SOPHOS
Cybersecurity delivered.

Playbook dos Adversários Ativos 2022

Comportamentos, táticas e ferramentas de invasores cibernéticos observados na linha de frente de resposta a incidentes durante 2021

Por **John Shier**, Consultor sênior em segurança, Departamento do CTO

Documento técnico Sophos Junho de 2022

Introdução

O desafio de defender uma organização contra ataques cibernéticos cada vez mais complexos e acelerados pode ser grande. Continuamente, os adversários adaptam e expandem seus comportamentos e conjuntos de ferramentas, aproveitando-se de antigas vulnerabilidades para criar novas vulnerabilidades e utilizando-se de ferramentas comuns de TI para escapar da detecção e se manter um passo à frente das equipes de segurança.

Não é fácil para os profissionais de operações de segurança e TI das organizações acompanhar as diferentes abordagens usadas pelos adversários – particularmente quando se trata de ataques ativos direcionados que envolvem mais de um golpista, como um intermediador de acesso inicial (IAB) que atinge seu alvo para depois vender esse acesso a uma quadrilha de criminosos para usar em seus ataques de ransomware.

O Playbook dos Adversários Ativos 2022 detalha os principais adversários, ferramentas e comportamentos de ataque vistos em ação durante 2021 pela linha de frente das equipes de resposta a incidentes da Sophos. Ele dá prosseguimento ao Active Adversary Playbook 2021 e mostra como o panorama dos ataques continua a evoluir.

Nosso objetivo é ajudar as equipes de segurança a entender o que os adversários fazem durante os ataques e como detectar e defender-se contra esses ataques a suas redes.

Os resultados se baseiam em dados sobre incidentes investigados pela equipe Sophos Rapid Response durante 2021. Sempre que possível, comparamos esses dados aos resultados de respostas a incidentes descritos no Active Adversary Playbook 2021.

Dados demográficos de resposta a incidentes 2021

O relatório se baseia em 144 incidentes direcionados a organizações de todos os tamanhos, em uma grande diversidade de setores da indústria e localizadas nos EUA, Canadá, Reino Unido, Alemanha, Itália, Espanha, França, Suíça, Bélgica, Países Baixos, Áustria, Emirados Árabes Unidos, Arábia Saudita, Filipinas, Bahamas, Angola e Japão.

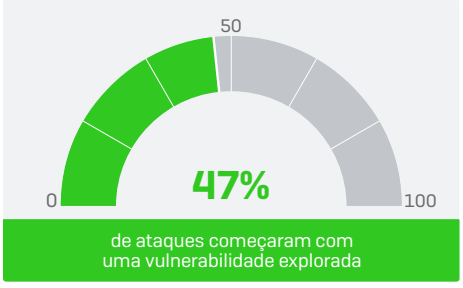
Os setores de maior representatividade são o de manufatura (17% dos casos de resposta a incidentes se deram neste setor) seguido por varejo (14%), saúde (13%), TI (9%), construção (8%) e educação (6%). Há mais informações sobre diferentes perfis nas tabelas de dados no fim deste relatório.

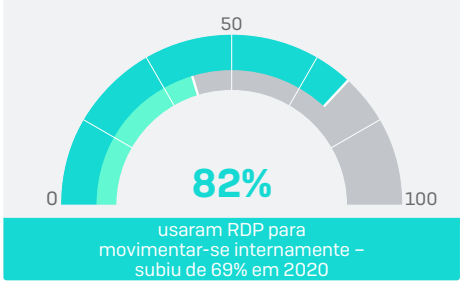
Painel: A anatomia dos ataques ativos em 2021

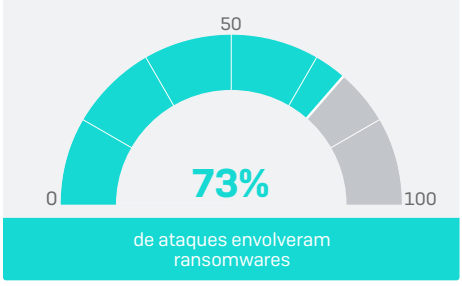
Dois dos acontecimentos em ataques cibernéticos que mais influenciaram 2021 ocorreram em março e agosto, quando foram confirmadas as vulnerabilidades ProxyLogon e ProxyShell nos servidores Microsoft Exchange. Conforme observado recentemente pela CISA e outras agências de segurança do governo, os bugs ProxyLogon e ProxyShell foram intensamente explorados pelos adversários. Não surpreende que apareçam em um grande número dos incidentes investigados pela Sophos durante 2021.

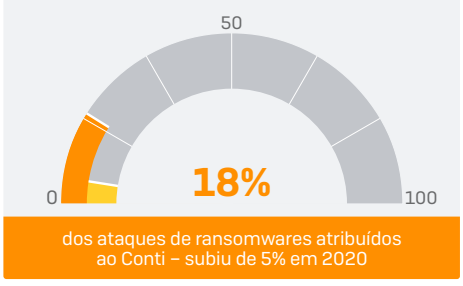
Painel: Anatomia dos ataques ativos em 2021

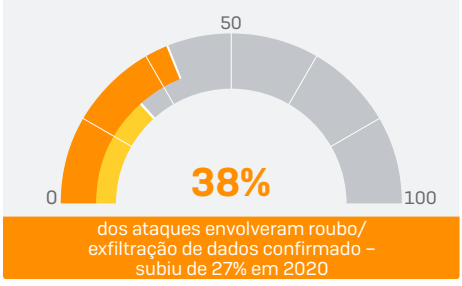
Principais descobertas das investigações de resposta a incidentes











É bem provável que haja muitas outras transgressões criadas pelo ProxyLogon e pelo ProxyShell que até então ainda são desconhecidas – situações em que web shells e backdoors foram implantados nas vítimas para acesso persistente e que, agora, estão apenas aguardando silenciosamente até que o acesso seja usado ou vendido.

