



RELATÓRIO DO CENÁRIO DE AMEAÇAS DE 2022 DA TENABLE

Um guia de navegação pela superfície de ataque
moderna para profissionais de segurança



Conteúdo

Prefácio	3
Resumo executivo	5
Metodologia	9
Como utilizar este relatório.....	9
Introdução.....	10
<hr/>	
SEÇÃO 1: O cenário de vulnerabilidades	11
Vulnerabilidades relevantes de 2022.....	11
Vulnerabilidades do Exchange favorecidas por uma ampla gama de agentes de ameaças	11
Problemas de divulgação complicam a defesa.....	11
Vulnerabilidades e ataques às cadeias de suprimentos	12
Outras vulnerabilidades de interesse	19
A nuvem.....	21
Problemas de transparência	21
Segurança de dados	21
As configurações incorretas reinam plenas	22
Descobertas de vulnerabilidades na nuvem	22
<hr/>	
SEÇÃO 2: O cenário de ameaças	24
Atividade de estados-nações	24
Vulnerabilidades conhecidas representam uma ameaça à infraestrutura crítica e ao setor privado.....	25
Ransomware: o novo normal	26
Nem todos os ataques de ransomware são levados a público	26
Como se acostumar com o novo normal	26
A ascensão e a queda do Conti	26
A importância de ataques exclusivos de extorsão aumenta.....	27
Novos grupos de ransomware e extorsão	29
O Active Directory permanece um componente crítico para ataques de ransomware bem-sucedidos	30
Violações.....	31
Ataques cibernéticos não especificados são a causa raiz de um quarto das ocorrências de violação.....	33
Por que a saúde é o setor mais afetado?	35
Ataques de criptomoedas resultaram no roubo de US\$ 2,4 bilhões	36
Como entender as tendências em ataques cibernéticos por meio dos dados de violação	37
Conclusão.....	38
Sobre a Tenable	39
<hr/>	
SEÇÃO 3: Um olhar mais atento sobre as principais vulnerabilidades de 2022	40

A grande variedade de ferramentas e sistemas de segurança cibernética isolados que as organizações têm não ajuda a reduzir o risco.

Prefácio

Vamos quebrar o ciclo

No início de 2022, equipes de segurança cibernética do mundo todo ainda estavam se recuperando da vulnerabilidade Log4Shell, que foi divulgada no final de 2021. Agora, ao entrarmos em 2023, a vulnerabilidade que afetou o Apache Log4j (uma biblioteca de logs Java amplamente utilizada) continua sendo uma grande preocupação. De fato, quando analisamos uma amostra representativa de dados de telemetria, descobrimos que, desde 1º de outubro de 2022, a grande maioria das organizações (72%) continua vulnerável ao Log4Shell. Um dado ainda mais preocupante é que 29% dos ativos vulneráveis tiveram o Log4Shell reintroduzido após a correção completa.

Além disso, dificilmente o Log4Shell foi o único risco que as organizações de segurança precisaram gerenciar em 2022. Marcado por choques macroeconômicos incitados pelo aumento da inflação e pela turbulência geopolítica após a Rússia invadir a Ucrânia, o ano trouxe consigo a divulgação de ainda mais vulnerabilidades em bibliotecas e dependências comuns, bem como uma intensificação dos ataques de ransomware.

O mais frustrante de tudo, talvez, é que vimos vulnerabilidades conhecidas, em alguns casos desde 2017, ainda sendo exploradas pelos invasores. Por quê? Porque as organizações não aplicaram patches nelas com eficácia.

Seria fácil acusarmos as organizações de segurança de não terem como prioridade a correção das vulnerabilidades. Seria fácil, e também ingênuo. A realidade é que as equipes de segurança enfrentam vários fatores que fazem da correção de vulnerabilidades um desafio. A lição de hoje é que a grande variedade de ferramentas e sistemas de segurança cibernética isolados que as organizações têm não ajuda a reduzir o risco.

Precisamos todos mudar nossa forma de pensar e, como líderes de segurança, nosso trabalho é gerenciar o risco. Gerenciar a exposição e gerenciar a incerteza. Tudo começa com uma visão holística da sua superfície de ataque, como mostrado neste relatório anual do cenário de ameaças, produzido pela equipe de resposta de segurança (SRT) da Tenable.

No decorrer do seu trabalho diário, a SRT da Tenable inspeciona dados de centenas de fontes para identificar eventos relevantes para os nossos clientes e para o setor de segurança cibernética como um todo. Desse ponto de vista, a equipe pode visualizar os cenários de vulnerabilidades e ameaças de forma holística para ajudar os profissionais



de segurança a identificar as tendências mais importantes. Essa visão contextual é essencial para as organizações que tentam evoluir de uma postura de segurança cibernética reativa para uma postura focada em medidas preventivas e proativas. Nós achamos que a superfície de ataque moderna – com seu mix de infraestruturas locais e baseadas em nuvem, sistemas complexos de gerenciamento de identidade e acesso e uma grande quantidade de aplicações Web e microserviços – demanda uma abordagem mais sofisticada.

O gerenciamento de vulnerabilidades das organizações de segurança cibernética precisa ser realizado de forma integrada. É hora de adotar o gerenciamento de exposição, um conceito relativamente novo projetado para transcender as limitações dos programas de segurança isolados. O desenvolvimento de um programa de gerenciamento de exposição envolve reunir dados de ferramentas associadas ao gerenciamento de vulnerabilidades, segurança de aplicações Web, segurança da nuvem, segurança de identidade, análise das vias de ataque e gerenciamento de superfície de ataque, e analisar tudo isso no contexto do seu próprio mix de usuários, TI, tecnologia operacional (OT) e ativos da internet das coisas (IoT) para que você possa executar um fluxo de trabalho baseado em riscos. O gerenciamento de exposição também oferece aos líderes de segurança cibernética a análise necessária para explicar claramente a eficácia de programas de segurança proativos e preventivos em uma linguagem que o negócio entenda.

O gerenciamento de exposição oferece uma maneira de operacionalizar a redução do risco em uma organização e oferece uma visão de futuro em que não veremos mais vulnerabilidades de cinco anos atrás continuarem sendo exploradas como uma coleção dos "maiores sucessos" na playlist do invasor.

Robert Huber
CSO e Head of Research
da Tenable

Resumo executivo

Logo após o Log4Shell, o ano de 2022 começou com preocupações relacionadas a cadeias de suprimentos e listas de materiais de software (SBOM), pois organizações do mundo todo foram forçadas a reconceitualizar sua resposta a incidentes em antecipação ao próximo grande acontecimento. A equipe de resposta de segurança (SRT) da Tenable monitora continuamente o cenário de ameaças ao longo do ano, nos colocando na linha de frente das vulnerabilidades e ameaças de segurança. Desse ponto de vista, nós compilamos e categorizamos os dados para este relatório anual.

Em um ano marcado por tensão geopolítica, hacktivismo, ransomware e ataques direcionados à infraestrutura crítica, junto a um ambiente macroeconômico turbulento, as organizações tiveram dificuldades de acompanhar as demandas de suas equipes e recursos de segurança cibernética. Mesmo com o mundo enfrentando esses desafios, os acontecimentos que observamos ao longo do ano representaram um ano bastante típico na segurança cibernética. Ataques contra infraestrutura crítica continuaram sendo uma preocupação comum. O ransomware continuou causando estragos, mesmo depois que alguns grupos tiveram suas operações encerradas pelas forças policiais, romperam com o peso de disputas internas pelo poder ou se dividiram em novos grupos. Novas vulnerabilidades surgiram, mas correções confiáveis eram um desafio para os defensores.

O mais alarmante, talvez, seja que, junto com a grande quantidade de novas vulnerabilidades descobertas em 2022, as vulnerabilidades de anos anteriores continuam assombrando as organizações. Na verdade, falhas de 2017 foram tão proeminentes este ano que achamos que elas merecem um lugar na lista das principais vulnerabilidades de 2022.

Nunca é demais destacar: os agentes de ameaças continuam tendo sucesso com vulnerabilidades passíveis de exploração conhecidas e comprovadas que as organizações não conseguiram corrigir como deviam.

A constante evolução do ambiente digital moderno introduz novos desafios para os profissionais de segurança. Programas de segurança bem-sucedidos precisam adotar uma abordagem abrangente e entender onde estão os dados e os sistemas mais sigilosos e quais vulnerabilidades ou configurações incorretas representam o maior risco. Dada a rapidez da transformação digital, é essencial ter uma compreensão completa da sua superfície de ataque externa.

Milhares de novas vulnerabilidades são corrigidas todos os anos, e apenas um pequeno subconjunto será exploradoativamente.

Ao concentrar recursos nas vulnerabilidades que podem ser exploradas e entender como os invasores encadeiam vulnerabilidades e configurações incorretas, as equipes de segurança conseguem projetar estratégias mais completas para reduzir a exposição geral ao risco.

Este relatório inspeciona os principais aspectos do cenário de segurança cibernética de 2022 e como as organizações podem revisar seus programas para focar de forma holística na redução da sua exposição. Nós examinamos:

Vulnerabilidades significativas divulgadas e exploradas ao longo do ano, incluindo como as configurações incorretas comuns da nuvem podem afetar até os gigantes da tecnologia;

As transformações contínuas do ecossistema de ransomware e o surgimento de grupos de ameaças exclusivos de extorsão;

Atuais riscos, vulnerabilidades e ataques na cadeia de suprimentos de software;

Táticas usadas por grupos de ameaças persistentes avançadas para atingir organizações com espionagem cibernética e ataques perturbadores com motivação financeira;

Fatores de violação e desafios da análise de dados de violação, decorrentes de informações limitadas disponíveis e da falta de requisitos de relatórios detalhados;

Os detalhes das principais vulnerabilidades que afetam softwares corporativos.



