SOPHOS

Relatório de Ameaças 2024 da Sophos: O crime cibernético em sua plenitude

O ransomware continua a ser uma das maiores ameaças cibernéticas para as pequenas empresas, mas há outras que também estão se intensificando.

Sophos X-Ops

Índice

Fundamentos

O crime cibernético afeta as pessoas em todas as esferas sociais, mas são as pequenas empresas que absorvem o maior impacto. Embora as notícias se concentrem, em sua maioria, nos ataques cibernéticos às grandes empresas e às agências governamentais, são as pequenas empresas (organizações com menos de 500 funcionários) que costumam estar mais vulneráveis aos criminosos cibernéticos e que, proporcionalmente, sofrem mais com as consequências dos ataques cibernéticos. A falta de pessoal experiente nas operações de segurança, o baixo investimento em segurança cibernética e orçamentos menores destinados à tecnologia da informação são fatores que contribuem para esse nível de vulnerabilidade. Quando atingidas por ataques cibernéticos, os gastos com a recuperação podem chegar a ponto de forçar muitas dessas pequenas empresas a fecharem suas portas.

As pequenas empresas representam grandes perdas. De acordo com o Banco Mundial, mais de 90% das empresas em âmbito mundial são organizações de pequeno e médio porte, respondendo a mais de 50% dos empregos em caráter global. Nos Estados Unidos, as pequenas e médias empresas respondem a 40% da atividade econômica geral. Neste relatório, os termos pequenas e médias empresas e organizações de pequeno e médio porte são intercambiáveis, refletindo nossos dados igualmente.

Em 2023, mais de 75% dos casos de resposta a incidentes dos clientes atendidos pelo serviço X-Ops Incident Response da Sophos ocorreram com pequenas empresas. Os dados coletados desses casos, somados à telemetria coletada de clientes do nosso software para proteção de pequenas e médias empresas, nos dão uma perspectiva exclusiva sobre as ameaças que atacam essas organizações diariamente.

Sumário executivo

Com base nesses dados e na pesquisa realizada pela Sophos sobre ameaças, observamos que os ransomwares continuam a ter maior impacto nas organizações de menor porte. Mas há outras ameaças que também representam um risco às pequenas empresas:

- O roubo de dados é o foco da maioria dos malwares que atinge as pequenas e médias empresas — ladrões de senhas, keyloggers, também conhecidos por registradores de teclas, e outros spywares respondem a praticamente metade das detecções de malware. O roubo de credenciais através de phishing e malware pode expor os dados de pequenas empresas em plataformas na nuvem e provedores de serviços, enquanto violações de rede podem ser usadas para atingir também seus clientes.
- Os invasores intensificaram o uso da distribuição de malware baseado na Web através de malvertising ou da otimização maliciosa de mecanismos de busca ("envenenamento de SEO") para vencer as dificuldades criadas pelo bloqueio de macros maliciosas em documentos, além de usarem imagens de disco para saturar as ferramentas de detecção de malware.
- Dispositivos sem proteção conectados à rede das organizações, incluindo computadores não gerenciados sem um software de segurança instalado, computadores configurados incorretamente e sistemas com softwares que tiveram seu suporte descontinuado pelos fabricantes, são o primeiro ponto de entrada para todos os tipos de ataques cibernéticos criminosos contra pequenas empresas.
- Os invasores agora se dedicam a abusar dos drivers — sejam drivers vulneráveis de empresas genuínas ou drivers que foram assinados com certificados roubados ou obtidos de modo fraudulento — para burlar e desativar as defesas contra malwares em sistemas gerenciados.
- Os ataques por e-mail começaram a se diversificar, indo da simples engenharia social para um engajamento mais ativo que tem como alvo threads de e-mails e respostas para criar armadilhas mais convincentes.
- Ataques a usuários de dispositivos móveis, incluindo golpes baseados em engenharia social vinculados ao abuso de serviços de terceiros e plataformas de redes sociais, crescem exponencialmente, afetando indivíduos e pequenas empresas. Isso engloba desde e-mails comerciais e serviços na nuvem comprometidos até golpes de abate de porcos (shā zhū pán (殺豬盤)).

Prefácio de nossos dados

Os dados usados em nossa análise provêm das seguintes fontes:

- Relatórios de clientes — telemetria de detecção do software de proteção da Sophos instalado na rede dos clientes, o que nos dá uma ampla visão das ameaças encontradas e cuja análise é realizada pelo SophosLabs, que neste relatório são citados como dataset do Labs.
- Dados de incidentes do MDR (Managed Detection and Response), coletados durante os escalonamentos realizados ao detectar atividades maliciosas na rede dos clientes de MDR, que neste relatório são citados como dataset do MDR.
- Dados da equipe de Resposta a Incidentes, extraídos de incidentes na rede dos clientes de empresas com até 500 funcionários onde havia pouca ou nenhuma proteção de detecção e resposta gerenciada em vigor, que neste relatório são citados como dataset do IR.

Para uma visão mais aprofundada dos dados extraídos estritamente dos casos externos atendidos por nossa equipe de IR (incluindo casos que envolvem clientes com mais de 500 funcionários), leia a nossa publicação Relatório de Adversários Ativos (AAR). As conclusões neste relatório se baseiam nesses datasets combinados e normalizados, a menos que indicado o contrário.

Os dados são o alvo principal

O maior desafio à segurança cibernética enfrentado pelas pequenas empresas — e organizações de todos os portes — é a proteção de dados. Mais de 90% dos ataques registrados por nossos clientes envolvem o roubo de dados ou credenciais de alguma forma, seja por meio de um ataque de ransomware, extorsão de dados, acesso remoto não autorizado ou o simples roubo dos dados.

O comprometimento de e-mails corporativos (BEC), em que contas de e-mail são tomadas pelos criminosos cibernéticos com a finalidade de fraude ou outros fins maléficos, é um problema substancial no cenário das pequenas e médias empresas. Ainda não cobrimos a pauta de BEC em nossa publicação Relatório de Adversários Ativos, mas os autores do AAR estimam que, em 2023, o comprometimento de e-mails corporativos foi identificado por nossa equipe de Resposta a Incidentes com mais frequência do que qualquer outro tipo de incidente, exceto ransomware.

Credenciais roubadas, incluindo cookies de navegadores, podem ser usadas para comprometer e-mails corporativos, acessar serviços de terceiros, como sistemas financeiros na nuvem, por exemplo, e acessar recursos internos que podem ser explorados para fraudar ou obter ganhos monetários. Elas também podem ser vendidas por "intermediadores de acesso" a qualquer pessoa que as queira explorar — a Sophos rastreou ofertas em fóruns clandestinos que dizem oferecer acesso à rede de várias pequenas e médias empresas.