Isso leva a outro acontecimento importante que moldou o panorama das ameaças cibernéticas em 2021: a crescente influência e poder dos intermediadores de acesso inicial (IAB).

Os IABs foram os primeiros a invadir e obter acesso a um alvo que pode ser vendido. Esse sucesso colocou os IABs rapidamente em evidência no cenário dos novos bugs, que esperam comprometer suas vítimas rapidamente antes que os patches sejam desenvolvidos e distribuídos. O objetivo dos IABs é estabelecer uma base de operações em uma vítima e, possivelmente, fazer alguns movimentos exploratórios iniciais para avaliar o valor do sistema conquistado – antes de vendê-la a outros adversários, como operadores de ransomware, para usarem em seus ataques, às vezes meses após a invasão inicial.

Como observado no Relatório de Ameaças 2022 da Sophos, o crescente consumo de IABs reflete o aumento do "profissionalismo" dos ataques em um mercado de ameaças cibernéticas que engloba um número crescente de fornecedores de serviços especializados. A progressão da indústria de ransomware como serviço (RaaS) é outro exemplo dessa tendência.

Por último, porém não menos importante, indícios forenses descobertos durante as investigações de resposta a incidentes em 2021 revelam situações em que vários adversários, incluindo IABs, gangues de ransomwares, criptomineradores e, ocasionalmente, até mesmo vários operadores de ransomware, direcionavam simultaneamente seus ataques a uma mesma organização. Esse é o modelo que continuará a dar forma ao panorama das ameaças cibernéticas em 2022 e além.

O intervalo de tempo que os invasores permanecem na rede das vítimas está aumentando, provavelmente devido a essas atividades. Outros adversários que se resguardam para vitimar as redes mais tarde, às vezes simultaneamente, incluem construtores de botnets e plataformas de entrega ou droppers.

Esses fatos são discutidos abaixo em mais detalhes.

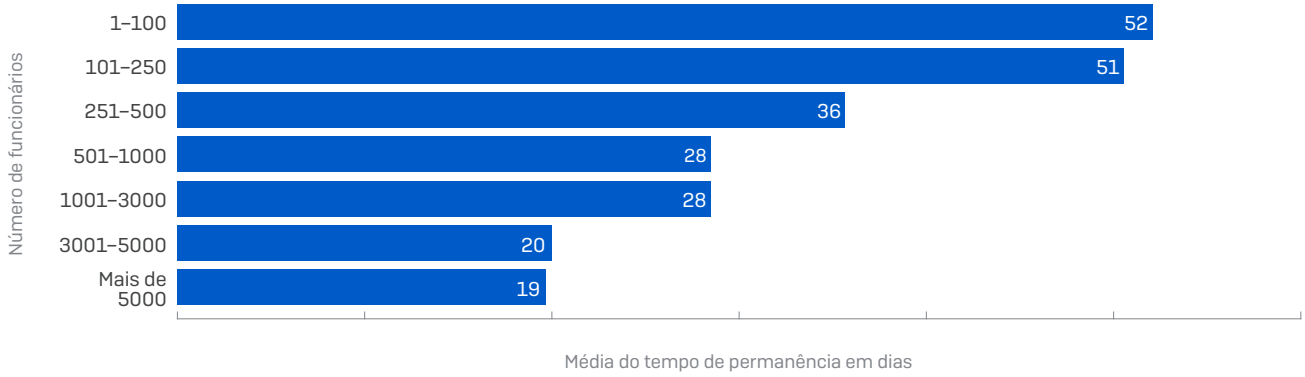
Os invasores invisíveis

Os dados dos incidentes mostram que a média de tempo de permanência aumentou em cerca de um terço entre 2020 e 2021, de 11 para 15 dias. Houve uma variação considerável, com ataques culminando em ransomwares com períodos de permanência mais curtos, em média cerca de 11 dias (abaixo dos 18 dias em 2020), enquanto os ataques que envolveram outras invasões duraram significativamente mais tempo, com permanência mediana de 34 dias.

Variações no tempo médio de permanência de um invasor (mediana)

Como sugere o acima exposto, tempos prolongados de permanência podem significar o envolvimento de um IAB. Para pequenas empresas ou setores de indústrias como a educação (com a média de tempo de permanência de um invasor de 34 dias), tempos de permanência prolongados também demonstram como pode ser difícil para o pessoal da segurança de TI interna sair no encalço de ameaças, investigá-las e responder a alertas e suspeitas de possíveis ataques de modo proativo.