AS 5 PRINCIPAIS VULNERABILIDADES DE 2022

1

Vulnerabilidades conhecidas (2017-2021)

CVE-20XX-XXXX

2

Log4shell:
Apache Log4j

CVE-2021-44228

3

Follina: Ferramenta de diagnóstico de suporte da Microsoft

CVE-2022-30190

5

ProxyShell:
Microsoft Exchange Server

CVE-2021-34473

4

Atlassian Confluence Server and Data Center

CVE-2022-26134

PRINCIPAIS CONCLUSÕES



Vulnerabilidades conhecidas desempenharam um papel importante nos ataques de 2022

Nos alertas do governo e nas análises do setor ao longo do ano, havia a presença de vulnerabilidades conhecidas em todos os tipos de ataque, incluindo os realizados por agentes patrocinados por estados. Vulnerabilidades de 2017 ainda são exploradas com sucesso em vários tipos de ataque.



Os ataques de ransomware se intensificaram, expondo muitos e muitos dados

2,29 bilhões de registros foram expostos em 2022. Os ataques de ransomware continuaram dominando, representando mais de 35% das violações de dados



Configuração incorretas na nuvem afetam até as organizações mais maduras

A Microsoft e a Amazon sofreram violações de informações confidenciais de clientes graças a configurações incorretas nos seus próprios ambientes de nuvem. Embora esses incidentes não ponham em risco o ambiente dos clientes, eles demonstram a importância de cuidar das configurações. Mais de 3% de todas as violações de dados de 2022 foram causadas por bancos de dados desprotegidos, com o vazamento de mais de 800 milhões de registros.



Vulnerabilidades da cadeia de suprimentos continuam assombrando as organizações

As organizações ainda estão enfrentando as consequências da vulnerabilidade Log4Shell, divulgada no final de 2021, enquanto mais vulnerabilidades em bibliotecas e dependências comuns foram divulgadas. Mais do que nunca, as equipes de TI, segurança e engenharia tiveram que responder de forma intensa a esses ataques, prejudicando muito as operações de segurança em 2022.



Fatores macro incentivam refinamentos no comportamento dos agentes de ameaças

Os ataques de ransomware prevaleceram como a maior preocupação das organizações na avaliação do cenário de ameaças em 2022, mas os grupos envolvidos nesses ataques continuaram refinando suas táticas e ferramentas. As tensões geopolíticas e as atividades dos países também influenciaram as considerações de segurança cibernética das empresas, mas em menor grau.



Metodologia

O Relatório do cenário de ameaças de 2022 foi compilado com base na nossa análise do cenário de ameaças ao longo de 2022. Ao longo do ano, a SRT monitorou comunicados, blogs e relatórios de governos, fornecedores e pesquisadores para entender as tendências que moldam o cenário de vulnerabilidades. Os dados de violação deste relatório foram compilados usando informações publicamente disponíveis de meios de comunicação do mundo todo que relataram violações de dados de novembro de 2021 a outubro de 2022. As pontuações do Common Vulnerability Scoring System (CVSS, Sistema de Pontuação de Vulnerabilidades Comuns) encontradas no relatório são derivadas do National Vulnerability Database (NVD) do National Institute of Standards and Technology (NIST). Nos casos de não haver pontuação do NVD disponível, a pontuação foi baseada em comunicados de fornecedores ou divulgações de vulnerabilidades.

Como utilizar este relatório

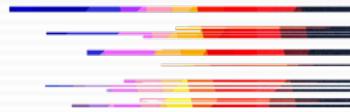
Reduza a exposição da sua organização ao identificar e corrigir as vulnerabilidades e os erros de configuração mencionados neste relatório.

Mantenha os invasores longe aprendendo como agentes de ameaças estão invadindo organizações e as táticas que estão empregando para manter organizações e seus dados confidenciais como reféns.

Proteja os dados examinando algumas das formas mais comuns pelas quais as violações de dados ocorrem e o que sua organização pode fazer para preveni-las.

Priorize as vulnerabilidades mais comumente exploradas e maximize a eficácia da sua estratégia de aplicação de patches e mitigação.

Amplie seus controles de segurança para abordar erros de configuração de nuvem e identidade que os invasores continuam tendo como alvo.



Introdução

Como parte do seu trabalho diário, a SRT da Tenable inspecciona dados de centenas de fontes para identificar eventos relevantes para os nossos clientes e para o setor de segurança cibernética como um todo. Como parte das nossas operações, podemos visualizar os cenários de vulnerabilidades e ameaças de forma holística para identificar as tendências. Nós coletamos e analisamos essas informações todos os anos no nosso Relatório do cenário de ameaças (TLR). As perspectivas e as orientações que apresentamos aqui têm como objetivo ajudar nossos colegas a entender como o cenário de segurança cibernética evoluiu, de modo que todos possamos estar em posição de enfrentar ameaças emergentes e proteger melhor o mundo ao nosso redor.

Na [Seção 1](#), exploramos o cenário de vulnerabilidades e eventos relevantes em 2022, incluindo:

- A presença contínua das vulnerabilidades do Microsoft Exchange Server nos ataques;
- O Log4Shell, vulnerabilidades relevantes e preocupações com a cadeia de suprimentos;
- Problemas de segurança e configurações incorretas na nuvem.

Na [Seção 2](#), exploramos os eventos que moldaram o cenário de ameaças, incluindo:

- Atividade de estados-nações;
- O impacto sustentado do ransomware e a evolução das táticas e do ecossistema;
- Eventos de violação de dados e observações importantes extraídas de uma compilação de dados disponíveis publicamente.

Na [Seção 3](#), apresentamos uma lista de todas as vulnerabilidades discutidas no relatório, incluindo vulnerabilidades relevantes destes fornecedores:





SEÇÃO 1

O cenário de vulnerabilidades

Todos os anos, dezenas de milhares de vulnerabilidades são divulgadas por membros da comunidade de segurança e equipes de pesquisa internas de organizações do mundo todo. Essas vulnerabilidades são catalogadas pelo National Vulnerability Database como CVEs (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns). Em um período de cinco anos, de 2018 a 2022, a quantidade de CVEs relatadas aumentou a uma taxa média anual de crescimento de 26,3%. Houve 25.112 vulnerabilidades relatadas em 2022 até 9 de janeiro de 2023, o que representa um aumento de 14,4% em relação às 21.957 relatadas em 2021 e um aumento de 287% em relação às 6.447 relatadas em 2016.

Vulnerabilidades relevantes de 2022

Não podemos começar uma discussão sobre vulnerabilidades relevantes em 2022 sem mencionar a CVE-2021-44228, conhecida como Log4Shell. Assim que foi divulgada no final de 2021, ficou claro que a falha teria efeitos consideráveis, mas a profundidade total do seu impacto demorou a surgir. Dito isso, decidimos primeiro discutir a exploração antiga e generalizada de várias vulnerabilidades do Microsoft Exchange Server em decorrência da exploração de várias cadeias de ataque ao longo dos anos.

Vulnerabilidades do Exchange favorecidas por uma ampla gama de agentes de ameaças

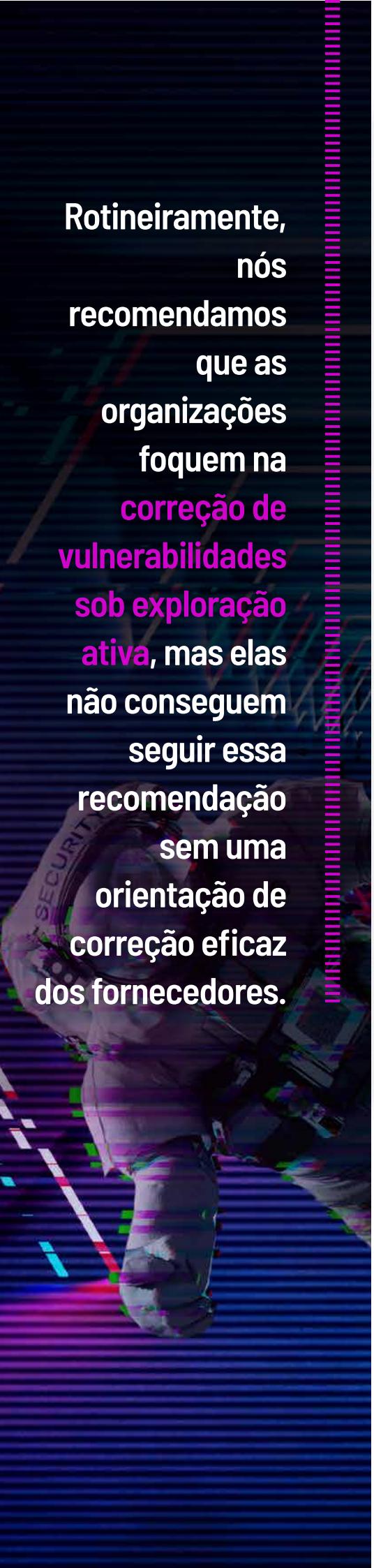
Quando falamos em amplitude de adoção por agentes de ameaças, impacto nas organizações e efeitos sobre os defensores, as vulnerabilidades do Microsoft Exchange Server lideraram o pacote desse ano. Como observado nas nossas 5 principais vulnerabilidades de 2022, a cadeia de vulnerabilidades ProxyShell divulgada por Orange Tsai estava entre as vulnerabilidades de maior impacto do ano. Além disso, os agentes de ameaças também utilizaram o antecessor do ProxyShell, o ProxyLogon – além de várias vulnerabilidades do Microsoft Exchange Server que seguiram ao longo de 2022 – para atingir empresas no mundo todo.