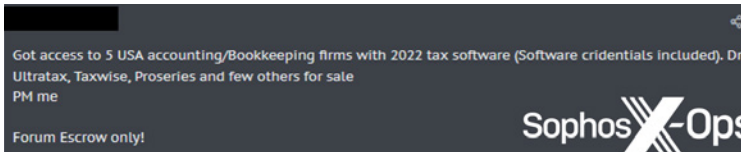


Figura 1: Uma postagem em um fórum anunciando o acesso a uma pequena firma de contabilidade nos EUA

Figura 2: Uma postagem em um fórum anunciando o acesso a uma pequena empresa na Bélgica

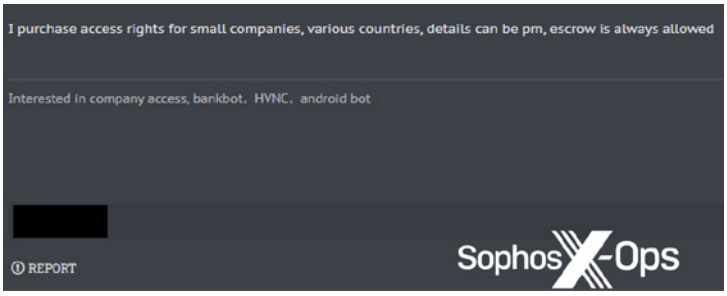


Figura 3: Um criminoso cibernético procurando adquirir o acesso a pequenas empresas

Figura 4: Acesso a uma pequena empresa na Itália à venda em um fórum criminoso

Por categoria, quase metade dos malwares detectados em 2023 tinha como alvo os dados de suas vítimas. A maioria deles é formada por malwares que classificamos especificamente como "stealers", que são malwares que se apoderam de credenciais, cookies de navegadores, pressionamentos de teclas e outros dados que podem ser convertidos em dinheiro na forma de venda de acesso ou utilizados para intensificar a exploração.

Contudo, devido à sua natureza modular, fica difícil categorizar um malware só por funcionalidade, já que praticamente todos os malwares têm a capacidade de roubar algum tipo de dado dos sistemas sob ataque. Essas detecções tampouco incluem outros métodos de roubo de credencial, como phishing por e-mail, mensagens de texto ou outros ataques de engenharia social. Há também outros alvos, como o macOS e dispositivos móveis, em que malwares, aplicativos potencialmente indesejados e ataques de engenharia social têm na mira os dados dos usuários, especialmente financeiros.

Categorias de malware por número de atualizações de assinatura em 2023

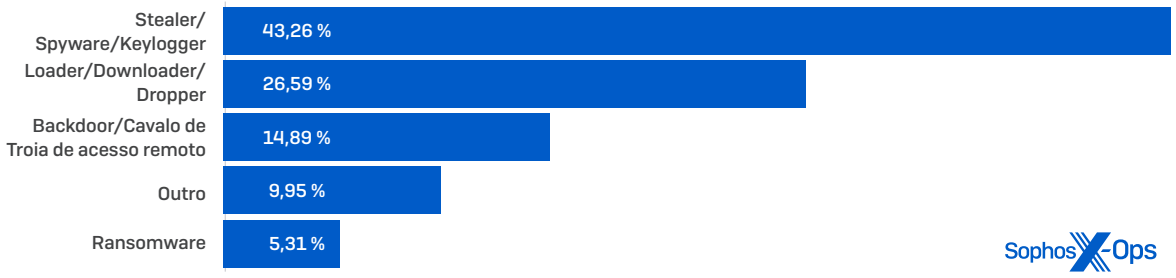


Figura 5: Detecções de malware por tipo em 2023, como visto nos datasets do Labs e MDR

Quase 10% dos malwares detectados foram classificados fora das quatro categorias principais mostradas acima. A categoria "Outro" inclui malwares que têm como alvo navegadores para injetar anúncios, redirecionar resultados de busca para fazer dinheiro com cliques, ou para modificar ou coletar dados em benefício do desenvolvedor do malware, entre outras coisas.

Alguns stealers são bastante específicos em seus alvos. Os stealers de "token" do Discord, que se prestam a roubar credenciais do serviço de mensagens Discord, são frequentemente utilizados para entregar outros malwares através dos servidores de chat ou pela rede de entrega de conteúdo do Discord. Mas outros grandes stealers, como o Strela, o Raccoon Stealer e a cultuada família do stealer RedLine, são muito mais agressivos para seus alvos, coletando áreas de armazenamento de senhas dos sistemas operacionais e aplicativos, além de cookies de navegadores e outros dados de credenciais. O Raccoon Stealer também já lançou "clippers" de criptomoedas que trocam os endereços de carteiras de criptomoedas copiados para a área de transferência por um endereço de carteira controlado pelo operador do malware.

Principais ladrões por número de relatos únicos de clientes em 2023

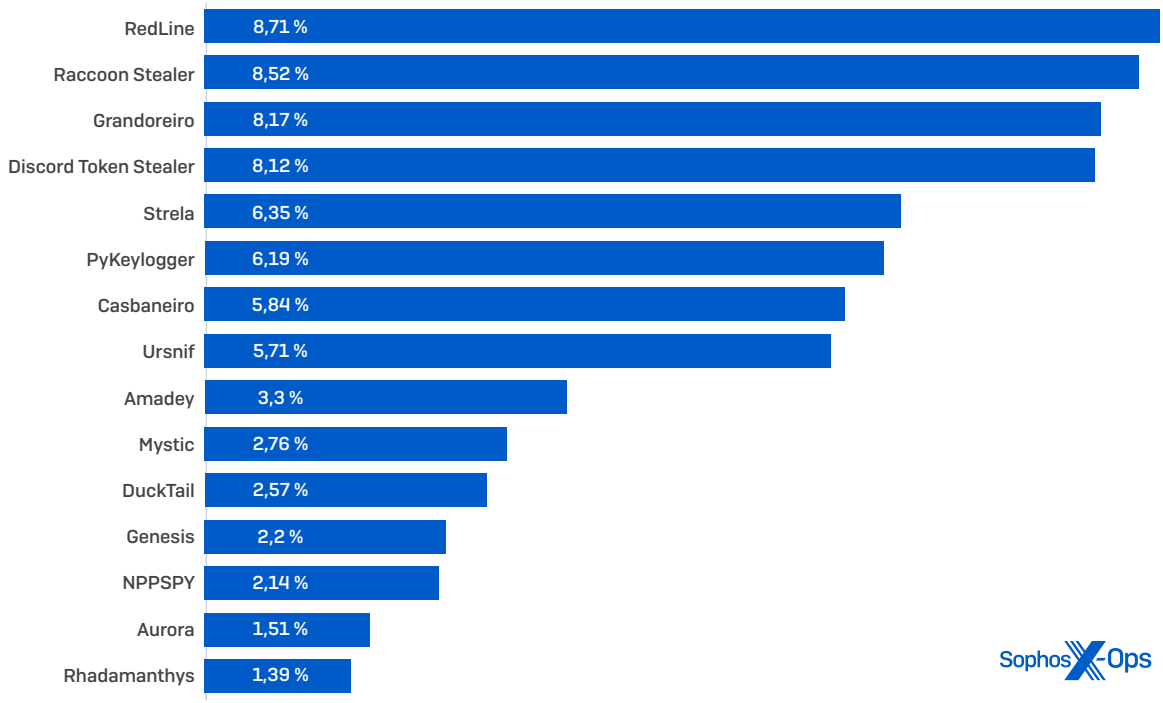


Figura 6: Detecções de malwares ladrões de informações em 2023: dados extraídos da telemetria de clientes da Sophos no dataset do SophosLabs

A Sophos tem observado um aumento no número de malwares ladrões de informações que têm o macOS como alvo, e acreditamos que essa tendência continuará. Esses stealers, alguns dos quais vendidos em fóruns clandestinos e canais do Telegram por até US$ 3.000, podem coletar dados de sistemas, dados de navegadores e carteiras de criptomoedas.

