidence Medium; metadata:efficacy Medium;
    \ metadata:mitre,T1071/004; \
    metadata:author RM; metadata:created 2020-07-07; \
    sid:200100001; rev:2020070701;)
```

Brute Ratel

O Brute Ratel é um *framework* C2 comercial que se tornou bem mais conhecido à medida que passou a ser utilizado por diversos agentes de ameaça.[192] Várias versões dele foram vazadas e quebradas no ano passado. Viu-se que ele pode ser personalizado e estendido com facilidade. Por padrão, o Brute Ratel se gaba de sua variedade de recursos que pode ser usada para evitar detecção, como a Detecção e Resposta de Endpoint (EDR) / antivírus (AV), uma variedade de mecanismos C2 e a execução indireta de APIs.

[192] 'When Pentest Tools Go Brutal: Red-Teaming Tool Being Abused by Malicious Actors', Palo Alto Unit 42, https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/ (5 de julho de 2022)

Detectando o Brute Ratel

Enquanto um defensor, existem vários padrões que permitem a detecção do Brute Ratel, quer seja na memória/em disco – usando, por exemplo, a YARA – quer seja no tráfego de rede que apresenta certificado SSL ou domínio padrão.

YARA

```
rule Brute_Ratel_PE_Badger_API_Loading_Routine : Heu-
ristic_and_General
{
   meta:
     description = "Detects Brute Ratel Badger payloads
     (PE and DLL) based on a unique routine used to dy-
     namically load APIs"
     TLP = "AMBER"
     author = "PwC Threat Intelligence" copyright =
     "Copyright PwCIL 2022 (C)" created_date = "2022-
     09-29"
     modified_date = "2022-09-29"
     revision = "0"
     hash = "4de333f164d70b59849c3aa12a9c95cd-
     cbecae3023386ee08c15b38874260941" hash
     = "dc71c5721fa6b3148a3a0564931dc063d-
     03694ca57aa61e8c2532b5a565b2548" hash = "ef803e-
     a871c974623ceb678548c938826b683c857adc85a6bf8af-
     34c8b61fc52"

   strings:
     // 8B5324     MOV EDX,DWORD PTR [RBX+24]
     // 4D01DB     ADD R11,R11
     // 8B431C     MOV EAX,DWORD PTR [RBX+1C]
     // 4D01D3     ADD R11,R10
     // 410FB71413 MOVZX EDX,WORD PTR [R11+RDX]
     // 498D1492   LEA RDX,[R10+RDX*4]
     // 8B0402     MOV EAX,DWORD PTR [RDX+RAX]
     // 4C01D0     ADD RAX,R10
     $ = {8B53244D01DB8B431C4D01D3410FB71413498D14928B-
     04024C01D0}

   condition:
     all of them
}
```

Rede

```
alert dns any any -> any any (msg:"[PwC] Generic -
Brute Ratel - C2 node evasionlabs[.]com in DNS query";
\
     dns.query; \ content:".evasionlabs.com"; endswith;
     \
     threshold: type limit, track by_src, count 1, sec-
     onds 3600; \ classtype:domain-c2; \
     metadata:copyright,Copyright PwC Threat Intelli-
     gence 2022; \ metadata:tlp green; metadata:confi-
     dence High; metadata:efficacy Low; \ metadata:mi-
     tre,T1071/004; \
     metadata:author RM; metadata:created 2022-09-29; \
     sid:222092910; rev:2022092901;)
```

Sliver

Diferentemente do Brute Ratel, o Sliver é um *framework* de código aberto que permite àqueles que o utilizam uma customização mais fácil. O Sliver dá suporte a uma variedade de mecanismos C2, incluindo Segurança da camada de Transporte (mTLS) e *Wireguard* mútuos, além de *beacon object files* (BOFs), tornando possível reutilizar plugins do CobaltStrike.

Detectando o Silver

A configuração mTLS é codificada e a impressão digital JARM é consistente (`28d28d28d00028d00043d28d28d43d47390d982d099a542ccbc90628951062`). Se um defensor puder inspecionar o tráfego HTTPS, os headers do servidor serão firmes, assim como o formato das solicitações HTTP. O tráfego *Wireguard* também será bastante identificável por assinatura e fácil de detectar no tráfego de rede.

YARA

```
rule Sliver_Protobuf_Symbol : Heuristic_and_General
{

   meta:
     description = “Detects symbol in Sliver implants
     (PE, ELF, Mach-O and shellcode) referencing a cus-
     tom protobuf module”
     TLP = “AMBER”
     author = “PwC Threat Intelligence” copyright =
     “Copyright PwCIL 2022 (C)” created_date = “2022-
     10-18”
     modified_date = “2022-10-18”
     revision = “0”
     hash = “41cf473fe535b932c68e9f295680f-
     e228cde0094a8bac70ccb68c21aaff22188” hash =
     “c12c33111b41bf2be458004d532f1255fd734057d2c7b-
     f59e0877e31dbedfd4e” hash = “3b4c57e04422825609b-
     c70dfa5bf741cded6961df87369b530c45720eee828fd”
     hash = “4c668595d6767e9cdb68f875aab9d4d39ae0ff94d-
     94e76dc301eb336f1d74096” reference = “https://
     github.com/BishopFox/sliver”

   strings:
     $ = “.sliverpb.

   condition:
    // Note, you can remove these file signature checks
    to wider the rule further (
     // PE
     uint16(0) == 0x5A4D or
     // Shellcode
     uint32be(0) == 0x4883e4f0 or
     // Mach-O
     uint32be(0) == 0xcffaedfe or
     // ELF
     uint32be(0) == 0x7f454c46
   ) and
   any of them
}
```

Rede

```
alert udp any any -> any any (msg:"[PwC] Policy - Tun-
nelling - Wireguard VPN client handshake"; flow:from_
client; dsize:148; \
    content:"|01 00 00 00|"; startswith; \
    content:"|00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00|"; endswith; \ flowbits:set,P-
    wC.Policy.Tunnelling.Wireguard; target:s-
    rc_ip; \ reference:md5,b82a587befc34c0db00eed-
    5c4117d88d343b8b895f03fc409a55d9240cf9fde1; \
    classtype:pup-activity; \
    metadata:copyright,Copyright PwC Threat Intelli-
    gence 2022; metadata:tlp green; \ metadata:confi-
    dence High; metadata:efficacy Low; \
    metadata:mitre,T1133; \
    metadata:author RM; metadata:created 2022-05-04; \
    sid:222050432; rev:2022050401;)
```

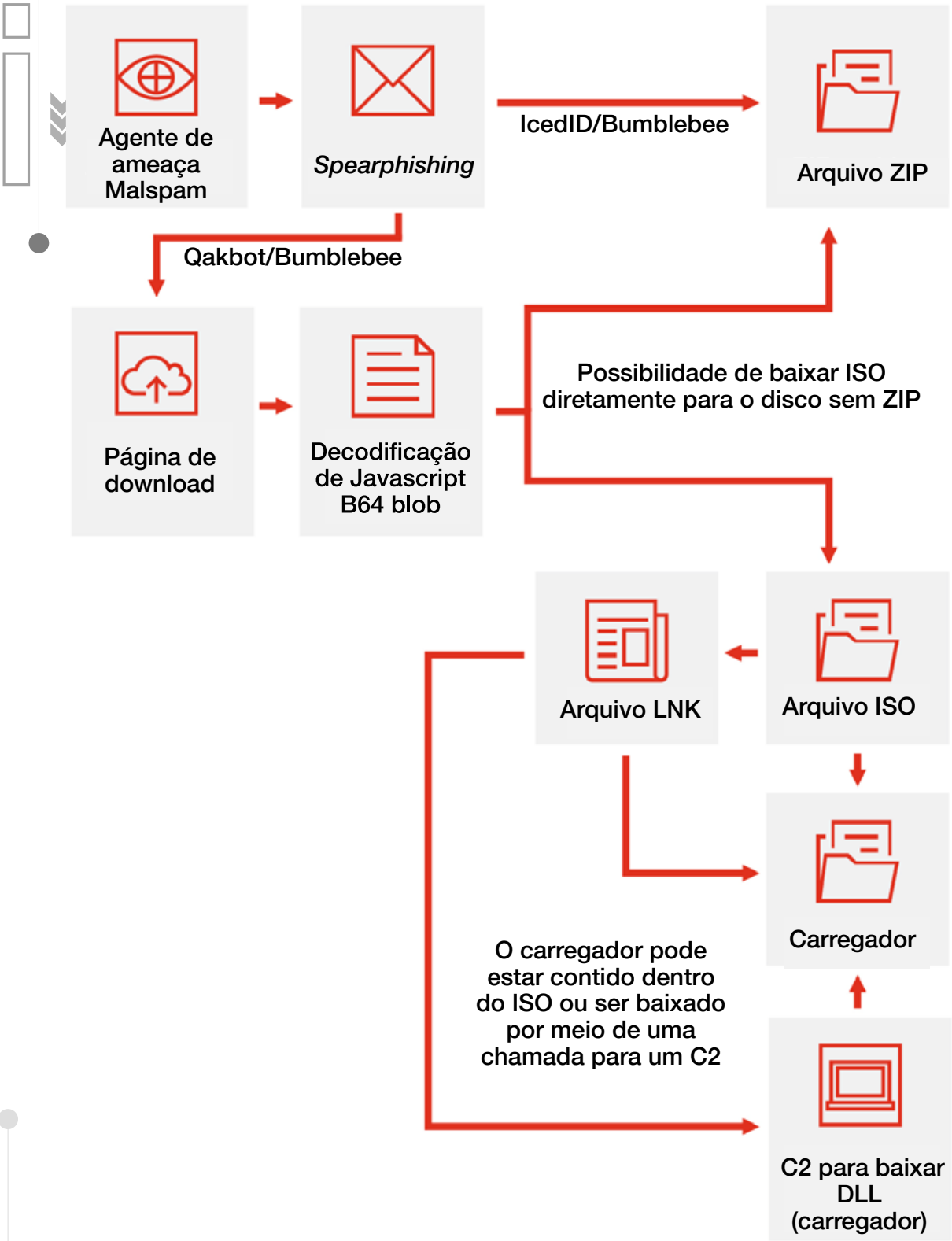
Sem macros, sem problemas?

