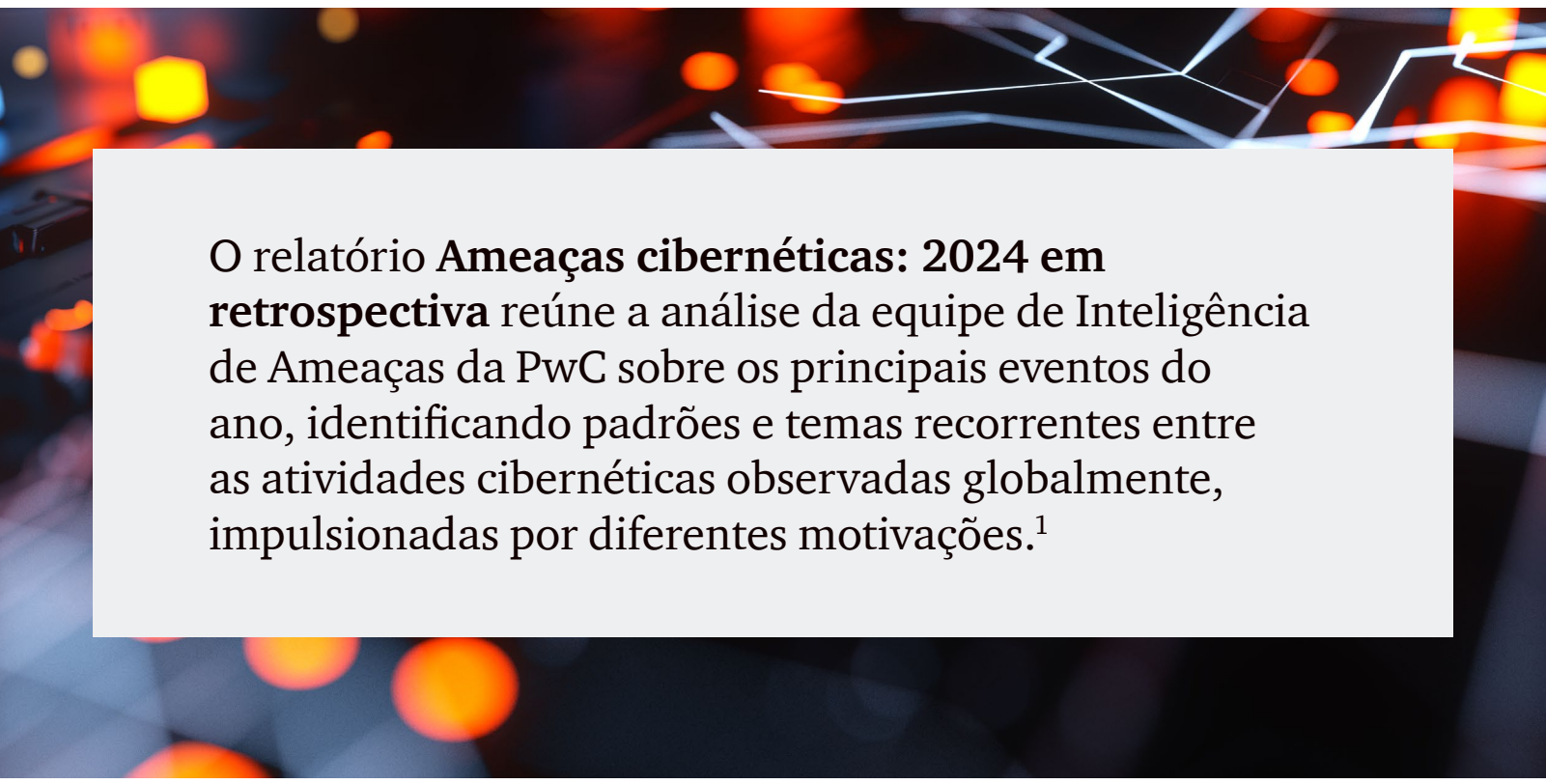
Ameaças cibernéticas:

2024 em retrospectiva

Sumário executivo



O relatório **Ameaças cibernéticas: 2024 em retrospectiva** reúne a análise da equipe de Inteligência de Ameaças da PwC sobre os principais eventos do ano, identificando padrões e temas recorrentes entre as atividades cibernéticas observadas globalmente, impulsionadas por diferentes motivações.[1]

Os insights deste relatório foram desenvolvidos com base em análises realizadas ao longo de 2024, combinando dados obtidos por coleta direta e em estreita colaboração com a equipe global de resposta a incidentes e segurança gerenciada da PwC – considerando que algumas atividades podem ainda não ter sido detectadas. Nosso objetivo é oferecer direcionamentos práticos que ajudem as organizações a fortalecer suas defesas e melhorar sua compreensão do panorama de riscos em 2025 e nos anos seguintes.

Em 2024, agentes de ameaças demonstraram uma postura mais ousada, mantendo um ritmo elevado de atividade cibernética – o que se torna ainda mais evidente quando analisado em retrospectiva. Vulnerabilidades críticas dominaram as manchetes, enquanto eventos relevantes, especialmente em um cenário geopolítico instável, influenciaram fortemente a dinâmica das ameaças no ano. Investigações conduzidas em incidentes confirmaram que operações de *ransomware* e fraudes orquestradas por cibercriminosos continuam a impactar significativamente diversas organizações.

[1] A PwC caracteriza as motivações de ameaça nas seguintes quatro categorias: espionagem, crime, hacktivismo e sabotagem. Mais informações sobre essas definições podem ser encontradas no Apêndice A deste relatório.

O cenário de ameaças também foi impactado pelo aumento da disponibilidade de códigos maliciosos e pela facilidade crescente de acesso a recursos que facilitam a execução de ataques. Fóruns e ecossistemas de código aberto foram inundados por ferramentas como *infostealers*, kits de *phishing* com suporte de IA, binários de *ransomware* e códigos de prova de conceito para exploração de vulnerabilidades. Esse ambiente beneficiou especialmente agentes de ameaças menos sofisticados, que agora têm à disposição capacidades antes restritas a grupos mais avançados.

Por trás do crescimento de uma atividade cibercriminosa menos sofisticada, muitos operadores com motivações de espionagem passaram 2024 desenvolvendo ferramentas, técnicas e procedimentos (TTPs) que provavelmente impactarão o cenário de ameaças nos próximos anos. Isso inclui a ampla adoção de redes *proxy* comerciais por agentes de ameaças baseados na China. Também houve uma mudança de abordagem por parte de grupos norte-coreanos, que vêm substituindo ataques de cadeia de suprimentos em larga escala por operações mais frequentes e tradicionais, sustentando um ritmo operacional elevado.

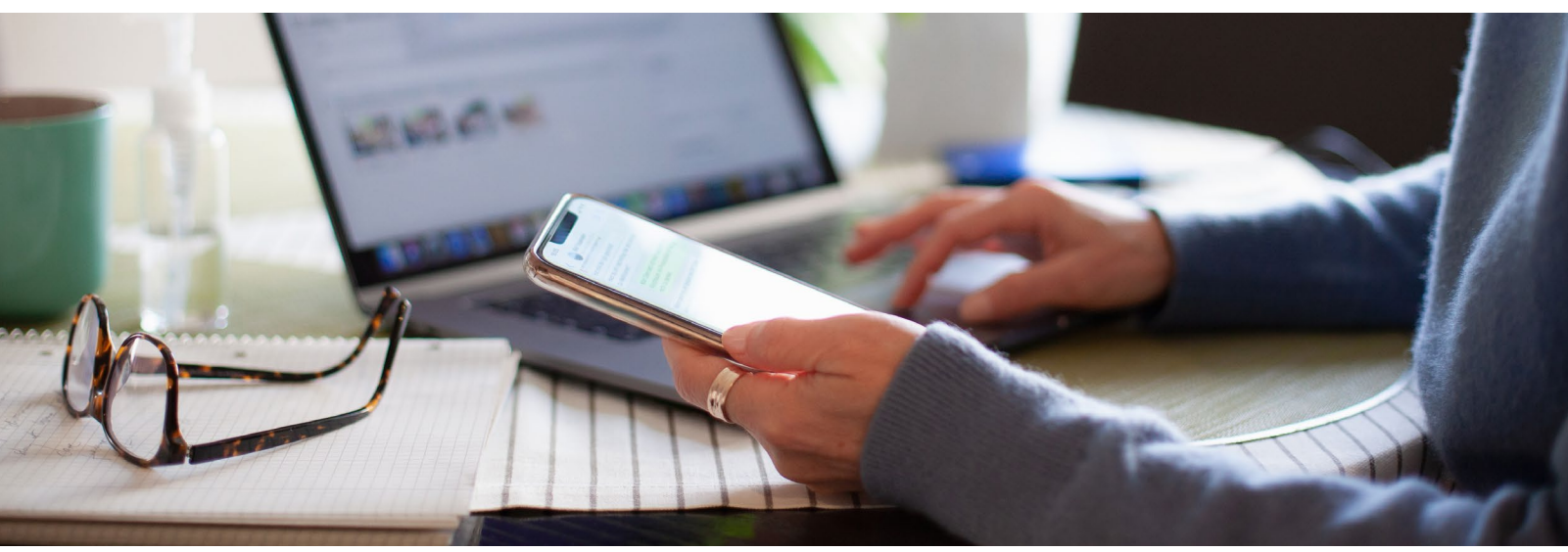
Em um cenário mais turbulento, a atividade cibernética agressiva observada no ano anterior continuou praticamente sem controle, em grande parte impulsionada por tensões geopolíticas. Campanhas conduzidas por agentes de ameaças ligados à Rússia mantiveram o foco na Ucrânia e em países aliados da OTAN, enquanto grupos associados ao Irã realizaram intrusões cibernéticas alinhadas ao papel do país na crise geopolítica em evolução na região.[2] [3] Além das operações com motivações de espionagem, o ecossistema de *ransomware* como serviço (RaaS) atingiu um novo pico: registrou-se, em 2024, o maior número de vítimas com dados expostos em sites de vazamento desde a popularização desse modelo em 2020.[4]

[2] 'Risk of long-feared regional war rises as Israel and Iran swap threats', Al Jazeera, https://www.aljazeera.com/news/2024/10/2/risk-of-long-feared-regional-war-rises-as-israel-and-iran-swap-threats (02/10/2024)
[3] 'Iran shifted focus of cyberattacks from US to Israel, Microsoft says', Iran International, https://www.iranintl.com/en/202410165266 (16/10/2024)
[4] Nota do analista: reconhecemos que o número total de vítimas listadas em sites de vazamentos não abrange todas as variantes de *ransomware*, pois há organizações que pagaram o resgate antes de os dados serem postados, bem como várias ameaças que não usam mais sites de vazamento. Consulte: "More LockBit 3.0 in the Asia Pacific", PwC Threat Intelligence, CTO-TIB-20241125-01A.

Embora algumas áreas do cenário estivessem relativamente claras, outras permaneceram muito turvas. As operações tradicionais de desinformação seguiram ativas em 2024, com Rússia e Irã recorrendo a táticas já conhecidas para manipular narrativas, especialmente durante os diversos processos eleitorais ao longo do ano. Além disso, técnicas anteriormente documentadas, como o uso de *spyware* comercial por agentes de ameaças, também contribuíram para tornar o ambiente mais nebuloso, como já havia ocorrido em 2023.

Em um retorno a técnicas clássicas do passado,[5] 2024 também foi marcado pelo comprometimento da infraestrutura cibernética de determinados agentes de ameaças por grupos adversários, com o objetivo de realizar operações disfarçadas, simulando a identidade da ameaça original. O ano também trouxe uma novidade: o uso estratégico de relatórios técnicos detalhados como forma de resposta a publicações de inteligência de ameaças emitidas por governos.

Embora a desinformação seja tradicionalmente associada a motivações políticas, a troca de relatórios entre os governos da China e dos Estados Unidos[6] [7] – como parte da disputa narrativa sobre a atuação de agentes chineses – emergiu como um novo instrumento de manipulação, contribuindo para um cenário ainda mais nebuloso e reduzindo a clareza no ecossistema de inteligência de ameaças.



[5] 'Hijacking of Iranian hacking infrastructure', Council on Foreign Relations, https://www.cfr.org/cyber-operations/hijacking-iranian-hacking-infrastructure (outubro/2019)
[6] 'People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations', Joint Cybersecurity Advisory (US), https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF (18/9/2024)
[7] 'Report reveals more conspiracies behind U.S. "Volt Typhoon" misinformation campaign', Ministry of Public Security (CN), https://www.mps.gov.cn/n2255079/N6865805/n7355748/n7355818/c9806794/content.html (14/10/2024)

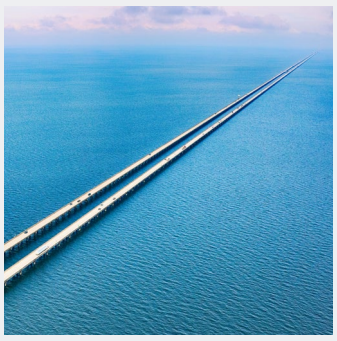
Sobre nós

A PwC atende mais de 180 mil clientes em mais de 145 países e usa sua posição privilegiada como um dos maiores networks internacionais de serviços profissionais para oferecer serviços globais de inteligência de ameaças, personalizados e entregues localmente aos nossos clientes. Nossa pesquisa apoia serviços de segurança que oferecemos e é usada por organizações dos setores público e privado em todo o mundo para proteger redes, fortalecer a conscientização situacional e orientar estratégias.

A **Inteligência de Ameaças** da PwC combina nossas capacidades de detecção com pesquisas focadas em ameaças e esforços proativos para identificar questões emergentes. Com isso, buscamos continuamente oportunidades para identificar e corrigir lacunas na detecção de atividades maliciosas, ampliar nosso conhecimento sobre ameaças e integrar inteligência prática aos nossos relatórios. Nossa equipe é composta por profissionais em diversas partes do mundo, como Alemanha, Austrália, Canadá, Estados Unidos, Itália, Noruega, Países Baixos, Reino Unido, República Tcheca e Suécia.

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

Conteúdo



Seção um

Visão de periscópio

O ano de 2024 foi marcado por um aumento geral na atividade de agentes de ameaças cibernéticas, com diferentes motivações. Esse crescimento foi impulsionado por um cenário geopolítico mais instável, mudanças nas lideranças políticas e maior acesso a ferramentas, técnicas e procedimentos – tanto novos quanto já conhecidos – que facilitam a atuação desses agentes.

Conflitos que já estavam em curso no ano anterior continuaram no radar de agentes de ameaças, enquanto novas zonas de conflito registraram aumento nas atividades cibernéticas, motivadas por espionagem, hacktivismo e sabotagem. Ao mesmo tempo, o crime cibernético foi alvo de várias operações de combate, mas, mesmo assim, 2024 foi o ano mais movimentado até agora em termos de número de sites utilizados para divulgação indevida de dados obtidos em ataques de *ransomware* e de atividade de programas de afiliados.

Linha do tempo de eventos cibernéticos em 2024

Os principais eventos cibernéticos de 2024 ilustram um fluxo constante de atividade agressiva por parte de agentes de ameaças, impulsionado pela crescente disponibilidade de abordagens sofisticadas, adoção de ferramentas inéditas e resiliência diante de tentativas de desestabilização – tudo em um contexto geopolítico volátil. O ano também foi marcado por uma atuação mais incisiva de autoridades ocidentais, com foco especial no combate a ameaças relacionadas a espionagem.

A disposição de governos ocidentais em conduzir operações públicas reflete a intensificação das tensões internacionais, com administrações de todo o mundo adotando posturas mais proativas diante das ameaças cibernéticas.

Além disso, 2024 manteve a tendência de crescimento tanto na divulgação quanto na exploração de vulnerabilidades. As estatísticas indicam um aumento de 31% no número de vulnerabilidades divulgadas em relação a 2023 – muitas delas com impactos relevantes em diversos setores da indústria.[8]

[8] NVD, https://nvd.nist.gov

Figura 1 – Principais eventos cibernéticos em 2024

Janeiro

Botnet KV desativado

Autoridades dos EUA confirmaram a desativação da *botnet* KV, usada pelo grupo Red Dev 49 (também conhecido como Volt Typhoon), como rede de ofuscação em campanhas direcionadas a alvos em escala global.

Fevereiro

Vazamentos do i-Soon revelam visão interna de parcerias público-privadas

Um grande vazamento de dados internos da empresa chinesa Shanghai Anxun expôs evidências de cooperação entre operações cibernéticas conduzidas pelo setor público e empresas privadas de tecnologia.

Autoridades de segurança desmantelam as maiores operações de *ransomware*

A Operação Cronus, conduzida por autoridades dos EUA, teve como alvo o LockBit 3.0 – um esquema de *Ransomware* como Serviço (RaaS). A ação empregou táticas de exposição pública e ofereceu recompensas por informações, pressionando os operadores da ALPH-V a tentar um golpe de saída (*exit scam*).

Março

Políticos alemães são alvo de *phishing* de grupo vinculado à inteligência russa

O grupo Blue Dev 5, passando-se por membros do partido CDU da Alemanha, visou políticos alemães com o *backdoor* WINELOADER.

Abril

EUA acusam a China de atacar infraestruturas críticas nacionais

O FBI acusou agentes de ameaças apoiados pela China de mirar setores críticos (como energia e água), com o objetivo de criar pontos de acesso para ataques futuros.

Maio

BreachForums derrubado

Autoridades de segurança derrubaram o BreachForums, um dos maiores fóruns da *dark web* para venda de credenciais e *malware*. O Telegram e o site do grupo foram retirados do ar em ação conjunta.

Coreia do Norte obtém acesso remoto a dados de emprego em TI

O Departamento de Justiça dos EUA revelou que agentes norte-coreanos roubaram identidades de cidadãos americanos para se candidatarem a empregos remotos em TI.

Junho

Blue Dev 5 ataca governos da União Europeia

A agência cibernética francesa ANSSI revelou campanha de espionagem persistente contra governos ocidentais, com foco em e-mails usados para coleta de inteligência.

Julho

Dark Angels exige pagamento de US$ 75 milhões

Segundo relatos, uma empresa da Fortune 50 pagou um resgate de US$ 75 milhões ao grupo RaaS conhecido como Dark Angels.

Agosto

Yellow Garuda tenta influenciar eleições dos EUA

O FBI informou que o grupo iraniano Yellow Garuda tentou fornecer informações ilegalmente obtidas sobre a campanha de Trump a membros da campanha de Kamala Harris.

Setembro

Governo dos EUA desativa *botnet* atribuída à China

Autoridades dos EUA analisaram publicamente uma *botnet* – supostamente operada por uma empresa privada chinesa.

Outubro

Salt Typhoon representa ameaça para empresas de telecom

O grupo Salt Typhoon, com origem na China, foi identificado como responsável pela infiltração em redes de grandes provedores de internet de banda larga nos Estados Unidos, segundo fontes de código aberto.

Novembro

Membros do Scattered Spider são indiciados por crimes cibernéticos

Autoridades dos EUA acusaram cinco membros do grupo de invasões e roubo de criptomoedas totalizando US$ 11 milhões.

Blue Yonder é atingida por *ransomware*; terceiros são afetados

A empresa Blue Yonder foi comprometida por um afiliado do *ransomware* Termite, o que desestabilizou a cadeia de suprimentos de diversas organizações.

Dezembro

Ransomware CL0P assume autoria por vulnerabilidade zero-day da Cleo

O grupo CL0P, responsável por explorações em massa de vulnerabilidades em 2023, reivindicou a autoria de um ataque com base em vulnerabilidade *zero-day* contra a solução FTP Cleo.

As intrusões do grupo Salt Typhoon em organizações de telecomunicações em várias partes do mundo[9] e a divulgação da exploração do protocolo de transferência de arquivos Cleo pelo grupo CL0P[10] [11] foram duas das campanhas mais importantes divulgadas em 2024.

Esses eventos, ocorridos no fim do ano, indicam que 2025 provavelmente seguirá com a exploração contínua de sistemas críticos por agentes de ameaças com diferentes motivações, visando obter acesso inicial.

[9] 'The emerging Salt Typhoon', PwC Threat Intelligence, CTO-SRT-20241126-02A
[10] 'Active exploitation of Cleo zero-day', PwC Threat Intelligence, CTO-TIB-20241212-01A
[11] 'Clop ransomware claims responsibility for Cleo data theft attacks', Bleeping Computer, https://www.bleepingcomputer.com/news/security/clop-ransomwareclaims-responsibility-for-cleo-data-theft-attacks/ (15/12/2024)

Figura 2 – Principais vulnerabilidades exploradas em 2024

Janeiro

Ivanti Connect Secure VPN

Duas vulnerabilidades (CVE-2023-46805, CVE-2024-21887) permitiam a execução de comandos arbitrários e autenticação não autorizada. Observada em uso por uma *botnet* conhecida como SuperJump.

Fortra GoAnywhere MFT

Uma vulnerabilidade (CVE-2024-0204) no GoAnywhere MFT permitia que um usuário não autorizado criasse uma conta com privilégios de administrador, além de ser usada para carregar um *payload* e executar código remotamente.

Fevereiro

Microsoft Defender SmartScreen

Duas vulnerabilidades (CVE-2024-21142, CVE-2024-21315) foram exploradas por um agente desconhecido para burlar os mecanismos de proteção do SmartScreen.

Fortinet FortiOS RCE

Uma vulnerabilidade de execução remota de código (CVE-2024-21762) no sistema operacional FortiOS foi explorada antes da divulgação oficial pela Fortinet.

Março

XZ Utils

Uma vulnerabilidade *zero-day* em um pacote de compressão UNIX (CVE-2024-3044), que permitia acesso remoto não autorizado, foi usada em ataques de engenharia social para alterar arquivos do sistema.

Abril

Palo Alto GlobalProtect Gateway

Uma vulnerabilidade explorada como *zero-day* contra a tecnologia GlobalProtect (CVE-2024-3400) foi depois usada por diversos agentes de ameaça.

Maio

Fortinet FortiPortal

Uma vulnerabilidade na plataforma de gerenciamento FortiPortal da Fortinet (CVE-2024-23105) permitia que um invasor não autenticado contornasse a proteção por IP.

Junho

Windows Error Reporting Service

Uma vulnerabilidade *n-day* no serviço de relatório de erros do Windows (CVE-2024-26169), divulgada originalmente em março de 2024, foi explorada por um afiliado do Black Basta, um programa de *Ransomware* como Serviço rastreado pela PwC como White Dev 184 (também conhecido como Storm-1811).

Julho

Vulnerabilidade em hipervisores ESXi explorada por afiliado de RaaS

Foi identificado que um afiliado do programa Black Basta explorou uma vulnerabilidade relacionada a grupos de domínio em hipervisores ESXi (CVE-2024-37085).

Agosto

Ivanti Virtual Traffic Manager

Uma vulnerabilidade crítica no Virtual Traffic Manager (vTM) da Ivanti (CVE-2024-7593) foi divulgada juntamente com a confirmação de que existia uma prova de conceito no momento da divulgação.

Setembro

Exploração do GeoServer por agente de espionagem na região APAC

Um agente de ameaça, identificado em fontes abertas como Earth Baxia, explorou uma vulnerabilidade no GeoServer (CVE-2024-36401), durante intrusões direcionadas a países da região APAC (Ásia-Pacífico).

Outubro

Black Shoggoth explora vulnerabilidade no Internet Explorer

O agente de ameaças Black Shoggoth, sediado na Coreia do Norte e conhecido também como APT37, foi identificado explorando uma vulnerabilidade *zero-day* em uma biblioteca do Internet Explorer para obter acesso inicial (CVE-2024-38178).

Novembro

Botnet desativada volta a operar

Uma rede *proxy* conhecida como *botnet* KV, derrubada em dezembro de 2023 por autoridades dos EUA, foi novamente observada visando dispositivos vulneráveis da Cisco e NetGear.