O ransomware continua sendo uma grande ameaça às pequenas empresas

Ainda que o ransomware seja responsável por uma porcentagem relativamente pequena de todas as detecções de malware, ele continua a ser o mais intenso em termos de impacto. Os ransomwares afetam empresas de todos os portes em todos os setores, mas são as pequenas e médias organizações que são atacadas com mais frequência. Em 2021, a Ransomware Task Force do Institute for Security and Technology revelou que 70% dos ataques de ransomware eram direcionados às pequenas empresas. Embora o número de ataques de ransomware tenha variado de ano a ano, nossas métricas destacam o mesmo valor percentual.

O ransomware LockBit foi a ameaça mais predominante nos casos de segurança em pequenas empresas registrados pelo Sophos Incident Response em 2023. O LockBit se enquadra na categoria Ransomware-as-a-Service, entregue por vários afiliados, sendo o ransomware mais implantado de 2022 de acordo com a Figura 7.

Incidentes de ransomware em pequenas empresas atendidos pelo Sophos Incident Response, 2023

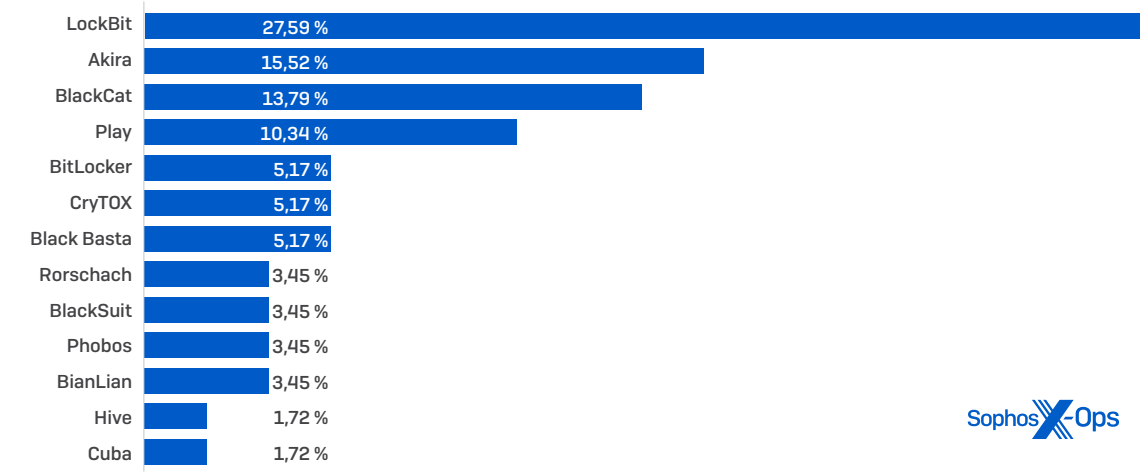


Figura 7: Detalhamento dos agentes de ransomware por trás dos incidentes ocorridos em pequenas empresas e investigados pelo Sophos Incident Response em 2023; esses números refletem o dataset de engajamentos práticos do IR com clientes que, no geral, não tinham proteções da Sophos em vigor

20 principais ransomwares por número de relatos únicos de clientes, 2023

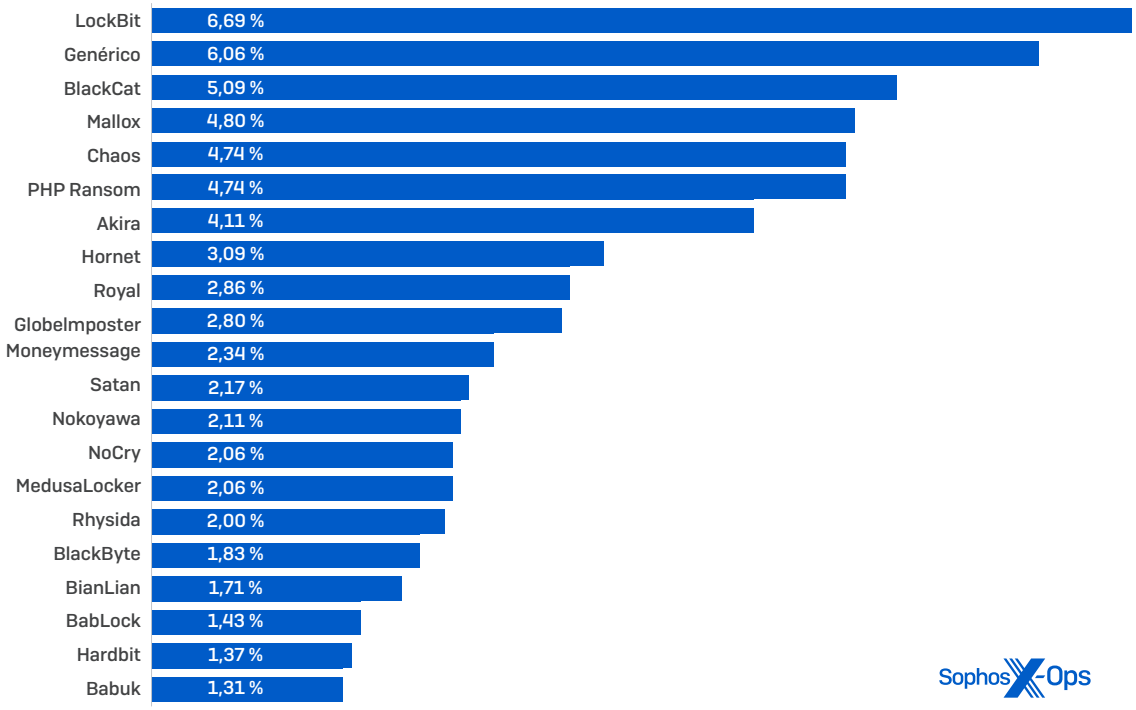


Figura 8: Principais lançamentos de ransomwares detectados por um software de proteção de endpoint da Sophos e presentes no dataset do Labs entre todos os nossos clientes em 2023 como um percentual de todos de ransomwares detectados; "Genérico" representa vários tipos de ransomware detectados com uma assinatura catch-all que não foram detectados sob outras definições

O LockBit foi o malware mais visto pelo grupo de Managed Detection and Response (MDR) da Sophos, que inclui a equipe do Incident Response e seus dados, com quase o triplo de incidentes com tentativa de lançamento de ransomware do que o segundo colocado, o Akira.

Principais malwares observados em 2023 em incidentes atendidos pelo MDR, por número de incidentes

