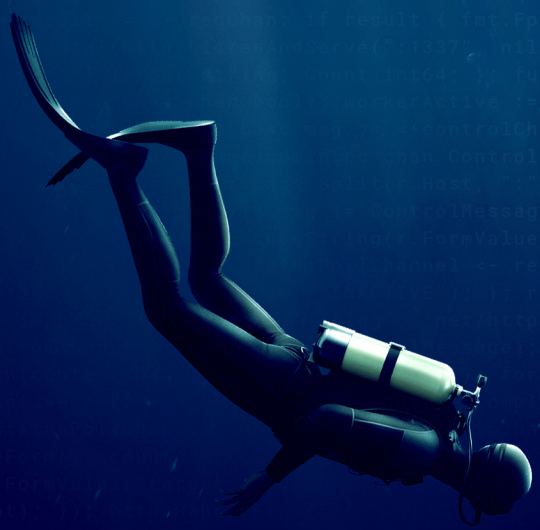


Rota de ataque

Análise aprofundada sobre tráfego de DNS mal-intencionado

Akamai

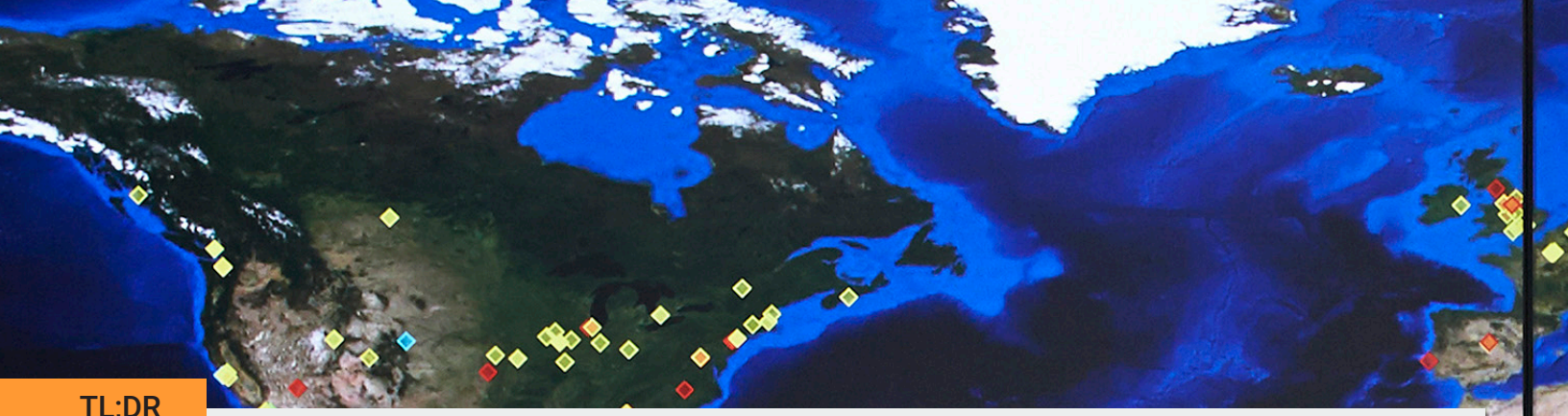
Sumário

Servidores de nomes de domínio – uma via para tráfego de ataque

O DNS (Sistema de Nomes de Domínio) é uma parte essencial da infraestrutura da Internet desde seus primórdios. Grande parte do uso da Internet, seja em casa ou no trabalho, deve ser facilitado pelo DNS para que possamos navegar corretamente até o nosso destino na World Wide Web. Não é novidade que os invasores geralmente optam por aproveitar essa infraestrutura para facilitar os ataques, seja uma ameaça que acesse servidores de comando e controle (C2) para aguardar comandos ou uma execução remota de código que chegue a um domínio para baixar arquivos maliciosos em uma máquina. Devido a essa onipresença, o DNS se tornou uma parte importante da infraestrutura de ataque.

Sendo uma empresa de segurança, a Akamai tem posição estratégica que nos permite examinar e proteger as empresas, bem como os usuários domésticos, contra tráfego DNS mal-intencionado que pode levar ao comprometimento do sistema e roubo de informações. Neste relatório, forneceremos uma análise do tráfego mal-intencionado direcionado a usuários domésticos e empresas em todo o mundo. Uma análise completa do tráfego DNS mal-intencionado, que inclui correlação com grupos ou ferramentas de invasores, pode armar as organizações com informações importantes sobre as ameaças mais prevalentes para elas. Dessa forma, essas informações podem ajudar os profissionais de segurança a analisar a postura de defesa e realizar avaliações de lacunas para conhecer as técnicas e metodologias utilizadas contra eles. Deixar de fazer isso pode resultar em violações que levam a perdas de dados confidenciais, perdas financeiras ou multas por violações de conformidade. Com a expectativa de que os custos dos crimes cibernéticos aumentem para US$ 10,5 trilhões anualmente até 2025, as organizações devem estar preparadas antes mesmo de ocorrerem ataques.

Ao analisarmos o tráfego DNS mal-intencionado de usuários corporativos e domésticos, conseguimos detectar vários surtos e campanhas no processo, como a disseminação do FluBot, um malware baseado em Android que se move de um país para outro em todo o mundo, bem como a prevalência de vários grupos de cibercriminosos voltados para empresas. Talvez o melhor exemplo seja a presença significativa de tráfego de C2 relacionado aos IABs (brokers de acesso inicial) que violam as redes corporativas e monetizam o acesso, vendendo para outros, como os gripos de RaaS (ransomware como um serviço). Essas atividades são visíveis para nós na rodovia da informação que é o DNS, e estamos compartilhando-as para benefício de nossos leitores.



TL;DR

De acordo com nossos dados, entre 10% e 16% das organizações encontraram tráfego de C2 nas redes em um determinado trimestre. A presença de tráfego de C2 indica a possibilidade de um ataque ou uma violação em andamento, e as ameaças variam de botnets de roubo de informações a IABs.

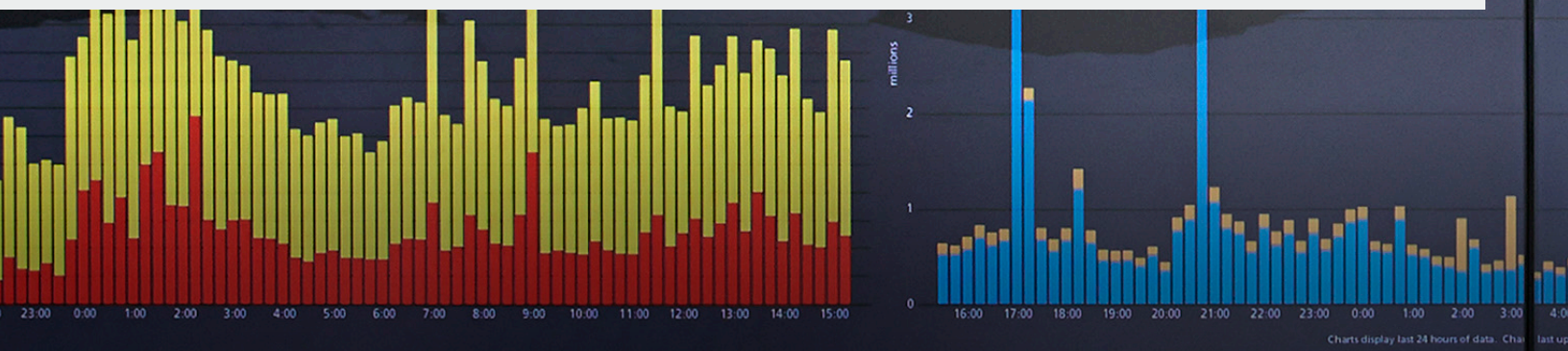
26% dos dispositivos afetados entraram em contato com domínios de C2 conhecidos de IABs (brokers de acesso inicial), incluindo domínios relacionados a Emotet e QakBot. Os IABs apresentam um grande risco para as organizações, pois a principal função deles é fazer a violação inicial e vender o acesso a grupos de ransomware e outros cibercriminosos.

Dispositivos NAS (armazenamento de rede anexados) são mais vulneráveis, pois têm menos probabilidade de receber patches e contêm muitos dados valiosos. Nossos dados mostram que os invasores estão abusando desses dispositivos por meio do QSnatch, com 36% dos dispositivos afetados em redes corporativas acessando domínios C2 relacionados a essa ameaça.

30% das organizações afetadas estão no setor de fabricação (duas vezes mais do que a segunda maior vertical) e destacam as implicações reais dos ataques cibernéticos, como problemas na cadeia de suprimentos e interrupções na vida cotidiana. Regulamentações como Segurança de rede e informações 2 (NIS2) podem ajudar a combater ataques contra setores essenciais ou infraestrutura crucial, como fabricação.

Os ataques a redes domésticas estão buscando violar não apenas dispositivos tradicionais, como computadores, mas também celulares e dispositivos de IoT (Internet das Coisas). Uma quantidade significativa de tráfego de ataque pode ser correlacionada a malware de celulares e botnets de Internet das coisas.

Com base em nossa análise de dados de DNS, notamos um crescente surto de malware FluBot na Europa, Oriente Médio e África (EMEA); América Latina (LATAM); e Ásia-Pacífico e Japão (APJ). As táticas de engenharia social de malware e o uso delas em vários idiomas da União Europeia (UE) podem ser alguns dos fatores que contribuem para o aumento da infecção.



Terminologia da análise de tráfego DNS da Akamai

O Akamai Edge DNS e a infraestrutura de DNS observam até 7 trilhões de solicitações de DNS diariamente. Para proteger usuários e empresas, a Akamai bloqueia solicitações que levam a domínios que servem malware ou websites que possam roubar suas informações. Examinar essas transações DNS mal-intencionadas também nos permite classificar esses domínios em três categorias (malware, websites de phishing e C2) e conduzir uma análise detalhada para determinar as maiores ameaças atuais às empresas e aos usuários domésticos.

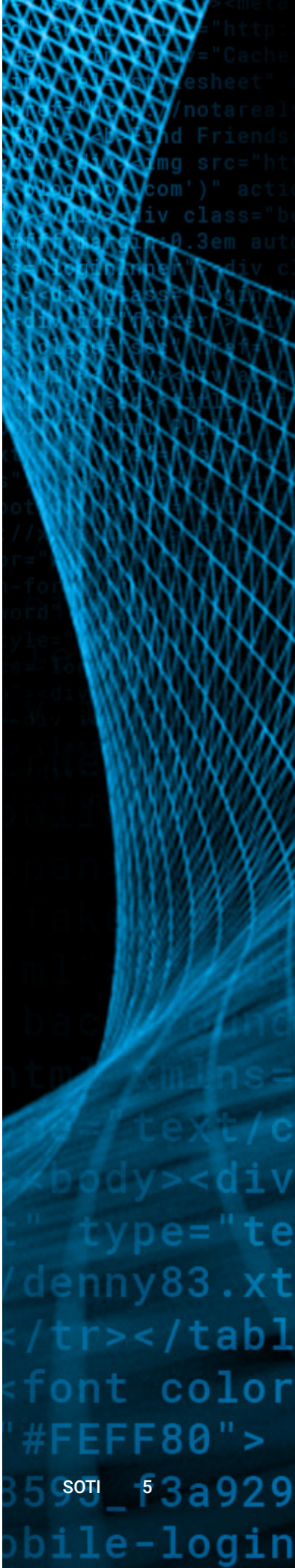
A partir de uma amostragem cuidadosa de dados de tráfego de DNS mal-intencionado, podemos tirar conclusões significativas sobre as ameaças mais predominantes. Nossa proteção abrange duas demografias: uma demografia consiste nas empresas nas quais a Akamai protege redes corporativas e a outra consiste nos usuários domésticos que acessam a internet em suas redes pessoais e estão sendo expostos a ameaças como botnets que visam assumir o controle de dispositivos para fins nefastos, como ganho financeiro por meio de criptomineração.

Primeiro, vamos definir os termos *websites de phishing*, *malware* e *C2* e explicar como são usados neste relatório.

Websites de phishing são domínios vinculados a kits de phishing que imitam e clonam a aparência de empresas de varejo, bancos, empresas de alta tecnologia e outros para enganar usuários e induzi-los a divulgar informações como credenciais e informações de identificação pessoal (PII). A Akamai observa esse tráfego via DNS para proteger usuários corporativos e domésticos contra roubo de identidade e perda de informações.

Malware é um domínio mal-intencionado (ou domínios) que serve ou contém arquivos mal-intencionados. Essa categoria também contém websites que hospedam JavaScript mal-intencionado e websites comprometidos que exibem anúncios indesejados ou redirecionam usuários para uma página que contém esses anúncios. Muitos ataques modernos exigem o download de um arquivo mal-intencionado para um dispositivo a partir de uma fonte externa para a execução de sua carga útil ou para o download do próximo estágio de um ataque em andamento. Observar e bloquear esse tráfego pode ajudar a proteger uma organização contra uma infecção inicial ou ataque contínuo.

C2, no contexto da nossa análise de tráfego de DNS, é um domínio usado para se comunicar com os dispositivos infectados para enviar comandos e controlar o dispositivo. Após o comprometimento inicial, os invasores estabelecem comunicações com C2 entre o sistema infectado e um servidor controlado pelos invasores para enviar comandos adicionais, como o download e a disseminação de outros malwares, a exfiltração de dados e o desligamento e a reinicialização do sistema, entre outros para comprometer ainda mais a segurança do sistema ou da rede. Detectar tráfego de C2 é crucial, pois sinaliza um ataque contínuo que ainda pode ser mitigado. Além disso, o bloqueio dos domínios associados a servidores C2 impede que as comunicações com C2 sejam estabelecidas e evita que o malware baixe instruções ou comandos adicionais, reduzindo as chances de invasores executarem atividades mal-intencionadas em sua rede.