Os agentes de ameaça historicamente confiaram nas macros para executar os *malwares* que entregam a suas vítimas por meio de documentos maliciosos anexados a e-mails de *phishing*, por exemplo. Sem eles, esses criminosos têm sido forçados a apostar em outros métodos autoexecutáveis – evitando, assim, o máximo possível de interações com as vítimas e a interdição do sistema. Com a atualização da Microsoft em 2022 para desativar o *Mark of the Web* (MotW) por padrão[193], observamos que eles tiveram de adaptar seu *targeting*. Além disso, agentes com diferentes recursos, níveis de sofisticação e motivações passaram a procurar formas alternativas de obter acesso inicial a seus alvos, como se viu em um vetor de infecção que gira em torno do uso de:

- Arquivos ISO (que efetivamente agem como arquivos de arquivamento) para entregar cargas maliciosas; e
- Arquivos LNK (atalho) para se disfarçar como documentos legítimos, que executam cargas maliciosas.

[193] 'Macros from the internet will be blocked by default in Office', Microsoft, https://learn.microsoft.com/en- us/deployoffice/security/internet-macros-blocked (11 de outubro de 2022)

Exemplo de cadeia de infecção usando arquivos ISO + LNK



Detectando arquivos ISO e LNK potencialmente maliciosos

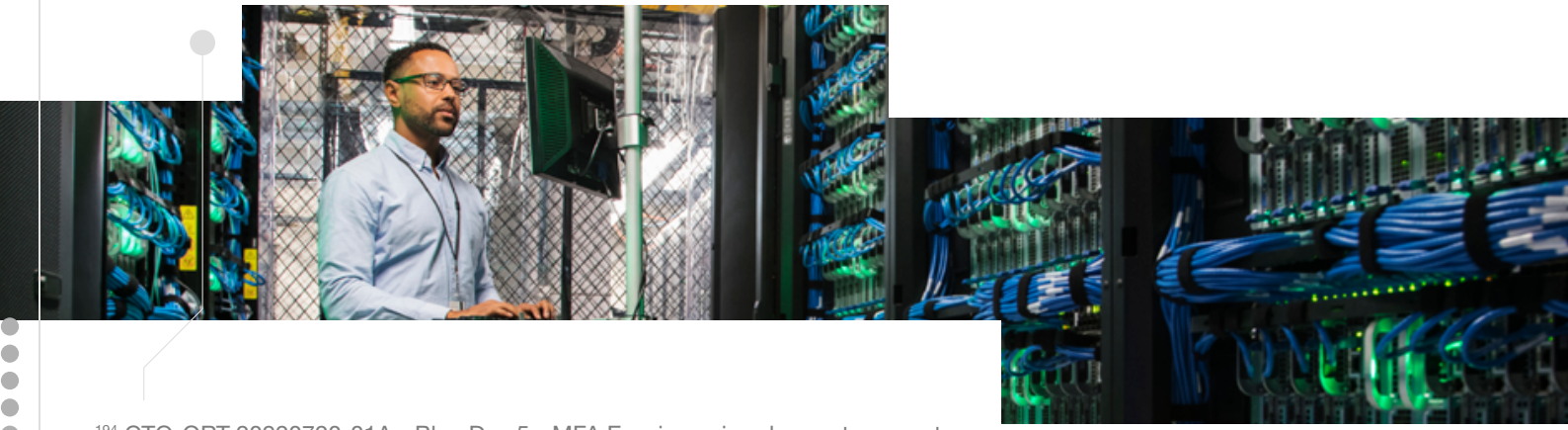
Arquivos ISO servem ao propósito legítimo de replicar uma imagem de disco físico. Para detectar esses arquivos com *malware,* devemos considerar o perfil de um legítimo e procurar desvios nessa linha de base. Por exemplo, em um ambiente corporativo, eles podem ser manipulados por contas administrativas para operações de instalação de software em larga escala. Dessa forma, detecções podem ser feitas para criações de arquivos ISO sob contas de usuário padrão ou arquivos menores. Podemos também criar assinaturas para aplicações comumente usadas de forma mal intencionada que gravam os arquivos no disco. Aplicações particularmente notáveis para criar assinaturas com esse comportamento incluem clientes de e-mail e navegadores da web, pois tendem a ser a principal via de acesso para *phishing.*

Quando um ISO é aberto a partir de um arquivo compactado, os temporários são criados no disco. Portanto, alertas desses eventos podem nos ajudar a detectar os estágios iniciais de um ataque. Esse mesmo mecanismo pode ser usado para detectar arquivos LNK dentro de outros compactados. Para muitas empresas, um LNK em um arquivo compactado pode ocorrer com alguma frequência, de modo que os alertas devem ser correlacionados com outros comportamentos para justificar incidentes. Porém, para algumas organizações, isso por si só já justifica uma análise mais aprofundada, dada sua popularidade entre criminosos.

Mais MFA, mais evasão

À medida que um número cada vez maior de empresas passou a adotar proteções MFA para acesso privilegiado e gerenciamento de acesso à identidade (IAM), os agentes de ameaças passaram a adotar técnicas de evasão. Elas variam da engenharia social, como visto no caso do White Dev 111 empregando ataques de MFA contra suas vítimas, até técnicas de desvio, como aquelas integradas em *malware*s comumente usados por criminosos cibernéticos e agentes mais sofisticados.

Um desses agentes é o Blue Dev 5 (também conhecido como NOBELIUM), o qual analisamos em um caso de resposta a incidentes. Descobrimos na ocasião que o criminoso havia evitado proteções MFA ao explorar uma conta inativa para obter acesso ao ambiente Microsoft Azure Active Directory (AD) da vítima. O Blue Dev 5 se autenticou na conta usando credenciais válidas, com a conta inativa tendo sido criada antes de a vítima implementar a MFA. Ele então inscreveu um novo método MFA, um *token* OATH de software, usando a conta comprometida.[194]



[194] CTO-QRT-20220720-01A - Blue Dev 5 - MFA Evasion using dormant accounts

Lições do incidente de evasão MFA do Blue Dev 5 (também conhecido como NOBELIUM)

Analisamos o incidente incluindo o seguinte indicador de comprometimento (IoC) associado ao Blue Dev 5 encontrado em julho de 2022, que pode ser consultado em logs históricos e adicionado a alertas de detecção:

`198.244.224[.]89`[195]

Recomendamos configurar detecções para inscrições MFA para todos os usuários que não fizeram login por ao menos 14 dias. Fazendo isso, seria possível detectar atividades semelhantes a essas descritas. Além disso, recomendamos impor MFA em ambientes de nuvem da Microsoft com um método de autenticação seguro, como correspondência de números, e identificar de forma proativa as contas que atualmente não têm MFA inscrito, usando, por exemplo, o seguinte comando fornecido pelo Módulo PowerShell do Microsoft Azure AD Incident Response:

`Get-AzureADIRMfaAuthMethodAnalysis`[196]

A nuvem como alvo

Um número crescente de agentes de ameaça está mirando os ambientes em nuvem para fazer vítimas, provavelmente em resposta ao fato de as empresas estarem integrando a tecnologia – terreno fértil para que esses criminosos se aproveitem de vulnerabilidades ou configurações ruins para destravar dados valiosos. No início de 2022, respondemos a um incidente relacionado ao Blue Dev 5, no qual ele ganhou acesso inicial ao ambiente em nuvem da vítima ao conseguir comprometer seu Provedor de Serviços em Nuvem (CSP).[197] Este tinha permissões de Administrador Delegado[198] para o inquilino Microsoft Azure AD e O365 da vítima. Em outras palavras, essa ocorrência efetivamente forneceu acesso ao ambiente em nuvem da Microsoft da vítima.

Graças a esse acesso, o Blue Dev 5 adicionou uma credencial de senha a um Azure AD Service Principal[199] usado por um aplicativo de backup. Isso o permitiu fazer login no ambiente da vítima com as mesmas permissões disponíveis ao aplicativo legítimo. O Blue Dev 5 usou então essas credenciais para se autenticar como o aplicativo de backup e fazer chamadas à API do Exchange Web Service (EWS)[200] para o Exchange Online (O365). Os privilégios abriram a possibilidade de acessar e vazar os e-mails de todas as contas de usuário O365 da vítima.