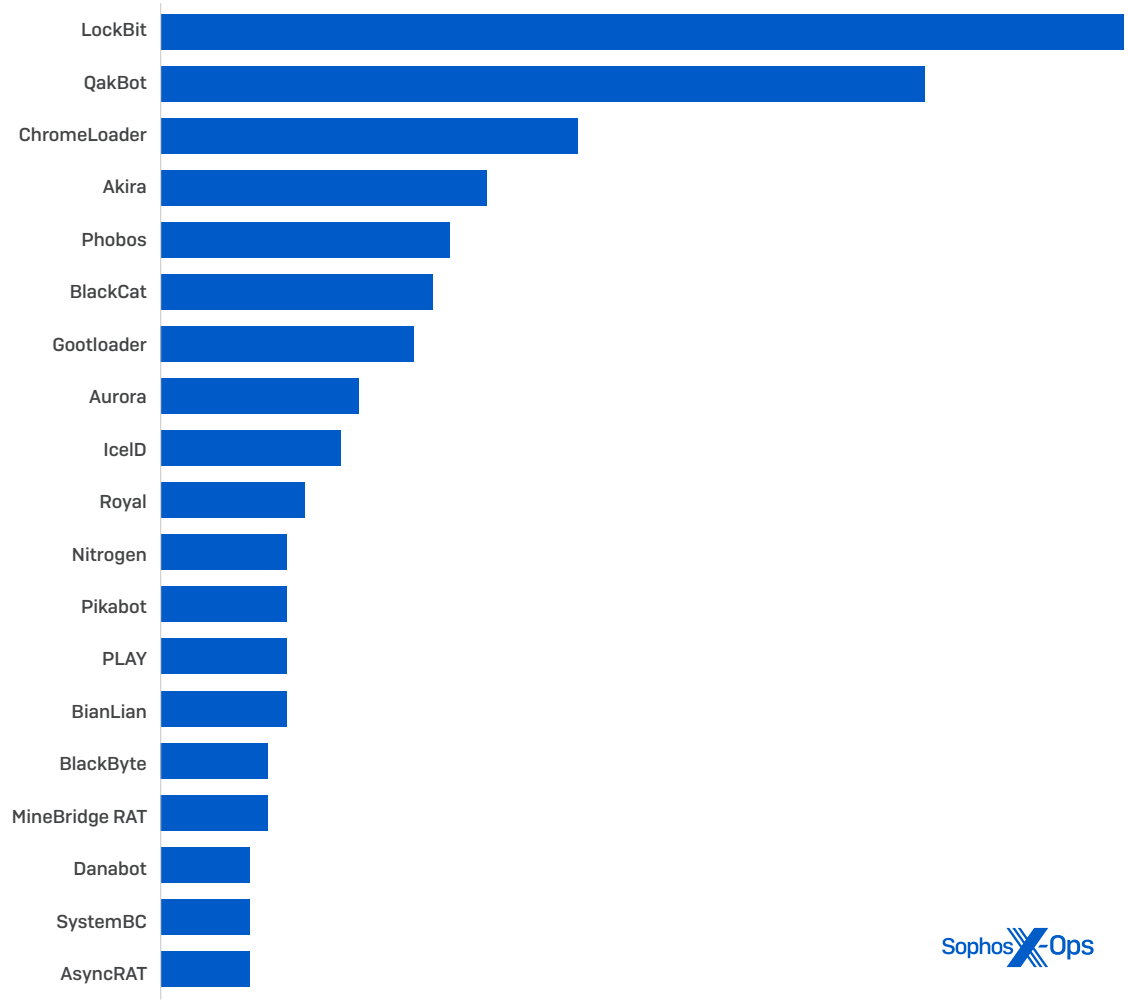


Figura 9: O malware mais frequente observado em incidentes atendidos pelo Sophos Managed Detection and Response em 2023, como visto no dataset do MDR. Observe as diferenças entre este gráfico e o apresentado na Figura 8; apesar da predominância do LockBit em 2023, vemos uma grande variedade de famílias de ransomware que tentaram contaminar os sistemas. Apenas um subconjunto deles progrediu para um estágio que exigisse a assistência prática do MDR. Observe que eles não são exclusivos, ou seja, pode ocorrer mais de uma detecção em um mesmo incidente.

No decorrer de 2023, acompanhamos o aumento na execução remota de ransomwares através do uso de dispositivos não gerenciados na rede das organizações para tentar criptografar arquivos em outros sistemas por meio do acesso a arquivos na rede.

Incidentes de ransomware remotos, 2022-2023

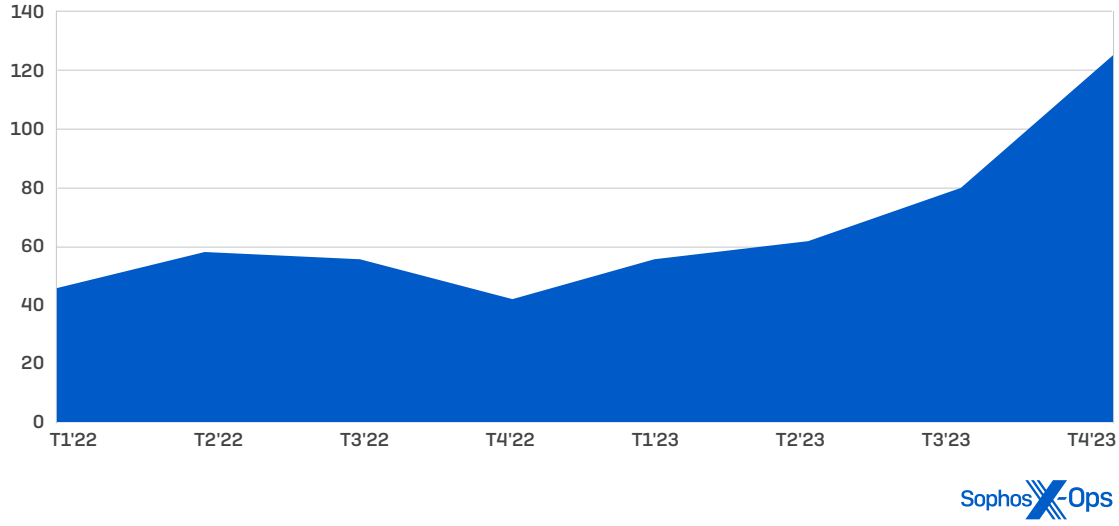


Figura 10: Os últimos dois anos de dados de telemetria coletados dos clientes da Sophos mostram um aumento na proporção de tentativas de ataque de ransomware envolvendo ransomwares remotos — um problema constante que vem adquirindo vida própria, especialmente na segunda metade de 2023

Esses tipos de ataques podem se estabelecer com a exploração de servidores, dispositivos pessoais e dispositivos de rede sem proteção que se conectam às redes baseadas em Windows das organizações. Uma defesa profunda pode evitar que esses ataques coloquem toda uma organização offline, mas, ainda assim, eles podem deixar as organizações vulneráveis à perda e ao roubo de dados.

Os sistemas Windows não são o único alvo que um ransomware busca. Cada vez mais, os desenvolvedores de ransomwares e outros malwares se utilizam de linguagens multiplataforma para criar versões para sistemas operacionais macOS e Linux e plataformas de hardware compatíveis. Em fevereiro de 2023, foi descoberto que uma variante para Linux do ransomware ClOp foi usada em um ataque em dezembro de 2022. Desde então, a Sophos tem observado versões vazadas do ransomware LockBit voltadas para macOS no próprio processador da Apple e Linux em várias plataformas de hardware.

Cybercrime as a Service

O mundo do malware continua a ser dominado pelo que chamamos de "Malware as a Service" (MaaS), que é o uso de estruturas de entrega de malware fornecidas por criminosos cibernéticos a outros criminosos cibernéticos em marketplaces clandestinos. Mas uma combinação de melhorias realizadas nas operações de desarmamento e segurança das plataformas pela indústria e por autoridades legais teve um certo impacto na formação desse cenário MaaS.

Depois de uma década de domínio no ramo de entrega de malware, o Emotet recuou, desde que foi desarmado pela Europol e Eurojust em janeiro de 2021. Em um grau menor, o mesmo aconteceu com o Qakbot e o Trickbot, depois de terem sido desbancados pelas autoridades em agosto de 2023. Mesmo com a volta do Qakbot de forma limitada, ele foi amplamente ultrapassado por seus pretensos sucessores: Pikabot e DarkGate.

Mas nada disso abalou a notoriedade do cultuado cavalo de Troia de acesso remoto AgentTesla, que subiu de posição no mercado de MaaS. Ele foi o malware detectado com mais frequência pela proteção de endpoint em 2023 (à parte dos arquivos maliciosos genéricos .LNK e malwares ofuscados), perfazendo 51% das detecções de estruturas de entrega de malware em nossa telemetria no último ano.