Ataques direcionados a vulnerabilidades do Microsoft Exchange Server foram atribuídos a pelo menos dez variantes ou grupos exclusivos de ransomware e seis operações de ameaças persistentes avançadas (APT). Essas vulnerabilidades, que muitas vezes resultam em escalonamento de privilégios ou execução remota de código (RCE), são particularmente úteis para o acesso inicial às redes pretendidas.

Problemas de divulgação complicam a defesa

Outro tema preocupante no cenário de vulnerabilidades este ano foi uma série de divulgações de vulnerabilidades deficientes de vários fornecedores e projetos importantes. Muitos dos incidentes mais relevantes envolveram a abordagem de vulnerabilidades de dia zero da Microsoft. Em maio, a comunidade de pesquisa descobriu e confirmou uma exploração disponível publicamente para uma [falha de execução remota de código na ferramenta de diagnóstico de suporte do Microsoft Windows](#). Inicialmente denominada Follina devido à falta de atribuição de uma CVE, e posteriormente designada como CVE-2022-30190, a Microsoft levou mais de duas semanas para lançar um patch. Aumentando a preocupação, houve [relatos](#) de que a Microsoft dispensou a divulgação inicial da falha já em abril.

Mais para a frente, a GTSC Cybersecurity Technology Company Limited publicou informações sobre dois ataques de dia zero no [Microsoft Exchange Server \(CVE-2022-41040 e CVE-2022-41082\)](#) que haviam sido explorados no mundo real. Essas falhas foram apelidadas de "ProxyNotShell" pela comunidade. Desta vez, a Microsoft levou quase seis semanas para lançar patches; a empresa publicou várias iterações



**Rotineiramente,
nós
recomendamos
que as
organizações
foquem na
correção de
vulnerabilidades
sob exploração
ativa, mas elas
não conseguem
seguir essa
recomendação
sem uma
orientação de
correção eficaz
dos fornecedores.**

de orientação de mitigação entretempo. Essa demora para confirmar e aplicar patches às vulnerabilidades, além de orientações insuficientes, deixam a defesa ainda mais difícil do que já é. Rotineiramente, nós recomendamos que as organizações foquem na correção de vulnerabilidades sob exploração ativa, mas elas não conseguem seguir essa recomendação sem uma orientação de correção eficaz dos fornecedores.

Do outro lado da moeda, alguns fornecedores criaram problemas com seu próprio comportamento proativo. Em outubro, a [Fortinet](#) e a [OpenSSL](#) causaram confusão ao fazer um prenúncio de vulnerabilidades. Nos dois casos, a falta de informações precisas disponíveis ao público gerou uma especulação desenfreada e consumiu recursos, pois a expectativa era que as equipes de segurança respondessem e produzissem resultados em um vácuo de informações. Quando as vulnerabilidades podem ser o elo crítico em cadeias de ataque devastadoras e a falta de comunicação cria um obstáculo intransponível para as equipes de segurança e engenharia, os fornecedores devem fazer o seu melhor para fornecer informações rápidas, mas que sejam práticas e precisas.

Vulnerabilidades e ataques às cadeias de suprimentos

A [vulnerabilidade Log4Shell](#), divulgada no final de 2021, deu início a um segundo ano de preocupações com as cadeias de suprimentos. Na Retrospectiva do cenário de ameaças de 2021, destacamos bibliotecas e repositórios comprometidos, e essa tendência continuou até 2022. Bibliotecas Python Packaging Index, Node Package Manager (NPM), pacotes [Javascript](#) e [plug-ins do WordPress](#) foram todos comprometidos por vários motivos: [roubo de senhas](#) ou [tokens de login](#), [instalação de backdoors](#) e [extração de dados confidenciais](#).

Embora 2021 certamente tenha tido vulnerabilidades significativas e ataques contra cadeias de suprimentos, tanto de software quanto físicas, 2022 foi mais caracterizado pelas vulnerabilidades do que pelos ataques. Parecia que, a cada poucos meses, o setor se preparava para "o próximo Log4Shell". Raramente as falhas assim apontadas correspondem à gravidade do Log4Shell, mas os efeitos que tiveram nos defensores e nas equipes de DevOps foram quase igualmente disruptivos. Mesmo com vulnerabilidades menos graves, as organizações precisaram ativar manuais de resposta a incidentes para lidar com as demandas de informação de clientes e parceiros.

Desde o incidente direcionado às organizações por meio da plataforma SolarWinds Orion em 2020, parece que o setor de segurança cibernética passa de um divisor de águas para outro, e as equipes de segurança ficam presas na confusão. Esse problema era aparente nas vulnerabilidades da OpenSSL (CVE-2022-3786 e CVE-2022-3602) abordadas no início de novembro.

O prenúncio da falha como uma vulnerabilidade crítica em um bloco estrutural fundamental de vários produtos e serviços, comprehensivelmente, desencadeou respostas de alta intensidade nas equipes de segurança. No entanto, a falta de informações práticas durante a semana de intervenção e a verdade sobre a severidade mais baixa não diminuíram a pressão para as equipes buscarem incansavelmente respostas e resultados. Esse não foi o único, mas foi o exemplo mais preocupante de vulnerabilidades que existem em uma escala móvel de severidade e comoção. Vulnerabilidades da biblioteca Apache Commons Text (CVE-2022-42889, "Text4Shell") e da [Spring Framework \(CVE-2022-22965, "Spring4Shell"\)](#) ocupam posições nessa escala.

Dada a verdadeira severidade e o [impacto de longo prazo do Log4Shell](#) e dos incidentes que envolveram a SolarWinds e a Kaseya, juntamente com a incerteza inerente da divulgação das vulnerabilidades, essas vulnerabilidades da cadeia de suprimentos continuarão a causar interrupções importantes, mesmo que nunca sejam exploradas. Até que o setor desenvolva táticas melhores para se comunicar e operar com a incerteza, recursos preciosos serão gastos no combate às vulnerabilidades erradas.

Não desperdice seu tempo com vulnerabilidades de dia zero, corrija suas vulnerabilidades conhecidas

Para 2022, nosso monitoramento de vulnerabilidades de dia zero inclui falhas que foram exploradas no mundo real e falhas que foram divulgadas publicamente antes da disponibilização de patches ou que não têm patches.

Embora as vulnerabilidades de dia zero atraiam muita atenção, essas ameaças raramente são exploradas em massa e acabam sendo usadas em ataques direcionados limitados. Em muitos casos, essas falhas recebem patches rapidamente e fazem a transição para o bucket de vulnerabilidades que chamamos de vulnerabilidades conhecidas. Ao longo de 2022, como parte da nossa análise de orientações de fornecedores, divulgações e artigos de notícias disponíveis publicamente, identificamos 101 vulnerabilidades de dia zero. Em contraste, identificamos 105 vulnerabilidades de dia zero em 2021.

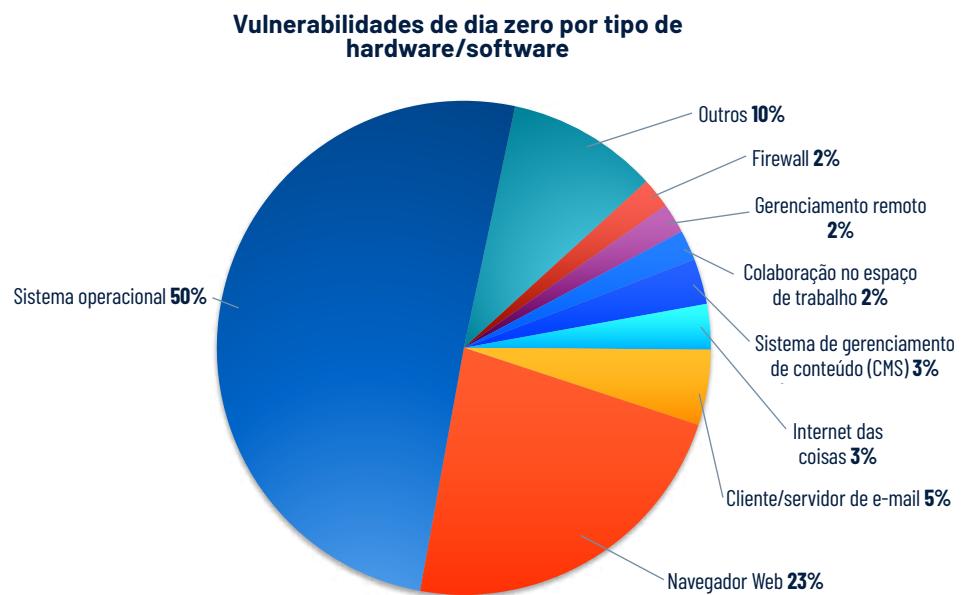
Com que velocidade as vulnerabilidades de dia zero se tornaram vulnerabilidades conhecidas

À medida que avaliamos o risco que as vulnerabilidade de dia zero representam, é importante entender e considerar quanto tempo elas permanecem desconhecidas do público – e é aí está o perigo. Uma vez que uma vulnerabilidade de dia zero é reconhecida pelo fornecedor e um patch é emitido, ela muda imediatamente para a categoria de vulnerabilidades conhecidas, e as equipes de segurança podem encontrar e corrigi-la. Ao avaliar o risco que uma vulnerabilidade de dia zero representa para sua organização, também é importante considerar se é, por exemplo, um sistema operacional fundamental para todos os seus usuários ou se é uma falha que ocorre em um software específico usado por apenas um pequena porcentagem de seus usuários. É importante ter em mente essa distinção ao examinarmos as cinco primeiras vulnerabilidades de dia zero de 2022 a serem exploradas no mundo real (consulte a tabela abaixo). Aqui, descobrimos que quatro delas foram divulgadas ao público no mesmo dia em que o fornecedor lançou os patches. Embora tenham sido usadas em ataques limitados e direcionados como dia zero, elas rapidamente se tornaram vulnerabilidades conhecidas com orientação prática de seus respectivos fornecedores. Como vemos frequentemente, novas ameaças podem causar distrações para as equipes de segurança, mesmo que o software em questão não represente realmente um grande risco para a organização devido ao seu uso limitado. É de extrema importância permanecer atento e corrigir ou mitigar as vulnerabilidades conhecidas e exploradas que representam o maior risco para sua organização, em vez de focar na janela restrita de um possível dia zero antes que um patch seja emitido.