---

[195] CTO-QRT-20220720-01A - Blue Dev 5 - MFA Evasion using dormant accounts
[196] 'Azure AD Incident Response PowerShell Module', Microsoft, https://github.com/AzureAD/Azure-AD-Incident- Response-PowerShell-Module
[197] 'What is a cloud service provider', Microsoft, https://azure.microsoft.com/en-us/resources/cloud-computing- dictionary/what-is-a-cloud-provider/
[198] 'Delegated admin privileges in Azure AD', Microsoft, https://learn.microsoft.com/en-us/azure/active- directory/enterprise-users/directory-delegated-administration-primer (12 de março de 2023)
[199] 'Application and service principal objects in Azure Active Directory', Microsoft, https://learn.microsoft.com/en- us/azure/active-directory/develop/app-objects-and-service-principals (15 de dezembro de 2022)
[200] 'Explore the EWS Managed API, EWS, and web services in Exchange', Microsoft, https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/explore-the-ews-managed-api- ews-and-web-services-in-exchange (13 de junho de 2022)

Lições do incidente de comprometimento CSP do Blue Dev 5 (também conhecido como NOBELIUM)

Embora avaliemos que os seguintes IoCs analisados não estejam mais em uso, optamos por fornecê-los mesmo assim para auxiliar na consulta de *logs* históricos e alertas:

`193.8.172[.]208` - Visto em julho de 2021 até agosto de 2021
`18.130.157[.]66` - Visto em julho de 2021
`18.169.208[.]15` - Visto em janeiro de 2022 até fevereiro de 2022
`79.143.87[.]14` - Visto em março de 2022[202]

Adicionalmente, esse caso nos permitiu desenvolver uma série de recomendações para fortalecer os ambientes Microsoft Azure AD e O365 contra o Blue Dev 5 e outros agentes de ameaças que utilizam TTPs semelhantes, como:

- Remover permissões de Administrador Delegado das relações com parceiros com provedores de serviços gerenciados (MSPs) e outras partes ou usar *Granular Delegated Administrator Privileges* [203] para permitir apenas acesso administrativo limitado e temporário a terceiros quando estritamente necessário;
- Configurar métodos fortes de MFA para todos os usuários (por exemplo, notificações push com correspondência numérica);[204]
- Embarcar logs do Azure AD e O365 em um SIEM existente ou uma nova implantação do Microsoft Sentinel;
- Configurar regras de detecção para técnicas comumente usadas para comprometer o Azure AD e O365;
- Auditar e proteger o uso de contas privilegiadas no Azure AD e O365;
- Auditar os Azure AD Service Principals e aplicativos para credenciais e permissões sensíveis e monitorar seu uso contínuo; e
- Proteger os Service Principals com uso de regras de Acesso Condicional[205] para restringir logins em Service Principals sensíveis a uma lista permitida de endereços IP.[206]

Insights adicionais de nossos casos de resposta a incidentes

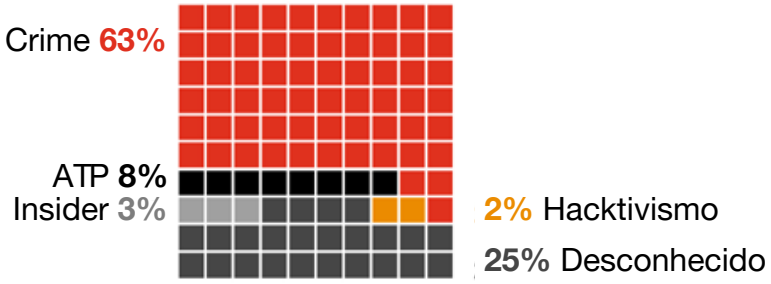
Para além dos casos de resposta a incidentes já destacados, analisamos nosso conjunto mais amplo de dados para obter tendências e insights adicionais. Em 2022, 63% dos casos que avaliamos resultaram de ataques realizados por agentes de ameaças que eram motivados financeiramente, e quase metade deles envolveu ataques de *ransomware*. Quando olhamos especificamente para esses últimos, notamos que os três principais setores impactados foram manufatura, construção civil e varejo – em conformidade com as tendências mais amplas que observamos a partir dos dados do site de vazamento de *ransomware* no decorrer do ano.

De todos os casos de resposta a incidentes que analisamos, os cinco setores mais impactados foram os de serviços profissionais, serviços financeiros, transporte e logística, varejo e manufatura.

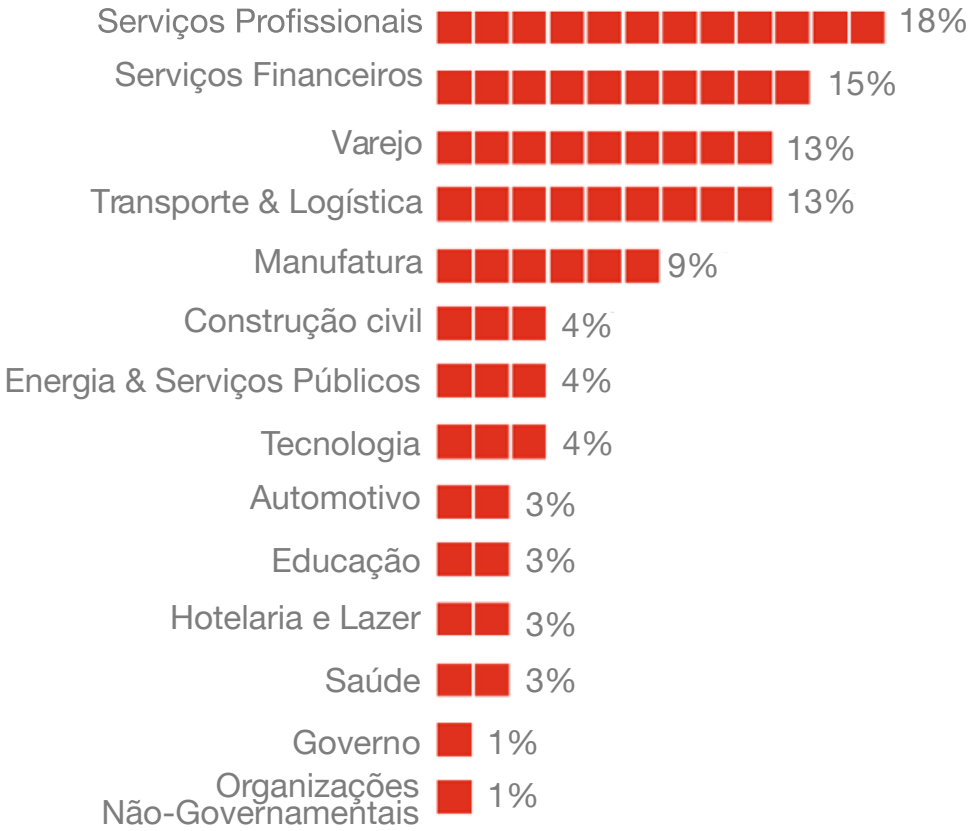
[201] CTO-TIB-20220429-01A - Bearing down on the Clouds
[202] CTO-TIB-20220429-01A - Bearing down on the Clouds
[203] 'Introduction to granular delegated admin privileges (GDAP)', Microsoft, https://docs.microsoft.com/en- us/partner-center/gdap-introduction (8 de agosto de 2022)
[204] 'How to use number matching in multifactor authentication (MFA) notifications (Preview) - Authentication Methods Policy', Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa- number-match (30 de novembro de 2022)
[205] 'Conditional Access for workload identities preview', Microsoft, https://docs.microsoft.com/en-us/azure/active- directory/conditionalaccess/workload-identity (21 de novembro de 2022)
[206] CTO-TIB-20220429-01A - Bearing down on the Clouds

Não conseguimos determinar uma motivação para cerca de um quarto de todos os casos, o que superou os 7,5% dessas ocorrências em 2021. Isso se deve provavelmente aos esforços de detecção e resposta acontecendo mais cedo no ciclo de vida da invasão, mas possivelmente também tem relação com tendência que vimos entre os agentes de ameaças de cada vez mais usarem capacidades e ferramentas compartilhadas e aprimorarem seus TTPs.

