

Relatório de Ameaças 2023 da Sophos

O amadurecimento do crime: os novos desafios dos marketplaces para as equipes de defesa

Conteúdo

Carta do CTO	2
Definindo o tom: a guerra na Ucrânia	4
Um conflito regional que ecoa mundialmente	4
No centro de tudo	5
A economia do malware	6
Os nove malfeitores	6
Do jargão 133t à engenhosidade	11
Infostealers	13
A evolução do ransomware	17
Ferramenta de ataque	20
Levando as ferramentas de segurança ofensiva para o mau caminho	21
Outras ferramentas de segurança exploradas pelo uso indevido	24
RATs com dupla finalidade	24
LOLBins e executáveis legítimos	25
Vulnerabilidades “Bring your own”	26
Ransomwares têm como alvo upgrades de segurança de endpoints	28
Malware Miner	28
Para além do Windows: o panorama das ameaças móveis, Linux e Mac	30
Ameaças ao Linux	30
Ameaças móveis	33
Conclusão	34

**Joe Levy**

CTO da Sophos

Carta do CTO

A indústria da segurança cibernética costuma fazer uma retrospectiva a cada fim de ano, e os últimos doze meses estão, categoricamente, entre os períodos mais nefastos da história dessa indústria. Ainda que não tenham ocorrido eventos marcantes como os ataques cibernéticos Aurora, Stuxnet, WannaCry ou Colonial Pipeline, 2022, infelizmente, entrou para os anais da história da era cibernética juntamente com uma avassaladora guerra na Europa – a maior nos últimos 50 anos.

Por que isso importa tanto para a segurança cibernética? Bem, é que o país que conhecemos como um dos principais promotores e paraíso do crime cibernético do mundo, o progenitor do ransomware como uma indústria nacional, invadiu seu vizinho.

Assim que a Rússia invadiu a Ucrânia, era inevitável que o governo russo, se não destacasse o seu próprio contingente governamental, incitaria a instituição doméstica do crime cibernético a agitar a opinião mundial a seu favor e tentaria sabotar a reputação que o presidente da Ucrânia conquistara mundialmente. E foi exatamente isso o que aconteceu quando grupos manipuladores de informações, ransomwares e malwares engendraram fincar a agressão da Rússia.

Todos esses esforços, até agora, se mostraram um total fracasso. A opinião geral sobre a criminalidade dos ransomwares já havia atingido seus níveis mais baixos, quando, durante a pandemia, as gangues criminosas direcionaram seus ataques às partes mais vulneráveis dos setores mais cruciais na época, incluindo o setor de saúde, as organizações de pesquisas médicas, as operações voltadas às cadeias de suprimentos, e alimentação e energia, chegando a atingir até o sistema de ensino. Na verdade, eles não geraram um manancial de simpatizantes quando gangues de ransomware deixaram o mundo ainda mais irado ao pronunciarem seu apoio incondicional à invasão russa e declararam que colocariam sob sua mira qualquer país ou organização que se opusesse a eles.

Mas alguns membros dessas mesmas facções sediadas na Ucrânia viram as coisas um pouco diferente. E foi assim que começou a retaliação e o vazamento de informações superconfidenciais sobre como as comunidades e os agentes de ameaças de ransomware operam. Aparentemente, a guerra abalou os vínculos entre os agentes de ameaças ucranianos e seus parceiros russos (e bielorrussos), provavelmente para sempre.

Durante esse mesmo período em que a Rússia tem se ocupado em promover sua contenda de agressões, a China tem dado lances drásticos no cenário do crime cibernético, direcionando sua mira não apenas a seus vizinhos e países considerados cruciais para a sua iniciativa do “cinturão e rota”, mas para a indústria da segurança propriamente dita. Em uma série crescente de ataques audaciosos contra empresas que atuam na linha de frente da proteção de informações e redes, grupos de agentes de ameaças baseados na China (e provavelmente com o seu patrocínio) atacam produtos de segurança de hardware criados por praticamente todas as empresas do setor de infraestrutura e segurança cibernética.

Em um aspecto real e muito pessoal, a sensação é de que a hostilidade despontou em 2022, e as duas maiores nações que representam uma ameaça à segurança cibernética para o restante do mundo decidiram parar de dissimular seu envolvimento nas grandes violações, nos principais ataques a infraestruturas e na interferência maléfica na educação, no comércio global e na saúde. Elas podem até mesmo chegar a exibir suas façanhas, sem reservas, como a perguntar: e então, o que pretendem fazer?

O que estamos fazendo sobre isso, e o que a Sophos continuará a fazer, é escorar nossas iniciativas que já estão em andamento visando a nossa proteção e a proteção de nossos clientes. A empresa tem trabalhado em um processo plurianual incremental de melhorias em detecção e intervenção automatizada do comportamento de ransomwares, atingindo tamanho sucesso ao sabotar os invasores que, agora, os adversários ativos estão tendo que aplicar mais e mais esforços em subterfúgios para tentar nos ludibriar antes que possam se beneficiar de suas ameaças.

No tocante aos ataques a infraestruturas de segurança incitados por grupos de ameaças baseados na China e na Rússia, a confiança em nossos fornecedores nunca foi tão importante quanto agora. Acreditamos que os fornecedores devam comunicar com transparência seus investimentos para conquistarem a confiança e mantê-la, especialmente quando um fornecedor está envolvido ativamente na oferta de produtos e serviços de segurança cibernética. A Sophos mantém o [Trust Center](#), que promove insights do trabalho que fazemos em consultorias e divulgações, nossos testes de segurança e programa de escrutínio na captura de bugs, e nossos planos de análise e resposta a incidentes. Fazemos investimentos contínuos para proteger a nossa própria infraestrutura contra ataques direcionados por APTs, e reforçamos hardwares e softwares em execução no ambiente de produção de nossos clientes. Nosso sucesso será gradual, já que os adversários não param de tentar descobrir e explorar vulnerabilidades, e, de fato, parecem ter intensificado seus esforços destinados a subverter a segurança de firewalls, switches e pontos de acesso a redes de todo e qualquer fornecedor. Continuamos a promover configurações de segurança inseridas como padrão em nossas ofertas e a introduzir práticas básicas, como verificações de integridade e correção de políticas, em nossos produtos e serviços para melhorar a higiene e a postura operacional.

As ameaças continuarão a evoluir, e a Sophos continuará a se adaptar, de modo implacável, para entregar segurança cibernética com resultados superiores.

Definindo o tom: a guerra na Ucrânia

Se a guerra é o prolongamento da política e o conflito cibernético é apenas outra ramificação dessa hostilidade, parece óbvio que o conflito na Ucrânia apresente o mesmo aspecto tanto online quanto offline. No momento em que este material é redigido, o panorama das ameaças se mostra hediondo dentro das fronteiras ucranianas, e ainda que não tenha penetrado de modo significativo no restante do mundo ocidental, o conflito traz uma preocupação imensa e um fardo significativo a todos – e o seu inquietante potencial de estender-se e infligir a falta de informação persiste.

Um conflito regional que ecoa mundialmente

Como seria de se esperar, o agravamento cinético dos ataques russos contra a Ucrânia que marcaram o dia 24 de fevereiro trouxe à tona os famigerados golpistas em busca de lucrar da dor e da desgraça alheias.

No início de março, rastreamos um número perturbador de e-mails de falsas entidades beneficentes pedindo donativos para aplacar a dor dos ucranianos. Nos primeiros dias da guerra, oficiais ucranianos apelaram ao mundo por donativos para ajudá-los em suas defesas, e esses apelos incluíam donativos em criptomoeda ao tesouro público da Ucrânia. Imediatamente, os golpistas se envolveram na transitoriedade da oportunidade na circulação de criptomoedas e enviaram milhões de mensagens de e-mail reiterando o pedido, mas alteravam o endereço da carteira de criptomoeda de modo a incluir endereços não associados ao governo ou sem envolvimento real com instituições ou agências de assistência não governamentais. No fim de semana de 5 e 6 de março, o volume de spams pedindo donativos a essas carteiras de criptomoedas enganosas foi tão alto que constituiu metade de todos os spams que recebemos durante esses dias – uma quantidade alarmante. Felizmente, essa campanha sucumbiu em poucos dias.

Porcentagem no volume diário de spams relacionados à Ucrânia, março de 2022

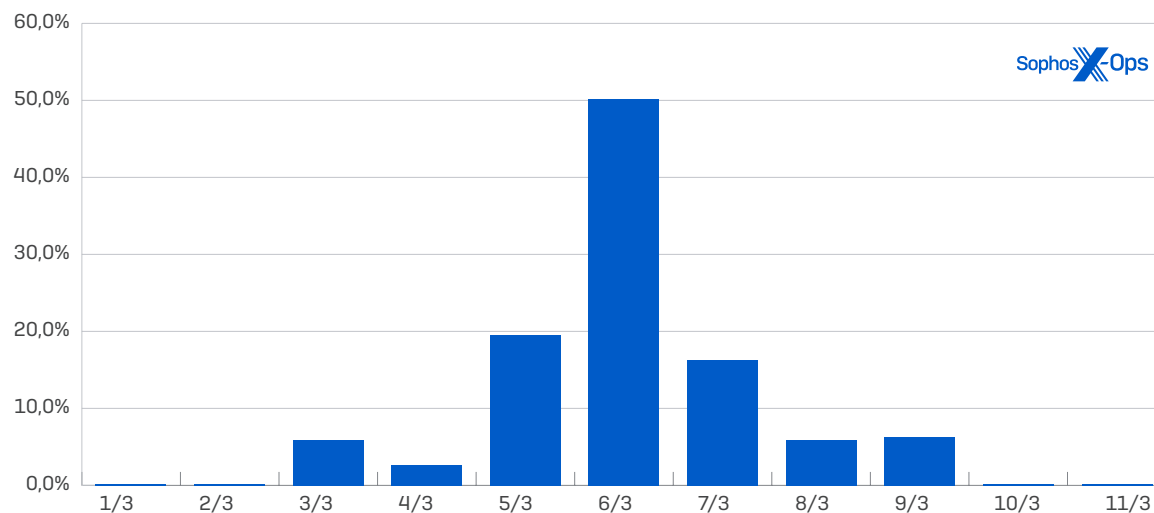











Fig. 1. O volume de e-mails de spam pedindo donativos com endereços enganosos de carteiras de criptomoedas subiu vertiginosamente, porém com curta duração.

Em maio, havia centenas de sites falsos pedindo “donativos”, mas como aconteceu com a primeira onda de spams, baseados em aspectos comuns das informações financeiras, muito provavelmente foram poucas as entidades envolvidas. A força motriz por trás desses ataques não foi sua sofisticação técnica. Pelo contrário, os ataques envolviam o nome do país ou de seus líderes como parte do engodo da engenharia social, mas se escoravam em vulnerabilidades e explorações disponíveis relativamente antigas.

Por exemplo, em uma campanha **notável** naquele mês, o grupo do malware **Emotet** distribuiu uma coletânea de documentos mal-intencionados em Word com títulos provocativos que imitavam a propaganda russa, do tipo “EUA e aliados fornecem armas químicas ao exército da Ucrânia.doc”, na tentativa de disseminar seu malware. Os documentos maliciosos usados no ataque se aproveitaram do exploit [CVE-2021-40444](#) para infectar os computadores das vítimas que abriram os documentos em equipamentos que não tinham o patch do Office instalado, o qual havia sido lançado na segunda metade do ano anterior.

Name	Date modified
 Chemical weapons use from Syrian war stokes Ukraine's fears.docx	5/10/2022 2:43 AM
 list of nato generals hiding in the basement of the Azovstal steel plant.docx	5/10/2022 2:46 AM
 Nato's generals who were hiding in the underground bunker of the Azovstal steel factory just surrendered.docx	5/10/2022 2:47 AM
 The US Violation of the Chemical Weapons Convention.docx	5/10/2022 2:44 AM
 Ukraine war Fact-checking Russia's biological weapons claims.docx	5/10/2022 2:43 AM
 US aircraft carrier approaches the black sea to support Ukraine.docx	5/10/2022 2:48 AM
 US and Allies provide chemical weapons to Ukraine's military.docx	5/10/2022 2:46 AM
 US 'deeply concerned' at report of Mariupol chemical attack.docx	5/10/2022 2:44 AM
 US, Allies Probe Claim of Chemical Agent in Ukraine.docx	5/10/2022 2:45 AM




Fig. 2. Título de documentos do spam Emotet seguindo a temática da guerra na Ucrânia faziam acusações falsas e aterradoras.

Quanto aos ataques cibernéticos aos Estados fora das fronteiras da Ucrânia, a atribuição de um dos dois incidentes de mais alto nível já é menos sólida. O ataque ao ViaSat, que afetou os serviços de satélite para os ucranianos e também para outros clientes em outras regiões da Europa horas antes da invasão ter início, foi, sem sombra de dúvida, [responsabilidade](#) dos oficiais russos. Porém, os ataques a sites de aeroportos voltados ao público feitos em outubro são mais difíceis de interpretar: tratavam-se de esforços do país para intimidar os aliados da Ucrânia, ou eram ataques independentes?

O bom senso nos leva a crer que foram ataques independentes. A obliteração com uso de baixa tecnologia e os serviços DDoS (inclusive nos sites dos aeroportos – sem mencionar a tentativa de atrapalhar a votação do Eurovision) foram outro ponto que marcou os primeiros dias da guerra, mas com o conflito se arrastando e adentrando o inverno, e as tensões globais se intensificando, alguns observadores não técnicos veem as trapalhadas promovidas pela afiliada russa KillNet nos sites como um lembrete de que nada que parta deles pode ser visto de forma resoluta.

No centro de tudo

Na Ucrânia, a situação é mais obscura e singular. Vários ataques visando ao governo ucraniano seguiram padrões observados em campanhas criminosas: o uso de e-mails de engenharia social, malwares como commodities e o abuso de ferramentas comerciais de segurança ofensiva. Um dos casos retrata um e-mail forjado contendo um link para uma “atualização de antivírus” que, na verdade, baixava um beacon do Cobalt Strike. Em outro caso, o qual examinaremos mais adiante neste relatório, um ladrão de informações alegava estar vendendo grandes quantidades de dados de cidadãos ucranianos e organizações governamentais – sem pedidos de resgate, que se saiba, mas pelo simples prazer da contravenção e da exposição dos dados.

A Ucrânia e a Rússia, embora sejam dois países independentes, têm cidadãos que têm sido parceiros de longa data no crime (literalmente), e várias gangues de ransomware usam afiliados sediados nos dois países. Quando a guerra irrompeu, certas gangues se dissolveram, aparentemente em um rompante de patriotismo.

Como um espetáculo à parte, a divisão entre membros russos e ucranianos das gangues de ransomware e seus afiliados pode ter levado à formação do Conti Leaks, um despejo de logs de chats de uma comunidade de ransomware. Uma conta do Twitter que teve uma vida curta, chamada @TrickbotLeaks, começou a fazer o [doxing](#) (revelando informações pessoais e privadas) de possíveis membros dos grupos criminosos Trickbot, Conti, Mazo, Diabol, Ryuk e Wizard Spiders.

O que foi desvendado? Mais indícios de que, como muitos pesquisadores já vinham dizendo há anos, o Serviço Federal de Segurança da Rússia (FSB) está intimamente ligado a vários grupos de ransomware, e pode até mesmo ter contratos com essas entidades para incursões específicas do Conti.