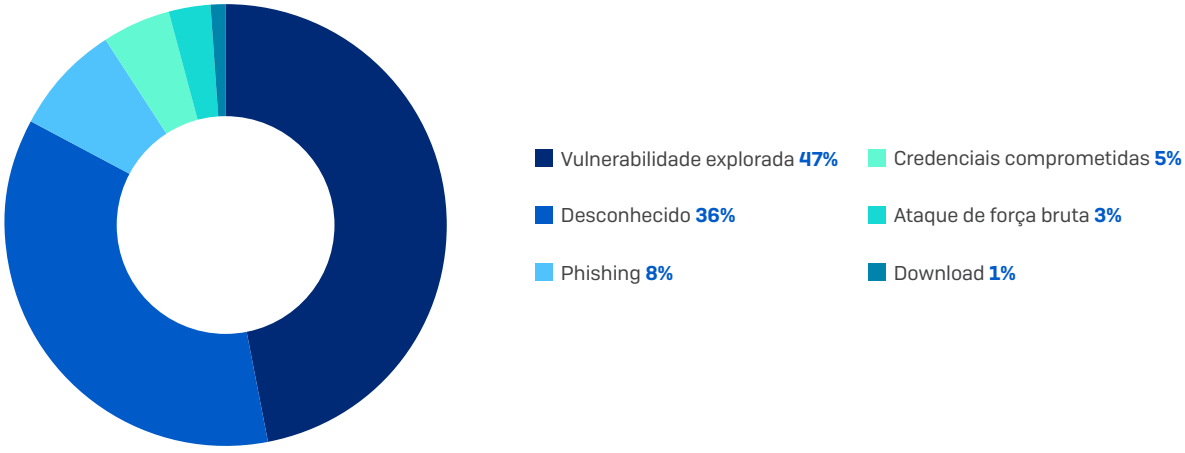
Tempo de permanência do invasor por tamanho da empresa (média)



As causas primárias dos ataques

Nem sempre é possível, ou fácil, determinar a causa primária de um ataque. Às vezes os invasores apagam intencionalmente os indícios de suas atividades e outras vezes, até que chegue o pessoal da equipe de resposta, os seus próprios profissionais de segurança de TI já terão limpado ou recriado a imagem das máquinas comprometidas. Apesar disso, evidências mostram que entre os incidentes investigados pela Sophos, a exploração de vulnerabilidades causadas pela falta de patches – no caso do ProxyLogon e ProxyShell – foi a causa primária de quase metade (47%) dos incidentes cibernéticos investigados em 2021.

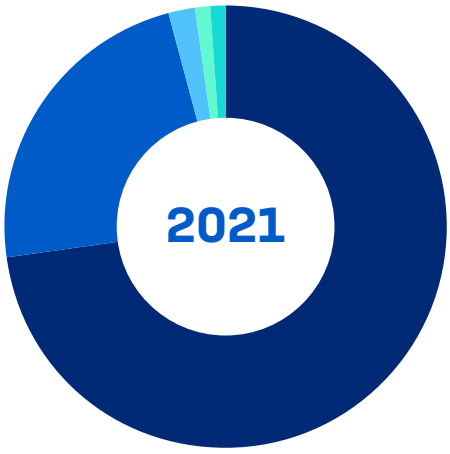
Causas primárias dos ataques



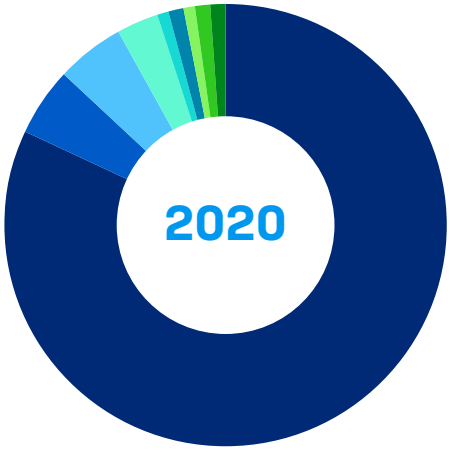
Os principais tipos de ataques

O lançamento de um ransomware geralmente marca o momento em que um ataque fica visível para as equipes de segurança de TI. Portanto, não nos surpreende que 73% dos incidentes respondidos pela Sophos em 2021 envolveram ransomwares. Ransomware também foi o tipo de ataque mais predominante em 2020, 82% (o número mais alto reflete o menor conjunto de dados). No caso de exfiltração de dados, responsável por 1% dos incidentes, as equipes de resposta acreditam que esses incidentes provavelmente teriam se transformado em ataques de ransomware, mas foram capturados e neutralizados a tempo.

Tipos de ataque



- Ransomware **73 %**
- Outras invasões **23%**
- Criptominerador **2%**
- Exfiltração de dados **1%**
- Dropper **1%**



- Ransomware **82 %**
- Desconhecido **5%**
- Exfiltração **5%**
- Criptominerador **3%**
- Cavalo de Troia/Dropper **1%**
- Cavalo de Troia bancário **1%**
- Wiper **1%**
- Ferramentas de Pen-Test/Ataque **1%**
- Impedido **1%**

O segundo tipo de ataque mais predominante revelado pelas investigações de resposta a incidentes foi a ampla categoria "outra invasão", responsável por 23% dos incidentes. Para os fins deste relatório, "outras invasões" se define como invasões que não resultaram em ransomware ou outro tipo de ataque.

Geralmente, a invasão é o resultado de uma vulnerabilidade sem patches que foi explorada, como o ProxyLogon e o ProxyShell, mas também inclui o uso indevido de serviços de acesso remoto ou VPNs desprotegidas, credenciais de conta roubadas ou descuido com a segurança (por exemplo, deixar pontos de entrada à Internet abertos).

O ponto crucial aqui é que as invasões foram detectadas e neutralizadas antes que uma carga maliciosa fosse entregue no destino. Parece-nos viável presumir que algumas, senão a maioria dessas invasões, pertenciam ao inventário abusivo dos IABs: um acesso "depositado" que ainda não foi vendido a outro adversário. Se as invasões ainda não foram detectadas, é provável que um grande número delas tenha ocorrido e se transformado em ataques de ransomware.