Dezembro

Nova exploração de vulnerabilidade no Cleo, originalmente identificada em outubro

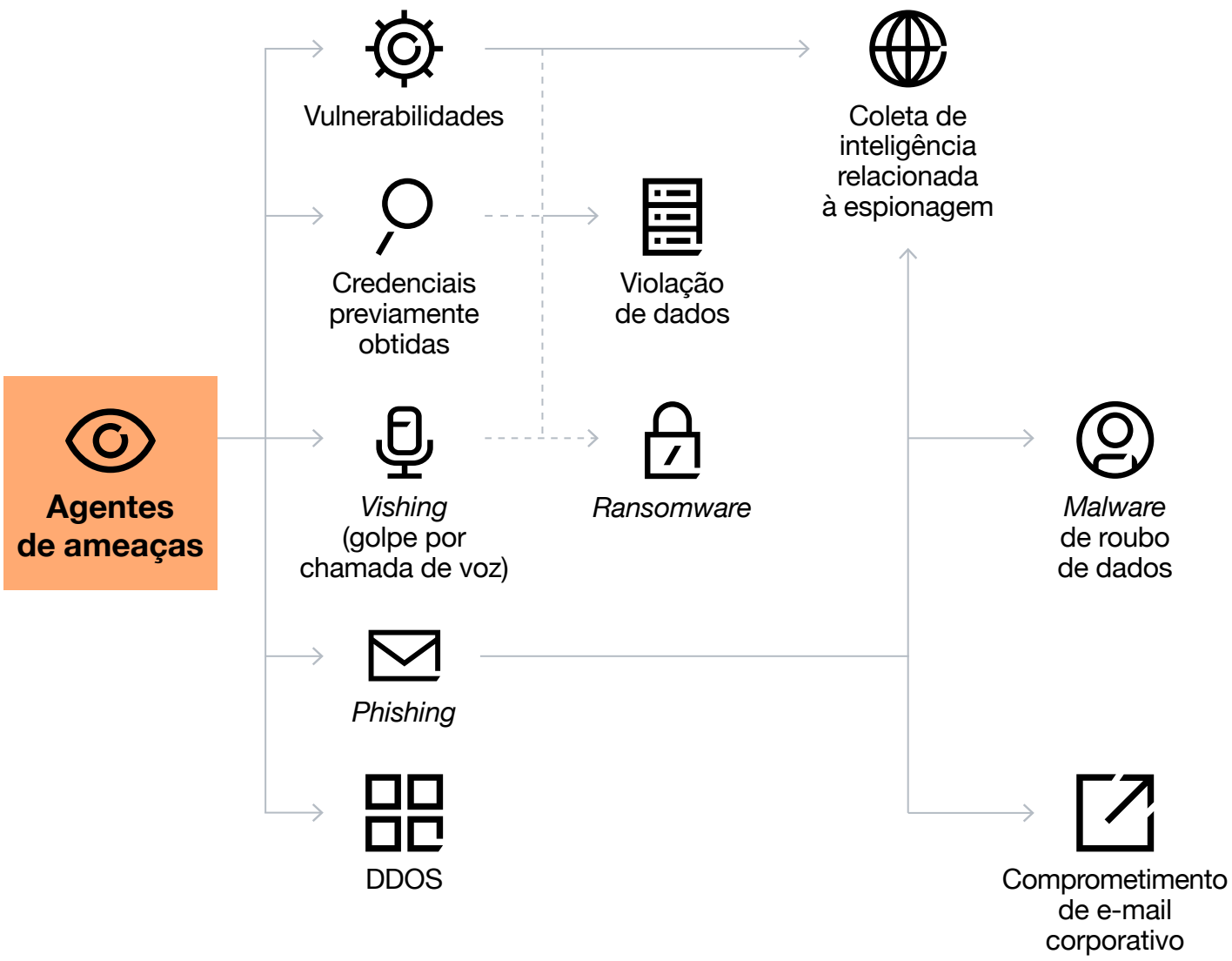
Após a divulgação e correção inicial de uma falha no Cleo em outubro de 2024 (CVE-2024-50623), foi revelado em setembro que agentes de ameaças estavam explorando a nova versão do sistema, mesmo após o *patch*. Até o momento, não havia uma solução definitiva disponível.

2024 em campo – a perspectiva das equipes de resposta a incidentes

Ao longo de 2024, em estreita colaboração com as equipes de resposta a incidentes da rede global da PwC, a equipe de Inteligência de Ameaças identificou tendências consistentes entre agentes com motivações tanto criminosas quanto ligadas à espionagem.

Os dados analisados indicam que o *ransomware* e o comprometimento de e-mails corporativos permaneceram como as principais ameaças no período. Também foram registradas violações de dados com baixa sofisticação, frequentemente seguidas por tentativas de extorsão.

Figura 3 – Principais vetores de acesso inicial e intrusões associadas observados em investigações de resposta a incidentes da PwC em 2024



Nos casos de *ransomware* e violação de dados analisados, poucas ocorrências envolveram técnicas de *phishing*. Em vez disso, os agentes de ameaças geralmente se apoiaram em corretores de acesso inicial (por exemplo, comprando credenciais para acessar o ambiente) ou na exploração de vulnerabilidades conhecidas. Na maioria das situações, essas vulnerabilidades não eram *zero-day*, mas sim falhas mais antigas e já corrigidas, exploradas em tecnologias como:[12]

- Dispositivos Ivanti VPN
- Oracle WebLogic Server
- FortiClient EMS
- VEEAM
- ESXi NAS
- Vulnerabilidade SSL do FortiGate

[12] Nota do analista: a tendência observada em nossos casos de resposta a incidentes não está necessariamente alinhada com os dados históricos mais amplos divulgados por agências de inteligência ocidentais, segundo as quais: “a maioria das vulnerabilidades mais exploradas [em 2023] foi inicialmente utilizada como zero-day, o que representa um aumento em relação a 2022, quando menos da metade das vulnerabilidades mais exploradas foram zero-day.” (Fonte: 2023 Top Routinely Exploited Vulnerabilities, Joint Cybersecurity Advisory, https://media.defense.gov/2024/Nov/12/2003581596/-1/-1/0/CSA-2023-TOP-ROUTINELY-EXPLOITED-VULNERABILITIES.PDF, 12/11/2024). Dados comparativos de 2024 ainda não estão disponíveis, mas avaliamos com probabilidade realista que a principal conclusão dos dados de 2023 – de que zero-days representaram a maioria dos casos – também se mantém válida para 2024. Dessa forma, avaliamos que a diferença entre nossas descobertas e os dados de inteligência se deve a dois fatores principais: a) o tamanho da amostra e b) a diversidade da amostra. A maioria dos casos de resposta a incidentes observados pela PwC teve motivação criminosa, com técnicas, táticas e procedimentos (TTPs) relativamente pouco sofisticados. Esses agentes de ameaça geralmente não dispõem dos recursos ou da capacidade técnica para pesquisar e desenvolver explorações zero-day e, por isso, dependem de provas de conceito mais antigas ou trechos de código disponíveis publicamente, relacionados a vulnerabilidades já conhecidas, para obter acesso aos ambientes das vítimas. Nos casos em que foi identificado o envolvimento de agentes com motivações ligadas à espionagem, observou-se, de fato, o uso de vulnerabilidades zero-day, o que está mais alinhado com o padrão mais amplo de exploração ativa de falhas em ambientes reais (*in-the-wild*).

Muitos desses dispositivos são classificados como “de borda”, posicionados na periferia da infraestrutura de rede das organizações. Geralmente, eles acabam fora dos inventários formais de arquitetura, caracterizando-se como Shadow IT, ou seja, ativos desconhecidos pelos administradores, mas que continuam operando. Como resultado, esses dispositivos permanecem expostos a varreduras públicas de vulnerabilidades e, em muitos casos, ficam fora dos ciclos regulares de atualização de segurança.

Um caso que se destacou por fugir a essa tendência envolveu o *ransomware* White Rabbit, em que há fortes indícios de que o agente de ameaças explorou uma vulnerabilidade do FortiGate recém-divulgada em 2024, coincidentemente no momento exato do comprometimento.

70 das CVEs

adicionadas ao catálogo de Vulnerabilidades Conhecidamente Exploradas envolveram falhas publicadas antes de 2024

Fonte: CISA – Known Exploited Vulnerabilities Catalog (dados acessados em 16/01/2025)

Estudo de caso

Ransomware White Rabbit

Em 2024, uma equipe de Resposta a Incidentes da PwC investigou e analisou uma intrusão realizada por um agente de ameaças que utilizava um binário de criptografia conhecido como White Rabbit. De forma incomum, a exfiltração de dados da vítima ocorreu após a execução do binário de criptografia, e não antes.

A atividade mais antiga identificada no incidente ocorreu três dias antes da criptografia, quando o agente de ameaças acessou o *appliance* de segurança de rede FortiGate, utilizando uma conta de usuário (também chamada de Conta 1).

Embora não tenha sido possível identificar de imediato como o agente de ameaças obteve acesso, avaliou-se com probabilidade realista que uma vulnerabilidade representava uma via de entrada plausível. O *appliance* FortiGate associado estava executando uma versão com duas vulnerabilidades críticas, divulgadas publicamente por volta da época da intrusão. Isso indica que ambas poderiam ter sido exploradas para viabilizar o acesso.

Considerou-se também a possibilidade de que o agente de ameaças tenha obtido previamente as credenciais por meio de um corretor de acesso inicial, embora nenhuma evidência de venda tenha sido encontrada nos fóruns da *dark web* disponíveis. A vítima, por sua vez, não tinha conhecimento da existência da Conta 1 em seu sistema, e essa falta de visibilidade e controle sobre privilégios pode ter permitido que o agente de ameaças acessasse o ambiente sem ser detectado.

Um dia após a atividade inicial de comprometimento, verificou-se que a Conta 1 tinha feito o download de uma variante do *malware* de roubo de credenciais RedLine. Não houve nova atividade por dois dias, até que o agente de ameaça, por meio de uma nova conta de domínio comprometida (Conta 2), realizou uma conexão remota com um servidor da vítima (Servidor 1).

Em seguida, ele implantou uma variante da *botnet* Amadey, renomeada como svchost.exe. A funcionalidade dessa instância do Amadey era fazer o download e a execução de um *payload* de segunda etapa.[13]

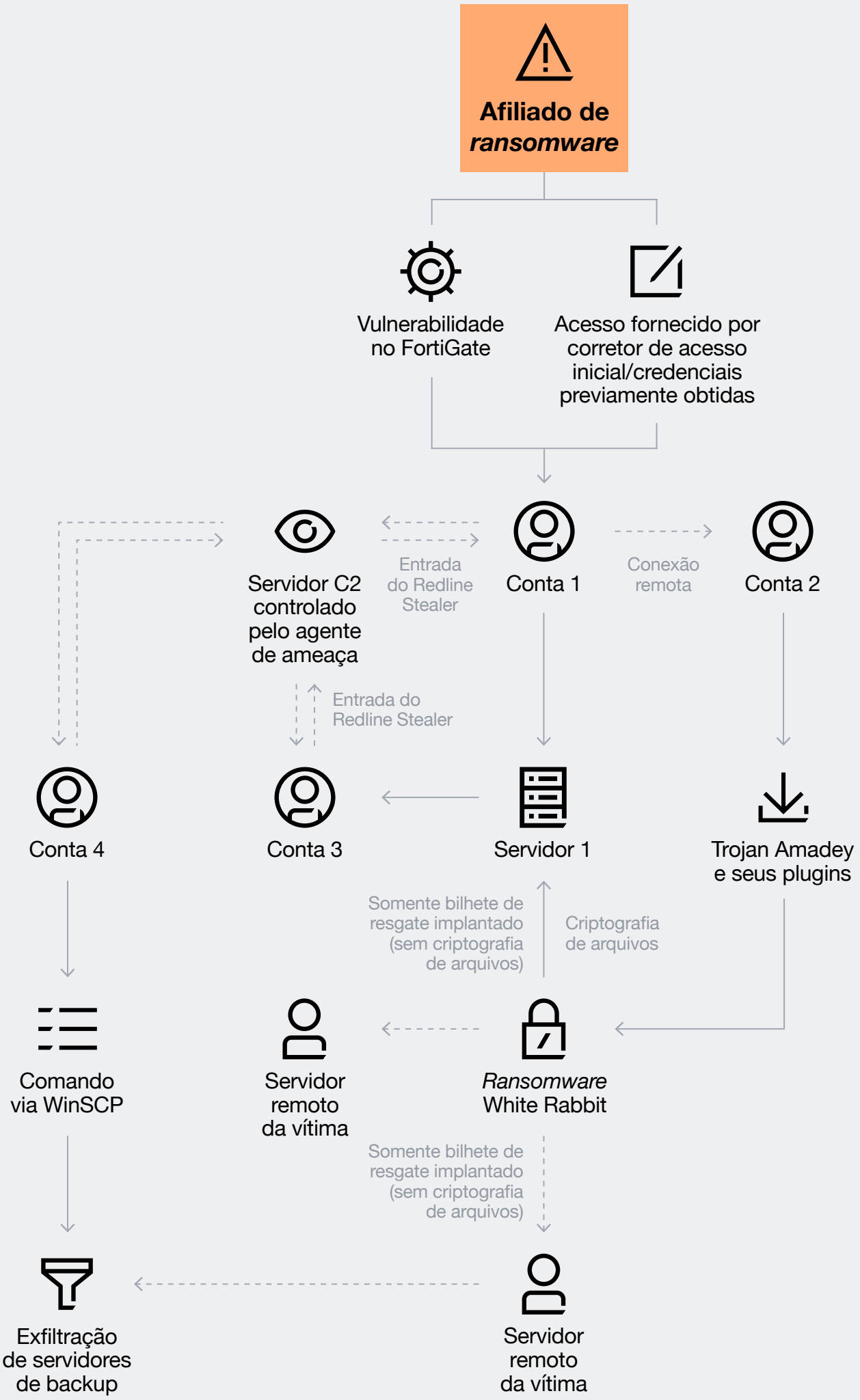
No momento da análise, esse arquivo já havia sido removido do sistema. No entanto, evidências forenses obtidas por meio da análise de *logs* levaram a PwC a avaliar que o *payload* da segunda etapa era, com alta probabilidade, uma variante do binário de criptografia White Rabbit. O momento em que o bilhete de resgate foi inserido em pastas locais, assim como a criptografia de determinados arquivos, coincidiu com a execução desse *payload*.

O agente de ameaças retornou ao ambiente no dia seguinte, provavelmente porque o processo de criptografia do sistema de arquivos da vítima não foi concluído como planejado – apenas um servidor ESXi e um servidor Windows foram afetados, enquanto os demais servidores remotos e virtuais permaneceram intactos.

Durante a investigação, foi identificada uma Conta 3, que também realizou o download do mesmo binário do RedLine. Já uma Conta 4 foi responsável por baixar três discos de *backup*, utilizando a ferramenta legítima WinSCP para transferir os arquivos a um servidor remoto controlado pelo agente de ameaça. Esse comportamento indica uma tentativa do agente de manter persistência no ambiente da vítima mesmo após a criptografia.

[13] Nota do analista: diante dos plugins residuais do Amadey encontrados no ambiente da vítima, é provável que o agente de ameaça tenha utilizado essa ferramenta para realizar uma identificação mais aprofundada do ambiente (*fingerprinting*) e manter persistência. Para mais informações, consulte: "I Amadey-ngerous stealer", PwC Threat Intelligence, CTO-TIB-20241209-01A.

Figura 4 – Visualização da intrusão do *ransomware* White Rabbit observada por uma equipe de resposta a incidentes da PwC



2024 termina – um novo ano de incerteza começa

Como em todas as retrospectivas, as lições aprendidas e observações feitas ao longo do ano também podem ser usadas para projetar meses à frente. As tensões geopolíticas se intensificaram em praticamente todas as principais regiões, acompanhadas por mudanças significativas de liderança em um número incomum de países – resultado de uma sucessão de eleições previstas e inesperadas, assim como de instabilidades políticas. Embora essas dinâmicas já tenham influenciado consideravelmente a atividade no domínio cibernético ao longo de 2024, é provável que seus efeitos se estendam por todo o ano de 2025.

Crime

- O ecossistema do crime cibernético permaneceu como um dos principais agentes de disrupção em praticamente todos os setores, com números sem precedentes de vazamentos de sites de *ransomware*, apesar do sucesso de ações de combate e repressão conduzidas por autoridades legais.
- Também foi um ano com ataques de grande repercussão, que levaram a pagamentos milionários e afetaram cadeias de suprimento, mostrando que empresas de todos os portes permanecem vulneráveis a ameaças de *ransomware*.
- Avaliamos como altamente provável que, mesmo com os avanços das autoridades, o ecossistema de *ransomware* continue representando uma das principais ameaças em 2025 para organizações de todos os portes e setores.

Avaliamos que o cenário de ameaças cibernéticas em 2025 provavelmente será igualmente influenciado pelas tensões políticas atuais:

China/Taiwan

- É provável que agentes de ameaças sediados na China continuem a mirar entidades em Taiwan para atividades de espionagem,[14] [15] [16] [17] com foco específico em departamentos de defesa e governo. Também existe a possibilidade de que esses agentes tentem se infiltrar em infraestruturas críticas nacionais, com o objetivo de preparar terreno para possíveis operações de sabotagem, caso isso se torne necessário.[18]

- Consideramos muito provável que os exercícios militares realizados pelas Forças Armadas da China (Exército de Libertação Popular) no final de 2024 indiquem que Pequim continuará demonstrando interesse estratégico no Mar da China Oriental em 2025,[19] quase certamente acompanhado por atividades cibernéticas relacionadas.

[14] PingPong pings on FortiGates in Taiwan', PwC Threat Intelligence, CTO-TIB-20241204-01A
[15] 'Into the Spyder-verse', PwC Threat Intelligence, CTO-TIB-20240620-01A
[16] 'Look what the ToddyCat dragged in', PwC Threat Intelligence, CTO-TIB-20240524-01A
[17] 'New targets, same Moros', PwC Threat Intelligence, CTO-TIB-20240219-01A
[18] Nota do analista: agentes de ameaça ligados à China já haviam sido identificados, tanto no passado quanto ao longo de 2024, infiltrando redes de infraestrutura crítica nacional com o objetivo de estabelecer pontos de apoio que possam ser usados em futuras operações de sabotagem. Para informações sobre a atividade de 2024, consulte: 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure', CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a (7/2/2024)
[19] 'Big Chinese naval exercise leaves Taiwan and US struggling for response', Financial Times, https://www.ft.com/content/025a81f1-2cb2-459d-8427-46fd44b1b2c3 (14/12/2024)

Relações China/EUA

- A atividade de grupos de ameaças ligados à China contra os Estados Unidos e seus aliados já era substancial antes de 2024, com foco principalmente em campanhas de espionagem voltadas a governos e setores de defesa em escala global. Essa atividade aumentou ainda mais ao longo de 2024. Tendências anteriores, como o uso intenso de redes *proxy* comerciais para infiltrar sistemas (conhecido como CNE – exploração de redes por computador), também continuaram, com um interesse crescente em manter infraestruturas críticas adversárias em risco.

- O ano também registrou aumento no número de comunicados conjuntos emitidos por órgãos do governo dos EUA sobre atividades atribuídas à China, assim como alertas das autoridades chinesas a respeito de campanhas supostamente conduzidas por agências norte-americanas.[20] As declarações de Pequim trouxeram ainda novas queixas, classificando os relatos ocidentais sobre ações de espionagem chinesa como "manipulação".[21] [22] Avaliamos, com probabilidade realista que, se as tensões entre China e Estados Unidos continuarem, esse jogo de acusações e contra-acusações no campo cibernético deve persistir em 2025. No entanto, não esperamos que isso afete significativamente as operações ofensivas conduzidas por nenhum dos dois países.

- Consideramos provável que o ritmo atual das operações de grupos de ameaça ligados à China e aos Estados Unidos aumente ou comece a se intensificar, especialmente em setores considerados parte da infraestrutura crítica nacional, à medida que crescem as tensões entre Pequim, Washington e outras capitais ocidentais.

[20] 'CNCERT发现处置两起美对我大型科技企业机构网络攻击事件', CNCERT/CC, https://www.cert.org.cn/publish/main/49/2024/20241218184234131217571/20241218184234131217571_.html (18/12/2024)
[21] 'China hits out at US and UK over cyber hack claims', BBC, https://www.bbc.com/news/world-asia-china-68655786 (24/3/2024)
[22] 'The Scapegoat Strikes Back', Beijing Review, https://www.bjreview.com/Opinion/Pacific_Dialogue/202410/t20241028_800381804.html (28/10/2024)

Ásia de forma mais ampla

- A dinâmica regional entre China e Índia continuou complexa em 2024, com tensões entre os dois países levando agentes de ameaça, tanto chineses quanto indianos, a se concentrarem em objetivos de espionagem, não apenas um contra o outro, mas também envolvendo outros países asiáticos.[23] [24] [25] [26] Avaliamos que, caso essas tendências persistam, a relação política entre Índia e China continuará influenciando de forma relevante as atividades cibernéticas realizadas por agentes desses dois países em 2025 e nos anos seguintes.

- Agentes de ameaça vinculados à Coreia do Norte estiveram mais ativos em 2024 do que no ano anterior, deixando de lado ataques em larga escala a cadeias de suprimento e retomando operações de intrusão mais tradicionais, como as dos anos anteriores. O escândalo envolvendo trabalhadores de TI – embora não tenha surgido em 2024 – se destacou como uma das campanhas mais recorrentes, combinando ganhos financeiros (por meio de salários legítimos e tentativas de extorsão) com coleta de dados sensíveis por motivações de espionagem.

Rússia, Ucrânia e OTAN

- Grande parte da atividade cibernética russa observada em 2024 permaneceu alinhada com as prioridades da política externa do país – ou seja, a Ucrânia e o bloco da OTAN.[27] [28]

- Avaliamos como altamente provável que agentes de ameaças com base na Rússia continuem direcionando seus ataques a instituições ucranianas, especialmente nas áreas de governo, defesa e infraestrutura crítica nacional, além de adotarem alvos semelhantes em países aliados que oferecem apoio militar à Ucrânia.

[23] 'Red Ishtars snea-key return', PwC Threat Intelligence, CTO-TIB-20240215-01A
[24] 'Red Lich's Nim-ble Loaders', PwC Threat Intelligence, CTO-TIB-20241223-01A
[25] 'SuperJumping to Connect Secure', PwC Threat Intelligence, CTO-QRT-20240124-01A
[26] 'The elephant in many rooms - a technical analysis', PwC Threat Intelligence, CTO-TIB-20241118-01A
[27] Blue Dev 8's net on Ukraine', PwC Threat Intelligence, CTO-TIB-20240520-01A
[28] 'Blue Athena Dumps Webhooks into the Water', PwC Threat Intelligence, CTO-TIB-20240214-01A

Oriente Médio

- Grupos de ameaças iranianos aumentaram novamente o ritmo de suas operações em 2024, em linha com os acontecimentos que marcaram a região ao longo do ano. Entidades de outros países do Oriente Médio – como Turquia e Azerbaijão,[29] além de Omã e Emirados Árabes Unidos – também foram alvo de ataques.[30]

- Em contraste, houve queda significativa nas atividades cibernéticas de agentes regionais associados a grupos apoiados pelo Irã, como o Grey Karkadann e o Grey Hades. Essa redução coincidiu com o aumento dos ataques de Israel contra infraestrutura física nos países onde esses grupos provavelmente estão baseados.[31]

[29] 'There's plenty more SeaSickle on the C2', PwC Threat Intelligence, CTO-TIB-20241218-01A
[30] 'Muddy, muddle tools and trouble; FranChis loader, SeaSickle, Bubble', PwC Threat Intelligence, CTO-TIB-20241030-01A
[31] 'Battlefield setbacks reduce cyber capacities for Hamas and Hezbollah but not Iran', PwC Threat Intelligence, CTO-SRT-20241213-01A

Seção dois

Maré crescente que levanta todos os barcos

Por trás de grande parte das atividades de agentes mal-intencionados ao longo de 2024 está a crescente disponibilidade de códigos e ferramentas de código aberto, além do avanço na sofisticação e da facilidade de uso desses recursos.

Essa combinação trouxe grandes benefícios, especialmente para os agentes com menor nível técnico, principalmente no cenário do crime cibernético. Muitos operadores conseguiram criar seus próprios *malware* e programas de afiliados a partir de bases de código abertas, exigindo pouca habilidade técnica para desenvolver ou manter essas ferramentas.