Perigo à frente: a onipresença de tráfego mal-intencionado nas organizações

Com base na análise da Akamai de tráfego de DNS, podemos ver que 13% dos dispositivos tentaram acessar pelo menos uma vez domínios associados a malware no quarto trimestre de 2022 (Figura 1). Além disso, 6% se comunicaram com domínios relacionados a phishing. Na área de C2, na qual nos concentraremos fortemente neste relatório, observamos uma tendência crescente ao longo do ano, com uma ligeira diminuição no quarto trimestre.

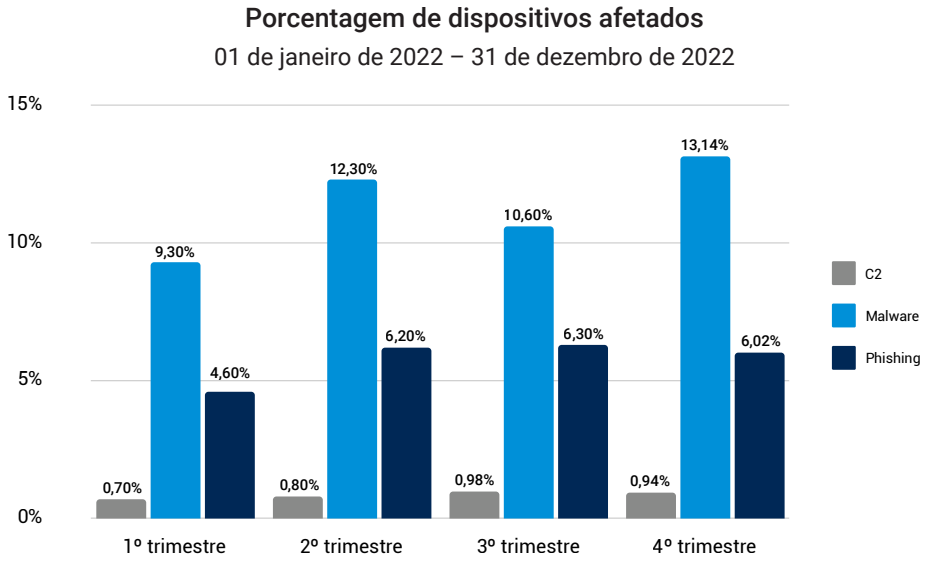


Fig. 1: Vemos uma tendência crescente de dispositivos protegidos que atingem destinos mal-intencionados

Observe que a Figura 1 refere-se apenas a dispositivos individuais que tentaram se comunicar com domínios mal-intencionados. É importante destacar a disparidade entre dispositivos que chegam a destinos de malware (que podem ser usados por invasores para baixar malware) e dispositivos que chegam a domínios de C2 (que geralmente são usados durante um ataque contínuo para facilitar a comunicação entre o invasor e o malware e podem ser usados para baixar malware adicional para um ciclo de ataque). Essa disparidade pode ser indicativa das diferenças entre as investidas de infiltração da rede, que podem ser bloqueadas na primeira tentativa de baixar malware em uma máquina, e infiltração bem-sucedida (que, em nossos dados, pode não ter percorrido o DNS) ou ataques contínuos, que podem entrar em contato com um domínio de C2 para executar o ataque.

Esse relatório se concentrará principalmente no tráfego de C2 como um indicador potencial de uma instância quando um invasor tiver pousado com êxito em um dispositivo. Para que possamos entender a prevalência desses ataques, precisamos analisar os dados usando uma lente diferente. Em vez de olhar para dispositivos individuais, podemos agregar os dados por organização para examinar a frequência com que um ataque contínuo (indicado pela existência de tráfego de C2) aparece dentro do conjunto de dados.

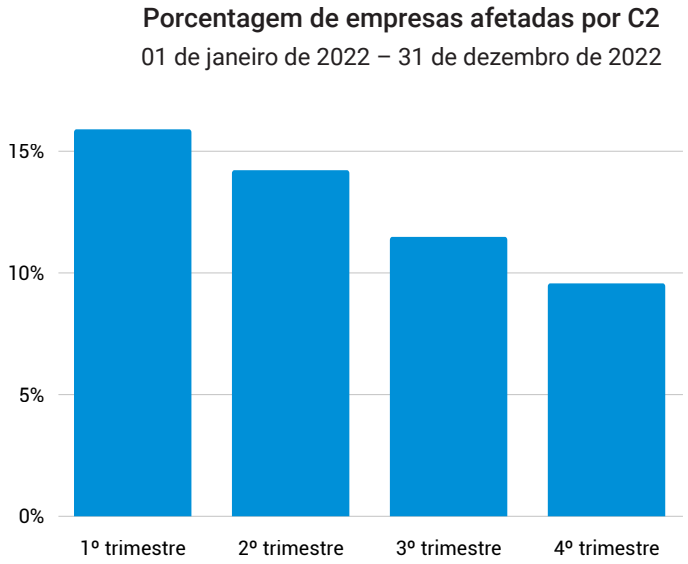


Fig. 2: Uma análise do tráfego de C2 mal-intencionado mostra a porcentagem de organizações que tiveram pelo menos um dispositivo atingindo um domínio de C2 ao longo do ano

> **De acordo com nossos dados de DNS, entre 10% e 16% das organizações tiveram pelo menos uma instância em que o tráfego de C2 foi observado saindo da rede, em um determinado trimestre.**

De acordo com nossos dados de DNS, entre 10% e 16% das organizações tiveram pelo menos uma instância em que o tráfego de C2 foi observado saindo da rede, em um determinado trimestre (Figura 2). Isso pode ser indicativo de malware tentando se comunicar com um operador e é um possível sinal de violação. Esse tráfego de C2 foi bloqueado por nossa solução e não chegou ao seu destino, mas ataques bem-sucedidos podem ter resultado na exfiltração de dados, ataques de ransomware e muito mais.
A partir do primeiro semestre de 2022, foram detectadas 2,3 bilhões de variedades de malware, com média de 1.501 por dia. Nossa pesquisa destaca a eficácia de aproveitar o DNS para impedir que o malware progrida em uma rede ou cause danos.

Os brokers de acesso inicial representam uma ameaça predominante para as organizações

Os ataques de vários estágios se tornaram um elemento básico do cenário moderno de ataques (Figura 3). Os invasores estão obtendo mais sucesso quando conseguem trabalhar em conjunto (ou contratar uns aos outros) ou quando conseguem combinar várias ferramentas em um único ataque. O C2 é fundamental para o sucesso desses ataques. Eles podem ser usados não apenas para comunicação, mas também para facilitar o download de uma carga útil e o malware do próximo estágio para avançar o ataque. Isso é melhor exemplificado pela cadeia de ataques de ransomware Emotet/TrickBot/Ryuk observada nos últimos anos. O Emotet primeiro se infiltra na rede da vítima e, uma vez estabelecido o acesso inicial, entra em contato com um domínio para baixar a carga útil do TrickBot para obter dados pessoais, credenciais e muito mais. Se a vítima for considerada um alvo de alto valor para os invasores, o malware chega até os servidores de C2 e baixa a carga final: Ransomware Ryuk.

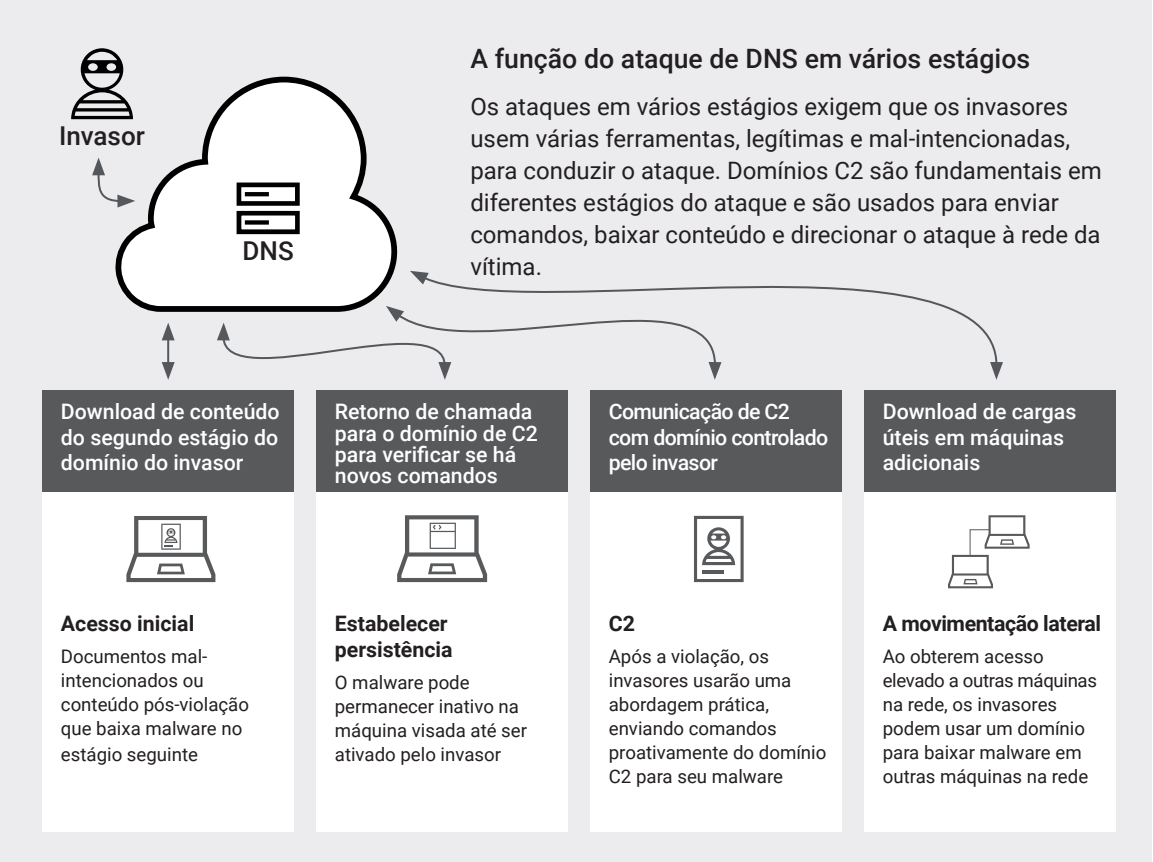


Fig. 3: A função de C2 em cada estágio do ataque

É importante considerar essa cadeia de eventos ao avaliar as informações neste relatório. A comunicação com C2 pode ocorrer em vários estágios do ataque. Nossa recente análise da metodologia de grupos de ransomware modernos, como o grupo Conti, mostrou que invasores sofisticados geralmente designam operadores para trabalhar "com acesso prático" e progredir de forma rápida e eficiente em um ataque. A capacidade de visualizar e bloquear o tráfego de C2 pode ser fundamental para interromper um ataque em andamento.

Os domínios de C2 que observamos podem ser categorizados em domínios com e sem atribuição a uma família de ameaças ou a um grupo de invasores específico. Nesta seção, vamos nos aprofundar em domínios de C2 associados a um tipo de ameaça e ajudar os leitores a avaliar o nível de risco de acordo com as capacidades e metodologias de cada grupo. Observe que algumas dessas famílias de malware podem se adequar a vários casos de uso, dependendo de como os invasores as utilizam durante um ataque.

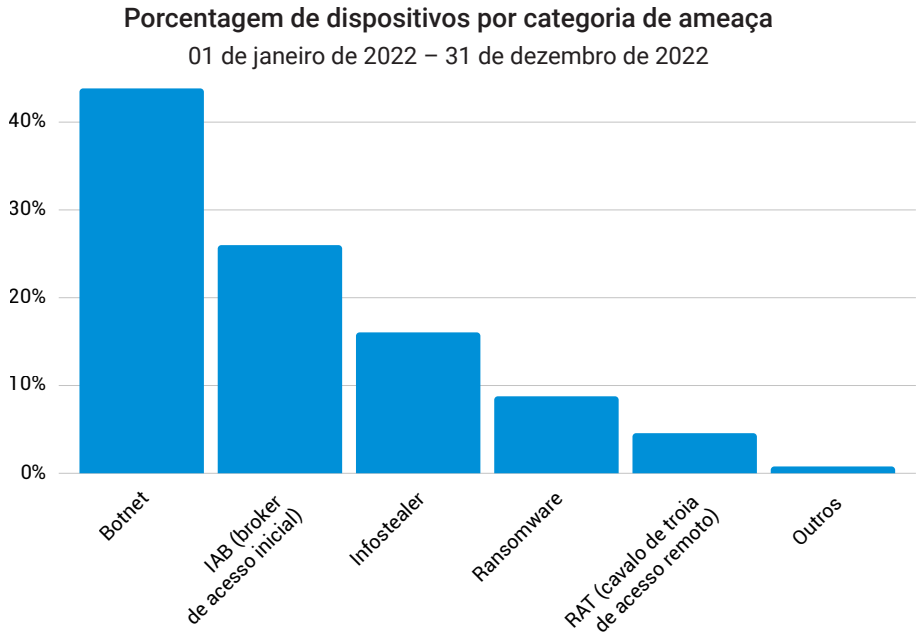


Fig.4: As empresas são predominantemente visadas por botnets, seguido por IABs e infostealers

Na Figura 4, os grupos de invasores são classificados em grupos IABs, botnets e RaaS. Nossas descobertas de dados revelam que os IABs representam uma das maiores ameaças às redes corporativas, assim como botnets destinados à exfiltração de dados.

Brokers de acesso inicial
Os IABs se concentram principalmente em fornecer um ponto de entrada inicial para outros cibercriminosos, incluindo grupos de ransomware, para ganhar espaço nas redes das organizações. persistência, execução remota da carga após invasão e exfiltração de dados.

Grupos de ransomware como um serviço
São grupos que permitem que outros invasores (mesmo aqueles sem experiência técnica) se tornem afiliados e usem o software de ransomware por uma taxa.

Botnets
Os invasores podem usar botnets para uma infinidade de propósitos, desde ataques de criptomineração e DDoS até exfiltração de dados, implantação de malware e movimento lateral.

Ladrões de informações
Os ladrões de informações coletam vários tipos de dados como nomes de usuário, senhas, informações do sistema, credenciais bancárias, cookies e assim por diante.