CVE	Produto	Divulgação ao público	Patch lançado
CVE-2022-21882	Microsoft Windows	11/01/2022	11/01/2022
CVE-2021-35247	SolarWinds Serv-U	18/01/2022	18/01/2022
CVE-2022-22587	Apple iOS/iPadOS/macOS	26/01/2022	26/01/2022
CVE-2022-24682	Zimbra Collaboration	16/12/2021	05/02/2022
CVE-2022-22620	Apple iOS/iPadOS/macOS	10/02/2022	10/02/2022

Uma vulnerabilidade de dia zero é uma falha em um software ou hardware que é desconhecida para o fornecedor antes de sua divulgação pública, ou que foi divulgada publicamente antes que uma correção estivesse disponível. Assim que uma vulnerabilidade de dia zero é divulgada e um patch é disponibilizado, ela entra para a lista de vulnerabilidades conhecidas.



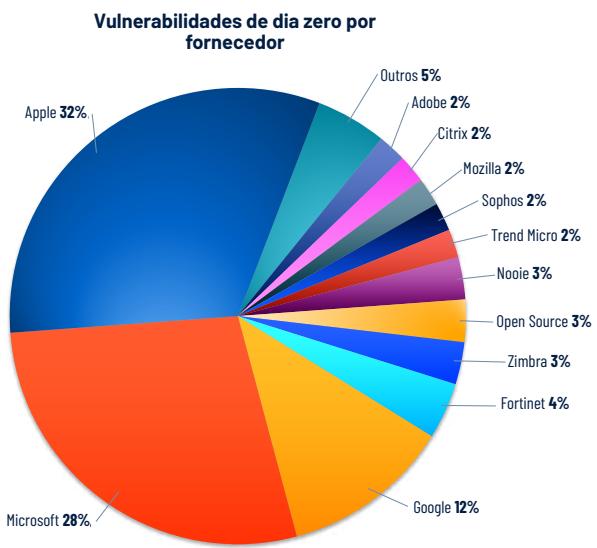


Em 2022, observamos mudanças gritantes nas tendências de vulnerabilidades de dia zero. Ao contrário dos dois anos anteriores, em que as vulnerabilidades de navegador estavam à frente, este ano as vulnerabilidades de sistema operacional subiram para o topo das paradas, representando mais da metade de todas as vulnerabilidades de dia zero.

Principais vulnerabilidades por tipo de software/hardware

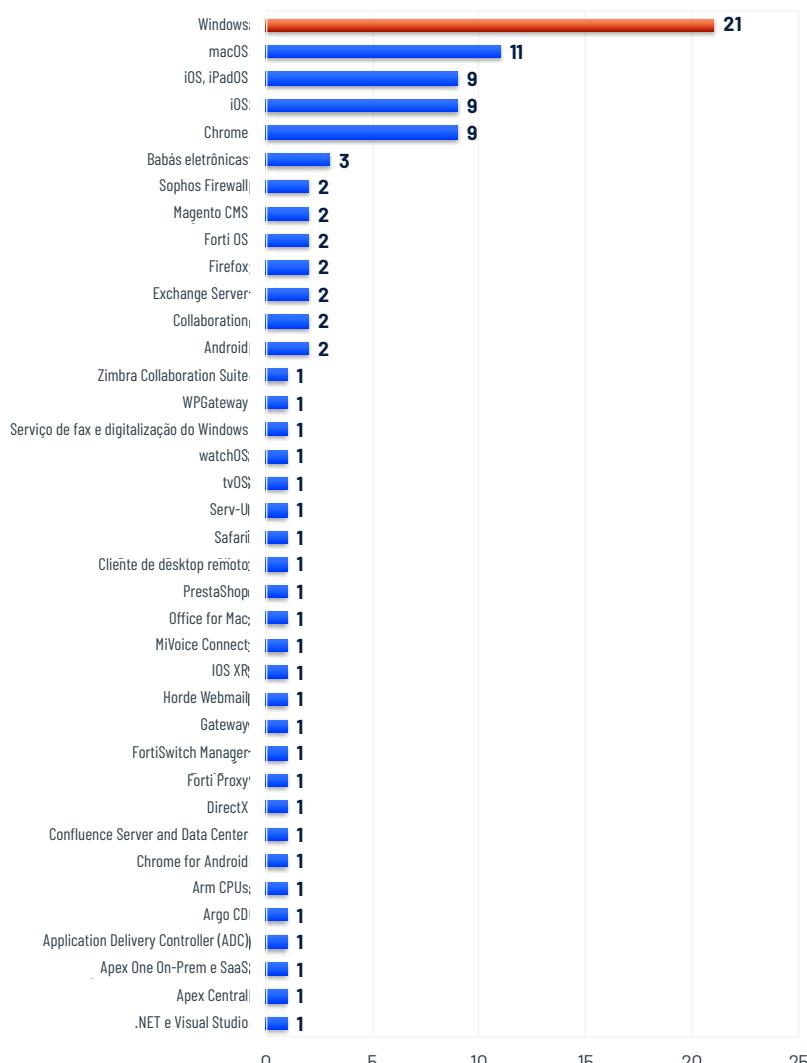
2020	2021	2022
35,7%	30,5%	50,5%
Vulnerabilidades de navegador	Vulnerabilidades de navegador	Vulnerabilidades de sistema operacional

A categoria de vulnerabilidades de sistema operacional inclui vulnerabilidades nativas em sistemas operacionais, além de ferramentas e serviços originários do sistema operacional em si. Essa categoria inclui falhas como as encontradas no Windows Print Spooler e no Windows COM+ Event System Service, entre outras.



Como nos anos anteriores, plataformas com maior base de usuários tiveram a maior quantidade de vulnerabilidades em 2022. Entre todas as vulnerabilidades de dia zero, as presentes nos produtos da Apple representaram 31,7%, seguidas pelas da Microsoft, com 27,7%. Os produtos da Apple e da Microsoft representaram um total combinado de 59,4% de todas as vulnerabilidades de dia zero divulgadas em 2022.

Vulnerabilidades de dia zero por produto



As vulnerabilidades do Microsoft Windows representaram 21% de todas as vulnerabilidades de dia zero divulgadas, seguidas por um trio de produtos da Apple: macOS (11%), iOS (9%) e iPadOS (9%). Em 2022, as vulnerabilidades do Google Chrome representaram apenas 9% de todas as vulnerabilidades de dia zero divulgadas.

Declínio nas vulnerabilidades de navegador

2021	2022
32	23
-	-28,1%

Em 2021, foram divulgadas 32 vulnerabilidades de dia zero em navegadores, e o navegador Google Chrome foi responsável por 17 delas. Em 2022, as vulnerabilidades de dia zero em navegadores diminuíram quase 30% (28,1%), totalizando 23, sendo que nove delas estavam associadas ao Google Chrome. Não está claro por que houve esse declínio acentuado nas vulnerabilidades de dia zero em navegadores, mas uma teoria é que os sandboxes baseados em navegadores dificultaram a exploração pelos invasores. Outra possibilidade é que os agentes de ameaças estejam desistindo das vulnerabilidades de dia zero e focando seus esforços em vulnerabilidades conhecidas que permanecem sem patches.

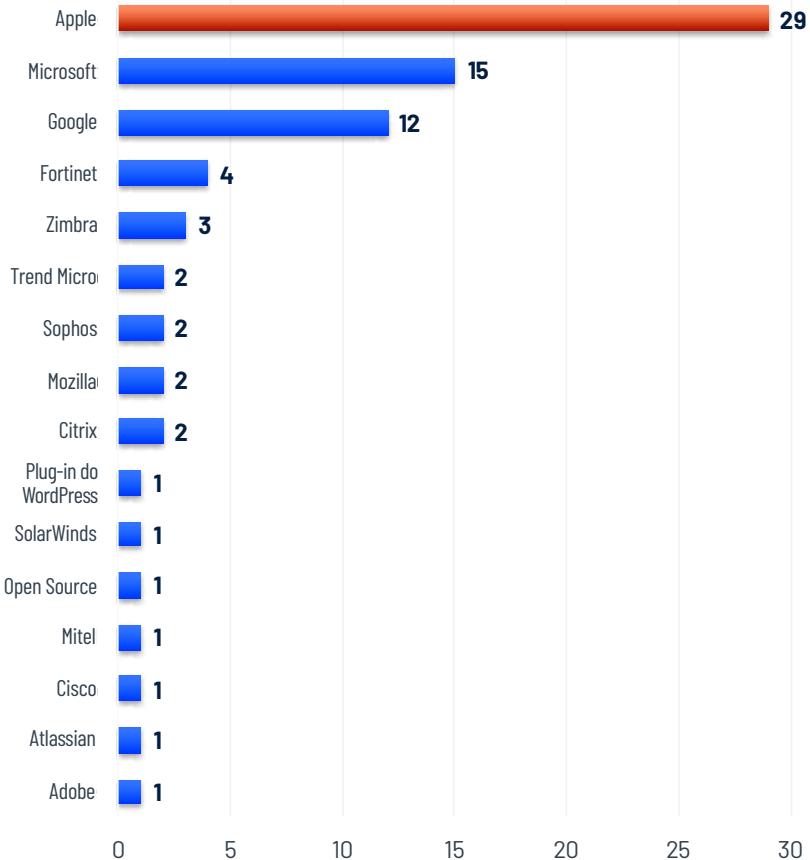
Vulnerabilidades de dia zero por status de exploração



A grande maioria (77,2%) das vulnerabilidades de dia zero divulgadas em 2022 foram exploradas no mundo real. Ainda assim, houve uma queda de 5,8% em relação a 2021, quando 83% das vulnerabilidades de dia zero divulgadas foram exploradas no mundo real.