As operações de agentes de ameaças foram muito impactadas pelos seguintes fatores:

Ferramentas geradas por IA: em sua maioria, essas ferramentas têm sido usadas em ataques de engenharia social, mas já há indícios de que agentes maliciosos também as usam no desenvolvimento de suas próprias ferramentas.

Aumento geral no número de provas de conceito (POCs) e soluções para vulnerabilidades de dia zero e dia N. Esse crescimento provavelmente está relacionado ao maior número de pessoas capacitadas pesquisando tecnologias vulneráveis. O avanço dos programas de recompensas por *bugs* (*bug bounty*) e o acesso mais fácil a treinamentos e capacitação em exploração de falhas estão entre os principais impulsionadores dessa tendência.

Vulnerabilidades se tornando mais acessíveis a um número maior de agentes de ameaças. Isso ocorre devido à disponibilidade de códigos de exploração em POC e à existência de comunidades ativas – que incluem tanto pesquisadores de segurança quanto agentes maliciosos – focadas em descobrir novas formas de explorar códigos.

Crescimento geral de ecossistemas facilitadores, como os mercados de *ransomware* e de *stealers* (*malwares* que roubam dados): com mais pessoas envolvidas em atividades maliciosas, o volume de ferramentas, ideias e operações cresceu, alimentando ainda mais a fragmentação do cenário cibernético. Isso deve tornar o controle desse ambiente cada vez mais difícil nos próximos anos.

A intervenção da IA

A IA é uma área relevante de pesquisa e investimento na área de cibersegurança há algum tempo, e certamente ela não foi novidade em 2024. No entanto, do ponto de vista do comportamento dos agentes de ameaças, o ano marcou o início do que podemos considerar um passo rumo à popularização do uso da IA nesse contexto.

Os avanços em tecnologias baseadas em IA, amplamente disponíveis, abriram várias possibilidades para os agentes maliciosos, especialmente nas fases iniciais da cadeia de ataque (como reconhecimento e acesso inicial).[32] Embora se espere que esses agentes continuem testando diferentes técnicas de acesso, é provável que algumas abordagens e métodos se tornem mais padronizados à medida que demonstrem ser mais eficazes do que outros.

Com isso, avaliamos que em 2025 haverá uma continuidade nos testes e uso de ferramentas baseadas em IA, com algumas delas se consolidando como preferidas entre os agentes de ameaças com menor nível técnico.

[32] 'The Evolution Of Social Engineering And Phishing In The Age Of Artificial Intelligence', Lumen, https://blog.lumen.com/the-evolution-of-social-engineeringand-phishing-in-the-age-of-artificial-intelligence/ (5/8/2024)

Tabela 1 – Desenvolvimento e detecção relacionados a conteúdo gerado por IA e seu uso por agentes de ameaças

Fácil | Moderado | Moderado/Difícil | Difícil | Muito difícil

Tipo de conteúdo gerado por IA	Exemplos de uso por agentes de ameaças	Dificuldade de gerar conteúdo	Dificuldade de detecção sem meios técnicos	Dificuldade de detecção com meios técnicos
Texto: comunicação	E-mails de *phishing* para tentativas de intrusão e ataques com fins financeiros	Diversas ferramentas com dados de treinamento disponíveis; possibilidade de adicionar dados	Requer alfabetização midiática elevada e que o conteúdo seja geralmente impreciso ou irregular, o que nem sempre acontece	Existem diversas ferramentas com diferentes níveis de precisão
Texto: código de computador	Desenvolvimento de *malware*	Diversas ferramentas disponíveis; possibilidade de adicionar dados de treinamento	Requer habilidade para detectar irregularidades ou erros no código, que podem não estar presentes	Existem diversas ferramentas com diferentes níveis de precisão
Imagem	Campanhas de desinformação	Diversas ferramentas com dados de treinamento disponíveis	Avanços nas tecnologias de IA generativa estão superando os indicadores detectáveis	Existem poucas ferramentas com diferentes níveis de precisão
Áudio	*Deepfake* da voz de um executivo em ataque com motivação financeira	Ferramentas disponíveis para texto-para-fala com áudio realista; possibilidade de adicionar amostras de voz como dados de treino	Avanços nas tecnologias de IA generativa estão produzindo amostras de áudio quase indistinguíveis da fala humana	Existem poucas ferramentas com diferentes níveis de precisão
Vídeo (com e sem áudio)	*Deepfake* de executivo usado em videochamada em ataque com motivação financeira	Poucas ferramentas com dados de treinamento disponíveis	Inconsistências na geração são compensadas pela baixa conscientização do público	Existem poucas ferramentas com diferentes níveis de precisão

A engenharia social, especialmente nas técnicas de acesso inicial, que já é um método popular usado por cibercriminosos para se infiltrar em organizações,[33] [34] foi amplamente explorada em 2024. Grupos afiliados de *ransomware* (além do White Dev 164, também conhecido como Scattered Spider) e agentes de comprometimento de e-mails corporativos (BEC) utilizaram textos de e-mail, áudios e até vídeos gerados por IA para manipular e enganar as vítimas.[35] [36] [37] [38]

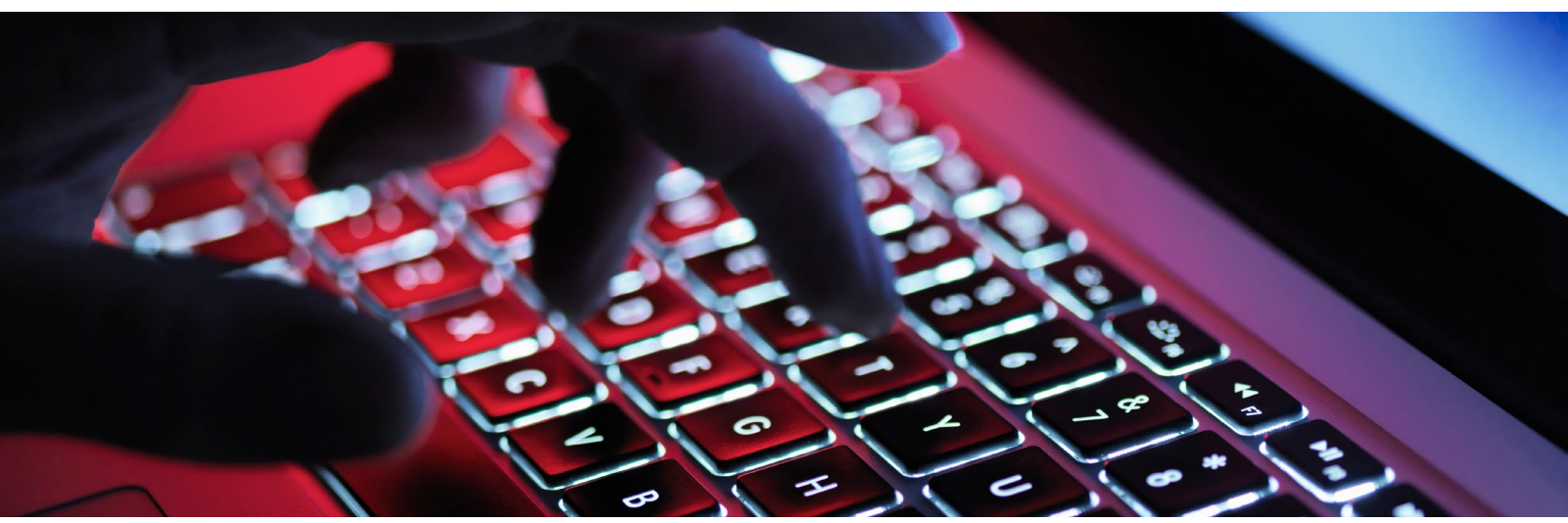
O uso de *malwares* gerados por IA também se consolidou como uma tendência ao longo de 2024, com diversos *loaders* (carregadores de *malware*) e scripts em PowerShell identificados como tendo sido criados com o auxílio de modelos de linguagem de grande escala (LLMs).[39] [40] [41]

[33] 'Scattered Spider', US CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a (16/11/2023)
[34] 'Business Email Compromise – A Primer', PwC Threat Intelligence, CTO-TIB-20240729-01A)
[35] 'White Dev 184's ScreenConnect Obsession', PwC Threat Intelligence, CTO-TIB-20240827-01A
[36] 'UK engineering firm Arup falls victim to £20m deepfake scam', *The Guardian*, https://www.theguardian.com/technology/article/2024/may/17/uk-engineeringarup-deepfake-scam-hong-kong-ai-video (17/5/2024)
[37] '#StopRansomware: Black Basta', US CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a (8/11/2024)
[38] "Quishing', 'vishing' and AI scams – the new cybercriminal techniques duping Australians', *The Guardian*, https://www.theguardian.com/technology/2024/nov/20/quishing-vishing-and-ai-scams-the-new-cybercriminal-techniques-duping-australians (19/11/2024)
[39] 'Security Brief: TA547 Targets German Organizations with Rhadamanthys Stealer', ProofPoint, 10/4/2024
[40] 'Threat Insights Report: September 2024', HP Wolf Security, https://threatresearch.ext.hp.com/wp-content/uploads/2024/09/HP_Wolf_Security_Threat_Insights_Report_September_2024.pdf (24/9/2024)
[41] 'An update on disrupting deceptive uses of AI', OpenAI, https://openai.com/global-affairs/an-update-on-disrupting-deceptive-uses-of-ai/ (9/10/2024)

Essas tendências relacionadas à IA não ocorrem de forma isolada – elas ocorrem em paralelo a outras mudanças significativas que marcaram o ano de 2024. A criação de LLMs menos regulamentados,[42] o crescimento do ecossistema do crime cibernético em termos de ferramentas, e o aumento na presença de provas de conceito (POCs) ao longo do ano apontam para um futuro em que tanto agentes de ameaças menos sofisticados, com baixa barreira de entrada, quanto grupos mais experientes e organizados, encontrarão mais facilidade e sucesso na fase de acesso inicial das operações:

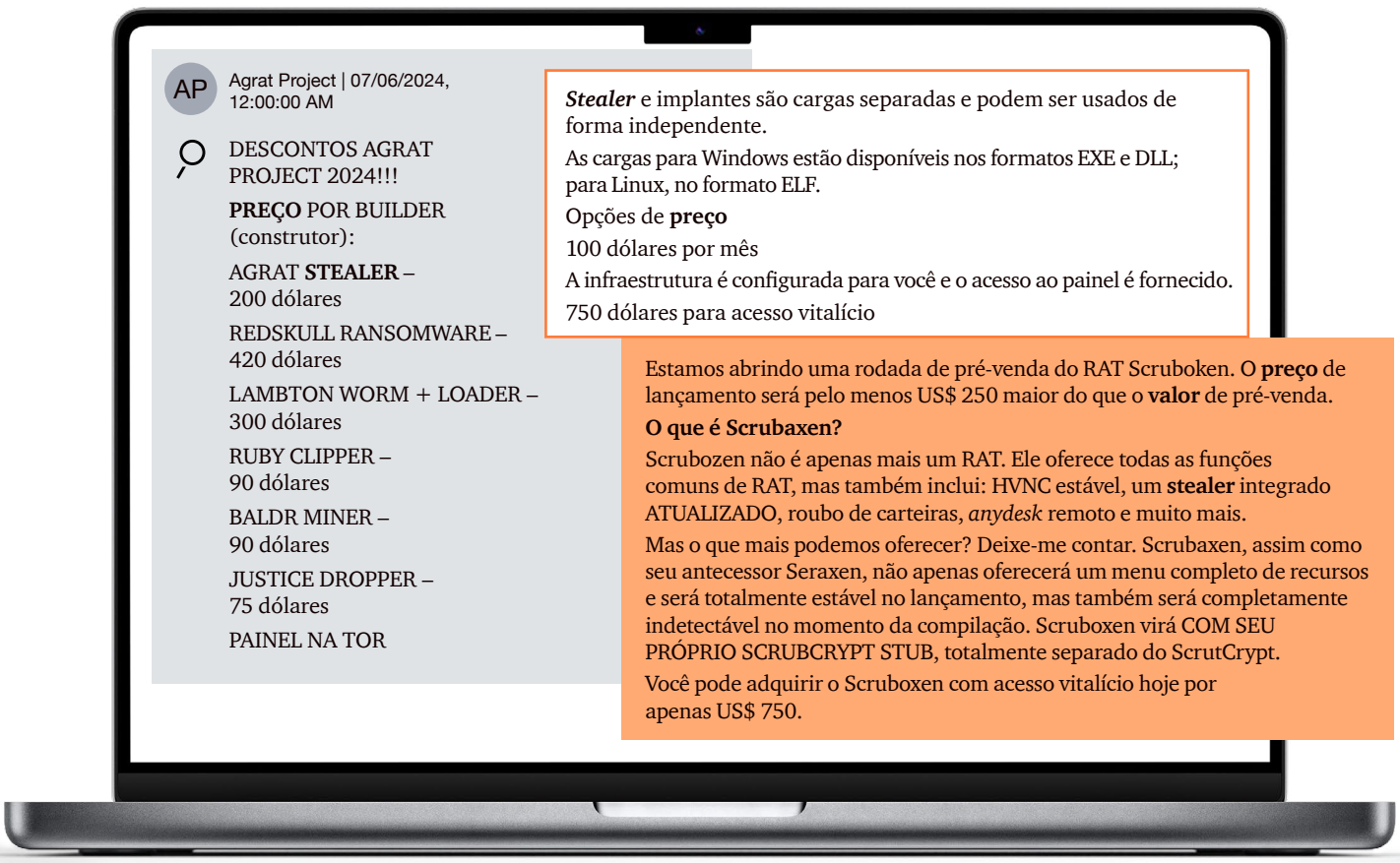
Ameaças com baixa barreira de entrada: esses agentes representam um desafio pelo grande volume de ataques, normalmente utilizando *phishing* ou engenharia social gerados por IA, combinados com programas de roubo de informações de código aberto ou de baixo custo, para capturar credenciais.[43]

Essas credenciais podem ser vendidas em grande quantidade na *dark web* ou negociadas individualmente como parte de serviços de acesso inicial (*initial access brokering*). A tendência é que esse tipo de intrusão se torne cada vez mais comum, e os elementos baseados em IA tendem a tornar essas operações ainda mais eficazes.



[42] 'Dark LLMs aka BlackHat GPTs and Malicious AIs', GitHub, https://github.com/cybershujin/Threat-Actors-use-of-Artifical-Intelligence/blob/main/Dark%20LLMs%20and%20Malicious%20AIs.MD (15/5/2024)
[43] 'Breaking down the -as-a-Service industry', PwC Threat Intelligence, CTO-SIB-20240814-01A

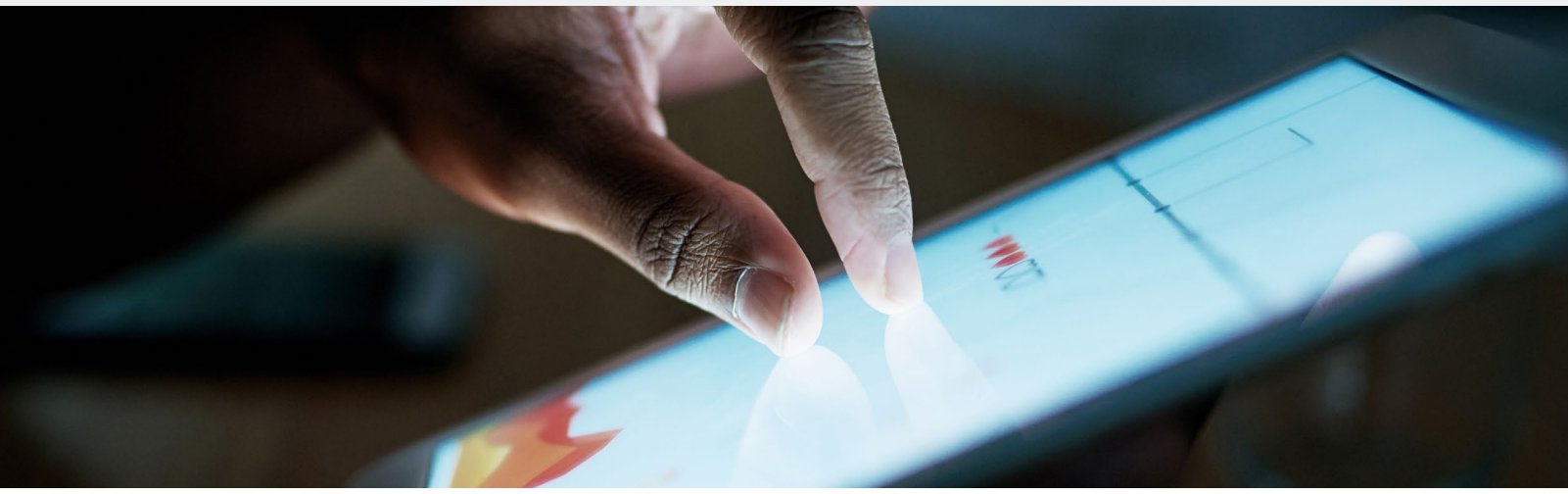
Figura 5 – Exemplos de *stealers* sendo anunciados em diversos fóruns da *dark web* em 2024



Ameaças mais sofisticadas: esses agentes de ameaças provavelmente não vão alterar muito suas táticas, técnicas e procedimentos (TTPs), mas buscarão iterar continuamente sobre seus processos de ataque. Isso deve continuar ocorrendo principalmente nas fases de reconhecimento e acesso inicial da operação, em que esforços de engenharia social e coerção, assim como meios eficazes de coleta de inteligência sobre o alvo, podem se beneficiar do fácil acesso a modelos de linguagem de grande porte (LLMs) e ferramentas de IA generativa.

- Em 2024, observamos um aumento significativo no oportunismo dentro do ecossistema do crime cibernético, tanto entre afiliados de *ransomware* quanto entre agentes de ameaças mais genéricas, como ladrões de informações e grupos focados em comprometimento de e-mails corporativos (BEC). As táticas incluíram a compra de credenciais, ataques automatizados de *credential stuffing*, varredura e exploração de vulnerabilidades, além de campanhas massivas de *phishing*.

- Ferramentas baseadas em IA podem contribuir de alguma maneira para todas essas técnicas, mas, de forma significativa, o surgimento de ferramentas orientadas por IA cria o potencial para um aumento na segmentação de alvos – e o retorno do chamado *"Big Game Hunting"*.[44] O ano de 2024 trouxe exemplos de como esse tipo de ataque pode ser lucrativo,[45] [46] e avaliamos, com uma probabilidade realista, que o cenário atual da IA oferece mais oportunidades do que nunca para esse tipo de ofensiva.



[44] Nota do analista: Big Game Hunting é o termo usado para descrever intrusões – neste caso, especificamente relacionadas a ransomware – que têm como alvo entidades específicas, geralmente com um esforço considerável nas fases de reconhecimento e desenvolvimento de recursos da operação. O objetivo do Big Game Hunting é concentrar o máximo de recursos em uma única intrusão para aumentar ao máximo as chances de sucesso e o retorno financeiro resultante.
[45] 'Dark Angels ransomware receives record-breaking $75 million ransom', *Bleeping Computer*, https://www.bleepingcomputer.com/news/security/dark-angelsransomware-receives-record-breaking-75-million-ransom/ (30/7/2024)
[46] Nota do analista: isso não significa que ataques oportunistas também não tenham sido lucrativos. O agente de ameaça por trás do ataque de ransomware que resultou em um pagamento de US$ 22 milhões à Change Healthcare utilizou *credential stuffing* como método de acesso inicial (ver: "Testemunho de Andrew Witty, CEO do UnitedHealth Group, ao Subcomitê de Supervisão e Investigações do Comitê de Energia e Comércio da Câmara – 'Examinando o Ciberataque à Change Healthcare'", TechCrunch, https://www.documentcloud.org/documents/24626988-uhgs-witty-house-testimony – 1/5/2024).

A lacuna de competências em *zero-day* continua diminuindo

- Na retrospectiva de 2023, destacamos como o uso crescente de vulnerabilidades como ponto de acesso inicial estava se espalhando – especialmente no contexto do crime cibernético.[47]
- Em 2024, não só essa tendência continuou como também foi possível observar um aumento no número de incidentes envolvendo o uso de vulnerabilidades *zero-day* e *n-day* – tanto por grupos com motivação criminosa quanto por aqueles voltados à espionagem.[48 49 50] Os dados mostram um aumento de 20% no número de vulnerabilidades exploradas entre 2023 e 2024,[51] além de um crescimento de 31% nas vulnerabilidades divulgadas publicamente.[52]
- Agentes de ameaças com capacidade para pesquisar e desenvolver *zero-days* fizeram isso de forma consistente, enquanto grupos criminosos – especialmente afiliados de *ransomware* – exploraram códigos de prova de conceito (PoC) liberados após as divulgações iniciais.[53 54 55]
- Ainda assim, observamos que agentes menos sofisticados estão aproveitando vulnerabilidades mais antigas nas fases iniciais de acesso,[56 57] enquanto agentes mais avançados – com foco em espionagem – tendem a evitar o uso dessas falhas após as intrusões iniciais.[58] Avaliamos que o uso contínuo de vulnerabilidades antigas provavelmente visa estabelecer acessos rápidos e eficazes em ambientes das vítimas – com foco especial em dispositivos de borda obsoletos (*end-of-life*) que frequentemente permanecem sem atualizações de segurança.

[47] 'Cyber Threats 2023: A Year in Retrospect', PwC Threat Intelligence, CTO-YIR-20240624-01A
[48] 'Breaking down the -as-a-Service industry', PwC Threat Intelligence, CTO-SIB-20240814-01A
[49] '541 Jump street, PwC Threat Intelligence, CTO-TIB-20241121-01A
[50] 'Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption', Microsoft, https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/ (24/7/2024)
[51] 2024 Trends in Vulnerability Exploitation', *VulnCheck*, https://vulncheck.com/blog/2024-exploitation-trends (3/2/2025)
[52] NVD, https://nvd.nist.gov/
[53] 'SonicWall SSLVPN access control flaw is now exploited in attacks', *Bleeping Computer*, https://www.bleepingcomputer.com/news/security/sonicwall-sslvpnaccess-control-flaw-is-now-exploited-in-attacks/ (6/9/2024)
[54] 'Critical Veeam Vulnerability Exploited to Spread Akira and Fog Ransomware', *The Hacker News*, https://thehackernews.com/2024/10/critical-veeamvulnerability-exploited.html
[55] 'CISA confirms critical Cleo bug exploitation in ransomware attacks', *Bleeping Computer*, https://www.bleepingcomputer.com/news/security/cisa-confirmscritical-cleo-bug-exploitation-in-ransomware-attacks/ (13/12/2024)
[56] 'A look into an affiliates operations', *PwC Threat Intelligence*, CTO-TIB-20240426-02A
[57] Threats Under the Spotlight 2024 Issue 4, *PwC Threat Intelligence*, CTO-TUS-20240607-01A
[58] Nota do analista: isso nem sempre é o caso, como demonstrado pelo agente de ameaça Blue Dev 5, com base na Rússia (também conhecido como APT29 ou Midnight Blizzard); ver: 'Update on SVR Cyber Operations and Vulnerability Exploitation', Joint Cybersecurity Advisory, https://www.ic3.gov/CSA/2024/241010.pdf (10/10/2024)

Crescimento dos ecossistemas

O mercado do crime cibernético se expandiu em 2024, impulsionado pela crescente disponibilidade de bases de código aberto e pela maturidade cada vez maior de agentes consolidados, capazes de iterar continuamente sobre suas TTPs.

O resultado dessas condições pode ser observado no aumento do número de ferramentas disponíveis no cenário criminoso – que, assim como um mercado legítimo, avança com base na concorrência saudável, sendo a facilidade de uso, o preço e a funcionalidade os principais atrativos para os agentes de ameaças.

O mercado de *information stealers* e o ecossistema de *ransomware* tiveram um 2024 especialmente bem-sucedido, em parte graças à capacidade de novos agentes de reaproveitar bases de código mais antigas.[59] [60] [61]

Por outro lado, programas mais estabelecidos – como StealC, DarkGate e Latrodectus –[62] [63] apostaram em ciclos contínuos de desenvolvimento, com seus desenvolvedores atualizando constantemente as bases de código para incluir novas funcionalidades.