Mas, infelizmente, nenhum desses conflitos destrutivos levaram a uma redução significativa na atividade do ransomware globalmente. Ainda que 2022 tenha começado com a captura de vários membros da comunidade REvil de ransomware-as-a-service ([em janeiro](#)) e de uma gangue de exploração de cartões de crédito ([em fevereiro](#)) por oficiais do FSB, que chegaram até a [extraditar](#) um membro do REvil para ser julgado nos EUA no início de março, no meio do ano esse tipo de colaboração na luta contra o crime internacional parecia inimaginável – e havia indícios de que o REvil, ou alguém que tentava se passar pelo serviço, já havia [despertado](#). E a guerra continua.

A economia do malware

Ainda que vários aspectos do panorama das ameaças tenham evoluído no último ano, talvez o mais significativo de todos seja o desenvolvimento continuado da economia do crime cibernético. Esse ecossistema vem se transformando em uma indústria, com uma rede de serviços de suporte e uma abordagem profissional e bem-estabelecida às suas operações.

Assim como as empresas de tecnologia da informação mudaram para as ofertas “as-a-service”, o ecossistema do crime cibernético também mudou. Agentes de acesso, ransomwares, malwares que roubam informações, entrega de malwares e outros elementos das operações cibernéticas criminosas abaixaram seus padrões para tentar uma chance de entrar no mundo do crime digital.

Essa tendência se dá, em parte, com o surgimento da economia do crime cibernético. Marketplaces de criminosos, como o [Genesis](#), permitem oferecer aos aspirantes do crime cibernético a possibilidade de adquirir malwares e serviços de implantação de malware para então vender credenciais roubadas e outros dados em pacotes. Os agentes de acesso normalmente usam explorações de vulnerabilidades de softwares para montar suas bases de operações em centenas de redes e depois vendê-las a outros criminosos – geralmente vendendo o mesmo ponto de acesso várias vezes. E as afiliações de ransomwares e outros invasores adquirem essas credenciais e acesso para desempenhar atividades criminosas altamente arriscadas e altamente lucrativas.

A industrialização do ransomware permitiu que as “afiliações” de ransomwares se desenvolvessem em operações mais profissionais, especializadas na exploração. Trabalhando com ferramentas profissionais de segurança ofensiva, softwares técnicos e administrativos legítimos, malware-as-a-service, e outros exploits e malwares obtidos no mercado, temos visto uma convergência dos agentes de ataque a conjuntos de ferramentas, táticas e práticas que não podem mais ser associados a operações específicas de ransomware, espionagem internacional ou outros motivos específicos. Esses grupos de profissionais se especializaram em obter (ou comprar) acesso para qualquer criminoso que esteja disposto a pagar.

Esses grupos imitam a indústria de serviços da Web e da nuvem de várias formas diferentes em seus modelos de negócios. Ainda que uma grande proporção da TI corporativa tenha adotado o modelo “as-a-service” em seu escopo de operações, praticamente todos os aspectos do kit do crime cibernético podem ser terceirizados a provedores de crime-as-a-service que anunciam nos subterrâneos da dark Web. Rapidamente, cobriremos nove variantes do tema, e deixaremos a décima para um exame mais minucioso.

Os nove malfeitores

Access-as-a-service: o acesso a contas e sistemas comprometidos é vendido individualmente ou em pacotes através de serviços clandestinos, incluindo protocolo RDP e credenciais de VPN, contas, bancos de dados, Web shells e vulnerabilidades exploráveis.

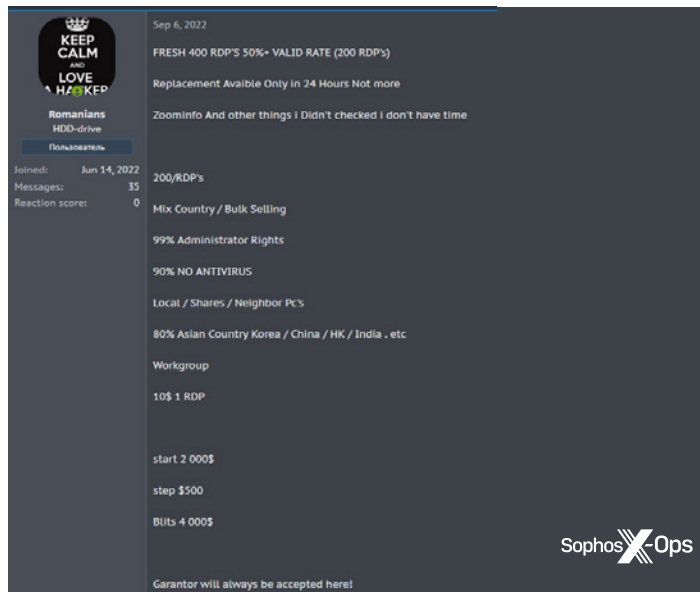


Fig. 3. Um agente de acesso, buscando uma venda fácil de sua mercadoria.



VPN-RDP / TOP-EU / 5kk
By LummA, Tuesday at 08:45 AM in Auctions

LummA
byte

Posted Tuesday at 08:45 AM

Geo: EU BE Belgium
Access: VPN - RDP
Revenue: 5kk
Activity: Wholesale industry, supply to EU, busy active company
Rights: DA Admin
AV: Bit Defender

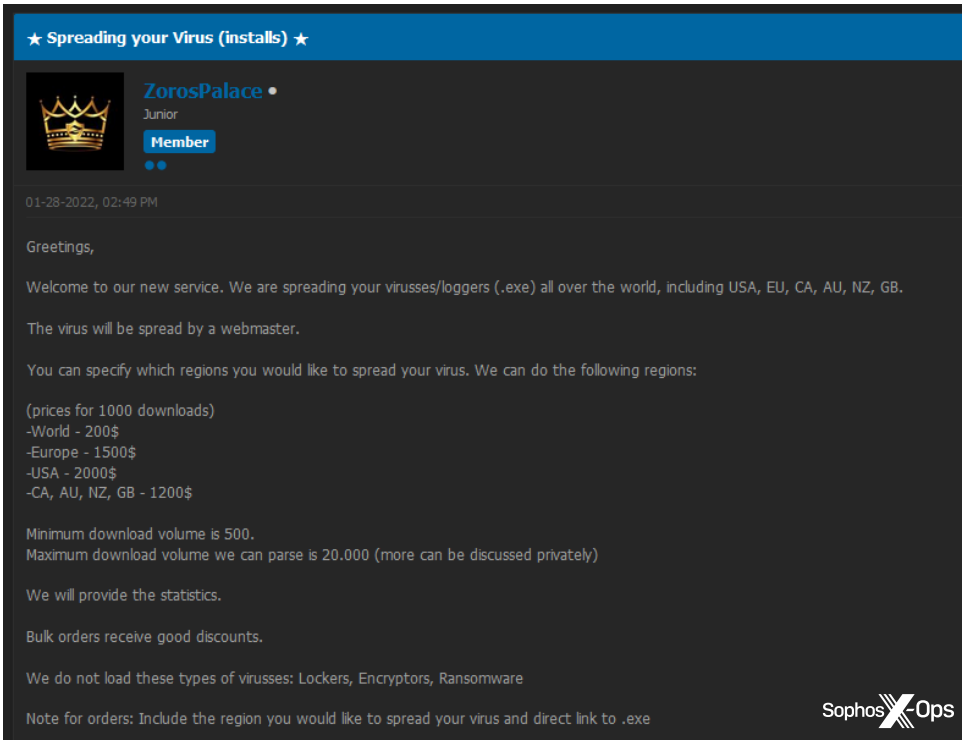
Paid registration
● 0
4 posts
Joined
03/05/22 (ID: 126577)
Activity
хакинг / hacking

Start: 250\$
Step: 250\$
Blitz: 750\$
PPS: 24 hours

Дам доступ тем кто с репой или с депозитом, остальные через гарант

Fig. 4. Dados de uma empresa europeia em leilão

Distribuição de malware/spreading-as-a-service: facilita a distribuição de malwares em regiões ou setores específicos, ou de maior alcance. Nos anúncios que vimos desses serviços, não está claro como isso é feito exatamente, mas os possíveis vetores incluem ataques watering-hole, exploração de vulnerabilidades ou interseções em listas de AaaS (access-as-a-service).



★ Spreading your Virus (installs) ★

ZorosPalace • Junior Member

01-28-2022, 02:49 PM

Greetings,

Welcome to our new service. We are spreading your virusses/loggers (.exe) all over the world, including USA, EU, CA, AU, NZ, GB.

The virus will be spread by a webmaster.

You can specify which regions you would like to spread your virus. We can do the following regions:

(prices for 1000 downloads)
-World - 200\$
-Europe - 1500\$
-USA - 2000\$
-CA, AU, NZ, GB - 1200\$

Minimum download volume is 500.
Maximum download volume we can parse is 20.000 (more can be discussed privately)

We will provide the statistics.

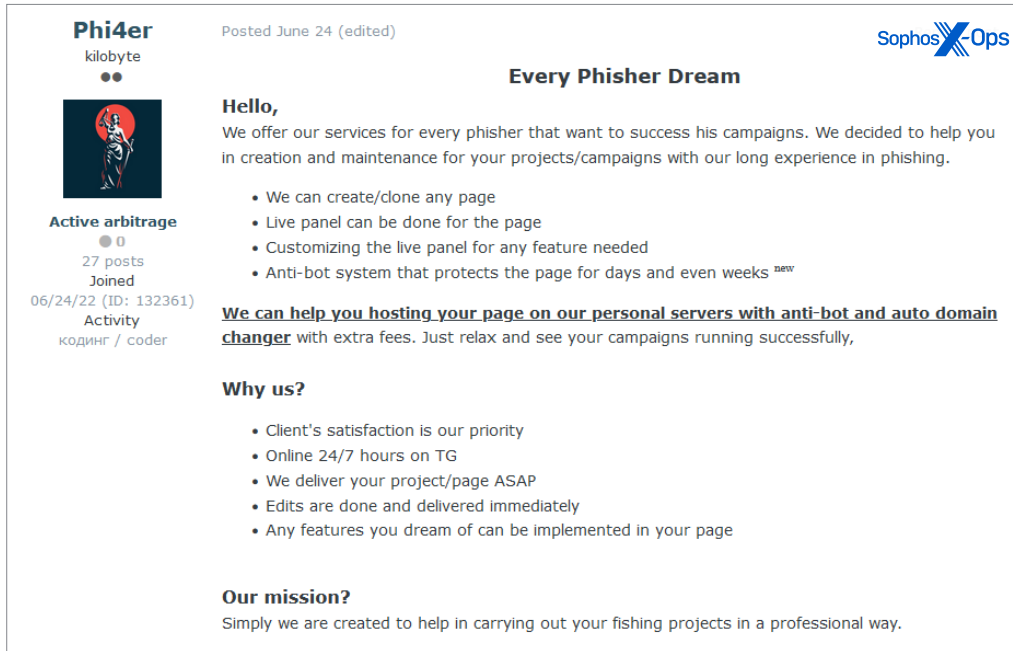
Bulk orders receive good discounts.

We do not load these types of virusses: Lockers, Encryptors, Ransomware

Note for orders: Include the region you would like to spread your virus and direct link to .exe

Fig. 5. Um novo empreendimento que oferece serviços de propagação de malware.

Phishing-as-a-service: agentes de ameaças oferecem serviços de ponta a ponta para campanhas de phishing, incluindo sites clonados, hospedagem, e-mails criados para burlar filtros de spam e painéis para monitorar resultados.



The screenshot shows a forum post by user 'Phi4er' (kilobyte) titled 'Every Phisher Dream'. The post is dated June 24 and includes a Sophos X-Ops logo. The content is as follows:

Phi4er
kilobyte
●●
27 posts
Joined
06/24/22 (ID: 132361)
Activity
коддинг / coder

Posted June 24 (edited)

Every Phisher Dream

Hello,
We offer our services for every phisher that want to success his campaigns. We decided to help you in creation and maintenance for your projects/campaigns with our long experience in phishing.

- We can create/clone any page
- Live panel can be done for the page
- Customizing the live panel for any feature needed
- Anti-bot system that protects the page for days and even weeks ^{new}

We can help you hosting your page on our personal servers with anti-bot and auto domain changer with extra fees. Just relax and see your campaigns running successfully,

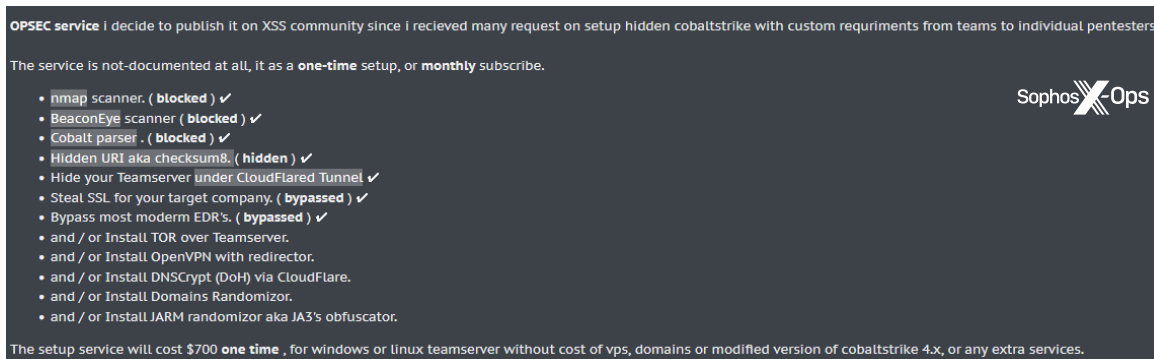
Why us?

- Client's satisfaction is our priority
- Online 24/7 hours on TG
- We deliver your project/page ASAP
- Edits are done and delivered immediately
- Any features you dream of can be implemented in your page

Our mission?
Simply we are created to help in carrying out your fishing projects in a professional way.

Fig. 6. Uma suíte de serviços de phishing fornecida com garantia de atendimento ao cliente.

OPSEC-as-a-service: um serviço particularmente interessante, que vimos acompanhado do Cobalt Strike em um fórum do crime. O vendedor oferece assistência aos compradores através de um serviço OPSEC – para uma instalação única ou uma assinatura mensal – criado para ocultar infecções por Cobalt Strike e minimizar o risco de detecção e atribuição.



The screenshot shows an advertisement for 'OPSEC service' on a dark background. It includes a Sophos X-Ops logo and a list of services with checkmarks indicating they are available. The text is as follows:

OPSEC service | I decide to publish it on XSS community since I recieved many request on setup hidden cobaltstrike with custom requirments from teams to individual pentesters.

The service is not-documented at all, it as a **one-time** setup, or **monthly** subscribe.


- nmap scanner. (**blocked**) ✓
- BeaconEye scanner (**blocked**) ✓
- Cobalt parser . (**blocked**) ✓
- Hidden URI aka checksum8. (**hidden**) ✓
- Hide your Teamserver under CloudFlared Tunnel ✓
- Steal SSL for your target company. (**bypassed**) ✓
- Bypass most modern EDR's. (**bypassed**) ✓
- and / or Install TOR over Teamserver.
- and / or Install OpenVPN with redirector.
- and / or Install DNSCrypt (DoH) via CloudFlare.
- and / or Install Domains Randomizor.
- and / or Install JARM randomizor aka JA3's obfuscator.

The setup service will cost \$700 **one time** , for windows or linux teamserver without cost of vps, domains or modified version of cobaltstrike 4.x, or any extra services.


Fig. 7. Serviço especializado oferece assistência a invasores para encobrir seus rastros.