Criptomineradores foram o principal tipo de ataque em 2% dos incidentes investigados. A presença de criptomineradores mal-intencionados é geralmente detectada pelo impacto causado ao desempenho do sistema, pois a mineração ilícita de criptomoedas consome a capacidade de processamento dos computadores. Você pode até tentar renegar os criptomineradores a uma ameaça indesejada de baixa repercussão, mas o fato de eles estarem na rede prova que existe um ponto de entrada vulnerável em algum lugar dela, podendo ser um precursor de ameaças mais graves.

O mesmo se aplica a droppers e sistemas de entrega de malware em geral, projetados para entregar, carregar ou instalar outras cargas maliciosas no sistema sob a mira. Eles são perpetradores de um ataque iminente, oferecendo uma plataforma para módulos mal-intencionados adicionais, como backdoors e ransomwares. As equipes de resposta devem tratar a presença de droppers e sistemas de entrega de malwares, incluindo Trickbot, Emotet e outros, com a mesma seriedade que tratam os ransomwares mais relevantes, pois geralmente são precursores de ataques maiores.

Um playground movimentado

Os tipos de ataques não são mutualmente exclusivos. Como mencionado anteriormente, vários adversários, incluindo IABs, gangues de ransomwares e criptomineradores, podem ser encontrados em uma mesma rede ao mesmo tempo.

Por exemplo, ainda que os criptomineradores tenham sido o principal tipo de ataque em apenas 2% dos casos de resposta a incidentes, eles também estavam presentes em 7% dos incidentes de ransomware. Os criptomineradores costumam varrer as redes infectadas e remover os outros mineradores, mas podem perfeitamente coexistir com outras ameaças, como ransomwares.

Incidentes de ataques simultâneos relatados pela Sophos em 2021 incluem um ataque que envolveu o ransomware Atom Silo e dois criptomineradores, e um ataque duplo de ransomware envolvendo o Netwalker e o REvil. Essa tendência continua em 2022.

A caixa de ferramentas do adversário

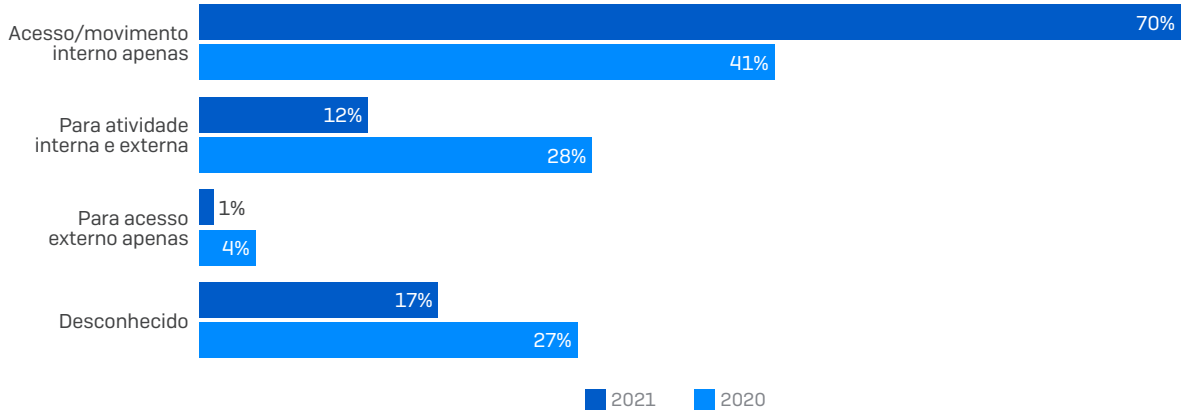
Serviços de desktop remoto são uma grande ameaça interna

O protocolo RDP foi parte integrante de pelo menos 83% dos ataques, um aumento em relação a 2020, quando apareceu em 73% dos ataques. O uso interno despontou em 82% dos casos e o uso externo foi observado em 13% dos casos. Esses valores se comparam aos de 69% e 32%, respectivamente, em 2020.

Contudo, vale comentar sobre o modo como os invasores usam o protocolo RDP. Em menos de três quartos (70%) dos incidentes que envolveram RDP, a ferramenta foi usada *somente* para acesso interno e movimentos laterais — um aumento significativo em comparação aos 41% em 2020.

O protocolo RDP foi usado *somente* para acesso externo em apenas 1% dos casos, uma queda em relação aos 4% em 2020; e apenas 12% dos ataques mostrou invasores usando RDP para acesso externo e para movimentos laterais, menos da metade do índice de 2020 (quando registrou 28%).

Invasores usam o protocolo RDP (Remote Desktop Protocol)