[59] 'The Curious Case of an Open Source Stealer: Phemedrone', SpyCloud, https://spycloud.com/blog/phemedrone-stealer/ (6/9/2024)
[60] 'Kematian-Stealer : A Deep Dive into a New Information Stealer', Cyfirma, https://www.cyfirma.com/research/kematian-stealer-a-deep-dive-into-a-newinformation-stealer/ (6/7/2024)
[61] 'RansomHub Ransom Run', PwC Threat Intelligence, CTO-TIB-20241108-01A
[62] 'Closing the DarkGate after the horse has DanaBot(ted)', PwC Threat Intelligence, CTO-TIB-20241203-01A
[63] 'Digging through a Badgers (data)Sett', PwC Threat Intelligence, CTO-TIB-20241015-02A

Figura 6 – Visualização do papel dos *infostealers* no ecossistema mais amplo do cibercrime

Em destaque: StealC

O StealC é um *infostealer* multifuncional que foi anunciado pela primeira vez no fórum da *dark web* Russian Marketplace em janeiro de 2023 e se manteve entre os mais procurados ao longo de 2024. O desenvolvedor do StealC (monitorado pela PwC sob o codinome White Dev 183) admitiu ter se inspirado em outras bases de código de *infostealers*, incluindo Vidar, Raccoon, Mars e Redline.

Figura 7 – Trecho de uma publicação do desenvolvedor do StealC no fórum XSS

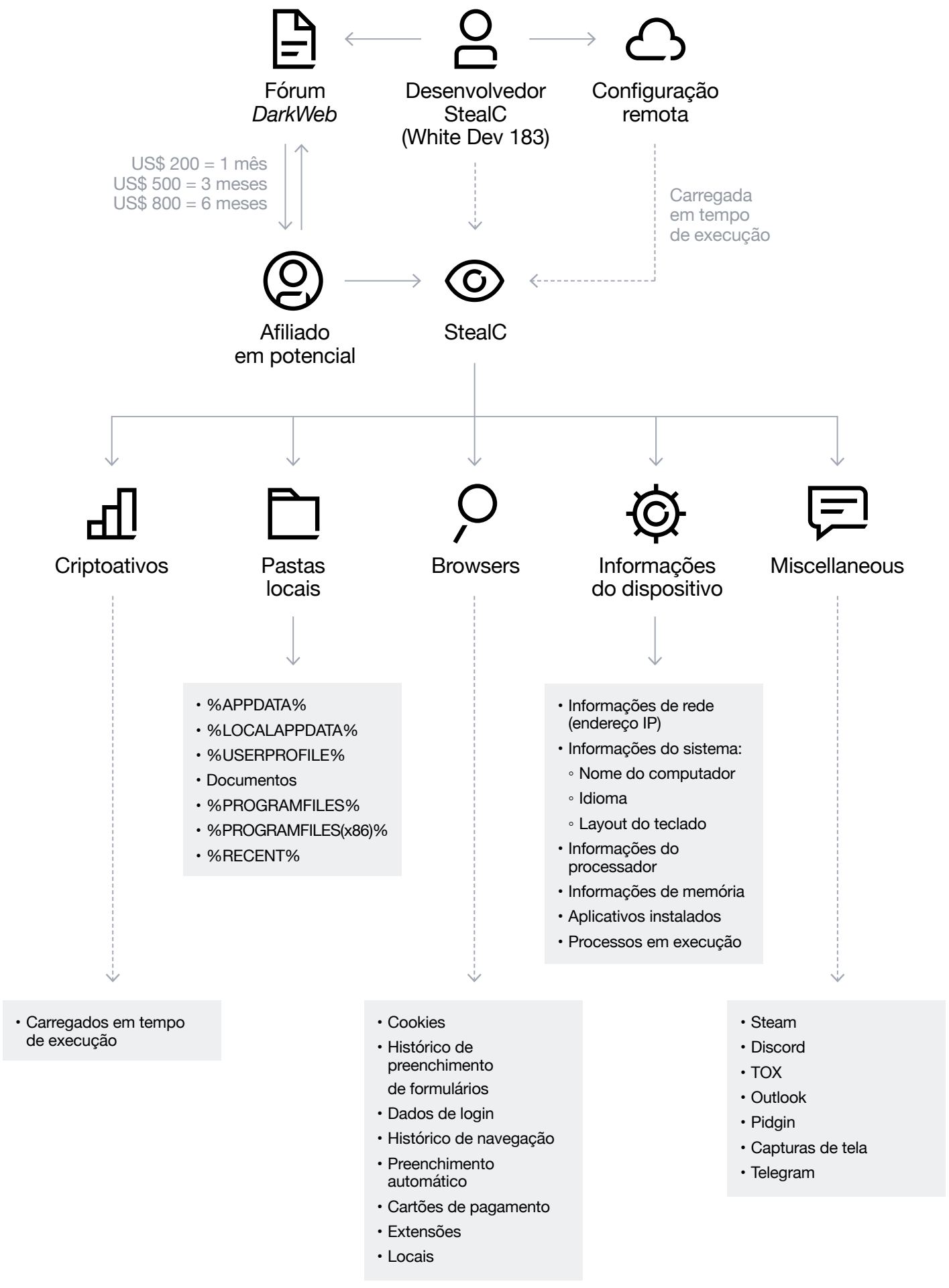
Assim como outros *infostealers* populares, o StealC é comercializado por meio de um modelo de assinatura: US$ 200 por um mês de acesso, US$ 500 por três meses e US$ 800 por seis meses.

Esse valor inclui acesso a um painel com interface gráfica que permite ao afiliado pesquisar e filtrar os *logs* obtidos. O painel também permite personalizar a *build* do *malware* – como as plataformas das quais roubar informações, o destino dos *logs* e a configuração de funcionalidades adicionais (por exemplo, capacidade de capturar *screenshots* e de se autoexcluir do disco).

O StealC se apresenta como tendo uma funcionalidade única: a capacidade de baixar seus módulos e componentes de *infostealer* durante a execução, em vez de tê-los codificados diretamente na base de código. Em teoria, isso garante que o *stealer* seja sempre executado com as funcionalidades mais atualizadas.

O comportamento de roubo do StealC é estruturado da seguinte forma: antes de extrair qualquer dado de qualquer categoria (como navegadores), o *malware* entra em contato com seu servidor de Comando e Controle (C2) por meio de uma requisição POST, para obter instruções sobre o que deve ser coletado. Em seguida, realiza o roubo e se comunica novamente com o C2 para enviar os dados obtidos.

Figura 8 – Visualização da funcionalidade do StealC



Um dos aspectos mais interessantes do programa StealC é a discussão oficial em fóruns da *dark web* que o acompanha, incluindo conversas sobre o uso de vários *infostealers* em conjunto com o StealC para maximizar a eficiência operacional. Para um mercado que funciona de forma semelhante ao ecossistema de *ransomware* – com concorrentes disputando o mesmo grupo de afiliados – esse nível de cooperação é surpreendente.

Embora nem todos os desenvolvedores de *infostealers* ajam dessa forma, o StealC se tornou um dos *stealers* mais populares de 2024, provavelmente devido a uma combinação de facilidade de uso, preço acessível e à comunicação do desenvolvedor com os afiliados.

O StealC é apenas um entre muitos *infostealers*, em um mercado que continua crescendo com a chegada de novos participantes, impulsionado por bases de código vazadas ou publicadas como *open source*, além da troca de técnicas entre desenvolvedores experientes.

Muitos desses *stealers* apresentam funcionalidades semelhantes – ou até idênticas – em geral por serem versões derivadas (*forks*) de uma mesma base de código. O sucesso de um programa geralmente depende da capacidade do agente de ameaças de promover seu produto de forma eficaz, aliada à facilidade de uso oferecida.

Seção três

Águas calmas, profundezas perigosas

Entre as novas e mais evidentes tendências que surgiram em 2024 – e aquelas que se mantiveram de anos anteriores – há mudanças sutis nas TTPs utilizadas por agentes de ameaças que, embora não tenham dominado a narrativa de 2024, alteraram de forma significativa o panorama.

Um dos elementos que mais chamou a atenção do público foi o uso de redes *proxy* comerciais por agentes de ameaças com base na China, uma tendência que identificamos pela primeira vez em 2021, com a adoção da rede RedRelay por vários grupos. Em 2024, observou-se uma rápida expansão do uso dessas redes, com muitos agentes chineses agora utilizando uma infraestrutura de rede de ofuscação para suas operações.[64 65 66 67 68]

Destaque: redes *proxy* usadas por grupos baseados na China

O fenômeno das redes *proxy* se soma a uma tradição de abordagens e ferramentas compartilhadas para intrusões cibernéticas por agentes de ameaças com base na China. Antes dessas redes, havia o *framework* de armamento 8.t,[69] que foi precedido por famílias de malware compartilhadas como PlugX,[70] PoisonIvy[71] e ShadowPad.[72]

A consolidação e o compartilhamento de TTPs de intrusão têm sido avaliados historicamente como parte de uma tentativa mais ampla de dificultar os esforços de atribuição, além de reduzir os recursos necessários para realizar intrusões individuais.

As redes *proxy* são uma continuação dessa tendência, mas também representam um desdobramento – e, em muitos aspectos, uma evolução. O design, a topologia, as capacidades e os modos de uso dessas redes avançaram muito além das ferramentas empregadas em operações anteriores, passando a incorporar infraestruturas complexas e hierarquizadas, compostas por múltiplas camadas, cada uma com funções ou finalidades específicas (como nós de entrada, nós intermediários de "salto" e n de saída).[73]

[64] 'Red Vulture & Red Dev 38: Covert Network Links', PwC Threat Intelligence, CTO-TIB-20240129-01A
[65] 'Scratching a Lich', PwC Threat Intelligence, CTO-TIB-20240829-01A
[66] 'A New MONSOON Season', PwC Threat Intelligence, CTO-TIB-20240628-03A
[67] 'When it rains, it DOWNPOURs', PwC Threat Intelligence, CTO-TIB-20240517-01A
[68] 'Just our LuckyORB', PwC Threat Intelligence, CTO-TIB-20240802-01A
[69] 'On the RoyalRoad again', PwC Threat Intelligence, CTO-TIB-20211222-01A
[70] 'An xWav on Kyrgyzstan', PwC Threat Intelligence, CTO-TIB-20210222-01A
[71] 'Beware the GreenHugeMan', PwC Threat Intelligence, CTO-TIB-20221103-02A
[72] 'Whats dat malware', PwC Threat Intelligence, CTO-TIB-20230821-01A
[73] 'Into the Spyder-verse', PwC Threat Intelligence, CTO-TIB-20240620-01A

Desde que identificamos o uso de uma rede *proxy* que chamamos de RedRelay em 2021 – que já estava ativa pelo menos desde 2018 – o ecossistema de redes *proxy* cresceu exponencialmente.

Figura 9 – As diferentes formas de redes *proxy*

Definimos uma rede *proxy* como um conjunto de *hosts* conectados cujo propósito é encaminhar o tráfego entre os nós, desde um *host* de origem inicial até um host de destino.

Definimos uma rede de ofuscação como uma rede *proxy* que encaminha tráfego com o objetivo de ocultar sua origem ou destino. As redes de ofuscação são desenvolvidas e fornecidas principalmente para permitir a navegação privada aos usuários.

01 ***Proxy* network**
O termo genérico mais abrangente

02 **Rede de ofuscação**
Uma rede *proxy* especificamente para navegação privada

Ofuscação de atribuição de tráfego de rede

03 **Rede encoberta**
Uma rede *proxy* destinada a dificultar a atribuição

04 ***Botnet***
Redes *proxy* que comprometem dispositivos para serem usados como nós

Definimos uma rede encoberta como uma rede de ofuscação projetada por seus desenvolvedores e operadores especificamente para ocultar qualquer tentativa de atribuição. Sinônimo de rede ORB.

Embora algumas redes *proxy* possam ser *botnets*, nem todas são. Consideramos redes *proxy* como botnets quando consistem em dispositivos de terceiros comprometidos que são usados especificamente para o encaminhamento de tráfego.

As redes *proxy* são utilizadas, em última instância, para ofuscação de atribuição. A forma como essa infraestrutura foi usada ao longo de 2024 alterou nossa perspectiva sobre o panorama dos agentes de ameaças baseados na China, em termos das tendências operacionais de TTPs:

- Do ponto de vista do acesso inicial, observamos uma queda acentuada no uso de documentos maliciosos e tentativas de *phishing* contra os alvos. Em vez disso, vemos agora um aumento da adoção de exploração de vulnerabilidades conhecidas (*n-day*) e desconhecidas (*zero-day*).[74]

- Essa mudança inclui tanto ataques altamente direcionados quanto eventos de exploração em larga escala, que ocorreram logo após – ou, em alguns casos, até mesmo antes – da divulgação pública da vulnerabilidade. Esses dispositivos provavelmente são escolhidos e pesquisados devido ao seu uso disseminado em vários setores, criando uma oportunidade para um número significativo de comprometimentos com o uso de apenas um único *exploit*. Como já foi observado em pesquisas públicas de segurança em 2024,[75] também parece haver uma grande superfície de ataque nesses produtos, o que significa que, mesmo quando uma vulnerabilidade é corrigida, é provável que o mesmo produto possa ser reutilizado para outro *exploit* diferente, porém semelhante.

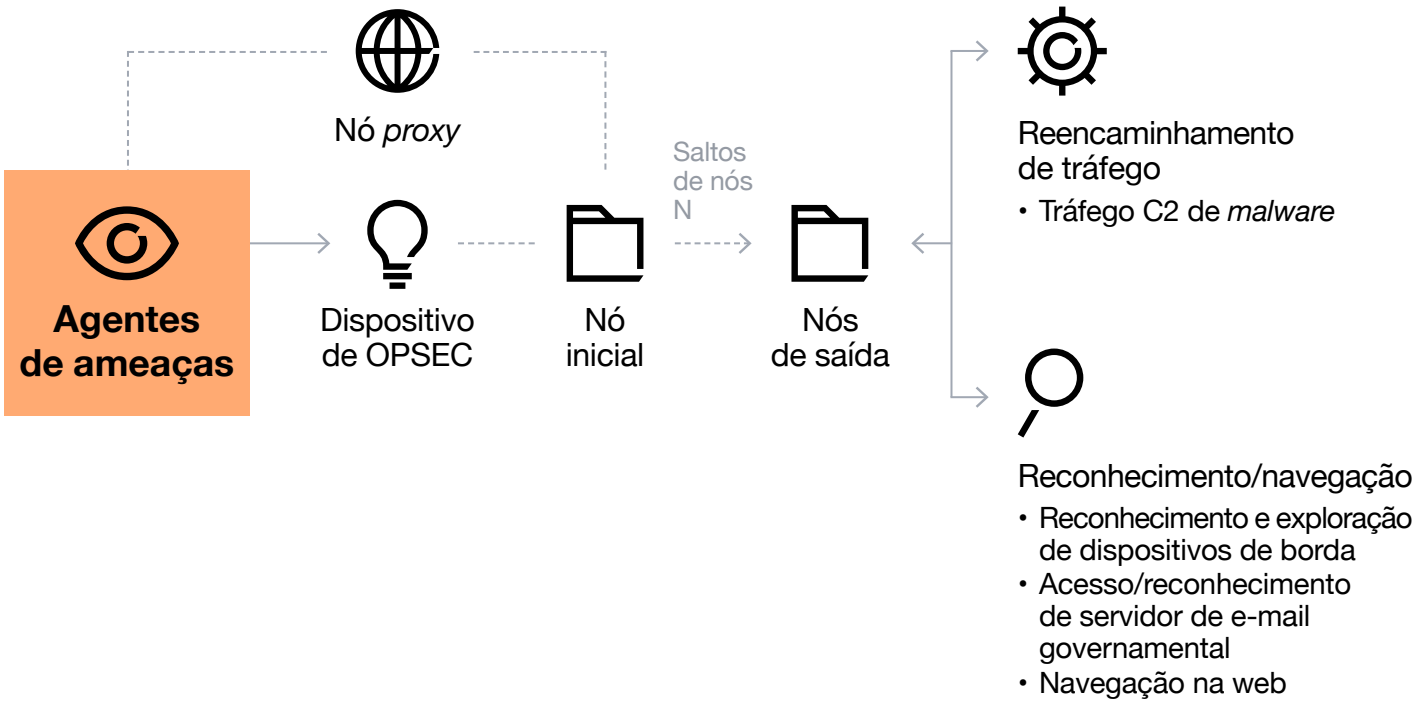
- Os dispositivos mais visados para essas tentativas iniciais de acesso têm sido:
  - Produtos Microsoft (por exemplo: Windows, Exchange e SharePoint)
  - Dispositivos de segurança e de borda:
    - Redes privadas virtuais (VPN)
    - *Firewalls*
    - Infraestrutura de virtualização

[74] 'Defending against the zero-day deluge', PwC Threat Intelligence, CTO-SIB-20231212-01A
[75] 'Hop-Skip-FortiJump-FortiJump-Higher - Fortinet FortiManager CVE-2024-47575', watchtower Labs, https://labs.watchtowr.com/hop-skip-fortijump-fortijumphigher-cve-2024-23113-cve-2024-47575/ (15/11/2024)

- Após o acesso inicial, os agentes de ameaças baseados na China continuam usando técnicas do tipo *living-off-the-land*, como o comprometimento de contas com privilégios de administrador e o abuso de ferramentas nativas, como o PowerShell, em vez de implantar *backdoors* customizados.[76] Essa atividade após o acesso inicial não é nova em 2024. Trata-se de uma prática recorrente nas cadeias de intrusão chinesas há anos. O que se destacou neste ano foi a eficácia com que esses grupos conseguiram estabelecer presença inicial nos ambientes das vítimas.

A importância do modelo organizacional das redes de *proxy*, além do elemento de ofuscação, está no fato de alterar fundamentalmente a forma como os agentes de ameaças baseados na China operam.

Figura 10 – Visualização de uma das redes de *proxy* monitoradas pela PwC Threat Intelligence



[76] 'CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance', US CISA, https://www.cisa.gov/news-events/alerts/2024/02/07/cisa-and-partners-release-advisory-prc-sponsored-volt-typhoon-activity-and-supplemental-living-land (7/2/2024)

A quantidade de agentes de ameaças adotando essas redes – inclusive grupos que antes não as utilizavam – indica que isso vai além de uma simples inspiração: avaliamos que o uso de redes de *proxy* se consolidou como um componente integrado aos procedimentos operacionais padrão.

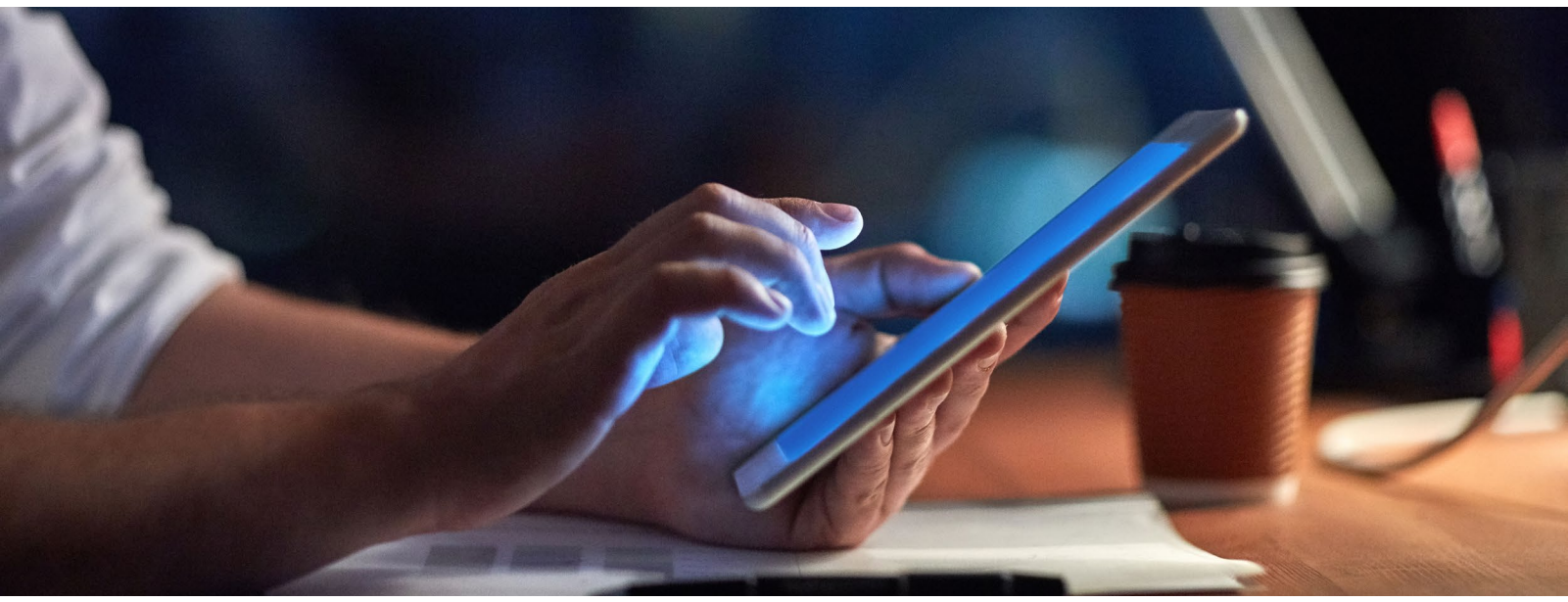
O ecossistema baseado na China manteve um ritmo operacional elevado, com TTPs semelhantes (após o estabelecimento do ponto de apoio) aos dos anos anteriores. No entanto, a adoção generalizada de redes de *proxy* alterou fundamentalmente a forma como as equipes de defesa de rede se preparam para essas intrusões e as mitigam, além de representar novos desafios para a comunidade de inteligência de ameaças e para os processos de atribuição.

Para as equipes de defesa de rede, a prevenção de intrusões começa com a segurança do ambiente interno, o que inclui mapear integralmente a arquitetura da organização e, em seguida, garantir que todos os dispositivos – especialmente os localizados na "borda" do perímetro – estejam atualizados com as versões mais recentes das tecnologias utilizadas.

Como uma medida adicional de segurança, a análise contínua de *logs* dos dispositivos de borda, seguindo orientações emitidas por fontes confiáveis, aumenta as chances de identificar um comprometimento em caso de exploração de vulnerabilidades *zero-day*.