Observamos também ransomware, ferramentas de acesso remoto (RATs) e infostealers. Todos esses grupos têm um papel fundamental em vários estágios de ataque. E com ferramentas prontamente disponíveis nas camadas para invasores novatos e cibercriminosos experientes que permitem que eles tenham acesso inicial, permaneçam ocultos na rede e promovam o ataque, as organizações estão mais suscetíveis do que nunca a crimes cibernéticos. À medida que explicarmos esses agrupamentos, também estabeleceremos as interseções nas quais eles operam e as possíveis implicações e impactos nas organizações.

Grupos de brokers de acesso inicial

Apelidada de "brokers de acesso inicial" (IABs), essa classe específica de cibercriminosos se concentra principalmente em fornecer um ponto de entrada inicial para que outros cibercriminosos e invasores consigam entrar nas redes das organizações. Embora vários grupos de cibercriminosos tenham metodologias de violação semelhantes, como explorar vulnerabilidades relacionadas a RDP e a VPN, usar ataques de força bruta, coletar descartes de credenciais e enviar e-mails de phishing com malware, os IABs se especializam em obter acesso a esses sistemas infectados e em vender esse acesso a outros grupos de invasores, em vez de executar todo o ataque. Grupos de ransomware por trás de LockBit, Darkside, Conti e BlackByte, entre outros, supostamente usaram IABs como parte de suas operações. Uma pesquisa de 2023 observou que o preço médio de venda para acesso inicial é de aproximadamente US$ 2.800.

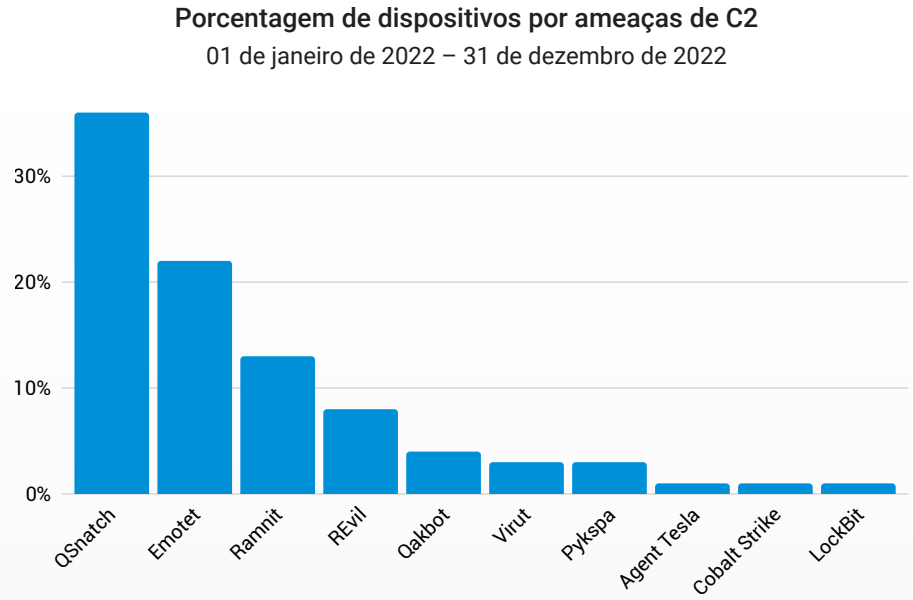
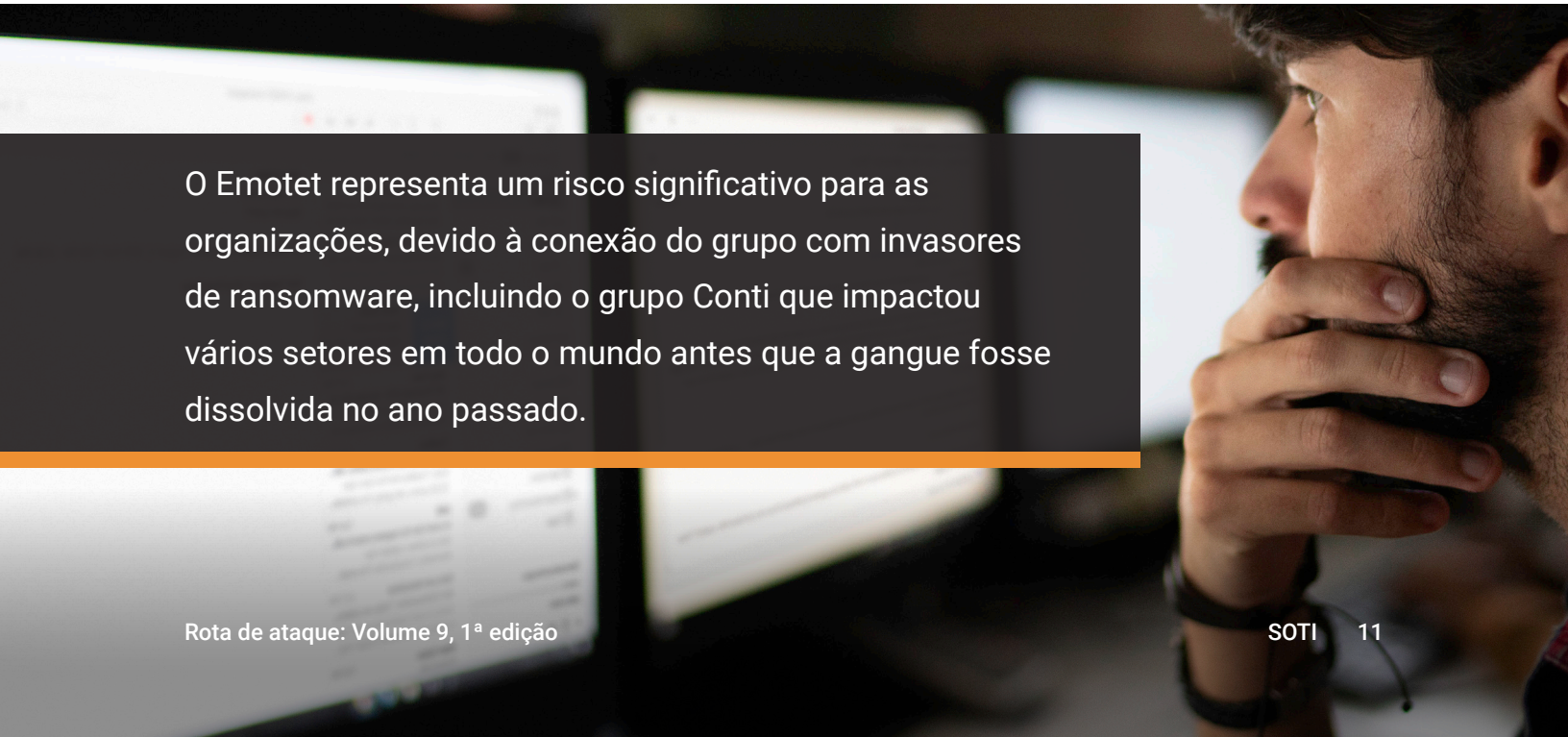


Fig. 5: QSnatch, Emotet e Ramnit são as principais famílias de C2 vistas no tráfego de rede corporativa

Com base em nossos dados de DNS (Figura 5), 26% dos dispositivos infectados atingiram domínios relacionados a IABs, como Qakbot (4% dos dispositivos infectados) e Emotet (22% dos dispositivos infectados). Os IABs desempenham um papel importante no modelo de negócios de RaaS e no cenário de crime cibernético. Os invasores de ransomware e os cibercriminosos precisam de acesso remoto e credenciais não apenas para se infiltrar nas redes de suas vítimas, mas também para se mover lateralmente, estabelecer persistência e obter privilégios de acesso, entre outras atividades. Os invasores aproveitam os IABs para realizar tarefas demoradas de reconhecimento, verificação de alvos em potencial e infecção inicial. O acesso prontamente disponível vendido na clandestinidade elimina essa etapa e reduz o nível de experiência ou o tempo necessário para os invasores lançarem um ataque. Como tal, introduz uma infinidade de possíveis ataques contra as organizações-alvo pretendidas, resultando em ransomware, roubo de informações confidenciais e sigilosas, espionagem e violações de dados.

O Emotet surge como um dos IABs mais proeminentes em nossos dados. O Emotet representa um risco significativo para as organizações devido à conexão do grupo com invasores de ransomware, incluindo o grupo Conti que afetou vários setores em todo o mundo antes de ser dissolvido no ano passado. Ao longo dos anos, o Emotet adicionou mais módulos, como DDoS (negação de serviço distribuída) e recursos de roubo de e-mail, e expandiu as metas pretendidas. De um cavalo de troia/botnet bancário com uma infinidade de funcionalidades, o Emotet se transformou em um MaaS (malware como um serviço), distribuindo ameaças como o cavalo de troia bancário IcedID, TrickBot e o ransomware UmbreCrypt. Observou-se também que o grupo TrickBot usa o Emotet para distribuir várias variedades de ransomware, incluindo Ryuk, ProLock e Conti, entre outras. Uma visão mais detalhada das técnicas usadas por Emotet pode ser encontrada na estrutura MITRE ATT&CK sobre o tópico.



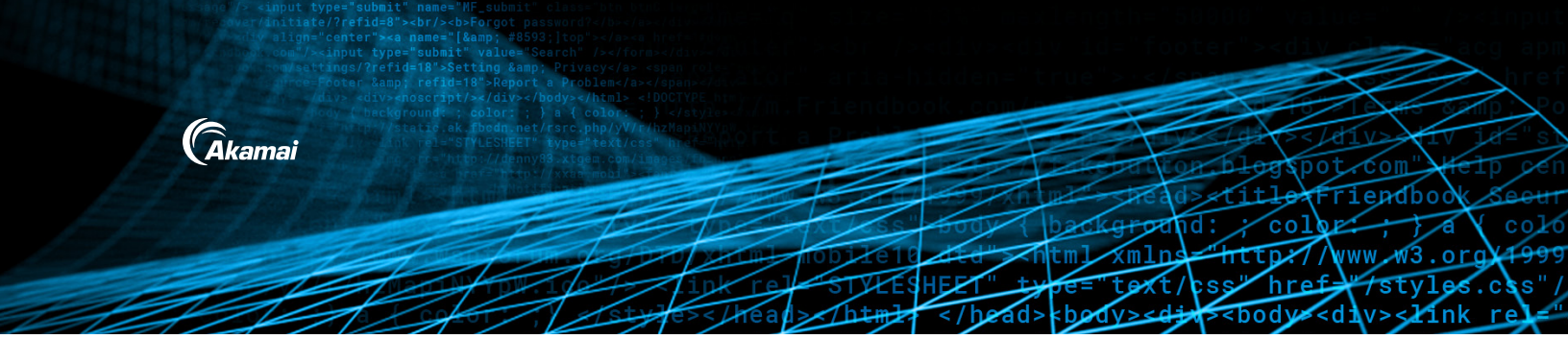
O Emotet representa um risco significativo para as organizações, devido à conexão do grupo com invasores de ransomware, incluindo o grupo Conti que impactou vários setores em todo o mundo antes que a gangue fosse dissolvida no ano passado.

O segundo IAB mais proeminente nos dados é o Qakbot. Esse grupo é conhecido por ter colaborado com o grupo de ransomware Black Basta que supostamente afetou pelo menos 50 organizações de várias partes do mundo. A equipe da Qakbot é conhecida pelos recursos de roubo de informações e por fornecer malware em segundo estágio para comprometer ainda mais a segurança do sistema. De acordo com a pesquisa, o Qakbot aproveita o Cobalt Strike, uma ferramenta legítima de pentesting usada por equipes vermelhas e usada indevidamente por adversários, para realizar uma série de atividades maliciosas após a invasão e facilitar um backdoor em um ambiente da vítima. Esta é uma técnica cada vez mais usada pelos IABs nos últimos anos. A estrutura MITRE ATT&CK pode fornecer inteligência adicional relacionada às técnicas utilizadas pelo Qakbot durante o ataque.

Grupos de botnet

Em nossa análise, os botnets formam o maior agrupamento de tipos de ameaças em 44% do tráfego de C2 analisado. Uma grande variedade de invasores é representada nesse agrupamento, e é essencial lembrar que nem todos os botnets são criados da mesma forma. As variantes mais benignas podem plantar criptomineradores ou aproveitar a máquina da vítima para conduzir ataques DDoS. Embora representem um custo por si só, os botnets que encontramos nas empresas podem ser usados para exfiltração de dados e ataques em vários estágios, o que pode representar um risco mais significativo. Os botnets podem se espalhar lateralmente na rede e podem ser usados para implantar ransomware, como no caso do TrickBot. Ou podem se concentrar especificamente no roubo de informações e na coleta de credenciais.

Descobrimos que o QSnatch, o maior botnet presente em ambientes empresariais, faz exatamente isso: exfiltração de dados de dispositivos conectados à rede. De acordo com nossos dados, o QSnatch foi responsável por 36% dos dispositivos infectados. Esse malware visa especificamente o QNAP, um tipo de dispositivo NAS usado para backups ou armazenamento de arquivos pelas empresas. Embora o método de infecção ainda seja desconhecido, os pesquisadores supõem que o QSnatch pode infectar por meio da exploração de vulnerabilidades de firmware ou ataques de força bruta em dispositivos com um nome de usuário/senha padrão. É altamente recomendável que as empresas que usam a QNAP mantenham o firmware atualizado (uma vez infetado, o QSnatch impedirá a instalação de patches e desativará os produtos de segurança) e alterem as senhas padrão imediatamente. O QSnatch é usado por invasores para fazer captura de credenciais, registro de senhas, acesso remoto e exfiltração de dados, para citar alguns. Os invasores podem estar atacando dispositivos de armazenamento, pois eles contêm trunfos de informações valiosas, e o comprometimento desses dispositivos deixa as empresas sem backups em caso de ataques de ransomware. Detalhes sobre táticas e contramedidas são destacados neste alerta de CISA.