Crypting-as-a-service: um serviço comum à venda em vários fóruns, a criptografia como serviço foi desenvolvida para criptografar malwares de modo a burlar a detecção – especialmente pelo Windows Defender e SmartScreen, e também por produtos antivírus, mas com menor amplitude de ação. No exemplo abaixo, o serviço é oferecido por US\$ 75 para uma aquisição de uso único, e por US\$ 300 para uma assinatura de um mês, que inclui o uso ilimitado do serviço.

Helium
Malware Services



Paid registration
+3
68 posts
Joined
08/16/21 (ID: 119109)
Activity
вирусология / malware



Posted 16 hours ago (edited) Report post

Our WD crypting service is one of a kind. You won't have to go through the hassle of finding a reputable crypting service any longer.
With our exclusive .bat encryption - your executable (.exe) will be transformed into a small, 6-25 kb batch (.bat) file.
This ensures the best results for manual file distribution.

Using a .bat file has many advantages over the classic .exe file.

- **Guaranteed WD Bypass**
- **Bypass ChromAlert & SmartScreen** (bypasses SmartScreen with non-passworded .zip or .rar file)
- Easy to run and your file will stay undetected for much longer than with a classic .exe
- No need for an EV Signing Certificate compared to regular .exe files

Features:


- Adds a **Windows Defender exclusion** for your file when ran on a computer - this way you won't lose connection.
- Loads your executable from an external host straight to the computer when the .bat file is executed.
- Your file will receive a ripped signature for further anti-detection.

Fig. 8. Para quem quer se esquivar da detecção, um serviço especializado oferece transformar arquivos .exe em arquivos .bat.

Scamming-as-a-service: vimos alguns exemplos de “kits de scam” particularmente relacionados a golpes com criptomoedas anunciados em fóruns do crime. Nem sempre fica claro o que está sendo vendido, mas um deles oferecia um kit pronto para uso por US\$ 450: “Elon Musk Giveaway BTC Scampage”. Esse kit é bastante popular desde 2018, e apareceu no [Twitter](#), [Medium](#), e também teve vez como um [vídeo deepfaked](#).

Vishing-as-a-service: um serviço de phishing por voz (“vishing”), em que um agente de ameaça aluga um sistema de voz para receber chamadas, e um “sistema de IA”, de modo que o arrendatário coloca as vítimas para falar com um robô, em vez de um humano.

Mr.Wizard
byte



User
+1
19 posts
Joined
03/17/18 (ID: 86273)
Activity
кодинг / coder

Posted August 18 (edited)

Renting a Voice SYSTEM TO RECEIVE CALLS With Live Panel to get CC + OTP.

The victim will call the number then will follow the steps during the calls.

Also there AI system Incase your victim to speak to the bot.

All Language.
All Accent.

1 Month = \$1500 (1 Bank or Service).

Guarantor Accepted (Buyer pay the fees)

I can customize it to your needs.
Contact me to show you a demo.




Fig. 9. Um vishing-as-a-service cuja oferta inclui “todos os idiomas e todos os sotaques”.

Spamming-as-a-service: nosso velho conhecido, e ainda bastante proeminente nos fóruns do crime, o spamming-as-a-service oferece spam em massa através de uma diversidade de mecanismos, incluindo SMS e e-mail. Em alguns casos, o agente de ameaça oferece instalar toda a infraestrutura do zero; em outros casos, ele opera a infraestrutura e a utiliza para enviar mensagens de spam personalizadas.

Scanning-as-a-service: um serviço particularmente interessante oferecido em um fórum do crime, que oferece aos usuários o acesso a uma suíte de ferramentas comerciais legítimas – incluindo Metasploit, Invicti, Burp Suite, Cobalt Strike e Brute Ratel – para encontrar (e supostamente explorar) vulnerabilidades. Como vemos na Figura 10, os preços são oferecidos com grandes descontos. Toda a infraestrutura é aparentemente criada e mantida pelo vendedor, que afirma que “você só precisa esperar pelos resultados do golpe”.

Our selection

Metasploit Professional \$30000/year
 /> \$35 / scan || \$100/month unlimited scans (webapps and services)
 /> \$200 / C2 server setup
<https://metasploit.com>

Invicti Enterprise \$20000/year
 /> \$35 / scan || \$100/month unlimited scans (webapps)
<https://invicti.com>

Acunetix \$4500/5-scans
 /> \$35 / scan || \$100/month unlimited scans (webapps)
<https://acunetix.com>

Burp Suite Enterprise \$6995/year
 /> \$35 / scan || \$100/month unlimited scans (webapps)
<https://portswigger.net/burp/enterprise>

Nmap
 /> \$35 / scan || \$100/month unlimited scans (services) (using our specialized nse scripts)
<https://nmap.org>

Cobalt Strike \$5900/year
 /> \$100 / C2 server setup
<https://cobaltstrike.com>

Brute Ratel \$2250/year
 /> \$100 / C2 server setup
<https://bruteratel.com>


Sophos  Ops

Fig. 10. Provedor de scanning-as-a-service lista o acesso a várias suítes de ferramentas comerciais populares.

Do jargão 133t à engenhosidade

Conforme a indústria do “as-a-service” se expande e os marketplaces do crime se aproximam cada vez mais dos commodities, sua aparência também muda. Em um desses fóruns proeminentes, os usuários podem pagar pelo espaço para anunciar, por exemplo, e exibir propagandas animadas aos milhares de usuários do fórum. Observe que um dos anúncios no exemplo abaixo é do Genesis, o popular marketplace [do qual falamos anteriormente](#).

Fig. 11. Um fórum criminoso de esportes anuncia uma variedade de marketplaces e serviços.

Os agentes de ameaças estão se dando conta das vantagens do design e do layout gráfico profissional. Enquanto alguns anos atrás as listas de serviços e malwares eram tipicamente postagens simples e com texto puro apresentando uma lista de recursos e funcionalidades, as ofertas de hoje geralmente são acompanhadas de imagens atraentes criadas para dar aos produtos um ar de profissionalismo e diferenciar a marca e sua legitimidade.

Fig. 12. O serviço Zed Point propõe fornecer informações que podem facilitar a alteração ou o roubo de identidade.

Fig. 13. NoCryi reúne e mantém o acesso a cookies de sessão roubados.

Não são só apenas produtos e serviços que são anunciados nos marketplaces. Com o profissionalismo e o crescimento contínuos da economia do crime, as postagens de ofertas de trabalho e contratações estão cada vez mais comuns. Vários marketplaces têm páginas de classificados dedicadas, tanto para quem procura emprego (geralmente “pentesters”, um eufemismo para afiliações de ransomware) quanto para empregadores.

▲ 0 ▼

[JOB - BTC/XMR] I operate dozens of phishing websites of all kinds. Looking for some "marketers" who can bring people in for a 50/50 split
 by /u/carderman · 1 week ago in /d/Jobs4Crypto

Like the title states, I've got a bunch of different custom-built phishing websites, ranging from fake darknet markets, fake crypto exchanges, email templates with fake giveaways & crypto promos, fake carding sites, simple landing pages, and so on.

I'm looking for someone or someones who'd like to bring people in, via spamming, social engineering, whatever method works for you... and if they take the bait, we split their generous donations 50/50.

I've had some of these up for anywhere from over a year to some I just created this week. These sites bring in a decent chunk of change as they are, but I've never been opposed to more money.

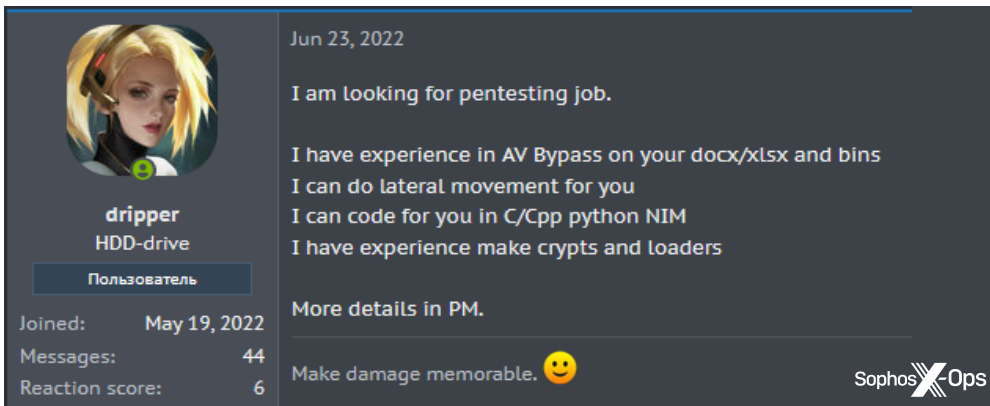
If interested in getting started, or simply learning more about them, just DM me and I can send you some links and you can choose which ones you think you might be able to do something with.

We can keep track of which ones are yours using a coupon code or custom "referral" url. I have a couple ideas for making sure we're on the same page when it comes to keeping track of which "sales" are yours. I'm keen to ensure you're compensated fairly for the hits you bring in because that's just good business - this shit is already passive AF and basically free money for me at the end of the day. But if you can bring in more free money then I'm more than happy to keep you happy if that means you'll keep selling.

Hell, if you're really good, I'd be more than happy to give you the lions share.

Let's make some money, ladies!

Fig. 14. Alianças entre entidades com diferentes habilidades ajudam a aumentar a eficiência.



Jun 23, 2022

I am looking for pentesting job.

I have experience in AV Bypass on your docx/xlsx and bins
I can do lateral movement for you
I can code for you in C/Cpp python NIM
I have experience make crypts and loaders

More details in PM.

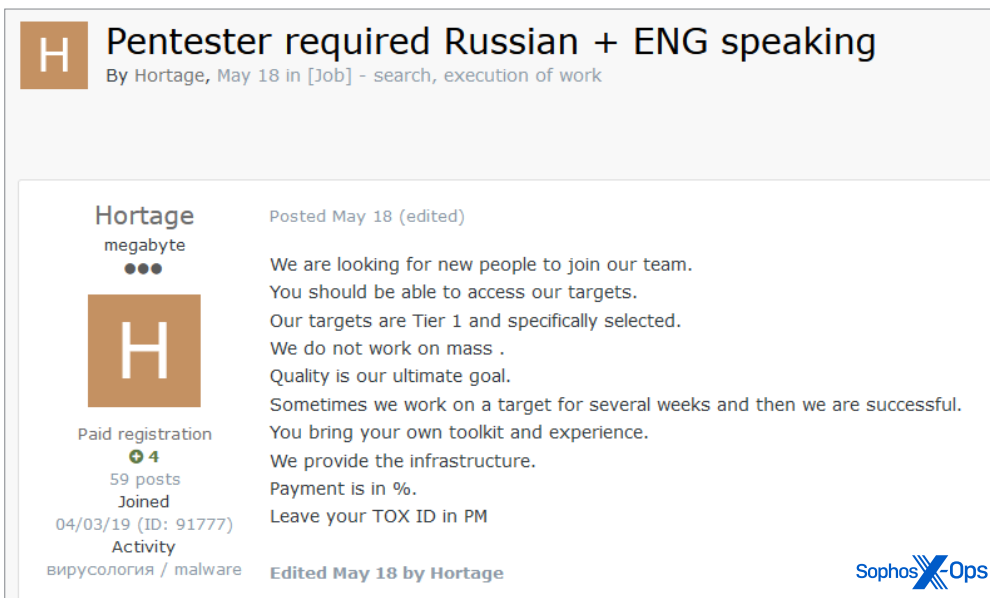
Make damage memorable. 😊

Sophos X-Ops

driper
HDD-drive
Пользователь

Joined: May 19, 2022
Messages: 44
Reaction score: 6

Fig. 15. Um "pentester" experiente procurando trabalho em uma entidade estabelecida.



H Pentester required Russian + ENG speaking
By Hortage, May 18 in [Job] - search, execution of work

Hortage
megabyte
●●●

Posted May 18 (edited)

We are looking for new people to join our team.
You should be able to access our targets.
Our targets are Tier 1 and specifically selected.
We do not work on mass .
Quality is our ultimate goal.
Sometimes we work on a target for several weeks and then we are successful.
You bring your own toolkit and experience.
We provide the infrastructure.
Payment is in %.
Leave your TOX ID in PM

Paid registration
+4
59 posts
Joined
04/03/19 (ID: 91777)
Activity
вирусология / malware

Edited May 18 by Hortage

Sophos X-Ops

Fig. 16. Uma quadrilha criminosa bem-estabelecida procura associados.

Infostealers

Serviços de roubo de informações são parte da estrutura de suporte da economia do malware – semelhantes, porém mais amplos, às ofertas “[qualquer coisa má]-as-a-service” que acabamos de enumerar. Graças às ofertas de malware-as-a-service e implantação-de-malware-as-a-service, os aspirantes ao crime cibernético podem começar com pequenos investimentos e sem muita perícia técnica, além das habilidades de saber se conectar a painéis de controle da Web e obter acesso a marketplaces de credenciais.

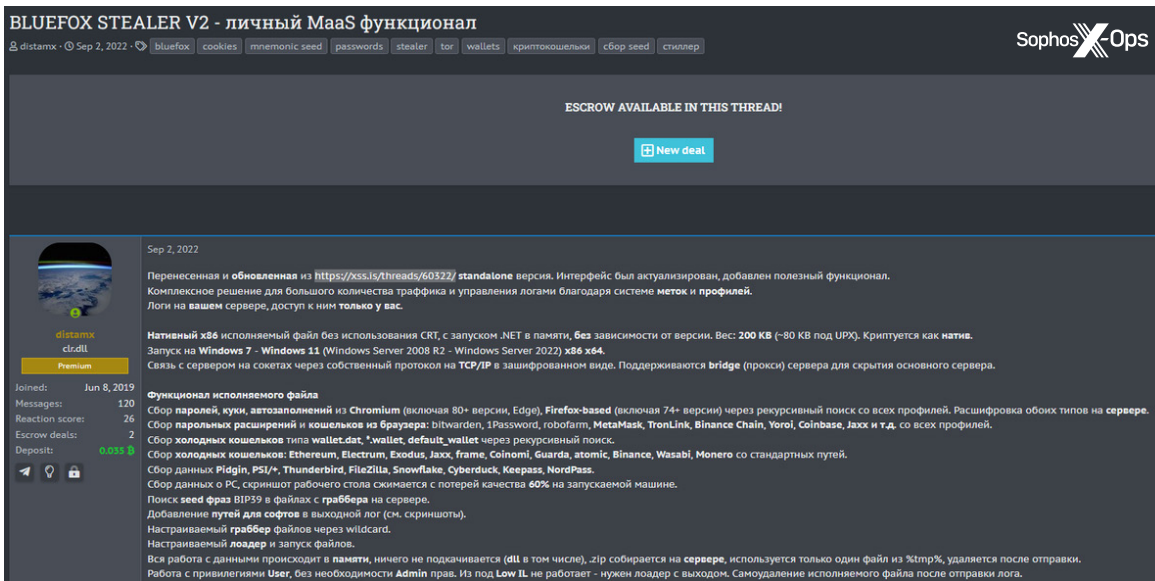


Fig. 17. Serviços de roubo de informações prosperam no ecossistema do crime cibernético para os menos especializados.

A organização empresarial do crime cibernético pode, assim, revender credenciais roubadas em diferentes marketplaces paralelos. Em alguns casos, essas credenciais são apenas subprodutos de informações, coletados nas transações de roubo de criptomoedas ou outros métodos de monetização de malware.