Entre as 78 vulnerabilidades de dia zero exploradas no mundo real este ano, a maior parte está em produtos Apple, Microsoft e Google. A Apple foi responsável por 37,2% das vulnerabilidades de dia zero exploradas no mundo real em vários produtos, incluindo iOS, iPadOS e macOS, seguida pela Microsoft com 19,2%. O Google foi responsável por 15,4%, incluindo Chrome e Android.

Vulnerabilidades de dia exploradas no mundo real



Sete fornecedores tiveram apenas uma única vulnerabilidade de dia zero que afetasse seus produtos. Entre estes quatro fornecedores – Citrix, Mozilla, Sophos e Trend Micro – cada um foi responsável por duas vulnerabilidades de dia zero exploradas no mundo real, enquanto a Zimbra foi responsável por três. No caso da Fortinet, duas vulnerabilidades de dia zero afetaram o FortiOS e um CVE afetou o FortiProxy e o FortiSwitchManager.





As vulnerabilidades de dia zero significam problemas para as organizações?

Determinar o possível impacto de vulnerabilidades de dia zero em sua organização pode ser desafiador. Vamos analisar em mais detalhes para compreender melhor o que significa um dia zero para uma empresa.

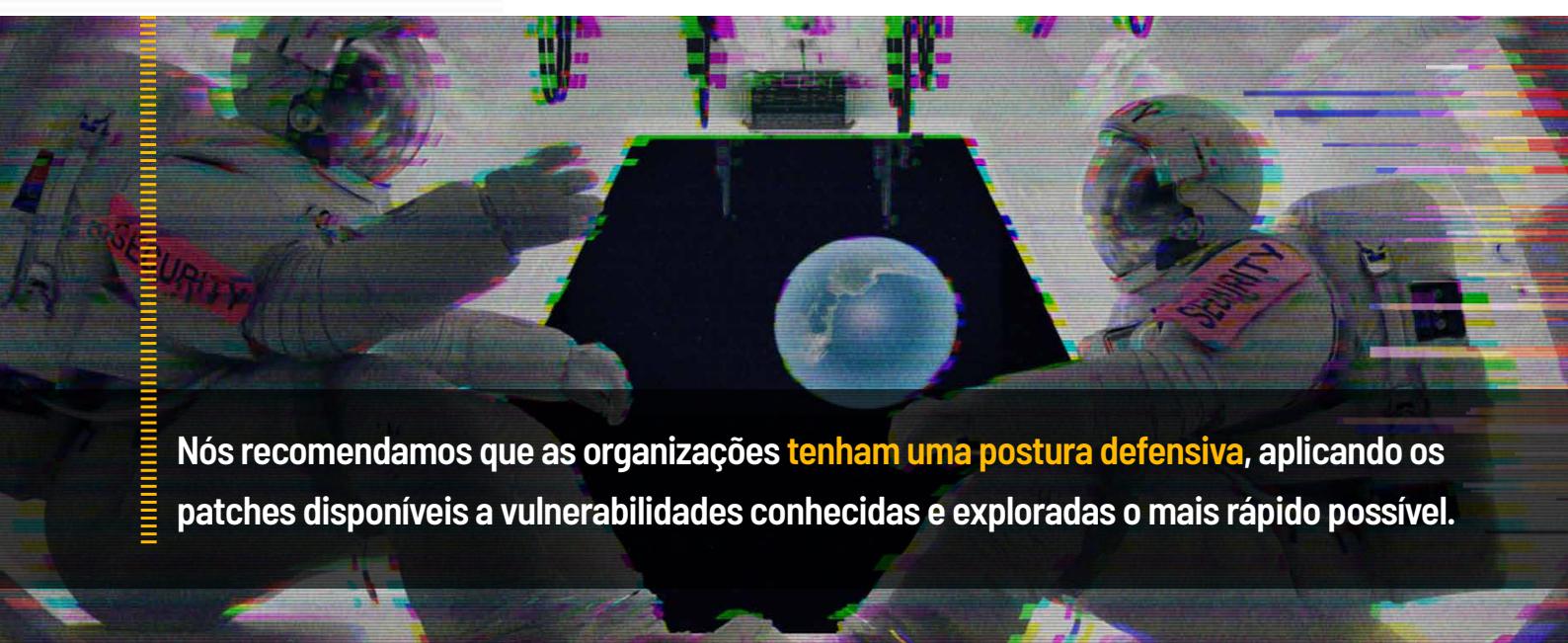
Em primeiro lugar, é relativamente raro que um dia zero seja explorado em massa antes da divulgação. Em geral, esse tipo de falha é explorado em ataques limitados e direcionados. Em outros casos, dias zero são divulgados de forma responsável por pesquisadores de segurança cibernética aos fornecedores, que lançam patches o mais rápido possível.

A Apple é um caso em questão. Apesar de ser responsável por mais de um terço das vulnerabilidades de dia zero exploradas no mundo real, os produtos da Apple, até onde sabemos, não tiveram exploração generalizada de nenhuma vulnerabilidade de dia zero em 2022.

Em contrapartida, a CVE-2022-26134, uma vulnerabilidade de dia zero no Atlassian Confluence Server and Data Center, tornou-se uma das cinco principais vulnerabilidades de 2022, pois observamos um aumento significativo na exploração após sua divulgação no início de junho de 2022. Essa vulnerabilidade, que foi originalmente explorada no mundo real como dia zero, foi inicialmente divulgada quando a Atlassian lançou o patch para lidar com o problema. Nos dias seguintes à divulgação, a exploração aumentou assim que a falha tornou-se uma vulnerabilidade conhecida, tornando-se uma ameaça significativa às organizações que usavam versões afetadas do Confluence Server and Data Center.

Também é importante reconhecer que vulnerabilidades de dia zero são muito usadas por invasores para aproveitar diretamente falhas conhecidas que são exploradas de forma rotineira por agentes de ameaça de todos os tipos, incluindo afiliados de ransomware e grupos de APT. ProxyLogon (CVE-2021-26855) uma vulnerabilidade de dia zero no Microsoft Exchange Server foi divulgada e teve uma correção disponibilizada em 2 de março de 2021 e é um ótimo exemplo de uma falha que começou como dia zero e continuou a ser explorada mais de um ano depois por grupos de ransomware, seus afiliados e agentes de ameaça patrocinados por nações.

Em resumo: as vulnerabilidades aumentam o risco, não importando se começaram como dia zero ou não. Nós recomendamos que as empresas operem com uma postura defensiva ao aplicar patches disponíveis a vulnerabilidades conhecidas e exploradas o mais rápido possível.



Nós recomendamos que as organizações **tenham uma postura defensiva**, aplicando os patches disponíveis a vulnerabilidades conhecidas e exploradas o mais rápido possível.

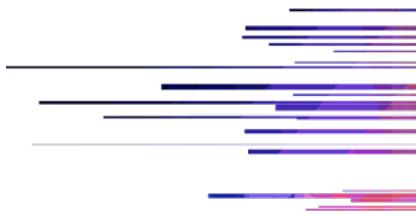
Outras vulnerabilidades de interesse

Embora muitas vulnerabilidades nomeadas estivessem na nossa mente ao longo de 2022 (as várias "Shells" e "Proxys"), como de costume, as vulnerabilidades não nomeadas também eram uma preocupação. Além das vulnerabilidades sem marca do Microsoft Exchange Server discutidas acima, havia falhas sem nome em vários outros produtos amplamente usados em ataques.

CVE	Produto afetado	Descrição	CVSSv3
CVE-2022-35405	Zoho ManageEngine Password Manager Pro	RCE não autenticado	9,8
CVE-2022-26134	Atlassian Confluence Server and Data Center	Injeção de Object-Graph Navigation Language (OGNL)	9,8
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager	Injeção de template do lado do servidor	9,8
CVE-2022-1388	F5 BIG-IP	Desvio de autenticação	9,8
CVE-2022-40684	Fortinet FortiOS e FortiProxy	Desvio de autenticação	9,6
CVE-2022-24682	Zimbra Collaboration Suite	Script entre sites	6,1
CVE-2022-27924	Zimbra Collaboration Suite	Injeção de comando	7,5
CVE-2022-27925	Zimbra Collaboration Suite	Upload arbitrário de arquivos	7,2
CVE-2022-37042	Zimbra Collaboration Suite	Desvio de autenticação	9,8

Vulnerabilidades mais antigas também se destacaram entre as exploradas em ataques. Falhas no Fortinet FortiOS e no Zoho ManageEngine foram detectadas encadeadas em ataques com o Log4Shell e várias vulnerabilidades do Microsoft Exchange Server. Os invasores continuam mirando nessas vulnerabilidades conhecidas porque elas permanecem eficazes ao serem associadas a novas vulnerabilidades e vulnerabilidades de dia zero com o passar do tempo. Nós destacamos muitas dessas falhas há anos, e todas elas estão listadas no catálogo de vulnerabilidades exploradas conhecidas, Known Exploited Vulnerabilities (KEV), da Cybersecurity and Infrastructure Security Agency (CISA).