Grupo de ransomware como um serviço

Em nossa análise do tráfego de DNS, 9% dos dispositivos infectados que chegaram a famílias de C2 acessaram domínios associados aos grupos de RaaS. Esse tipo de grupo de cibercriminosos permite que outros invasores (mesmo sem a experiência técnica) se tornem uma de suas afiliadas e usem o software de ransomware por uma taxa. As organizações atingidas por ransomware enfrentam inúmeras consequências que não se limitam à perda de dados confidenciais da empresa. As empresas podem lidar com custos de correção e recuperação, honorários advocatícios, multas, tempo de inatividade resultando em perda de produtividade e danos à marca e à reputação. A CyberSecurity Ventures opinou que o custo dos ataques de ransomware seria de aproximadamente US$ 265 bilhões por ano até 2031. O relatório global de ransomware da Akamai também destaca os impactos incapacitantes do ransomware que vão além das perdas financeiras, como a interrupção da cadeia de suprimentos, e, em alguns casos, o ransomware pode ser uma questão de vida ou morte.

Um grupo prolífico de RaaS é a gangue REvil que se tornou notória por ter como alvo um fornecedor de gerenciamento de TI em um ataque à cadeia de suprimentos que afetou mais de 1.500 provedores de serviços gerenciados. As operações deles cessaram com a detenção de vários membros pelo governo russo. No entanto, alguns meses após a dissolução, os pesquisadores de segurança observaram que o website de vazamento do REvil estava novamente ativo com informações de suas últimas vítimas, incluindo algumas universidades nos Estados Unidos. Os pesquisadores especularam que pode não ser a mesma gangue REvil que está executando esta campanha e advertiram contra estados-nação que afirmam ser o grupo REvil, a fim de esconder seus rastros. Em termos de táticas, o REvil é conhecido por customizar o fluxo de ataque, dependendo das vítimas pretendidas, o que exemplificou o nível de conhecimento que o grupo tem de seus alvos. Para saber mais sobre táticas, técnicas e procedimentos relacionados ao REvil, leia a publicação do MITRE.

> **Os invasores podem estar atacando dispositivos de armazenamento, pois eles contêm trunfos de informações valiosas, e o comprometimento desses dispositivos deixa as empresas sem backups em caso de ataques de ransomware.**

Outro grupo de RaaS que observamos em nosso exame do tráfego de DNS é o LockBit. Após o "desaparecimento" do Conti, o grupo LockBit tornou-se um dos provedores de RaaS mais ativos. Antes disso (de novembro de 2019 a março de 2022), era o RaaS com maior número de organizações vitimizadas após o Conti, de acordo com este relatório.

A gangue LockBit se orgulha de ter um mecanismo de criptografia mais rápido do que outros grupos de RaaS e alega ter impactado mais de 12.000 empresas com o LockBit 2.0. Em junho de 2022, o grupo lançou o LockBit 3.0, com funcionalidades adicionais, incluindo um programa de recompensa por bugs. Eles também supostamente usaram a vulnerabilidade Log4j para obter acesso inicial aos alvos, destacando a importância da aplicação de patches. As organizações que não solucionaram essas falhas de segurança podem correr o risco maior de serem infectadas com o LockBit. O LockBit continua a se reinventar. Uma adição recente é a tática de extorsão tripla na qual eles criptografam arquivos, os publicam em websites de vazamento e lançam ataques DDoS se as vítimas se recusarem a pagar o resgate.

As ferramentas necessárias

As ferramentas identificadas nesta seção podem desempenhar um papel específico em um ataque, seja por violação do sistema, obtenção de informações ou aumento de privilégios. O arsenal que vimos de vários grupos de invasores geralmente requer comunicação para operar como ladrões de informações e RATs. Entender essas ferramentas, juntamente com as táticas usadas pelos grupos de invasores, pode ajudar os profissionais de segurança a entender como os ataques ocorrem e planejar adequadamente.

Infostealers

Projetado para obter vários tipos de dados, como nomes de usuário, senhas, informações do sistema, credenciais bancárias e cookies, entre outros, os ladrões de informações continuam sendo uma das ofertas de MaaS frequentemente usadas em ataques. Os invasores que podem não ter o conhecimento técnico e/ou as habilidades podem simplesmente adquirir infostealers a um custo relativamente baixo e lançar os próprios ataques.

Na lista de famílias de malware de C2, observamos 16% dos dispositivos que acessaram a atribuição conhecida de C2 entrando em contato com os infostealers. O Ramnit (13% dos dispositivos infectados) não é apenas outro ladrão comum de informações. A força dele reside na alta capacidade modular, permitindo que os invasores aproveitem as diversas funcionalidades, como roubar outros dados confidenciais e baixar/implantar outros malwares para atingir sua meta final ou continuar o ataque. Em 2021, o Ramnit foi considerado o maior cavalo de troia bancário, com notícias recentes citando como outro malware compartilhou código semelhante com o Ramnit.

A presença de infostealers em sua rede é um sinal de aviso de que as credenciais de seu usuário podem estar em risco. As informações roubadas coletadas podem ser vendidas nos mercados paralelos e usadas para obter acesso inicial por outros invasores. Os grupos de ransomware podem implantar um infostealer por phishing ou botnets para obter credenciais válidas, alugar uma licença de acesso a um infostealer em um fórum clandestino que ofereça MaaS ou comprar acesso à rede por meio de IABs. Em alguns casos, os operadores de infostealer podem se tornar IABs e vender credenciais de alto valor coletadas (como acesso VPN ou RDP) para os maiores concorrentes ou outros agentes de ameaça que poderiam lançar um ataque muito mais sofisticado.

Ferramentas de acesso remoto

O Cobalt Strike tem sido usado exaustivamente por vários grupos de invasores como parte de suas operações. Há vários meios pelos quais esse poderoso RAT está sendo utilizado pelos invasores, incluindo reconhecimento, escalonamento de privilégios, movimento lateral pela rede, estabelecimento de persistência, execução remota de carga após invasão (como ransomware) e exfiltração de dados. Embora a ferramenta seja usada principalmente após a violação para movimento lateral e exfiltração, ela também é capaz de ser o vetor de acesso inicial, pois tem um módulo spear-phishing. Os grupos conhecidos por usar essa ferramenta são Conti, Qakbot, TrickBot e Emotet, para citar alguns. Para ajudar na detecção do Cobalt Strike em um ambiente, esse conjunto de regras da YARA foi criado para determinar o uso mal-intencionado da ferramenta.

Nossos dados também mostram a presença de tráfego de C2 do Agent Tesla. Esse RAT está sendo vendido no mercado paralelo e seu preço acessível e sua facilidade de uso tornam essa ferramenta atraente para os cibercriminosos. Os invasores podem usar essa ferramenta para coletar credenciais de vários navegadores, capturar pressionamentos de teclas e capturas de tela e executar keylogging. Uma das táticas notáveis dele é a captura de formas, permitindo que os invasores coletem PII e outras informações confidenciais. Essas informações roubadas podem ser usadas para roubo de identidade ou fraude. A PCrisk publicou mais detalhes sobre as técnicas do Agent Tesla e como isso impacta os usuários afetados.

O cenário de atividades mostra campanhas esporádicas de malware ao longo do ano

Ao longo de um ano, vimos flutuações nas atividades de malware de C2 (Figura 6). Caso em foco: O Emotet parece estar particularmente ativo em janeiro e fevereiro de 2022, após seu ressurgimento em novembro de 2021. Esse impulso na atividade demonstra uma campanha formidável para ajudar a recuperar o status dele após meses de inatividade. Nos meses seguintes ao regresso, o Emotet aprimorou as próprias táticas, incluindo formas de contornar a mudança da Microsoft para desativar as macros do Visual Basic for Applications. Alguns relatórios indicam que o Emotet se tornou inativo novamente entre julho e novembro de 2022; nossas observações de dados demonstram um declínio no tráfego de C2 em julho, conforme observado na menor porcentagem de dispositivos infectados que atingem os domínios do Emotet. Isso pode indicar que o grupo permaneceu ativo ao longo do ano, ou pode ser um caso de malware instalado que ainda está se comunicando com uma infraestrutura desatualizada. As observações em 2023 podem nos ajudar a determinar se o grupo Emotet realmente ficou inativo.

Porcentagem mensal de dispositivos por principais ameaças de C2

janeiro de 2022 – dezembro de 2022

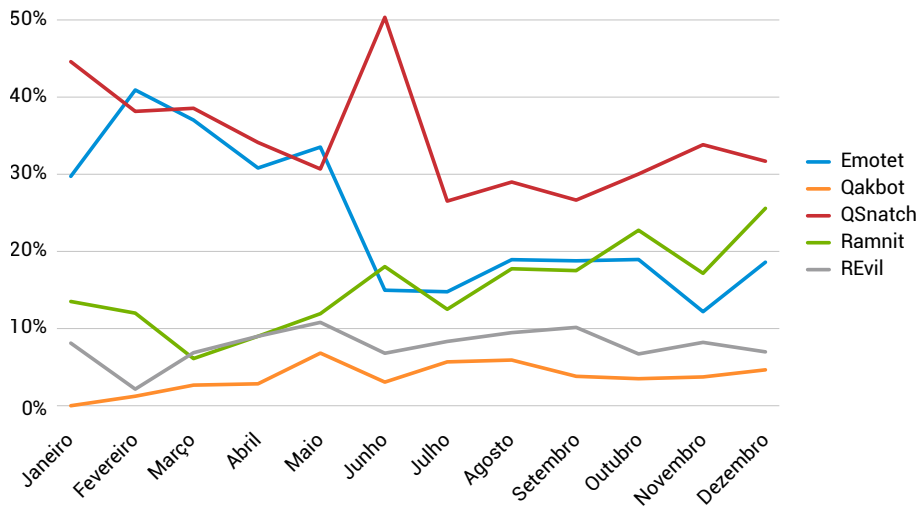


Fig. 6: O gráfico de tendências mensais mostra que o QSnatch esteve consistentemente ativo ao longo de 2022

> **O Emotet parece estar particularmente ativo por volta de janeiro e fevereiro de 2022, após seu ressurgimento em novembro de 2021. Esse impulso na atividade demonstra uma campanha formidável para ajudar a recuperar o status dele após meses de inatividade.**

O QSnatch está sempre ativo ao longo do ano, atingindo o pico em junho, mostrando a predominância dessa ameaça. Os servidores NAS são alvos viáveis para invasores por vários motivos: primeiro, eles contêm dados confidenciais; segundo, há menos probabilidade dos servidores NAS serem corrigidos; e, terceiro, esses dispositivos são potencialmente mais acessíveis na rede organizacional e podem servir como um hub para a movimentação lateral. Embora haja mudanças nos últimos anos, como a adição de soluções de segurança integradas, os cibercriminosos as contornaram desativando produtos de segurança instalados e/ou impedindo que os dispositivos sejam atualizados com novas correções. Dessa forma, esses dispositivos permanecem vulneráveis contra novas ameaças desse malware.

Também vemos o número crescente de Ramnit nas redes corporativas de agosto a dezembro. Isso é preocupante, pois esse malware pode roubar uma grande variedade de informações confidenciais que os invasores poderiam vender posteriormente a outros agentes de ameaça para ataques futuros.

QSnatch e Emotet: ameaças comuns entre todas as regiões

Para determinar as ameaças predominantes por região, examinamos a porcentagem de dispositivos da região individual que atingem domínios de C2 (Figura 7). Cada porcentagem é relativa ao número de dispositivos afetados por região, que também difere dependendo da região. Curiosamente, estamos vendo tendências de ataque semelhantes em todas as regiões, embora com poucos outliers. Portanto, recomendamos que cada região siga as recomendações fornecidas na seção "conclusão e recomendações" ou em cada grupo de malware nas seções acima.

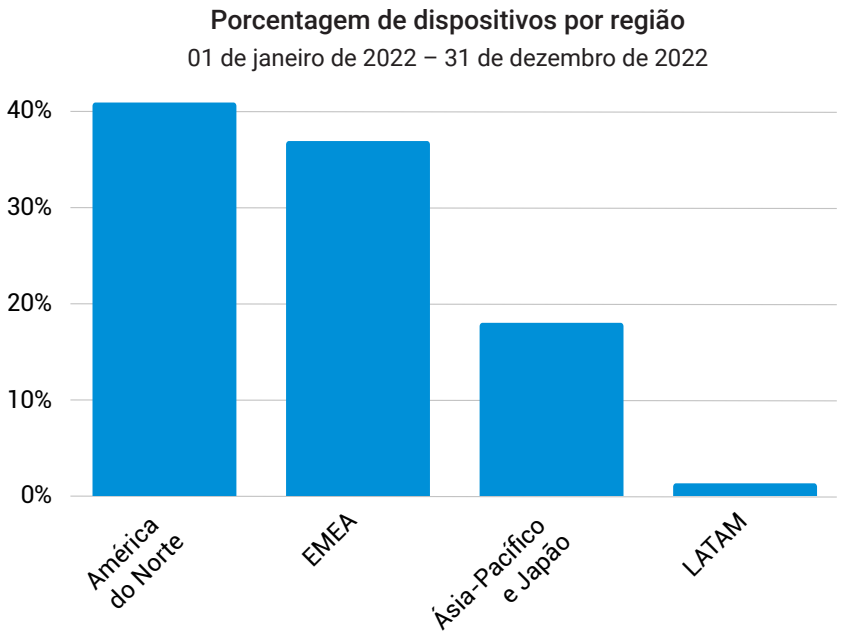


Fig. 7: A América do Norte assume a liderança em 41%, seguida pela EMEA (37%) e APJ (18%), quando se trata do número de dispositivos afetados por região

América do Norte

A maioria das organizações em todo o mundo sofreu com essas duas grandes ameaças: QSnatch e Emotet. Na América do Norte, aproximadamente 29% dos dispositivos afetados na região foram impactados pelo Emotet, enquanto 33% foram impactados pelo QSnatch (Figura 8). De acordo com um relatório Dark Reading, uma pesquisa da Shodan mostrou que existem 300.000 dispositivos QNAP conectados à Internet, o que o torna um alvo atraente. Além disso, dispositivos NAS como QNAP podem ser usados como backup e servem como servidores de mídia ou de arquivos.

