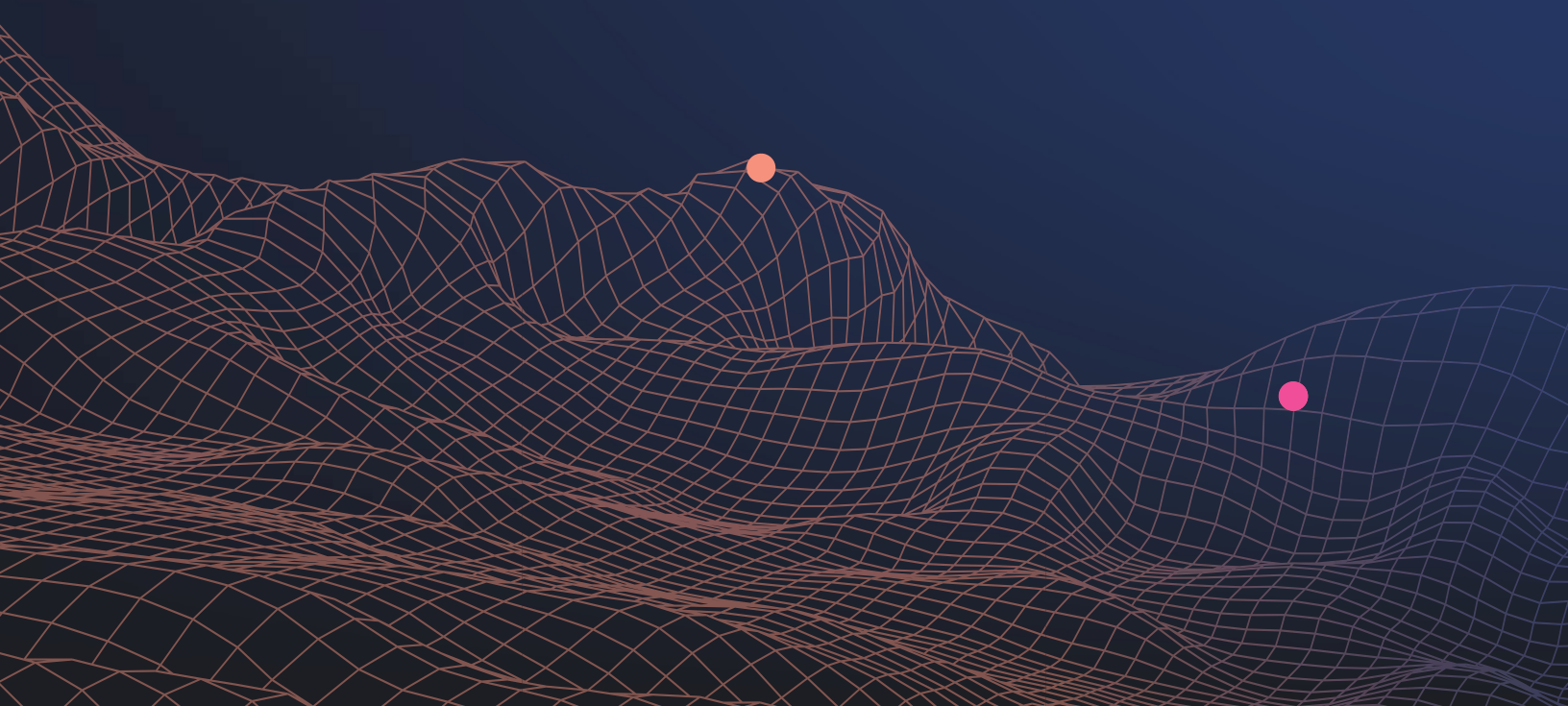
elastic security labs

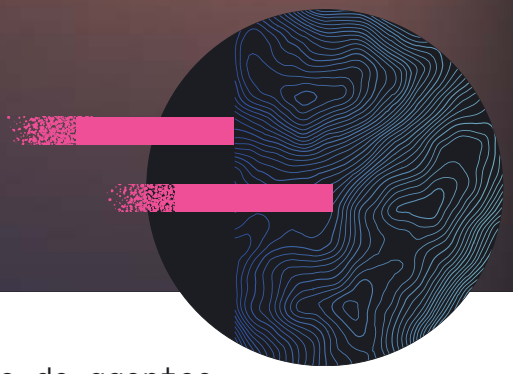
Relatório Global de Ameaças

Vol. 1 2022

Conteúdo



Introdução



"O futuro da segurança está em aberto. Em um mundo de agentes de ameaças dinâmicos, ágeis e bem equipados, a melhor esperança da segurança digital é reunir defensores com ideias semelhantes em torno de plataformas que sejam tão abertas e interoperáveis quanto possível."

– Nate Fick

Embaixador geral dos EUA para políticas digitais e de ciberespaço e antigo gerente geral do Elastic Security e CEO da Endgame

Este Relatório Global de Ameaças é um produto do Elastic Security Labs, nosso ramo de pesquisa de ameaças com experiência na investigação de invasões de redes de computadores, análise de software malicioso, desenvolvimento de mitigações para amplas categorias de ameaças e realização de análises de inteligência. O Elastic Security Labs é um grupo de profissionais de segurança altamente empenhados que pesquisam tópicos de segurança para melhorar o produto Elastic Security e compartilhar o que aprendemos com a comunidade em geral.

Nossa filosofia é direta: a melhor maneira de proteger os dados do mundo é armar tecnologias defensivas. Criamos ambientes hostis às ameaças porque essa é a maneira mais eficaz de mudar o cenário das ameaças. Enquanto muitos fornecedores de segurança escolhem uma mentalidade passiva de "esperar para ver", as ameaças estão constantemente se adaptando e evoluindo, exigindo assim uma abordagem mais proativa.

Este relatório descreve fenômenos de ameaças, tendências e recomendações que acreditamos que ajudarão as organizações a se preparar para o futuro. A Elastic divulga pesquisas de malware, padrões de ataque e grupos de atividades maliciosas para a comunidade, resumidos neste relatório inaugural.

Ao longo deste relatório, observamos que as ameaças com motivação financeira são as mais ativas, e os grupos responsáveis por elas estão agindo com velocidade cada vez maior. Essas ameaças em rápida expansão afetam as organizações que trabalham para a mitigação em seus ambientes, resultando em maiores vitórias para os adversários.

A telemetria da Elastic, compartilhada voluntariamente e enriquecida com inovações de ponta e dados públicos e de terceiros, fornece o material para este relatório. As informações foram tratadas com responsabilidade para proteger as identidades dos clientes, quando aplicável.

A Elastic usa principalmente a telemetria para melhorar a eficácia dos recursos e fornecer às organizações um contexto de segurança adicional por meio de publicações como esta. Recebemos de braços abertos a oportunidade de trabalhar em parceria com nossos clientes para analisar seus dados, compartilhando anonimamente o que aprendemos com o setor de segurança de forma geral.

Para prevenir com eficácia as ameaças à segurança cibernética, uma organização precisa de visibilidade, capacidade e experiência. O Elastic Security oferece essa base, e nossa instrumentação global nos permite implantar rapidamente proteções da comunidade contra ameaças. Este relatório contém informações sobre as ameaças que vemos e às quais respondemos, informações estas que são essenciais para o desenvolvimento de futuros recursos da Elastic.

Ao compartilhar esses insights, nós do Elastic Security Labs esperamos normalizar a discussão sobre a visibilidade do fornecedor e demonstrar como nossa perspectiva única capacita os desenvolvedores de tecnologias de segurança a maximizar resultados positivos para seus usuários e para a comunidade em geral.

Resumo executivo

Para muitos, o estado atual da segurança é frustrante — um fluxo interminável de vulnerabilidade, exploração, comprometimento e roubo. A Elastic também está frustrada com esse estado, e esse é um dos motivos pelos quais escolhemos trabalhar em uma cura em vez de simplesmente ganhar dinheiro inventando novos tratamentos para os muitos, caros e perturbadores sintomas.

Como as tecnologias de detecção e prevenção conseguiram aumentar sua eficácia de forma drástica, o compartilhamento de informações se elevou para um ponto mais alto. Até o público em geral entende as implicações de um cenário de ameaças globais cada vez maior e os desafios implícitos enfrentados pelos administradores da segurança cibernética.

Ameaças de todos os tipos ganharam novas capacidades e métodos, aumentando a cadência de sua atividade. Enquanto as organizações acompanhavam a diminuição nas métricas de tempo médio para detecção (MTTD) e tempo médio para remediação (MTTR), as ameaças agiram com velocidade ainda maior para minar esses esforços.

Os adversários também não desconhecem os esforços liderados pela inteligência para rastreá-los, expô-los e detê-los. Em vez disso, muitas ameaças financeiras estabeleceram programas de afiliados e outras relações de representação que garantem que continuem a ganhar dinheiro enquanto se livram das sanções do governo — um dos poucos custos sobre os quais eles parecem respeitosamente cautelosos. Infelizmente para suas vítimas, esses fatores raramente têm um impacto direto no local onde vivem e trabalham.

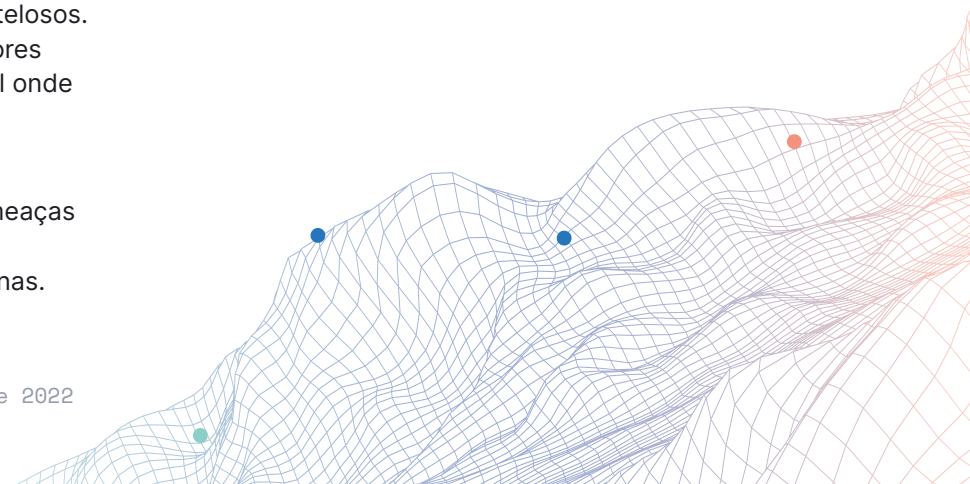
O Elastic Security Labs observa que uma porcentagem significativa de todas as ameaças alcança um certo grau de sucesso contra mitigações técnicas, processuais e humanas.

> *Nós escolhemos trabalhar em uma cura em vez de simplesmente ganhar dinheiro inventando novos tratamentos para os muitos, caros e perturbadores sintomas.*

Observamos ameaças com desenvolvimento de software maduro e recursos de pesquisa próprios, contornando a sofisticada detecção e resposta de endpoint (EDR), antivírus, sistemas de detecção de invasão de rede (NIDS) e controles de política de serviço de diretório. Provedores de serviços comprometidos, cadeias de suprimentos de software e frameworks de sistema operacional integrados como o Berkeley Packet Filter (BPF) não são mais ficções implausíveis, e sim a superfície de ataque de hoje.

Os clientes e usuários da Elastic vão querer entender o conteúdo deste relatório e como nossa visibilidade do cenário global de ameaças os afeta.

Nossa equipe é composta por profissionais que atuam na resposta a incidentes, analistas de inteligência e malware, engenheiros de segurança, pesquisadores, cientistas de dados e outros especialistas com décadas de experiência coletiva, e estamos ansiosos para compartilhar nosso conhecimento com a comunidade.



Tendências e correlações

As tendências a seguir representam as principais ferramentas, táticas e procedimentos empregados pelas ameaças e foram identificadas na telemetria da Elastic. Como cada fornecedor tem sua própria visibilidade, relatórios como este oferecem insights valiosos sobre os métodos que cada um usa para monitorar e mitigar ameaças. A telemetria da Elastic incorpora dados do Elastic Endgame, do Elastic Endpoint e da solução Elastic Security, e implanta mitigações por meio dessas tecnologias.

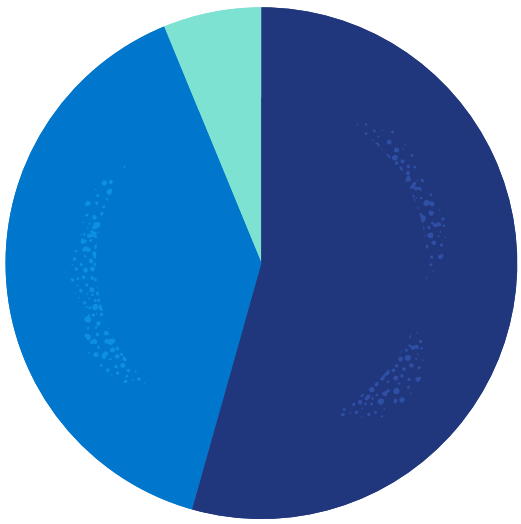
A seguir, apresentamos uma visão geral das tendências e correlações, com subseções para assinaturas de malware, comportamentos de endpoint e recursos de segurança na nuvem. Onde aplicável, essas seções foram organizadas para o leitor.

Tendências de assinatura de malware

As assinaturas do YARA fornecem uma camada de defesa dentro da solução Elastic Security, identificando atividades de ameaças relacionadas a malware com base em strings ou sequências de bytes. O Elastic Endpoint Security oferece assinaturas nos níveis de arquivo e memória para todos os sistemas operacionais de endpoint comuns. A Elastic disponibiliza assinaturas para a comunidade por meio do repositório de artefatos de proteção como parte do nosso compromisso gratuito e aberto.

Para começar, o Elastic Security Labs analisou tendências específicas do sistema operacional para malware de acordo com nossa telemetria. A partir disso, identificamos que ~54% de todas as infecções por malware estavam em endpoints do Windows, enquanto ~39% estavam em endpoints do Linux.

~54% de todas as infecções por malware estavam em endpoints do Windows, enquanto ~39% estavam em endpoints do Linux



Sistema operacional do endpoint com malware

Windows.....54,4%

Linux.....39,4%

MacOS.....6,2%

Figura 1: *sistema operacional do endpoint com malware*

[1] *A telemetria da solução Elastic Security é gerada por uma população diversificada de sensores e fontes de dados que são muito numerosos para serem descritos de forma concisa, incluindo sensores não desenvolvidos pela Elastic.*

À medida que as empresas continuam a adotar uma abordagem de nuvem híbrida e a implementar mais endpoints baseados em Linux como infraestrutura de backend, isso cria a possibilidade de os adversários usarem binários como armas para essa arquitetura e distribuí-los por meio de suas técnicas de entrega customizadas.

Indo um pouco mais fundo, identificamos que quem mais contribuiu com malware/carga útil baseado em Linux foi o Meterpreter com ~14%, seguido pelo Gafgyt com ~12% e o Mirai com ~10%. Embora isso não seja uma surpresa, podemos dizer com confiança que os adversários ainda estão usando frameworks como CobaltStrike e Metasploit para implantar cargas úteis, mirar em exploits e configurar backdoors para posterior execução de comandos. Isso se mostra especialmente útil se um shell é estabelecido em um endpoint do Linux hospedado em um provedor de serviços em nuvem (CSP) onde a CLI padrão do CSP está instalada e scripts ou módulos pré-criados podem ser chamados para fácil descoberta e enumeração.

Embora não entremos em detalhes sobre o BPFDoor, o Elastic Security Labs publicou uma extensa pesquisa sobre esse implante do Linux e também sobre um binário de cliente de comunicação para aproveitar o implante.