Principais estruturas de entrega de malware por número de relatos únicos de clientes, 2023

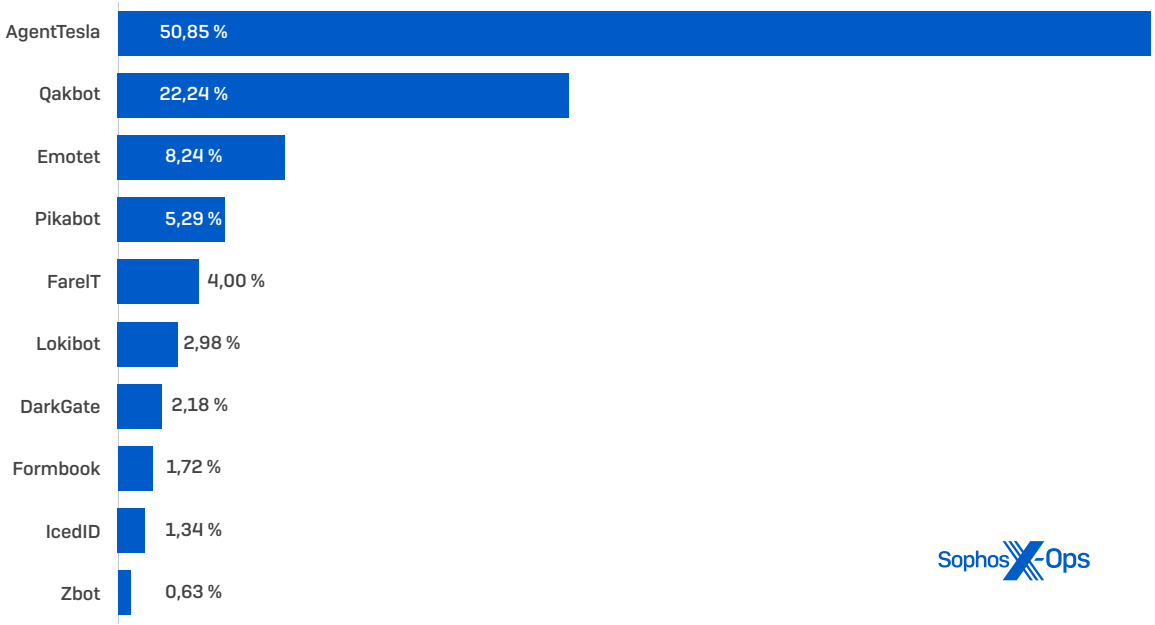


Figura 11: Detalhamento das estruturas comuns utilizadas para entrega de malware pelos invasores com base no número de detecções de endpoint nas redes de clientes protegidos pela Sophos; os números do Qakbot representam detecções antes da ação policial internacional de agosto de 2023 contra sua infraestrutura

Encontrando uma rota de entrega diferente

Os ataques de malware exigem uma forma de acesso inicial. Normalmente, isso envolve um destes meios:

- E-mails de phishing
- Anexos de e-mail maliciosos
- Exploração de vulnerabilidades em sistemas operacionais e aplicativos
- Atualizações falsas de software
- Exploração e abuso do protocolo RDP de acesso remoto
- Roubo de credenciais

Anteriormente, os operadores de MaaS eram bastante dependentes do uso de anexos de e-mail como forma de estabelecer uma base de operações inicial. Mas as mudanças à segurança padrão da plataforma do Microsoft Office impactou o mercado de MaaS. Com as mudanças feitas pela Microsoft aos aplicativos do Office que agora, como padrão, bloqueiam as macros VBA (Visual Basic for Applications) em documentos baixados da Internet, ficou mais difícil para os operadores de MaaS usar esse método preferido de disseminar malwares.

Isso levou a algumas mudanças em relação aos tipos de anexos que os invasores usam — quase que exclusivamente anexos de arquivos PDF. Contudo, há algumas exceções bastante marcantes. No início de 2023, os operadores do Qakbot se voltaram ao uso de documentos maliciosos do OneNote para evitar as mudanças ao Excel e Word, dissimulando em seus documentos links para arquivos de script que eram ativados quando o alvo clicava em um botão em um arquivo de um bloco de anotações do OneNote.

Em 2021, observamos que as ofertas de "malware-as-a-service", como o backdoor Raccoon Stealer, começaram a depender intensamente da entrega pela Web, frequentemente usando truques de otimização de mecanismos de busca (SEO) para ludibriar as vítimas a baixarem seus malwares. Em 2022, vimos o "envenenamento de SEO" sendo usado como parte de uma campanha de roubo de informações do SolarMarker. Esses métodos estão novamente em ascensão, e os agentes por trás deles estão mais sofisticados.

Observamos várias campanhas notáveis utilizando anúncios maliciosos na Web e o envenenamento de SEO para atrair suas vítimas. Uma delas foi a de um grupo que usou um malware que chamamos de "Nitrogen". O grupo usou anúncios no Google e Bing vinculados a palavras-chave específicas para levar suas vítimas a baixar um instalador de software de um site falso usando a identidade visual da marca de um desenvolvedor de software legítimo. A mesma técnica de malvertising foi usada em conexão com vários outros malwares de acesso inicial, incluindo o agente de botnet Pikabot, o ladrão de informações IcedID e as famílias de malware do backdoor Gozi.

No caso do Nitrogen, os anúncios eram direcionados a pessoas com conhecimentos gerais em TI e ofereciam downloads que incluíam softwares desktop remotos bastante conhecidos para suporte a usuários finais e utilitários de transferência de arquivo. Os instaladores executavam o que anunciavam, mas entregavam também um conteúdo em Python que, quando iniciado pelo instalador, trazia com ele um shell remoto do Meterpreter e beacons do Cobalt Strike. Baseado nas descobertas de outros pesquisadores, esse foi, provavelmente, o primeiro passo nos ataques do ransomware BlackCat.

Ferramentas de “uso duplo”

O tão usado Cobalt Strike, que é um kit de software utilizado em “operações de Red Team e simulação de adversários”, continua a servir a adversários reais e também a organizações legítimas de teste de segurança. Mas ele não é o único software desenvolvido comercialmente que é usado pelos invasores — e também deixou de ser o mais comum.

Ferramentas remotas de desktop, ferramentas de compactação de arquivos, softwares de transferência de arquivos comuns, outros utilitários e ferramentas de teste de segurança de código aberto são comumente usados pelos invasores pelo mesmo motivo que são empregados pelas pequenas e médias empresas: facilitar o trabalho.