Outras ameaças notáveis na América do Norte incluem Ramnit, Qakbot e REvil. Isso é interessante, já que IABs como Emotet abriram o caminho para outras infecções, incluindo (mas não se limitando a) ransomware.

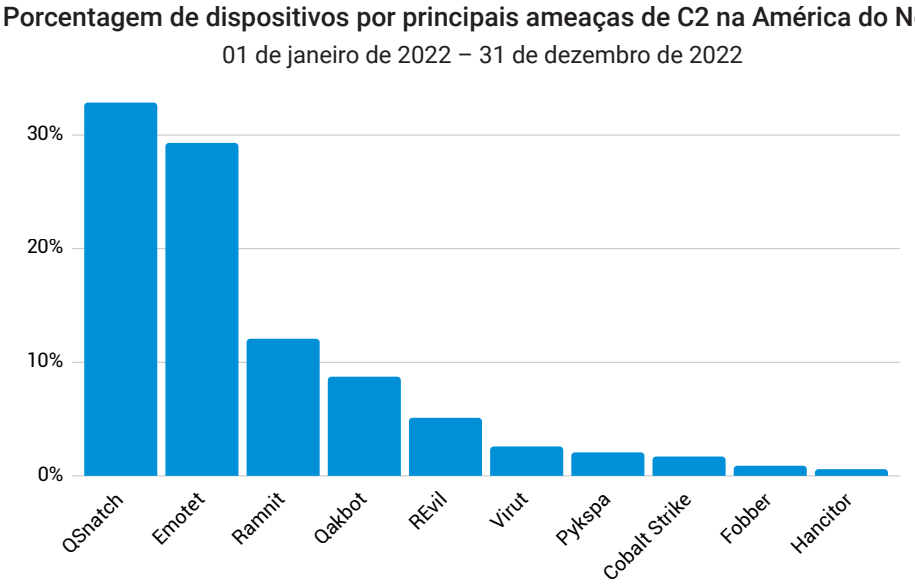


Fig. 8: A maioria dos dispositivos afetados em organizações norte-americanas acessou domínios relacionados a QSnatch, Emotet e Ramnit pelo menos uma vez

Europa, Oriente Médio e África

A EMEA tem a porcentagem mais alta de dispositivos afetados ao lado da América do Norte. As principais ameaças que vimos na região (Figura 9) incluíram QSnatch (28%) e Ramnit (21%). Não surpreende ver a ascensão de Ramnit na região, pois seus operadores visavam instituições bancárias/financeiras na Itália, no Reino Unido e na França no passado. Em uma das iterações, a configuração de Ramnit incluiu os países da UE como principais alvos. Na verdade, se compararmos o número de dispositivos afetados com Ramnit globalmente, a EMEA ainda é responsável pelo maior número de infecções por Ramnit. Além disso, os dispositivos com infecção por Emotet também foram altos na região em 19%.

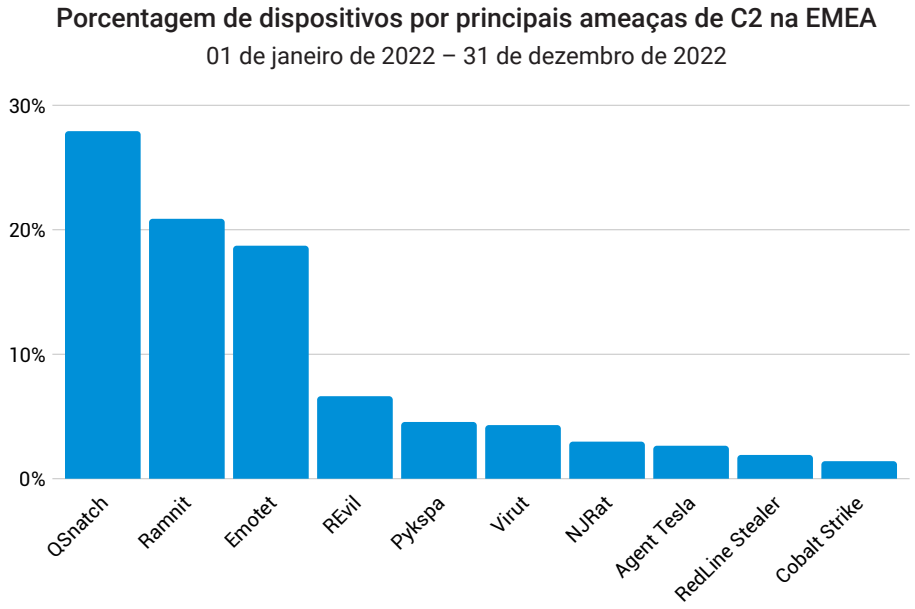


Fig. 9: Vimos mais dispositivos atingindo Ramnit de C2 na EMEA do que em outras regiões, aumentando significativamente o risco das organizações

Ásia-Pacífico e Japão

Na APJ, vimos que as infecções por QSnatch afetam significativamente a região (Figura 10). Quando comparamos os números de cada região, a região APJ fica em segundo lugar ao lado da América do Norte em termos de dispositivos com infecções por QSnatch. Por outro lado, a APJ também deve estar atenta às variedades de ransomware REvil e LockBit que estavam entre as cinco principais ameaças observadas nos dispositivos afetados na região. Embora os membros da gangue REvil tenham sido presos no ano passado, esse malware foi visto novamente no mundo real vários meses depois. É possível que os antigos membros que têm acesso ao código tenham tentado reavivar o REvil. Não é de estranhar ver ameaças de ransomware (que são amplamente motivadas financeiramente) como LockBit e REvil. E, como os operadores de RaaS continuam a aproveitar IABs como o Emotet, o ransomware continua sendo um desafio de segurança crucial para empresas de todos os setores e regiões.

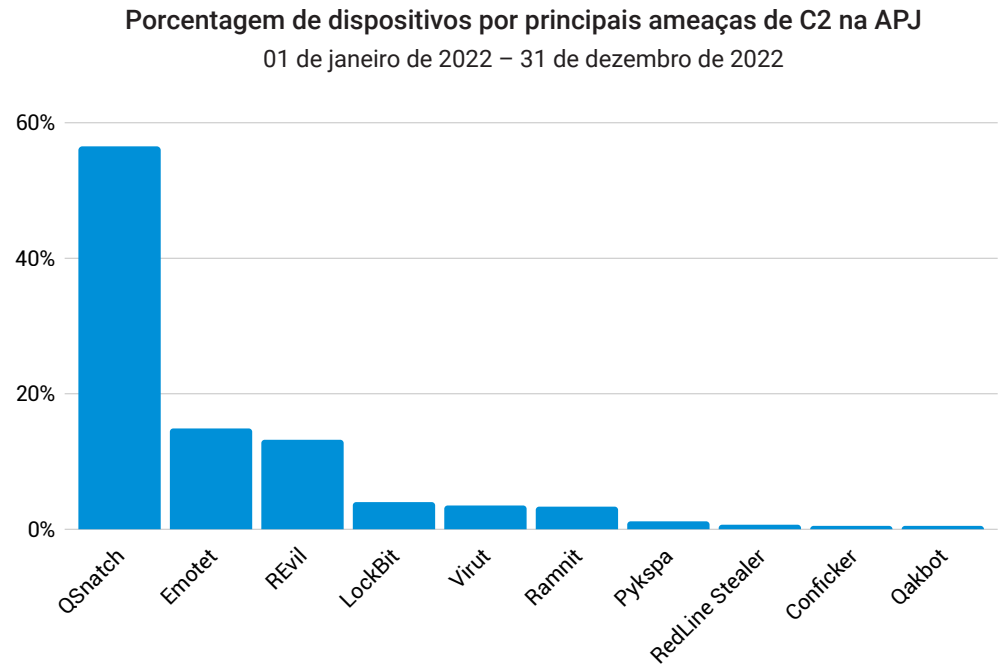


Fig. 10: A Akamai observou um número significativo de infecções por QSnatch na região

América Latina

Vamos agora examinar as tendências na América Latina. Embora essa região tenha o menor número de dispositivos afetados, isso não significa necessariamente que ela seja menos visada ou impactada. Semelhante às tendências globais, essa região foi impactada pelo QSnatch e Emotet (Figura 11). O simples exame dessa região revelaria que Agent Tesla, Virut e Ramnit são proeminentes.

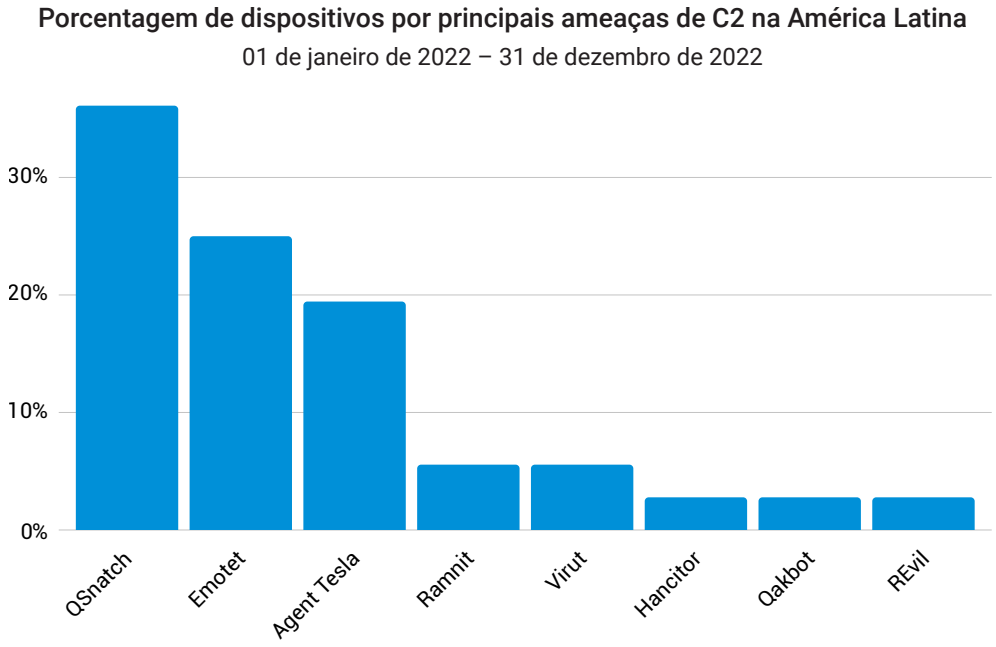


Fig. 11: As tendências globais também ressoam no cenário de ameaças da América Latina

As avarias regionais são importantes não só para ver as semelhanças, mas também para identificar quais ameaças específicas são exclusivas de cada região. Embora o QSnatch seja sempre a principal família de ameaças, as próximas quatro principais ameaças mudam entre as regiões com uma combinação de Elmotet, REvil, Ramnit e Agent Tesla. As ameaças regionais fazem toda a diferença à medida que você decide em que suas equipes de gerenciamento de vulnerabilidades e pentest devem se concentrar.

Tendências do setor e verticais: a fabricação é fortemente atingida pelos brokers de acesso inicial, botnets

Uma análise das tendências do setor nos permite ver o nível de risco de cada vertical individual e como elas se apresentam em comparação com outros setores. Em vez de examinarmos o número de dispositivos afetados, agregamos os dispositivos por clientes para chegar a quantas empresas são impactadas por vertical (Figura 12). Com base em nossos dados de DNS, vimos que mais de 30% das organizações analisadas com tráfego de C2 mal-intencionado estão no setor de fabricação. Além disso, empresas nos setores de serviços comerciais (15%), alta tecnologia (14%) e comércio (12%) foram afetadas. Os dois principais mercados verticais em nossos dados de DNS (fabricação e serviços comerciais) também ressoam com os principais setores atingidos pelo ransomware Conti, que abordamos em nosso relatório global de ransomware. Nesse relatório, mergulhamos profundamente nas vítimas do ransomware Conti e traçamos o perfil delas de acordo com a vertical, a receita e a região, ilustrando as tendências de ataque dessa prolífica ameaça.

> **Com base em nossos dados de DNS, vimos que mais de 30% das organizações analisadas com tráfego de C2 mal-intencionado estão no setor de fabricação. Além disso, as empresas nos mercados verticais de serviços comerciais (15%), alta tecnologia (14%) e comércio (12%) foram afetadas de forma semelhante.**

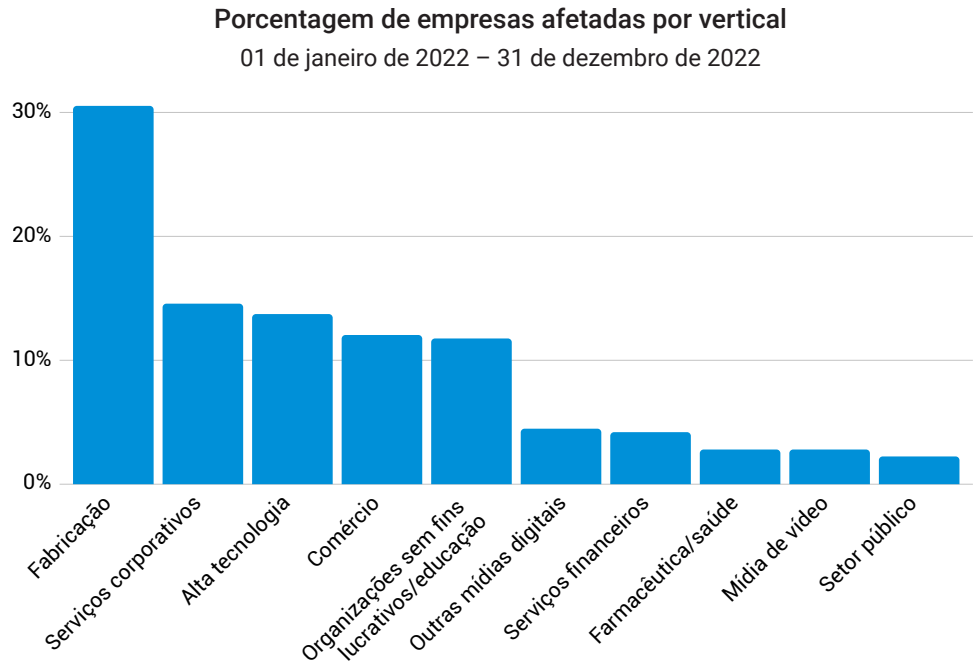


Fig. 12: Fabricação, serviços comerciais e alta tecnologia são os setores mais afetados por infecções de C2

O fato de que estamos vendo que a fabricação é fortemente atingida por vários ataques de C2 é preocupante, já que ela é considerada uma infraestrutura essencial, e ataques bem-sucedidos nesse setor podem causar efeitos no mundo real, como interrupções na cadeia de suprimentos. Os dados não demonstram razões específicas de por que a fabricação é a vertical mais impactada, mas uma investigação mais aprofundada sobre os tipos de ameaças nesse setor pode deixar um pouco mais claro.