Casos de resposta a incidentes que analisamos por tipo de agente de ameaça em 2022



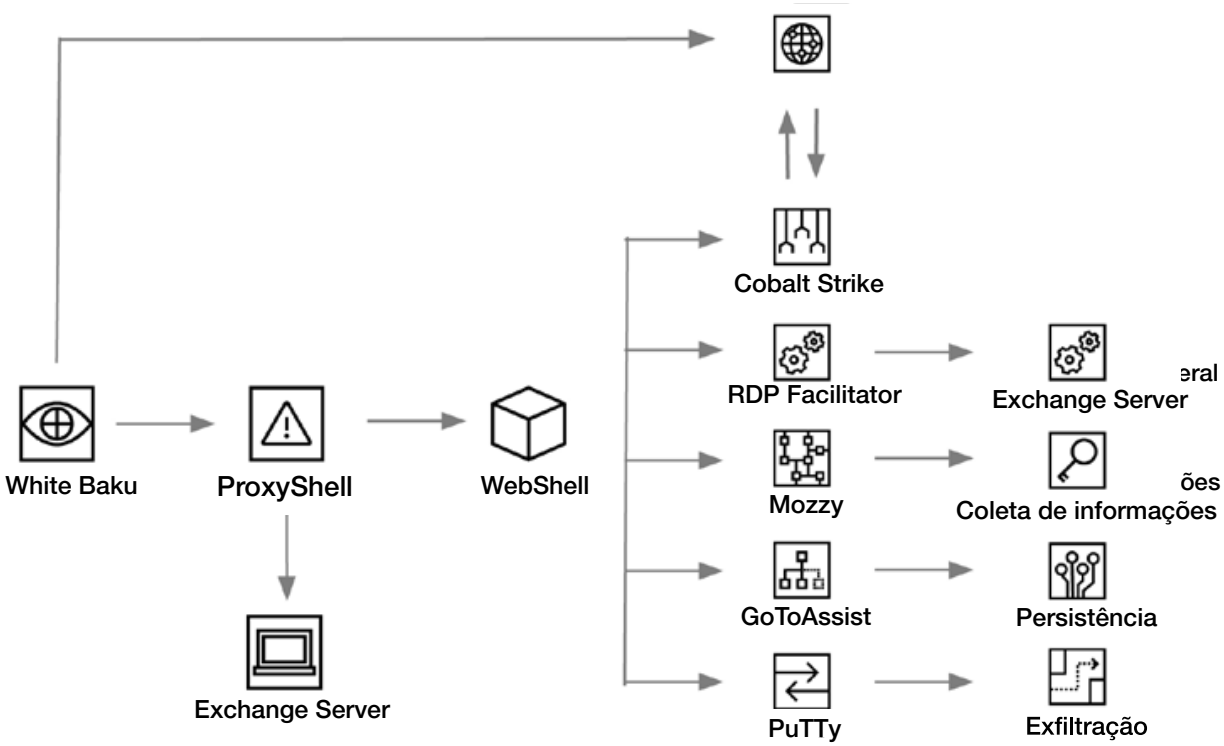
Casos de resposta a incidentes que analisamos por setor em 2022



É imperativo que as organizações gravem e mantenham o máximo de telemetria possível de toda a pilha de segurança, pois ser capaz de revisar metadados históricos de rede, ou de atividade do *host*, ajudará àqueles que devem responder aos incidentes a entender o impacto de um ataque não detectado na hora. Os volumes de dados para tipos de *log* de chave e telemetria são relativamente baixos e adequados para armazenamento do tipo "arquivamento de longo prazo".

Estudo de caso do White Baku

Respondemos em março a um incidente envolvendo o White Baku, o agente de ameaça por trás do *ransomware* Cuba.[207] Ele obteve acesso inicial à vítima ao explorar vulnerabilidade ProxyShell e instalar webshells nos servidores Microsoft Exchange – em conformidade com outros incidentes públicos de *ransomware* que lhe foram atribuídos. Ele então usou o Cobalt Strike para estabelecer Comando e Controle (C2) e fazer uma movimentação lateral, instalando o Mozzy – um *malware* personalizado projetado para coletar informações sobre o EDR da vítima – e o RDP Facilitator – um *malware* usado para configurar backdoors para facilitar o RDP. Para reforçar sua posição na rede da vítima, o White Baku instalou a ferramenta de suporte remoto GoToAssist. Para coleta e vazamento de dados, o agente instalou o WinRAR para compactar arquivos e o PuTTY Secure Copy (PSCP) para a tarefa de transferir arquivos e vazar dados. Assim, foi possível que ele roubasse arquivos de sua vítima antes da criptografia do sistema. Finalmente, ele usou o PsExec para implantação final do *ransomware.*



[207] CTO-TIB-20220608-01A - White Baku grabs a foothold

Lições do incidente do White Baku (também conhecido como Cuba) envolvendo ProxyShell

Obtivemos insights a partir de vários aspectos do incidente do White Baku, abrangendo várias etapas de sua cadeia de ataque e estratégias potenciais de detecção e mitigação.

Acesso inicial: a detecção de atividades pouco usuais originadas em processos de servidores web, como o ProxyShell, ou de escritas incomuns vindas desses processos, é a principal estratégia para identificar atividades de *web shell* em geral. Esse é, com frequência, o primeiro ponto de acesso do invasor à rede, seguido pelo aprendizado acerca do ambiente da vítima. Os profissionais encarregados da defesa podem procurar por processos "filhos" e comandos associados à descoberta de redes que podem revelar atividades suspeitas.
MITRE ATT&CK T1505.003 - Server Software Component: Web Shell

Persistência: é fundamental monitorar a instalação de ferramentas de acesso remoto (por exemplo, GoToAssist) não apenas por causa das detecções simples que podem ser implementadas, mas também porque elas geralmente são instaladas logo nas primeiras etapas de um ataque. Com um entendimento sobre ferramentas administrativas remotas aprovadas pela política de permissão, regras de detecção podem ser criadas para que busquem as comuns que estejam fora dessa lista. Caso um invasor astuto instale justamente ferramentas administrativas remotas aprovadas, as detecções podem ser construídas para identificar instalações anômalas, como as que ocorrem no espaço do usuário ou conduzidas por contas inesperadas. Além desse monitoramento, os profissionais de defesa também podem procurar por linhas de comando específicas do processo de instalação, pois algumas ferramentas usam instaladores com *flags* que deveriam levantar suspeitas. Alguns exemplos são uma *flag* silenciosa – ou seja, sem interface do usuário (UI) para instalação –, que impeça a visibilidade do usuário para uma ação em andamento, ou uma *flag* que adicione o programa na lista do "Inicializar", o que é também bastante incomum para ferramentas de suporte remoto.
MITRE ATT&CK T1219 - Remote Access Software

Movimentação Lateral: a PsExec é uma ferramenta altamente popular entre os agentes de *ransomware*. Destinada à gestão à distância, a capacidade de a PsExec executar códigos em sistemas remotos via Server Message Block (SMB) é ideal para propagação de *ransomware*. Se não for uma ferramenta administrativa autorizada, os profissionais de defesa conseguem monitorar qualquer execução da PsExec. Usuários que realizam execuções legítimas podem ser simplesmente orientados a meios alternativos de gerenciamento à distância. Ela é também renomeada com frequência por adversários. Esse é geralmente um sinal de que há um invasor tentando evitar uma detecção à procura por seus parâmetros exclusivos na linha de comando, ou pelo artefato no registro associado à aceitação do contrato de licença do usuário final (EULA) na ausência do nome padrão do processo. Se a PsExec é largamente utilizada pelos administradores na rede, então uma lógica mais complexa terá de ser implantada para identificar suas atividades. Essa ferramenta também é construída como um recurso de movimentação lateral de ferramentas pós-exploração, como o Metasploit e a Cobalt Strike – cada uma implementa a PsExec de maneiras ligeiramente diferentes. Detecções devem ser construídas para monitorar os processos de cada uma. Os profissionais de defesa devem usar expressões regulares para capturar o aleatório que essas ferramentas tentam injetar na operação. MITRE ATT&CK T1021.002 - Remote Services: SMB/Windows Admin Shares

Coleta: mais uma vez, é importante enfatizar que, por mais que ferramentas de compressão como o WinRAR e outras sejam perfeitamente legítimas, elas também são usadas por criminosos cibernéticos e por ameaças persistentes avançadas. Detectar quando elas são baixadas ou instaladas em pastas específicas, como a %TEMP%, pode ser uma heurística útil para identificar atividades suspeitas que podem ser sinalizadas para revisão. MITRE ATT&CK T1560.001: Archive Collected Data: Archive via Utility

Exfiltração: da mesma forma que as ferramentas de compressão usadas para coleta, agentes que facilitam o vazamento (exfiltração) de dados via ferramentas legítimas de transferência de arquivos, como a PuTTY Secure Copy (PSCP),que também podem se misturar a atividades legítimas. Para diferenciar essa exfiltração, pode ser útil alertar especificamente sobre origens, destinos e volumes de transferências de dados de saída incomuns para o ambiente. Além disso, assinaturas endpoint podem ser criadas para detectar ferramentas de transferência de arquivos em linha com a política da organização. Da mesma forma, processos que exibam comportamento idêntico ao de conhecidas ferramentas benignas, mas que estejam usando nomes de processos incomuns, podem ser alertados por meio de assinaturas endpoint. MITRE ATT&CK T1048.002 - Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

Estudo de caso do Black Artemis

No fim do ano, respondemos a uma invasão persistente e longa de uma empresa do setor químico pelo agente de ameaça norte-coreano Norte Andariel (também conhecido como Stonefly ou Silent Chollima), o qual havíamos rastreado internamente como um subgrupo do Black Artemis. Ele tinha obtido acesso persistente ao ambiente da vítima e voltou à rede para realizar novas atividades ao menos uma vez, o que ocorreu dois meses após o comprometimento inicial. Dada a natureza da organização atingida, sua experiência no assunto e as evidências encontradas durante nosso trabalho, concluímos que essa invasão provavelmente foi motivada por espionagem cujos alvos foram a sua propriedade intelectual e seu conhecimento únicos.

Nossa revisão das evidências nos levou à hipótese de que o comprometimento inicial no ambiente da vítima teria sido provavelmente facilitado pela exploração de um servidor de internet vulnerável ao Log4Shell pelo Andariel. Após acessar a rede pela primeira vez, ele implantou carregadores executáveis para o backdoor DTrack[208] em vários *hosts* e obteve a persistência graças a uma variedade de métodos – como a configuração de chaves Autorun e a criação de serviços de inicialização – enquanto o próprio backdoor era executado exclusivamente na memória.