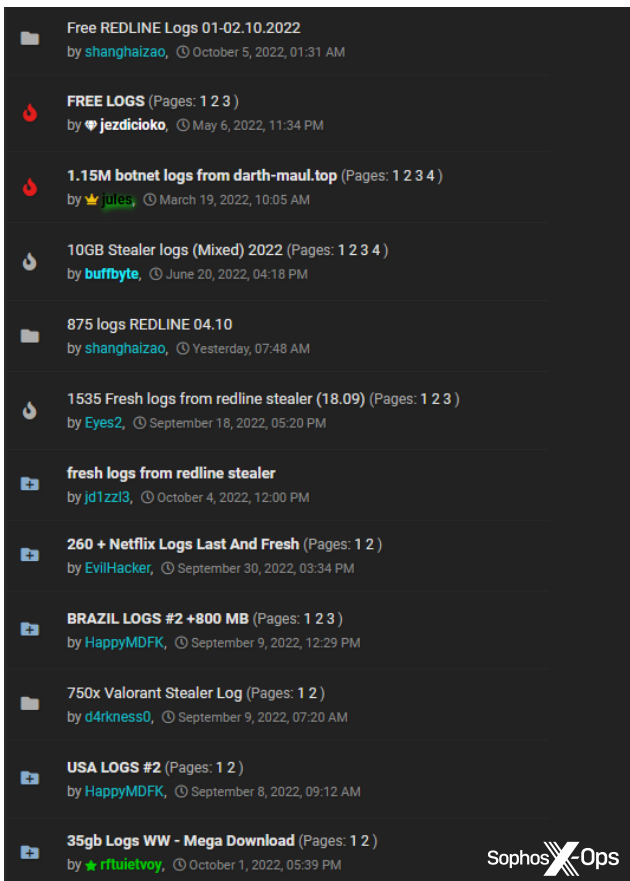


Fig. 18. “Logs” roubados, incluindo senhas e outras credenciais, à venda

Por fim, o ecossistema do infostealer está ciente de que os defensores estão interessados em seus feitos – e, como é de se esperar, vê uma oportunidade de lucro. Recentemente, um fórum clandestino, o XSS, [tentou](#) monetizar os esforços dos hackers white-hat a fim de aproveitarem ao máximo seu fórum oferecendo uma assinatura anual por US\$ 2.000 para acesso livre à sua coleção de dados.

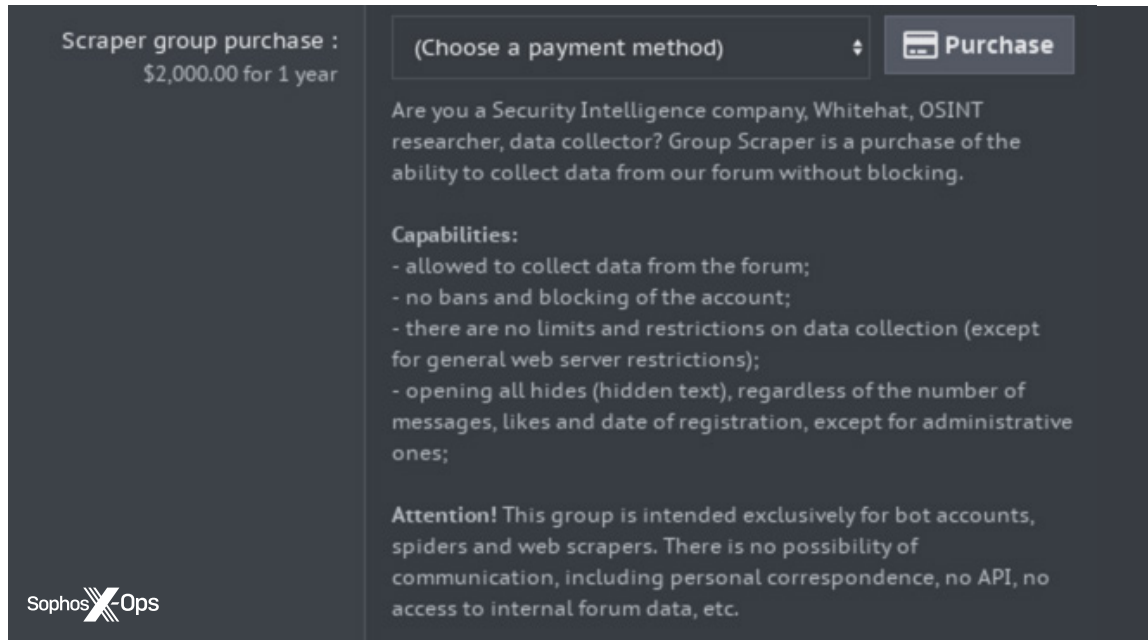


Fig. 19. Um fórum oferece acesso pago aos hackers blue-hat para monitorarem as atividades criminosas. [A segunda imagem mostra o texto traduzido do russo para o inglês.]

Malware para roubo de informações é um rótulo bastante abrangente. Ele inclui vários tipos de malware referenciados neste relatório, incluindo ferramentas de acesso remoto (RATs), keyloggers, “clippers” focados em criptomoedas e outros malwares que se apoderam de [credenciais](#), cookies de navegadores, transações de criptomoedas ou quaisquer outros dados que possam ser rapidamente roubados e vendidos ou reutilizados para outros fins maléficos.

Ladrões de informações forneceram os cookies Slack usados pela gangue Lapsus\$ para obter acesso à rede corporativa da Electronic Arts em 2021. Eles foram implicados em outras prováveis atividades mais recentes que se aproveitavam de tokens roubados de sessões a aplicativos da Web em acessos mais persistentes e nocivos – do comprometimento de sistemas de e-mail de pequenas empresas a ataques de ransomware.

Ladrões de informações rastreados por porcentagem de computadores exclusivos

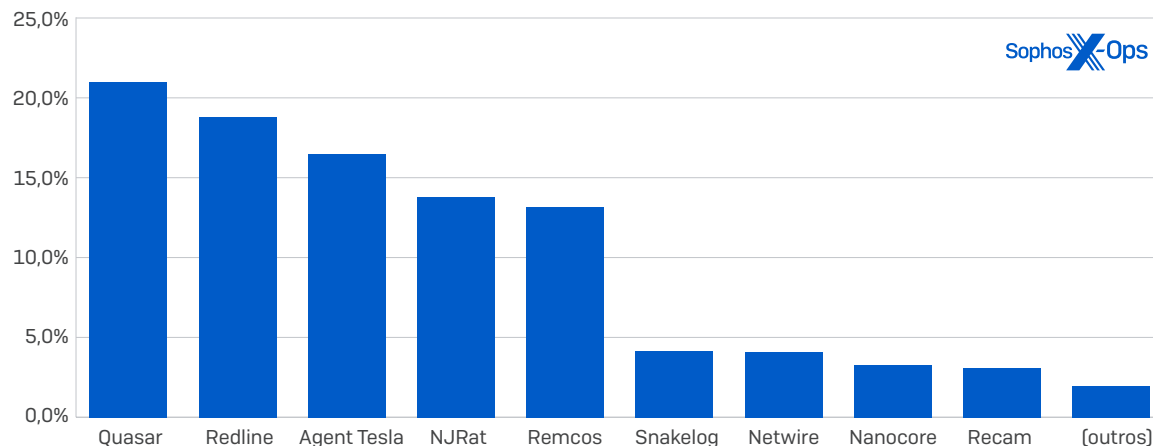


Fig. 20. Quasar, Redline e Agent Tesla são responsáveis pela maior parte dos malwares de roubo de informações descobertos: o Quasar foi encontrado em mais de um quinto dos computadores infectados durante um período de seis meses.

Os mais por dentro do espaço infostealer devem ter notado a ausência do famigerado Raccoon Stealer no gráfico acima. Após seu surgimento em 2019, esse malware direcionado ao Windows, que tinha sua base de operações na Ucrânia, parecia ter desaparecido temporariamente do cenário do crime no início de 2022 após uma ação conjunta do FBI com as autoridades holandeses e italianas, voltando à cena sob nova direção. Uma nova versão ainda em desenvolvimento foi lançada em junho, e o anúncio da nova versão concluída foi feito pelos autores no canal do Telegram em setembro. Entretanto, apesar da ampla divulgação sobre o seu relançamento, até agora vimos pouquíssimas instâncias do novo Raccoon Stealer. No fim de outubro, o Departamento de Justiça dos EUA [instaurou](#) uma ação formal acusando um ucraniano, atualmente sob custódia holandesa, por operar o serviço.

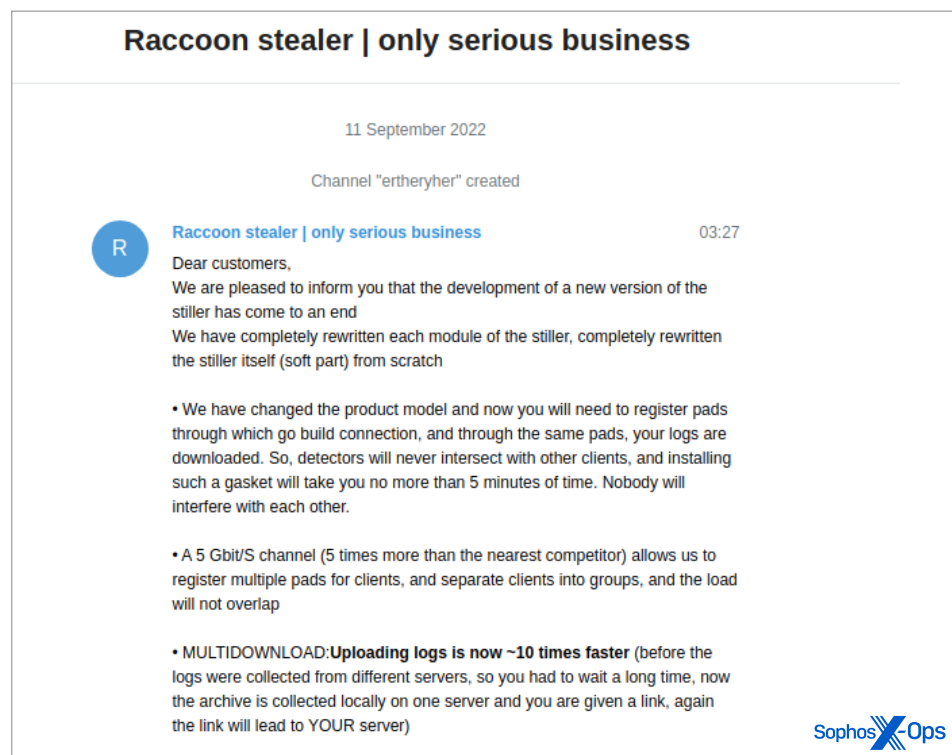


Fig. 21. Raccoon Stealer anuncia a sua nova versão no canal do grupo no Telegram em setembro.

Os ladrões de informações se propagam através de diferentes canais. Um dos mais comuns são as ofertas de downloader-as-a-service baseado em engenharia social, que induzem os usuários a baixar arquivos compactados ou imagens de disco supostamente contendo instaladores de softwares legítimos, em geral anunciados como versões "decodificadas" que burlam os esquemas de licenças. Os downloads também incorporam instaladores de vários pacotes de malware. Esses sites de download usam técnicas de otimização de mecanismos de pesquisa para colocá-los no topo das listas de pesquisa de softwares "crackeados". Outras formas de distribuição paga se dão através de botnets como Emotet ou Qakbot/Qbot.

Alguns ladrões, como o Agent Tesla, normalmente usam abordagens mais direcionadas, criando e-mails mal-intencionados direcionados um grupo específico de vítimas. Esses e-mails contêm anexos disfarçados de documentos urgentes, que são, na verdade, instaladores de malware.

Mas os ladrões de informações podem ser implantados de muitas outras formas mais direcionadas. A Sophos rastreou incidentes em que os invasores de uma rede usaram um backdoor implantado via Cobalt Strike para lançar um malware ladrão de cookies e outro malware ladrão de credenciais de dentro da rede. Foram feitas tentativas para coletar cookies de navegadores de sistemas que incluíam um servidor. Esses poderiam então ser usados para dar acesso, como usuários legítimos, a recursos na Web das organizações para incrementar os movimentos laterais.

A Sophos implantou várias medidas para bloquear os ladrões de informações e adicionou uma proteção contra o roubo de cookies para prevenir as tentativas de furtar informações dos cookies das sessões coletadas.

A evolução do ransomware

Ainda que alguns grupos de ransomware tenham se exaurido nos últimos anos, em parte graças a inquietações geopolíticas e alguns processos instaurados, novos grupos surgiram e a atividade de ransomware continua a ser uma das ameaças do crime cibernético mais presentes entre as organizações. Os operadores de ransomwares continuam a aprimorar suas atividades e mecanismos, tanto em termos de detecção quanto em incorporação de novas técnicas.

Alguns grupos de ransomware abarcaram o uso de novas linguagens de programação em um esforço contínuo de dificultar mais a detecção, transformar ransomwares em executáveis mais fáceis de compilar em diferentes sistemas operacionais ou plataformas, ou simplesmente porque as pessoas que desenvolvem cargas de malware incluem essas capacidades e ferramentas em suas proezas. A linguagem de programação Rust foi adotada pelos desenvolvedores dos ransomwares BlackCat e Hive, e o malware BlackByte foi codificado em Go (ou GoLang).

O ransomware mais predominante observado nos engajamentos do Sophos Rapid Response durante os primeiros dez meses de 2022 foi o LockBit, seguido de perto pelo BlackCat e Phobos. Mas observamos também que “outros” contribuiu com um quinto das famílias mencionadas, o que indica que o cenário do ransomware não se limita a apenas algumas poucas famílias em evidência. A distribuição é bastante similar à distribuição geral atual de ataques de ransomware em âmbito mundial.

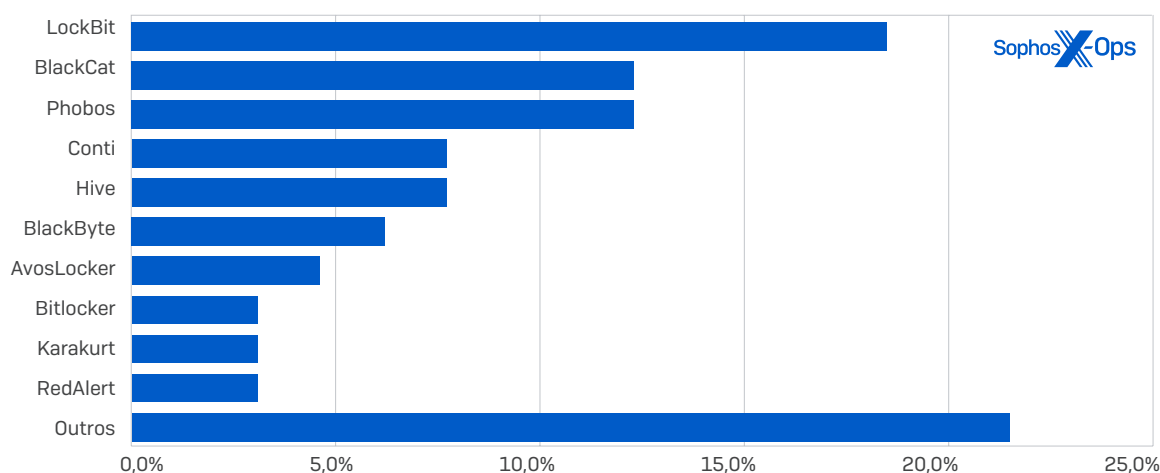


Fig. 22. Entidades de maior evidência, como LockBit, BlackCat e Phobos, são mais comuns, mas o âmbito geral do Response varia enormemente.