Destaque para ameaças baseadas na Coreia do Norte

Assim como os agentes de ameaças baseados na China, agentes norte-coreanos também vêm alinhando suas TTPs ao longo de 2024, destacando-se pelo uso cada vez mais frequente de atividades por meio de *proxies* comerciais baseados em VPN.[77]

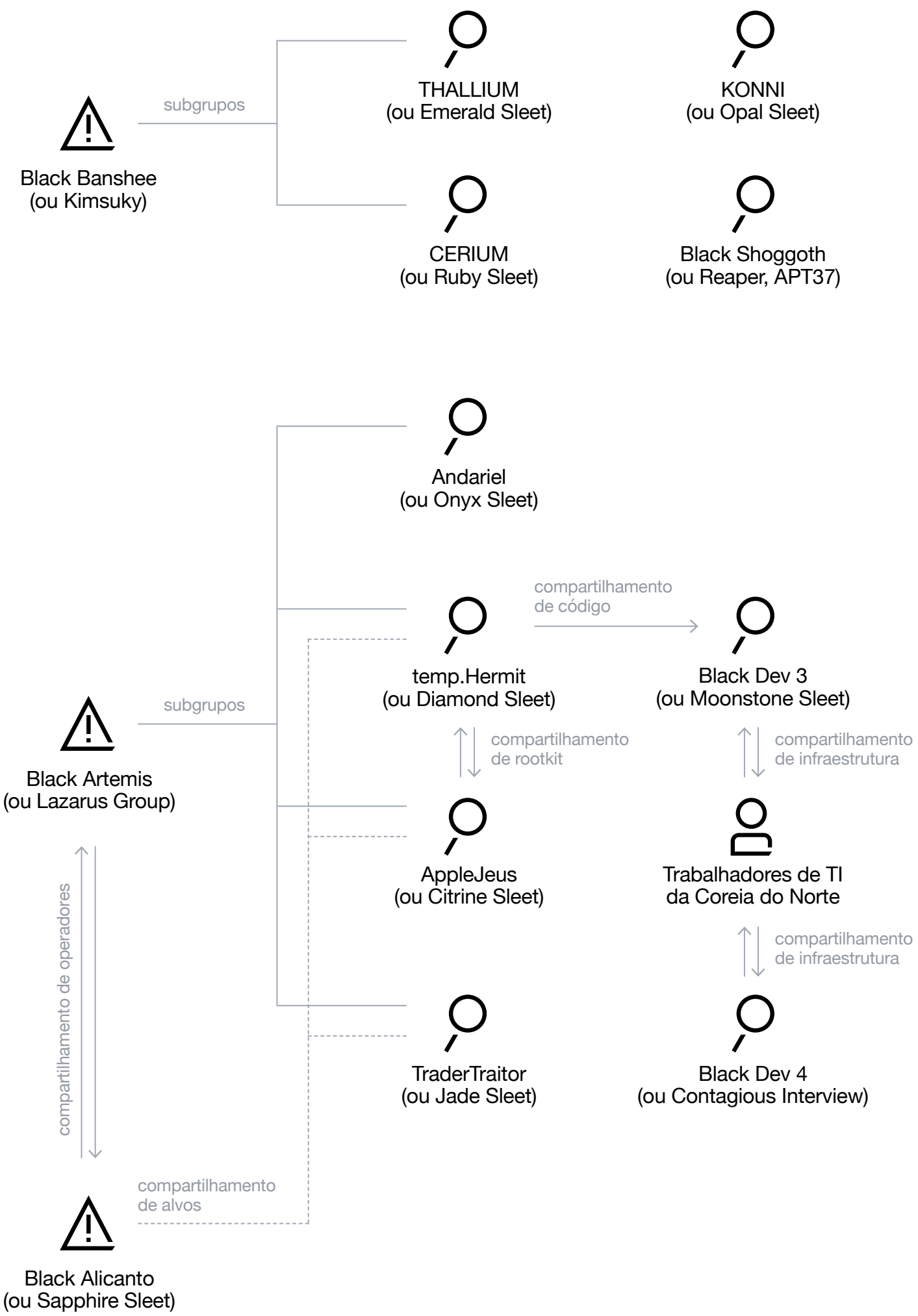


Observa-se ainda uma crescente consolidação e compartilhamento de *malware* e vetores de ataque entre diferentes grupos de intrusão, com o reaproveitamento de variantes aprimoradas de *malwares* já conhecidos,[78] além do desenvolvimento de novos *backdoors*.[79] [80]

Notamos também a evolução contínua de grupos como o Black Alicanto (também conhecido como Sapphire Sleet), que vêm ampliando suas capacidades voltadas para sistemas macOS.[81]

[77] 'DPRK proxying activity', PwC Threat Intelligence, CTO-TIB-20240502-01A
[78] 'New FASTCash malware Linux variant helps steal money from ATMs', Bleeping Computer, https://www.bleepingcomputer.com/news/security/new-fastcashmalware-linux-variant-helps-steal-money-from-atms/ (14/10/2024)
[79] 'SHROUDED#SLEEP: A Deep Dive into North Korea's Ongoing Campaign Against Southeast Asia', Securonix, https://www.securonix.com/blog/shroudedsleep-a-deep-dive-into-north-koreas-ongoing-campaign-against-southeast-asia/ (3/10/2024)
[80] 'APT Actors Embed Malware within macOS Flutter Applications', Jamf, https://www.jamf.com/blog/jamf-threat-labs-apt-actors-embed-malware-withinmacos-flutter-applications/ (12/11/2024)
[81] 'A video call with Black Alicanto', PwC Threat Intelligence, CTO-TIB-20241211-01A

Figura 11 – Visualização dos agentes de ameaças da Coreia do Norte e suas relações entre si, de acordo com a telemetria da PwC



Esse cenário ocorre após um 2023 marcado por um número sem precedentes de intrusões com alvo na cadeia de suprimentos, conduzidas por agentes de ameaças baseados na Coreia do Norte,[82] [83] [84] uma tendência tão expressiva que foi avaliada como provável de se consolidar como técnica operacional predominante em 2024.

No entanto, a recente movimentação em direção à consolidação das TTPs sugere um esforço deliberado para elevar o nível de sofisticação e reforçar a segurança operacional dessas operações.

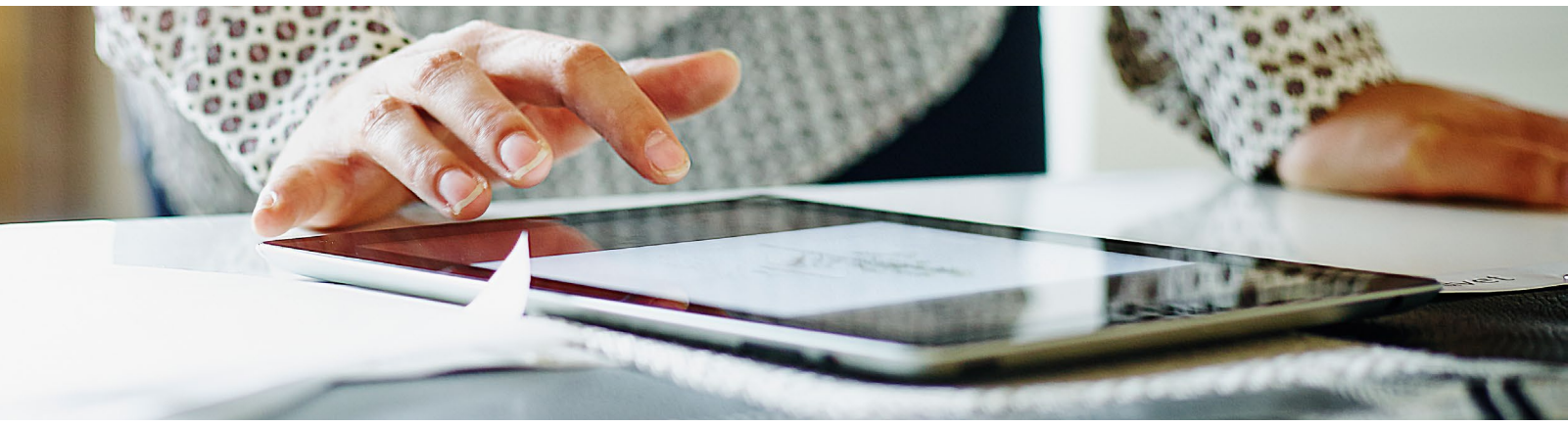
Figura 12 – Visão geral das TTPs de agentes de ameaças baseados na Coreia do Norte

Técnica/ Grupo	Diamond Sleet	Jade Sleet	Citrine Sleet	Onyx Sleet	Black Dev 3	Black Dev 4	Black Alicanto	Trabalhadores de TI da Coreia do Norte
Spearphishing por e-mail	●	●	●	●	●	●	●	
Spearphishing por redes sociais	●	●			●	●	●	
Comprometimento estratégico de sites	●				●	●		
Exploração de vulnerabilidades	●		●	●				
Ataques à cadeia de suprimentos	●	●			●			
Binários trojanizados	●		●		●	●		
Pacotes maliciosos npm/PyPi		●	●		●	●		
Emprego direto					●			●

[82] ‘North Korea: supply chain attacks and cryptocurrency targeting’, PwC Threat Intelligence, CTO-SIB-20231024-01A
[83] ‘3CX Supply Chain Compromise’, PwC Threat Intelligence, CTO-QRT-20230330-01A
[84] ‘Black Artemis CyberLink supply chain compromise’, PwC Threat Intelligence, CTO-QRT-20231124-01A

Esse retorno a TTPs mais tradicionais veio acompanhado de um novo foco em técnicas de engenharia social para obter acesso inicial – uma abordagem historicamente usada por agentes de ameaças da Coreia do Norte, como a criação de falsos anúncios de emprego direcionados a profissionais do setor de defesa.[85]

Mesmo assim, a engenharia social também evoluiu, com esses agentes adotando uma técnica inédita para obter acesso: candidatar-se a vagas de trabalho remoto em organizações de interesse, fingindo ser cidadãos de outros países. Essa prática passou a integrar o manual operacional em 2022[86] e continuou sendo observada em 2023.[87]



A diferença entre o fenômeno dos trabalhadores de TI dos anos anteriores e a atividade registrada em 2024 está na escala e no grau de organização, com estimativas apontando para mais de 10 mil indivíduos atuando dentro da chamada equipe de "trabalhadores".[88] [89]

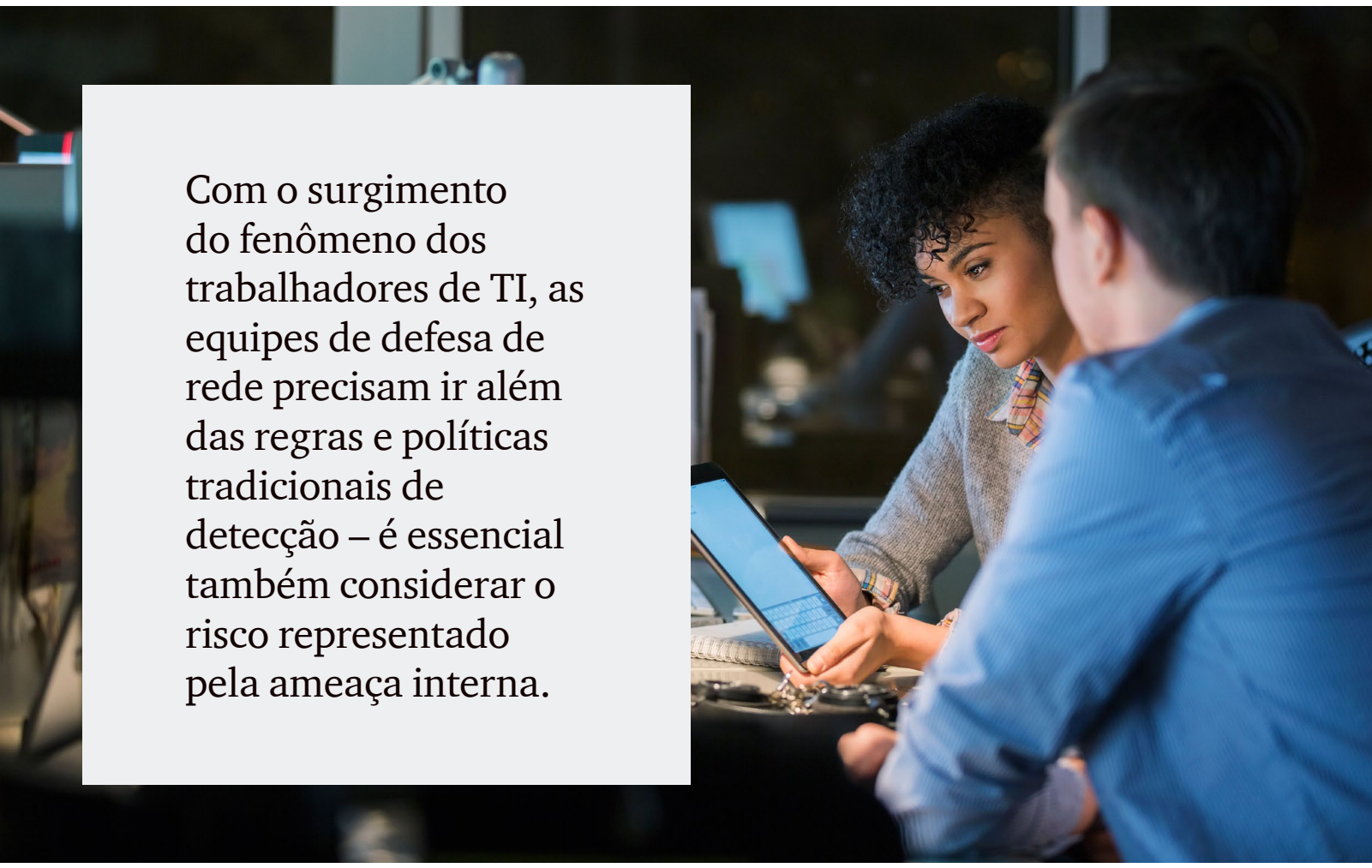
Embora essa tendência possa parecer menos lucrativa financeiramente do que o direcionamento anterior (e ainda em curso) a empresas de criptomoedas,[90] [91] seu crescimento traz implicações estratégicas importantes.

[85] 'Bluenoroff recruitment drive', PwC Threat Intelligence, CTO-TIB-20190605-01A
[86] 'Guidance On The Democratic People's Republic Of Korea Information Technology Workers', US DOJ, https://ofac.treasury.gov/media/923126/download?inline (16/5/2022)
[87] 'Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers', FBI, https://www.ic3.gov/PSA/2023/PSA231018 (18/10/2023)
[88] 'Advisory on Democratic People's Republic of Korea (DPRK) information technology (IT) workers', Australian Government (Department of Foreign Affairs and Trade), https://www.dfat.gov.au/international-relations/security/sanctions/guidance/advisory-democratic-peoples-republic-korea-dprk-information-technologyit-workers (26/8/2024)
[89] 'Black Dev 4 is hiring', PwC Threat Intelligence, CTO-TIB-20240625-01A
[90] 'Black Artemis CyberLink supply chain compromise', PwC Threat Intelligence, CTO-QRT-20231124-01A
[91] 'DPRK Supply Chain Attacks', PwC Threat Intelligence, CTO-SIB-20231024-01A

Além de continuarem gerando receita por meio de vínculos empregatícios formais, os operadores norte-coreanos, uma vez inseridos nas organizações, passam a ter acesso privilegiado – que pode ser explorado para fins de espionagem corporativa e extorsão. Isso não apenas amplia as fontes potenciais de financiamento, como também transforma o perfil de ameaça representado por esses agentes.

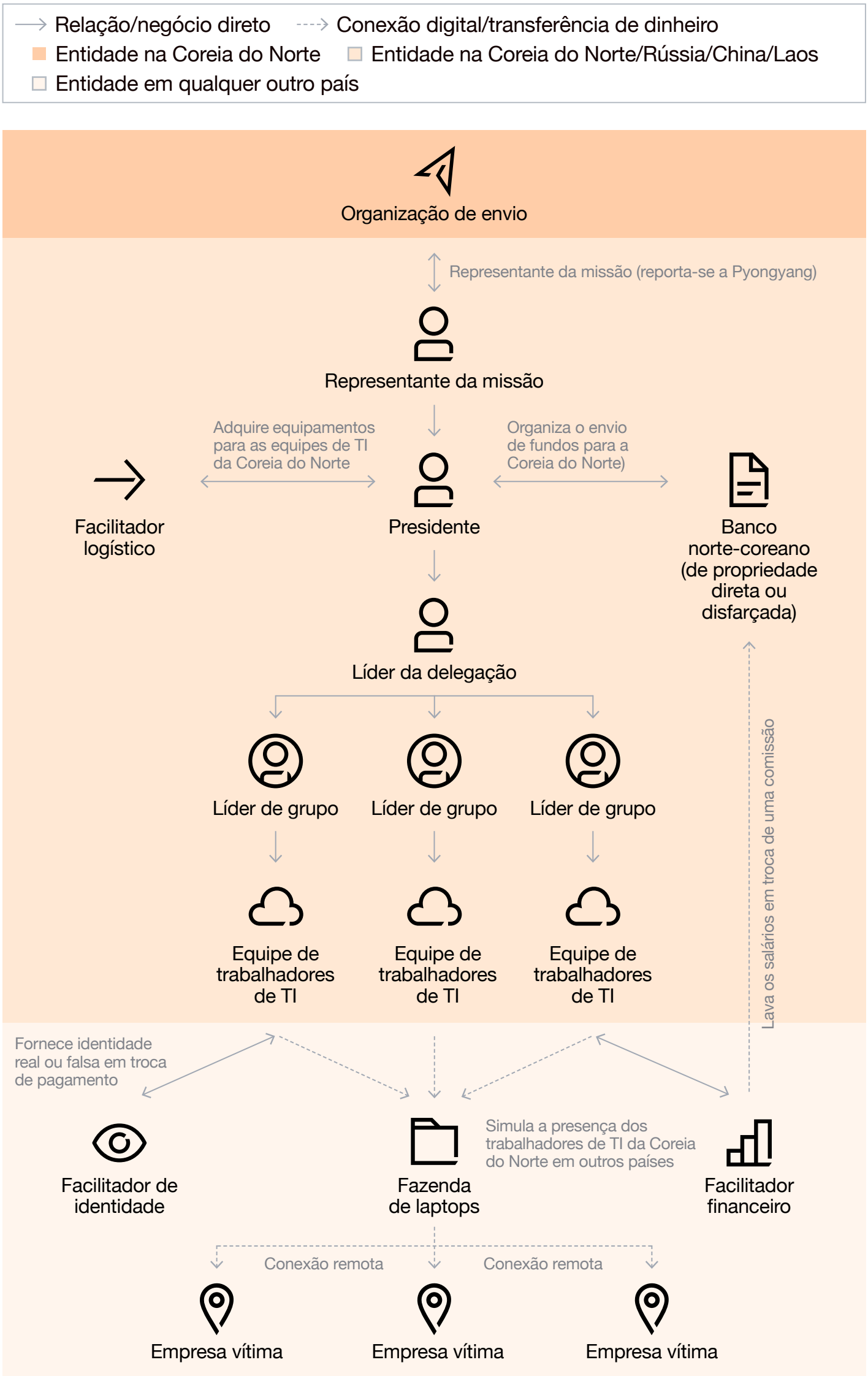
A integração observada entre ataques à cadeia de suprimentos em menor escala, manutenção de alvos tradicionais e aumento no ritmo das operações sugere, com forte probabilidade, uma mudança de foco – ou mesmo uma necessidade estratégica – de que diferentes grupos de intrusão norte-coreanos estejam priorizando a coleta de inteligência, em detrimento da exclusiva exploração de organizações voltadas ao setor de criptomoedas.

Essa mudança de abordagem é evidente até mesmo na campanha dos trabalhadores de TI, que permitiu a exfiltração de dados sensíveis enquanto gerava receita por meio de extorsão pós-comprometimento ou salários legítimos.



Com o surgimento do fenômeno dos trabalhadores de TI, as equipes de defesa de rede precisam ir além das regras e políticas tradicionais de detecção – é essencial também considerar o risco representado pela ameaça interna.

Figura 13 – Visão geral da infraestrutura necessária para operar a campanha de trabalhadores de TI da Coreia do Norte



Em comparação com o ano passado, quando agentes de ameaças baseados na Coreia do Norte foram destaque em diversas matérias da grande mídia devido a seus ataques em larga escala à cadeia de suprimentos,[92] [93] 2024 teve poucos exemplos semelhantes. A atenção se voltou, na verdade, para a coleta de informações, especialmente nas áreas militar e de defesa.[94]

O aperfeiçoamento das TTPs de infraestrutura de rede, aliado ao aumento do volume e do foco em operações motivadas por espionagem, gerou uma mudança geral na forma como as ameaças vindas da Coreia do Norte foram avaliadas em 2024.

Embora as motivações por trás das atividades desses agentes geralmente permaneçam as mesmas, os conjuntos de invasão que monitoramos mostraram mudanças em suas metodologias e técnicas, o que dificultou tanto a atribuição de operações específicas quanto a identificação de qual grupo está responsável por quais funções.

[92] 'North Korean hackers breach software firm in significant cyberattack', CNN, https://www.cnn.com/2023/04/20/politics/north-korea-hacking-supply-chain-3cx-mandiant/index.html (20/4/2023)
[93] 'North Korean hackers breached a US tech company to steal crypto', Reuters, https://www.reuters.com/technology/n-korea-hackers-breached-us-itcompany-bid-steal-crypto-sources-2023-07-20/ (20/7/2023)
[94] 'NCSC and partners issue warning over North Korean state-sponsored cyber campaign to steal military and nuclear secrets', UK NCSC, https://www.ncsc.gov.uk/news/ncsc-partners-vigilant-dprk-sponsored-cyber-campaign (25/7/2024)

Seção quatro

Águas turbulentas

A paisagem geopolítica tem moldado a atividade cibernética desde os primeiros anos da digitalização, embora apenas a partir de 2022 tenha ficado evidente como o “domínio cibernético” pode ser usado em tempos de conflito.

O ano de 2024 registrou uma expansão geral das atividades em “tempos de guerra”, com certos conflitos se espalhando (por exemplo, aumento das tensões entre Irã e Israel) e outros sem dar sinais de recuo (como a guerra da Rússia na Ucrânia, que agora envolve oficialmente a Coreia do Norte).[95]

A retórica cada vez mais hostil entre os EUA e a China, em grande parte centrada em questões do domínio cibernético, também influenciou o panorama de ameaças observáveis. Com um fluxo contínuo de operações sendo reveladas publicamente, o ritmo geral tem sido fortemente influenciado por manobras políticas e mudanças nas relações internacionais.

O ecossistema de *ransomware* também esteve mais ativo do que nunca em 2024, apesar das tentativas das autoridades de restringir sua atuação. O número de sites de vazamento atingiu níveis recordes, mas isso representa apenas parte do cenário. O aumento no volume de operações de *ransomware* reforça ainda mais a resiliência e a capacidade de adaptação desse ecossistema.

Rússia-Ucrânia: mais um ano de desgaste

Conforme a ofensiva da Rússia na Ucrânia passou de ganhos territoriais rápidos para avanços graduais em várias frentes, a atividade cibernética também se adaptou para acompanhar esse ritmo.

No início da guerra, agentes de ameaças com base na Rússia foram vistos utilizando *wipers* (*malwares* com capacidade destrutiva) contra a infraestrutura crítica da Ucrânia,[96] [97] ao mesmo tempo que conduziam operações de espionagem direcionadas a setores como defesa,[98] governo[99] e instituições correlatas.[100]

[95] ‘North Korea goes to Russia’, PwC Threat Intelligence, CTO-SIB-20241113-01A
[96] Ukraine One Year On’, PwC Threat Intelligence, CTO-TIB-20230428-01A
[97] ‘Cyber Threats 2022: A Year in Retrospect’, PwC Threat Intelligence, CTO-YIR-20230403-01A
[98] ‘Blue Dev 4 phishing operations in 2022’, PwC Threat Intelligence, CTO-QRT-20220303-01A
[99] ‘Blue Otso retains Ukraine interest’, PwC Threat Intelligence, CTO-TIB-20220203-01A
[100] ‘The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access’, Volexity, https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/ (22/11/2024)

Em 2023, o uso de *wipers* diminuiu visivelmente, dando lugar a uma coleta de informações mais tradicional, com a ampliação dos alvos para organizações do setor privado envolvidas em temas econômicos ou políticos urgentes, como a indústria de alimentos e agricultura durante as negociações do acordo de grãos.[101] [102]

Como já era esperado, 2024 trouxe a continuidade das operações de coleta de inteligência por parte de agentes russos, com foco substancial na Ucrânia. As TTPs da maioria dos grupos russos que monitoramos permaneceram constantes desde 2022:

- Blue Callisto (também conhecido como COLDRIVER, Star Blizzard) manteve o foco em ONGs e centros de pesquisa, utilizando infraestrutura própria e e-mails de *phishing* com injeção remota de modelos e iscas em PDF.[103] Blue Dev 8 e Blue Athena (também conhecidos como Forest Blizzard, BlueDelta) realizaram operações semelhantes às do Blue Callisto, com foco específico em instituições de defesa e governo sediadas na Ucrânia.[104] [105]
- Blue Dev 5 (também conhecido como NOBELIUM, Midnight Blizzard) foi observado ao longo de 2024 utilizando os mesmos *malwares* dos anos anteriores, explorando temas da OTAN e da Ucrânia em campanhas de HTML *smuggling*, com a ferramenta EnvyScout, que carrega um segundo estágio com *payload* do Cobalt Strike.[106]
- Blue Otso (também conhecido como Gamaredon Group) manteve sua infraestrutura histórica e os mesmos TTPs em operações contra a Ucrânia em 2024, continuando a usar *Cloudflare Tunnels* em conjunto com arquivos PowerShell e MSHTA.[107]

[101] 'Cyber Threats 2023: A Year in Retrospect', PwC Threat Intelligence, CTO-YIR-20240627-01A
[102] 'Russian threat actors dig in, prepare to seize on war fatigue', Microsoft, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue (7/12/2023)
[103] 'Does this phish smell Blue to you?' PwC Threat Intelligence, CTO-TIB-20240205-01A
[104] 'Blue Dev 8's net on Ukraine', PwC Threat Intelligence, CTO-TIB-20240520-01A
[105] 'Making a Mock(er)y of credential harvesting', PwC Threat Intelligence, CTO-TIB-20240702-01A
[106] 'RSVP at your peril!', PwC Threat Intelligence, CTO-TIB-20241018-02A
[107] 'Blue Otso with chance of TryCloudflare', PwC Threat Intelligence, CTO-TIB-20241030-02A

Outros grupos, como Blue Athena (também conhecido como APT28), mantiveram suas missões tradicionais, visando diversos Ministérios das Relações Exteriores de países ocidentais.[108]

O Blue Dev 5 também continuou suas operações contra instituições de defesa, ONGs e entidades do setor educacional em países ocidentais e aliados do Ocidente. Dado o estado das relações entre a Rússia e os países da OTAN no fim de 2024 – marcadas por várias acusações de sabotagem feitas por autoridades ocidentais contra Moscou –,[109] [110] é altamente provável que esse nível de atividade persista, senão aumente.