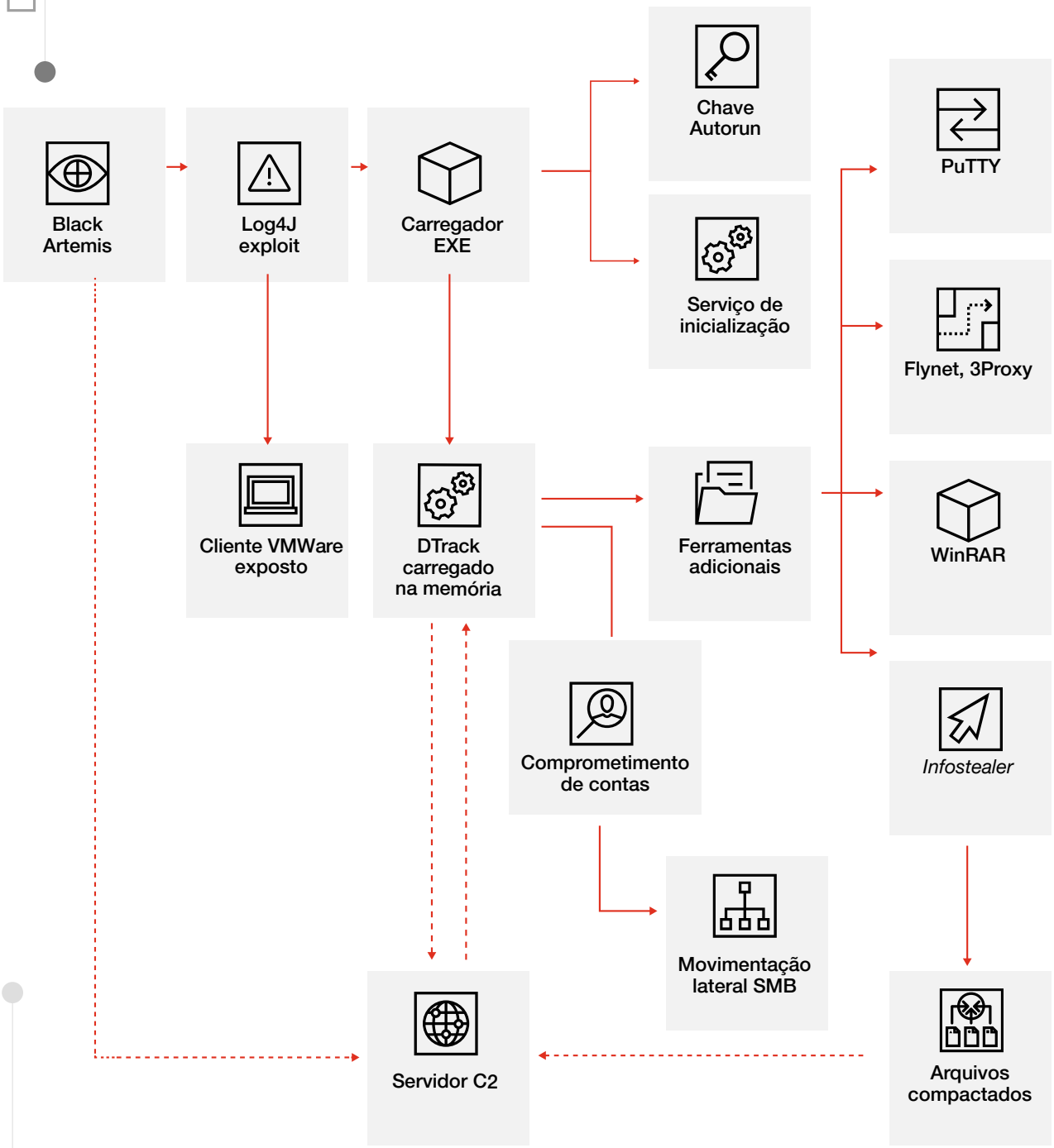
O Andariel instalou então ferramentas adicionais no disco rígido:

- Clientes PuTTY legítimos;
- Uma construção personalizada de uma versão específica e mais antiga do cliente PuTTY Secure Shell Protocol (SSH)/Telnet para Windows, compilado a partir do código-fonte;
- Muitas vezes em combinação com o Flynet, uma ferramenta de *proxy* de código aberto Go TCP/UDP para Windows; e,
- Em pelo menos um caso, Andariel também implementou o 3Proxy, uma ferramenta de *proxy* de código aberto.

[208] 'Dtrack activity targeting Europe and Latin America', Kaspersky, https://securelist.com/dtrack-targeting-europe- latin-america/107798/ (15 de novembro de 2022)

Essas ferramentas receberam nomes de arquivos que lhes permitiram se disfarçar como se fossem um antivírus presente no ambiente da vítima. Avaliamos que o Andariel provavelmente as usou para fazer *proxy* do tráfego de entrada e saída. Isso é consistente com outras atividades dele encontradas pela Cisco Talos em casos de resposta a incidentes em redes de outras vítimas[209]. Possivelmente, o agente de ameaça tem um playbook muito bem definido e consistente em todas as suas invasões.

Cadeia de invasão do Black Artemis



O Andariel conseguiu comprometer diversas contas, desde Administradores Locais até Administradores de Domínio. Observamos ainda evidências de que o agente estava se movendo lateralmente pela rede, inclusive pulando de *hosts* por meio de conexões SMB. Ele instalou uma versão específica do WinRAR em vários, a qual foi usada para descompactar arquivos com carregadores DTrack a serem executados e provavelmente para compactá-los para exfiltração. Também colhemos evidências de que o Andariel usou um *infostealer* personalizado – parecido com a descrição fornecida pela Symantec em um blog sobre atividade DTrack – que foi implantado especificamente em servidores de arquivos.[210]

Lições do incidente do Andariel envolvendo o DTrack

Há muitas possibilidades de detecção e oportunidades de mitigação na cadeia de invasão do Andariel. Quando se compara esse caso com o do White Baku, é importante considerar as similaridades em algumas etapas do ataque. É fundamental se defender contra técnicas amplamente utilizadas pelos agentes de ameaça.

Acesso inicial: por favor, veja a seção do Estudo de caso do White Baku. MITRE ATT&CK T1505.003 - Server Software Component: Web Shell.

Persistência: os agentes de ameaça continuaram a usar mecanismos de persistência bem conhecidos, como chaves de registro e serviços. Embora seja fácil para eles os utilizarem, é igualmente simples detectar e monitorar. Eles podem ser identificados tanto no momento da criação quanto durante verificações rotineiras de higiene de segurança do ambiente. Ainda que esses itens sejam parte legítima e normal dos ambientes corporativos, e possam ser configurados pelos agentes para se misturar entre softwares e tarefas corriqueiras, algumas regras de detecção podem ser criadas para monitorar a criação ou modificação de métodos Autorun. MITRE ATT&CK T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder, T1543.003 - Create or Modify System Process: Windows Service

Movimentação Lateral: por favor, veja a seção do Estudo de caso do White Baku. MITRE ATT&CK T1021.002 - Remote Services: SMB/Windows Admin Shares

Coleta: mais uma vez, é importante enfatizar que, por mais que ferramentas de compressão como o WinRAR e outras sejam perfeitamente legítimas, elas também são usadas por criminosos cibernéticos e por ameaças persistentes avançadas. Detectar quando elas são baixadas ou instaladas em pastas específicas, como a %TEMP%, pode ser uma heurística útil para identificar atividades suspeitas que podem ser sinalizadas para revisão. MITRE ATT&CK T1560.001: Archive Collected Data: Archive via Utility

Exfiltração: Como o White Baku, o Andariel usou ferramentas de transferência de arquivos com o propósito de exfiltrar dados, cujas medidas defensivas foram detalhadas aqui. Esse agente de ameaça também empregou ferramentas legítimas de *proxy* de rede, para as quais pontos semelhantes se aplicam, já que os profissionais de defesa devem procurar desvios em relação às características básicas do ambiente. No entanto, os cenários legítimos para o *proxy* de tráfego de rede são tipicamente mais limitados, o que pode permitir assinaturas um pouco mais rigorosas. MITRE ATT&CK T1048.002 - Exfiltration Over Alternative, Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol, T1090.001 - Proxy: Internal Proxy

Olhando para o futuro

Para 2023, prevemos que o cenário de ameaça será dominado pelo *targeting* às capacidades de acesso privilegiado e identidade, à medida que muitos agentes continuam a evoluir e a empregar TTPs para escapar dos mecanismos de segurança. Criminosos mais ativos e motivados por espionagem deverão ter como alvos as cadeias de suprimentos e a exploração de vulnerabilidades do tipo 0-day para ter acesso a essas operações.

À medida que os agentes de ameaça operam por meio de arranjos de quartel-mestre e usam ferramentas, *frameworks e malwares* compartilhados ou comuns, acreditamos que o mercado comercial dessas capacidades evoluirá e estimulará uma adoção mais ampla. Existem indicadores que incluem um mercado crescente para explorar vulnerabilidades 0-day e agentes comerciais acumulando *exploits*, como o NSO Group (também conhecido como Grey Anqa)[211] e outros. Essa evolução fará com que mais agentes motivados por espionagem surjam a partir de capacidades nascentes que normalmente eram subutilizadas ou subfinanciadas.

No que compete às tendências específicas para os quartéis-mestre, prevemos que os agentes motivados por espionagem aumentarão seus investimentos em redes *proxy* de ofuscação como serviço. Antecipamos ainda que dispositivos vulneráveis da Internet das Coisas (IoT) e de pequenos escritórios/domésticos (SOHO) continuarão a ser alguns dos principais alvos para exploração e cooptação de sistemas executados pelos provedores comerciais dessas redes.