Assim como a diversidade de linguagens usadas, o ransomware também ampliou suas metas de ataque, se abrindo a outros sistemas além do Windows. O RedAlert, ou N13V, [criptografa servidores ESXi Windows e Linux](#), assim como o [Luna](#) (outra vertente de ransomware baseado no Rust). Mas não são apenas os da primeira linha que dão o tom: pesquisadores encontraram uma [variante Linux-ESXi do LockBit](#) no começo do ano. Mudanças nas plataformas na mira de ataque significa mais oportunidades para os agentes de ameaças: uma superfície de ataque maior, mais pressão nas vítimas e, potencialmente, menor risco de detecção, já que a maioria das medidas anti-ransomware foca no Windows. Veremos isso em maiores detalhes mais adiante neste relatório, quando abordaremos o cenário de ameaças às plataformas móveis, Linux e Mac.

Vimos também alguns desenvolvimentos em como os ransomwares são implantados em sistemas comprometidos. Dois incidentes de ransomware que a nossa equipe do SophosLabs analisou no início do ano – um que envolvia o Darkside e outro envolvendo o ransomware Exx – tratavam do uso abusivo de aplicativos até então benignos para [sideload de DLL](#). No caso do Darkside, o agente de ameaça usava um programa antivírus utilitário de limpeza; no caso do Exx, relacionava-se ao atualizador do Google. Após anos de popularidade em certos nichos de invasores, o sideload de DLL está se tornando rapidamente uma tática popular entre os agentes de ameaças, pois os ajuda a burlar a detecção ao executar cargas mal-intencionadas sob a forma de um processo legítimo.

Quanto à entrega e disseminação do ransomware, os agentes de ameaças continuam a improvisar e adaptar. Vimos também o [Impacket](#), uma coleção de módulos Python de código-fonte aberto que trabalha com protocolos de rede, sendo usado para explorar a movimentação lateral em redes comprometidas. O conjunto de ferramentas do Impacket inclui recursos para execução remota, sniffing de credenciais e scripts de despejo, exploits de vulnerabilidades

conhecidas e módulos de enumeração, fazendo dele um pacote atraente para os agentes de ransomware. Ele é, supostamente, uma ferramenta de testes legítima, mas, como o Metasploit e o Cobalt Strike, seus recursos e funcionalidades atraem clientes inescrupulosos. Nesse mesmo ritmo, encontramos também o Brute Ratel sendo usado na entrega de cargas, como mencionamos acima. O aumento no abuso pelos invasores de ferramentas de segurança legítimas [“dupla finalidade”] exige que a defesa seja meticulosa sobre o que tem em operação na rede (e por que) e quem tem direito a utilizar.

Grupos de ransomwares também parecem explorar oportunidades mais gerais, para diversificar suas operações. Um exemplo básico é o aumento no número de sites de vazamento, em que os agentes de ameaça publicam detalhes de suas vítimas. O modelo é bastante simples: se as organizações pagam, seus dados não são publicados online. Se não pagam, são publicados. Mas esse ano também apresentou fatos muito interessantes sobre isso.

Um dos grandes grupos de ransomware, o LockBit, se adiantou no assunto. O seu novo site de publicação de vazamentos, acompanhando o lançamento da nova versão do seu ransomware, [LockBit 3.0](#) (também chamado de LockBit Black, possivelmente porque muitas de suas funcionalidades e uma parte significativa de seu código parecem se basear no ransomware BlackMatter), contém algumas novidades. Por exemplo, um dos negócios visionários do grupo é oferecer aos visitantes, ou à vítima, a chance de destruir ou adquirir os dados roubados, ou estender o timer até a publicação.

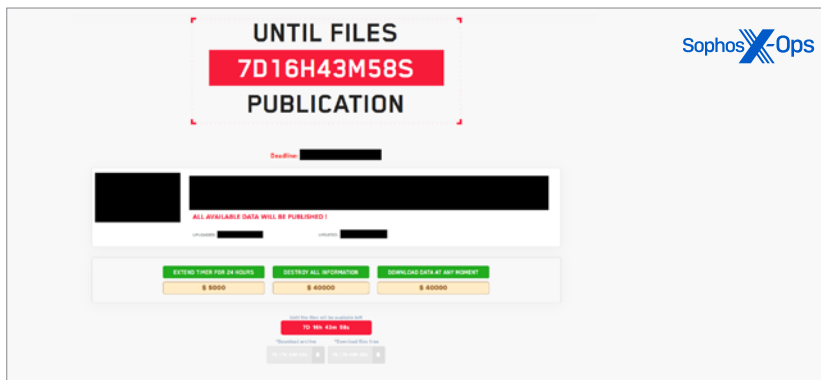


Fig. 23. Opções para estender o timer do ransomware, ou baixar (ou destruir) os dados, são apresentadas a uma vítima do LockBit.

Outros grupos de ransomware, como o Karakurt e o AvosLocker, pegaram carona nessa ideia, facilitando os leilões de dados roubados. E outros mais, como o Snatch, estão considerando mudar seus vazamentos de dados para um modelo por assinatura. Alguns sites injetam uma sutileza na visibilidade pós-descoberta: se a vítima pagar, a informação não só é mantida fora do alcance público, mas a violação em si também é mantida longe do conhecimento público (ou, se a situação da vítima tiver sido publicada em sites de vazamento, a notícia é removida) – o que faz da vítima um cúmplice na ocultação da atividade que, em muitos países, deve ser denunciada por lei.

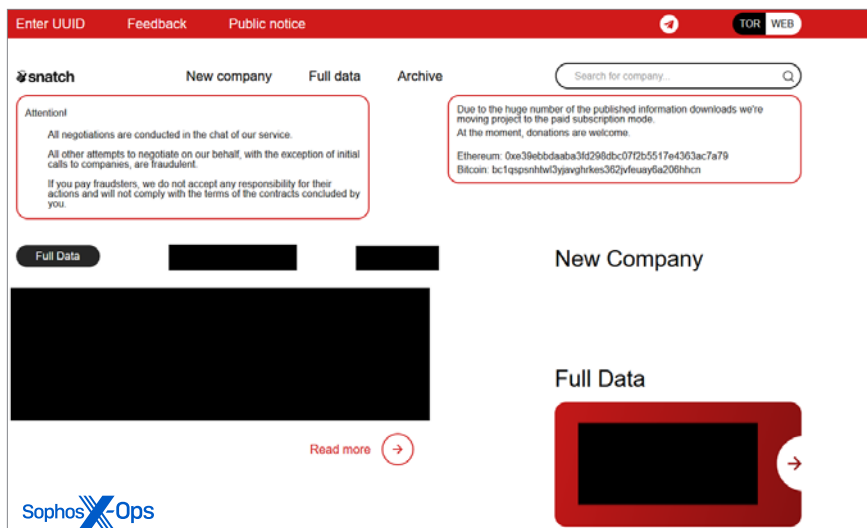


Fig. 24. O ransomware Snatch mudou para um modelo por assinatura.

Porém, o LockBit deu um passo à frente, inovando não apenas o seu produto de base, mas também suas interações e posicionamento na comunidade do crime. O seu novo site de vazamentos, por exemplo, oferece uma recompensa por bug, com valores que vão “de US\$ 1.000 a US\$ 1 milhão” para uma variedade de atividades, pretendendo, com isso, fortalecer seu serviço:

- Divulgação privada de bugs no seu site ou malware
- Um doxxing de sucesso do chefe do programa de afiliação do próprio LockBit, com detalhes sobre como foi feito, de modo que o LockBit possa reforçar seu OPSEC: esse leva o prêmio de um milhão
- Vulnerabilidades no programa de mensagens TOX (um pacote de mensagem instantânea muito usado pelos agentes de ameaças)
- Ideias para melhorar o ransomware LockBit
- Vulnerabilidades de divulgação de informações em seu domínio em camadas onion ou outros aspectos da rede TOR

O LockBit não é o primeiro agente de ameaças a oferecer recompensas por bugs – em novembro de 2021, All World Cards, um grupo proeminente que explora cartões de crédito, ativo em vários fóruns de crime cibernético no idioma russo, oferecia prêmios de até US\$ 10.000 por vulnerabilidades encontradas em seu repositório. E provavelmente não será o último. Esse é um método eficiente de crowdsourcing em pentests e avaliações de vulnerabilidades, além de assegurar que quaisquer descobertas fiquem entre o pesquisador e o agente de ameaça.

The screenshot shows a Telegram channel post from 'AW_cards' (RAM) dated Nov 9, 2021. The post announces a bug bounty program and lists vulnerability types and rewards. The channel has 138 messages and a reaction score of 124. The user 'Пользователь' joined on May 21, 2021, with a deposit of 0.27. The Sophos X-Ops logo is visible in the bottom right corner.

Nov 9, 2021

We are opening the bug bounty program!
List of vulnerability types and rewards:

Low risk bug

- Bug with displaying items
- Insufficient Authentication
- Session Prediction
- Directory Indexing
- Information Leakage

Reward: 10-100 usd

Medium risk bug

- Weak Password Recovery Validation
- Insufficient Authorization
- Content Spoofing
- XSS
- HTTP Response Splitting
- Predictable Resource Location
- Sensitive Data Exposure
- Path Traversal

Reward: 100-500 usd

High risk bug

- Abuse of Functionality

Reward: 500-1000 usd

Critical risk bug

- SQL Injection
- RCE
- File Inclusion (read, execute file)

Reward: 1000-10000 usd

If you want to inform us about the vulnerability, then you need to:

- 1) Type of vulnerability and its description
- 2) Instructions on how to reproduce this problem
- 3) Video demonstration of the vulnerability (fully replaying it)
- 4) Your login to our store.

Sophos X-Ops

Fig. 25. All World Cards revelou um programa modesto de recompensa por bugs no fim de 2021.

Notamos também alguns ransomwares ou grupos de vazamento bem menos conhecidos, diferentemente de seus companheiros mais famosos, que parecem ser motivados por questões políticas. Um deles é um site de vazamento de dados dedicado a compartilhar materiais obtidos da violação de cidadãos ucranianos e organizações governamentais, embora não esteja claro onde os dados se originam e se há ransomwares envolvidos.

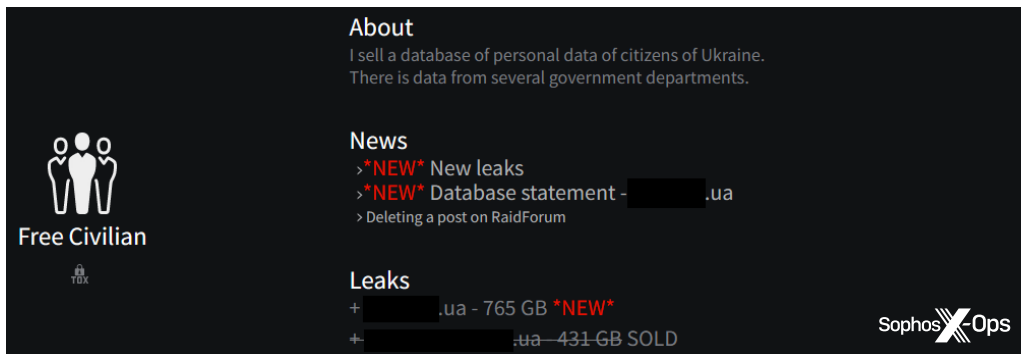


Fig. 26. Cidadãos ucranianos alvos de ataques com tendências políticas

Existe um grupo conhecido como Moses Staff, que parece ter as organizações israelenses sob a mira, com táticas semelhantes às de um ransomware, mas que não exige resgate.

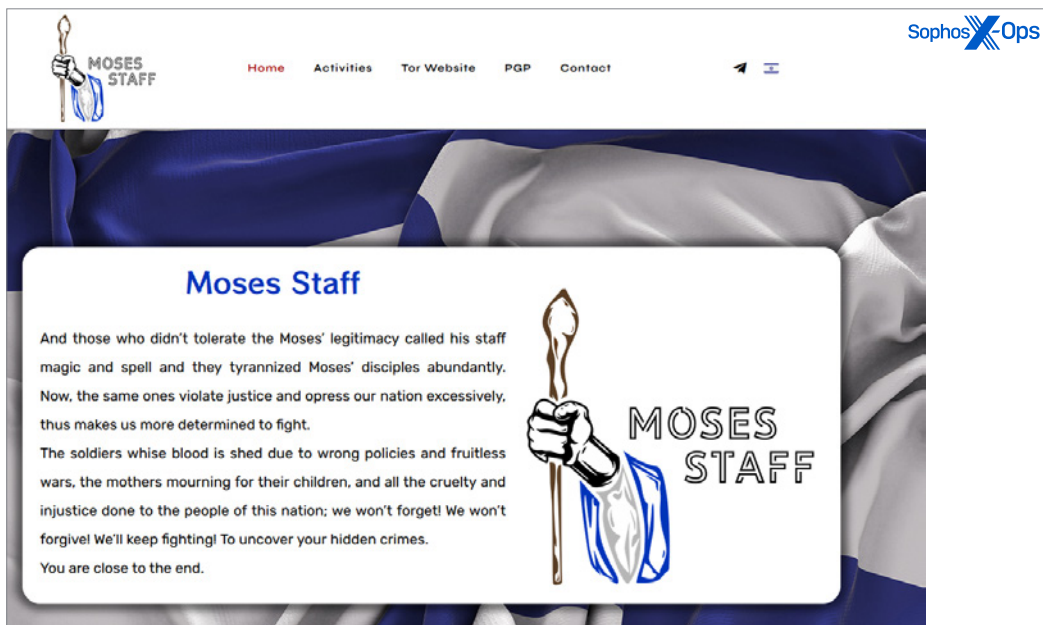


Fig. 27. Grupo anti-Israel usa táticas semelhantes a um ransomware para assediar

Ferramenta de ataque

Para a maioria das equipes de defesa, o “quem” é menos imediatista do que o “como” na hora de agir. Nesta seção, analisaremos as formas como os invasores estão subvertendo ferramentas de segurança ofensiva para os seus próprios fins. As ferramentas de pentest são ótimas candidatas ao abuso, mas não são as únicas ferramentas de segurança legítimas que estão sendo abaladas. Faremos aqui um breve levantamento sobre outras técnicas, incluindo o uso de ferramentas de acesso remoto (RATs) legítimas. Depois disso, traremos à sua atenção o aumento em “LOLBins” – uma técnica que usa indevidamente os binários já presentes nos sistemas sob ataque – e a recente virada no uso de outros drivers e DLLs legítimos de terceiros para inserir, sorrateiramente, códigos mal-intencionados. Por fim, passaremos um tempo falando sobre duas espécies de malware que achamos particularmente interessantes em 2022: o ransomware, que foca em upgrades de segurança de endpoints, e o software “miner”, que rouba recursos de máquina das vítimas para a criação de criptomoedas. Fecharemos nosso relatório com alguns destaques sobre o cenário de ameaças às plataformas móveis, Linux e Mac.