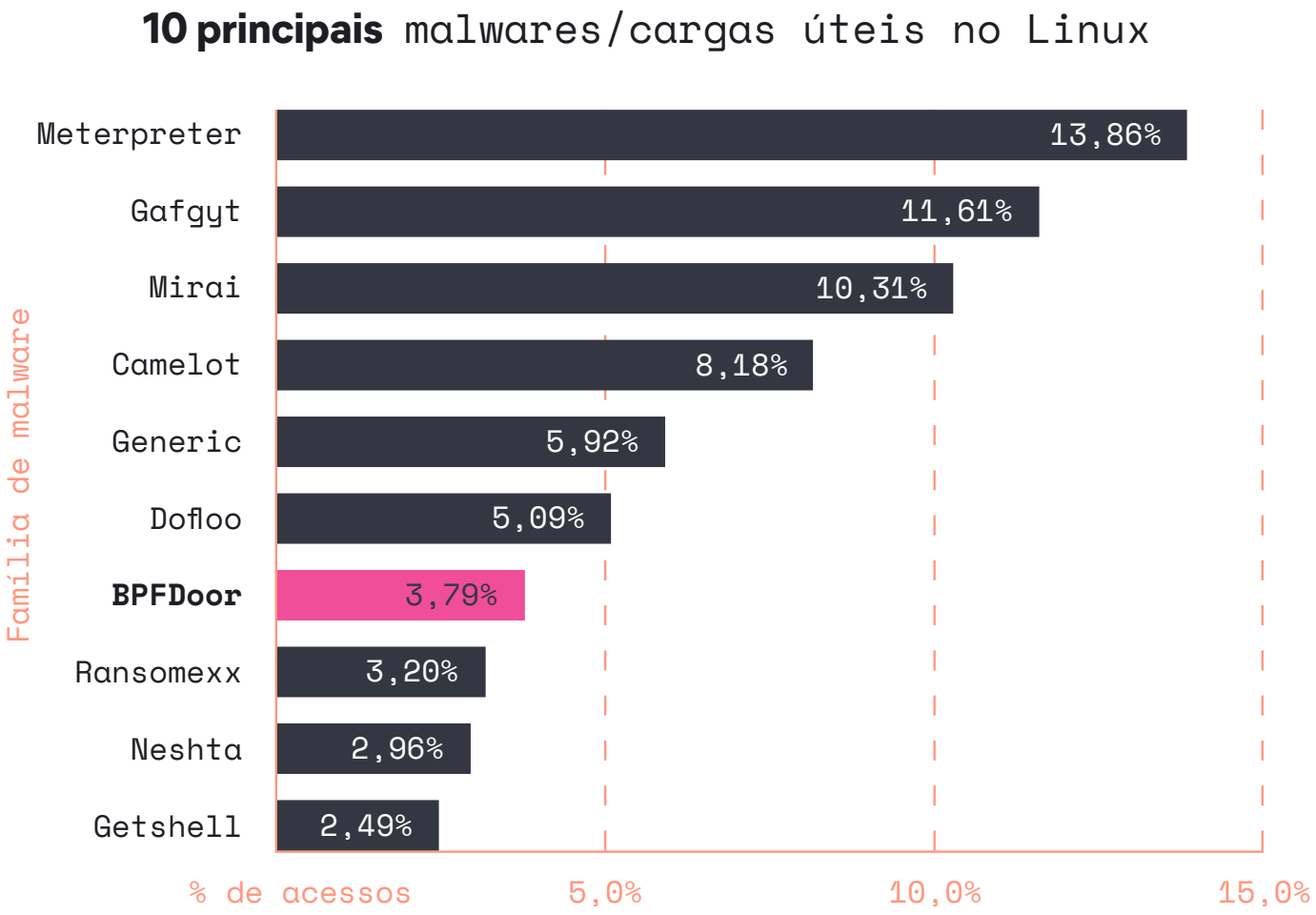


Figura 2: *10 principais malwares e cargas úteis do Linux, mostrando o aumento da atividade do BPFDoor*

Malware **por categoria**

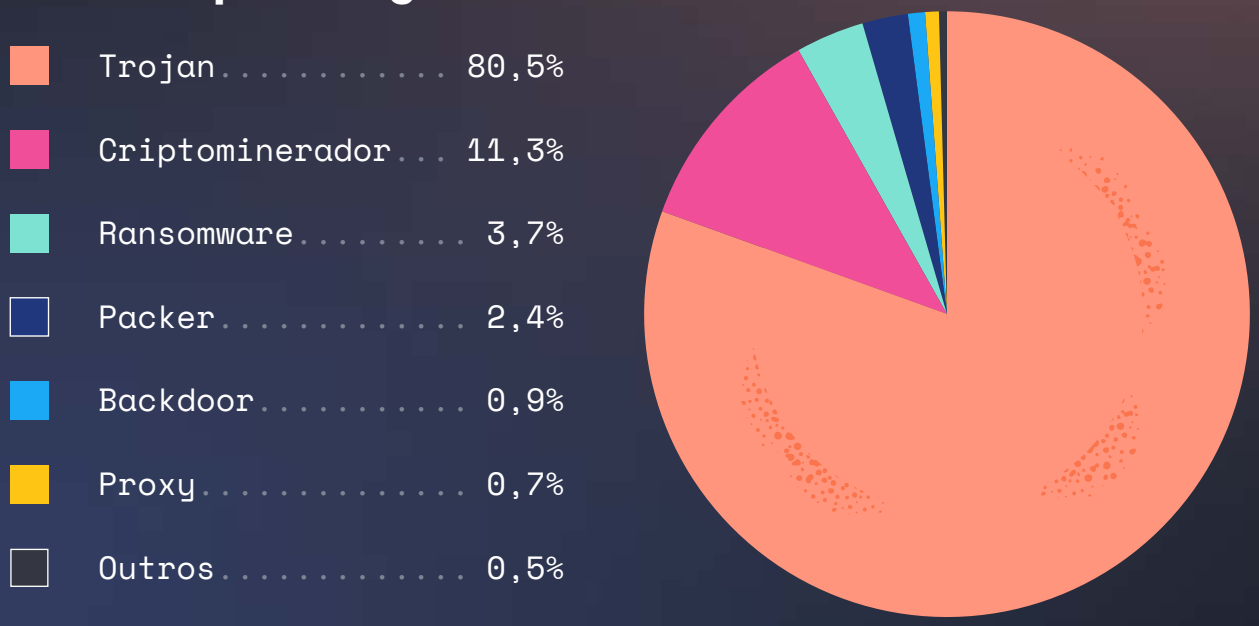


Figura 3: *malware por categoria*

Depois disso, o Elastic Security Labs analisou quais categorias de malware estávamos vendo globalmente, e descobrimos que ~81% do malware era baseado em trojan, seguido por criptomineradores com ~11%. Os trojans, ou cavalos de Troia, continuam a ser uma forma preferida de usar binários entregáveis como armas que implementam stagers e droppers para realizar a invasão, mas podem ser multifuncionais com técnicas adicionais. Nossa equipe viu muitos trojans compactados antes da entrega ao destino para evitar uma possível mitigação por mecanismos de detecção baseados em assinatura.

Os criptomineradores, embora não sejam inerentemente maliciosos, foram frequentemente implantados inicialmente como um meio de usar os recursos de computação da vítima para minerar uma criptomoeda de sua escolha — geralmente o Monero devido aos fins de anonimato. Os criptomineradores são comumente implantados junto com outras famílias de malware como um plano de contingência para agentes motivados financeiramente, para o caso de tudo mais falhar.

Embora o XMRig e o KWorker sejam ferramentas muito comuns, os criptomineradores costumam usá-los de forma inadequada devido à disponibilidade pública do código-fonte. O Elastic Security Labs encontrou outra família de criptomineradores predominante recentemente: o LoudMiner. Mostradas no gráfico abaixo, as detecções do LoudMiner foram poucas até novembro de 2021. Porém, houve um pico nas detecções em fevereiro de 2022, e elas permaneceram consistentes desde então. O LoudMiner é baseado no popular código open source XMRig e foi projetado para minerar a criptomoeda Monero, que inclui recursos adicionais para anonimato. Embora as detecções tenham ocorrido especificamente em endpoints do Linux, o LoudMiner é multiplataforma e utiliza a CPU para processamento de transações contábeis no blockchain do Monero.

Recentemente, o Elastic Security abriu o código das nossas regras customizadas de comportamento do YARA e do endpoint em nosso repositório Protections Artifacts, onde a lógica `Linux.Cryptominer.LoudMiner` pode ser encontrada.

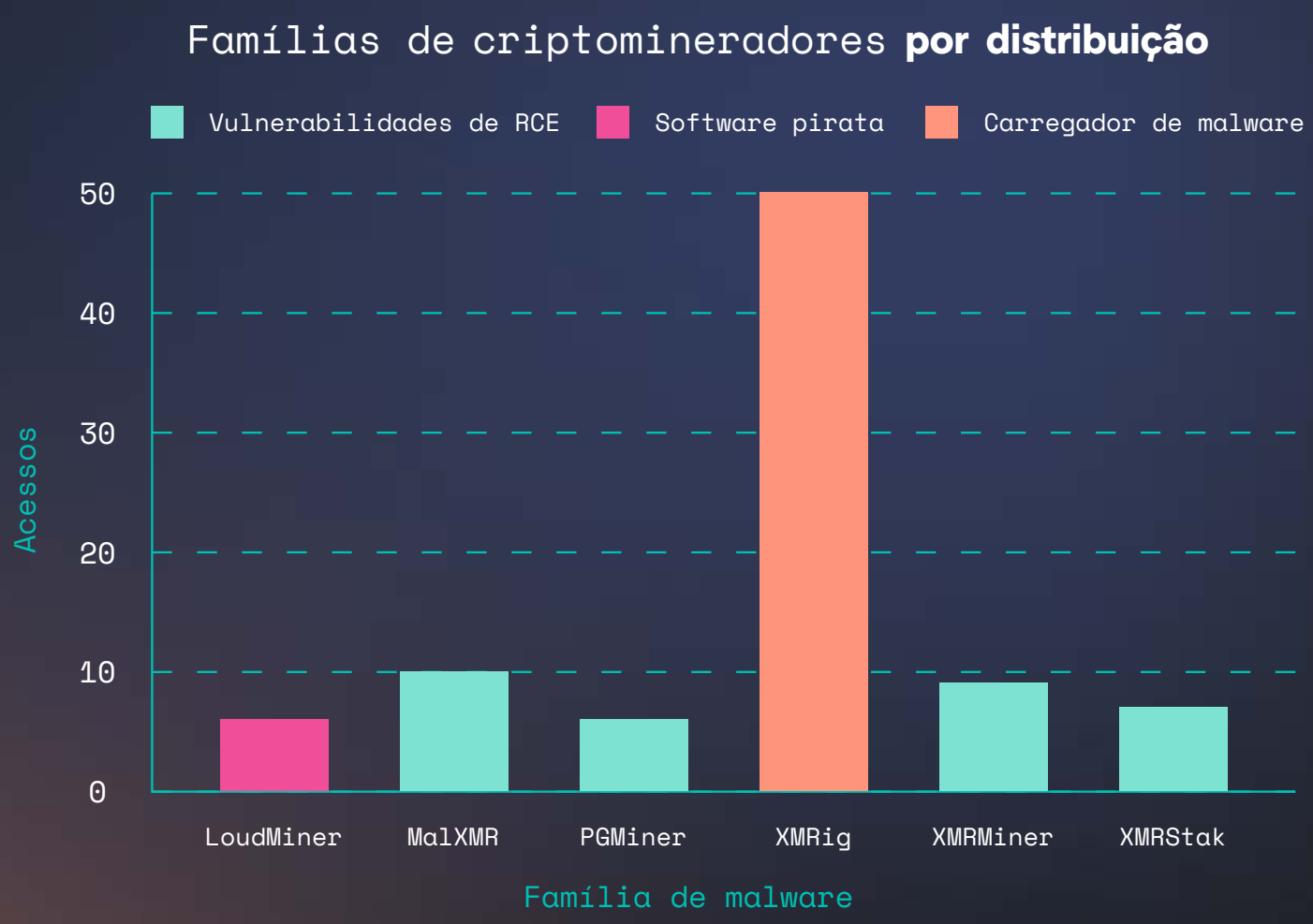


Figura 4: *famílias de criptomineradores por distribuição*

Enquanto continuamos analisando as tendências nas categorias de malware, notamos alguns aumentos em tipos menos comuns, como backdoors e cargas úteis de proxy, conforme mostrado no gráfico abaixo. Entre março e maio de 2022, o Elastic Security Labs notou um aumento nas detecções relacionadas a backdoors para vários clientes correspondentes às nossas assinaturas do YARA customizadas listadas abaixo.

- Linux.Backdoor.Bash
- Linux.Backdoor.Generic
- Linux.Backdoor.Tinyshell
- MacOS.Backdoor.Applejesus

Os backdoors do Linux permitem que os adversários tenham contínua persistência e acesso a um endpoint comprometido. Em ambientes baseados em nuvem, o acesso inicial pode ser mais alcançável por meio de exploits de aplicações voltadas para o público, onde o backdoor é implantado, seguido pela descoberta e enumeração do ambiente de nuvem. O acesso aos endpoints do Windows seria mais alcançável se aproveitado nas mesmas configurações de rede VPC ou adjacentes.

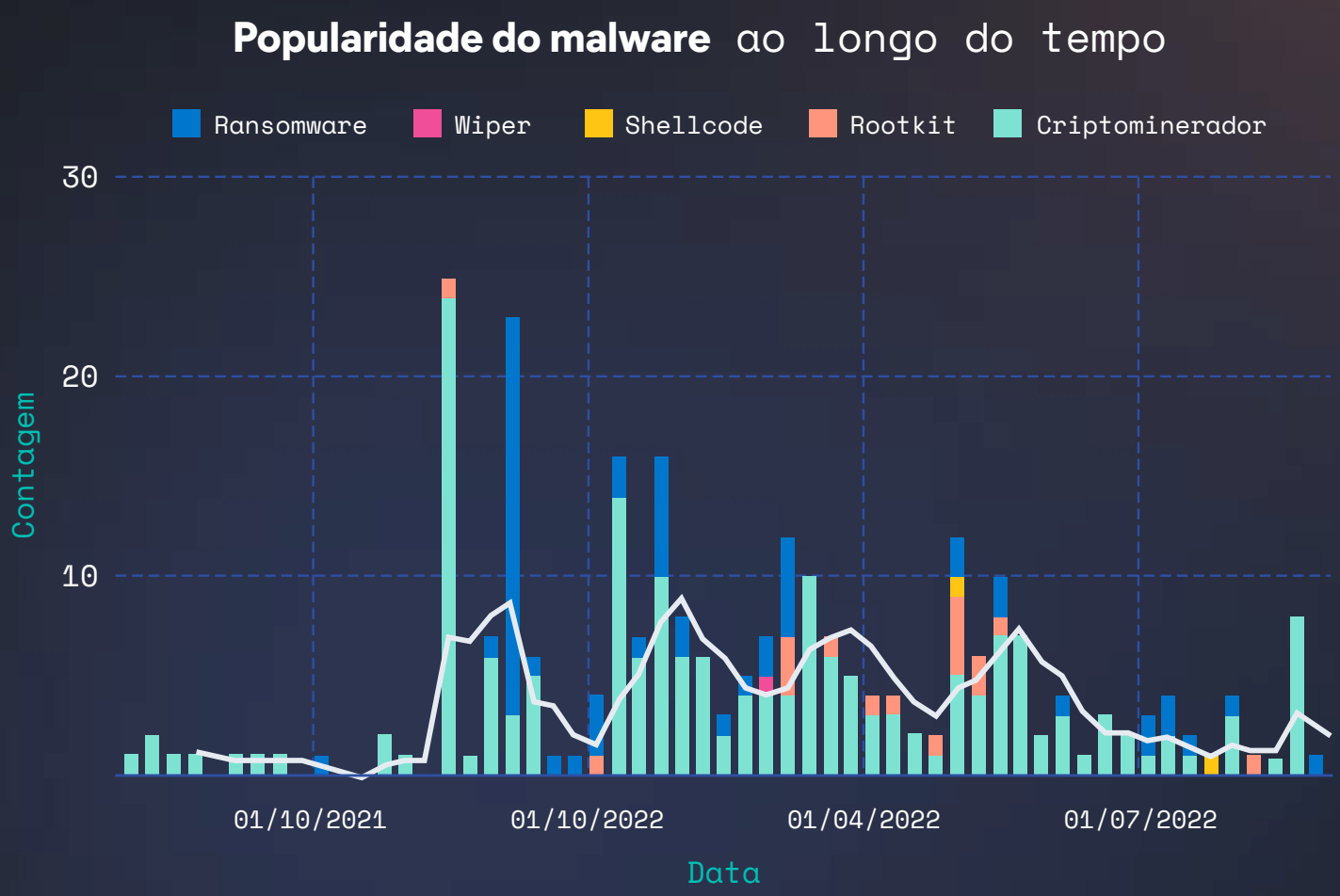


Figura 5: *popularidade do malware ao longo do tempo*

Com base na *Figura 5*, o Elastic Security notou um leve aumento nos binários do Linux com a capacidade de aproveitar um proxy para possíveis fins de comando e controle, graças à nossa lógica `Linux.Proxy.Frp`. Ao mirar os endpoints do Linux, os procedimentos dos adversários geralmente incluem o uso de um binário de backdoor, conforme discutido anteriormente, seguido pela instalação de um servidor proxy para comando e controle. Isso pode se tornar uma ocorrência mais comum à medida que os ambientes de nuvem híbrida utilizam mais servidores de backend do Linux com configurações incorretas ou implementações com segurança insatisfatória acessíveis publicamente.

Conforme declarado na *Figura 3*, os trojans foram responsáveis por ~80% das detecções de malware na Elastic, a maioria das quais relacionadas ao Windows. Para aprofundar um pouco mais, decidimos analisar a popularidade da família de trojans para endpoints do Windows, conforme mostrado na *Figura 6*.