O Sophos MDR observou esses utilitários, aos quais nos referimos como “ferramentas de uso duplo”, sendo abusados como parte de um processo pós-exploit realizado pelos invasores:

- **Descoberta:** Advanced IP Scanner, NetScan, PCHunter, HRSword
- **Persistência:** Anydesk, ScreenConnect, DWAgent
- **Acesso a credenciais:** Mimikatz, Veeam Credential Dumper, LaZagne
- **Movimento lateral:** PsExec, Impacket, PuTTy
- **Coleta e exfiltração de dados:** FileZilla, WinSCP, megasync, Rclone, WinRar, 7zip

AnyDesk e PsExec também foram observados pelo Sophos MDR em mais incidentes do que o Cobalt Strike, conforme abaixo:

Principais ferramentas de “uso duplo” observadas em 2023 em incidentes atendidos pelo MDR, por número de incidentes

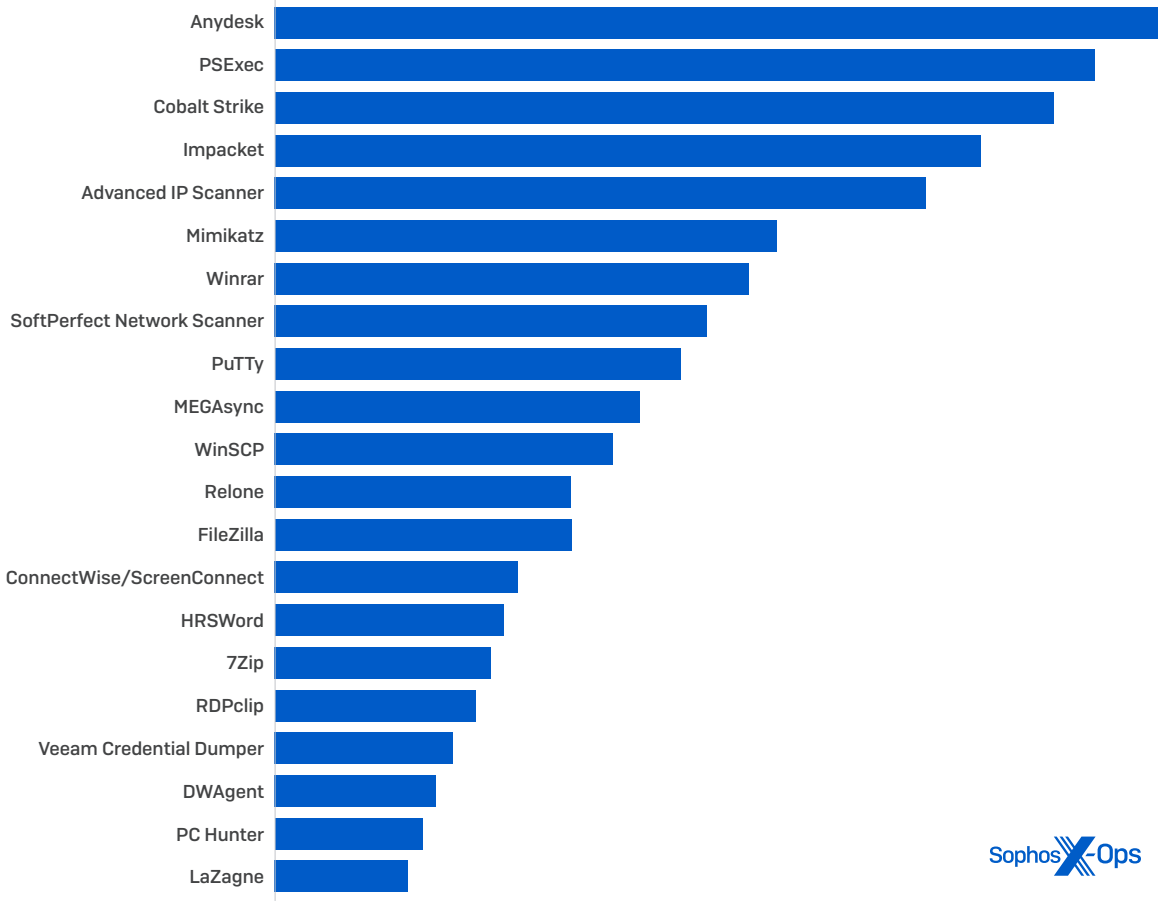


Figura 12: Ferramentas de “uso duplo” encontradas com mais frequência nos incidentes de segurança cibernética, baseado no número de casos em que cada uma delas foi observada no dataset do Sophos MDR

Ataques de dia zero e outros ataques

Em maio de 2023, a Progress Software relatou vulnerabilidades na plataforma de proteção de transferência de arquivos gerenciada e amplamente utilizada pela empresa, o MOVEit — incluindo uma vulnerabilidade que foi explorada por, pelo menos, um grupo de agentes mal-intencionados. Em consequência disso, a empresa descobriu outras vulnerabilidades e lançou vários patches para corrigi-las.

Os ataques foram atribuídos a agentes associados à gangue do ransomware Cl0p. Os invasores utilizaram a vulnerabilidade para implantar Web shells nas interfaces da Web voltadas ao público para os servidores do MOVEit Transfer — Web shells que, em determinados casos, persistiram após a correção das vulnerabilidades com patches lançados pela Progress para os seus clientes.

O MOVEit foi apenas uma das várias vulnerabilidades de "dia zero" que desafiaram as equipes de defesa em 2023. O GoAnywhere, outro sistema gerenciado de transferência de arquivo, divulgou uma vulnerabilidade em fevereiro que outro grupo afiliado ao CL0p tentou explorar. Além dessas, outra vulnerabilidade de execução de código remoto nos produtos de software do servidor de impressão PaperCut MF e NG foi explorada pela gangue do ransomware Bl00dy em março e abril, após informado aos desenvolvedores em janeiro.

Em alguns casos, essas vulnerabilidades simplesmente não podem ser corrigidas. Por exemplo, uma vulnerabilidade encontrada em junho nos dispositivos do Barracuda Email Security Gateway foi tão grave que não foi possível aplicar patches e exigiu a substituição total dos dispositivos físicos e virtuais, mas um grupo criminoso chinês continuou a explorar os dispositivos vulneráveis até o fim de 2023.

As vulnerabilidades em softwares e dispositivos não precisam ser novas para os golpistas se aproveitarem da ocasião. Os agentes de ameaças procuram como alvo softwares cujo suporte esteja prestes a expirar — como é o caso de firewalls de rede antigos e softwares de servidores Web —, sabendo que não haverá patches para eles.

Ataques a cadeias de suprimentos e malwares assinados digitalmente

As pequenas empesas também precisam se preocupar com a segurança dos serviços que utilizam para gerenciar seus negócios e sua infraestrutura de TI. Os ataques a cadeias de suprimentos não são apenas para agentes de estados-nações. Temos observado os ataques contra provedores de serviços gerenciados se tornarem parte integral do playbook dos ransomwares.

Em 2023, a equipe do Sophos MDR respondeu a cinco casos nos quais clientes de pequenas empresas foram atacados através de um exploit no software RMM de monitoramento e gerenciamento remoto de um provedor de serviços. Os golpistas usaram o agente RMM NetSolutions em execução nos computadores dessas organizações para criar novas contas administrativas nas redes visadas e depois implementaram ferramentas comerciais de desktop remoto, exploração de rede e implantação de software. Em dois desses casos, os golpistas implantaram o ransomware LockBit com sucesso.

É difícil se defender contra ataques que utilizam softwares confiáveis, especialmente quando o software dá aos golpistas a capacidade de desativar a proteção de endpoint. Pequenas empresas e provedores de serviços que contam com esses softwares devem se manter vigilantes para o caso de alertas indicarem que a proteção de endpoint foi desativada em seus sistemas na rede, pois isso pode ser um sinal de que o invasor obteve acesso privilegiado a uma cadeia de suprimentos através de uma vulnerabilidade — ou por meio de outro software que, à primeira vista, parecia ser legítimo.

Por exemplo, em 2023, observamos, em diversas ocasiões, invasores usando drivers kernel vulneráveis, tanto de softwares mais antigos que ainda tinham assinaturas digitais válidas como de softwares maliciosos criados especialmente e que usavam assinaturas digitais obtidas de forma fraudulenta, incluindo drivers kernel maliciosos assinados digitalmente através do programa de compatibilidade de hardware do Windows (WHCP) da Microsoft, para escapar da detecção por ferramentas de segurança e executar um código que desabilitasse a proteção contra malwares.