CVE	Produto afetado	Descrição	CVSSv3
CVE-2017-11882	Microsoft Office Equation Editor	Corrupção de memória	7,8
CVE-2018-0798	Microsoft Office Equation Editor	Corrupção de memória	8,8
CVE-2018-0802	Microsoft Office Equation Editor	Corrupção de memória	7,8
CVE-2018-13379	Fortinet FortiOS	Travessia de caminho	9,8
CVE-2020-14882	Oracle WebLogic	RCE não autenticado	9,8
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus	Desvio de autenticação para RCE	9,8
CVE-2021-40444	Microsoft MSHTML (Trident)	RCE não autenticado	7,8
CVE-2021-44077	Zoho ManageEngine ServiceDesk Plus	RCE não autenticado	9,8



A nuvem

De acordo com uma pesquisa conduzida pela [O'Reilly](#), 90% dos entrevistados usam tecnologia em nuvem. Conforme a adoção da nuvem pública continua a acelerar, as empresas precisam se adaptar às novas complexidades ao entender os riscos que correm no mundo da segurança da nuvem. Adotar uma postura "cloud-first" traz novas formas de risco, pois o fortalecimento da segurança e patches silenciosos costumam ser feitos pelos provedores de serviços de nuvem (CSPs) sem nenhum aviso. Embora haja um forte apelo para que provedores, como a Amazon Web Services (AWS), o Google Cloud Platform (GCP) ou o Microsoft Azure, gerenciem os aspectos de segurança, os riscos impostos aos clientes corporativos desses serviços costumam ser mal compreendidos por profissionais de segurança e do negócio. Quando as organizações migram para esses serviços de nuvem gerenciados, elas perdem a visibilidade da sua superfície de ataque, não podem confiar nos seus controles de segurança normais e precisam confiar no que é fornecido pelos CSPs.

Apesar das preocupações com a segurança, os condutores do negócio, como a necessidade de crescimento e escalabilidade mais rápidos, continuarão a impulsionar a adoção de serviços de nuvem pública em organizações de todos os portes. Conforme as organizações mudam o foco para serviços em nuvem, é preciso tomar cuidado para que a segurança fique em primeiro lugar – uma abordagem inteligente de nuvem. Destacamos abaixo quatro áreas importantes de preocupação quando falamos em segurança da nuvem.

Problemas de transparência

Um dos maiores desafios que as organizações enfrentam com a nuvem é que as vulnerabilidades que afetam os CSPs não são relatadas em um comunicado de segurança ou não recebem um identificador CVE; elas costumam ser abordadas pelo CSP sem aviso algum para o usuário final. Essa falta de transparência faz com que a avaliação de riscos seja um desafio. Sem notas de versão, comunicados de segurança ou qualquer identificador para rastreamento, as equipes de InfoSec enfrentam grandes desafios para avaliar a postura de segurança de um provedor de nuvem. Para aumentar a dificuldade, muitos provedores não mencionam quando os processos de resposta a incidentes são iniciados ou se há evidências de exploração de uma vulnerabilidade relatada. Os vários pontos cegos que essas práticas criam para as organizações são uma preocupação crescente. Embora haja muito debate sobre como rastrear essas vulnerabilidades, hoje não existe nenhuma solução.

Segurança de dados

Embora cada CSP ofereça suas próprias [práticas recomendadas](#) com dicas de controles de acesso apropriados, continuamos observando violações de dados causadas por recursos de nuvem desprotegidos ou protegidos de forma inadequada. Este ano, a [Microsoft divulgou](#) que um endpoint do Azure estava desprotegido e com configurações incorretas, o que possivelmente permitia o acesso a dados de transações comerciais da Microsoft e de possíveis clientes. O problema foi relatado à Microsoft pelo [SOCRadar](#) e destaca que até os CSPs estão sujeitos a erros de configuração incorreta.

Provedores de serviços em nuvem (CSP) são empresas que fornecem a infraestrutura e os componentes usados para computação em nuvem, incluindo recursos de nuvem privada e pública. As nuvens privadas são ambientes exclusivos a uma única entidade e podem ser isoladas facilmente para grupos e usuários, conforme a necessidade. As nuvens públicas são desenvolvidas para alocar recursos a vários locatários e clientes, geralmente gerenciados por provedores terceirizados, como Amazon Web Services (AWS), Google Cloud Platform (GCP) e Microsoft Azure.



Em outro exemplo, a Amazon enfrentou um incidente de segurança de dados quando um pesquisador encontrou um **banco de dados Elasticsearch desprotegido** contendo dados de visualização de usuários da Amazon Prime. Com mais de 215 milhões de entradas no banco de dados, até o vazamento de dados pseudonimizados é preocupante para qualquer usuário final do serviço.

Os exemplos acima ilustram como até grandes CSPs pertencentes a gigantes da tecnologia não estão imunes a erros simples de configuração. Na nossa própria análise de violações de dados relatadas publicamente, descobrimos que mais de 3% das violações de dados divulgadas em 2022 resultaram de um banco de dados desprotegido. Coletivamente, essas violações de dados expuseram mais de 800 milhões de registros em vários setores.

As configurações incorretas reinam plenas

Além de bancos de dados abertos e desprotegidos, uma variedade de erros de configuração da nuvem pode abrir portas para riscos às organizações. O Kubernetes, uma das plataformas de gerenciamento de contêineres de fato, é uma área específica de preocupação. Um estudo da **Cloud Native Computing Foundation** conduzido em 2021 descobriu que 96% dos entrevistados usavam Kubernetes e quase 70% usavam Kubernetes na produção. Em um estudo recente conduzido por pesquisadores da **Shadowserver Foundation**, 84% das instâncias identificáveis da API do Kubernetes foram expostas à Internet. Como o relatório indica, isso não sugere que cada uma delas seja vulnerável, mas é improvável que existam motivos válidos para expor essas APIs. Em 2021, pesquisadores da **Trend Micro detalharam** como um grupo mal-intencionado, conhecido como TeamTNT, comprometeu milhares de clusters Kubernetes para instalar aplicações de criptomineração abusando da API Kublet, que havia sido deixada exposta em cada um dos clusters pretendidos.

Como o Kubernetes é um alvo muito atrativo para os agentes de ameaças, a CISA e a National Security Agency (NSA) dos EUA continuam fornecendo atualizações do seu **relatório técnico conjunto** sobre o fortalecimento do Kubernetes para incentivar práticas seguras e recomendadas em implementações do Kubernetes.

Descobertas de vulnerabilidades na nuvem

Ao longo do ano, várias descobertas foram feitas e relatadas aos CSPs por uma variedade de empresas e pesquisadores independentes. Conforme observado acima, em muitos casos, as únicas informações de descobertas de vulnerabilidades na nuvem vieram de artigos divulgados por pesquisadores de segurança, e não dos próprios CSPs. Com dezenas de serviços de CSPs em uso por empresas do mundo todo, os pesquisadores estão na camada mais superficial desses alvos descomunais.

Jimi Sebree, pesquisador da Tenable, fez várias descobertas ao trabalhar com o Microsoft Azure. Confira a tabela a seguir:

Produto	CVE	Tipo de vulnerabilidade	Pontuação do CVSSv3
Microsoft Azure Synapse Analytics	N/A	Escalonamento de privilégios	N/A - Severidade crítica
Microsoft Azure Synapse Analytics	N/A	Envenenamento de arquivos de hosts	N/A - Severidade baixa
Microsoft Azure Site Recovery	CVE-2022-33675	Escalonamento de privilégios	7,8
Microsoft Azure Arc	N/A	Divulgação de informações	6,5

Com a falta de transparência sobre as vulnerabilidades da nuvem, é improvável que os usuários desses serviços realmente entendam o risco imposto aos seus recursos de nuvem. Embora algumas vulnerabilidades recebam CVEs ou comunicados de segurança, outras podem ser corrigidas silenciosamente por um CSP. Esses fatores fazem com que a avaliação da postura de segurança de um provedor em relação ao outro seja uma tarefa assustadora para os profissionais de segurança. Com a contínua adoção da nuvem pública, as organizações precisam se planejar com antecedência para ter a certeza de avaliar suas próprias práticas e as dos CSPs de modo a manter o foco em implementações de nuvem seguras. É razoável presumir que os serviços em nuvem e seus equivalentes locais teriam uma ocorrência semelhante de vulnerabilidades, mas a falta de transparência deixa os usuários de nuvem no escuro no que se refere à sua exposição ao risco.



SEÇÃO 2

O cenário de ameaças

A análise do cenário de vulnerabilidades isolado é apenas parte da história. Também precisamos entender o cenário de ameaças: como os invasores usam essas vulnerabilidades, juntamente com outras ferramentas e táticas, para atingir empresas, governos e organizações sem fins lucrativos. Vamos explorar os principais recursos do cenário de ameaças de 2022 e como os defensores devem enfrentar os desafios mais recentes.

Atividade de estados-nações

Os ataques cibernéticos conduzidos por estados-nações — ou a pedido de estados-nações — são uma preocupação constante no cenário de ameaças. Isso foi válido particularmente em 2022, quando tensões geopolíticas, eleições e acontecimentos em todo o mundo influenciaram as considerações de segurança cibernética corporativa.

No início de 2022, vários órgãos governamentais dos EUA, incluindo CISA, Federal Bureau of Investigation (FBI) e NSA, [emitiram um comunicado conjunto de segurança cibernética \(AA22-011A\)](#) com uma lista de táticas, técnicas e procedimentos (TTPs) usados como parte das operações de segurança cibernética conduzidas por agentes de ameaças patrocinados pelo estado russo. O comunicado incluía uma lista de vulnerabilidades conhecidas usadas por grupos de APT patrocinados pelo estado russo. Em fevereiro de 2022, outro comunicado dos mesmos órgãos americanos confirmou que os criminosos cibernéticos patrocinados pelo estado russo têm como alvo constante os prestadores de defesa aprovados pelos EUA. Esse comunicado foi publicado pouco antes de a Rússia iniciar a invasão da Ucrânia, em 24 de fevereiro de 2022.