Popularidade dos trojans para endpoints do Windows

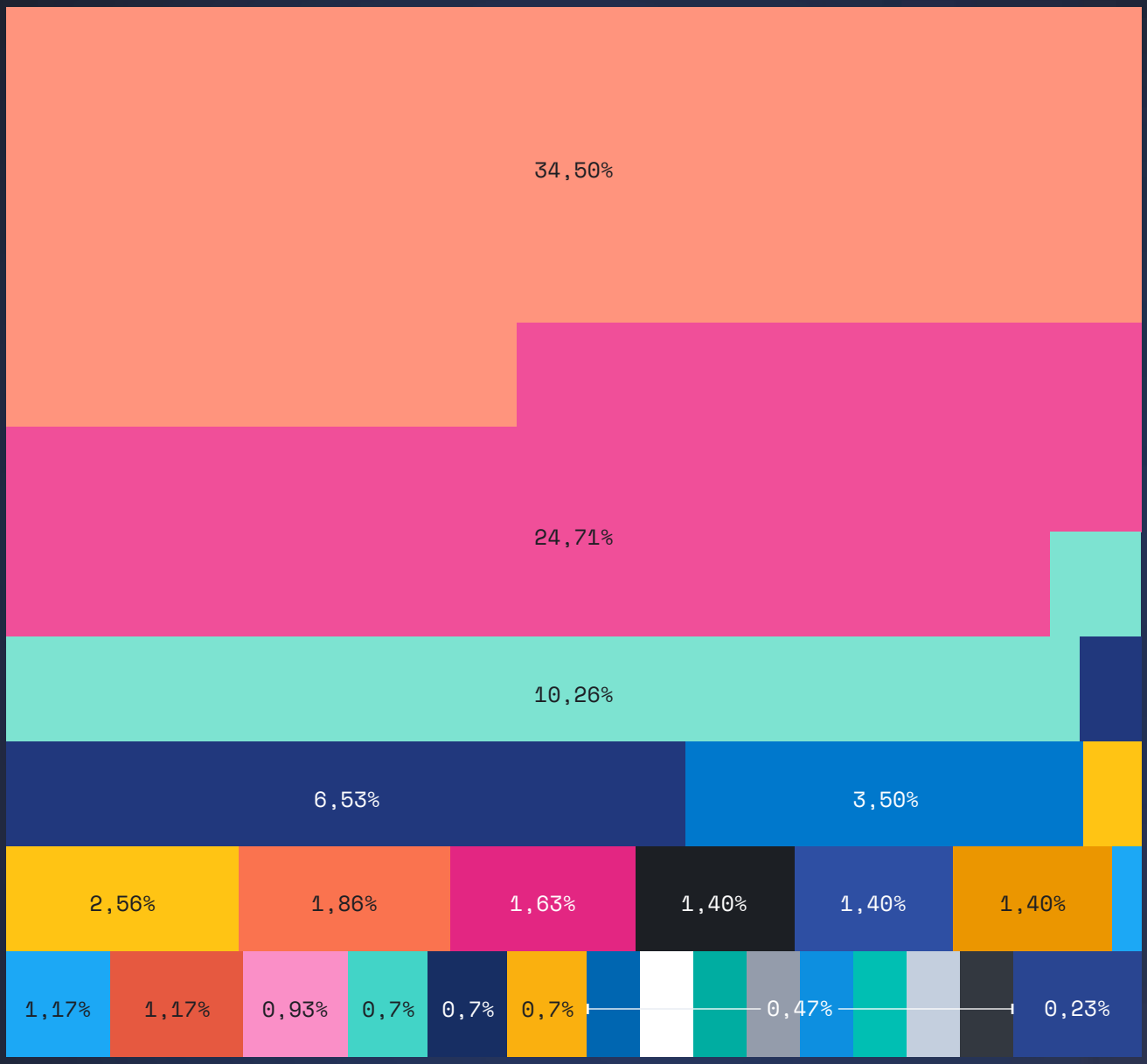


Figura 6: *popularidade dos trojans para endpoints do Windows*

As famílias de malware comercial pronto para uso como COBALTSTRIKE e METASPLOIT estiveram fortemente representadas com detecções na memória, bem como ferramentas maliciosas e implantes de malware em massa. Sem nenhuma surpresa, o CobaltStrike foi o binário ou carga útil malicioso mais popular para endpoints do Windows com ~35% de todas as detecções, seguido pelo AgentTesla com ~25% e pelo RedLineStealer com ~10%. O Elastic Security Labs já havia analisado o CobaltStrike em profundidade e discutido o uso dessa ferramenta e das cargas úteis. Para continuar avançando com abertura e transparência, também lançamos um extrator de beacon do CobaltStrike para uso. Não é de surpreender que ferramentas ofensivas como COBALT STRIKE, METASPLOIT e MIMIKATZ continuem no topo da nossa lista, não mostrando nenhuma desaceleração no uso dessas ferramentas.

Embora o AgentTesla seja muito popular como keylogger e seu mau uso por adversários continue a incluir recursos adicionais, o Elastic Security Labs também quis destacar o SnakeKeylogger. Ambos os keyloggers são distribuídos ativamente por email como anexos maliciosos. Conforme discutido anteriormente neste relatório, o acesso inicial por meio de documentos do Microsoft Office é comumente usado para distribuir essas famílias de malware, seguido pela execução de proxy de um binário assinado e confiável. As credenciais visadas geralmente estão relacionadas a clientes de email e FTP, navegadores da web e outros. Em um ambiente onde uma solução de nuvem híbrida está presente, isso pode permitir que contas válidas sejam usadas para movimentação lateral no ambiente de nuvem, onde os agentes podem buscar acessar recursos e dados críticos ou sensíveis.

Assinaturas do AgentTesla e SnakeKeylogger:

- `Windows.Trojan.SnakeKeylogger`
- `Windows.Trojan.AgentTesla`

Relacionada a keyloggers, outra família de malware de interesse que continua em alta é o RedLine Stealer, detectado no Elastic Security Labs como `Windows.Trojan.RedlineStealer`. Esse ladrão de informações também é comumente distribuído em campanhas maliciosas de spam (malspam) e se tornou popular durante a pandemia de COVID-19, quando os assuntos e temas dos emails estavam relacionados a esse tópico popular, muitas vezes incentivando os usuários a baixar e executar anexos. O RedLine Stealer continua a ser adotado e desenvolvido, permitindo que agentes com motivação financeira também tenham como alvo carteiras de criptomoedas (se houver), como uma alternativa aos criptomineradores populares discutidos anteriormente. À medida que os contratos inteligentes e a tecnologia de blockchain continuam a ganhar popularidade e se mostram úteis para manutenção de registros e rastreamento de distribuição por meio de registros contábeis imutáveis, o Elastic Security Labs prevê que esse recurso seja comumente usado como arma em mais famílias de ladrões de informações.

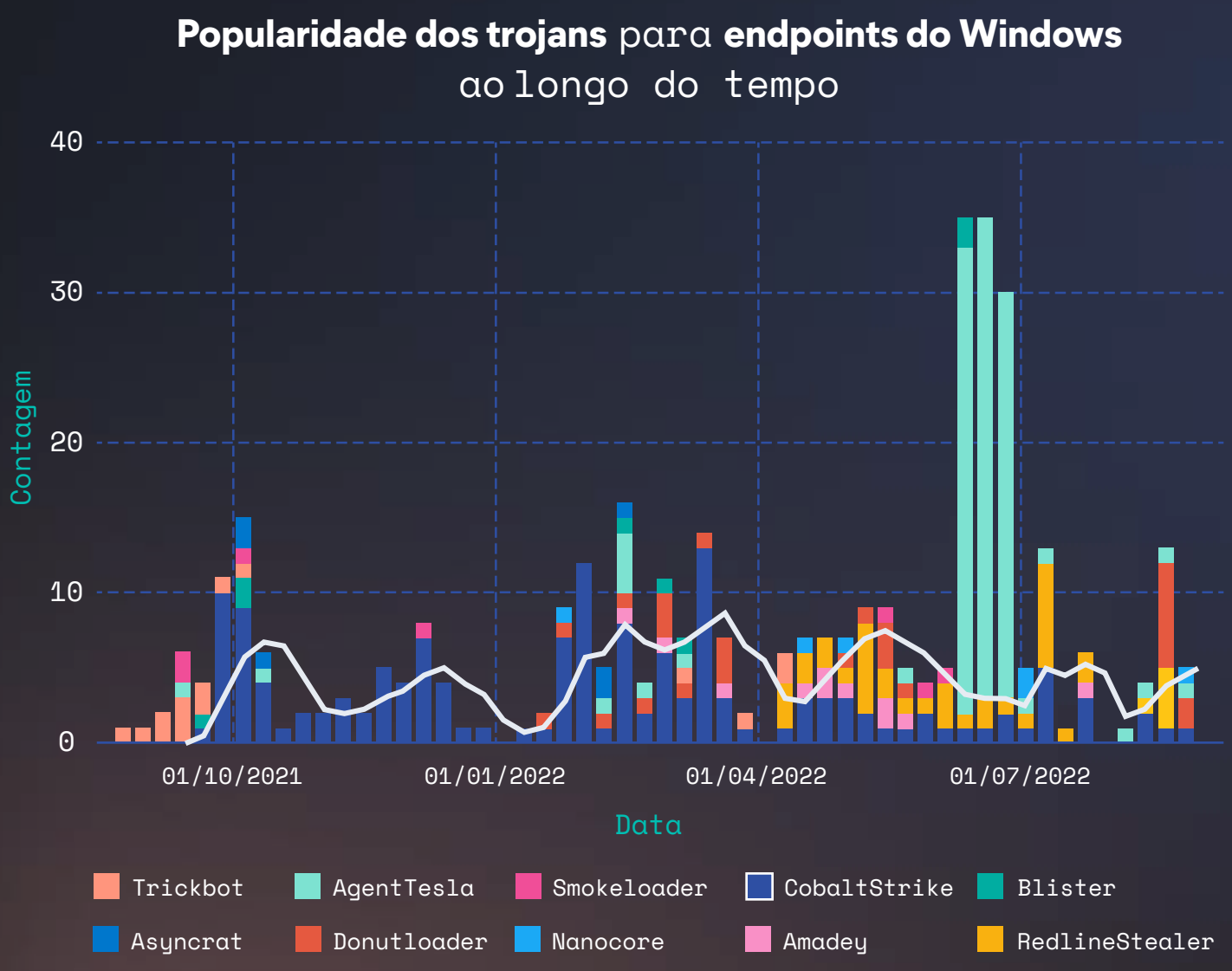


Figura 7: *popularidade dos trojans para endpoints do Windows ao longo do tempo — excluindo AgentTesla, Redline Stealer e CobaltStrike*

Embora não seja tão popular em pesquisas públicas recentes, o Elastic Security Labs continua a detectar o uso inadequado do framework carregador open source Donut. Na pesquisa da BitDefender, o shellcode injetado de um binário Orcus RAT foi detectado como o carregador do Donut durante a exploração de dia zero da vulnerabilidade Log4j2, que a Elastic abordou em uma publicação separada. O Elastic Security acha o DonutLoader interessante por causa de seus diversos recursos para carregar cargas úteis maliciosas e fazer a execução de VBScript, JScript, EXE, arquivos DLL e assemblies .NET na memória. Conforme mostrado na *Figura 7*, o DonutLoader permanece consistentemente popular ao longo do tempo, enquanto o uso de famílias populares de malware de commodities, como Trickbot e Emotet, não é detectado com tanta frequência.

Para assinaturas de arquivos do MacOS, o MacKeeper classificou-se em primeiro lugar com ~48% de todas as detecções, e o XCSSet ficou na segunda posição com quase 17%. O MacKeeper é um pacote de software utilitário para endpoints do MacOS projetado para ajudar a otimizar recursos e monitorar recursos internos. Embora seu objetivo inicial seja ajudar os usuários do MacOS, muitas vezes pode sofrer mau uso por parte de adversários, pois já tem amplas permissões e acesso a processos e arquivos.

Popularidade das assinaturas do MacOS

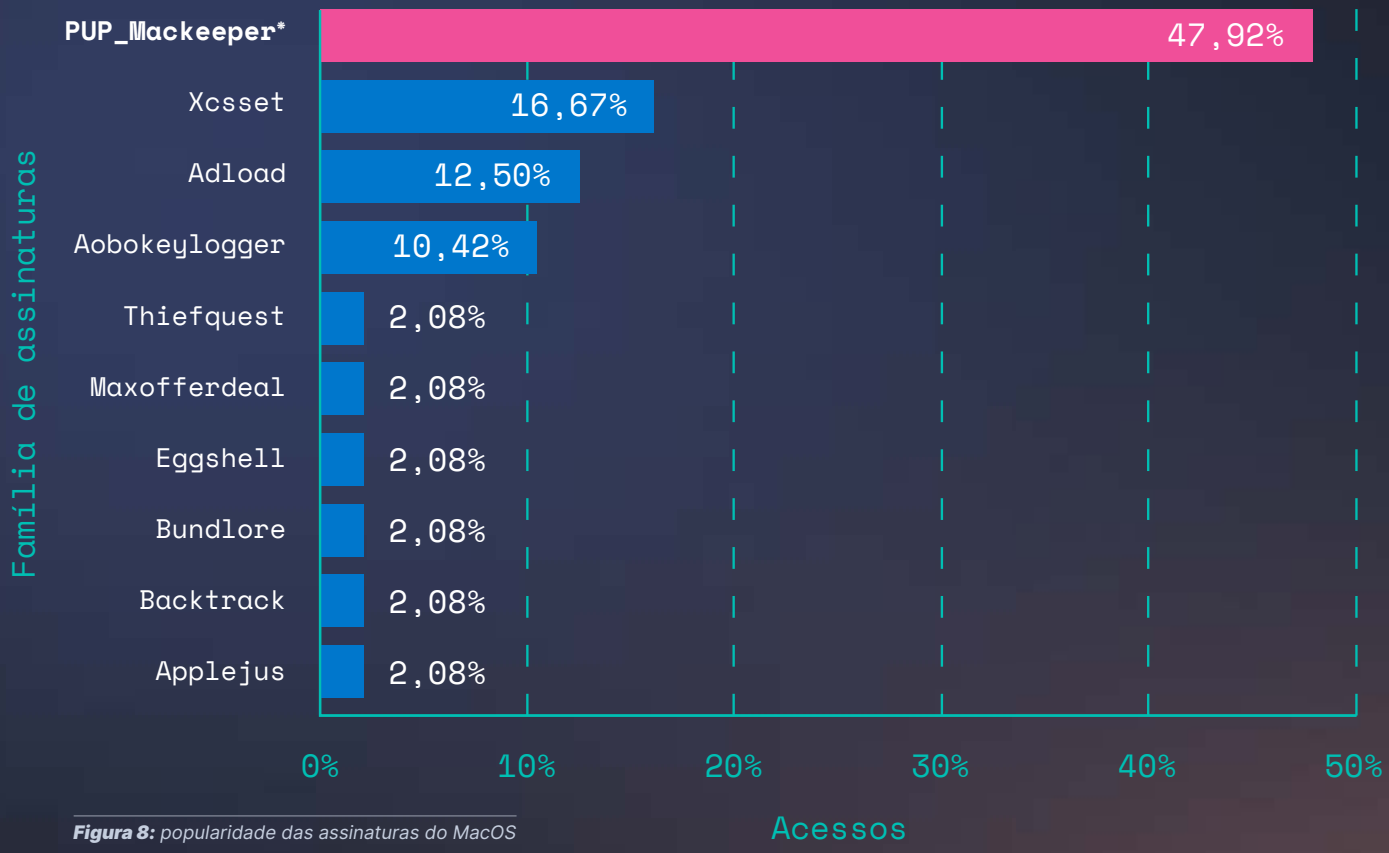


Figura 8: *popularidade das assinaturas do MacOS*

*Não caracterizamos o MacKeeper como malware, mas ele pode ser usado de forma inadequada

Embora a instalação e o uso de criptomineradore geralmente mirem endpoints do Linux e do Windows, o Elastic Security Labs observou algum uso em endpoints do MacOS, bem como variantes como mshelper e CreativeUpdater sendo populares. Deve-se notar que a distribuição e a vitimologia dos criptomineradores do MacOS podem se tornar cada vez mais populares, e os desenvolvedores utilizam o MacOS e o JavaScript para tarefas relacionadas ao trabalho. Como o Node Package Manager (NPM) é um gerenciador de pacotes comum para JavaScript, os criptomineradores podem ser distribuídos em pacotes maliciosos para endpoints do MacOS onde o trabalho de desenvolvimento é conduzido, contribuindo assim para a popularidade.

Tendências de comportamento dos endpoints

Abertura, transparência e colaboração são elementos centrais do Elastic Security. Como continuamos a defender esses princípios, nossa recente publicação de artefatos de proteção compartilhou a lógica comportamental dos endpoints que desenvolvemos para identificar o modus operandi do adversário usando a Elastic. Para este relatório, reunimos telemetria global sobre os alertas e recursos de prevenção integrados a partir dessa lógica de detecção.

Começando com os mapeamentos do MITRE ATT&CK® para nossas regras de comportamento do endpoint, o Elastic Security Labs descobriu que ~34% dos alertas se situavam no intervalo de evasão de defesas, seguidos pela execução em ~22% e pelo acesso a credenciais em ~10% conforme mostrado abaixo.

Isto indica *o papel que a evasão de defesas desempenha não apenas em ataques direcionados, mas em todos os ataques.* Além de contornar a instrumentação de segurança, as técnicas desta categoria também contornam a visibilidade, *resultando em maiores tempos de permanência para as ameaças e maiores sucessos.* Também sugere que a evasão de defesas tornou-se necessária para as ameaças que pressupõem que a instrumentação de segurança estará presente.