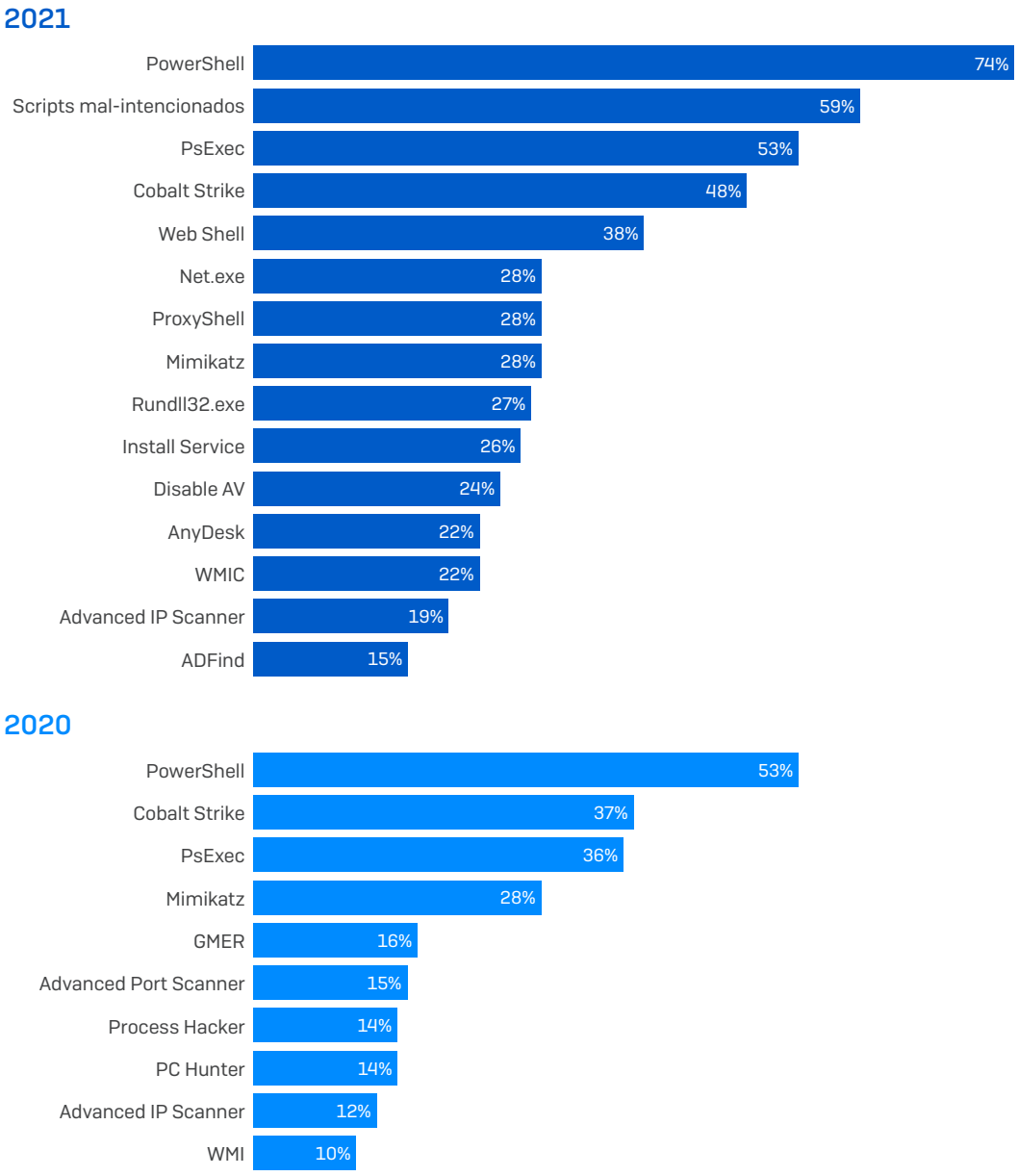
O declínio no uso do protocolo RDP para o acesso externo é, provavelmente, reflexo das melhorias na segurança, incluindo o poder de desabilitar o serviço. Contudo, o RDP permanece amplamente acessível dentro de seu perímetro, e proteger esse acesso é um ponto-chave para as equipes de segurança.

O conjunto de ferramentas de ataque em 2021

O gráfico abaixo mostra os "artefatos", incluindo ferramentas, técnicas e serviços, mais encontrados nos kits de ataque de um invasor em 2021. Muitos deles também podem ser usados por profissionais de TI para fins benéficos. Eles são populares entre os adversários porque permitem realizar atividades como roubo de credenciais, descobertas, movimentos laterais e execução de malwares, entre outras, enquanto se mesclam às atividades inócuas e cotidianas do departamento de TI.

A quantidade e a natureza dos artefatos destacam o desafio que os profissionais na linha de defesa enfrentam para diferenciar as atividades mal-intencionadas das atividades legítimas na rede.

Principais artefatos usados nos ataques



Uma análise mais minuciosa dos itens mais populares usados nos ataques revela a estrutura e estratégia dos ataques cibernéticos em 2021.

Os artefatos que formam os conjuntos de ferramentas

Os artefatos identificados durante as investigações de resposta a incidentes podem ser divididos em três categorias: ferramentas legítimas e exploratórias, binários da Microsoft e artefatos adicionais (scripts, técnicas, serviços e mais).

No geral, as investigações de resposta a incidentes encontraram 525 artefatos diferentes, bem mais do que os 132 em 2020 (embora o tamanho de base da amostra tenha sido maior), compreendendo 209 ferramentas legítimas e fraudulentas, 107 binários da Microsoft e 209 artefatos adicionais.

Ferramentas legítimas e exploratórias

Incluem softwares que foram usados para auxiliar no ataque. Cobalt Strike (48%) e Mimikatz (28%) mantiveram as duas primeiras posições de 2020, seguidos pelo AnyDesk (22%), Advanced IP Scanner (19%) e ADFind (15%). Comparado a 2020, o Cobalt Strike aumentou seu alcance (subiu de 37%), o Mimikatz manteve-se estável (28%) e três novas ferramentas chegaram para fechar o placar dos cinco mais presentes.

O **Cobalt Strike** é um pacote de ferramentas de exploração produzidas comercialmente para ajudar as equipes de segurança a recriarem uma grande variedade de cenários de ataques. Os invasores tentam estabelecer um "beacon" de backdoor com o Cobalt Strike na máquina infectada. Os beacons podem ser configurados para executar comandos e downloads, executar softwares adicionais, retransmitir comandos para outros beacons instalados em uma rede alvo e comunicar-se de volta com o servidor do Cobalt Strike. As intenções do Cobalt Strike na rede devem ser investigadas imediatamente.