Dada a saturação do mercado, acreditamos que os cibercriminosos continuarão a se adaptar profundamente nos crimes monetizados. Diante disso, apostamos que os ataques *smash-and-grab* de alto perfil estimulem atividades semelhantes no próximo ano – tanto no caso daqueles agentes de ameaça motivados por dinheiro quanto por hacktivistas. Vulnerabilidades em bibliotecas de software também serão provavelmente um foco de exploração no próximo ano.

Por fim, à medida que pesquisamos o desenvolvimento e a implantação de capacidades de sabotagem por parte de agentes como os baseados no Irã, esperamos uma continuação dos ataques *hack-and-leak*, do uso de *wipers*, da busca por operações destrutivas duradouras contra sistemas de controle industrial (ICS) e de técnicas em evolução que poderiam incluir ataques com alteração de dados.

---

[211] Já compartilhamos informação sobre esse agente de ameaças no nosso relatório 'Ameaças Cibernéticas: 2021 em Retrospectiva', PwC Threat Intelligence https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2023/Retrospectiva-Cyber-22.pdf (julho de 2022).

Alvos específicos dos agentes de ameaças previstos para 2023

Devido à guerra na Ucrânia e ao rompimento das relações diplomáticas em grande parte do planeta, prevemos que os agentes de ameaças baseados na Rússia vão mirar, cada vez mais, setores e empresas em retaliação a seu apoio explícito, ou até apenas percebido, aos ucranianos, ou por desinvestimentos realizados na Rússia. Há de se esperar também que eles se voltem aos setores de logística, transportes e manufatura à medida que a guerra persista, bem como outros ramos em que o país enfrenta desafios significativos de suprimentos – semelhante ao direcionamento de espionagem industrial. Esses agentes também deverão continuar a mostrar interesse em entidades governamentais, de defesa e relacionadas a operações de espionagem de longa data.

Quanto aos agentes baseados na China, acreditamos que aumentarão suas operações de direcionamento *(targeting)* contra a indústria de semicondutores e alta tecnologia, especialmente perante as sanções que os EUA impuseram a eles.[212] Prevemos ainda que as tensões geopolíticas na região também impulsionarão as operações de *targeting* desses criminosos. Dado que protestos eclodiram em toda a China no final do ano, algo a se observar é como esses agentes vão responder para apoiar as atividades internas de vigilância.

No caso dos agentes de ameaça baseados no Irã, acreditamos que continuarão a mirar aqueles setores que são relevantes para o regime de Teerã, bem como os relacionados ao desenvolvimento de seus interesses estratégicos. Prevemos ainda que esses agentes seguirão visando entidades de Israel, da Arábia Saudita e dos EUA, enquanto mantêm seu ritmo de direcionamento interno contra alvos domésticos e dissidentes.

Por fim, antecipamos que ações no Ocidente, emanadas de países como os Estados Unidos, provavelmente permanecerão consistentes e refletirão questões geopolíticas, como se viu na admissão do país de que conduziria operações cibernéticas em apoio à Ucrânia em meio à guerra russa.[213]

[212] CTO-SIB-20221117-01A - US export controls on semiconductors
[213] 'US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command', Sky News, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (1º de junho de 2022)

PwC Cybersecurity

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

A PwC é reconhecida mundialmente por ser líder em segurança cibernética e uma firma capaz de atuar globalmente, além de apresentar soluções para os desafios de segurança e risco que seus clientes enfrentam.

Apoiamos nossos serviços de assessoria e estratégia em segurança no nível do conselho na experiência e no conhecimento adquiridos nas linhas de frente da defesa cibernética, como Defesa Cibernética Gerenciada, Red Teaming, resposta a incidentes e inteligência de ameaças.

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

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

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

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

Apêndice A – Metodologia

Ao longo do ano, trabalhamos com clientes e *stakeholders*, bem como com especialistas da área de segurança, para validar e refinar nossos requisitos de inteligência à medida que transformamos nossa visibilidade, ferramentas sob medida e habilidades e esforços analíticos em inteligência acionável por nossos clientes. Este relatório cobre especificamente uma seleção de nossa análise desenvolvida ao longo de 2022. Somando-se às nossas capacidades proprietárias e acesso a ferramentas comerciais e de fontes abertas, atuamos em estreita colaboração com as firmas da rede PwC nos casos de resposta a incidentes e outros compromissos. As seguintes firmas da PwC forneceram suas percepções para enriquecer nossa análise: Alemanha, Austrália, Áustria, Brasil, Canadá, Coreia do Sul, Estados Unidos, Holanda, Hong Kong, Indonésia, Itália, Malásia, Nova Zelândia, Reino Unido, República Tcheca e Vietnã.

Linguagem probabilística

Interpretações de linguagem estimativa ou probabilística (por exemplo, “provável” ou “quase certamente”) podem variar muito. Para evitar interpretações errôneas, usamos os seguintes termos qualitativos neste relatório quando nos referirmos ao nível de confiança que temos em nossas avaliações. A menos que indicado de outra forma, elas não são baseadas em análise estatística.

Termo qualitativo	Linguagem de probabilidade associada
Remoto ou altamente improvável	Menos de 10%
Improvável	10%-25%
Realisticamente provável	26%-50%
Provável	51%-75%
Altamente provável	76%-90%
Quase certo	90%

No Apêndice B – Referência de agentes de ameaças, descrevemos a metodologia por trás de nossa convenção de nomenclatura de agentes de ameaças e como definimos as motivações e capacidades deles.

No Apêndice D – Índice de Defesa, fornecemos definições e explicações adicionais sobre nossa metodologia de detecção e mitigação.

Apêndice B – Referência de agentes de ameaças

Nós monitoramos muitos agentes de ameaça em todo o mundo e aplicamos nossa convenção de nomenclatura, que consiste primeiramente em uma cor referente ao local onde avaliamos que ele esteja. Designamos a cor “branca” para ameaças em avaliação. A tabela abaixo traz parte do nosso mapeamento por cores. Além da cor, atribuímos uma figura mitológica para estabelecer um nome único ao agente. Se observamos que determinada atividade não pode ser atribuída a nenhuma entidade conhecida, referimo-nos ao criminoso como um “conjunto dev” para facilitar o desenvolvimento e a análise futura. Em alguns casos, atribuímos um conjunto nomeado a um conjunto dev se nossa análise resultar em uma avaliação de atribuição. Quando vemos sobreposições entre nossa pesquisa e as de outras organizações, fornecemos os respectivos nomes dos agentes.

*Austrália, Canadá, Estados Unidos, Nova Zelândia e Reino Unido

Termos e frases-chave relacionados aos agentes de ameaça:

Ofertas de *cyber criminal* -as-a-Service: serviços cibernéticos criminosos que são desenvolvidos e depois anunciados para uso em troca de pagamento, como os seguintes:

- *Access-as-a-Service* (AaaS): a oferta criminosa de um serviço que cobra dos clientes pelo acesso a redes, predominantemente corporativas.
  Esse tipo de oferta pode ser dividida nas seguintes categorias:
  - *Initial access broker* (IAB): quando um criminoso vende a seus clientes credenciais de login para infraestrutura exposta à internet, como protocolos de área de trabalho remota (RDP) e redes privadas virtuais.
  - Sistema de entrega de *malware*: quando um serviço criminoso faz o upload de um *malware* do cliente em um host comprometido como carga secundária, como o White Taranis via Emotet e o White Horoja via Qakbot. - pág. 45-48
- *Distributed Denial of Service-for-hire* (DDoS-for-hire): a oferta criminosa de um serviço em que cibercriminosos pagam uma taxa de uma capacidade ilícita para conduzir ataques DDoS; como, por exemplo, no caso do Blue Kurama (também conhecido como Killnet) que começou como uma capacidade DDoS-for-hire. - pág. 20
- *Phishing-as-a-Service* (PHaaS): a oferta criminosa de um serviço em que cibercriminosos pagam uma taxa para uma capacidade ilícita de *phishing* para enviar e-mails desse tipo, como os kits de ferramentas EvilProxy, Caffeine e Robin Banks. - pág. 50, 50-51

- *Ransomware*-as-a-Service (RaaS): o modelo de programas *ransomware* que envolve operadores, os quais o desenvolvem e as operações gerais de marca, e afiliados, ou aqueles que usam o *ransomware* em ataques.- pág. 40-48.