Oriente Médio – um ano de conflitos

Durante 2024, os conflitos no Oriente Médio também se refletiram no ambiente cibernético, dando continuidade à atividade registrada no fim de 2023, após os eventos de 7 de outubro.

[108] 'Blue Athena Dumps Webhooks into the Water', PwC Threat Intelligence, CTO-TIB-20240214-01A
[109] 'UK spy chief says Russia behind 'staggeringly reckless' sabotage in Europe', Reuters, https://www.reuters.com/world/europe/russia-behind-staggeringlyreckless-sabotage-europe-uk-spy-chief-says-2024-11-29/ (29/11/2024)
[110] 'Finlandization: More Please', CEPA, https://cepa.org/article/finland-challenges-russian-sabotage/ (30/12/2024)

Grupos vinculados ao Irã intensificaram ataques contra instituições israelenses, com o retorno de táticas já conhecidas – como roubo de credenciais por *phishing*, implantação de *backdoors* e ações de sabotagem – além de campanhas com foco psicológico direcionadas à população israelense.[111] Essas atividades também miraram outros adversários, tanto regionais (como entidades em Omã, Emirados Árabes Unidos e Jordânia) quanto globais (como os Estados Unidos).

O aumento da atividade desses agentes iranianos, em um ano marcado por dificuldades na política externa e ambições regionais do Irã, reforça a tese de que operações cibernéticas são uma ferramenta-chave de projeção de influência estatal.[112]

Com o colapso do regime de Assad no fim de 2024 – amplamente atribuído, entre outros fatores, à perda da capacidade do Irã de enviar recursos de forma imediata à região –, ainda não está claro como os grupos cibernéticos iranianos atuarão em 2025. No entanto, é altamente provável que suas operações continuem alinhadas com os interesses estratégicos de Teerã.

Diante dos acontecimentos de 2024 e olhando agora para 2025, avaliamos como altamente provável que grande parte da infraestrutura cibernética do Hamas – especialmente os elementos localizados diretamente na Palestina – tenha se tornado inoperante.

Ainda assim, também é altamente provável que partes da organização poupadas pelas operações militares israelenses continuem conduzindo campanhas, como fizeram em outubro e novembro. Já os agentes de ameaças vinculados ao Hezbollah provavelmente foram menos afetados, e avaliamos com probabilidade realista que retomem suas operações, caso os confrontos prossigam em 2025.

[111] 'Yellow Dev 19 influence campaign goes ballistic', PwC Threat Intelligence, CTO-QRT-20241029-01A
[112] 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities', US CISA, https://www.cisa.gov/newsevents/cybersecurity-advisories/aa23-335a (18/12/2024)

Coreia do Norte – não tão isolada assim

Em 2023, os agentes de ameaças vinculados à Coreia do Norte se destacaram por ataques de alto impacto à cadeia de suprimentos, tanto com objetivos de espionagem quanto financeiros — como o roubo de criptomoedas.[113]

Apesar da intensidade dessas operações, não havia uma ligação clara com a política externa do país. O provável é que muitas dessas ações tenham sido realizadas para aliviar a grave crise econômica do país. Já em 2024, houve um aumento no ritmo das operações, acompanhado por uma postura internacional consideravelmente mais agressiva.

[113] 'Cyber Threats 2023: A Year in Retrospect', PwC Threat Intelligence, CTO-YIR-20240627-01A

Figura 14 – Cronologia das principais manobras políticas da Coreia do Norte em 2024

Janeiro de 2024

- EUA afirmam que a Coreia do Norte está fornecendo mísseis balísticos à Rússia
- Kim Jong Un enfatiza esforços de construção em meio à crise na economia rural
- Black Artemis conduz campanha contra desenvolvedores de software de criptomoedas

Fevereiro de 2024

- Coreia do Sul afirma que a Coreia do Norte está fornecendo artilharia à Rússia em troca de alimentos
- Primeiro satélite espião da Coreia do Norte entra em órbita
- Black Banshee permanece ativo, visando alvos sul-coreanos com *malware* AppleSeed

Março de 2024

- Transferências diretas de petróleo da Rússia para a Coreia do Norte seguem entrega de armas
- Black Artemis conduz operação contra *exchange* de criptomoedas sediada no Japão, resultando no roubo de US$ 308 milhões

Abril de 2024

- Kim Jong Un convoca preparativos para a guerra, com capacidades ampliadas
- Exercício tático testa “contra-ataque nuclear”
- Polícia sul-coreana relata que contratados foram alvo de agentes norte-coreanos

Maio de 2024

- Japão e Coreia do Sul sancionam entidades que fornecem munição norte-coreana à Rússia
- Alerta conjunto de agências dos EUA destaca uso indevido de DMARC por parte do grupo Black Banshee

Junho de 2024

- Kim Jong-Un e Putin assinam nova parceria estratégica com cláusula de assistência mútua
- Black Dev 4 identificado como grupo que visa desenvolvedores de software com pacotes maliciosos do NPM, em um ataque à cadeia de suprimentos

Julho de 2024

- Alerta conjunto acusa grupos norte-coreanos de espionagem que visam minar a estabilidade do regime

Agosto de 2024

- Coreia do Norte testa drones suicidas enquanto Coreia do Sul se prepara para empregar lasers contra atividade de drones
- Subgrupo do Black Artemis explora falha "*zero-day*" no Chromium para instalar *malware rootkit* conhecido como FudModule, motivado por espionagem

Setembro de 2024

- Coreia do Norte revela nova instalação de enriquecimento de urânio
- FBI emite alerta para ataques norte-coreanos visando plataformas DeFi para roubo de criptomoedas

Outubro de 2024

- Ameaça cibernética Black Shoggoth, baseada na Coreia do Norte, identificada como atuante no Sudeste Asiático com *malware* de espionagem
- Black Artemis visa instituições norte-americanas com *ransomware*

Novembro de 2024

- Coreia do Norte testa mísseis balísticos intercontinentais (ICBMs) no voo mais longo já registrado
- Coreia do Sul acusa Coreia do Norte de aumentar uso de ataques "não cinéticos", incluindo ciberataques

Dezembro de 2024

- Catorze cidadãos coreanos são indiciados pelo Departamento de Justiça dos EUA por participação contínua em campanha de trabalhadores de TI

Fonte: PwC Threat Intelligence.

É plausível que as intrusões cibernéticas motivadas por espionagem estejam suprindo carências tecnológicas em setores estratégicos para a sobrevivência da Coreia do Norte – como defesa, indústria aeroespacial, tecnologia, construção civil e agricultura – [114] [115] [116] enquanto as atividades criminosas continuam, com alta probabilidade, a financiar os objetivos do regime.

Avaliamos que os progressos obtidos pela Coreia do Norte na esfera cibernética nos últimos anos possivelmente desempenharam papel determinante no endurecimento de sua política externa observada em 2024.

O fortalecimento da capacidade tecnológica de combate obtida ilicitamente,[117] [118] a modernização de seu programa nuclear[119] e o aprofundamento da inteligência sobre adversários políticos, via ciberespionagem,[120] são, com grande probabilidade, elementos-chave desse desenvolvimento.

A entrada oficial da Coreia do Norte na guerra da Rússia contra a Ucrânia, com o envio de munições e pessoal no fim de 2024, simbolizou uma cooperação militar mais ampla entre dois Estados relativamente isolados.[121]

Avaliamos como provável que, em 2025, os agentes de ameaças cibernéticas baseados na Coreia do Norte continuem a mirar entidades em busca de tecnologia proprietária para espionagem, além de manterem o foco no roubo de criptomoedas.

[114] North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs', Joint Cybersecurity Advisory, https://media.defense.gov/2024/Jul/25/2003510137/-1/-1/1/Joint-CSA-North-Korea-Cyber-Espionage-Advance-Military-Nuclear-Programs.PDF (25/7/2024)
[115] 'An Offer You Can Refuse: UNC2970 Backdoor Deployment Using Trojanized PDF Reader', Mandiant, https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader (17/9/2024)
[116] 'APT Group Kimsuky Targets University Researchers', Resilience, https://www.cyberresilience.com/threatintel/apt-group-kimsuky-targets-universityresearchers/ (7/8/2024)
[117] 'North Korea's first spy satellite is 'alive', can manoeuvre, expert says', Reuters, https://www.reuters.com/technology/space/north-koreas-first-spy-satellite-isalive-can-manoeuvre-expert-says-2024-02-28/ (28/2/2024)
[118] 'South Korea says DPRK hackers stole spy plane technical data', BleepingComputer, https://www.bleepingcomputer.com/news/security/south-korea-saysdprk-hackers-stole-spy-plane-technical-data/ (12/8/2024)
[119] 'North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs', US CISA, https://www.cisa.gov/newsevents/cybersecurity-advisories/aa24-207a (25/7/2024)
[120] '코니(Konni) 위협 세계관의 확장 분석 리포트 - Expanded Analysis of Konni Threat Universe', Genians, https://www.genians.co.kr/blog/threat_intelligence/konni_universe (setembro/2024)
[121] 'North Korea goes to Russia', PwC Threat Intelligence, CTO-SIB-20241113-01A

Independentemente de os métodos predominantes em 2024 –[122] como o uso de profissionais de TI – continuarem sendo a norma ou não, avaliamos como provável que a necessidade de gerar fluxos financeiros ilícitos continue impulsionando as campanhas cibernéticas maliciosas conduzidas pela Coreia do Norte.

29,5%

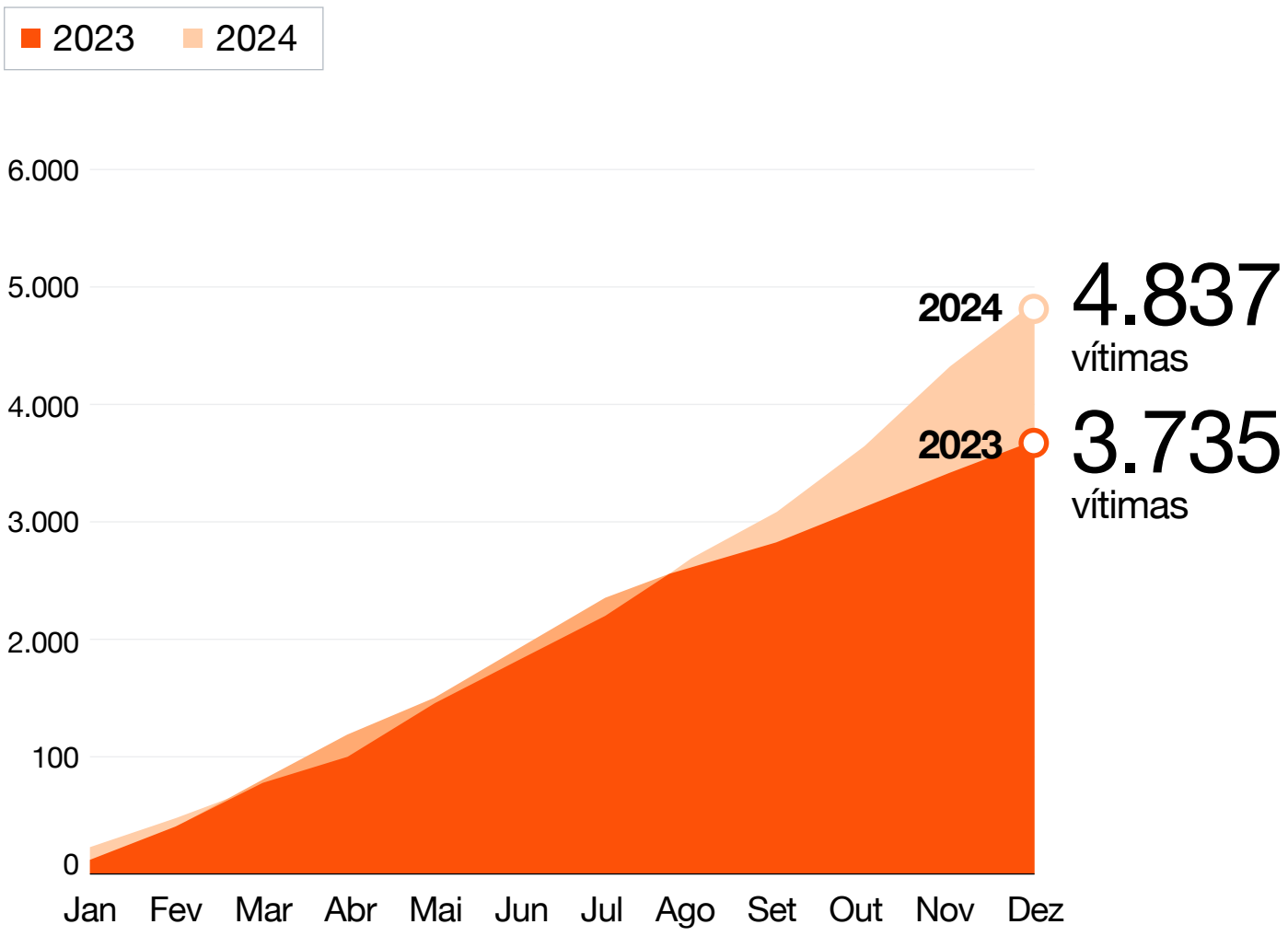
de aumento no número de vítimas em sites de vazamento de *ransomware* em comparação com 2023.

Ransomware – impossível parar

O ecossistema de *ransomware* segue como a principal ameaça, impactando todos os setores, públicos e privados, sem distinção. Em termos de número de sites de vazamento, o pico de 2023 foi alcançado em setembro de 2024,[123] tornando esse o ano mais ativo já registrado para operações de *ransomware* como serviço (RaaS).[124]

[122] 'A video call with Black Alicanto', PwC Threat Intelligence, CTO-TIB-20241211-01A
[123] 'Ransomware report: 2024 Issue 9', CTO-CTS-20241029-01A
[124] As estatísticas de *ransomware* baseadas em sites de vazamento não contam a história completa, já que muitas organizações vítimas desse tipo de ataque acabam pagando o resgate antes que os dados sejam publicados, ou enfrentam ataques que não envolvem a tática da dupla extorsão. Como ocorre com qualquer levantamento de dados sobre *ransomware*, avaliamos que o número real de incidentes é maior do que aquele obtido apenas a partir da soma das informações divulgadas por sites de vazamento.

Figura 15 – Total de vítimas em sites de vazamento



185%

de aumento no número de sites de vazamento em operação.

As ações das autoridades no primeiro trimestre de 2024 – incluindo a Operação Endgame e a pressão exercida pela promessa de recompensas por informações sobre o ALPH-V –[125] [126] funcionaram como um teste crucial para medir a verdadeira resiliência do ecossistema de *ransomware*.

Com os dois maiores programas fora do mercado, os afiliados afetados teriam que continuar sob outro modelo RaaS ou encerrar as operações por medo de serem presos em novas ações das autoridades.

Apesar das prisões e condenações resultantes da Operação Cronus,[127] nossa avaliação inicial foi de que o ecossistema era guiado demais por dinâmicas de mercado e padronizado demais em seus modos de operação para que as ações policiais causassem impactos duradouros no funcionamento geral.[128]

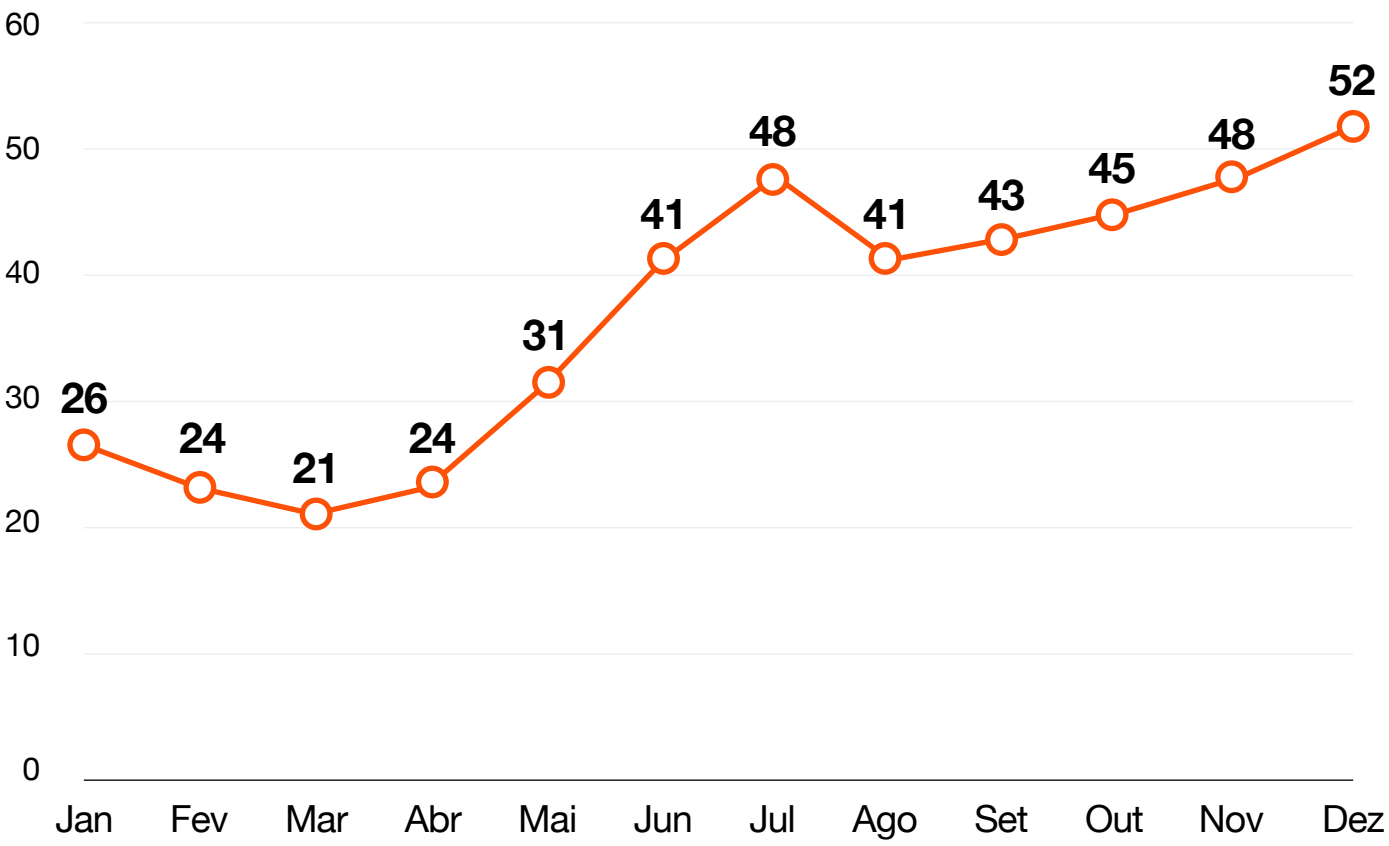
O que aconteceu ao longo do restante de 2024 só reforçou essa avaliação. O número total de sites de vazamento foi o mais alto da história, apesar dos contratempos causados pelas ações policiais. No entanto, o dado mais relevante do ano foi o número de programas ativos.

Em janeiro de 2024, havia 26 diferentes grupos de *ransomware* vazando informações de vítimas. O restante do ano registrou um aumento constante no número de programas RaaS ativos, especialmente após março (quando avaliamos que o ecossistema pós-Operação Cronus começou a se estabilizar), atingindo o pico em dezembro, com 52 agentes de ameaças distintos operando sites de vazamento ativos e dedicados.

[125] 'The NCA announces the disruption of LockBit with Operation Cronos', UK NCA, https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruptionof-lockbit-with-operation-cronos
[126] 'BlackCat was its own bad omen', PwC Threat Intelligence, CTO-SIB-20240322-01A
[127] 'Two Foreign Nationals Plead Guilty to Participating in LockBit Ransomware Group', US DOJ, https://www.justice.gov/opa/pr/two-foreign-nationals-pleadguilty-participating-lockbit-ransomware-group (18/7/2024)
[128] 'Ransomware report 2024 Issue 2', PwC Threat Intelligence, CTO-CTS-20240404-01A

Esses programas são uma mistura de “marcas” já estabelecidas que atuam há anos e ainda não foram oficialmente alvo das autoridades (como PLAY e BlackByte), novos participantes que tiveram sucesso limitado (como DragonForce e Space Bears), além de outros novos que alcançaram sucesso mais expressivo.

Figura 16 – Número de sites de vazamento de *ransomware* registrados por mês em 2024



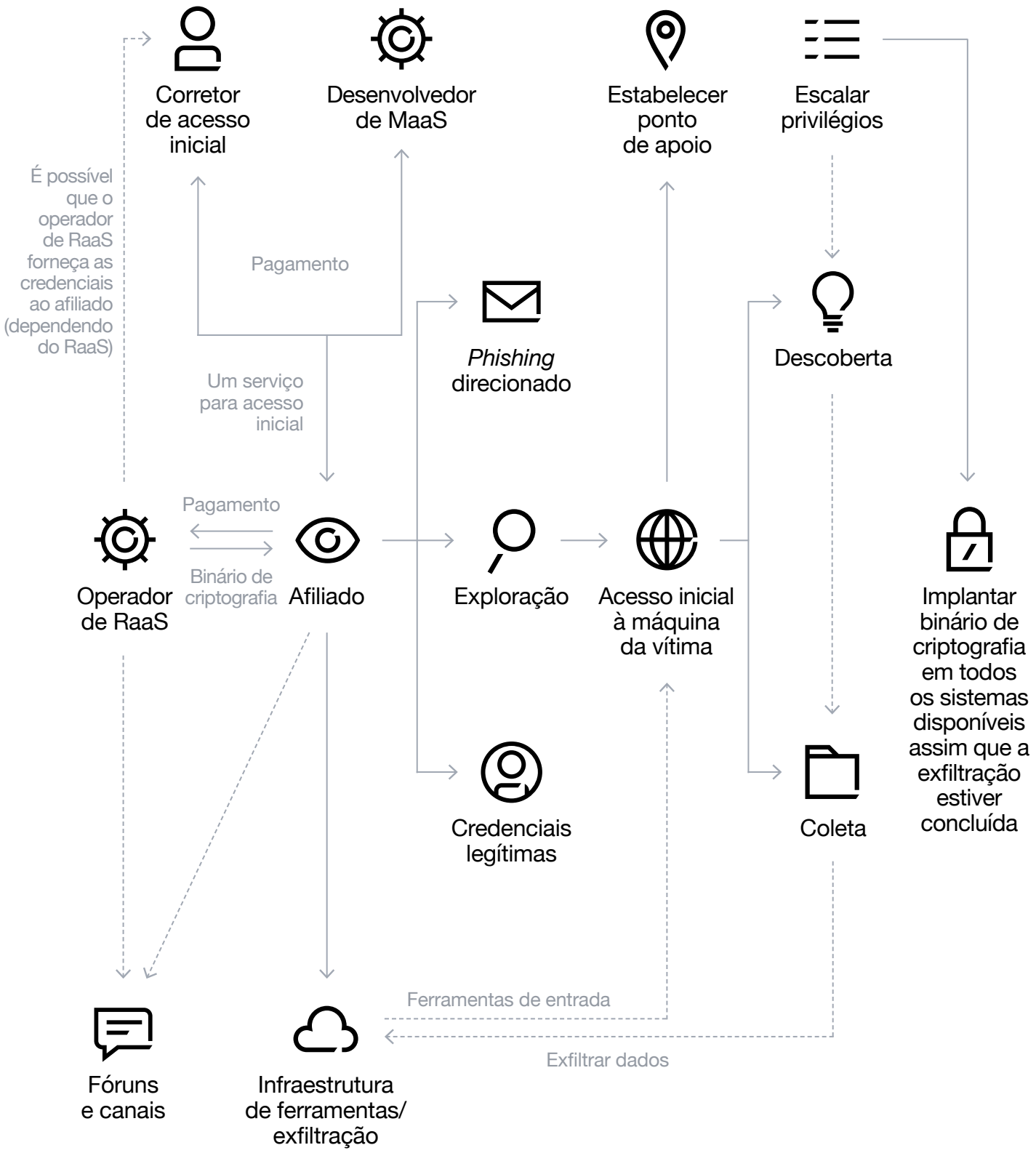
Os dados dos sites de vazamentos em 2024 mostram como o aumento de pequenos grupos ativos mudou drasticamente o cenário do *ransomware*. Em 2023, quando havia menos concorrência, o LockBit 3.0 dominava o ecossistema, sendo responsável por 27% de todas as vítimas, seguido pelo ALPH-V, com 10%.