Os drivers kernel funcionam em um nível bastante baixo no sistema operacional e são normalmente carregados antes dos outros softwares durante a inicialização do sistema operacional. Isso significa que, muitas vezes, eles são executados antes do software de segurança ser iniciado. Podemos dizer que as assinaturas digitais funcionam como uma carteira de habilitação: desde o Windows 10 versão 1607, os drivers kernel precisam ter uma assinatura digital válida em todas as versões do Windows, ou eles não são carregados pelos sistemas operacionais Windows com Secure Boot habilitado.

Em dezembro de 2022, a Sophos notificou a Microsoft sobre a descoberta de drivers kernel maliciosos que transportavam certificados assinados da Microsoft. Como esses drivers tinham certificados assinados da Microsoft, eles eram aceitos por padrão como softwares benignos, permitindo que fossem instalados — para depois desativar as proteções de endpoint nos sistemas em que estavam instalados. A Microsoft emitiu um comunicado de segurança e, em julho de 2023, revogou um rol de certificados de drivers maliciosos que foram obtidos através do WHCP.

Os drivers não precisam ser maliciosos para serem explorados. Vimos muitos casos de drivers e outras bibliotecas de versões antigas de softwares, e também de versões atuais, em que os invasores os utilizaram para carregar clandestinamente o malware na memória do sistema.

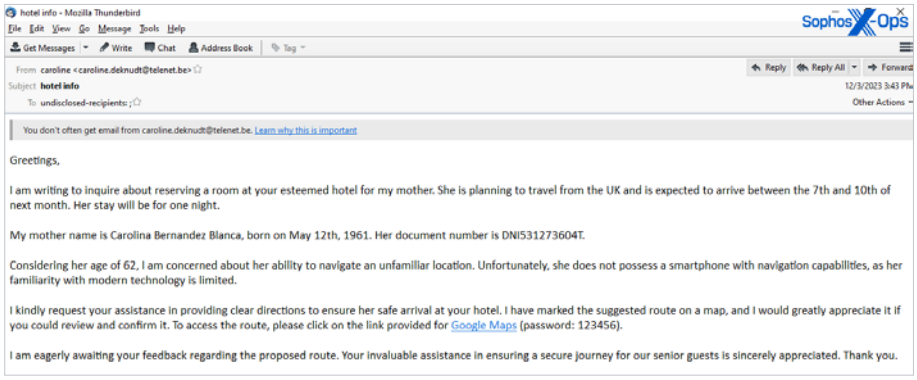
Também observamos drivers da própria Microsoft usados nos ataques. A versão vulnerável de um driver do utilitário Process Explorer da Microsoft foi utilizada várias vezes por operadores de ransomware para tentar desativar produtos de proteção de endpoint. Em abril de 2023, informamos sobre uma ferramenta chamada "AuKill" que usava esse driver em vários ataques na tentativa de implantar o Medusa Locker e o ransomware LockBit.

Às vezes temos sorte de encontrar os drivers vulneráveis antes que eles possam ser explorados. Em julho, as regras de comportamento da Sophos eram disparadas pela atividade de um driver de um produto de segurança de outra empresa. O alerta foi disparado pelo teste de simulação de invasão do próprio cliente, mas nossa investigação sobre o evento descobriu três vulnerabilidades que foram relatadas para o fornecedor do software e posteriormente corrigidas.

Spammers rompem as barreiras da engenharia social

O e-mail se tornou um método ultrapassado de comunicação na era do bate-papo com criptografia de ponta a ponta, mas os spammers não parecem ter se dado conta (ou se importar com isso). O tradicional método BEC de simplesmente se fazer passar por um funcionário e pedir a um funcionário legítimo que envie vales-presentes persiste, mas os spammers também ficaram mais criativos.

No ano passado, a equipe de segurança de mensagens da Sophos se deparou com uma série de novos truques e técnicas de engenharia social projetados para burlar os controles de e-mail convencionais. Mensagens em que os golpistas enviam um anexo ou um link em um e-mail sem mais nem menos estão no passado: quanto mais eficiente for o spammer, maior será a probabilidade de iniciar uma conversa para então avançar e dar o bote nos próximos e-mails.


hotel info - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From caroline <caroline.deknudt@telenet.be>

Subject hotel info

To undisclosed-recipients:;

Reply Reply All Forward

12/3/2023 3:43 PM

Other Actions

You don't often get email from caroline.deknudt@telenet.be. Learn why this is important

Greetings,

I am writing to inquire about reserving a room at your esteemed hotel for my mother. She is planning to travel from the UK and is expected to arrive between the 7th and 10th of next month. Her stay will be for one night.

My mother name is Carolina Bernandez Blanca, born on May 12th, 1961. Her document number is DNI531273604T.

Considering her age of 62, I am concerned about her ability to navigate an unfamiliar location. Unfortunately, she does not possess a smartphone with navigation capabilities, as her familiarity with modern technology is limited.

I kindly request your assistance in providing clear directions to ensure her safe arrival at your hotel. I have marked the suggested route on a map, and I would greatly appreciate it if you could review and confirm it. To access the route, please click on the link provided for Google Maps (password: 123456).

I am eagerly awaiting your feedback regarding the proposed route. Your invaluable assistance in ensuring a secure journey for our senior guests is sincerely appreciated. Thank you.

Figura 13: Apenas depois de receber uma resposta da vítima é que o spammer envia um e-mail para ela com um link para um arquivo malicioso dentro de um arquivo Zip protegido por senha

Observamos essa metodologia nos ataques em que os spammers se passavam por entregadores de uma firma e ligavam para os clientes das empresas pedindo-lhes que abrissem um e-mail minado. Em 2023, registramos ataques direcionados a diferentes setores em que spammers enviavam um e-mail inicial solicitando uma transação comercial ou fazendo uma queixa, que era seguido por um link para baixar um arquivo minado disfarçado após a empresa responder ao primeiro e-mail.

A prevenção convencional contra spam envolve processos que inspecionam o conteúdo das mensagens e tomam as decisões com base nesse conteúdo. Os spammers jogam com diferentes métodos para substituir o conteúdo de texto em suas mensagens por imagens incorporadas: alguns fazem com que as imagens pareçam ser uma mensagem escrita, enquanto outros utilizam gravuras e códigos QR que parecem ser faturas (com números de telefone que os golpistas incitam as vítimas a ligar) como forma de escapar da detecção.

Figura 14: Anexo em PDF em um spam que incorpora uma miniatura fora de foco e ilegível de uma fatura de cobrança e um link para um site que hospeda um conteúdo malicioso

Também os anexos maliciosos estão retomando o seu espaço, com PDFs minados voltando à cena para se vincular a sites ou scripts mal-intencionados e, às vezes, usando códigos QR incorporados. A família do malware Qakbot abusou ostensivamente do formato de documento do OneNote da Microsoft, o bloco de anotações (ou arquivo .one), na entrega de cargas antes de encerrar suas atividades mais tarde em uma ação de desarmamento coordenada. Os invasores também se aproveitaram do formato de arquivo MSIX — um tipo de formato de arquivamento usado pela Microsoft para distribuir aplicativos através do Windows App Store — como forma de escapar da detecção.