Estamos vendo alguns países usarem regulamentações para reforçar a segurança em setores essenciais, como a fabricação. A legislação da UE chamada NIS2 reforçou os padrões de segurança cibernética e os requisitos de segurança, como análise de risco e políticas de segurança de sistemas de informação, segurança da cadeia de suprimentos e tratamento de incidentes para entidades essenciais (por exemplo, energia, transporte, serviços bancários, saúde etc). Também expandiu o escopo dos verticais impactados.

Porcentagem de dispositivos por principais ameaças de C2 na fabricação

01 de janeiro de 2022 – 31 de dezembro de 2022

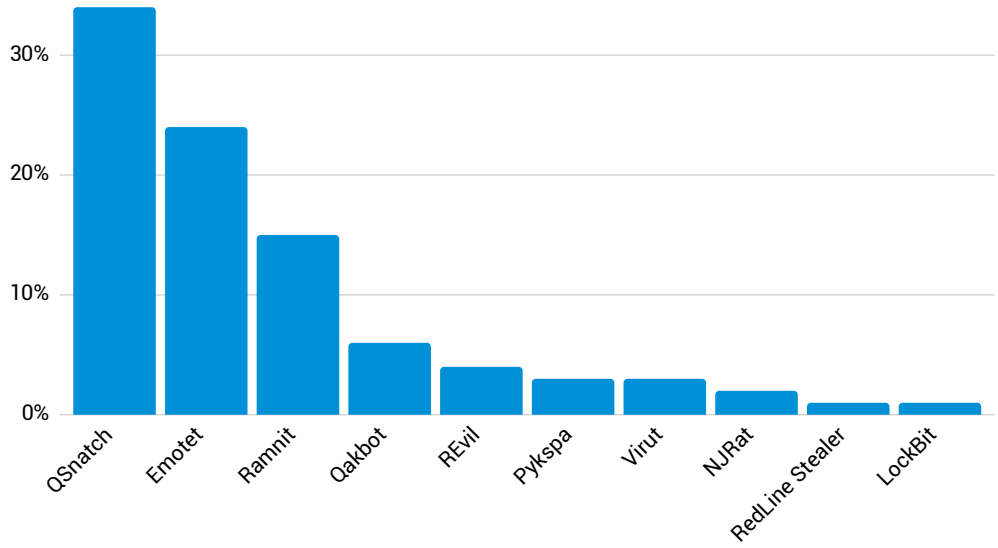


Fig. 13: As principais famílias de ameaças de C2 encontradas no setor de fabricação são QSnatch, Emotet e Ramnit

Uma análise aprofundada do setor de fabricação revela que QSnatch, IABs e Ramnit são alguns dos principais domínios de C2 relacionados que foram acessados por organizações neste vertical (Figura 13). A presença de IABs na rede deles pode indicar que os invasores estão coletando informações sobre possíveis alvos e, depois de terem acesso a máquinas comprometidas, eles podem vender esses dados para outros cibercriminosos, como grupos de RaaS. Além disso, também podemos ver os infostealers na lista de malwares de C2 que ameaçam esse setor. Uma ameaça a observar é o Redline Stealer, que tem a capacidade de coletar informações do navegador, como credenciais e detalhes de cartão de crédito, e está sendo vendido atualmente como MaaS por uma assinatura mensal de US$ 100 a US$ 150. De acordo com a pesquisa do Grupo-IB, este infostealer colheu cerca de 35.585.412 logs, que podem conter contas de login único, entre a segunda metade de 2021 e a primeira metade de 2022. Além disso, os domínios de C2 relacionados a este infostealer aumentaram 409% apenas no T3 de 2022.

As tendências do setor são sempre interessantes de acompanhar. O que está acontecendo em um vertical é, muitas vezes, apenas um trampolim à medida que os cibercriminosos avançam pelo cenário para todas as verticais do setor. Às vezes, vemos que os invasores se concentram em uma tecnologia que é proeminente em um setor. Outras vezes, eles vão atrás daqueles com maior probabilidade de pagar ou daqueles que pagariam mais. Também os vimos perseguir setores que tradicionalmente não investem tanto em cibersegurança. A conclusão é que, quando você vê fumaça na casa ao lado, é uma boa ideia verificar seu próprio sistema de prevenção de incêndio.

Usuários domésticos sob ataque

Os invasores estão de olho nas empresas porque isso representa uma recompensa maior quando eles violam as redes delas com sucesso. Eles usam uma ampla gama de ferramentas e táticas para infiltrar um perímetro empresarial, manter a persistência e, em alguns casos, exfiltrar informações confidenciais. Dessa forma, vemos ameaças como infostealers e IABs em redes corporativas, conforme discutido na seção anterior. No entanto, é um cenário diferente em redes domésticas, em relação a quais ameaças estão sendo empregadas e com que finalidade.

Os usuários domésticos representam uma demografia que geralmente não é tão segura quanto um ambiente corporativo, mas essa demografia não apresenta o mesmo retorno monetário. Os invasores sabem disso e, portanto, procuram maneiras de monetizar sua capacidade de infectar mais facilmente dispositivos domésticos. Por exemplo, eles lançam campanhas em larga escala com a intenção de comprometer o máximo de dispositivos possível nas táticas "spray and pray", enquanto os ataques contra empresas são altamente direcionados. Uma vez que esses dispositivos domésticos se tornem parte de uma enorme botnet, os invasores podem mobilizar esses dispositivos zumbis para realizar inúmeras atividades cibercriminosas sem o conhecimento do usuário, como spams e lançamento de ataques DDoS contra organizações. E para que os botnets sejam bem-sucedidos ou para que os cibercriminosos aluguem os botnets, eles precisam infectar o máximo possível de dispositivos. Outra forma desses invasores obterem benefícios financeiros por afetar os usuários domésticos é usar os recursos de computação de dispositivos infectados para fins de criptografia.

> **Uma vez que esses dispositivos se tornem parte de uma enorme botnet, os invasores podem mobilizar esses dispositivos zumbis para realizar inúmeras atividades cibercriminosas sem o conhecimento do usuário, como spams e lançamento de ataques DDoS contra organizações.**

As redes domésticas mostram tráfego intenso de botnets

À medida que mudamos nosso foco para usuários domésticos, examinaremos o tráfego de DNS mal-intencionado das redes domésticas analisando uma amostra anonimizada de milhões de consultas sinalizadas como mal-intencionadas dos últimos seis meses para demonstrar com quais ameaças os usuários devem se preocupar. Em resumo, as principais ameaças pertencem aos botnets, que podem explicar como os invasores estão aproveitando os dispositivos de IoT para diferentes finalidades, que discutiremos nas próximas seções.

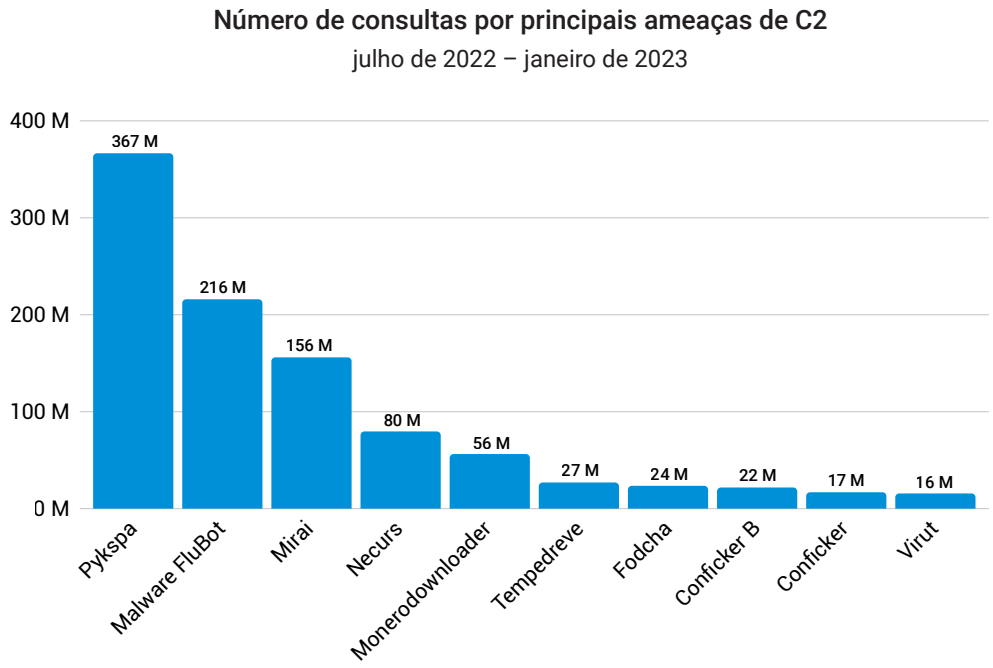


Fig. 14: Pykspa, malware FluBot e Mirai são os três principais botnets observados no tráfego de DNS de redes domésticas

Pykspa: propagação via mídia social

Com base em nossas descobertas de dados, Pykspa respondeu por 367 milhões de consultas de DNS sinalizadas globalmente (Figura 14). Essa ameaça se espalha pelo Skype enviando links maliciosos para os contatos dos usuários afetados. Em alguns casos, quando o Twitter é aberto na guia do navegador, ele também cria um tweet com um link de download para o malware. Além disso, ele usa um algoritmo de geração de domínio (DGA) para estabelecer a comunicação com C2. No passado, o v2 usava um subconjunto do DGA para evitar ser detectado e permanecer dentro da rede por um período mais longo.

Os recursos de backdoor permitem que um invasor se conecte a um sistema remoto e execute comandos arbitrários, como download de arquivos, encerramento de processos e propagação por vários meios (por exemplo, unidades mapeadas, compartilhamentos de rede), entre outros. O Pykspa também consulta a configuração do Skype para coletar informações pessoais sobre os usuários afetados. Ele também impede que os usuários acessem determinados websites, especialmente se contiverem certas strings relacionadas a soluções antimalware. Curiosamente, ele verifica a interface de idioma do Skype do usuário afetado e, se for um dos vários idiomas que ele está monitorando, incluindo inglês, alemão, francês, espanhol e italiano, o malware ajusta a mensagem de spam do Skype adequadamente.

FluBot: Botnet de malware de Android

O malware FluBot é a principal família de malware de C2 após Pykspa. Ele infecta principalmente telefones Android via mensagens de texto, incitando os usuários a clicar em um link mal-intencionado, o que leva posteriormente ao download do malware. Como parte dessa tática de propagação, o malware FluBot carrega as listas de contatos dos usuários afetados no servidor de C2 e também envia os contatos das vítimas com a mesma isca de engenharia social. Para os usuários, ter o FluBot em seus dispositivos coloca as informações bancárias e financeiras em risco, pois esse malware tem a capacidade de sobrepor uma página falsa quando os usuários acessam apps bancários legítimos. Como tal, essas credenciais podem ser usadas para roubo de identidade ou para fazer transações fraudulentas.

Esse malware usa várias iscas de engenharia social. Por exemplo, pode sugerir que os usuários cliquem em um link para verificar o status da entrega de encomendas; em outras situações, pode induzir os usuários a baixar um app de correio de voz falso dizendo que há uma mensagem de correio de voz. Ele também pode fingir ser uma atualização de segurança e incitar os usuários a clicar no link. Depois que os usuários clicarem no link, ele os instrui a baixar um app. Este app, por sua vez, pede permissão para acessar listas de contatos e fazer chamadas telefônicas etc. O que torna essa ameaça tão perigosa é que ela também solicita permissão para serviços de acessibilidade, permitindo que os invasores controlem os toques na tela, levando potencialmente à instalação de mais apps. Os usuários são aconselhados a redefinir seus dispositivos para os padrões de fábrica para remover esse malware.

Mirai: aproveitando o poder da Internet das Coisas para causar interrupções em larga escala

Em nossa pesquisa, o Mirai segue de perto o malware FluBot, com 156 milhões de consultas de DNS sinalizadas. Conhecido por ter como alvo dispositivos de IoT com portas telnet abertas, o Mirai se tornou famoso pelo ataque DDoS contra um dos maiores provedores de DNS. Esse worm de autopropagação procura dispositivos vulneráveis que usam as combinações padrão de nome de usuário e senha. A certa altura, ele acumulou um rebanho de mais de 100.000 dispositivos zumbis que os invasores usaram em ataques DDoS contra alvos importantes. Em um de seus ataques anteriores, o Mirai usou 145.000 dispositivos para um ataque a uma empresa de tecnologia. Este é um exemplo de como dispositivos não seguros podem ser armados para cometer ataques cibernéticos e causar interrupções em larga escala contra as empresas.

Em 2016, o grupo por trás do Mirai liberou o código fonte, possivelmente para impedir que as autoridades o rastreassem até os autores originais (e para, portanto, evitar prisão). Com isso, outros grupos começaram a usar o código do Mirai, modificando-o e aprimorando-o com mais funcionalidades, como a capacidade de infectar sistemas. Um dos efeitos da liberação do código no mundo real é que vimos novas variantes, como Okiru, Satori, Masuta e PureMasuta, com o objetivo de lançar também ataques DDoS. Embora a reinicialização do dispositivo infectado ajude, como o malware está verificando constantemente dispositivos, há uma grande probabilidade de ser reinfectado, a menos que o usuário altere as senhas.