Sinais do endpoint por tática

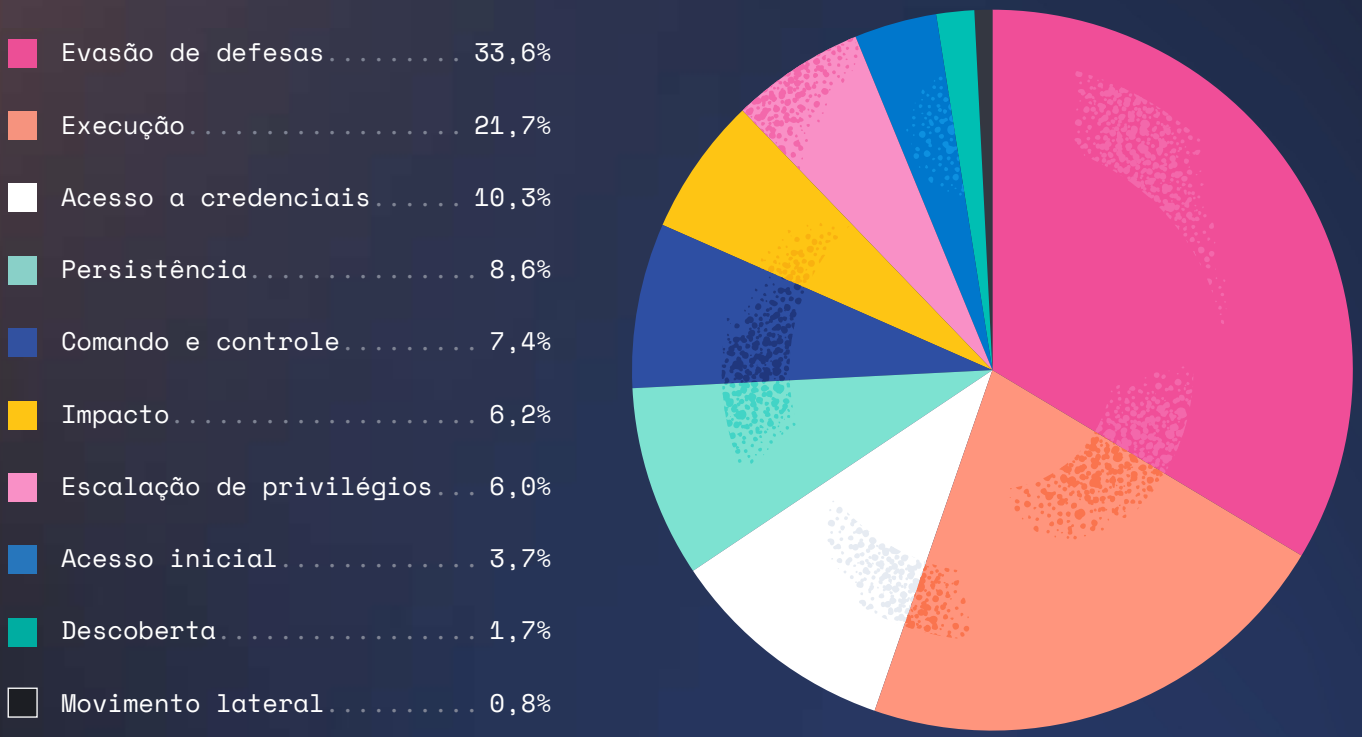


Figura 9: *Táticas do MITRE ATT&CK para regras de comportamento do endpoint*

Evasão de defesas

A técnica mais significativa que contribuiu para a evasão de defesas foi o mascaramento e a execução de proxy binário do sistema para uma porcentagem combinada de 72% de todas as técnicas de evasão de defesas. A execução de proxy binário do sistema descreve utilitários integrados e frequentemente assinados legitimamente que podem ser cooptados pelas ameaças para executar software malicioso, como malware. Muitos procedimentos para as subtécnicas conhecidas são conhecidos, com algumas tecnologias de segurança tendo dificuldade para identificar o software que elas são responsáveis por executar.

Disfarçar-se como um processo legítimo é outra técnica comum usada para evasão de defesas, buscando fugir de tecnologias de segurança que inspecionam software, scripts ou código em execução.

Aprofundando-se nos detalhes, a Elastic descobriu que o Rundll32 continua sendo fortemente usado de forma inadequada em diferentes estágios de ataques que afetam os sistemas Windows. Os adversários favorecem essa subtécnica, pois ela se encaixa na metodologia living-off-the-land (LotL), pela qual um adversário cria DLLs maliciosas que podem ser executadas a partir de um binário confiável e assinado do Windows. Esse utilitário é fortemente usado de forma inadequada durante muitas fases do ciclo de vida do ataque.

Além disso, o Regsvr32 é outro binário nativo do Windows comumente usado de forma inadequada, contribuindo para a alta porcentagem de alertas de evasão de defesas. Normalmente, o Regsvr32 é usado de forma inadequada em documentos maliciosos do Microsoft 365 (maldocs) para executar DLLs maliciosas ou registrar arquivos maliciosos.

Técnica	Porcentagem do sinal
Mascaramento	44,29%
Execução de proxy binário do sistema	30,00%
Manipulação de token de acesso	12,32%
Injeção de processo	7,62%
Trabalhos de BITS	4,74%
Execução de proxy de utilitários de desenvolvedores confiáveis	0,90%
Processamento de script XSL	0,66%
Enfraquecimento de defesas	0,65%
Exploração para evasão de defesas	0,64%
Execução de proxy de script do sistema	0,13%
Modificação do Registro	0,03%
Remoção do indicador no host	0,01%

Tabela 1: *técnicas de evasão de defesas*

Altas prioridades para monitorar incluem aplicações mshtml, msiexec, svchost, wefault, wemgr e runtimebroker. As organizações também devem examinar os utilitários padrão do Windows quando renomeados ou quando executados de diretórios não padrão — essas são metodologias comuns. Não é incomum que os adversários adulterem direta e indiretamente o Windows Defender.

Acesso inicial e execução

O acesso inicial e a execução geralmente estão próximos um do outro durante uma invasão, com uma relação clara entre os estágios da invasão.

Durante a análise das técnicas de acesso inicial, o Elastic Security identificou uma proporção significativa de alertas de endpoints do Windows provenientes de ambientes nos quais o Microsoft Office foi implantado e emails com links ou anexos maliciosos foram recebidos.

Iscas de vários tipos (por exemplo, documento anexado, objeto ISO, arquivo LNK, objeto de script) usadas como armas continuam a representar as abordagens mais comuns para o acesso inicial. Essas técnicas miram o destinatário e, na maioria das vezes, dependem de sua cooperação para obter sucesso.

> *Os leitores devem observar que as decisões da Microsoft de desabilitar o suporte para macros até 27 de julho de 2022 tornaram os objetos LNK e ISO mais confiáveis para o uso de cargas úteis como armas do que iscas de documentos. Prevemos que isso seja provável, e famílias de malware amplamente distribuídas como o ICEDID já estão adotando essa abordagem.*

A tabela a seguir descreve as técnicas de acesso inicial e execução mais comuns.

Nome da regra	Porcentagem do sinal
Processo filho suspeito do Microsoft Office	34,00%
Ofuscação do PowerShell gerada via Microsoft Office	16,33%
Cargas do RunDLL32/Regsvr32 soltaram um executável	13,47%
Execução suspeita por meio de um arquivo de imagem montado	5,24%
Execução de um arquivo ISO baixado	5,00%
Processo filho do Microsoft Equation Editor	3,66%
Carregamento de imagem WMI via Microsoft Office	2,93%
Execução suspeita via suplementos do Microsoft Office	2,56%
Possível execução remota de arquivo via MSIEXEC	2,44%
Acesso inicial ou execução via aplicativo do Microsoft Office	2,44%

Tabela 2: *10 principais regras de acesso inicial da Elastic disparadas*

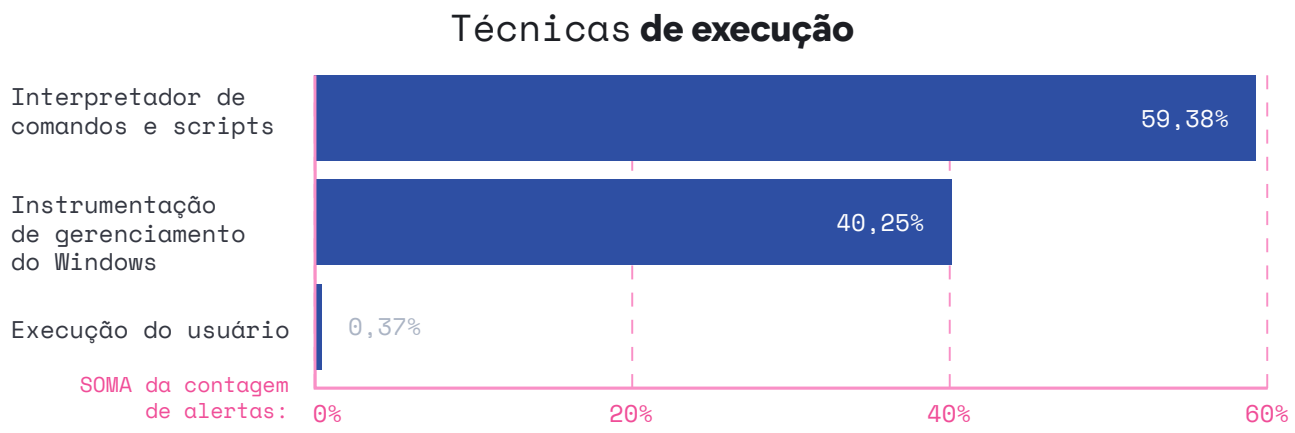


Figura 10: *técnicas de execução*

Com relação à execução, o Elastic Security Labs descobriu que ~59% das técnicas de execução estavam relacionadas a interpretadores de scripts nativos e de comando, seguidas por 40% atribuídos exclusivamente a uso inadequado da Instrumentação de Gerenciamento do Windows (WMI). Isso é especialmente verdadeiro para endpoints do Windows, onde os adversários usam o PowerShell, o Windows Script Host e arquivos de atalho do Windows de forma inadequada para executar comandos, scripts ou binários.

Conforme mostrado abaixo, novamente vemos o *RunDLL32*, um binário nativo do Windows, sendo usado de forma inadequada por adversários durante estágios posteriores de uma invasão. Além disso, o Elastic Security geralmente observa que o Windows Script Host (*`wscript.exe`* ou *`cscript.exe`*) é usado para executar código malicioso em arquivos do Visual Basic Script (VBS) e do JavaScript (JS).

Nome da regra	SOMA da contagem de alertas
Atividade do shell de comando iniciada via RunDLL32	27,53%
Execução de um script do Windows com extensão de arquivo incomum	25,95%
Processo filho suspeito do interpretador de script do Windows	13,51%
Execução de um diretório incomum	11,56%
Processo de script do Windows suspeito	9,07%
Execução suspeita do PowerShell via scripts do Windows	4,21%
ImageLoad incomum do mecanismo do PowerShell	2,88%
Execução de um arquivo gravado pelo Windows Script Host	1,91%
Execução de um script do Windows a partir do arquivo morto	0,63%
Execução de um script do Windows baixado por meio de um LOLBIN	0,60%

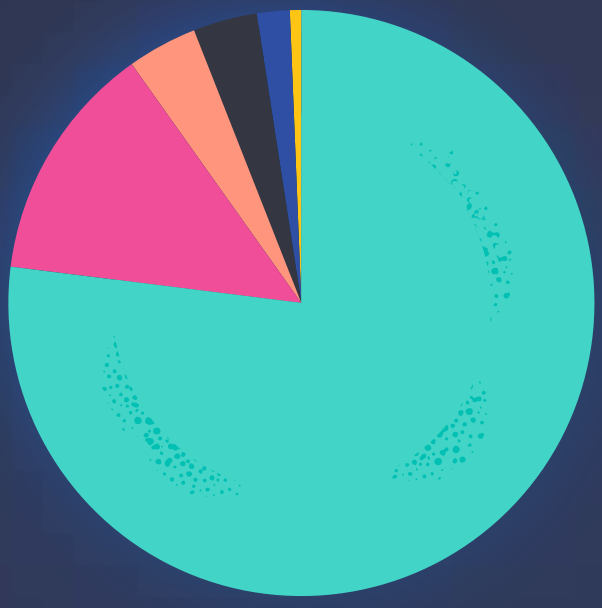
Tabela 3: *regras de execução da Elastic disparadas*

Acesso a credenciais

Com a tendência contínua nos ambientes de implantação híbrida entre hospedagem local e provedores de serviços em nuvem (CSPs), os adversários continuam a usar contas válidas, pois essas contas atraem menos suspeitas para os administradores. Isso, aliado a técnicas de living-off-the-land (LoTL), pode causar dificuldades para os defensores distinguirem as atividades esperadas das potencialmente maliciosas. Como resultado, o acesso a credenciais não é apenas uma tática comum em endpoints, mas também em ambientes de CSP; isso foi destacado na seção de descobertas globais das tendências de segurança na nuvem.

Aproximadamente 77% de todas as técnicas de acesso a credenciais são atribuídas ao despejo de credenciais do sistema operacional com utilitários comumente conhecidos, também conhecidos como "ferramentas de despejo", pois permitem que o adversário despeje credenciais na forma de um hash ou texto não criptografado do sistema operacional.

Técnicas de acesso a credenciais



- Despejo de credenciais do sistema operacional.....76,98%
- Credenciais de armazenamentos de senhas.....13,19%
- Captura de entrada.....3,86%
- Credenciais não seguras.....3,53%
- Roubar ou forjar tíquetes do Kerberos.....1,81%
- Roubar cookies de sessão da web.....0,63%

Figura 11: *técnicas de acesso a credenciais*

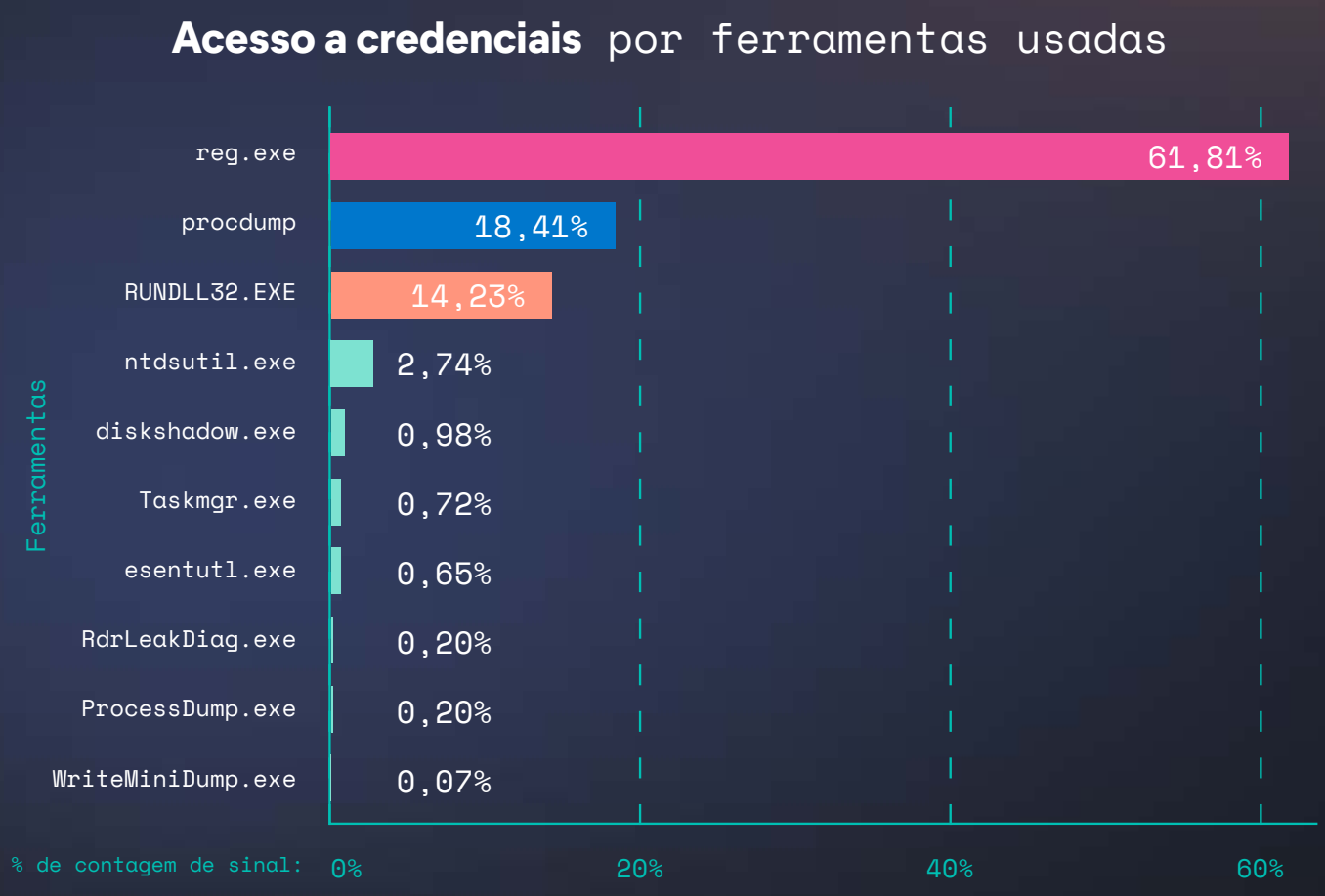
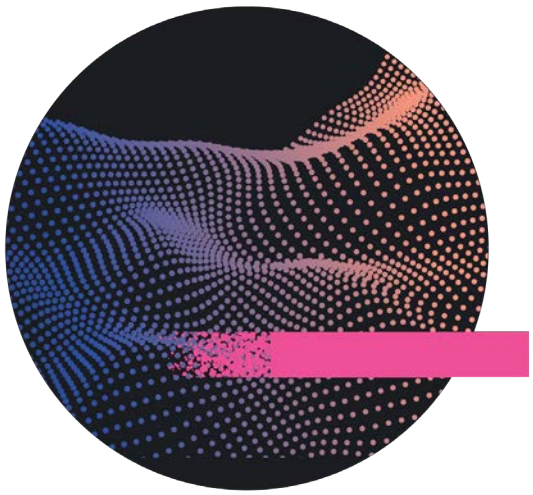


Figura 12: *acesso a credenciais por ferramentas usadas*

Conforme mostrado abaixo, reg, procdump e RunDLL32 estão fortemente representados em nossos dados devido, em grande parte, ao fato de serem utilitários benignos nos quais os recursos antimalware da Elastic normalmente não interferem. Ferramentas comumente usadas como o Mimikatz costumam ser vistas com muito menos frequência, devido a uma abordagem em camadas para a proteção contra malware. Em relação ao Registro em endpoints do Windows, reg save e reg export podem ser usados para interagir diretamente com o Registro por meio do gerenciador de contas de segurança (HKLM\\SAM) ou do banco de dados de políticas LSASS (HKLM\\SECURITY).