Levando as ferramentas de segurança ofensiva para o mau caminho

O mau uso de ferramentas de segurança ofensiva – softwares que são usados pelas equipes de segurança da informação para simular ataques ativos – é comum em muitas campanhas de ransomware. Como observamos no ano passado, as cópias piratas da ferramenta comercial de pentest Cobalt Strike têm sido cada vez mais usadas por adversários, como as afiliações de ransomwares. Ferramentas de código aberto desenvolvidas pela comunidade de segurança ofensiva – como a ferramenta de coleta de credenciais Mimikatz (versões que contabilizam quase dois quintos das detecções da ferramenta de ataque exclusivamente na telemetria da Sophos), outras ferramentas de exploração baseadas em PowerShell, como PowerSploit, e componentes “Meterpreter” conectados à plataforma de exploração desenvolvida parcialmente em código aberto, MetaSploit – permanecem o maior componente das detecções gerais de ferramentas de ataques.

Mas as cópias piratas das ferramentas comerciais de segurança ofensiva se tornaram uma parte comum de ataques mais complexos e profissionais. Como documentado acima, alguns grupos anunciam vagas de emprego para pessoas com habilidades nessas ferramentas. As cópias piratas do Cobalt Strike e a versão comercial do Metasploit ficaram tão comuns que links para cópias gratuitas são frequentemente publicados em sites clandestinos (ainda que, em alguns casos, possa ser, de fato, um malware).

The screenshot shows a forum post from a user named 'sommerdev' on a platform with a Sophos X-Ops logo. The post title is 'cobalt strike 4.7 cracked version chinese version'. The user's profile shows they are a 'Пользователь' (User) with a registration date of 05.12.2021, 73 messages, and 28 reactions. The post content is a screenshot of a file manager interface with a table of files:

名称	修改日期	类型	大小
cobaltstrike			1 KB
cobaltstrike.auth			1 KB
cobaltstrike.jar			69,537 KB
cobaltstrike.store			3 KB
cobaltstrike-client.jar			33,696 KB
ddosi.org.bat			1 KB

The file 'ddosi.org.bat' is highlighted with a red box in the original image.

Fig. 28. Uma versão em chinês do Cobalt Strike 4.7 foi decodificada e revendida.

The screenshot shows a forum post from a user named 'nX3' on a platform with a Sophos X-Ops logo. The post title is 'other Metasploit PRO 20220928'. The user's profile shows they are a 'CD disc' user with a registration date of 02.10.2022. The post content includes a date '02.10.2022', the text 'Trial is not required. Release from Pwn3rzs', and a 'Download' link.

Fig. 29. A versão paga do Metasploit é pirateada e oferecida para download.

O Cobalt Strike marcou presença em 47% dos incidentes com clientes que a equipe Rapid Response da Sophos teve que lidar durante os primeiros três trimestres de 2022. A grande maioria deles estava relacionada a ransomwares, ou eram atividades “pré-ransomware” em que os agentes de ameaças foram detectados usando técnicas, ferramentas e práticas associadas a ataques de ransomware iminentes. Mas o Cobalt Strike também foi observado como parte de ataques voltados ao Estado, como na campanha da SolarWinds de 2020 e em ataques a alvos na Ucrânia por agentes aliados da Rússia.

O Cobalt Strike sozinho foi responsável por 8% de todas as detecções desse tipo por ferramentas de ataque. Além disso, seu protocolo de comunicação foi incorporado a outras ferramentas desenvolvidas pelos invasores. O TurtleLoader, por exemplo, tem versões que se conectam à sua rede de comando e controle (C2) através do protocolo de conexão do Metasploit ou do Cobalt Strike. Esses manipuladores multiferramentas apresentam desafios interessantes no âmbito de defesa, especialmente porque diferentes camadas dessa defesa estão engajadas na proteção contra ataques.

Há sempre mais a se esperar. Enquanto este documento era escrito, por exemplo, vimos ataques envolvendo a ascensão do Brute Ratel no placar de disponibilidade dos novos kits de ferramentas de ataque; quando o documento estava pronto para publicação, as detecções do Brute Ratel eram um mero ponto no radar, aparecendo em menos de 1% de nossas detecções em memórias. Isso certamente mudará em 2023, com a proliferação em violações do produto.

Detecções mais marcantes de ferramentas de ataques (computadores exclusivos durante um período de 6 meses)		
Ferramenta de ataque	Porcentagem de computadores infectados	Observações
Mimikatz	24,7%	Utilitário de despejo de credencial pós-exploração de código aberto
Apteryx	14,5%	Uma versão compilada do Mimikatz
PowerSploit suite	11,7%	Código aberto; sem suporte oficial desde agosto de 2020
SrpSuite	8,3%	PowerShell Suite de código aberto pela FuzzySecurity
Cobalt Strike	8,0%	Software proprietário, geralmente pirata/"craqueado"
Meterpreter	7,8%	Carga de ataque Metasploit de código aberto; suporte comercial disponível
Nishang	6,8%	Estruturas e scripts/cargas para uso com o PowerShell
TheFatRat	6,2%	Automação de carga/backdoor do Metasploit de código aberto
TurtleLoader	5,4%	Backdoor, normalmente visto em conjunto com o Metasploit ou Cobalt Strike
JMeter	5,1%	Metasploit baseado em Java
Juicy Potato	5,0%	Exploit BITS de código aberto (ferramenta de escalonamento de privilégio)
winPEAS	4,8%	Scripts de roubo de informações e escalonamento de privilégio
Swrort	4,6%	Backdoor baseado em Metasploit
Empire	4,5%	Estrutura pós-exploração de código aberto; fusão do PowerShell Empire e Python EmPyre; sem suporte oficial desde julho de 2019

Fig. 30. A porcentagem de computadores infectados analisados pela Sophos em que o nome da ferramenta estava presente, acompanhada de mais informações sobre as ferramentas. Dados extraídos em um período de seis meses (abril a setembro de 2022), e as ferramentas detectadas em menos de 4,5% de máquinas exclusivas foram omitidas devido ao espaço.



Até setembro de 2022, o desenvolvedor do Brute Ratel dizia ter firme controle do acesso da ferramenta através da provisão de licenças. Ainda assim, os agentes associados ao conluio do ransomware Conti parecem ter criado empresas falsas para adquirir a plataforma, e houve pelo menos um caso de uma licença que vazou para um funcionário de um cliente legítimo. Em setembro, cópias piratas de uma versão recente do Brute Ratel estavam amplamente disponíveis nos marketplaces paralelos.

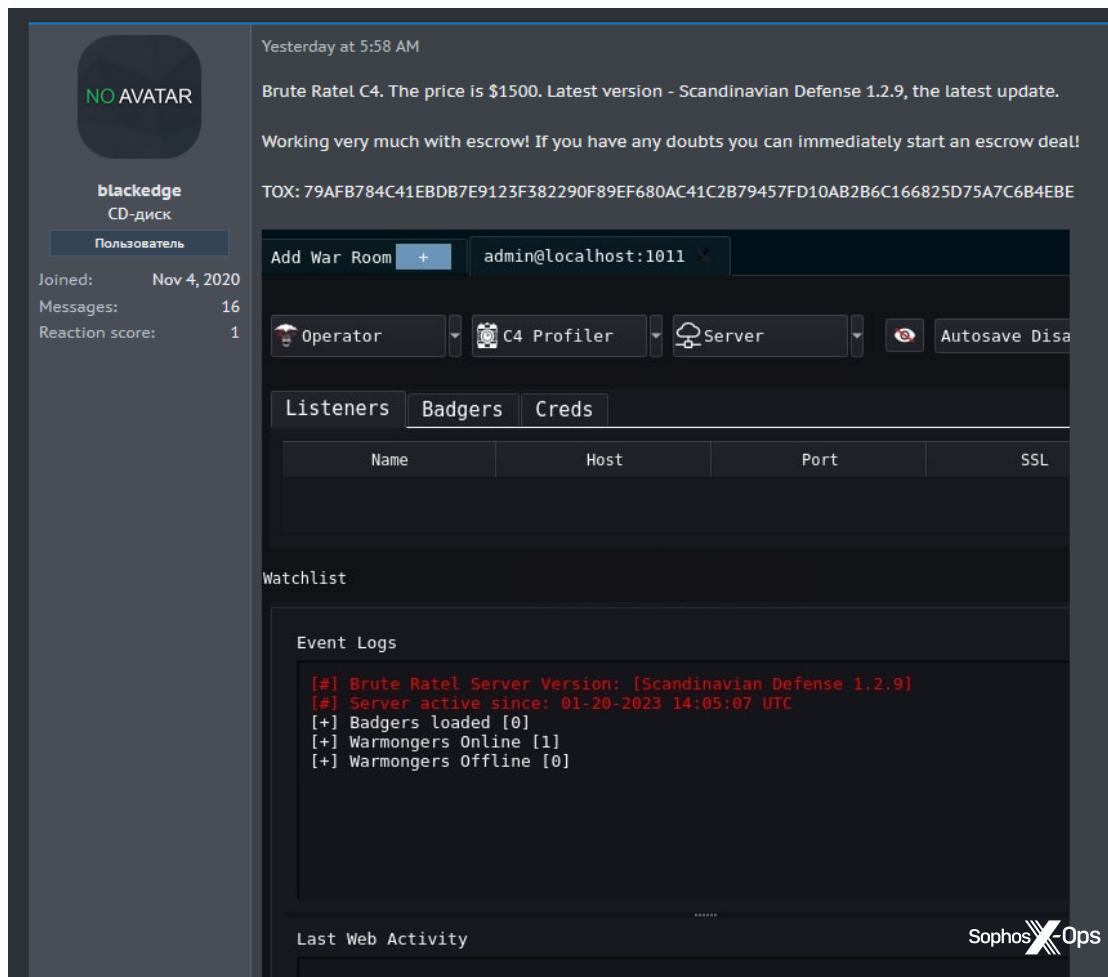


Fig. 31. Uma versão "craqueada" do Brute Ratel estreia no mercado clandestino.

Até agora, documentamos alguns poucos ataques associados a componentes do Brute Ratel. Durante a triagem de um incidente realizada pelo Sophos MDR, observamos os invasores tentando inicialmente usar o Cobalt Strike. Quando o Cobalt Strike foi detectado e bloqueado, os adversários tentaram implantar o Brute Ratel – que também foi bloqueado.

Mas outros incidentes assim são altamente prováveis. Talvez devido à grande disponibilidade do Brute Ratel, pesquisas recentes descobriram agentes do Brute Ratel sendo disseminados pelo [Qakbot](#), como aconteceu com a disseminação de beacons do Cobalt Strike que ocorreu no passado.

Outras ferramentas de segurança exploradas pelo uso indevido

O Brute Ratel não tem nada de especial em termos de ter sua intenção maléfica “reformulada”: os agentes de ameaças também recebem várias ofertas de ferramentas de segurança legítimas à venda nos marketplaces do crime. Alguns exemplos incluem o Core Impact, uma estrutura de pentest; o Nexpose, um scanner de vulnerabilidades; o VirusTotal Enterprise, e o Carbon Black, uma plataforma de proteção de endpoint.

VirusTotal Enterprise(Downloader)
by mbrk256 - Wednesday September 28, 2022 at 12:48 PM

September 28, 2022, 12:48 PM (This post was last modified: September 28, 2022, 02:31 PM by mbrk256.)

I'm selling software that provides VirusTotal Enterprise with an annual fee of \$10,000.

You can download any file in virustotal you want using this software.

Using the software is quite simple. You just need the virustotal scan result link.

Usage Video:

virustotal-enterprise
Powered by **dailymotion**

Pricing:
\$400 annual license
\$1.200 unlimited license
\$6.000 exploit

Contact for purchase:
Telegram: @mbrk256

It has support for Windows, Linux and MacOS.
Exclusive to the Breached Forum: 3 days license free to the first person who posts in the thread.

Fig. 32. VirusTotal Enterprise na mira dos sucateiros de dados

Os casos de uso de agentes de ameaças dessas ferramentas perfeitamente legítimas variam: eles podem ser dissecados do EDR e plataformas de proteção de endpoints para testar vulnerabilidades e táticas de evasão, varreduras automáticas de vulnerabilidades e exploração com teste de penetração e estruturas de exploit, e obter amostras de malware e contra-inteligência através de ferramentas como o VirusTotal.

RATs com dupla finalidade

Na crescente e ampla estrutura de uso inapropriado ou abusivo das ferramentas de segurança no cenário das ameaças, vale uma especial menção às ferramentas de acesso remoto. A frequência com que essas ferramentas legítimas são transformadas em ferramentas ilegítimas – um exemplo da toxicidade da “dupla finalidade” – exige que a defesa se mantenha em alerta constante, buscando indícios de abuso e comportamentos questionáveis.

Ferramentas de acesso remoto são usadas para estabelecer uma conexão persistente a sistemas comprometidos dos quais lançar os ataques. Algumas das ferramentas de acesso remoto mais proeminentes são:

- NetSupport Manager [NetSupport]
- TeamViewer Remote Access [TeamViewer]
- ConnectWise Control / Screenconnect Remote Access [ConnectWise]
- AnyDesk [AnyDesk Software]
- Atera [Atera Networks]
- Radmin [Famatech]
- Remote Utilities [Remote Utilities]
- Action1 RMM [Action1]

Essas ferramentas podem ser implantadas pelos próprios invasores, ou por intermediadores de acesso que vendem acesso persistente a redes comprometidas. Alguns criminosos cibernéticos solicitam abertamente o acesso de vítimas através dessas ferramentas nos sites clandestinos:

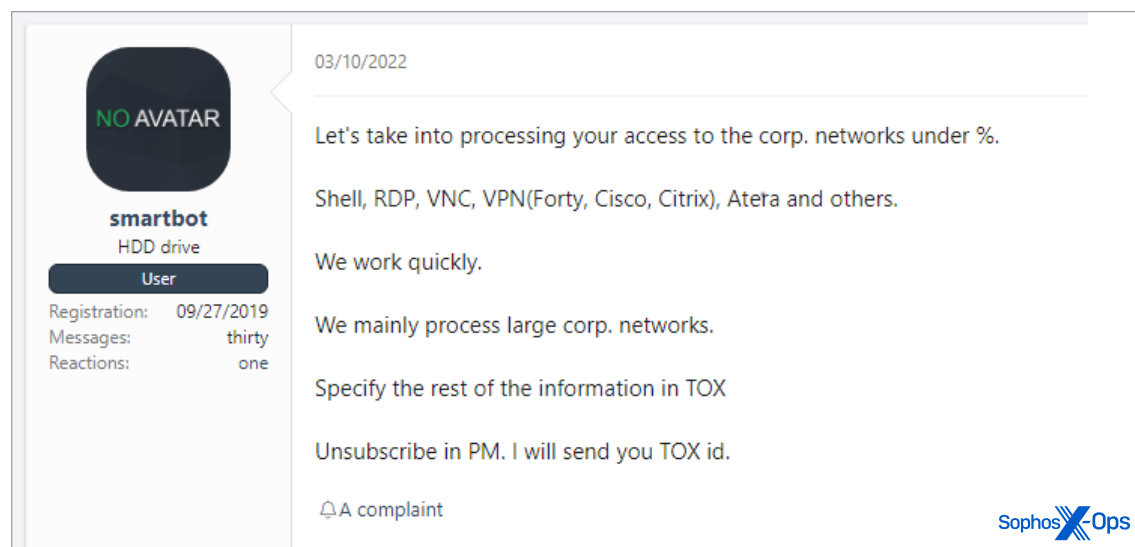


Fig. 33. Oferta de acesso a redes comprometidas via ferramentas comprometidas

O Atera foi detectado como parte de várias investidas investigadas pela Sophos, incluindo uma série de tentativas de implantação de malwares que se aproveitavam da vulnerabilidade Log4J, e em vários casos de ransomware investigados pelo Sophos Rapid Response. Nas tentativas de exploração do Log4J, que focavam nos servidores VMWare Horizon, os invasores tentaram executar um script remoto do PowerShell para baixar e instalar silenciosamente um agente do Atera com uma licença de avaliação (juntamente com outra ferramenta legítima de acesso remoto que fora explorada, o Splashtop Streamer). Nos incidentes registrados pelo Rapid Response, as instalações do Atera foram concretizadas explorando servidores Microsoft Exchange vulneráveis. Os agentes do ransomware BlackCat exploram o uso do TeamViewer e AnyDesk em incidentes recentes investigados pelo Rapid Response.