Em março, em uma [coletiva de imprensa sobre ameaças cibernéticas aos Estados Unidos](#), Anne Neuberger, assessora adjunta de segurança nacional do governo Biden, fez um apelo ao setor privado sobre possíveis ataques cibernéticos conduzidos pelo estado russo contra a infraestrutura crítica. Em sua fala, Anne destacou como "elemento mais preocupante" a presença de "vulnerabilidades conhecidas" usadas até por "agentes cibernéticos sofisticados para comprometer empresas americanas, para comprometer empresas do mundo todo", deixando as coisas "muito mais fáceis do que deveriam ser para os invasores".

“O elemento mais preocupante que mencionei agora há pouco é que continuamos vendo vulnerabilidades conhecidas, para as quais temos patches disponíveis, usadas até por criminosos cibernéticos sofisticados para comprometer empresas americanas, para comprometer empresas do mundo todo. E [...] isso deixa as coisas muito mais fáceis do que deveriam ser para os invasores.”

— Anne Neuberger, Assessora adjunta de segurança nacional do governo Biden

Em novembro de 2021, a CISA lançou a [Binding Operational Directive 22-01](#), que determina prazos de correção para vulnerabilidades exploradas conhecidas em órgãos e organizações do Federal Civilian Executive Branch nos EUA. Juntamente com a diretiva, a CISA estabeleceu seu catálogo KEV para rastrear vulnerabilidades significativas que foram observadas em ataques. Desde sua divulgação, o KEV tornou-se uma ferramenta de priorização útil para organizações em todos os setores.

Em setembro, órgãos americanos, junto com o centro de segurança cibernética da Austrália, o centro de segurança cibernética do Canadá e o centro nacional de segurança cibernética do Reino Unido, [publicaram um comunicado conjunto de segurança cibernética \(AA22-257A\)](#) referente à atividade de APT afiliada ao corpo de guardas revolucionários islâmicos (IRGC) do Irã, uma continuação do [comunicado anterior emitido por esses órgãos em novembro de 2021 \(AA21-321A\)](#). Sem surpresa, o comunicado mais recente destaca algumas vulnerabilidades conhecidas exploradas por agentes de APT afiliados ao IRGC, incluindo Log4Shell, ProxyShell e falhas no FortiOS da Fortinet (discutidas anteriormente na seção "Vulnerabilidades relevantes" deste relatório).

Em junho, a CISA, a NSA e o FBI emitiram um comunicado conjunto de segurança cibernética detalhando o uso de vulnerabilidades conhecidas publicamente por agentes com apoio governamental afiliados à República Popular da China (RPC), seguido por [outro comunicado de segurança cibernética conjunto \(AA22-279A\)](#) dos mesmos órgãos em outubro, detalhando as 20 principais CVEs que foram exploradas ativamente por agentes cibernéticos com apoio governamental da RPC.

Vulnerabilidades conhecidas representam uma ameaça à infraestrutura crítica e ao setor privado

Um tema importante desses comunicados do governo é que vulnerabilidades conhecidas com patches disponíveis estão sendo exploradas rotineiramente para a obtenção de acesso inicial às organizações e posterior elevação de privilégios. De fato, quando analisamos coletivamente todos os avisos, várias vulnerabilidades sobrepostas estão sendo usadas por cada um desses agentes de ameaças com apoio governamental.

CVEs sobrepostos	Tipo de produto	Exploração com apoio governamental
CVE-2018-13379	VPN de SSL	Irã, Rússia
CVE-2019-11510	VPN de SSL	RPC, Rússia
CVE-2019-19781	VPN de SSL	RPC, Rússia
CVE-2020-0688	Servidor de e-mails	Irã, Rússia
CVE-2020-5902	Servidor de gerenciamento de tráfego	RPC, Rússia
CVE-2021-26855	Servidor de e-mails	RPC, Rússia
CVE-2021-26857	Servidor de e-mails	RPC, Rússia
CVE-2021-26858	Servidor de e-mails	RPC, Rússia
CVE-2021-27065	Servidor de e-mails	RPC, Rússia
CVE-2021-44228	Biblioteca de logs	RPC, Irã

Nós abordamos várias falhas sobrepostas em relatórios do cenário de ameaças anteriores, incluindo o trio de falhas de VPN de SSL e vulnerabilidades do servidor de e-mail, como o ProxyLogon. Esses tipos de produtos amplamente usados são explorados rotineiramente todos os anos por uma variedade de agentes de ameaças, incluindo esses agentes de ameaças com apoio governamental. Há uma forma clara de impedir que essas falhas continuem a estar presentes nos kits de ferramentas dos invasores: aplicar os patches disponíveis. Gostaríamos que essas vulnerabilidades desaparecessem nas futuras versões desse relatório.

"Vimos apenas que o problema continua piorando [...] Observamos um volume mais alto de ataques de ransomware, e o prejuízo financeiro também está aumentando."

– Paul Abbate,
diretor adjunto do FBI

Ransomware: o novo normal

Para obter um panorama dos diferentes agentes envolvidos em ataques de ransomware, consulte nosso [Relatório do ecossistema de ransomware](#) publicado em junho de 2022.

Ao longo de 2022, houve [relatos de que os ataques de ransomware tiveram um declínio](#) em relação aos anos anteriores. No entanto, os dados analisados para o Relatório do cenário de ameaças deste ano mostram que a frequência dos ataques de ransomware permanece igual à dos anos anteriores: de acordo com a nossa análise dos dados de violação disponíveis publicamente, 35,5% das violações de 2022 foram resultantes de um ataque de ransomware, uma queda de 2,5% em relação a 2021.

Em novembro, no Aspen Cyber Summit, Paul Abbate, diretor adjunto do FBI, [disse que](#) o órgão "só vê o problema piorar, tem observado um volume maior de ataques de ransomware, além de um aumento no prejuízo financeiro."

Nem todos os ataques de ransomware são levados a público

Uma das maneiras pelas quais nós quantificamos os ataques de ransomware na nossa análise são as notícias; a outra, via entradas em sites de vazamento de ransomware. Nesses sites, grupos de ransomware ameaçam publicar dados roubados das organizações vitimadas. O grande desafio de confiar nos dados dos sites de vazamento é que pode haver casos em que uma organização opte por pagar o pedido de resgate antes de o grupo publicar uma entrada no site de vazamento, o que faz com que as métricas extraídas desses sites sejam pouco confiáveis.

Outro desafio é que nem todos os ataques de ransomware são conhecidos do público. Em alguns casos, as empresas usam uma linguagem genérica cuidadosa, como "ataque cibernético" ou "incidente", ao anunciar uma violação de dados ou evento de segurança. Os países e os setores afetados têm requisitos de denúncia e comunicação diferentes, e não há uma exigência universal para as organizações relatarem a causa raiz de um dado incidente, embora algumas possam optar por divulgar essas informações. Isso faz com que seja desafiador quantificar de forma exata os ataques de ransomware e as violações em geral. Portanto, é importante reconhecer que, provavelmente, a quantidade real de ataques de ransomware nos últimos anos foi bastante subestimada.

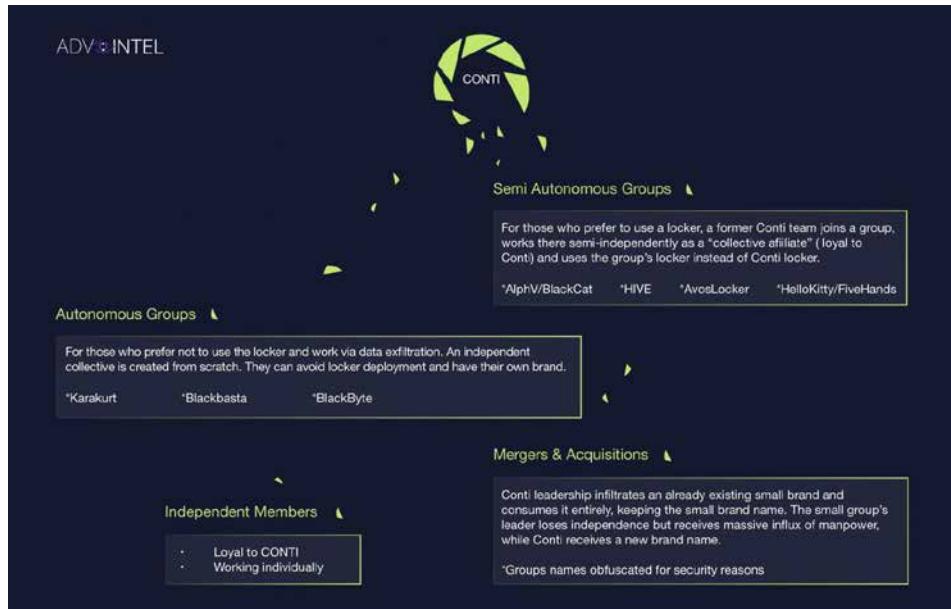
Como se acostumar com o novo normal

Toda novidade, em algum momento, perde sua popularidade. No cenário de ameaças, a novidade dos ataques de ransomware esvaiu-se, mas eles persistem. Os ataques de ransomware tornaram-se o novo normal.

A ascensão e a queda do Conti

O Conti, um grupo de ransomware que ganhou notoriedade em um período de dois anos, durante o qual teve pelo menos US\$ 180 milhões de lucro, encerrou suas operações em maio de 2022. A queda do Conti foi considerada uma vitória por muitas pessoas, pois ele consolidou-se como um dos grupos de ransomware mais dominantes dos últimos anos. Porém, como vimos no passado com o desaparecimento de outros grupos de ransomware, como o DarkSide e o BlackMatter, esse não é o fim do Conti, de seus membros ou táticas e técnicas do grupo.