Agentes de ameaças motivados por espionagem: frequentemente referidos como "Ameaças Persistentes Avançadas" (*Advanced Persistent Threats*, APTs na sigla em inglês), esses agentes normalmente buscam acesso e informações para atender a requisitos de coleta de inteligência e fornecer vantagem econômica ou política ao seu benfeitor. - pág. 61 (insights específicos em alto nível para os casos analisados de resposta a incidentes)

Agentes de ameaças motivados financeiramente: esses agentes de ameaças podem agir indiscriminadamente sobre quem atacam, pois apenas procuram monetizar suas atividades. A escala de sofisticação deles é bem vasta e exibe um conjunto bastante variado de TTPs. - pág. 40-51, 62

Agentes de ameaça motivados por sabotagem: sabotadores que buscam danificar, destruir ou subverter a integridade dos dados e sistemas. - pág. 2-3, 8, 11-14, 28-29, 68-69

Data Broker: no contexto deste relatório, uma entidade ilícita que coleta, agrega e vende acesso a informações sensíveis roubadas das vítimas. - pág. 38

Hacktivismo: os hacktivistas conduzem seus ataques para ganhar reconhecimento público e ampliar a conscientização em torno de sua causa. Isso é tipicamente feito por meio da interrupção de serviços, como ataques de negação de serviço (DoS) e desfigurações de sites. - pág. 1, 11, 18-19, 61, 68

Insider: um funcionário atual ou antigo, empresa prestadora de serviço ou outro parceiro comercial que tem ou teve acesso autorizado à rede, ao sistema ou aos dados de uma determinada organização e, intencionalmente, usou isso para comprometer os dados ou sistemas dela. - pág. 39, 44, 49, 61

Operational Security, Segurança Operacional (OPSEC): as medidas tomadas para proteger operações e ativos para que não possam ser interrompidos, antecipados ou atribuídos. - pág. 23, 31

Proxy network, rede proxy: no contexto deste relatório, é uma rede tornada anônima ou um sistema de retransmissão ofuscado que é usado por agentes de ameaça para conduzir operações, como o RedRelay. - pág. 2, 20,22-23, 68

Quartermaster, quartel-mestre: uma entidade que possibilita a operação dos agentes de ameaça por meio do desenvolvimento, provisionamento e intermediação de ferramentas, capacidades e estruturas. - pág. 20, 22, 68

Tools, techniques and procedures (TTPs): as TTPs se referem aos comportamentos do agente de ameaça e o Apêndice D – Índice de defesa fornece uma referência rápida para exemplos das citadas neste relatório.

Agentes de ameaça incluídos neste relatório

- Abraham's Ax - pág. 30
- Agentes de ameaças de business e-mail compromise (BEC) - pág. 51
- Andariel (também conhecido como Stonefly, Silent Chollima), um subgrupo do Black Artemis - pág. 65-66
- Black Alicanto (também conhecido como COPERNICIUM, DangerousPassword, CryptoMimic, CryptoCore, Operation SnatchCrypto) - pág. 33, 35
- Black Artemis (também conhecido como Lazarus Group, Hidden Cobra, ZINC) - pág. 33-35, 65-66
- Black Dev 2 (também conhecido como Operation Gold Hunting, Operation SnatchCrypto) - pág. 33
- Blue Athena (também conhecido como APT28, FANCY BEAR) - pág. 10-12, 16, 38
- Blue Callisto (também conhecido como Callisto Group) - pág. 16
- Blue Cronus (também conhecido como Conti): após os vazamentos das comunicações do grupo Conti no início de 2022, combinamos vários agentes de ameaças sob a organização criminosa Blue Cronus: o White Magician (também conhecido como TrickBot, Bazar, Anchor), o White Onibi (também conhecido como Conti, Ryuk), o White Taranis (também conhecido como Emotet) e o White Dev 115 (também conhecido como BlackBasta) - pág. 18, 43-44, 46-47
- Blue Dev 4 (também conhecido como Ghostwriter, UNC1151) - pág. 16-17

Apêndice C – Visão de negócios

Segundo a 26ª Pesquisa Global de CEOs da PwC, cibersegurança e conflitos geopolíticos foram identificados como as maiores preocupações dos CEOs entrevistados para os próximos cinco anos. Em 2022, os agentes de ameaça cibernética continuaram a adaptar e modificar seus comportamentos para superar as práticas de segurança em vista dos conflitos na Ucrânia, do ritmo elevado e sustentado na atividade de *ransomware* e do uso de sabotagem para aumentar ganhos políticos e criminais. Enquanto esse cenário de ameaça evoluiu e os riscos aumentaram, a pesquisa Global Digital Trust Insights 2023 da PwC destacou a colaboração entre CISOs, executivos C-suite e membros dos conselhos de administração das empresas como um elemento crítico para realizar melhorias na segurança cibernética e para aproveitar ao máximo investimentos cumulativos e sustentados na mitigação de riscos.

A PwC Threat Intelligence identificou os principais riscos cibernéticos a partir de nossa pesquisa focada em ameaças de 2022, bem como de nossos esforços proativos para detectar e avaliar questões cibernéticas emergentes.

1. **A geopolítica se refletiu nas atividades dos agentes de ameaça - pág. 2-3, 68-69**
    - As capacidades cibernéticas foram extensivamente utilizadas por agentes de ameaça para complementar os métodos tradicionais de guerra observados na guerra na Ucrânia (pág. 9-20).
    - Agentes de ameaça baseados na China. aprimoraram as habilidades para ofuscar suas atividades contra alvos tradicionais e demonstraram grande interesse em inteligência relacionada à guerra na Ucrânia, bem como referente à resposta da comunidade internacional (pág. 21-27)
    - Agentes de ameaças baseados no Irã intensificaram seu alvo a dissidentes e mostraram disposição para usar o ciberespaço como arma política nos Bálcãs (pág. 28-32).
    - Agentes de ameaças baseados na Coreia do Norte continuaram a mirar os serviços financeiros e as criptomoedas como forma de gerar receita e compensar os efeitos das sanções aplicadas ao país (pág. 33-36).
    - Muitas nações elevaram a um patamar superior a prioridade de aumentar a resiliência cibernética em nível nacional, depois que autoridades cibernéticas como a Cybersecurity and Infrastructure Security Agency (CISA), nos Estados Unidos, e o National Cyber Security Centre (NCSC), no Reino Unido, alertaram para o potencial de as organizações colherem danos indiretos no rescaldo do crescimento das tensões geopolíticas (pág. 11).

2. **Evolução e perspectivas do *ransomware* - pág. 40-49**
    - O *ransomware* permaneceu como a principal ameaça cibernética para a maioria das empresas em todo o mundo, à medida que os agentes de ameaça profissionalizaram seus modelos de negócios para operações 24/7, alvejando setores de alto valor, como manufatura, construção civil e varejo (pág. 42-43, 45-46).
    - O interesse dos agentes de ameaça também se estendeu a empresas de pequeno e médio porte, incluindo governos locais, o que implicou significativos custos para mitigação e remediação e divulgação de ataques e interrupções em sites de vazamento (pág. 42-43).
    - Os grupos de *ransomware* e os principais agentes de ameaça continuaram a se fragmentar e lançar “novas marcas” (rebrand) ao longo de 2022, com o *Ransomware-as-a-Service* (RaaS) se revelando cada vez mais popular como modelo de negócios (pág. 40-46).

3. **As operações de sabotagem escalam - pág. 2-3, 68-69**
    - Agentes de ameaça baseados na Rússia implantaram várias formas de *malware*s destrutivos contra entidades baseadas na Ucrânia e esperamos um padrão semelhante em 2023 (pág. 2, 12-14).
    - Agentes de ameaça baseados no Irã lançaram ataques de sabotagem contra organizações do governo albanês. O sucesso deles potencialmente prenuncia tentativas mais audaciosas de exercer influência estratégica por meio de ações cibernéticas ofensivas no futuro por parte deles, bem como de outros com motivações e capacidades de sabotagem (pág. 3, 28-29, 68-69).

4. **Fatiga e burla/evasão da Autenticação Multifator (MFA) - pág. 50-52, 59-60**
    - Os agentes de ameaça mostraram capacidade de se adaptar e burlar controles de segurança aprimorados, como algumas formas de MFA, e personalizar engenharia social (pg. 50) e ferramentas de roubo de credenciais (pg. 50-51) para maximizar sua capacidade de obter acesso irrestrito a ambientes corporativos, entre os quais estão os baseados em nuvem (pág. 60-61).
    - Falhas no uso da MFA em ambientes corporativos, especialmente em contas com acesso privilegiado, contribuíram para o sucesso de alguns ataques *ransomware* e outros comprometimentos criminais cibernéticos verificados em 2022. A MFA torna excepcionalmente difícil para um criminoso acessar uma rede remotamente, mesmo que tenha um nome de usuário e senha legítimos (pg. 51).

5. **Mirando na identidade digital e no acesso privilegiado - pág. 2, 58-60, 68**
    - Proteger a identidade e o acesso privilegiado é a prioridade mais alta para preservar o ambiente e os dados de uma organização.
    - Os agentes de ameaça se concentraram sobremaneira em comprometer identidades digitais para obter acesso inicial, muitas vezes usando, para tanto, engenharia social sofisticada (pág. 50).
    - Os agentes de ameaça também usaram *infostealer*s, que sugam credenciais de usuário e outras informações para obter acesso inicial às redes (pág. 50-51).

6. **Ambientes em nuvem na mira - pág. 60-61**
    - À medida que mais organizações migraram para a nuvem e colheram os benefícios dessa segurança aprimorada, os agentes de ameaça também trabalharam duro para desenvolver novas ferramentas e novos conhecimentos para comprometer os serviços nela baseados (pág. 59-61).
    - Responder a ataques que visam os ambientes e serviços baseados em nuvem requer abordagens diferentes, já que os agentes de ameaça predominantemente abusam de identidades, serviços e interfaces de programação de aplicativos (APIs) (pág. 60).
    - Vulnerabilidades em bibliotecas de software também provavelmente serão um foco de exploração em 2023 (pág. 69).
    - Desenvolvemos várias recomendações para fortalecer os ambientes em nuvem com base em casos de resposta a incidentes com os quais trabalhamos em 2022 (pág. 60-61).

Olhando para o futuro, os provedores de serviços em nuvem, de serviços gerenciados e de gerenciamento de identidade e acesso (IAM), com acesso privilegiado a redes de seus clientes, vão se tornar cada vez mais alvos para agentes de ameaça mais sofisticados – tudo isso para conquistar o acesso escalonado que precisam para comprometê-los em suas operações de roubo de propriedade intelectual e espionagem (pág. 68).