Veja abaixo uma tabela de sinais de acesso a credenciais da telemetria do Elastic Security com detalhes adicionais sobre o que está sendo detectado.



Nome da regra	SOMA da contagem de alertas
Acesso a credenciais via utilitários conhecidos	33,37%
Acesso ao Registro do Security Account Manager (SAM)	17,96%
Acesso suspeito ao Registro de segredos de LSA	11,18%
Possível acesso a credenciais via Mimikatz	10,72%
Possível descoberta do armazenamento do Gerenciador de Credenciais do Windows	3,99%
Possível phishing de credenciais via OSASCRIPT	3,86%
Possível descoberta de chaves mestras DPAPI	3,57%
Acesso a arquivos sensíveis – chaves SSH salvas	3,16%
Acesso a arquivos do Security Account Manager (SAM)	2,92%
Acesso a credenciais do navegador da web por meio de um processo incomum	2,14%

Tabela 4: *nome da regra e soma dos alertas*

Persistência

Mecanismos comuns de persistência envolvendo as subchaves Run/RunOnce do Registro e tarefas agendadas foram os mais observados. Embora essa seja uma tendência nada surpreendente, ela representa técnicas em uso perpétuo por um tempo significativo — tão válida hoje quanto em 2012.

Esses mecanismos de persistência contam com a funcionalidade básica do sistema operacional com casos de uso benignos e consistentes, que é um dos motivos pelos quais os adversários os usam. Essas informações são confirmadas pelo gráfico abaixo, onde vemos que ~87% de todas as técnicas de persistência são de inicialização ou de execução de início automático no logon.

Técnicas **de persistência**

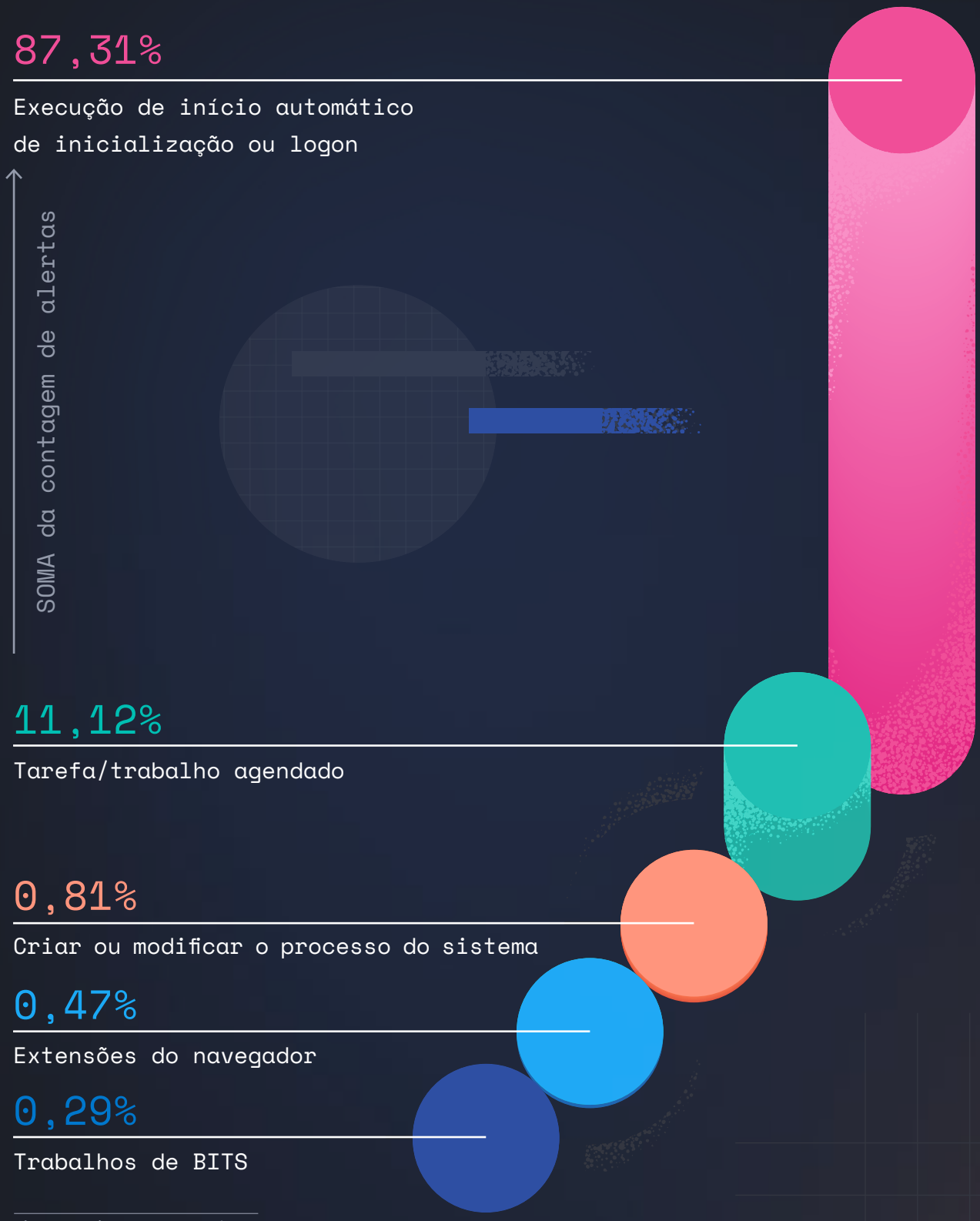


Figura 13: *técnicas de persistência*

O Elastic Security Labs descobriu que a maioria desses sinais se relacionava à criação ou modificação de chaves ou arquivos de execução do Registro na pasta de inicialização dos endpoints do Windows. Ações não executadas pela conta do sistema local — processos esperados como PowerShell, Windows Update Agent, Windows Installer e alguns outros — indicariam atividades atípicas dignas de investigação.

Uma ação particularmente comum que identificamos foi a criação de arquivos de atalho do Windows (LNK) pelo Host de Serviço (svchost) do Windows na pasta Inicializar de um usuário, que geralmente aponta diretamente para um binário nativo como cmd.exe ou powershell.exe para executar uma carga útil ou script previamente instalado. Isso geralmente é feito como um mecanismo de persistência para garantir que o código malicioso seja executado mesmo se o endpoint for reinicializado. O Elastic Security Labs observou essa mesma técnica durante nossa descoberta e análise do BLISTER.

Devido em grande parte aos servidores Exchange locais sem patches, o Elastic Security Labs observou uma correlação notável, mas estatisticamente insignificante, entre as vulnerabilidades do Exchange anunciadas no início deste ano e a presença de webshells (malware baseado na web que as ameaças podem chamar sob demanda).

Tendências de segurança na nuvem

O Elastic Security utiliza a telemetria global dos clientes que utilizam as regras de detecção pré-configuradas para analisar ameaças baseadas na nuvem e possíveis ataques. Essa telemetria proporciona ao Elastic Security Labs um tremendo insight sobre as possíveis ameaças que os clientes veem diariamente no Microsoft Azure, na Amazon Web Services (AWS) e no Google Cloud.

> *Para a análise a seguir, o Elastic Security Labs concentrou-se em eventos baseados na nuvem dos nossos clientes e recebidos entre abril e agosto de 2022.*

Descobertas globais

O Elastic Security Labs analisou a telemetria dos clusters de clientes que utilizavam nossas regras de detecção pré-criadas de SIEM para Microsoft Azure, AWS e Google Cloud — um subconjunto de todos os clientes que compartilham a telemetria. Aproximadamente 57% desses eventos foram atribuídos especificamente à AWS, seguidos por ~22% para o Google Cloud e ~21% para o Microsoft Azure. Comparando isso com os alertas gerais de detecção de ameaças, incluindo endpoints, as detecções baseadas na nuvem representaram ~5% de todos os alertas globais de detecção de SIEM.

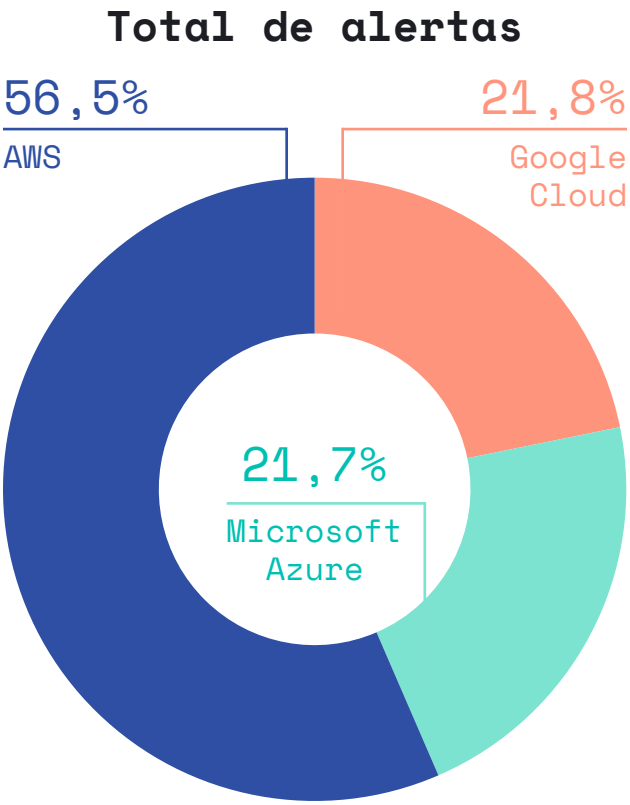


Figura 14: *porcentagens do total de alertas de detecção baseados na nuvem por CSP*

Os eventos relacionados às detecções da AWS representam mais da metade de todos os eventos baseados na nuvem que recebemos. De acordo com a Statista, a AWS detém cerca de 34% da participação no mercado de provedores de serviços de infraestrutura de nuvem. entretanto, é possível que nossos clientes prefiram a AWS, e isso poderia influenciar nossa visibilidade. A AWS e o Microsoft Azure expõem mais de 200 serviços em seus portfólios e mais de 100 outros estão disponíveis para o Google Cloud, o que sugere que a superfície de ataque para esses CSPs é substancial.

Com foco nas táticas e técnicas, as regras de detecção pré-criadas do Elastic Security são mapeadas para a matriz do MITRE ATT&CK para cada CSP. Quase 33% de todos os alertas de nuvem estavam relacionados ao acesso a credenciais em todos os CSPs, e a Elastic notou que o acesso inicial frequentemente coincidia.

À medida que as empresas continuam a adotar os serviços e recursos oferecidos pelos CSPs, os ambientes locais tradicionais estão lentamente fazendo a transição para modelos híbridos e, em alguns casos, implantações completas na nuvem. Isso aumenta a necessidade de gerenciar não apenas usuários de gerenciamento de identidade e acesso (IAM), mas também contas de serviço que acessam esses recursos e aplicações. Se esses ambientes se tornarem inseguros (por exemplo, com senhas fracas permitidas, funções com excesso de privilégios, chaves de API e tokens de acesso armazenados em texto não criptografado ou em cache em máquinas virtuais), os riscos associados, independentemente da implantação, aumentarão significativamente.

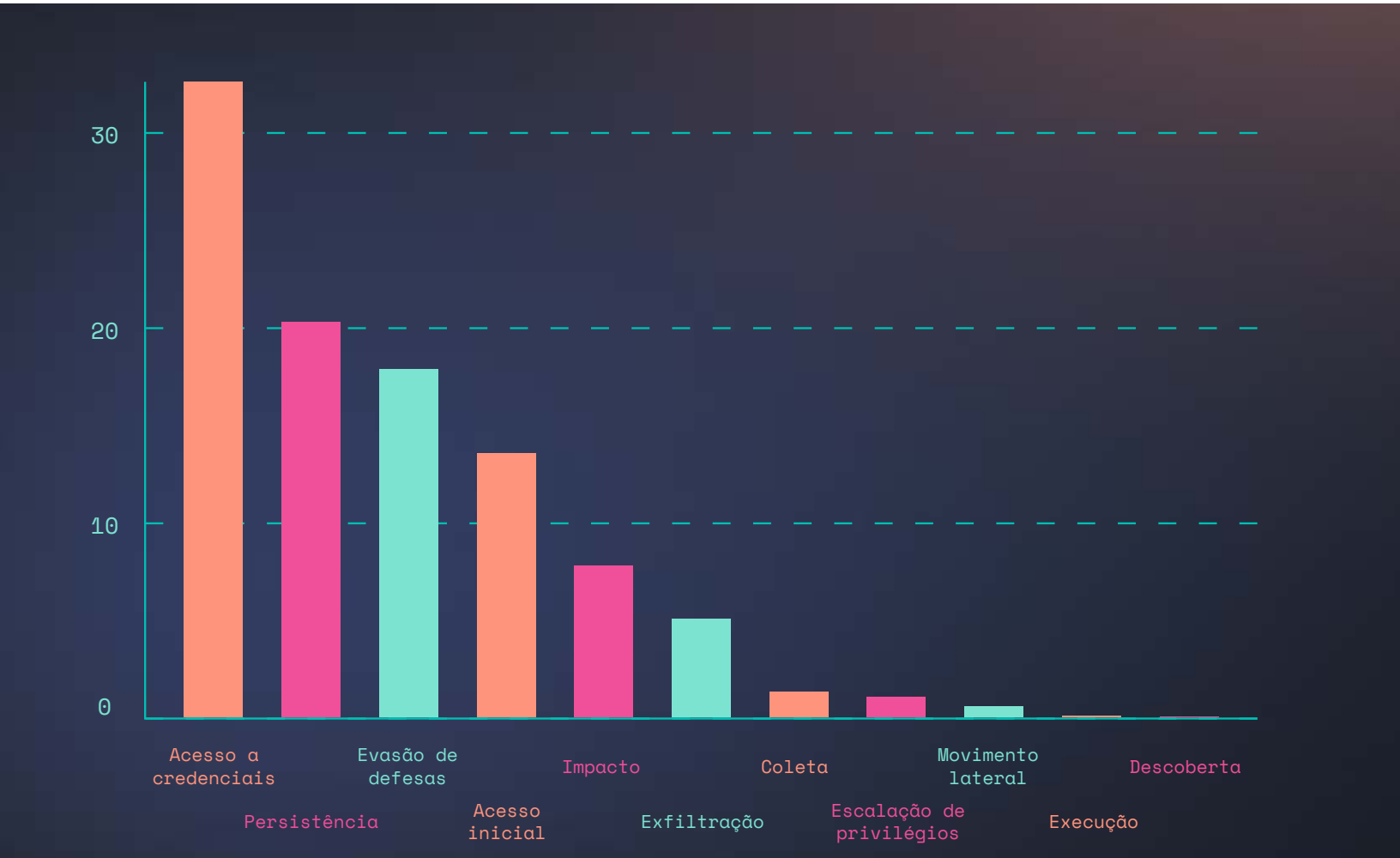


Figura 15: *porcentagens do total de nomes de táticas do MITRE ATT&CK para alertas de detecção baseados na nuvem*

O Elastic Security Labs descobriu que cerca de 58% das tentativas de acesso inicial usaram uma combinação de tentativas tradicionais de força bruta e password spraying de contas anteriormente comprometidas. Quase 41% dos alertas de acesso a credenciais estavam tentando roubar tokens de acesso a aplicações (em comparação com outros elementos com credenciais), com aproximadamente 1% das tentativas contando com credenciais inseguras padrão. Embora 1% possa parecer uma pequena porcentagem, observamos que essas tentativas afetaram o Google Cloud e o Microsoft Azure, mas não a AWS, o que pode representar um viés em nossa visibilidade.

Os riscos associados ao roubo de credenciais geralmente são grandes, pois esses serviços permitem que os adversários se movimentem lateralmente dos espaços de trabalho para os consoles de gerenciamento dos CSPs se uma conta válida é comprometida e as funções ou permissões não são definidas corretamente.