Em muitos casos, esse uso abusivo de ferramentas legítimas pode ser detectado e bloqueado em contextos anômalos, como eventos de instalação anormais (por exemplo, uma versão do NetSupport instalada pelo PowerShell em uma diretório irregular). Além desses, a exploração dessas ferramentas pode ser detectada em alguns casos pela utilização de uma licença de avaliação para implantação. A Sophos implantou regras de comportamento que detectam o uso indevido da licença de avaliação do Atera e continua a desenvolver detectores de comportamento para indicar o abuso desse e de outros pacotes de acesso remoto.

LOLBins e executáveis legítimos

Uma característica importante nos ataques de adversários ativos, bem como em alguns ataques totalmente automatizados, é o uso de “binários living off the land” ou LOLBins. Esses componentes Windows nativos são aproveitados por invasores para executar comandos de sistema, burlar recursos de segurança predefinidos, baixar e executar arquivos remotos maliciosos, e mover-se lateralmente pelas redes.

Esse importante LOLBin, o shell de comando do Windows (cmd.exe), é usado pela maioria dos backdoors e shells para executar comandos de sistema e lançar malwares, de modo que está presente, de alguma forma, em praticamente todo ataque de malware. Cada uma dessas plataformas de script do Windows – PowerShell, o Host de Aplicativo HTML da Microsoft (mshta.exe) e o Windows Scripting Host (wscript.exe) – são usadas como ferramentas para executar chamadas de API do Windows, baixar e executar outros conteúdos maliciosos, executar comandos de sistema e coletar dados. Além disso, o PowerShell é usado por muitas das ferramentas de ataque utilizadas pelos criminosos cibernéticos.

Outro componente do Windows usado frequentemente de modo indevido, o rundll32.exe, é muitas vezes recrutado pelos agentes de ransomware para carregar malwares lançados em formato de biblioteca de vínculo dinâmico (DLL). Mas há outros executáveis legítimos assinados que podem ser explorados de modo semelhante e que são incorporados à tarefa de execução de um backdoor ou ransomware.

Já outros LOLBins não são tão óbvios. O utilitário de certificação do Windows (certutil.exe), que pode recuperar conteúdo de servidores da Web remotos, é frequentemente usado indevidamente por operadores de ransomwares e outros criminosos cibernéticos para baixar e decodificar arquivos mal-intencionados. O Bitsadmin.exe, um utilitário de linha de comando do Background Intelligent Transfer Service, é usado para mover arquivos de/para/em uma rede visada sem exigir o processo que deu início à ativação da transferência, fazendo dele um acessório ideal para a movimentação lateral de um malware ou para a exfiltração de dados.

Esse tipo de comportamento pode ser detectado e bloqueado de diversas maneiras. O comportamento mal-intencionado usando o PowerShell e outros mecanismos de script pode ser detectado pelo monitoramento da Interface de Verificação de Antimalware (AMSI) da Microsoft. Análises comportamentais de execução dos LOLBins através de chamadas de sistema ou de uma linha de comando podem também detectar esse abuso.

Dez principais LOLBins por porcentagem de computadores afetados		
LOLBin	Porcentagem de detecções brutas	Observações
cmd	92,26%	Interpretador de comando padrão
powershell	1,79%	Shell de script e linha de comando mais avançado
certutil	1,09%	Programa de linha de comando instalado como parte do Certificate Services
mshta	1,01%	Host de Aplicativo HTML da Microsoft, permite a execução de .HTA (aplicativo HTML)
bitsadmit	0,95%	Background Intelligent Transfer Service, usado como parte do Windows Update para a transferência de arquivos
wscript	0,93%	Windows Scripting Host suporta a execução de JScript e VBScript
bcdedit	0,83%	Ferramenta de linha de comando para gerenciar Boot Configuration Data
rundll32	0,52%	Usado para carregar e executar bibliotecas de vínculo dinâmico (DLL) de 32 bits
nltest	0,39%	Ferramenta que fornece informações de diagnóstico
procdump	0,21%	Aplicativo de linha de comando que oferece informações sobre processos de sistema

Fig. 34. O ubíquo cmd.exe é, com certeza, o LOLBin geral mais explorado nos sistemas Windows (abril a setembro de 2022).



Vulnerabilidades “Bring your own”

À parte dos LOLBins, outros executáveis legítimos são frequentemente usados como peça nos ataques de ransomware e outros crimes cibernéticos; nesses casos, os aplicativos usados indevidamente são trazidos pelo invasor. Em alguns casos, são executáveis vulneráveis que podem ser usados no sideload de códigos mal-intencionados. Esse foi o caso ocorrido com um componente arcaico assinado pela McAfee usado em um ataque do ransomware AtomSilo no [ano passado](#) para implantar o backdoor Cobalt Strike.

Outra versão desse método é a técnica “Bring Your Own Vulnerable Driver”, que se aproveita de um driver assinado legítimo com uma vulnerabilidade explorável para dar acesso de baixo nível ao sistema operacional. Por exemplo, os pesquisadores da Sophos [descobriram](#) que os agentes que exploraram o ransomware BlackByte usaram indevidamente o RTCore64.sys e o RTCore32.sys, drivers usados pelo utilitário de overclock da placa gráfica Micro-Star MSI AfterBurner 4.6.2.15658, que é amplamente utilizado. Uma vulnerabilidade nesses drivers (CVE-2019-16098) permite que um usuário autenticado leia e grave na memória arbitrária, que, nesse caso, foi usada para burlar e desabilitar alguns softwares de segurança.

Outros incidentes recentes de implantação da técnica Bring Your Own Vulnerable Driver incluem um invasor desconhecido que explorou um driver anti-cheat vulnerável do jogo Genshin Impact, em julho, e um relato, em maio, de uma variante do ransomware AvosLocker que explorou um driver anti-rootkit vulnerável da Avast. Nos dois casos, os [drivers foram explorados](#) para burlar ou encerrar o software de segurança.

Em síntese, nossa equipe do Rapid Response observou atividades suficientes que desvendam um grande número de indícios que advertem que um ataque de ransomware pode estar a caminho. Em uma pesquisa sobre resposta a incidentes realizada nos primeiros nove meses de 2022, pelo menos 83% dos ransomwares foram precedidos por algum tipo de indicação de que havia algum problema. Os cinco presságios mais comuns de um ataque de ransomware, e suas classificações MITRE ATT&CK, são:

- ▶ **T1003** – Acesso a credenciais – Despejo de credencial de SO
 - Despejo de credenciais, em texto não criptografado ou com hash, para obter informações de credenciais e login da conta do software e sistema operacional de destino
- ▶ **T1562** – Evasão de defesas – Prejudicar as defesas
 - Modificar ou desabilitar componentes de um ambiente da vítima a fim de burlar ou desacelerar as ações de defesa já em vigor, incluindo medidas preventivas e recursos de auditoria/log
- ▶ **T1055** – Escalonamento de privilégios – Injeção do processo
 - Injetar código em espaços de endereço de processos confiáveis, permitindo que o código do invasor burle as defesas e/ou eleve seus privilégios; pré-carregamento ou sideload de DLL entram nessa categoria
- ▶ **T1021** – Movimento lateral – Serviços remotos
 - Usar serviços remotos via contas válidas/sem proteção para fazer login em um sistema e desempenhar ações como se fosse o usuário conectado, talvez usando um RAT ou um RAT com dupla finalidade, como descrito acima
- ▶ **T1059** – Execução – Interpretador de comandos e scripts
 - Uso indevido de interpretadores de comandos e scripts para executar comandos, scripts, de binários, ou via terminais interativos ou shells, ou via serviços remotos, como acima

Alguns outros padrões encontrados, ainda que não precisamente categorizados, de interesse para os profissionais:

- ▶ 64% dos ataques de ransomware (especificamente, a implantação do ransomware) começou entre as 22h e as 6h, horário local
- ▶ O período mais comum do início dos ataques foi nas noites de segunda-feira/manhãs de terça-feira, durante o “turno da noite”
- ▶ A exfiltração precedeu a fase de demandas do ransomware em aproximadamente duas horas
- ▶ O tempo médio de permanência do invasor foi de 11 dias

Ransomwares têm como alvo upgrades de segurança de endpoints

Na lista de presságios de ataques de ransomwares acima, o ponto “T1562 – Evasão de defesas – Prejudicar as defesas” vale um pouco mais de escrutínio. Um acontecimento que foi mais predominante nos engajamentos do Rapid Response em 2022 abrange o sucesso da Sophos em impedir que os ransomwares causem danos e o reconhecimento desse sucesso pelos grupos de ransomwares dominantes e seus afiliados. Os ataques de ransomware, agora envolvem habitualmente, como um precursor à implantação do malware de criptografia, tentativas de acesso a controles administrativos que gerenciam a postura de segurança do alvo.

Como descrito em uma seção anterior, “adversários ativos” do ransomware – as pessoas que se engajam em atividades práticas durante um ataque – comumente usam ferramentas de extração ou de sniffing de senhas na intenção de capturar credenciais administrativas. Agentes de ameaças usam indevidamente utilitários como o Mimikatz – originalmente criados como uma ferramenta para melhorar a segurança – para detectar e extrair senhas de usuários de redes sob ataque.

Anteriormente, essas senhas administrativas eram utilizadas para controlar as ferramentas de gerenciamento (como controladores de domínio do Windows) que os invasores podiam aproveitar para implantar o ransomware. Mas em ataques mais recentes, os invasores estão usando cada vez mais essas credenciais para acessar os controles centrais usados para gerenciar a proteção de segurança de endpoint. Em alguns casos, os invasores usaram imediatamente essas credenciais roubadas para se conectarem às ferramentas de gerenciamento central e desativar os recursos de proteção contra adulteração nas ferramentas de segurança de endpoint ou, em alguns casos, para desabilitar totalmente a segurança de endpoint.

Para frustrar esses tipos de ataques, a Sophos e outras empresas adicionaram recursos de autenticação multifator (MFA) às páginas de login no painel de gerenciamento e também aos dispositivos físicos, como firewalls, que têm logins administrativos. Mas os usuários finais desses produtos – administradores de TI e segurança – precisam habilitar esses recursos e se registrar para usá-los antes que possam ser eficientes para bloquear os agentes de ameaças. A Sophos recomenda a todos os seus clientes que habilitem essas proteções assim que possível.

Malware Miner

Softwares de mineração de criptomoedas consomem capacidade de computação para desempenhar o trabalho criptográfico na esperança de produzir novas “moedas” (tokens), normalmente operando como parte de um pool de processadores ou computadores em rede. Para muitas criptomoedas, a mineração requer hardware especializado com unidades de processamento gráficas dedicadas para o trabalho pesado. Mas ainda assim há oportunidades para explorar o hardware para fazer a mineração de criptomoedas – e há uma vastidão de bots de mineração que se associam na autodisseminação que continua tentando explorar sistemas vulneráveis e roubar a capacidade de processamento para o seu benefício.

Tais malwares não impactam os dados das organizações, mas os recursos computacionais absorvidos são extremos, e o consumo de energia elétrica e os custos de refrigeração são enormes. O malware Miner é em geral o precursor dos malwares, pois é geralmente implantado via redes facilmente exploráveis e vulnerabilidades de software.

A maioria dos malwares mineradores se concentra no Monero (XMR), por várias razões. O tipo de trabalho exigido para produzir XMR não necessariamente requer placas gráficas especializadas, o que significa que pode ser minerado com servidores que não têm muitos recursos gráficos em termos de hardware. Além disso, o XMR é menos rastreável do que muitas outras criptomoedas, tornando-o mais atraente para as atividades criminosas.

Esses robôs mineradores são, frequentemente, o primeiro malware a explorar as vulnerabilidades recém-publicadas. A vulnerabilidade Log4J do Java e os exploits ProxyLogon/ProxyShell do Microsoft Exchange Server foram rapidamente explorados pelos botnets mineradores. Em muitos dos casos de ransomware abordados pelo Rapid Response, o pessoal de resposta da Sophos encontrou indícios do malware minerador usando o mesmo ponto de comprometimento inicial que o ransomware – e, em alguns casos, meses antes do ataque de ransomware.

Os mineradores também são um problema em diferentes plataformas. Vários malwares de robôs mineradores que a Sophos detecta são baseados em Windows (e se utilizam do PowerShell e de outros mecanismos de script do Windows para instalação e persistência), porém também há versões para Linux desses botnets, geralmente direcionados a servidores da Web e dispositivos de rede sem patches.

Ainda que os mineradores XMR se mantenham predominantes e populares, as flutuações (na sua maioria negativas) no valor de algumas criptomoedas afetaram os operadores de mineradores. Como o valor do XMR caiu, a lucratividade dos botnets mineradores diminuiu, o que parece ter tido um impacto no empenho que os operadores de robôs dedicam para aumentar seus pools de mineração. Algumas flutuações nas taxas de detecção de implantações de mineradores acompanharam as flutuações no valor do XMR, como mostrado abaixo. Observe, em particular, a queda registrada em meados de junho tanto no valor do XMR quanto no número de detecções de mineradores.

Detecções do Monero Miner e as flutuações de preços, de abril a setembro de 2022

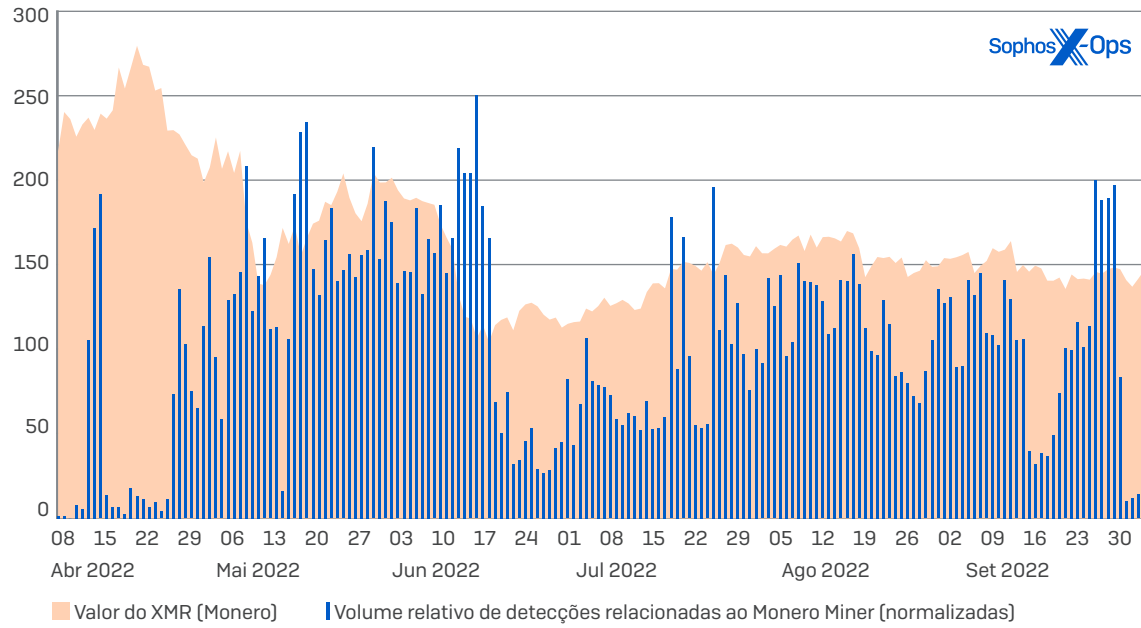


Fig. 35. Detecções do Monero no último ano (em azul no gráfico, totais normalizados) mostram uma certa coerência com os valores do Monero durante o período (em laranja).