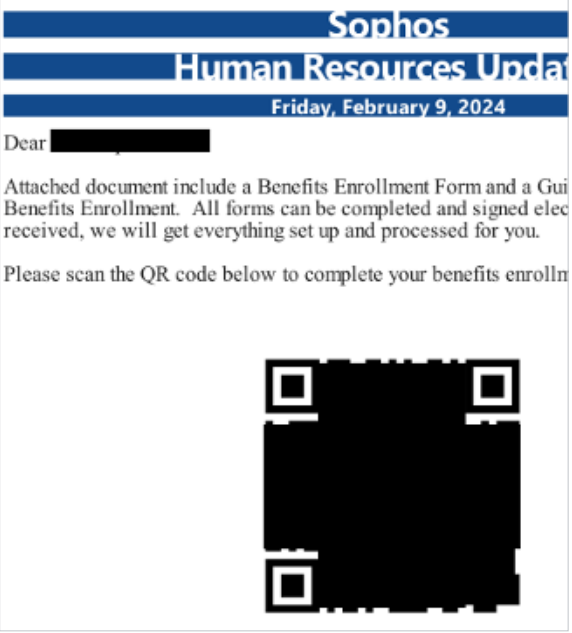

Sophos
Human Resources Updat
Friday, February 9, 2024
Dear [redacted]
Attached document include a Benefits Enrollment Form and a Gui
Benefits Enrollment. All forms can be completed and signed elec
received, we will get everything set up and processed for you.
Please scan the QR code below to complete your benefits enrolln

Figure 15: Um anexo de PDF malicioso enviado por e-mail aos funcionários da Sophos e que incorpora a imagem de um código QR que leva a uma página de phishing

Os invasores também abusaram dos serviços da Microsoft: no fim do ano, cerca de 15% do total de spam que a Sophos bloqueou foram enviados usando contas de e-mail criadas no sistema de mensagens onmicrosoft.com da Microsoft orientado a corporações.

Ameaças por engenharia social e malwares móveis

As pequenas empresas dependem muito de dispositivos móveis como parte de seus sistemas de informações aprovados ou ad-hoc. Mensagens de texto, aplicativos de mensagens ou comunicação, e aplicativos conectados a serviços de nuvem, incluindo aplicativos móveis de pontos de vendas, são sistemas imprescindíveis para as pequenas empresas distribuídas. Os criminosos cibernéticos sabem disso e continuam a encontrar formas de direcionar seus ataques aos usuários de dispositivos móveis para obter acesso a dados ou defraudá-los.

Spywares e "bankers" são um grupo de malwares de Android particularmente preocupante, o qual acreditamos que continuará a ser uma ameaça. Spywares são usados para coletar dados de telefones, chegando, às vezes, a cadastrar o usuário em serviços com números premium para obter ganhos monetários diretos. Eles coletam dados pessoais, incluindo mensagens de texto SMS e logs de chamadas dos dispositivos afetados que, posteriormente, são vendidos a golpistas ou usados para chantagem, ou ambos. Já houve casos em que as vítimas chegaram a cometer suicídio por causa das ameaças recebidas de operadores de spyware.

Esses aplicativos móveis maliciosos são distribuídos de diferentes formas. Eles se disfarçam de aplicativos genuínos na loja de aplicativos Google Play ou em lojas de terceiros, geralmente como aplicativos móveis de empréstimo financeiro. Também se disseminam através de links enviados por mensagem de texto.

Os bankers são malwares que focam em aplicativos financeiros, incluindo carteiras de criptomoeda, para coletar dados de contas e obter fundos, usando permissões de acessibilidade para obter acesso a dados confidenciais em aparelhos de telefone.

Temos ainda o fenômeno do "abate de porcos", ou sha zhu pan. Começamos rastreando aplicativos falsos em plataformas iOS e Android vinculadas a alguma forma de golpe que inicialmente chamamos de "CryptoRom" no início de 2021. Desde então, os golpes ficaram mais sofisticados.

As quadrilhas que executam esses golpes — geralmente operados de "escritórios" com "funcionários" que foram sequestrados por facções do crime organizado — já se apossaram de bilhões de dólares de vítimas de todo o mundo, e, geralmente, se concentram nas pessoas vinculadas a pequenas empresas. Em 2023, um pequeno banco em Kansas faliu e foi confiscado pelo FDIC depois do CEO do banco enviar mais de US$ 12 milhões em depósitos para golpistas na intenção de reaver os fundos perdidos em uma dessas transações fraudulentas. Esse exemplo trágico mostra como um golpe normalmente associado à vida privada de um indivíduo pode ter ramificações e impactar as pequenas empresas.

Os golpistas do sha zhu pan atraem suas vítimas através de sites de redes sociais, aplicativos de relacionamento e outros aplicativos e plataformas de comunidades e até por meio de mensagens de texto "descuidadas". Eles costumam se concentrar em indivíduos que buscam relacionamentos amorosos ou amizade. Após levar a vítima para um aplicativo de mensagens seguro, como o WhatsApp ou Telegram, conquistam sua confiança e incutem nela a ideia de fazer dinheiro através de canais sobre os quais eles garantem ter conhecimentos privilegiados e que, geralmente, envolve criptomoedas.

No último ano, observamos aplicativos falsos usados nesses golpes se infiltrando nas lojas de aplicativos Google Play e iOS. Eles ludibriam as avaliações de segurança das lojas como sendo aplicativos do bem até que o processo de avaliação termine; depois mudam seu conteúdo remoto e se transformam em apps falsos de transações de criptomoedas. Qualquer depósito realizado através desses apps é imediatamente embolsado pelos golpistas.

Recentemente, observamos esses golpes adotando uma tática de outro golpe de criptomoeda que não exigia aplicativos falsos — em vez disso, usavam a funcionalidade "Web3" dos aplicativos móveis de carteiras de criptomoedas para entrar diretamente nas carteiras criadas pelas vítimas. Identificamos centenas de domínios associados a essas variantes de "mineração DeFi (Decentralized Finance)" do sha zhu pan, e como fazemos com os aplicativos falsos que identificamos, continuamos a denunciá-los e a trabalhar arduamente para desarmá-los.

Conclusões

O que não falta para as pequenas empresas são ameaças, e a sofisticação dessas ameaças quase sempre se equipara à daquelas usadas em ataques a grandes corporações e órgãos do governo. Ainda que a quantidade de dinheiro possível de ser roubada seja menor do que a disponível nas grandes organizações, os criminosos ficam satisfeitos em roubar o que você tem e compensar essa diferença no volume.

Os grupos criminosos esperam que as pequenas empresas sejam menos seguras e utilizem ferramentas não tão modernas e sofisticadas para proteger seus usuários e ativos. A chave para se defender com sucesso contra essas ameaças é provar a eles que essas suposições estão erradas: eduque os seus funcionários, implante a autenticação multifator em todos os seus recursos de acesso externo, aplique patches nos servidores e dispositivos de rede com prioridade máxima, e considere a possibilidade de migrar os seus recursos de gerenciamento mais complexo, como os servidores Microsoft Exchange, para plataformas de e-mail SaaS.

Com base em nossa experiência, a maior diferença entre as empresas que foram mais afetadas pelos ataques cibernéticos e as que foram menos afetadas está no tempo de resposta. Ter especialistas em segurança a postos 24 horas para monitoramento e resposta é o mínimo para uma defesa eficaz em 2024. Manter-se protegido não é impossível, apenas exige um bom planejamento e defesa em camadas para você ganhar tempo na hora de responder e minimizar os danos.

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

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

24-04-11 PTBR (NP)

SOPHOS