Já em 2024, a distribuição de vítimas foi muito mais equilibrada: o Ransomhub liderou com o maior número de ataques, mas representando apenas 11% do total (LockBit 3.0 ficou em segundo lugar, com 10%).

O fato de o Ransomhub – um programa de RaaS que só surgiu em fevereiro de 2024 – ter liderado os números nesse ano é significativo. Ao observar as operações de RaaS como um todo, que envolvem desde negociação de pagamentos, gestão de afiliados até manutenção de ferramentas e códigos, percebe-se que há muitos processos complexos funcionando em paralelo, semelhantes aos de uma empresa legítima.

O que torna tudo ainda mais desafiador é que essas operações são criminosas, executadas por pessoas com diferentes níveis de profissionalismo. Mesmo assim, esses novos grupos mostraram que são capazes de operar com eficiência.

Figura 17 – Visão geral do modelo operacional de *Ransomware* como Serviço (RaaS)



Isso é relevante porque, até então, apenas alguns grupos de *ransomware* conseguiam manter um número consistente de vítimas em sites de vazamento ao longo do tempo – e geralmente levavam bastante tempo para chegar a esse ponto.[129] Em 2024, no entanto, vários programas de RaaS surgiram e romperam com essa lógica, alcançando mais de 40 vítimas em apenas alguns meses de atividade.

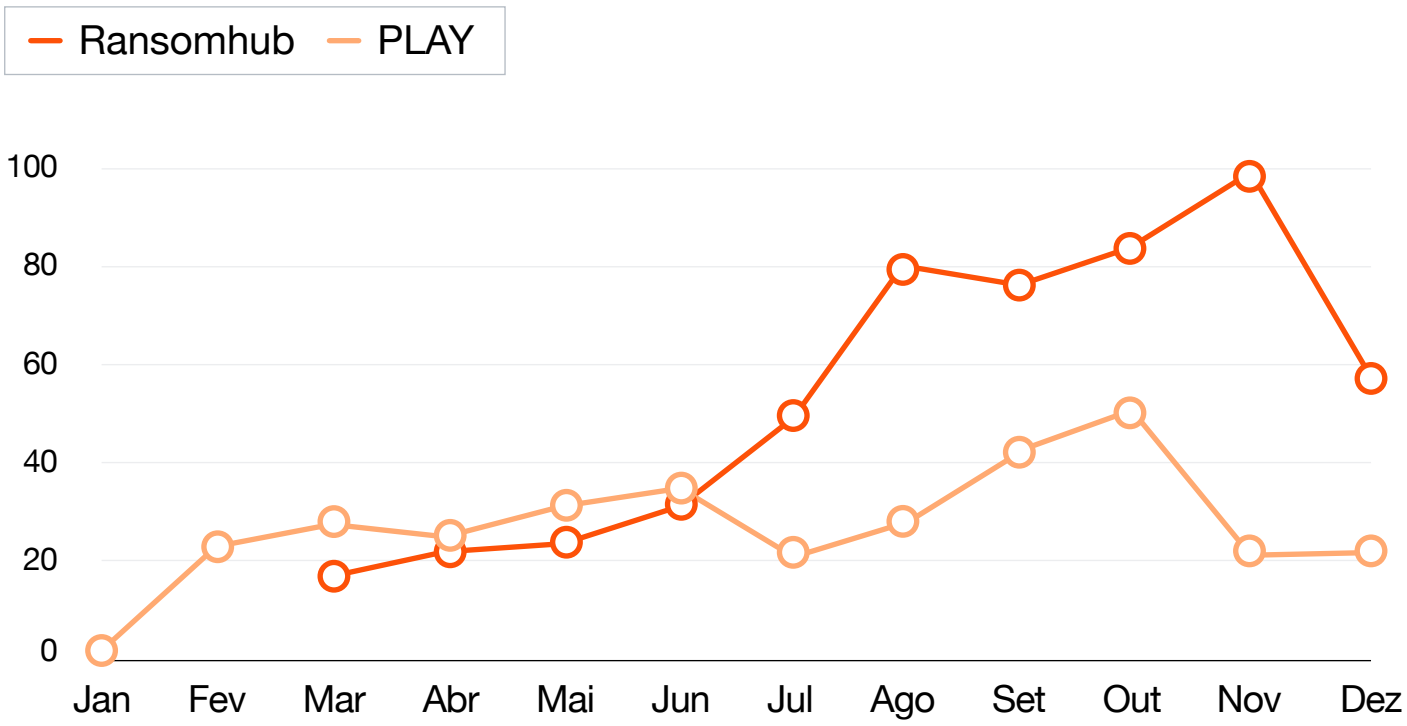
Destaque: RansomHub

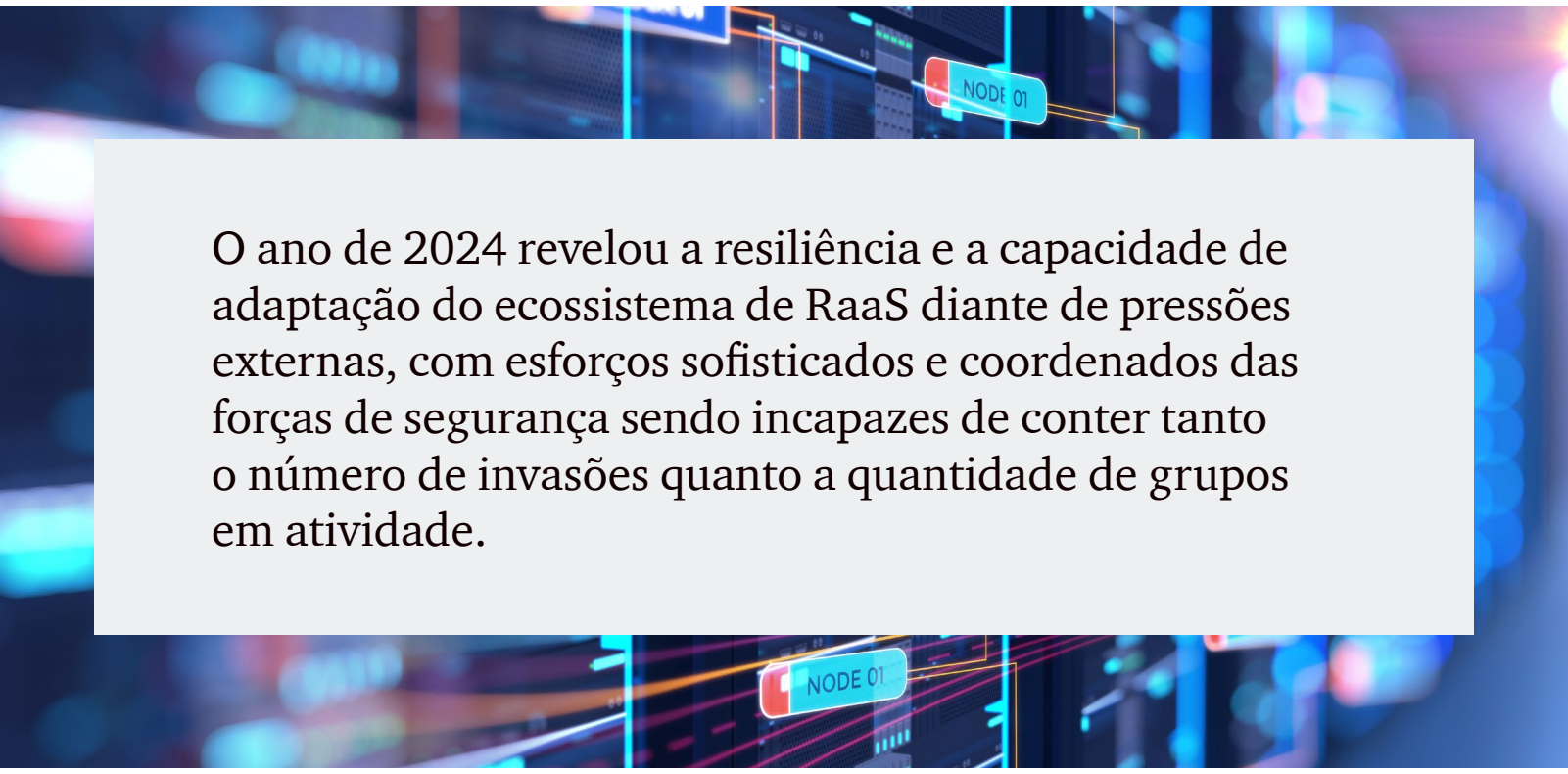
O RansomHub foi anunciado pela primeira vez no fórum clandestino RAMP em 2 de fevereiro de 2024, por um usuário com o codinome "koley", que parece ter se registrado no fórum em 3 de maio de 2023. Embora a maior parte do anúncio seguisse o padrão já observado em postagens anteriores sobre programas RaaS, um ponto chamou atenção de imediato: a alegação de que a divisão de lucros do RansomHub seria estruturada para repassar 90% ao afiliado e apenas 10% ao desenvolvedor.[130]

Embora os aspectos técnicos do binário de criptografia sejam reveladores – com sobreposições claras no código-fonte com o *ransomware* Knight e vários vínculos adicionais às chaves de configuração do LockBit e do ALPHV –[131] o que realmente chama atenção é a rapidez com que o RansomHub se tornou o programa mais bem-sucedido em tão pouco tempo.

[129] Nota do analista: os arquivos vazados do Conti forneceram uma visão sobre a escala enorme necessária para operar um programa de RaaS do porte do Conti (de longe o maior RaaS no período de 2020 a 2022) – ver: 'Negotiation tactics and internal dynamics', PwC Threat Intelligence, CTO-SIB-20220324-01A.
[130] Nota do analista: as informações sobre a economia das operações de RaaS são escassas, sendo a maioria proveniente de postagens em fóruns feitas por operadores (ou, ocasionalmente, por afiliados), de discussões privadas vazadas ou, em raros casos, de entrevistas concedidas a veículos de mídia.
[131] 'RansomHub Ransom Run', PwC Threat Intelligence, CTO-TIB-20241108-01A

Figura 18 – Discrepância entre as estatísticas dos sites de vazamento do Ransomhub e do *ransomware* PLAY





O ano de 2024 revelou a resiliência e a capacidade de adaptação do ecossistema de RaaS diante de pressões externas, com esforços sofisticados e coordenados das forças de segurança sendo incapazes de conter tanto o número de invasões quanto a quantidade de grupos em atividade.

Comparado a um programa como o PLAY RaaS – que está em operação há muito mais tempo que o RansomHub – o número de vítimas registradas no site de vazamentos do RansomHub é bastante expressivo.

No entanto, é preciso cautela ao tirar conclusões a partir desses dados, já que muito do funcionamento interno do RansomHub – e, na verdade, da maioria das operações de RaaS – ainda é um mistério. Há, no entanto, vários fatores inter-relacionados que avaliamos como fundamentais para esse crescimento sem precedentes:

Uma lacuna no mercado: o contexto do lançamento do RansomHub provavelmente foi o principal fator por trás de sua ascensão meteórica. Ele foi introduzido no ecossistema criminoso poucos dias antes da ação coordenada das autoridades contra o LockBit 3.0 e da dissolução do ALPHV – os dois maiores programas da época – o que criou um vácuo para afiliados.

Uma proposta atrativa: o ecossistema de RaaS conta com um número limitado de afiliados. Embora esse número provavelmente nunca tenha sido tão alto, os operadores do RansomHub precisavam atrair afiliados que já atuavam em outros programas. A oferta de divisão de lucros em 90/10 (90% para o afiliado, 10% para o desenvolvedor) deve ter convencido afiliados já estabelecidos a migrar para o RansomHub – especialmente quando muitos buscavam novas oportunidades.

Fácil de usar, fácil de entender: para que um programa de RaaS cresça, ele precisa atrair o maior número possível de afiliados. Nem todos têm o mesmo nível de sofisticação – alguns são grupos experientes com metodologias consolidadas de invasão, como o White Dev 164 (também conhecido como Scattered Spider), enquanto outros são novatos no cenário. O código do RansomHub aproveita comandos de outros *ransomwares* e oferece várias opções de configuração, o que facilita sua integração com operações já em andamento.

Gestão eficaz: assim como em uma empresa legítima, a eficácia de um programa de RaaS depende de sua estrutura organizacional. Sabemos que operar um *ransomware* vai muito além de manter um site de vazamentos. A complexidade aumenta conforme o programa cresce.

Para que o RansomHub conseguisse se expandir tão rapidamente, é quase certo que seus operadores sejam pessoas com experiência prévia no universo do *ransomware*, ou então uma equipe com habilidades variadas capazes de manter a operação funcionando bem em todas as frentes.

Avaliamos que a ascensão do RansomHub provavelmente reflete um ecossistema impulsionado por fatores históricos, como oportunidades inesperadas, mas também por características modernas, como consolidação e organização. Quanto mais tempo o ecossistema de RaaS existe, mais seus procedimentos operacionais se consolidam, e os indivíduos envolvidos se tornam mais experientes na gestão de programas e no desenvolvimento de ferramentas para invasões mais eficientes.

Isso leva a uma situação em que os esforços de repressão das autoridades – pelo menos no aspecto tecnológico – tendem a ter cada vez menos impacto, à medida que afiliados e operadores se acostumam a retomar suas atividades e continuar operando normalmente.

Em meio ao caos: um avanço importante

As estatísticas revelam um ano bastante ativo para os operadores de *ransomware* – um fato difícil de negar ao se analisar os dados brutos. No entanto, uma história que acabou ofuscada pelos altos números nos sites de vazamentos foi o sucesso das ações das autoridades. Antes de fevereiro de 2024, o LockBit 3.0 era o programa de RaaS mais ativo por vários anos seguidos,[132] tendo divulgado quase 3 mil vítimas ao longo de seus aproximadamente três anos de existência.

A Operação Cronus foi uma vitória importante das forças de segurança, não apenas por ter conseguido conter o aumento no número de sites de vazamento, mas também porque, em retrospecto, mostrou uma compreensão fundamental do ambiente de RaaS (*Ransomware* como Serviço). Os afiliados do programa LockBit foram considerados um elemento central da Operação Cronus – algo que não havia sido tão enfatizado em operações anteriores desse tipo.

Além disso, tudo indica que as autoridades entenderam bem o operador do LockBit (identificado como o cidadão russo Dmitry Yuryevich Khoroshev), com base nas reações dele às ações tomadas durante a operação. Em cada fase, a divulgação pública de informações parecia provocar exatamente a resposta esperada de Dmitry, que ou republicava vítimas antigas no site de vazamentos ou adicionava vítimas que supostamente já haviam pago.[133]

Mesmo que o LockBit 3.0 ainda estivesse tecnicamente em operação no final de 2024 – promovendo o suposto lançamento do LockBit 4.0 no início de 2025 –[134] ele mal funcionava como um programa RaaS ativo, tendo publicado apenas quatro vítimas em seu site em dezembro de 2024.

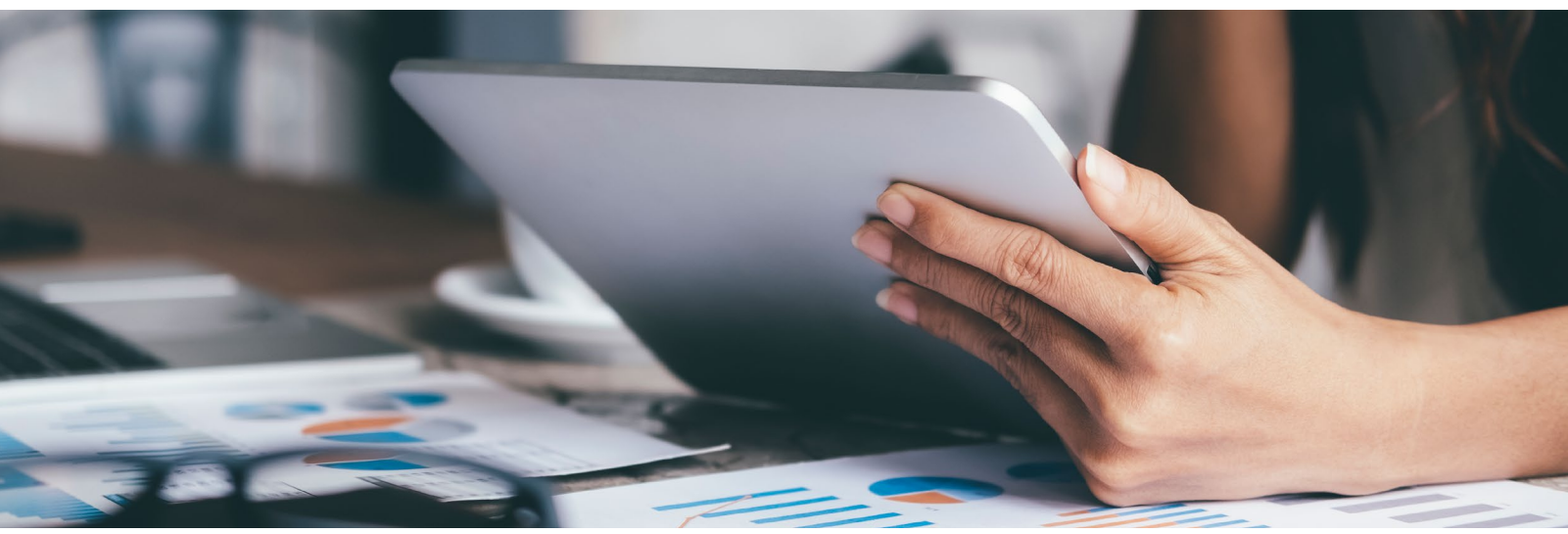
[132] 'Ransomware report for November 2023', PwC Threat Intelligence, CTO-SRT-20240103-01A
[133] Nota do analista: isso foi confirmado pela Operação Cronus, a qual revelou que dados pertencentes a entidades que já haviam pago o valor exigido de resgate ainda estavam sendo hospedados nos servidores de *backend* do LockBit (ver: 'International investigation disrupts the world's most harmful cyber crime group", NCA do Reino Unido, https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group – 20/2/2024).
[134] 'LockBit Admins Tease a New Ransomware Version', *Infosecurity Magazine*, https://www.infosecurity-magazine.com/news/lockbit-admins-tease-a-new/ (20/12/2024)

Ao minar a percepção pública desses operadores mais proeminentes – mostrando que, sob pressão, eles recorrem a táticas desesperadas que comprometem seu próprio modelo de negócios (como publicar vítimas que já pagaram) – o provável objetivo era fazer com que as organizações deixassem de pagar resgates a operadores que não cumprem sua parte no acordo.

Uma avaliação quantitativa completa do impacto da Operação Cronus provavelmente nunca será possível, devido à falta de um conjunto de dados completo sobre os pagamentos. Como mencionado no início desta seção, o número de vítimas em sites de vazamento em 2024 aponta para uma resiliência que não pôde ser totalmente contida, mesmo com a derrubada de dois programas RaaS (incluindo o ALPH-V), independentemente de sua fatia de mercado.

No entanto, ao retirar esses atores do cenário, as forças de segurança colocaram a responsabilidade pela criação, disseminação e manutenção do *ransomware* nas mãos de operadores menos experientes e, em tese, menos capacitados.

Com tantos programas afiliados utilizando bases de código reutilizadas disponíveis em código aberto,[135] espera-se que a falta de inovação por parte dos agentes de ameaças abra uma janela de oportunidade para que equipes de defesa de rede e fornecedores de antivírus comecem a desenvolver formas mais seguras de descriptografar esses códigos antigos ou criar planos de resposta abrangentes que possam ser aplicados assim que o *ransomware* for ativado.



[135] Nota do analista: há muitas bases de código antigas em circulação entre os programas RaaS, como Babuk, LockBit 3.0 e Phobos, apenas para citar alguns exemplos.

Seção cinco

Águas turvas

O uso de campanhas e técnicas para controlar, dominar ou, de alguma forma, distorcer a narrativa predominante de um adversário foi mais frequente do que em anos anteriores. Essas operações são conduzidas por meio de uma combinação de *misinformation* e *disinformation* dependente de recursos cibernéticos.[136]

[136] Nota do analista: normalmente, *misinformation* refere-se a informações falsas compartilhadas por indivíduos mal-informados, sem intenção maliciosa, enquanto *disinformation* diz respeito a informações falsas divulgadas com a intenção deliberada de enganar o público. De forma geral, esse tipo de atividade pode ser dividido entre as que são viabilizadas pelo meio digital (por exemplo, técnicas tradicionais de propaganda que utilizam canais digitais, como redes sociais) e as que são dependentes de recursos cibernéticos (como invasões de rede). Grande parte das atividades monitoradas pela PwC está relacionada a campanhas ciberdependentes.

Para analistas de inteligência de ameaças, um dos principais desafios dessas campanhas maliciosas está na etapa de atribuição, já que os agentes mal-intencionados costumam mascarar suas atividades por trás de contas falsas ou automatizadas, utilizando infraestrutura hospedada por plataformas terceirizadas de redes sociais. Por isso, há casos em que as evidências disponíveis não são suficientes para identificar com precisão a origem da atividade.

A prática de "embaralhar o jogo" é uma tática recorrente com quase duas décadas de uso,[137] [138] [139] e os agentes responsáveis por essas ações vêm aprimorando suas técnicas ao longo do tempo. Eles exploram tanto a disposição dos adversários (ou a falta dela) para escalar conflitos quanto a constante transformação das redes sociais como variáveis para definir a melhor forma de conduzir suas campanhas.

O ano de 2024 ofereceu a esses agentes tradicionais diversas oportunidades específicas para executar operações direcionadas (como eleições e eventos internacionais em um cenário geopolítico fragmentado), o que levou à ampliação do uso dessas técnicas, assim como à diversificação de abordagens e métodos empregados.

A desinformação tradicional foi observada por meio da continuidade de operações de anos anteriores realizadas por agentes de ameaça com base na Rússia e no Irã.