A segunda ferramenta mais vista, **Mimikatz**, também foi originariamente projetada como uma ferramenta de segurança ofensiva e pode roubar senhas e outras credenciais de contas para usar em um ataque.

Ferramentas de varredura de rede legítimas, como **Advanced Port Scanner** e **IP Scanner**, são usadas para gerar listas de IPs e nomes de dispositivos, o que possibilita aos invasores focar na estrutura de rede da vítima e em seus mecanismos computacionais mais críticos.

O uso indevido da ferramenta de gerenciamento de TI **AnyDesk** é altamente comum, oferecendo aos invasores o controle direto do computador sob a mira, incluindo o controle do mouse, teclado e a capacidade de ver a tela. Serviços legítimos de acesso remoto, como o **TeamViewer**, **Screen Connect**, **Atera RMM** e **Splashtop**, também estavam presentes entre os destaques de 2021.

Process Hacker, **PCHunter** e **GMER** são todas ferramentas legítimas que incluem drivers do kernel. Se um invasor instalar o driver do kernel correto, em geral conseguirá desabilitar seus produtos de segurança.

Binários da Microsoft

Separar as ferramentas da Microsoft das ferramentas gerais mostra como os invasores se aproveitam da situação. Estas ferramentas são assinadas digitalmente pela Microsoft. Sem muita surpresa, o **PowerShell** (74%) encabeça a lista, seguido por **PsExec** (53%), "**net.ex**e" (28%), "**rundll32.exe**" (27%) e a ferramenta **WMI Command-line** (WMIC) (22%). O uso do PowerShell, PsExec e WMIC aumentou em 2021, em comparação a 2020.

A ferramenta "net.exe" foi usada em muitas das fases de ataque, em geral como ferramenta de descoberta, enquanto a ferramenta "rundll32.exe" foi usada amplamente para a execução e evasão de defesas.

Outras ferramentas da Microsoft que poderiam revelar um ataque escondido na rede são "**whoami.exe**", **Task Scheduler** (para manter a persistência) e "**schtasks.exe**" (para executar códigos mal-intencionados). O uso de tais ferramentas deve ser monitorado de perto.

Artefatos adicionais

Esta categoria inclui ferramentas e técnicas, como tentar desabilitar a proteção, vulnerabilidades como ProxyShell, uso de serviços de nuvem como **Mega.io**, malwares adicionais encontrados, infecções secundárias e protocolos de transporte usados.

Scripts mal-intencionados (exceto o PowerShell) foram observados em 59% dos incidentes investigados. Scripts mal-intencionados são códigos de software que possibilitam atividades maliciosas. Exemplos de scripts usados indevidamente por invasores incluem scripts de linha de comando e em lote DOS/CMD, scripts do Python (uma coleção de comandos em um arquivo executado como programa) e VBScripts (scripts do Visual Basic que podem ser executados no Windows ou Windows Explorer).

Web shells foram o segundo tipo mais comum de ameaça encontrado (em 38% dos incidentes), com grande destaque ao ProxyShell (28%) e ProxyLogon (11%). Instalar serviços, desabilitar a proteção, despejar LSASS, criar contas ilegítimas, modificar o registro e limpar logs estão entre os 10 principais usos.

Exfiltração de dados

Em 2021, o **Rclone** entrou na lista dos principais artefatos usados para exfiltração. Rclone é uma ferramenta de linha de comando que se conecta a uma grande variedade de provedores de armazenamento em nuvem, como o Mega, e, em 2021, foi a ferramenta mais usada na exfiltração de dados. Outros provedores de armazenamento em nuvem que se destacaram nos dados do ano incluem **Dropbox**, **DropMeFiles**, **M247**, **pCloud** e **Sendspace**.

Além do Rclone, outras ferramentas encontradas nas investigações de incidentes que auxiliaram na exfiltração incluem **Megasync**, **FileZilla**, **Handy Backup**, **StealBit**, **WinSCP** e **Ngrok**.

O aparecimento de ferramentas de exfiltração entre as principais na lista de 2021 era de se esperar, considerando-se o fato de que 38% de todos os incidentes investigados envolveram a exfiltração de dados, subindo de 27% em 2020. Vários outros incidentes (8% no geral) mostram sinais de dados coletados e preparados para uma possível remoção. Nos casos em que a exfiltração ocorreu, indícios sugerem que as informações roubadas foram vazadas em 46% dos incidentes.

Via de regra, os invasores removem as informações no estágio final, antes de implantarem o ransomware. A análise de incidentes da Sophos mostra que, em 2021, o tempo médio entre a exfiltração de dados e a implantação do ransomware era de aproximadamente 44 horas. O intervalo médio ficou apenas um pouco acima de quatro dias (4,28 dias), enquanto o ponto mediano ficou abaixo dos dois dias (1,84 dia).

Independentemente da média usada, a mensagem aqui é que após a exfiltração existe a oportunidade de o pessoal na linha de defesa evitar o estágio mais dramático e final do ataque que se desenrola. A detecção de ferramentas sabidamente usadas na exfiltração de dados deve, portanto, ser investigada com urgência.