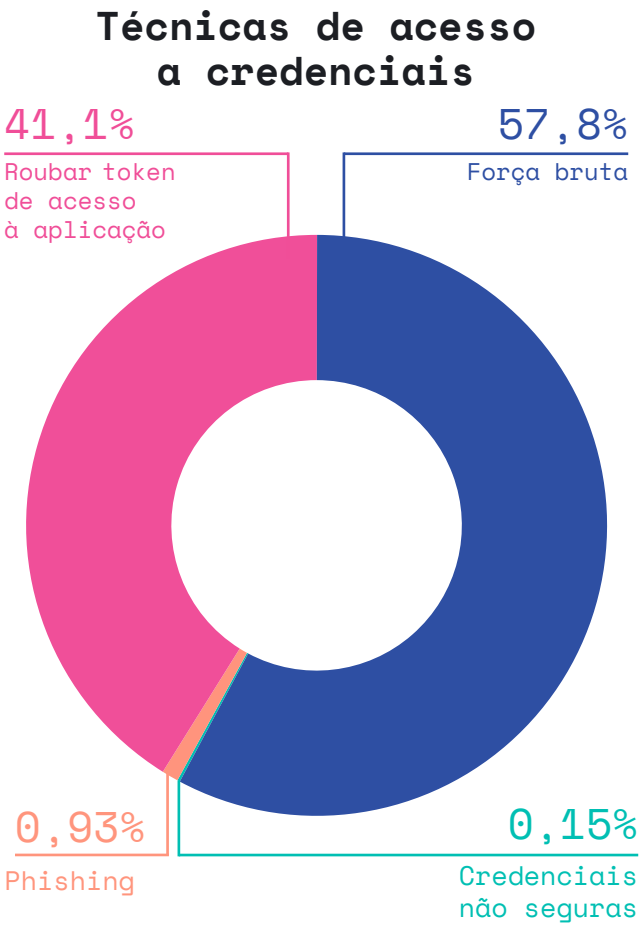


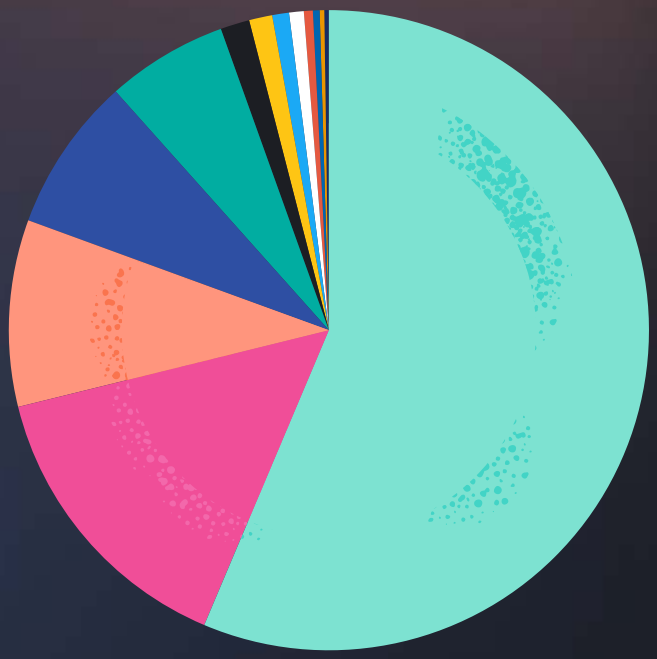
Figura 16: *porcentagens de técnicas do MITRE ATT&CK para tática de acesso a credenciais*

Enquanto os CSPs competem para fornecer serviços semelhantes aos clientes e, portanto, a superfície de ataque das ameaças pode ser semelhante, o Elastic Security Labs optou por analisar brevemente os alertas de detecção de cada CSP para identificar tendências de ameaças específicas que devem ser trazidas à atenção dos nossos leitores.

Descobertas da AWS

Conforme afirmamos anteriormente, a AWS responde por quase 34% do mercado atual de CSPs, com um vasto catálogo de ofertas. Durante a análise, o Elastic Security Labs descobriu que o acesso a credenciais, o acesso inicial e a persistência totalizaram 74% de todos os alertas de detecção. Embora a escalação de privilégios seja algo que poderíamos supor ser maior, ela representou menos de 2% dos alertas.

Técnicas **da AWS**



Roubar token de acesso a aplicação	56,36%
Execução	14,78%
Enfraquecimento de defesas	9,43%
Transferência de dados para conta na nuvem	7,82%
Destruição de dados	6,12%
Interrupção do serviço	1,47%
Contas válidas	1,17%
Uso de material de autenticação alternativo	0,85%
Mecanismo de controle de elevação de abuso	0,74%
Manipulação de conta	0,45%
Outros	0,34%
Remoção de acesso a conta	0,23%
Serviços remotos externos	0,23%

Figura 17: *porcentagens relativas às técnicas do ATT&CK identificadas nas técnicas da AWS*

Conforme mostramos acima, ~57% de todas as técnicas observadas na AWS estavam relacionadas à tentativa de roubo de token de acesso à aplicação. Isso geralmente está relacionado a credenciais temporárias recuperadas do Security Token Service (STS) da AWS por meio da chamada de API GetSessionToken. Com a execução, o Elastic Security Labs observou o uso inadequado da AWS CLI para aproveitar o recurso Systems Manager para chamar documentos pré-criados em uma instância gerenciada no EC2. Isso pode ser especialmente útil para descoberta e enumeração ou pode ser mais avançado e usado para mirar um host do Windows em combinação com um documento criado para execução do PowerShell localmente.

Embora possa parecer trivial e produzir sinais verdadeiros positivos benignos, o Elastic Security Labs cria uma lógica de detecção para cada CSP no qual recursos de logging, armazenamento ou arquivos são excluídos. Muitas vezes, os ambientes dos CSP são configurados de forma que o logging é ingerido em um único pipeline ou recurso de armazenamento e se torna um único ponto de falha se excluído, pois não existiria qualquer vestígio de invasão de um adversário e seria problemático para o trabalho de resposta a incidentes (IR). Quase 9% dos sinais da AWS envolviam uma combinação de fluxo de log, grupo e exclusão de alarme.

Vimos que 57% dos alertas da AWS vieram de ambientes do Elastic Compute Cloud (EC2). Quando um ambiente do EC2 é configurado incorretamente e permite acesso remoto com credenciais padrão, o procedimento mais comum instrui o adversário a identificar usuários, tokens e chaves de acesso do IAM. Os metadados da instância do EC2 frequentemente incluem informações semi-sensíveis. Nessas condições, até ameaças de baixa maturidade conseguem obter acesso de forma trivial. Cerca de 39% dos alertas gerados pelo EC2 CloudTrail enfatizaram que o alvo eram as contas de usuário do IAM — chaves secretas nesses ambientes podem estar em maior risco.

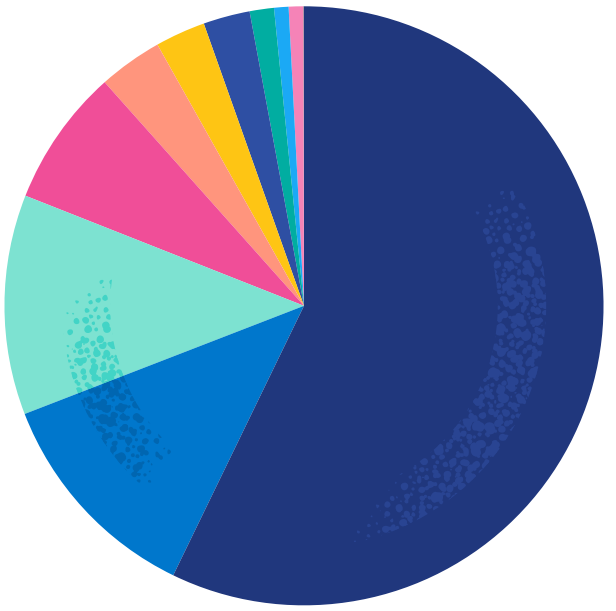
Descobertas do Microsoft Azure

O Microsoft Azure pode apresentar um risco maior do que a AWS ou o Google Cloud à medida que as empresas fazem a transição de modelos locais para ambientes híbridos ou integralmente na nuvem. Recursos críticos e que são alvos frequentes, como o Active Directory (AD) e o SharePoint, são gerenciados no Microsoft Azure. O Elastic Security descobriu que 96% dos alertas observados do Microsoft Azure estavam relacionados a eventos de autenticação. As contas válidas foram usadas com mais frequência na tentativa de recuperar tokens OAUTH2, realizar ataques de phishing e outras técnicas.

O efeito combinado de várias técnicas maliciosas juntas também estava presente no Microsoft Azure, onde uma técnica como a criação de um runbook de automação do Microsoft Azure posteriormente resultou na criação de backdoors ou um ataque de concessão de consentimento permitiu que um invasor solicitasse detalhes sobre usuários válidos. Muitas vezes, as entidades de serviço do Microsoft Azure são o alvo para o comprometimento inicial da conta válida, pois essas identidades são criadas para uso com aplicações, ferramentas de automação e serviços locais nos quais um código pode ser executado em uma VM como o usuário SYSTEM local.

Se um adversário conseguiu comprometer uma conta válida e tem acesso a uma máquina virtual, a invasão típica é utilizar a interface de linha de comando (CLI) do Microsoft Azure para descoberta e enumeração adicionais. O uso de comandos como account, resource, keyvault e network permite que um adversário visualize informações sensíveis de assinatura do Microsoft Azure sobre esse usuário autorizado específico. Relacionado a isso, o run-command foi frequentemente observado sendo executado em VMs do Microsoft Azure. Esse recurso no Microsoft Azure usa um agente que é instalado nas máquinas virtuais do Microsoft Azure quando elas são provisionadas. O risco associado é baseado nos scripts pré-configurados do PowerShell que vêm instalados com o recurso e que, se usados inadequadamente, permitem que um adversário modifique ou obtenha insights facilmente sobre a infraestrutura do Microsoft Azure, execute scripts na VM ou acesse recursos e aplicações críticos.

Técnicas do Microsoft Azure



Contas válidas	57,19%
Roubar token de acesso a aplicação	11,93%
Phishing	11,87%
Uso de material de autenticação alternativo	7,42%
Manipulação de conta	3,45%
Sequestro de recursos	2,71%
Credenciais não seguras	2,52%
Interpretador de comandos e scripts	1,31%
Exploração de aplicação voltada para o público	0,78%
Descoberta de serviço na nuvem	0,78%
Transferência de dados para conta na nuvem	0,02%
Dados do objeto de armazenamento na nuvem	0,02%

Figura 18: *porcentagens relativas às técnicas do ATT&CK identificadas em ambientes do Microsoft Azure*

O Microsoft Azure PowerShell é outro recurso nativo comumente usado de forma inadequada que os adversários podem aproveitar se uma conta válida com permissões ou funções não restritivas é comprometida. Existem vários módulos pré-criados para interagir não apenas com a VM na qual a conta está, mas também com recursos e aplicações como Microsoft Azure SQL, Blobs de Armazenamento do Microsoft Azure e, é claro, Microsoft Azure Active Directory.

Descobertas do Google Cloud

Da mesma forma que o Microsoft Azure e o Office 365 representam uma superfície de ataque combinada, a superfície de ataque do Google Cloud é aumentada pelo Google Workspace, onde aplicações como Google Drive e Gmail são vitais para as empresas. Embora este relatório não se concentre especificamente no Google Workspace, o Elastic Security Labs desenvolve ativamente regras de detecção de ameaças disponíveis publicamente.

O Google Cloud oferece aos clientes e desenvolvedores uma arquitetura e configuração diretas que oferecem intermitência de nuvem gerenciável, chatbots para prevenção de perda de dados (DLP), suporte de backend para apps para celular, endpoints virtuais no Google Compute Engine (GCE) e muito mais.

Independentemente dos motivos pelos quais os clientes confiam no Google Cloud, o comprometimento das contas de serviço permanece desenfreado quando as credenciais padrão da conta não são alteradas. Cerca de 54% dos alertas dos ambientes do Google Cloud estavam relacionados ao uso inadequado de contas de serviço, embora não esteja claro quantos deles se aproveitaram das credenciais padrão. Embora a geração de chave de conta de serviço seja um método de persistência válido, muitas vezes é desnecessário se o "iam.serviceAccountTokenCreator" é simplesmente aplicado a uma conta válida que o adversário já tenha comprometido.

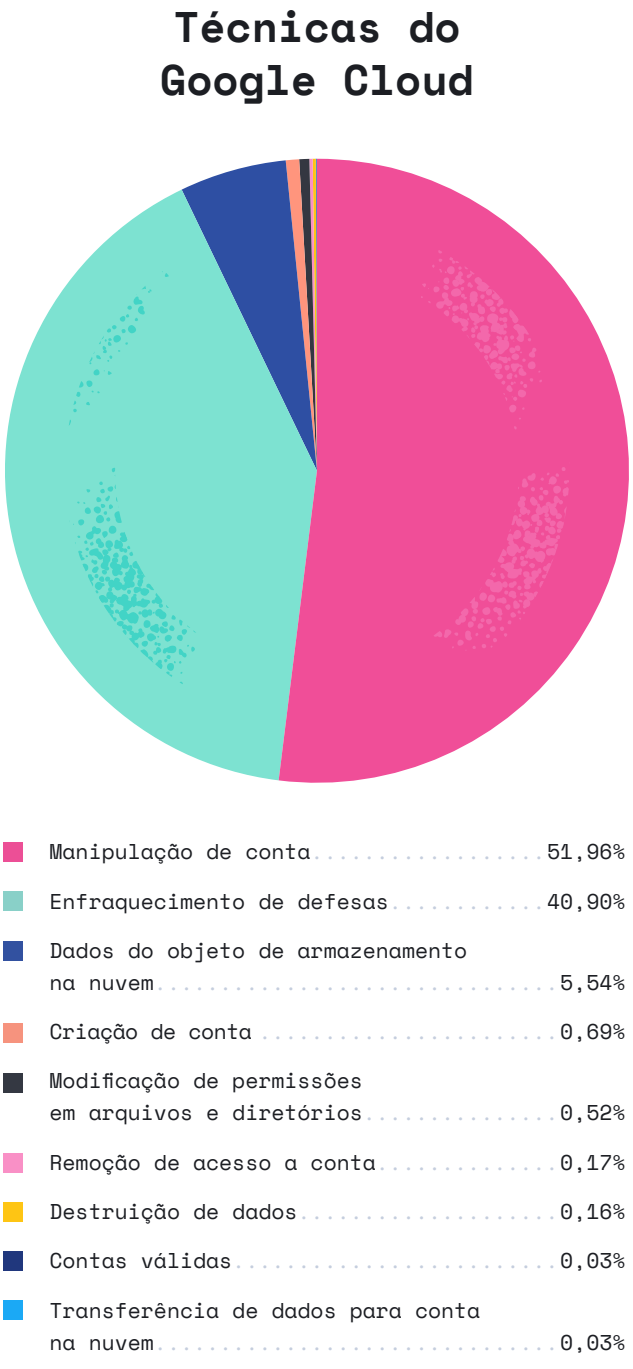


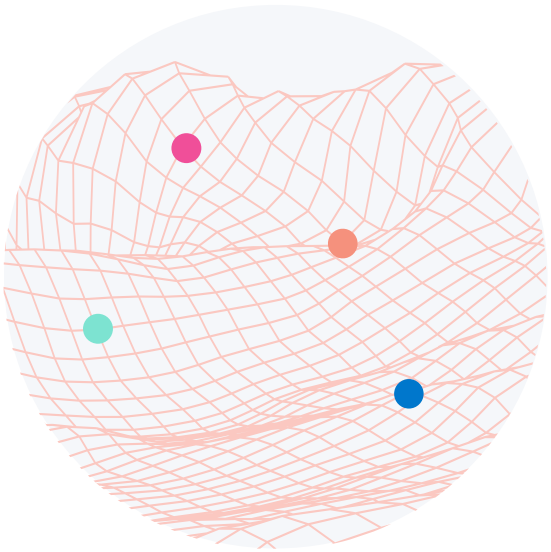
Figura 19: *porcentagens relativas às técnicas do ATT&CK identificadas nas técnicas do Google Cloud*

Perfis de ameaças

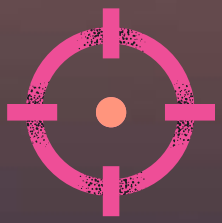
Esta seção resume os perfis de ameaças desenvolvidos pela Elastic no último ano e para os quais temos insights de telemetria exclusivos. A Elastic utiliza os dados de telemetria para descobrir e rastrear ameaças.

Quatro grandes grupos de atividades estão representados:

- **BLISTER** [REF7890]
- **PHOREAL** [REF4322]
- **CUBA** [REF9019]
- **QBOT** [REF3726]



Para cada grupo listado, forneceremos um diagrama convencional conhecido como Modelo Diamante, que descreve as relações entre adversários, infraestrutura, recursos e vítimas. Para melhorar a legibilidade, reduzimos as sobreposições com grupos rastreados por outros fornecedores, mas os leitores devem observar que isso não indica acordo ou desacordo com esses fornecedores.



O Modelo Diamante

Utilizamos o Modelo Diamante para descrever relacionamentos gerais entre adversários, recursos, infraestrutura e vítimas de invasões. Esse modelo costuma ser usado de maneira centrada na invasão, mas aqui o empregamos com foco no adversário para demonstrar observações sobre muitos incidentes.

Terminologia

Grupo de atividade: indivíduos, grupos ou organizações que se acredita estarem operando com intenção maliciosa. Prefixamos esses grupos de atividades com a string REF e uma sequência de números para distinguir nossa visibilidade da visibilidade de outros.

Padrão de ataque: descreve as maneiras pelas quais os adversários tentam comprometer os alvos.

Conjunto de invasão: comportamentos adversários e recursos com propriedades comuns que se acredita serem orquestrados por uma única organização.

Blister [REF7890]

Em 22 de dezembro de 2021, a Elastic descobriu uma nova forma de carregador de malware que chamamos de BLISTER. Após a execução, o carregador BLISTER descriptografou um backdoor de dentro de si e o executou na memória, afetando o ambiente de um único cliente. Este grupo de atividade se sobrepõe a alguns rótulos de terceiros.

A Figura 20 mostra os metadados de assinatura de código presentes nesse carregador inicial, o que indica que o binário tinha sido preparado quase dois meses antes de sua descoberta pela Elastic. A assinatura digital listou "Blist LLC" como a entidade de assinatura, daí o nome desta família de carregadores. Os leitores devem estar cientes de que uma carga útil afetada pelo BLISTER pode ser assinada por qualquer uma das várias autoridades certificadoras de baixo custo, nenhuma das quais deveria legitimamente assinar o binário com backdoor.

"BLISTERizar" uma aplicação benigna tem o efeito de garantir que a maior parte do código do binário também seja benigna. Os recursos de machine learning que não incorporam software benigno nos dados de treinamento podem ser enganados por essa abordagem, e o uso de assinaturas de código válidas geralmente engana os analistas humanos. Essa metodologia de ofensa detalhada pode ser eficaz para contornar uma ampla gama de mitigações empresariais.