Mas a lucratividade dos mineradores é afetada não apenas pelo valor da moeda que mineram, mas pela longevidade do minerador. Em verdade, muitos saem à caça e removem mineradores semelhantes dos servidores que exploram. Em alguns casos, os mineradores chegam a implantar patches para corrigir as vulnerabilidades que usaram na instalação na intenção de impedir que outros mineradores os suplantem, o que lhes permite persistir quando as organizações fazem a varredura em busca de sistemas vulneráveis.

Para além do Windows: o panorama das ameaças móveis, Linux e Mac

Até agora, falamos principalmente sobre ferramentas de malware e ataques que afetam o Windows – o que é de se esperar, considerando a proeminência do Windows como alvo de ataques pela maioria dos invasores. Contudo, o Windows não é o único alvo viável no negócio, e ouvimos falar cada vez mais de campanhas de ataque com cargas “com suporte” multiplataforma. Elas são desenvolvidas usando linguagens com suporte multiplataforma, como Go ou Python (geralmente encapsuladas em pyinstaller), ou estruturas como Electron; ou também em binários criados em estruturas mais populares. Nesta seção final, transcorreremos rapidamente o panorama de plataformas móveis, Linux e Mac, lembrando que muitos dos mineradores estão presentes nessas e em outras plataformas.

Ameaças ao Linux

Os sistemas Linux têm sido um alvo de longa data de serviços que, frequentemente, são implantados no sistema operacional, incluindo sites organizacionais, servidores de máquinas virtuais, dispositivos de rede, servidores de repositório e infraestrutura de aplicativos corporativos. Os criminosos estão desenvolvendo cada vez mais ransomwares multiplataforma e outros malwares para permitir-lhes explorar com mais afinco seus recursos lucrativos. Nos primeiros seis meses depois que a Sophos revelou suas proteções voltadas para Linux, detectamos 14 servidores Linux individuais atacados por ransomwares.

A maioria dos malwares que afetam os sistemas Linux (bem como outras plataformas de servidores) é desenvolvida para minerar criptomoedas. Mais de 40% de todas as nossas detecções, e 72% dos dispositivos Linux detectados com malware, são resultado de mineradores.

Ameaças ao Linux por percentagem de detecções Linux		
Ameaça	Porcentagem de detecções	Observações
Minerador	43,0%	Detecção de minerador genérico
DDoS	27,1%	Detecção relacionada ao Mirai
Tsunami	12,3%	Cliente DDoS baseado em IRC
Gognt	11,5%	Detecção genérica de malware codificado em Go
Rst	1,3%	Vírus infectante há vinte anos
Loit	1,1%	Exploração local
Swrort	0,9%	Mettle (implementação Meterpreter) para Linux
SSHDoor	0,7%	Backdoor SSH
XpMmap	0,6%	Explorações relacionadas à memória
DrtyCoW	0,6%	Exploração Dirty COW (CVE-2016-5195)
ProcHid	0,4%	Cavalo de Troia de ocultamento de processo
Ngioweb	0,2%	Bornet de proxy
Psdon	0,1%	Agente Poseidon para estrutura de Red-Team Mythic
GoScan	0,1%	Scanner Go procurando computadores vulneráveis

Fig. 36. Apesar do caos no cenário das criptomoedas em 2022, os mineradores são, infelizmente, um tipo de infecção comum no Linux.

Os mineradores dominaram as pesquisas em Linux nesse ano – mais do que essa tabela sugere. “Miner” é o termo genérico de detecção usado pela Sophos para um minerador. Os mineradores também podem ser detectados sob outros nomes; por exemplo, “Gognt” é o termo que usamos para famílias de malwares não relacionados, mas codificados em Go. Isso significa que há outros mineradores fora da nossa detecção de “miner”, o que significa que há muito mais do que os mostrados aqui.

Ameaças ao Linux por porcentagem de detecções exclusivas no Linux		
Ameaça	Porcentagem de computadores exclusivos	Observações
Minerador	74,3%	Detecção de minerador genérico
Gognt	5,1%	Detecção genérica de famílias de malwares codificadas em Go
DDoS	4,3%	Detecção relacionada ao Mirai
Swort	3,2%	Mettle (implementação Meterpreter) para Linux
DrtyCoW	3,1%	Exploração Dirty COW (CVE-2016-5195)
Ngioweb	2,8%	Bornet de proxy
Tsunami	2,7%	Cliente DDoS baseado em IRC
Roopre	0,9%	Backdoor visando a servidores Web
SSHBrut	0,9%	Cracker de senha de força bruta SSH
Loit	0,8%	Exploração local
Shell	0,8%	Malware dando acesso shell ao invasor
Bckdr	0,6%	Detecção de backdoor genérico
Ransm	0,6%	Ransomware

Fig. 37. Quando separados por computadores exclusivos afetados, o impacto dos mineradores no espaço do Linux fica ainda mais claro.



O próximo grupo com mais detecções do Linux em sistemas afetados está associado ao Gognt e a kits de ferramentas de negação de serviço distribuído (DDoS). Quase todos esses malwares que visam a vulnerabilidades têm sido abordados em versões mais recentes do Linux, mas continuam sem patches em um grande número de dispositivos e equipamentos.

Existem vários backdoors e botnets entre as maiores ameaças restantes do Linux, mas talvez, o mais interessante das outras ameaças principais à plataforma, do ponto de vista de uma corporação, é o Tsunami, um backdoor do Linux que está presente desde muito e que, recentemente, esteve envolvido em ataques a servidores de aplicativo Jenkins e WebLogic.

Ameaças a Mac

Em 2022, notamos um número crescente de ferramentas de ataque de código aberto e estruturas pós-exploit/C2, que suportam macOS, encontradas em espaços como o GitHub. A mera presença do código em um repositório não exatamente se correlaciona à surpreendente explosão de grandes ataques ao Mac, mas certamente indica pelo menos um aumento interessante – e uma predisposição ao compartilhamento.

Na plataforma macOS, a ameaça primária continua a ser os aplicativos potencialmente indesejados, incluindo aplicativos que instalam plug-ins para o navegador Safari da Apple (bem como outras plataformas de navegadores). Esses aplicativos injetam conteúdo nas páginas da Web a fim de redirecionar os usuários a conteúdo mal-intencionado ou fraudulento.

Aplicativos potencialmente indesejados (PUA) em macOS, abril a setembro de 2022		
Detecção	Porcentagem de computadores exclusivos	Observações
Adloadr	16,2%	Detecção de adware genérico
Genieo	8,9%	Sequestro de navegador (pesquisa)
Bundlore	8,4%	Adware
Dynji	4,6%	Sequestro de navegador (barra de ferramentas)
Pirrit	3,7%	Adware
AdvMac	3,2%	Adware
HistColl	3,0%	Coleta de dados do navegador
Keygen	2,3%	Ferramenta de pirataria de software

Fig. 38. Adloadr lidera a lista de PUAs de Mac em 2022 por uma boa margem.



O aplicativo Adloadr, um dos muitos PUAs predominantes caracterizáveis como adware, atingiu o primeiro lugar em nossas estatísticas de telemetria de Mac em 2022 com cerca de duas vezes mais infecções de computadores exclusivos que o sequestrador de navegador Genieo, que ocupa a segunda posição.

Pela perspectiva do malware, observamos altos números de NukeSped, VSearch e Dwnldr – um cavalo de Troia de acesso remoto, um pacote de adware e uma detecção de um cavalo de Troia downloader de uso geral. Chropex e ProxAgnt, dois aplicativos auxiliares associados à família Adloadr, também aparecem em nossa lista de detecções comuns.

Detecções de malware em macOS, abril a setembro de 2022		
Detecção	Porcentagem de computadores exclusivos	Observações
NukeSped	22,2%	Cavalo de Troia de acesso remoto
VSearch	15,6%	Sequestro de navegador/Adware
Dwnldr	10,8%	Detecção de cavalo de Troia genérico
Agent	10,8%	Detecção de malware genérico
Keygen	6,4%	Principal gerador para burlar a proteção de cópia
FkCodec	6,2%	Adware; se passa por um instalador codec de vídeo
Chropex	5,0%	Adware; também demonstra comportamento de sequestro de navegador
ProxAgnt	1,9%	Cavalo de Troia
Swrort	1,5%	Cavalo de Troia de acesso remoto

Fig. 39. NukeSped, VSearch e Dwnldr estão no topo do placar de detecções de malware de macOS.



Até outubro, observamos cinco novas ameaças a macOS em 2022. Nenhuma delas despontaram em nossas tabelas de malware de macOS, mas estamos atentos a novas detecções com grande interesse.

Ameaças recém-observadas ao macOS em 2022			
Mês	Nome	Deteção	Observações
Janeiro	SysJoker	OSX/SysJoker	Backdoor multiplataforma que suporta macOS
Janeiro	DazzleSpy	OSX/DazzleSpy	Técnica de infecção relacionada ao MACMA, um backdoor que visa a ativistas pró-democracia de Hong Kong
Março	Gimmick	OSX/Gimmick	Comunica-se via APIs do Google Drive para ocultar tráfego de rede dos sistemas de monitoramento
Maior	pymafka/CrateDepression	Troj/Pymaf, OSX/Cobalt	Ataque à cadeia de suprimento em um pacote hospedado no pypi; posteriormente lança um beacon do Cobalt Strike
Outubro	Alchemist	Exp/20214034-D	Estrutura de ataque multiplataforma codificada em Go

Fig. 40. Cinco novidades em ameaças a macOS surgiram nos primeiros dez meses de 2022.



Ameaças móveis

Como os aplicativos móveis se tornaram o caminho comum de interação das pessoas com a Internet, os dispositivos móveis estão no centro de uma nova classe de crimes cibernéticos. A plataforma Android continua a seguir um fluxo estável de invasões por malware na forma de aplicativos falsos e ladrões de informações. Porém, tanto o Android como o iOS têm sido alvos crescentes de aplicativos falsos e fraudulentos – e os criminosos encontraram formas de usar a engenharia social para violar até os jardins murados dos dispositivos móveis da Apple.

Injetores de malware, spywares e malwares associados a instituições financeiras continuam na liderança em nossas detecções, com os pacotes .APK do Android e apps que geram cliques em anúncios falsos. Entretanto, os aplicativos potencialmente indesejados – incluindo aqueles que não fazem nada além de atuar na coleta de “compras no aplicativo” ocultos das vítimas – são uma ameaça crescente aos usuários de aparelhos móveis. No ano passado, notamos o surgimento de quadrilhas de fraudes financeiras sofisticadas, usando aplicativos falsos, que se tornou uma verdadeira indústria no sul da Ásia.

Em 2021, a Sophos começou a rastrear uma campanha do crime organizado que chamamos de CryptoRom. A campanha se baseia em uma forma de fraude cibernética conhecida como sha zhu pan (杀猪盘) – literalmente “prato de açougueiro de porco” –, que tem o respaldo de um sindicato do crime muito bem-organizado de desenvolvedores de aplicativos fraudulentos para a Web, criadores de perfis sociais falsos e indivíduos engajados em manipulação de scripts de engenharia social via aplicativos de redes sociais e sites de relacionamento, para envolver as vítimas no golpe.

Em outubro de 2021, documentamos a [expansão global](#) da campanha. A fórmula mudou, indo dos falsos investimentos em criptomoedas aos falsos investimentos em derivativos de criptomoedas e adentrando na oferta a outros mercados financeiros falsos. Para fazer com que esses esquemas se pareçam legítimos, as quadrilhas criaram aplicativos e sites falsos se passando por instituições financeiras de renome. Muitos desses aplicativos passaram despercebidos pelas lojas de aplicativos móveis, como os aplicativos de “mineração de liquidez” que foram encontrados na Apple App Store e no Google Play Store.

Os golpistas também encontraram meios de usar indevidamente o iOS, aproveitando-se de Web Clips e programas de implantação de teste de desenvolvedores de aplicativos para inserir seus aplicativos nos dispositivos iOS. Isso inclui o uso abusivo do esquema de distribuição ad-hoc “Super Signature” da Apple, a versão de teste beta “Test Flight” e os esquemas de aplicativos corporativos para evitar a triagem de segurança da App Store da Apple. A mesma abordagem pode ser usada por outros malwares direcionados ao iOS, mas requer uma certa manipulação de engenharia social do alvo para permitir que a instalação prossiga.

Esses aplicativos resultaram em perdas que computam centenas de milhões de dólares às suas vítimas e fazem parte do crescente ecossistema do crime cibernético que se alastrou do envolvimento levado pelo romance à amplitude de alcance da engenharia social em plataformas como Facebook, Twitter e LinkedIn. Os golpes continuam a evoluir e estão sendo copiados por outras quadrilhas criminosas, cada qual com suas próprias singularidades.

O Android e o iOS também são alvos de campanhas publicitárias mal-intencionadas, incluindo alertas falsos que clonam os alertas de sistema – geralmente levando os usuários a uma loja de aplicativos para a compra de aplicativos que ocultam taxas de assinatura, instalam malwares, ou as duas coisas.

A Sophos continua a trabalhar em formas de bloquear essas ameaças e de alertar os desenvolvedores de SOs móveis sobre novos usos abusivos descobertos em suas lojas de aplicativos.

Conclusão

Em toda a extensão desse panorama, duas coisas se sobressaem: o rebaixamento continuado das barreiras de proteção à entrada dos pretensos criminosos cibernéticos e a transformação em commodities das táticas e ferramentas que foram, um dia, consideradas “ameaças avançadas persistentes”. Enquanto o marketplace das ferramentas para hackers continua a florescer e prosperar com ofertas de malwares e acesso a redes vulneráveis, as lições aprendidas com as histórias recentes sobre operações de ransomwares e outros agentes maliciosos e bem-financiados é que elas estão rapidamente sendo disponibilizadas à comunidade do crime, da mesma forma que as ferramentas de segurança comercial projetadas para malograr nossas defesas.

Condições geopolíticas continuam a dificultar a luta contra o crime cibernético. Este ano, a China encerrou o acordo de cooperação com as autoridades norte-americanas na luta contra o crime cibernético devido às tensões que abatem a relação EUA-China. E com a intensificação da repressão pela China aos golpes internos com criptomoedas e outros crimes cibernéticos domésticos, os criminosos chineses mudaram rapidamente para outra vertente de exploração: a exportação de suas operações criminosas. A guerra na Ucrânia interrompeu brevemente as quadrilhas do crime russo, mas elas estão se reorganizando com rapidez.

Não há defesa certa contra todas essas ameaças. O que é preciso é uma defesa ativa para prevenir que essas incursões causem danos, mas o fardo da defesa é tamanho que muitas organizações não conseguem carregá-lo sozinhas. A Sophos continua a trabalhar para aumentar sua capacidade de ajudar organizações de todos os portes contra a evolução incessante desse cenário de ameaças através de defesas de endpoint e rede, e serviços gerenciados de operações de segurança.

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

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