Combinação de ferramentas

As investigações de incidentes revelam um padrão na combinação de ferramentas na rede das vítimas que oferece um poderoso sinal de alerta para as equipes de segurança de TI (dados comparativos de 2020 estavam disponíveis em determinados casos):

- Em 2021, o PowerShell e scripts não PS mal-intencionados foram vistos juntos em 64% dos casos
- PowerShell e Cobalt Strike combinaram-se em 56% dos casos, comparado a 58% em 2020
- PowerShell e PsExec combinaram-se em 51% dos casos, comparado a 49% em 2020
- PowerShell, scripts mal-intencionados e Cobalt Strike foram vistos em 42% dos casos
- PowerShell, scripts mal-intencionados e PsExec foram vistos em 38% dos casos
- PowerShell, Cobalt Strike e PsExec ocorreram em 33% dos casos, mais do que os 12% em 2020
- Cobalt Strike e Mimikatz foram vistos juntos em 16% dos casos

Tais correlações continuam hoje tão importantes como no ano passado, pois detectá-las pode servir como um alerta antecipado de um ataque iminente ou confirmar a presença de um ataque ativo.

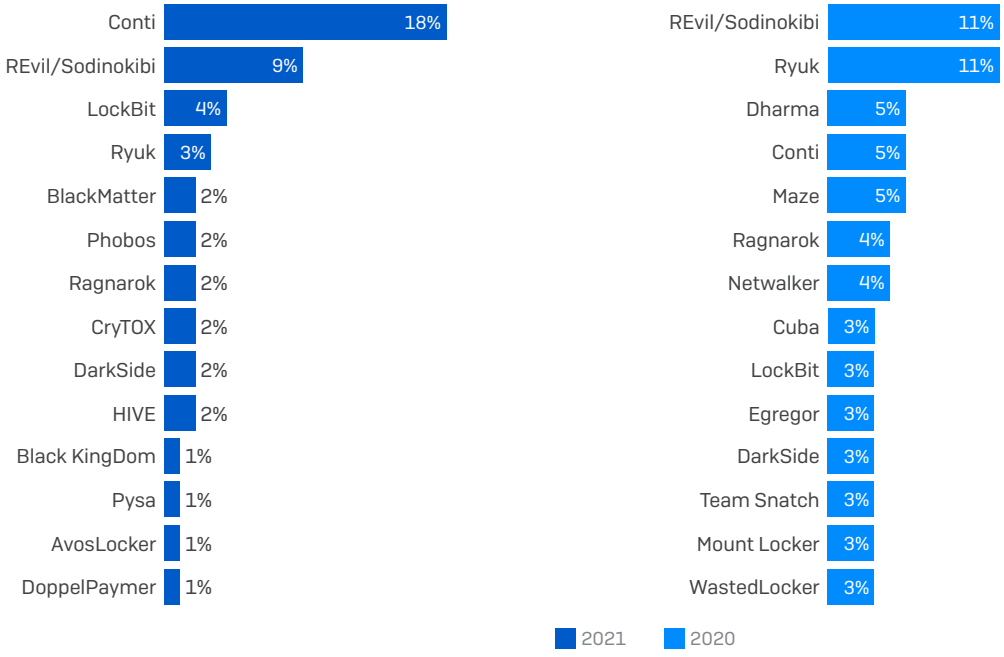
Os principais ransomwares adversários em 2021

Foram identificados 41 ransomwares adversários diferentes em meio aos 144 incidentes incluídos nesta análise. Desses, cerca de dois terços (28) eram de grupos novos que foram vistos pela primeira vez em 2021. Dezoito grupos de ransomwares observados em incidentes em 2020 desapareceram da lista em 2021, um claro indicativo da grande sobrecarga, dinamismo e complexidade que o cenário cibernético representa hoje e do quanto isso pode dificultar a vida do pessoal na linha de defesa.

De muitas formas, 2021 foi "dominado" pelo Conti, um prolífico operador de RaaS que esteve por trás de pouco menos de um em cada cinco (18%) incidentes investigados pela Sophos. Porém, vale notar que o ransomware REvil foi responsável por um em cada dez incidentes no geral, apesar de ter, aparentemente, encerrado suas operações em julho de 2021 (mas reaparecendo rapidamente em setembro de 2021 e, novamente, em 2022).

Outras famílias predominantes de ransomwares durante 2021 incluem DarkSide, o RaaS por trás dos notórios ataques ao Colonial Pipeline nos EUA, e Black KingDom, uma das "novas" famílias de ransomwares que surgiu em março de 2021, resultado da vulnerabilidade ProxyLogon.

Atribuição: Principais ransomwares adversários



Cerca de um quarto (24%) dos incidentes em 2021, e 25% em 2020, foram atribuídos a outros grupos de ransomwares – já o restante dos incidentes não pôde ser atribuído com certeza a nenhum outro grupo conhecido.

A Sophos fez um minucioso relato do ransomware Conti. Uma extensa lista de artigos sobre o Conti e outras famílias predominantes de ransomwares, incluindo LockBit, Ryuk e mais, pode ser encontrada no centro de inteligência da Sophos sobre ameaças de ransomware.

Conclusão

Toda organização é um alvo para um adversário em algum lugar, tornando-se progressivamente, um alvo para mais adversários. De phishing e fraudes financeiras a construtores de botnet, plataformas de entrega de malware, criptomineradores, IABs, roubo de dados, espionagem industrial, ransomware e mais – se existir um ponto de entrada na rede para uma vulnerabilidade, são grandes as chances de que os invasores estejam procurando por ela e que acabarão encontrando-a para explorar seu potencial.

Até que o ponto de entrada exposto seja fechado e que todo o trabalho de estabelecimento e retenção de acesso feito pelos invasores seja totalmente erradicado, qualquer um pode entrar depois deles. E provavelmente vai entrar.