Outros apêndices fornecem mais informações sobre nossa metodologia, as várias ameaças descritas e um índice ordenado de informações relevantes para defensores. Este relatório também contém insights voltados para o futuro na nossa seção Olhando para o futuro, bem como referências a incidentes que impactam os seguintes setores[214] e indústrias:

- Automotivo - pág. 62
- Química - pág. 64
- Construção - pág. 43, 61
  - Engenharia - pág. 32
- Infraestrutura crítica - pág. 17, 19, 30
- Defesa - pág. 9, 20, 24, 30, 34, 69
  - Instituto de defesa - pág. 17
  - Militar - pág. 16, 33
  - Ataques com o tema militar - pág. 16
  - Laboratórios de pesquisa - pág. 16

  Fornecedores - pág. 16
- Dissidentes - pág. 28, 30, 69
  - Ativistas - pág. 30
  - Manifestantes - pág. 28, 30, 69
- Educação e pesquisa - pág. 43, 62
  - Academia e pesquisadores - pág. 17, 28, 29, 31, 39
  - Estudantes - pág. 30
  - Think tanks - pág. 31
- Energia, serviços públicos e recursos - pág. 30-31, 34, 43, 62
  - Energia nuclear - pág. 31, 37
  - Petróleo e gás - pág. 31, 37
  - Redes de energia elétrica - pág. 9
- Entretenimento e jogos eletrônicos - pág. 50
- Serviços financeiros - pág. 3, 33, 36, 62
  - Criptomoeda e finanças descentralizadas (DeFi) - pág. 3, 33, 35, 42
  - Bancos comerciais - pág. 8, 17, 47
  - Softwares de gerenciamento financeiro - pág. 9
  - Seguradoras - pág. 18, 32
  - Capital de risco - pág. 33
- Exportadores de alimentos, supermercados e varejistas - pág. 37, 62
- Governo - pág. 2-3, 6, 9-20, 22-38, 42, 51, 62,69
  - Serviços de comunicação - pág. 12, 17
  - Resposta a emergências de computador - pág. 14 (nota de rodapé), 38
  - Entidades diplomáticas - pág. 25-27
  - Ataques com o tema das eleições - pág. 26
  - Serviços de emergência - pág. 19
  - Sistemas governamentais - pág. 29-30
  - Aplicação da lei e segurança - pág. 12, 34, 51
  - Parlamento - pág. 20

[214] CTO-SIB-20230223-01A - Sector shifts and insights - 2022

Mais conteúdo do time da PwC Threat Intelligence:

Leia os posts do blog que publicamos em 2022
Assista à nossa palestra na BlackHat USA 2022
Assista à nossa palestra na SANS CTI Summit 2022
Assista à nossa palestra na SANS Ransomware Summit 2022
Assista à nossa palestra na Virus Bulletin 2022

Apêndice D – Índice de defesa

Para nos manter sempre à frente das tendências do cenário de ameaças, aumentar nossa visibilidade das mudanças dos agentes e desenvolver estratégias de detecção e mitigação para nossos clientes, utilizamos os seguintes pilares principais, que servem como base para nossas capacidades de detecção:

1. ***Endpoint:*** no atual ambiente descentralizado e nativo da nuvem, ter uma detecção eficaz no endpoint – seja em um servidor virtual ou físico, no laptop ou em um dispositivo móvel – é uma das posições mais importantes que um defensor pode tomar.

2. **Rede:** embora o *Transport Layer Security* (TLS) continue a ser um desafio, quase todo *malware* usa a internet para comunicações C2. Ter visibilidade de todo o tráfego da rede significa que, mesmo quando um invasor evita a detecção no endpoint ou compromete um que não tem ferramentas de detecção, a atividade C2 geralmente pode ser detectada. A visibilidade da rede interna também pode ajudar na detecção e no rastreamento da movimentação lateral.

3. **Gerenciamento de Informações e Eventos de Segurança (SIEM) / Orquestração de Segurança, Automação e Resposta (SOAR):** uma visão centralizada de todos os eventos de detecção permite a um defensor correlacionar em um nível mais alto e conduzir detecções adicionais. Ela também reúne o contexto mais amplo da atividade de modo que, se bem feita, pode ajudar o profissional de defesa a encontrar sinal em meio ao ruído. As plataformas SOAR também permitem que um defensor automatize a remediação, o que é particularmente útil quando o *ransomware* está em ação e o tempo é essencial.

4. **YARA:** ainda que raramente usada para detecção em tempo real, a ferramenta YARA é incrivelmente útil para analisar binários suspeitos e escanear memória. Com ela, regras podem ser escritas para auxiliar na triagem de amostras suspeitas e agrupar artefatos como parte dos esforços de análise de intrusão e campanha.

Uma defesa em profundidade pode ser aprimorada ainda mais por meio do desenvolvimento de detecção para dois tipos de atividade: aquelas atribuídas a agentes de ameaça com alta confiança e aqueles comportamentos mais gerais, de modo que mudanças, ainda que pequenas ou sutis, possam ser detectadas.

Leia mais sobre o workshop YARA que realizamos no FIRST22

Vulnerabilidades e Exposições Comuns (CVEs) citadas neste relatório:

CVE-2021-40444 - pág. 30
CVE-2021-44228 (também conhecidos como Log4Shell) - pág. 2, 7, 65
CVE-2021-45046 - pág. 7
CVE-2021-45105 - pág. 7
CVE-2022-30190 - pág. 30
CVE-2022-41040, CVE-2022-41082 (conhecidos como ProxyNotShell) - pág. 8

Principais temas e exemplos das TTPs de agentes de ameaças

*Insights e tendências dos ataques - pág. 53
Adversary-in-the-middle (AitM): descrito no MITRE ATT&CK T1557 - Adversary-in-the- Middle, um exemplo neste relatório é o EvilProxy. - pág. 51
Arquivo atalho/LNK: extensão de arquivo que denota um atalho do Windows ou "link", que é usado por agentes de ameaças para se disfarçar como documentos legítimos e executar cargas maliciosas. - pág. 23, 26, 33, 47, 57-59
Arquivo ISO (imagem de disco óptico): um tipo de arquivo que atua como um compactado, que é usado por agentes de ameaças para entregar cargas maliciosas. - pág. 35, 47-49, 57-58
Ataque a ambientes em nuvem: este relatório contém detalhes sobre o Blue Dev 5 (também conhecido como NOBELIUM) que mira ambientes em nuvem, bem como nossas recomendações para fortalecer esses ambientes com base nesses casos. - pág. 60-61
Ataque *Smash-and-Grab*: neste relatório, um ataque *Smash-and-Grab* se refere a um agente de ameaça invadindo uma rede e rapidamente roubando dados para roubo ou extorsão, com o agente priorizando a velocidade sobre a descoberta. – pág 3, 40, 50, 68
Big game hunting: neste relatório, um ataque *big game hunting* se refere a um agente de ameaça selecionando alvos de alto perfil ou percebidos como de alto valor. - pág. 40
Carregamento lateral de biblioteca de vínculo dinâmico (DLL): descrito em T1574.002 - Hijack Execution Flow: DLL Side-Loading, um exemplo neste relatório envolve o ShadowPad. - pág. 23
Contrabando de HTML: um arquivo HTML malicioso é enviado a um usuário com uma carga útil ofuscada e incorporada ao HTML, a qual é decodificada e entregue por meio do JavaScript. - pág. 49
Correção em tempo real para obstruir análise forense (exemplo ScatterBee) - pág. 22
Exploração do Microsoft Installer (MSI) - pág. 33, 35, 48
Extorsão dupla: neste relatório, a extorsão dupla ocorre quando um agente de ameaça invade a rede de uma vítima e a criptografa, extorquindo primeiramente a vítima para recuperar o acesso à sua rede e depois novamente ao ameaçar vender ou vazar dados roubados dela. - pág. 40, 41 (organograma de uma típica cadeia de ataque)
Fadiga e evasão/desvio da autenticação multifator (MFA) - pág. 50-53, 59-61
Fingerprinting de navegador com JavaScript: um método que dado agente de ameaça adota para obter informações do usuário e do dispositivo quando o usuário navega em um site infectado (exemplo Yellow Liderc).- pág. 31
Fóruns de criminosos cibernéticos (Exploit e XSS, por exemplo) - pág. 47
Hack-and-leak ou lock-and-leak: eles implicam que um agente de ameaça invada uma rede, a criptografe e depois vaze dados roubados da vítima. - pág. 3, 28, 30, 40, 69
Ladrões de informações (também conhecidos como *infostealer*s) - pág. 50-51, 67, 76
Live-off-the-land (LOL): refere a um agente de ameaça que usa ferramentas com dupla finalidade legítimas, enquanto está dentro do ambiente da vítima, como serviços administrativos e ferramentas forenses, e elas também são chamadas de binários LOL (LOLBins). - pág. 37

[215] 'Macros from the internet will be blocked by default in Office', Microsoft, https://learn.microsoft.com/en- us/deployoffice/security/internet-macros-blocked (11 de outubro de 2022)

Métodos e lógicas de detecção

Insights de respostas a incidentes e outros estudos de caso

Referências MITRE ATT&CK

Todas as referências a capacidades e *malwares*

Contatos

Eduardo Batista
Sócio e líder de Cybersecurity & Privacy da PwC Brasil
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

www.pwc.com.br /cyber-security

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