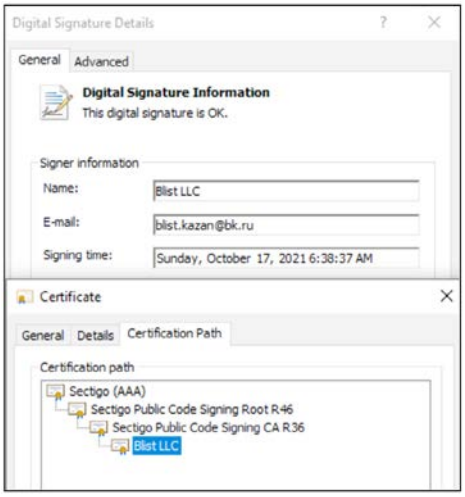


Figura 20: *metadados de assinatura de código do carregador BLISTER*

O que é a ameaça?

BLISTER é um carregador de malware furtivo usado para executar cargas úteis por meio de várias técnicas. Como praticamente qualquer aplicação benigna pode ser modificada para se converter em um carregador do tipo BLISTER, uma característica dessa metodologia é que os carregadores BLISTER herdam metadados de assinatura de código que geralmente contornam controles de segurança frágeis.

Qual é o impacto?

O REF7890 usa o BLISTER para carregar implantes, incluindo a ferramenta de segurança ofensiva (OST) Cobalt Strike e o backdoor BitRat. Eles fornecem uma ampla variedade de recursos de acesso remoto a um host infectado. Em todas as observações da Elastic, o BLISTER foi usado para facilitar o roubo de dados e a extorsão.

Qual foi a resposta da Elastic?

A Elastic fornece detecções e prevenções prontas para uso para o carregador BLISTER. Além disso, a Elastic divulgou publicamente regras do YARA, consultas de caça, uma análise detalhada da campanha e do malware e um extrator de configuração.

Saiba mais

- BLISTER Loader (Carregador BLISTER)
- BLISTER Malware Campaign (Campanha do malware BLISTER)
- BLISTER Configuration Extractor (Extrator de configuração do BLISTER)

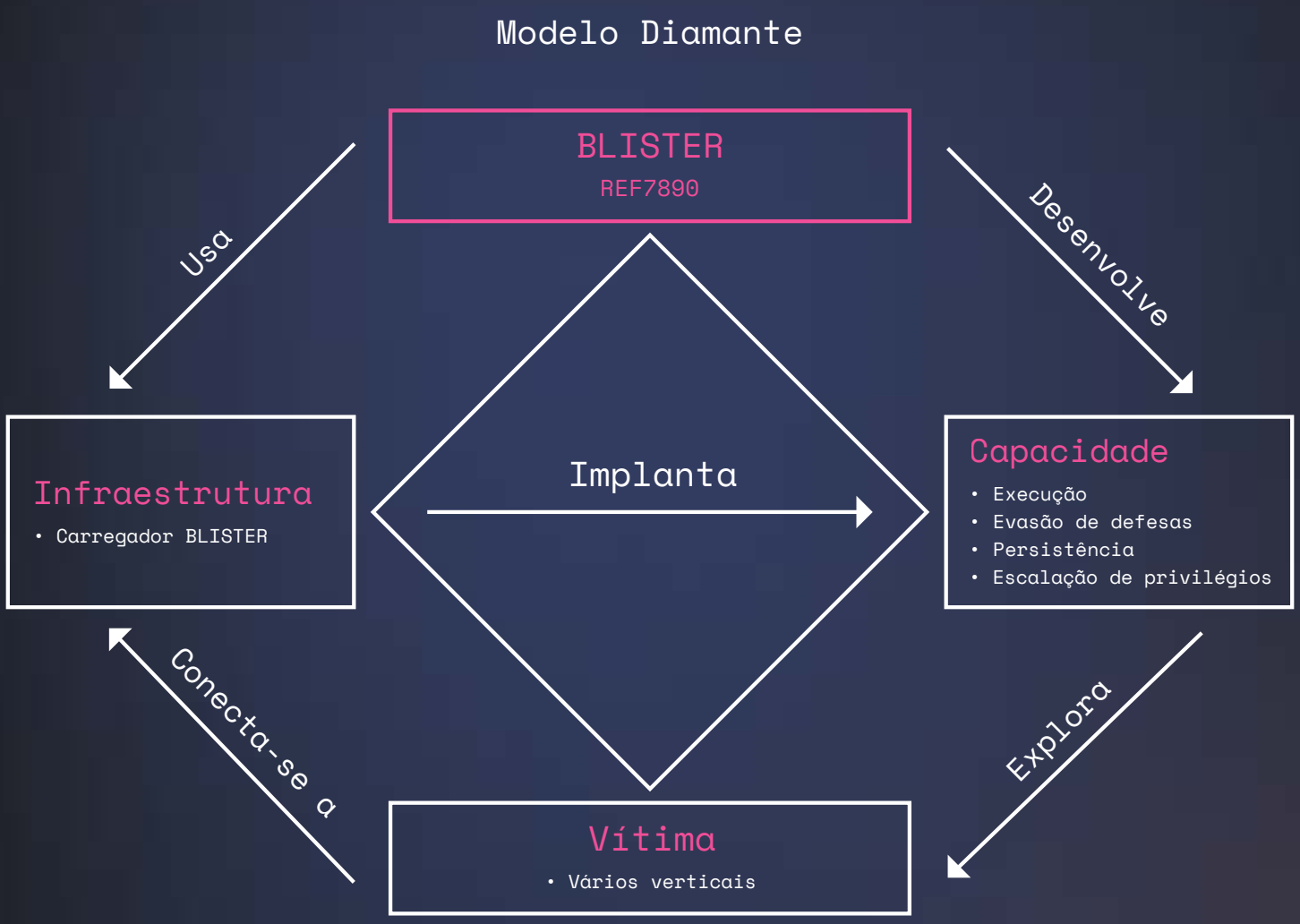


Figura 21: *Modelo Diamante do BLISTER*

Phoreal [REF4322]

No início deste ano, a Elastic identificou a presença do backdoor PHOREAL (muitas vezes chamado de backdoor RIZZO) afetando instituições financeiras vietnamitas. O que fez essa infecção se destacar foi o uso de evasões na memória que não foram vistas anteriormente no implante. Esses alertas específicos foram interessantes porque todos ocorriam no mesmo cluster e, de maneira incomum, visavam o processo control.exe. O processo control.exe do Windows lida com a execução dos itens do Painel de Controle, que são utilitários que permitem aos usuários visualizar e ajustar as configurações do computador. As notas da Elastic se sobrepõem aos rótulos de terceiros APT32 e OCEANLOTUS.

O que é a ameaça?

PHOREAL é um backdoor completo que permite acesso inicial e operações pós-exploração para obter os dados da vítima. Os operadores do PHOREAL estão ativos desde pelo menos 2014, embora a metodologia e as capacidades tenham evoluído ao longo do tempo.

Qual é o impacto?

O REF4322 tem como alvo principalmente vítimas dos setores público e privado no sudeste da Ásia, especificamente no Vietnã. A Elastic avalia com confiança moderada que essa ameaça persegue objetivos de estado, e a vitimologia sugere espionagem econômica, política e industrial como objetivos.

Qual foi a resposta da Elastic?

A equipe do Elastic Security detalhou como fazer a triagem de um desses alertas de ameaças, extraiu observáveis para filtragem de endpoint e rede e produziu uma nova assinatura de malware para identificação e mitigação da ameaça em toda a frota de Elastic Agents implantados.

Saiba mais

- PHOREAL Malware Targets the Southeast Financial Sector (Malware PHOREAL tem como alvo o setor financeiro do sudeste asiático)

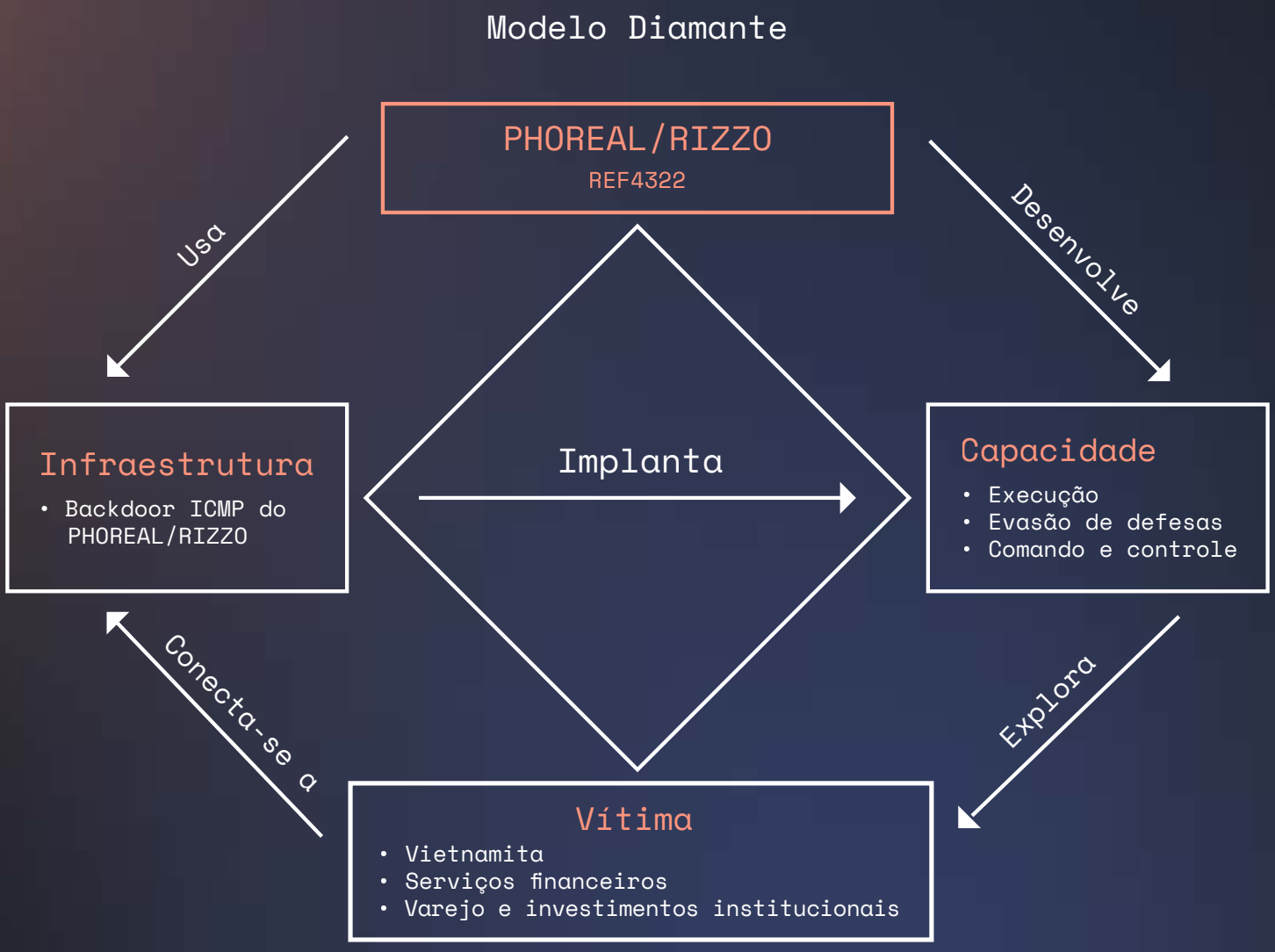


Figura 22: *Modelo Diamante do PHOREAL*

CUBA [REF9019]

Em junho deste ano, a Elastic observou várias tentativas de invasão relacionadas ao CUBA Ramsomware Group, com base no uso comum da infraestrutura compartilhada e da carga útil do ransomware CUBA. Embora vítimas em vários setores tenham sido afetadas, a Elastic não conseguiu identificar um método comum de acesso inicial. Algumas organizações foram comprometidas por meio de vulnerabilidades não corrigidas, outras parecem ter sido comprometidas por malware não relacionado em seus ambientes que não tinha sido remediado com eficácia. As notas da Elastic se sobrepõem ao rótulo de terceiros UNC2596.

Os padrões de atividade associados ao REF9019 envolveram uma variedade de implantes de malware, como COBALTSTRIKE, METASPLOIT, BUGHATCH e SYSTEMBC, além de utilitários de suporte remoto válidos, como o GoToAssist.

Um resumo das técnicas observadas em um ambiente selecionado com uma única vítima:

- Explorar aplicação voltada para o público
- Interpretador de comandos e scripts — PowerShell, shell de comando do Windows
- Tarefa/trabalho agendado — Tarefa agendada
- Execução de início automático de inicialização ou logon — Chaves Run do Registro/ pasta Inicializar
- Criar conta — Conta local
- Despejo de credenciais do sistema operacional — Segredos de LSA
- Dados criptografados para impacto
- Ocultar artefato — Janela oculta
- Mascaramento — Corresponder ao nome legítimo ou local
- Arquivos ou informações ofuscadas
- Carregamento de código reflexivo

O que é a ameaça?

Este grupo de atividade aproveita o ransomware CUBA e diversos recursos de acesso remoto para atingir varejistas e fabricantes norte-americanos e europeus. O grupo de ameaça seguiu um conjunto eficaz, mas repetitivo, de Táticas, Técnicas e Procedimentos (TTP) para acesso inicial, movimento lateral, exfiltração, implantação de ransomware e extorsão.

Qual é o impacto?

O REF9019 tem como alvo varejistas e fabricantes norte-americanos e europeus, envolvendo-se em extorsão após criptografar e roubar arquivos sensíveis.

Qual foi a resposta da Elastic?

A Elastic divulgou publicamente assinaturas do YARA, consultas de caça e proteções de endpoint para detectar essa família de ransomware.

Saiba mais

- CUBA Ransomware Campaign Analysis (Análise da campanha de ransomware CUBA)
- CUBA Ransomware Malware Analysis (Análise de malware do ransomware CUBA)

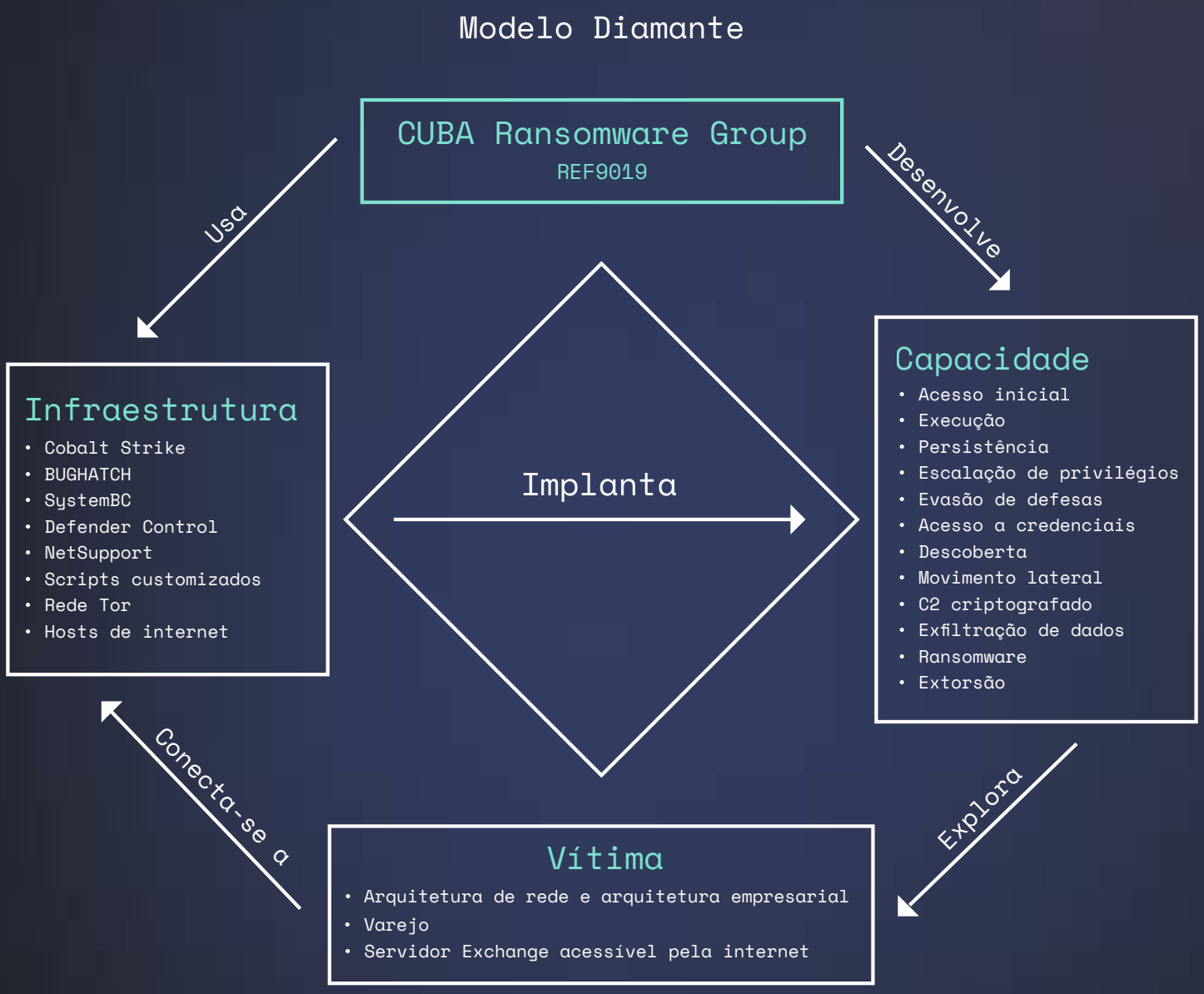


Figura 23: *Modelo Diamante do CUBA*

QBOT [REF3726]

O QBOT (também conhecido como QAKBOT) é atualmente uma das famílias de malware mais prolíficas em uso em todo o mundo e está em desenvolvimento desde aproximadamente 2007. Usado para facilitar crimes relacionados a ransomware, esse malware é notável por seu uso de execução em vários estágios e por empregar uma lista de exceções para evitar a infecção de sistemas nos estados do leste europeu. A Elastic rastreia esse padrão de atividade como REF3726 e observa sobreposições com um número significativo de rótulos de fornecedores como um recurso amplamente disponível para compra.