As equipes de segurança podem defender suas organizações monitorando e investigando atividades suspeitas. A diferença entre benigno e maligno nem sempre é fácil de identificar. Em qualquer ambiente, tanto cibernético como físico, a tecnologia pode ajudar, e muito, mas, por si só, ela não basta. Experiência, habilidades humanas e a capacidade de responder são partes vitais de uma solução de segurança.

Os grandes ensinamentos em resposta a incidentes de 2021 são em relação ao nível de rapidez e abrangência que vulnerabilidades facilmente disseminadas e exploradas são aproveitadas pelos adversários, o que contribui para invasões mais prolongadas e vários adversários. Para os defensores, esses ensinamentos mostram que detectar, investigar e responder aos indicadores da presença de ferramentas e técnicas adversárias é essencial.

Sophos Rapid Response

Os resultados expressos no relatório se baseiam em dados sobre incidentes investigados pela Sophos Rapid Response, uma equipe dedicada de resposta a incidente e especialistas em neutralização de ameaças. O serviço Sophos Rapid Response está disponível para os clientes Sophos existentes e para aqueles que não trabalham com a Sophos.

Se estiver enfrentando um incidente ativo e gostaria de falar com a equipe Rapid Response, ligue para um dos números abaixo a qualquer hora:

EUA: +1 4087461064

Austrália: +61 272084454

Canadá: +1 7785897255

França: +33 186539880

Alemanha: +49 61171186766

Reino Unido: +44 1235635329

Suécia: +46 858400610

Tabelas de dados adicionais

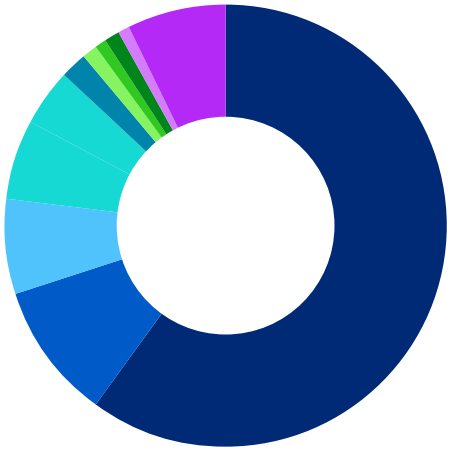
Artefatos da investigação de incidentes mapeados à cadeia de ataques MITRE

As ferramentas, técnicas e outros artefatos observados durante as investigações do incidente foram mapeados à estrutura MITRE ATT&CK. Mais detalhes serão divulgados em um artigo da empresa publicado no Sophos News.

Estágios do MITRE Attack											
Acesso inicial	Execução	Persistência	Escalonamento de privilégio	Evasão de defesas	Acesso a credenciais	Descoberta	Movimento lateral	Coleta	Comando e Controle	Exfiltração	Impacto
Artefatos											
Serviços remotos	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	Navegação na rede	Cobalt Strike	Rclone	Criptografia de dados
Exploits	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	Violação de rede

Dados demográficos de resposta a incidentes 2021

Casos de resposta a incidentes por país

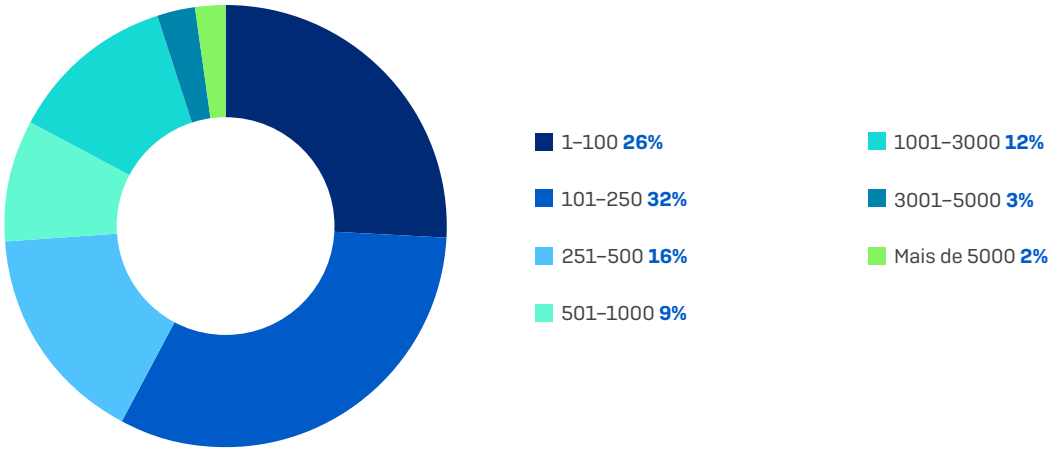


- EUA **60%**
- Alemanha **10%**
- Reino Unido **7%**
- Canadá **6%**
- Itália **4%**
- Espanha **2%**
- França **1%**
- Suíça **1%**
- Bélgica **1%**
- Filipinas **1%**
- Outro **7%** (Países Baixos, Áustria, Emirados Árabes Unidos, Arábia Saudita, Bahamas, Angola, Japão)

Casos de resposta a incidentes por setor

- Manufatura **17%**
- Varejo **14%**
- Saúde **12%**
- Tecnologia da Informação **9%**
- Construção **8%**
- Educação **6%**
- Alimentação **4%**
- Logística **4%**
- Financeiro **4%**
- Entretenimento **3%**
- Serviços **3%**
- Mídia de notícias **3%**
- Outro **13%** (Transporte, Farmacêutico, MSP/Hospedagem, Sem fins lucrativos, Governo, Hospitalidade, Jurídico, Agricultura, Energia, Imobiliário)

Casos de resposta a incidentes por tamanho da organização (nº de funcionários)



Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

2022-05-25 PTBR (DD)