⚠ Um dos grupos mais ativos, com base na Rússia, é o DoppleGanger, em operação desde maio de 2022. Ao longo de 2024, o grupo realizou diversas campanhas, que acabaram levando à aplicação de sanções e à derrubada de suas operações por parte de governos ocidentais.[140]

[137] 'The Russian Hybrid Warfare: Case of Estonia', The Foreign Policy Council, https://foreignpolicycouncilcom.wordpress.com/2021/11/04/the-russian-hybrid-warfare-case-of-estonia/ (4/11/2021)
[138] 'Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election', Departamento do Tesouro dos EUA, https://home.treasury.gov/news/press-releases/jy0494 (18/11/2021)
[139] 'Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections', Mandiant, https://www.mandiant.com/resources/blog/prc-dragonbridge-influenceelections (26/10/2022)
[140] 'Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere', Departamento de Justiça dos EUA, https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence (4/9/2024)

⚠ No Irã, o grupo Yellow Dev 19 (também conhecido como Emennet Pasargad ou Cotton Sandstorm) espalhou desinformação relacionada a atletas israelenses durante os Jogos Olímpicos de Paris.[141] As postagens falsas, que fingiam ser de um movimento francês de extrema-direita, tinham como objetivo provocar medo e causar impacto psicológico nos israelenses.

- Esse não foi o único caso em que o Yellow Dev 19 utilizou desinformação com o propósito de causar dano psicológico. Em outubro de 2024, o grupo enviou mensagens SMS a funcionários israelenses que trabalhavam em um porto em Haifa, alegando ter invadido a infraestrutura do local. A mensagem alertava os trabalhadores a evacuarem o porto, afirmando que ele se tornaria em breve alvo de um de seus mísseis.[142]

Figura 19 – Mensagem de ameaça da persona Yellow Dev 19 a funcionários do Porto de Haifa, alertando sobre um suposto ataque com míssil

[141] 'Yellow Dev 19's Olympic influence campaign', PwC Threat Intelligence, CTO-SRT-20240730-01A
[142] 'Yellow Dev 19 influence campaign goes ballistic', PwC Threat Intelligence, CTO-QRT-20241029-01A

2024 ficou conhecido como o “ano das eleições”, com diversos pleitos ocorrendo em vários países – alguns deles de forma inesperada. Em muitos casos, isso levou a tentativas de espalhar desinformação durante os períodos de campanha política.[143]

Além das iniciativas mais amplamente divulgadas para influenciar o resultado da eleição nos Estados Unidos por meio de desinformação e campanhas de influência maliciosa,[144] [145] houve diversas outras tentativas, ao longo do ano, de manipular narrativas e influenciar resultados eleitorais em outros países.

Durante o ciclo eleitoral da Geórgia, circularam nas redes sociais várias narrativas tentando convencer a população de que os países da OTAN estariam buscando usar a Geórgia como uma segunda frente de ataque contra a Rússia.[146]

Na Moldávia, não apenas foi identificada a disseminação de desinformação,[147] mas também tentativas ativas de fraude eleitoral.[148]

A eleição em Taiwan, realizada em janeiro, foi marcada por inúmeros episódios de desinformação nas redes sociais, atribuídos a grupos de ameaças com base na China.[149] Os temas incluíam suposta colaboração entre Washington e Taipei em armas biológicas, importação de carne suína contaminada dos EUA, além de vídeos *deepfake* e difamações contra candidatos.[150] [151]

[143] ‘The 2024 election cyber threat stress test’, PwC Threat Intelligence, CTO-SIB-20240520-01A
[144] ‘FBI links video falsely depicting voter fraud in Georgia to ‘Russian influence actors”, Associated Press, https://apnews.com/article/fbi-russia-georgia-frauddisinformation-eebea4ab200682ccd3e97fb9f164e6ca (1/11/2024)
[145] ‘Sanctions in Response to Attempted Iranian and Russian Interference in U.S. General Election’, Departamento de Justiça dos EUA, https://www.state.gov/sanctions-in-response-toattempted-iranian-and-russian-interference-in-u-s-general-election/ (31/12/2024)
[146] ‘“Global War Party,” “Second Front,” “Unprecedented election meddling” from the West, and other propaganda narratives dominating Georgian information space in the run-up to the key 2024 elections’, EDMO, https://edmo.eu/publications/global-war-party-second-front-unprecedented-election-meddling-fromthe-west-and-other-propaganda-narratives-dominating-georgian-information-spa/ (25th October 2024)
[147] ‘Moldova’s pro-Western president wins reelection in runoff shaken by alleged Russian meddling’, PBS, https://www.pbs.org/newshour/world/moldovas-prowestern-president-wins-reelection-in-runoff-shaken-by-alleged-russian-meddling (3rd November 2024)
[148] ‘Moldovans are voting in a pivotal presidential runoff. But voter fraud threatens its democracy’, Associated Press, https://apnews.com/article/moldovademocracy-election-russia-disinformation-corruption-0a23e330da7121dbc34b085fc5d0d8ad (2nd November 2024)
[149] ‘DPP wins historic third presidential term’, PwC Threat Intelligence, CTO-SIB-20240125-01A
[150] ‘China bombards Taiwan with fake news ahead of election’, Politico, https://www.politico.eu/article/china-bombards-taiwan-with-fakenews-ahead-of-election (10/1/2024)
[151] ‘As Taiwan voted, Beijing spammed AI avatars, faked paternity tests and ‘leaked’ documents’, Australian Strategic Policy Institute, https://www.aspistrategist.org.au/as-taiwan-voted-beijing-spammed-ai-avatars-faked-paternity-tests-and-leaked-fake-documents/ (18/1/2024)

Na Romênia, a eleição presidencial foi anulada pela Corte Constitucional após a apresentação de provas suficientes de que campanhas cibernéticas maliciosas ocorreram em paralelo a irregularidades no financiamento de campanha, com o objetivo de influenciar o resultado das eleições.[152]

O uso de redes de *proxy* e ofuscação já havia sido mencionado no contexto de agentes de ameaças ligados à China e Coreia do Norte, que utilizaram redes ORB comerciais e personalizadas para esconder suas operações em 2024. No entanto, esses não foram os únicos grupos a adotar essas práticas – a atividade nesse campo foi intensa e atingiu seu auge em 2024.

Empresas que fornecem *spyware* comercial, como a Grey Anqa (também conhecida como NSO Group) e a Grey Mazzikim (também conhecida como Candiru), baseiam seus modelos de negócios na proteção da identidade e origem de seus clientes. Por meio de ferramentas sofisticadas, como o Pegasus,[153] aliadas a *exploits* de um ou nenhum clique, esses clientes podem conduzir atividades de coleta de inteligência contra alvos permanecendo, ao menos em teoria, anônimos.

[152] 'The Romanian 2024 Election Annulment: Addressing Emerging Threats to Electoral Integrity', IEFS, https://www.ifes.org/publications/romanian-2024-electionannulment-addressing-emerging-threats-electoral-integrity (20/12/2024)
[153] 'Spyware among us', PwC Threat Intelligence, CTO-SIB-20231201-02A

- Observamos atividades de vários desses clientes em pesquisas realizadas ao longo de 2024, o que nos permitiu entender melhor como funcionam essas redes de anonimização.[154]

- Ano passado,[155] avaliamos que as capacidades de *spyware* enfrentariam um crescente escrutínio público ao longo de 2024. Em certa medida, isso de fato se confirmou: além de publicações mais aprofundadas,[156] processos judiciais continuaram a manter essas empresas fornecedoras de vigilância sob os holofotes.[157] No entanto, houve sinais – especialmente no fim do ano – indicando a retirada ou arquivamento de alguns desses processos,[158] [159] o que permitiu que o tema do *spyware* perdesse destaque no noticiário de cibersegurança.

Um dos casos mais inusitados de 2024 foi relatado pela Microsoft, envolvendo o grupo de ameaça russo Blue Python (também conhecido como *Secret Blizzard*), que utilizou a infraestrutura de outro grupo com base no Paquistão – o Storm-0156 (estreitamente ligado ao grupo White Dev 55, também conhecido como Operation SideCopy). O objetivo era se passar por esse grupo durante operações realizadas na região Ásia-Pacífico.[160]

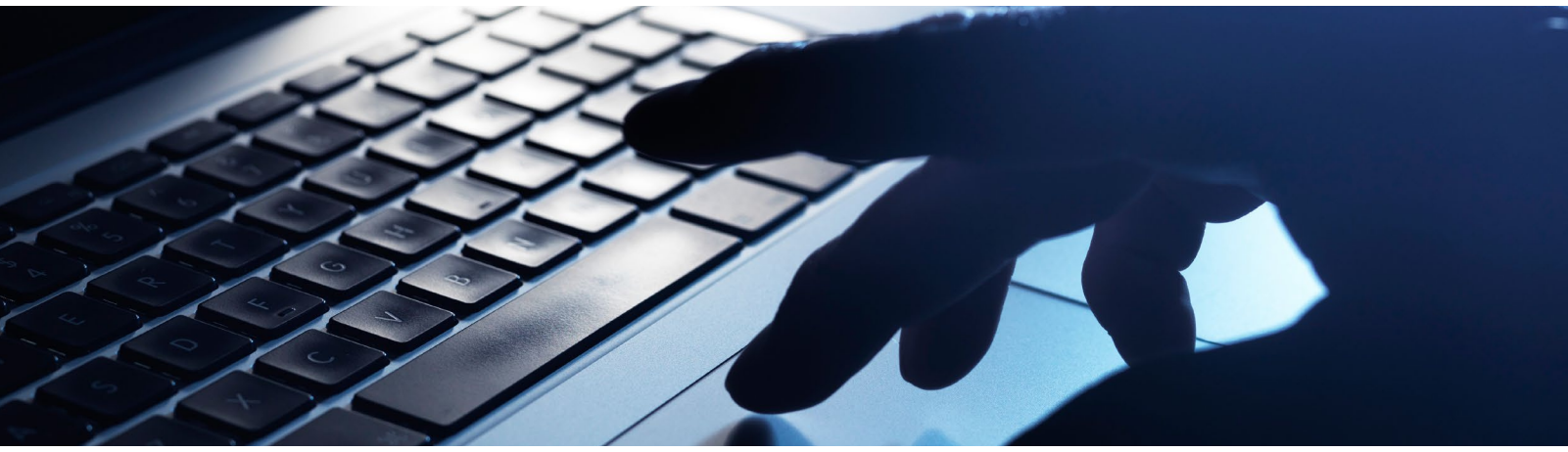
- Essa mesma tática foi repetida pelo Blue Python em suas intrusões na Ucrânia, onde se fez passar por uma entidade criminosa monitorada pela Microsoft sob o codinome Storm-1919, utilizando uma variante específica do *bot* Amadey para coletar informações das vítimas e instalar cargas maliciosas adicionais.[161]

[154] 'Uncovering Grey Anqa', PwC Threat Intelligence, CTO-TIB-20240903-01A
[155] Cyber Threats 2023: A Year in Retrospect", PwC Threat Intelligence, CTO-YIR-20240624-01A
[156] 'Global: A Web of Surveillance – Unravelling a murky network of spyware exports to Indonesia', Amnesty International, https://www.amnesty.org/en/latest/news/2024/05/unravelling-a-murky-network-of-spyware-exports-to-indonesia/ (2/5/2024)
[157] 'US judge finds Pegasus spyware maker liable over WhatsApp hack', The Guardian, https://www.theguardian.com/technology/2024/dec/20/whatsapppegasus-spyware-nso-group-hacking (20/12/2024)
[158] 'Thai court dismisses activist's spyware suit', The Bangkok Post, https://www.bangkokpost.com/thailand/general/2907406/thai-court-dismisses-activistsspyware-suit (23/112024)
[159] 'Apple seeks to drop its lawsuit against Israeli spyware pioneer NSO', Washington Post, https://www.washingtonpost.com/technology/2024/09/13/applelawsuit-nso-pegasus-spyware/ (13/9/2024)
[160] 'Frequent freeloader part I: Secret Blizzard compromising Storm-0156 infrastructure for espionage', Microsoft, https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/
[161] 'Frequent freeloader part II: Russian actor Secret Blizzard using tools of other groups to attack Ukraine', Microsoft, https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/ (11/12/2024)

Outro tipo de desinformação que ganhou força em 2024 – após surgir em 2023 – foi o esforço de diluir ou desacreditar informações de inteligência divulgadas por governos ocidentais, por meio de campanhas conduzidas por adversários geopolíticos.

Agências do governo dos EUA, em parceria com o setor privado, publicaram diversos relatórios sobre o grupo chinês Red Dev 49 (também conhecido como Volt Typhoon), apontado como responsável por ataques cibernéticos contra infraestruturas críticas nos Estados Unidos durante 2023 e 2024.[162]

Após a divulgação inicial, veículos de comunicação chineses não só contestaram as alegações como também passaram a afirmar ativamente que o Volt Typhoon seria, na verdade, uma invenção dos EUA com o objetivo de incriminar a China.[163]



Historicamente, as respostas a acusações de espionagem corporativa e coleta de inteligência costumavam vir em declarações à imprensa, comunicados oficiais ou postagens em redes sociais feitas por autoridades políticas. No caso do Volt Typhoon, porém, houve três investigações formais e publicações subsequentes divulgadas pelo Centro Nacional de Resposta a Emergências de Vírus de Computador da China (CVERC). Esses relatórios foram publicados sob o título da série: <Lie to me />.

[162] 'Volt Typhoon', PwC Threat Intelligence, CTO-QRT-20230525-01A
[163] 'Who is Volt Typhoon? A State-sponsored Actor? Or Dark Power?', Natto Thoughts, https://nattothoughts.substack.com/p/who-is-volt-typhoon-a-statesponsored (12/6/2024)

A importância desses documentos está na intenção evidente de não apenas lançar dúvidas sobre as atribuições feitas ao grupo, mas de inverter completamente a narrativa – alegando que o Red Dev 49 seria, na verdade, uma operação conduzida pelo próprio governo dos EUA.

Diferentemente de negações anteriores, esses relatórios têm caráter técnico e são longos, adotando o formato típico de relatórios de inteligência de ameaças. O objetivo provável desse formato é conferir legitimidade à linguagem utilizada, tanto para o público chinês quanto para audiências no Ocidente – a maioria das quais não tem o conhecimento técnico necessário para analisar criticamente as alegações.

A linguagem utilizada nos relatórios também parece, quase certamente de forma intencional, se apoiar no discurso on-line contemporâneo sobre desconfiança em relação ao governo dos EUA – um tema amplamente debatido tanto na sociedade quanto na academia.

A combinação entre o formato técnico do relatório e a linguagem cuidadosamente escolhida resulta em um tipo de resposta às comunicações conjuntas dos EUA que não havia sido visto anteriormente. Com o claro objetivo de não apenas negar as acusações, mas de abalar diretamente a confiança nos relatórios originais e nas instituições envolvidas, avaliamos que esse posicionamento do CVERC representa uma escalada na retórica.

Ainda não está claro como evoluirá a relação entre os Estados Unidos e a China em 2025. No entanto, já se observa uma tendência de aumento no número de comunicados conjuntos publicados por agências norte-americanas sobre atividades atribuídas a grupos de ameaças ligados à China.

Acreditamos que esse padrão de divulgação de informações deve continuar. E, caso as tensões entre Pequim e Washington se mantenham no nível observado em 2024, avaliamos com probabilidade realista que veremos novas respostas semelhantes às apresentadas nos relatórios do CVERC.

O ano de 2024 foi marcado por um aumento geral na disseminação de *misinformation* e *disinformation* em diversas sociedades. Embora isso esteja parcialmente ligado à quantidade de eleições ocorridas ao longo do ano, não consideramos esse o único fator.

Há uma erosão contínua da confiança nas instituições governamentais em muitas democracias,[164] [165] [166] impulsionada por uma combinação de campanhas históricas de desinformação, instabilidade política e decisões de políticas públicas vistas como míopes,[167] [168] além do surgimento de novas tecnologias que mudaram profundamente a forma como as pessoas se comunicam e se informam.

Esse cenário criou um ciclo negativo de desconfiança que vem sendo explorado por agentes mal-intencionados, enfraquecendo ainda mais a confiança pública. O ceticismo é hoje tão difundido em certos segmentos da população que publicações como as do CVERC provavelmente têm muito mais impacto e poder de convencimento agora do que teriam há cinco anos.

Avaliamos que, em 2025, as campanhas de desinformação devem continuar em alta, com as redes sociais se mantendo como o principal meio explorado por agentes de ameaças para manipular e distorcer narrativas.

Também é provável que a forma como os Estados respondem à divulgação pública de informações de inteligência siga a tendência observada em 2024 – com respostas mais estruturadas, técnicas e voltadas à disputa narrativa – em vez de um retorno aos comunicados breves e protocolares que eram comuns anteriormente.

[164] Nota do analista: embora os dados mais recentes do Pew Research Center indiquem um "aumento modesto" em relação a 2023, com a confiança geral no governo atingindo 22% – sendo 35% entre os democratas e apenas 11% entre os republicanos – esse índice ainda é considerado extremamente baixo (ver: "Public Trust in Government: 1958-2024", Pew Research Center, https://www.pewresearch.org/politics/2024/06/24/public-trust-in-government-1958-2024/, 24/6/2024).
[165] 'Trust and confidence in Britain's system of government at record low', National Centre for Social Research, https://natcen.ac.uk/news/trust-and-confidencebritains-system-government-record-low (12/6/2024)
[166] 'In welche der folgenden Institutionen und Berufsgruppen haben Sie großes Vertrauen?', Statista, https://de.statista.com/statistik/daten/studie/1283706/umfrage/vertrauen-in-institutionen-in-deutschland/ (Janeiro/2024)
[167] 'German Chancellor Olaf Scholz loses confidence vote', BBC, https://www.bbc.com/news/articles/ckg36pp6dpyo (16/12/2024)
[168] "Macron's brutal dissolution of the Assemblée resulted in the dissolution of his majority", Le Monde, https://www.lemonde.fr/en/politics/article/2024/07/01/macron-s-brutal-dissolution-of-the-assemblee-resulted-in-the-dissolution-of-his-majority_6676300_5.html (1/7/2024)

Apêndices

Apêndice A – Metodologia

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

Este relatório apresenta uma seleção das análises que elaboramos ao longo de 2024. Além de nossos recursos próprios e do acesso a ferramentas comerciais e de código aberto, trabalhamos em estreita colaboração com as firmas do Network PwC em situações de resposta a incidentes e em outras atividades.

Linguagem estimativa

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

Expressões de probabilidade

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

Níveis de confiança

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

Apêndice B – Referência de agentes de ameaças

Monitoramos uma ampla gama de agentes de ameaças em mais de 25 países e utilizamos uma convenção própria de nomenclatura. Primeiro, atribuímos uma cor que indica a região geográfica onde avaliamos que o agente está sediado. A cor branca é usada para ameaças cuja origem geográfica ainda está em avaliação.

A tabela abaixo inclui alguns exemplos desse mapeamento por cores. Após a cor, adicionamos o nome de uma figura mitológica para criar uma designação única para o agente de ameaças. Quando observamos atividades que não podem ser atribuídas a um grupo já conhecido, classificamos esse conjunto como um "*dev set*", para facilitar futuros desenvolvimentos e análises.

Em alguns casos, se nossa análise levar a uma atribuição conclusiva, o *dev set* é promovido a um grupo nomeado. Quando identificamos sobreposição entre nossas atribuições e as de outras organizações, também fornecemos os nomes correspondentes utilizados por esses terceiros.

*Refere-se a entidades ou agentes de ameaças que estão situados nos países que compõem a aliança de inteligência conhecida como Cinco Olhos (Five Eyes): Austrália, Canadá, Estados Unidos, Nova Zelândia e Reino Unido.

Apêndice C – Referência de agentes de ameaças

A seguir, estão listados todos os agentes de ameaças mencionados neste relatório, seja de forma direta no texto ou por meio de notas de rodapé. A tabela inclui o nome utilizado pela equipe de Inteligência de Ameaças da PwC, os nomes alternativos (ou apelidos) conhecidos e a motivação atribuída ao agente com base em nossa análise.

É importante observar que, embora um nome utilizado pela equipe da PwC possa ter correspondência com apelidos de outros agentes de ameaças conhecidos, isso não implica necessariamente uma equivalência direta entre os grupos. A correspondência pode indicar sobreposição parcial de atividade, similaridade de técnicas ou atribuição ainda em andamento.

Agente de ameaça	*Aliases* (nomes alternativos)	Motivação
Black Alicanto	Dangerous Password, LeeryTurtle, CryptoMimic, CryptoCore, Black Dev 1, Black Dev 2, COPERNICIUM, Sapphire Sleet, TA444, Stardust Chollima, Bluenoroff, Alluring Pisces, Genie Spider	Cibercrime
Black Dev 4	Contagious Interview, Famous Chollima, DEV#POPPER, Storm-1877	Cibercrime
Blue Athena	Fancy Bear, APT28, Pawn Storm, Sednit, STRONTIUM, TG-4127, Swallowtail, apt_tipsy_bear, Group 74, Crisis4, Sofacy, Tsar Team, SNAKEMACKEREL, IRON TWILIGHT, Forest Blizzard	Espionagem
Blue Callisto	Grey Pro, REUSE, Callisto Group, COLDRIVER, SEABORGIUM, Star Blizzard, BlueCharlie, TAG-53	Espionagem

Agente de ameaça	*Aliases* (nomes alternativos)	Motivação
Blue Dev 5	NOBELIUM, BoomBox, NobleBaron, Midnight Blizzard, BlueBravo	Espionagem
Blue Dev 8	N/D	Espionagem
Blue Otso	Gamaredon, Gamaredon Group, Dancing Salome, Shuckworm, ACTINIUM, IRON TILDEN, Primitive Bear, Aqua Blizzard	Espionagem
Grey Anqa	NSO Group, Night Tsunami	Espionagem
Grey Hades	Gaza Hacker Team, Molerats, Gaza Cybergang	Espionagem
Grey Karkadann	AridViper, APT-C-23, Desert Falcon, Mantis	Espionagem
Grey Mazzikim	SOURGUM, Candiru	Espionagem
Red Dev 38	BackdoorDiplomacy, CloudComputating	Espionagem
Red Dev 49	Volt Typhoon, BRONZE SILHOUETTE, Vanguard Panda, VOLTZITE, Insidious Taurus, UNC3236, TAG-87	Espionagem
Red Ishtar	Red Dev 26, Earth Preta, UNC4191, Stately Taurus, CeranaKeeper	Espionagem
Red Lich	Mustang Panda, BRONZE PRESIDENT, Red Delta, DarkPeony, Twill Typhoon	Espionagem
Red Vulture	APT25, Ke3chang, APT15, Vixen Panda, BRONZE PALACE, Mirage, Nylon Typhoon	Espionagem
White Dev 101	ALPHV-ng, ALPHV, BlackCat, Noberus	Cibercrime
White Dev 164	N/D	Cibercrime
White Dev 183	plym0uth, Plymouth, Steal-C	Cibercrime
White Dev 184	UNC4393, Storm-1811	Cibercrime
White Dev 55	Operation Sidecopy	Espionagem
White Eloko	Volatile Cedar, Lebanese Cedar	Espionagem
White Enbar	RansomHub	Cibercrime
White Janus	LockBit 3.0	Cibercrime

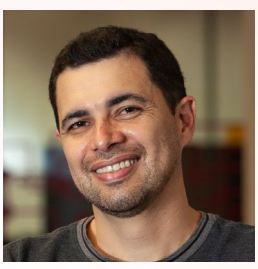
Agente de ameaça	*Aliases* (nomes alternativos)	Motivação
White Peryton	PLAY	Cibercrime
Yellow Dev 19	DEV-0198, ViceLeaker, Cotton Sandstorm, Emennet Pasargad, Ilia Net Gostar Atiq, Ilia Net Gostar Iranian Telecommunication and Electronic	Sabotagem, espionagem
Yellow Garuda	APT35, Charming Kitten, Newsbeef, Phosphorus, Mint Sandstorm, UNC788, ITG18, COBALT ILLUSION, TA453, Newscaster, APT42	Espionagem

Contatos

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

Fernando Mitre
Sócio
fernando.mitre@pwc.com

Larissa Escobar
Sócia
larissa.escobar@pwc.com



Magnus Santos
Sócio
magnus.santos@pwc.com

Rafael Cortes
Sócio
cortes.rafael@pwc.com

Siga a PwC nas redes sociais