As encarnações modernas desse malware dependem de recursos nativos, como o proxy de execução regsrv32.exe, para obter acesso inicial. Isso pode ser alcançado por meio de diversos mecanismos de acesso inicial, como exploração de software cliente, iscas de documentos usadas como armas, software legítimo com backdoor e comprometimento da cadeia de suprimentos de software. A Figura 24 descreve um método de execução inicial comum.

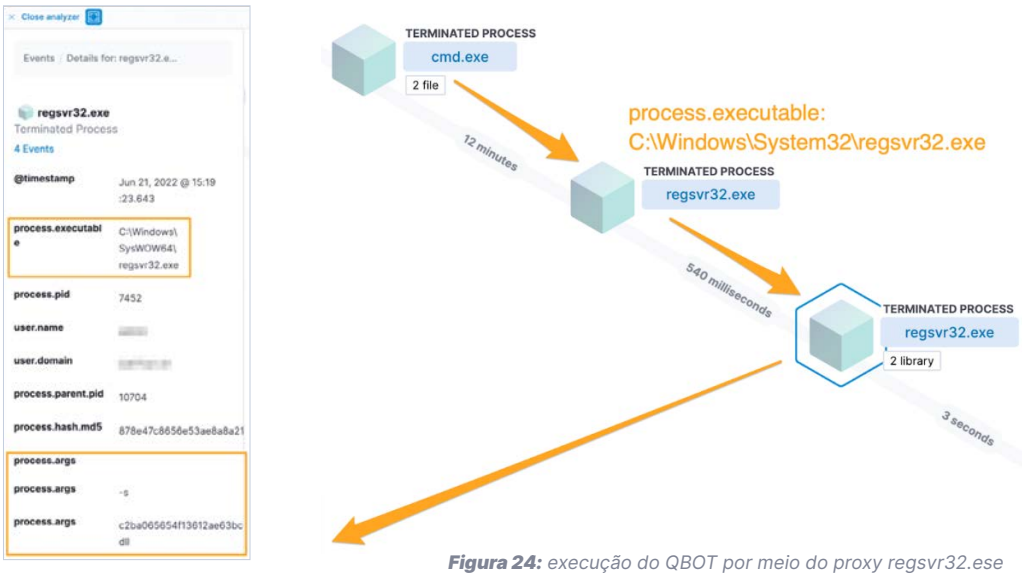


Figura 24: *execução do QBOT por meio do proxy regsvr32.ese*

O que é a ameaça?

O QBOT é um trojan modular prolífico que está ativo desde aproximadamente 2007 como um mecanismo de suporte a ameaças com motivação financeira.

Qual é o impacto?

O REF9019 tem como alvo varejistas e fabricantes norte-americanos e europeus, envolvendo-se em extorsão após criptografar e roubar arquivos sensíveis.

Qual foi a resposta da Elastic?

A Elastic divulgou publicamente proteções de endpoint, lógica pré-criada do mecanismo de detecção, regras do YARA e um extrator de configuração. Além disso, a Elastic usou a pesquisa do QBOT para associar 138 endereços IP controlados ou pertencentes a adversários a 339 arquivos maliciosos.

Saiba mais

- Exploring the QBOT Attack Pattern (Explorando o padrão de ataque do QBOT)
- QBOT Malware Analysis (Análise de malware do QBOT)
- QBOT Configuration Extractor (Extrator de configuração do QBOT)

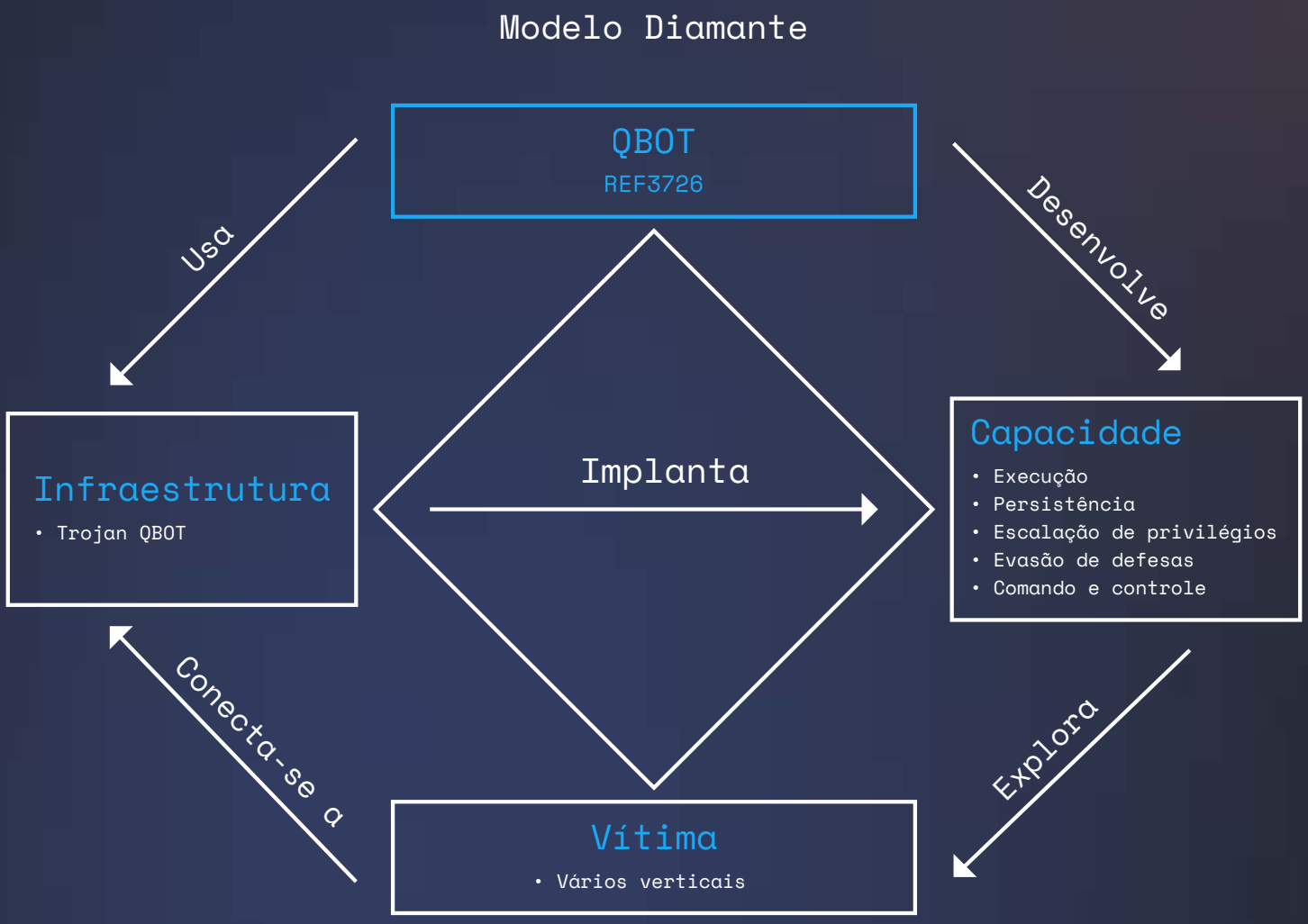


Figura 25: *Modelo Diamante do QBOT*

Previsões e recomendações

Com base em tendências, correlações e pesquisas contínuas sobre a evolução do cenário global de ameaças, a Elastic oferece as previsões e recomendações a seguir. Em vez de uma previsão, os leitores devem observar que as previsões indicam possíveis resultados que são influenciados por muitos fatores para serem antecipados com precisão. Os leitores também devem considerar as recomendações como sugestões e não como garantias contra ameaças cibernéticas.

Previsão 1:

Os adversários continuarão a usar os proxies binários integrados de forma inadequada para escapar da instrumentação de segurança.

Ameaças de todos os tipos continuam a utilizar ferramentas nativas como o Rundll32.exe como um proxy binário para carregar software malicioso, imitando de perto a finalidade pretendida dessas ferramentas. Elas permanecem populares porque funcionam e devem ser eficazes no longo prazo.

Recomendação 1

As empresas devem monitorar de perto o uso do software de proxy binário do sistema e estabelecer o conhecimento de padrões de atividade benignos e maliciosos. Essas ferramentas são onipresentes e desempenham um papel importante durante o acesso inicial. Restringir seu uso tem um efeito imediato na prevenção do comprometimento.

Previsão 2:

As cargas úteis de LNK e ISO substituirão as cargas úteis de documentos e scripts mais convencionais.

Devido às decisões da Microsoft de alterar a segurança do sistema Windows este ano, os tipos de carga útil LNK e ISO tornaram-se necessariamente viáveis para ameaças de todos os tipos. Poucas organizações examinam esses tipos de objeto, resultando em comprometimento mais frequente.

Recomendação 2

Com poucas exceções, as organizações devem tratar os anexos LNK e ISO como arriscados. O uso desses objetos pode ser controlado pela política, e os engenheiros de detecção podem fornecer estratégias para detectar seu uso.

Previsão 3:

As contas de IAM válidas continuarão a ser um alvo para os adversários.

Como porta de entrada para outros objetivos de invasão, o roubo de credenciais é uma etapa essencial para muitos adversários durante os estágios iniciais de um ataque. Durante este ano, a Elastic observou vários grupos de ameaça roubando credenciais válidas para autenticar recursos de nuvem e contornar a necessidade de exploração.

Recomendação 3

É essencial entender os padrões normais de atividade para diferentes tipos de contas, e os indivíduos devem saber identificar quando essas contas estão sendo usadas inadequadamente. A visibilidade dos recursos de nuvem nos níveis de CSP, orquestrador e trabalhador pode ser necessária para identificar padrões maliciosos de atividade que estão afetando aplicações hospedadas na nuvem ou serviços que estão sendo acessados usando contas válidas. O acesso a APIs de metadados ou credenciais usadas em DevOps também deve ser monitorado para acesso a recursos incomuns fora do comportamento normal da conta.

Previsão 4:

As contas de serviço gerenciadas por cada CSP principal (Google, Amazon, Microsoft), que não estiverem configuradas com permissões de privilégio mínimo ou que estiverem configuradas incorretamente serão o alvo dos adversários.

As credenciais da conta de serviço geralmente são um trampolim do acesso inicial ao acesso persistente e podem ser expostas acidentalmente. Commits para repositórios públicos do GitHub foram apenas uma das maneiras pelas quais vimos os agentes de ameaças obterem esses tipos de credenciais, e cada vez mais essa abordagem será viável à medida que as empresas buscarem automatizar mais sua infraestrutura. Além disso, as empresas devem estar cientes de que algumas ameaças desabilitam a auditoria para fugir da detecção.

Recomendação 4

Entenda e implemente o acesso seguro aos recursos da nuvem e prepare-se para a interferência do adversário. Organizações com mais de uma fonte de visibilidade (auditoria de CSP, logs do orquestrador, instrumentação de sensor de endpoint) demonstraram maior capacidade de detectar e mitigar ataques contra plataformas hospedadas na nuvem.

Previsão 5:

As máquinas virtuais Linux usadas para DevOps de backend, mas implantadas em ambientes de nuvem, podem se tornar mais visadas, com ênfase em ameaças à enumeração de contas e acesso a credenciais.

Embora os desenvolvedores continuem a representar uma superfície de ataque frágil para as organizações, as empresas que não entenderem esses riscos ficarão comprometidas. Compreender o escopo do conteúdo implantado em máquinas virtuais, juntamente com o acesso concedido inerentemente por esses sistemas, é fundamental para determinar quanto risco ele representa para a organização.

Recomendação 5

Entenda que os adversários podem alternar fácil e rapidamente de uma chave exposta no GitHub para o acesso ao CSP e, a partir daí, ter a capacidade de criar, modificar ou destruir recursos, incluindo instalação de malware, roubo de dados ou implementação de uma configuração incorreta deliberada.

Previsão 6:

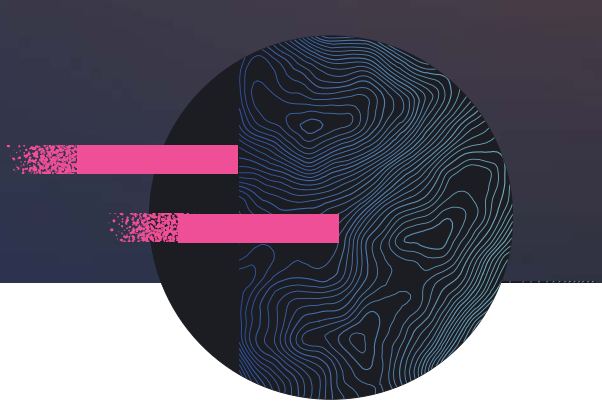
As organizações que investem demais em recursos de detecção que também não oferecem suporte à mitigação terão dificuldades com a resposta de segurança contra todas as categorias de ameaças.

Simplificando, as empresas não podem responder de forma eficaz e rápida às ameaças usando instrumentação somente de detecção. Aqueles incapazes de implantar recursos para mitigar as ameaças de forma centralizada estão em profunda desvantagem contra as ameaças que se movem rapidamente, sejam direcionadas ou não.

Recomendação 6

Avalie sua capacidade de reconstruir sistemas infectados, redefinir credenciais de contas comprometidas, redirecionar uma entrada de DNS, bloquear todo o tráfego de/para um endereço IP, isolar um host e restaurar dados críticos para os negócios de backups. Priorize instrumentação que dê suporte a esses resultados e selecione ferramentas que possibilitem a adoção de estratégias de mitigação automatizadas sempre que possível.

Conclusões



O cenário global de ameaças está em constante evolução, com novas ameaças e recursos preenchendo o nicho daqueles que os precederam. As iscas de phishing agora usam objetos ISO ou LNK em vez de macros maliciosas, refletindo as formas como a tecnologia molda esses recursos. No entanto, os ataques de phishing continuam a ser o método mais comum de acesso inicial. Isso é revelador, pois destaca um tipo de continuidade de risco que as empresas ainda não conseguiram debelar.

Também é informativo, ilustrando que alguns aspectos do cenário de ameaças não são facilmente resolvidos por meio da tecnologia. Em vez disso, o sucesso depende de se ter visibilidade, capacidade e experiência. Em quase todos os casos, descobrimos que esses três fatores cooperaram para alcançar o sucesso ou conspiraram para resultar em fracasso.

Observamos que a visibilidade desempenhou um papel importante para as empresas entenderem sua superfície de ataque. Até recentemente, muitas organizações não consideravam aplicações ou sistemas hospedados na nuvem como parte de sua empresa. Devido talvez à baixa visibilidade padrão oferecida por essas soluções, poucas organizações tinham motivos para contar com eles como parte de sua instrumentação de segurança.

A Elastic usa principalmente a telemetria para melhorar a eficácia dos recursos e fornecer às organizações um contexto de segurança adicional por meio de publicações como esta. Recebemos de braços abertos a oportunidade de trabalhar em parceria com nossos clientes para analisar seus dados, compartilhando anonimamente o que aprendemos com o setor de segurança de forma geral.

Nossa compreensão do cenário global de ameaças está fadada a mudar junto com o próprio cenário. Os investimentos na coleta de dados e em nosso aparato sensorial indicam que a visibilidade é o primeiro passo para a compreensão, e a compreensão nos capacita a agir. Para quem não tem visibilidade, pode não ser prático ou possível realizar uma ação, o que é cada vez mais relevante devido ao ritmo acelerado com que muitos grupos de ameaça evoluíram.

Organizações sem experiência foram aquelas que possivelmente enfrentaram os maiores obstáculos, dependendo de fornecedores e provedores de serviços para configurar, gerenciar e operar sua infraestrutura de segurança. Essa dependência, motivada por várias razões, muitas vezes deixou as entidades visadas em desvantagem, independentemente de a ameaça ser uma vulnerabilidade recém-anunciada, um grupo de ameaça determinado a extorquir ou um efeito colateral de um evento geopolítico.

Este ano, a Elastic saiu de trás da cortina e emergiu como uma empresa de segurança. Tendo um longo histórico de abertura, a comunidade obteve acesso à nossa pesquisa com o Elastic Security Labs e a grande parte de nossa tecnologia de segurança por meio de nosso recurso Protections Artifacts. Esses esforços aparentemente não relacionados eram, na verdade, parte de nossa abordagem para a natureza mutável do cenário de ameaças. É com visibilidade, capacidade e experiência que pretendemos ajudar você a criar ambientes hostis às ameaças. Se podemos encontrá-las uma vez, em um lugar, podemos interferir para lidar com elas em todos os lugares, ao mesmo tempo.

Estaremos aqui quando você precisar. Estaremos aqui quando você quiser se juntar a nós também.

Saiba mais sobre o Elastic Security e proteja-se contra as ameaças abordadas neste relatório (e outras vulnerabilidades) acessando nossa página do Elastic Security Labs. Você também pode nos seguir no Twitter para saber quando publicamos as últimas informações sobre nossas pesquisas de ameaças.

Para encontrar mais pesquisas:

www.elastic.co/pt/security-labs

Siga-nos no Twitter:

@elastic