Necurs: distribuidor de malware e vendedor de acesso

O botnet Necurs, que foi identificado pela primeira vez em 2012, foi responsável por 80 milhões de consultas sinalizadas nos últimos seis meses. Ele representa um sério risco para usuários domésticos e organizações, com sua capacidade de fornecer outras cargas de malware, como Dridex, TrickBot e Locky, entre outros. Um fator notável que vale a pena destacar é que esse botnet também vende acesso a computadores infectados para outros grupos como parte das ofertas de contratação de botnet. Como a maioria dos botnets, ele usa um DGA para executar a rotatividade de vários domínios para os servidores de C2 e para continuar as operações apesar dos domínios estarem bloqueados.

Além de distribuir ransomware e cavalos de troia bancários, o Necurs também é usado para distribuir vários ataques de spam, como golpes de relacionamento, etc. Durante uma investigação, a Microsoft monitorou as atividades desse botnet e descobriu que, em apenas 58 dias, ele enviou aproximadamente 3,8 milhões de mensagens de e-mail com spam. Em 2020, as operações do botnet Necurs foram interrompidas por meio da colaboração da polícia e da comunidade de segurança.

Monerodownloader: botnet de mineração

Uma das muitas maneiras pelas quais os invasores obtêm lucro é usando máquinas comprometidas para criptomineração. A crescente popularidade da criptomoeda Monero entre os cibercriminosos é uma razão pela qual estamos vendo botnets feitos especificamente para minerá-la. Os invasores preferem essa criptomoeda, pois a cadeia não é tão exposta e oferece anonimato; portanto, não é rastreada até eles. Embora muito pouco se saiba sobre o Monerodownloader, algumas das táticas que ele executa incluem a coleta de informações e a conexão com servidores de C2 para a carga real.

Deixar os sistemas sem patches abre caminho para ameaças como os criptomineradores de Monero. Outros mineradores de Monero similares aproveitam as vulnerabilidades, se apresentam como software gratuito para atrair os usuários a baixar o minerador e têm a capacidade de se mover lateralmente pela rede e infectar outros dispositivos para obter o máximo de receita possível. Embora a descrição do movimento lateral seja mais aplicável às empresas do que aos usuários domésticos, isso nos dá uma ideia de como os criptomineradores trabalham para maximizar a infecção.

Principais ameaças por região: os botnets continuam a reinar em redes domésticas

Vejamos mais atentamente os nossos dados regionais para elucidar quais botnets específicos são predominantes por região com base no tráfego de DNS das redes domésticas e para examinar alguns fatores possíveis que contribuem para essa tendência.

América do Norte

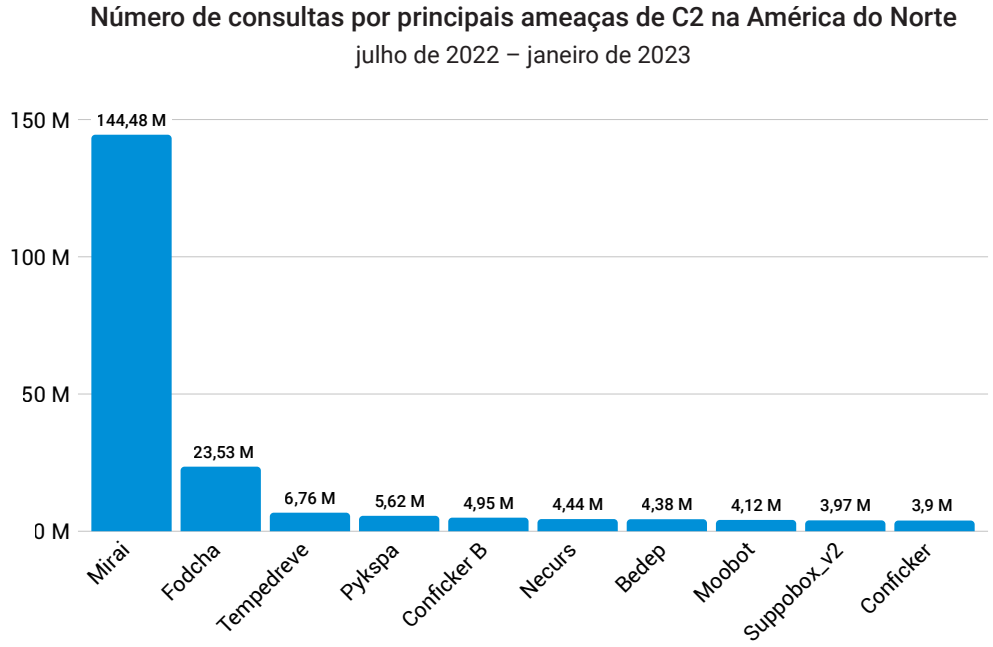


Fig. 15: O Mirai continua se propagando na América do Norte potencialmente por causa de dispositivos de IoT não seguros

Na América do Norte, mais de 144 milhões de consultas associadas ao botnet Mirai foram vistas em redes domésticas (Figura 15). Esse botnet é direcionado a dispositivos de IoT vulneráveis que ainda estão usando nomes de usuário e senhas padrão. O alto volume de consultas provenientes dessa região pode ser devido à popularidade ou ao alto uso de dispositivos de IoT em residências. Somente em 2022, as famílias dos EUA supostamente tinham uma média de 22 dispositivos conectados, o que diminuiu ligeiramente em relação aos 25 no ano anterior. E com as conexões de IoT previstas para aumentar na América do Norte (5,4 bilhões até 2025), há uma alta probabilidade de mais ameaças, como o Mirai, ou variantes semelhantes, que se aproveitam de dispositivos de IoT desprotegidos.

Para os usuários domésticos, o impacto de tal ameaça é que os cibercriminosos podem explorar os dispositivos deles sem seu conhecimento para cometer os crimes. Mas as organizações também sofrem com os efeitos de ataques DDoS, ou até mesmo de campanhas de spam mal-intencionadas, lançadas por botnets como o Mirai. Como prática recomendada, é sempre uma boa ideia alterar o nome de usuário e a senha padrão de seus dispositivos para protegê-los contra Mirai e outros ataques semelhantes.

Europa, Oriente Médio e África

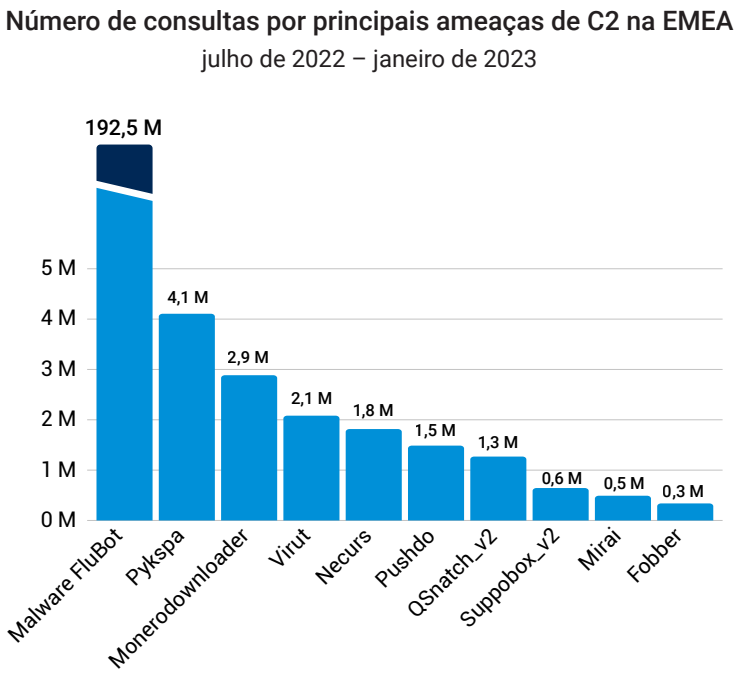


Fig. 16: Vimos um surto de malware FluBot na região EMEA possivelmente devido à tática de propagação e ao uso de vários idiomas europeus como parte da isca de engenharia social

Dizer que o malware FluBot está se espalhando como um incêndio na região EMEA seria minimizar a situação. O volume impressionante das consultas de DNS observadas nessa região (aproximadamente 193 milhões) é notável. E por meio de exame do tráfego de DNS, a Akamai conseguiu ver essas infecções acontecendo na EMEA (Figura 16). Um fator contributivo é a tática de propagação de smishing, uma forma de phishing na qual o invasor envia SMS para a lista de contatos da vítima. Além disso, ele engana os usuários para que baixem um app relacionado a uma entrega de pacote ou app de correio de voz que é, na verdade, o malware. Fora isso, o FluBot pede permissões adicionais e registra secretamente as credenciais bancárias/financeiras dos usuários sem o conhecimento deles. Segundo informado, o alvo eram usuários na Espanha, Alemanha, Finlândia e Reino Unido, entre outros. O SMS também é escrito em vários outros idiomas da UE, como alemão e húngaro, que pode ser um dos muitos fatores desse malware ter surgido na Europa.

América Latina

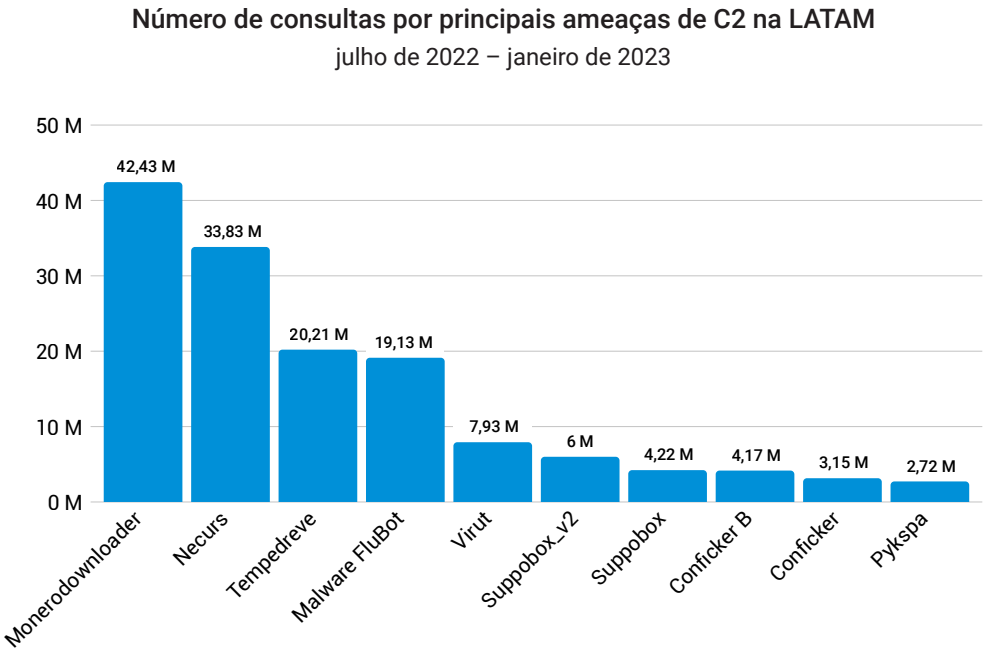


Fig. 17: O botnet de criptomineração Monerodownloader tornou-se a principal ameaça na América Latina, possivelmente devido ao alto uso de criptografia na região

Diferentemente da América do Norte e EMEA, a região da América Latina mostrou uma distribuição mais diversificada de botnets (Figura 17). O monerodownloader, um botnet de criptomineração, lidera a lista de grupos de botnet ativos com 42 milhões de consultas sinalizadas, seguidas por Necurs (34 milhões) e Tempedreve (20 milhões). A alta taxa de adoção da criptomoeda na região, alimentada por altas taxas de inflação e transferências, poderia explicar por que botnets como monerodownloader lideram a lista. Sem o conhecimento do usuário, os cibercriminosos podem estar usando os recursos dos dispositivos do usuário para fins de mineração e para seu próprio ganho financeiro. Também é importante observar que o FluBot é uma das principais ameaças observadas no tráfego de DNS, que mostra a prevalência do botnet mesmo fora da região da EMEA, onde vimos um alto volume de tráfego.

Ásia-Pacífico e Japão

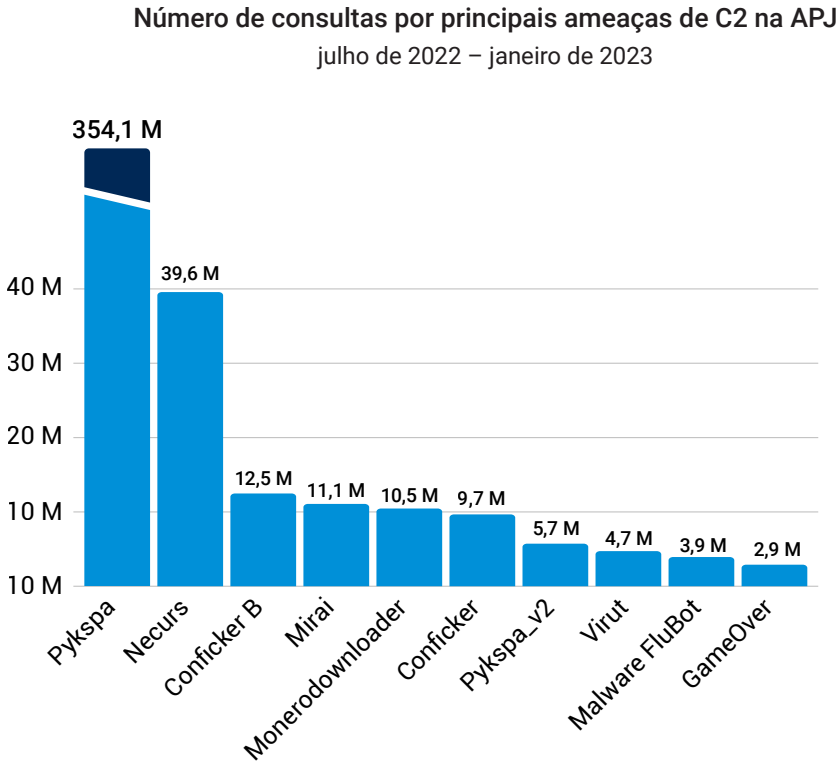


Fig. 18: As ameaças dominantes na APJ incluem Pykspa e Necurs

Mais de 350 milhões de consultas relacionadas ao Pykspa foram observadas na região APJ (Figura 18). Em uma publicação no blog de 2019, notamos que o Pykspa usou um mecanismo DGA seletivo para permanecer fora do radar por um longo período. Os domínios destacados nesse relatório foram encontrados principalmente no Leste Asiático. Também observamos consultas associadas a botnets, como Necurs, que é um forte indicador de que os sistemas estão infectados com outros malwares.

Visão geral do cenário de phishing

Na última parte de nossa análise de tráfego de DNS, examinamos kits de phishing e a função crucial deles no sucesso das campanhas de phishing. O phishing ainda é relevante, mais do que nunca, devido às táticas em constante evolução usadas pelos adversários e ao aumento da quantidade de informações pessoais disponíveis online. Os adversários estão usando engenharia social para fazer com que as tentativas de phishing pareçam legítimas, e evidências indicam que a taxa de sucesso desses ataques permanece alta. A pesquisa da Akamai sobre golpes de phishing em feriados revelou novas técnicas e táticas usadas por adversários para permanecer fora do radar. Essas novas táticas incluem o uso de depoimentos de usuários falsos como parte do golpe e a técnica recém-descoberta de usar a ancoragem HTML para garantir que somente usuários válidos sejam direcionados a websites fraudulentos.

O aumento do trabalho remoto devido à pandemia de COVID-19 também dificultou a detecção e a prevenção de ataques de phishing, tornando mais importante que indivíduos e organizações permaneçam atentos e tomem medidas para se protegerem. Além disso, o aumento da mídia social e o número cada vez maior de dispositivos conectados à Internet criaram mais oportunidades para os adversários.

Campanhas de phishing atingem serviços financeiros

Ao investigar quais marcas estão sendo violadas e imitadas por golpes de phishing, há várias maneiras de coletar os dados. Reunimos o número total de campanhas em relação ao número de vítimas. Isso nos permite avaliar a taxa de sucesso de uma determinada campanha, bem como ver qual porcentagem de cada setor está sendo visada.

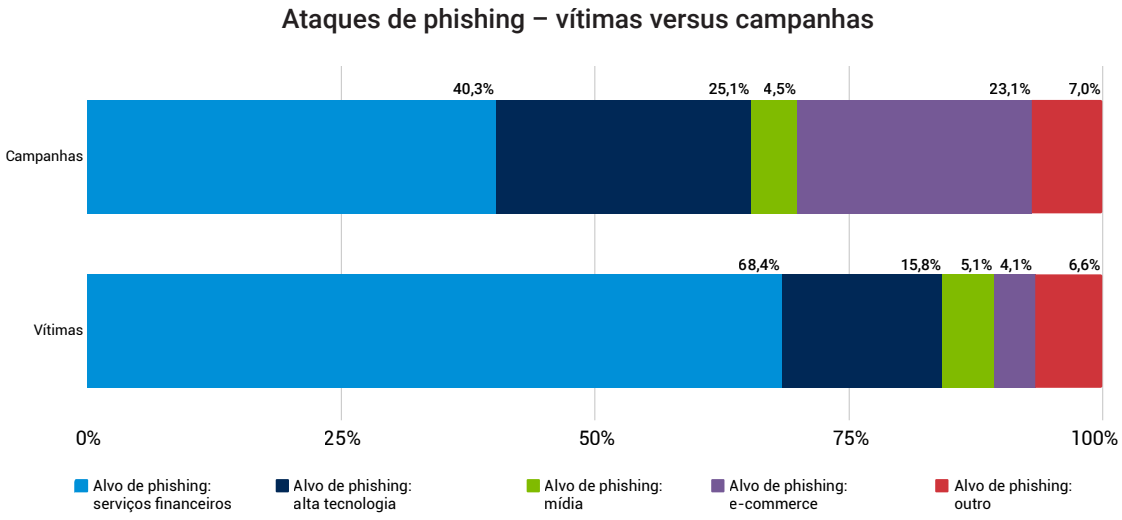


Fig. 19: A maioria das campanhas de phishing visou o setor de serviços financeiros (4º trimestre de 2022)

Nossa pesquisa descobriu que as marcas financeiras e de alta tecnologia lideraram tanto o número de campanhas quanto de vítimas (Figura 19). Observamos que 40,3% das campanhas em clientes de serviços financeiros foram ativadas, resultando em 68,4% das vítimas, o que indica que os ataques contra serviços financeiros foram altamente eficazes no 4º trimestre de 2022. Em nosso relatório de serviços financeiros Enemy at the Gates: Analyzing Attacks on Financial Services (A ameaça bate à porta: Análise de ataques a Serviços financeiros), enfatizamos como os ataques de phishing são financeiramente motivados e, na maioria das vezes, visam serviços financeiros e seus clientes. Os possíveis impactos desses ataques incluem danos à marca e à reputação e perda da confiança do cliente. O phishing também pode custar recursos da organização para corrigir o problema.

O comércio eletrônico observou 23% das campanhas de phishing ativadas no 4º trimestre de 2022. Embora tenhamos visto mais campanhas do que vítimas reais, também é importante observar que os invasores estão atacando esse setor e os usuários devem permanecer vigilantes, pois os cibercriminosos podem estar atrás de informações pessoais ou bancárias.

Kits de ferramentas de phishing: ativadores de tentativas de phishing

A impressionante escala e magnitude do cenário de phishing está sendo conduzida pela existência de kits de ferramentas de phishing. Os kits de ferramentas de phishing oferecem suporte à implantação e à manutenção de websites de phishing e permitem que até mesmo golpistas não técnicos se juntem ao cenário adverso de phishing e executem golpes de phishing.

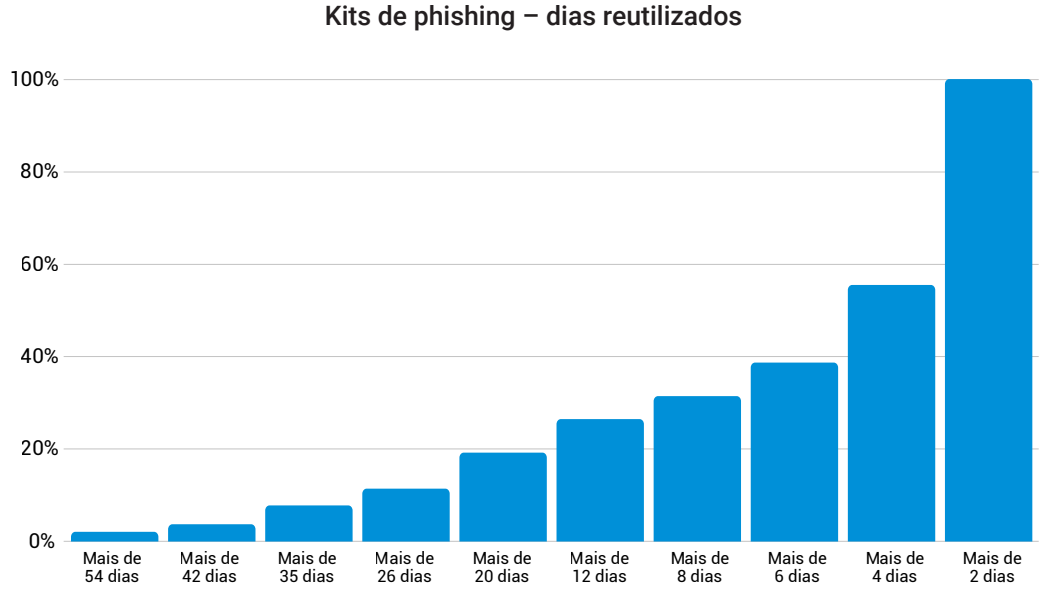


Fig. 20: Kits de ferramentas de phishing por número de dias de reutilização (4º trimestre de 2022)

De acordo com nossa pesquisa, que rastreou mais de 300 kits de ferramentas de phishing diferentes sendo usados no mundo real para lançar novas campanhas de ataques, 2,04% dos kits rastreados foram reutilizados em pelo menos 54 dias distintos no 4º trimestre de 2022 (Figura 20). Além disso, 55,5% dos kits foram reutilizados para lançar uma nova campanha de ataque em pelo menos quatro dias, e 100% dos kits rastreados foram reutilizados em pelo menos dois dias distintos no 4º trimestre.

Conclusão e recomendações: combata os ataques modernos com medidas proativas

Agora que abordamos grupos de ameaças e metodologias de invasores, vamos falar sobre como aproveitar todas essas informações. Começaremos explicando como gerenciar o DNS, internamente ou terceirizando o gerenciamento. Para organizações maiores ou mais complexas, faz sentido ter um provedor especializado em gerenciamento de DNS para cuidar disso para você. De qualquer forma, assegure de monitorar o desempenho e as proteções do seu DNS. Em seguida, considere os diferentes controles necessários. Proteção contra DDoS, ataques de malware e extração, movimento lateral e exfiltração são as principais áreas a serem mitigadas. Acompanhar essa jornada de dados e procurar todas as vulnerabilidades críticas que você pode interromper a cada etapa é um modelo de segurança cibernética geralmente chamado de cadeia de destruição.

Considere a criação de manuais para as técnicas de ataque abordadas neste relatório. Verifique com sua equipe pentest ou equipe vermelha para determinar se eles usam as mesmas ferramentas e técnicas que IABs, como Qakbot e Emotet, bots como QSnatch, ransomware como LockBit (em ambiente de laboratório) e ferramentas como Cobalt Strike. É importante se certificar de que seus controles de segurança estejam alertando e interrompendo esses tipos de ataques com eficiência e que suas equipes sejam treinadas para resolvê-los.

Se o Cobalt Strike for detectado em sua rede, é prudente criar imediatamente um relatório de incidentes e investigá-lo. Embora a ferramenta possa ser empregada por sua equipe vermelha (nesse caso, ela deve ser investigada e reportada mesmo assim), a presença desse tráfego deve soar o alarme, pois isso pode indicar invasão por outros grupos de invasores de RaaS ou agentes de ameaça, e sinalizar um ataque contínuo que ainda poderia ser mitigado.

Considere como seu centro de operações de segurança opera e determine como você está acompanhando processos (como bits, Wget ou cURL) que podem indicar a probabilidade de que uma ameaça relacionada a IAB esteja na rede fazendo reconhecimento. A parte crucial é descobrir o que foi baixado e interromper se ainda estiver em execução. Em seguida, investigue o que acionou o IAB: foi um arquivo LNK, macro ou VScript? E descobrir, a partir daí, como a violação começou.

Fique por dentro de nossas pesquisas mais recentes verificando nosso Hub de pesquisa de ameaças.

Metodologias

Tráfego de ataque de comando e controle

Os dados neste relatório são gerados por nosso produto SIA (Secure Internet Access) e descrevem o tráfego de ataque de comando e controle (C2). O SIA é um gateway da Web seguro baseado em nuvem que foi projetado para ajudar os usuários a conectar facilmente os dispositivos à Internet de maneira segura. Os dois conjuntos diferentes de dados utilizados em todo esse relatório refletem separadamente os dados de alerta de segurança de organizações empresariais com grandes quantidades de usuários ou provedores de Internet com usuários domésticos individuais. Esses dados foram medidos pelo número de dispositivos afetados e pelo número de consultas, respectivamente. Um dispositivo afetado foi definido como um dispositivo que atingiu um domínio de C2 conhecido e identificado pelo menos uma vez. Da mesma forma, uma consulta de C2 foi definida como uma consulta que chegou a um domínio de C2 conhecido e identificado. Nossas equipes de segurança usam esses dados internamente para pesquisar ataques, sinalizar comportamento mal-intencionado para notificar os clientes e fornecer inteligência adicional às soluções de segurança da Akamai.

Créditos

Editorial e redação

Or Katz

Eliad Kimhy

Badette Tribbey

Contribuição com revisão e material do assunto

Tanya Belousov

Shiran Guez

Ophir Harpaz

Stiv Kupchik

Grace Wang

Steve Winterfeld

Análise de dados

Ronan Ballantine

Gal Kochner

Chelsea Tuttle

Marketing e publicação

Georgina Morales Hampe

Shivangi Sahu

Mais informações sobre o State of the Internet / Segurança

Leia as edições anteriores e fique atento às próximas versões dos aclamados relatórios State of the Internet/Segurança da Akamai. akamai.com/soti

Mais informações sobre a pesquisa de ameaças da Akamai

Mantenha-se atualizado com as análises de inteligência de ameaças, os relatórios de segurança e as pesquisas mais recentes sobre cibersegurança. akamai.com/security-research

Acesse os dados deste relatório

Visualize versões em alta qualidade das tabelas e dos gráficos mencionados neste relatório. Essas imagens podem ser usadas e consultadas livremente, desde que a Akamai seja devidamente creditada como a fonte e que o logotipo da Akamai seja mantido. akamai.com/sotidata

Mais sobre as soluções da Akamai

Para saber mais sobre as soluções da Akamai para ameaças direcionadas a empresas, visite nossa página Secure Internet Access Enterprise. Os provedores de serviços direcionados aos mercados de consumo e PMEs podem visitar Serviços do Secure Internet Access para ISPs.

A Akamai potencializa e protege a vida online. As principais empresas do mundo escolhem a Akamai para criar, entregar e proteger suas experiências digitais, ajudando bilhões de pessoas a viver, trabalhar e jogar todos os dias. A Akamai Connected Cloud, uma plataforma de nuvem e edge amplamente distribuída, aproxima as aplicações e experiências dos usuários e afasta as ameaças. Saiba mais sobre as soluções da Akamai para computação em nuvem, segurança e entrega de conteúdo em akamai.com e akamai.com/blog ou siga a Akamai Technologies no Twitter e no LinkedIn. Publicado em 03/23