De acordo com pesquisadores da Advanced Intel, que foram os [primeiros a relatar a saída do Conti do ecossistema de ransomware](#), as parcerias existentes entre o Conti e outros grupos de ransomware, incluindo ALPHV/BlackCat, Hive, AvosLocker e HelloKitty/FiveHands, permitiram que os membros entrassem nesses grupos oferecendo ajuda com desenvolvimento, testes de penetração, intel e negociação.



Fonte da imagem: Advanced Intel

Membros independentes, que a Advanced Intel diz serem "leais à Conti", provavelmente atuam de forma individual, possivelmente como afiliados de outros grupos. Por fim, alguns ex-membros do Conti fizeram a transição para grupos que focam exclusivamente na extração de dados para operações exclusivas de extorsão, que incluem grupos como Karakurt, Black Basta e Blackbyte.

No ecossistema do ransomware, os grupos não são constantes; os membros do grupo, incluindo os afiliados, são os elementos importantes, e é por isso que o impacto a longo prazo da extinção de um grupo de ransomware é amenizado.

A importância de ataques exclusivos de extorsão aumenta

Os ataques de ransomware usufruíram de grande sucesso com técnicas de dupla extorsão, que envolvem:

1. **criptografar arquivos na rede pretendida;**
2. **extração e ameaça de publicar dados roubados.**

Uma característica importante no cenário de ameaças de 2022 foi o aumento da prevalência de ataques exclusivos de extorsão. Nesses ataques, os agentes de ameaças acessam as redes pretendidas com o objetivo específico de extrair dados confidenciais para pedir resgate ou vender na dark web, sem implementar nenhum malware de criptografia que dê o nome ao ransomware. Grupos que adotam uma abordagem exclusiva de extorsão estavam no auge em 2022. O mais notável foi o grupo LAPSUS\$, que extraiu dados de várias empresas na América do Sul e na Europa, além de empresas de tecnologia proeminentes, como Microsoft, Okta e



Nvidia. Alguns membros do grupo Conti também participaram de operações de extorsão existentes, como a Karakurt.

Esses grupos costumavam implementar táticas mais "simplistas", contando com phishing, spam de autenticação multifator (MFA) e explorando serviços de suporte técnico para obter acesso aos ambientes pretendidos. Como acontece com suas contrapartes de ransomware, os grupos de extorsão buscam acesso a contas com altos privilégios no Active Directory (AD), abusando de falhas, configurações incorretas e recursos da onipresente ferramenta de gerenciamento de identidade e acesso da Microsoft. Eles também têm como objetivo recursos de nuvem para apoiar a infraestrutura de ataque e acessar dados confidenciais.

As organizações não podem se dar ao luxo de ignorar esses agentes de ameaças só porque parecem "menos sofisticados". Seus ataques podem ser tão prejudiciais quanto os de ransomware e representam um risco considerável para as operações existentes e para a reputação da organização. Além disso, os grupos de ransomware mais sofisticados até adotaram hábitos exclusivos de extorsão como uma evolução dos seus manuais.

A orientação a seguir ajudará as organizações a se defenderem contra ataques de grupos de extorsão:

- Reavalie as políticas de suporte técnico e a conscientização de engenharia social;
- Fortaleça as políticas de senha: evite a MFA baseada em SMS, garanta o uso de senhas fortes e utilize autenticação sem senha;
- Use opções de autenticação robustas para aplicações voltadas à Internet;
- Encontre e aplique patches em vulnerabilidades exploradas conhecidas, que possam permitir que os invasores elevem privilégios e extraiam dados confidenciais;
- Reforce a postura de segurança da nuvem: aprimore a detecção de risco e fortaleça as configurações de acesso;
- Certifique-se de que os serviços de segurança de identidade, como o AD, sejam configurados adequadamente de acordo com as práticas recomendadas de zero trust.

Novos grupos de ransomware e extorsão

Pelo menos 31 novos grupos de ransomware e extorsão foram descobertos entre 1º de novembro de 2021 e 31 de outubro de 2022.

Grupo	Tipo	Data de descoberta
ALPHV/BlackCat	Ransomware	Novembro de 2021
Rook	Ransomware	Novembro de 2021
Sugar	Ransomware	Novembro de 2021
Night Sky	Ransomware	Dezembro de 2021
White Rabbit	Ransomware	Dezembro de 2021
RansomHouse	Extorsão	Dezembro de 2021
Ransom Cartel	Ransomware	Dezembro de 2021
Royal	Ransomware	Janeiro de 2022
Entropy	Ransomware	Fevereiro de 2022
Pandora	Ransomware	Março de 2022
Luna Moth	Extorsão	Março de 2022
Black Basta	Ransomware	Abril de 2022
DarkAngels	Ransomware	Maio de 2022
Cheerscrypt	Ransomware	Maio de 2022
Omega	Ransomware	Maio de 2022
Checkmate	Ransomware	Maio de 2022
BlueSky/Blue Sky	Ransomware	Maio de 2022
Luna	Ransomware	Junho de 2022
GwisinLocker	Ransomware	Junho de 2022
Play	Ransomware	Junho de 2022
RedAlert (N13V)	Ransomware	Julho de 2022
HavanaCrypt	Ransomware	Julho de 2022
Lilith	Ransomware	Julho de 2022
BianLian	Ransomware	Julho de 2022
Monti	Ransomware	Julho de 2022
Donut Leaks	Extorsão	Agosto de 2022
Agenda	Ransomware	Agosto de 2022
Venus	Ransomware	Agosto de 2022
TommyLeaks/SchoolBoys	Extorsão	Setembro de 2022
Hardbit	Ransomware	Outubro de 2022
Prestige	Ransomware	Outubro de 2022

Essas informações são baseadas em fontes disponíveis ao público, incluindo agências de notícias e publicações de blogs de fornecedores, e podem não refletir todos os novos grupos de ransomware ou extorsão.

Com a queda do Conti, outros grupos de ransomware surgiram para recolher os pedaços. O ALPHV/BlackCat é um desses grupos. Ele é um dos principais grupos de ransomware em operação hoje em dia no que se refere a execução e volume de ataques de ransomware.

O Active Directory permanece um componente crítico para ataques de ransomware bem-sucedidos

O comprometimento do Active Directory continua sendo um aspecto importante para permitir que o ransomware atinja seus objetivos de criptografia de sistemas em todo o domínio e extração de dados para facilitar a dupla extorsão. Como o vilão Thanos da Marvel, o comprometimento do AD é inevitável. Em 2022, os pesquisadores do DFIR Report [destacaram um dos casos de ransomware mais rápidos](#): ele envia o ransomware Quantum e resultou na propagação de ransomware em todo o domínio em menos de quatro horas. Nesse caso, foi o uso do [AdFind](#), uma ferramenta para coletar informações no AD, que por fim resultou na implementação de ransomware em todo o domínio. Historicamente, os grupos de ransomware também utilizam uma série de vulnerabilidades para elevar privilégios como administrador de domínio na organização vitimizada, incluindo a CVE-2020-1472, uma vulnerabilidade de elevação de privilégios (EoP) no Windows Netlogon, também conhecido como Zerologon, e a CVE-2021-36942, uma vulnerabilidade de falsificação na autoridade de segurança local do Windows, também conhecida como PetitPotam, que a Microsoft chama de "ataque de Relay NTLM clássico". Apesar da disponibilidade de patches para o PetitPotam, ataques de relay do New Technology LAN Manager (NTLM) do Windows ainda são possíveis, então as organizações precisam aplicar mitigações adicionais, descritas [aqui](#).

A exploração dessas falhas, combinada com uma variedade de ferramentas utilizadas por grupos de ransomware para coletar informações vitais do AD, destaca a importância de identificar os [indicadores de exposição](#) e os [indicadores de ataque](#) nos ambientes do seu AD. Ao [fortalecer o AD contra ataques de ransomware](#), as organizações podem impedir as tentativas desses grupos de criptografar e extrair dados roubados para uso e permitir que a organização opere em uma posição de defesa.



Violações

As estatísticas de violação da Tenable são do período entre 1º de novembro de 2021 e 31 de outubro de 2022 e incluem violações datadas dentro do intervalo especificado e violações relatadas nesse intervalo, sem a data da violação em si.

Como parte do monitoramento do cenário de ameaças, a SRT da Tenable acompanha os relatórios de violação diariamente para rastrear tendências em nível macro. Em 2022, rastreamos 1.335 ocorrências de violação durante o período especificado acima, uma redução de 26,8% dos 1.825 que rastreamos durante o mesmo período do ano anterior.

Nossa análise desses incidentes de violação é realizada da melhor forma possível e não foi criada para ser uma lista completa de todas as violações relatadas durante esse período. Com base no nosso exame anterior de dados de violação, reconhecemos que o processo de divulgação de violações leva tempo e, portanto, algumas violações podem não ser levadas a público até meses ou anos após a ocorrência. Além disso, também precisamos reconhecer que alguns setores e regiões têm requisitos de denúncia ou comunicação variáveis ou inexistentes, assim como autoridades centrais para denúncia. Isso faz com que seja quase impossível obter uma visão global abrangente das violações que ocorreram nesse período.

Em 2022, as ocorrências de violação analisadas resultaram na exposição de 2,29 bilhões de registros, uma queda acentuada em relação a 2021, que teve 40 bilhões de registros expostos. Isso foi acompanhado por um declínio comparável na quantidade de arquivos expostos em 2022: 389 milhões, incluindo documentos e e-mails. Apesar do declínio acentuado nos registros e arquivos expostos, o volume total de dados expostos como parte das ocorrências de violação em 2022 permaneceu estável em 257 Terabytes, comparado com 260 Terabytes em 2021.

Das 1.335 ocorrências de violação rastreadas em 2022, 88,2% das organizações afetadas relataram exposição de registros. Entretanto, 45% não divulgaram a quantidade de registros expostos e, em 6,1% das violações, as organizações afetadas não puderam confirmar se houve ou não exposição de registros.

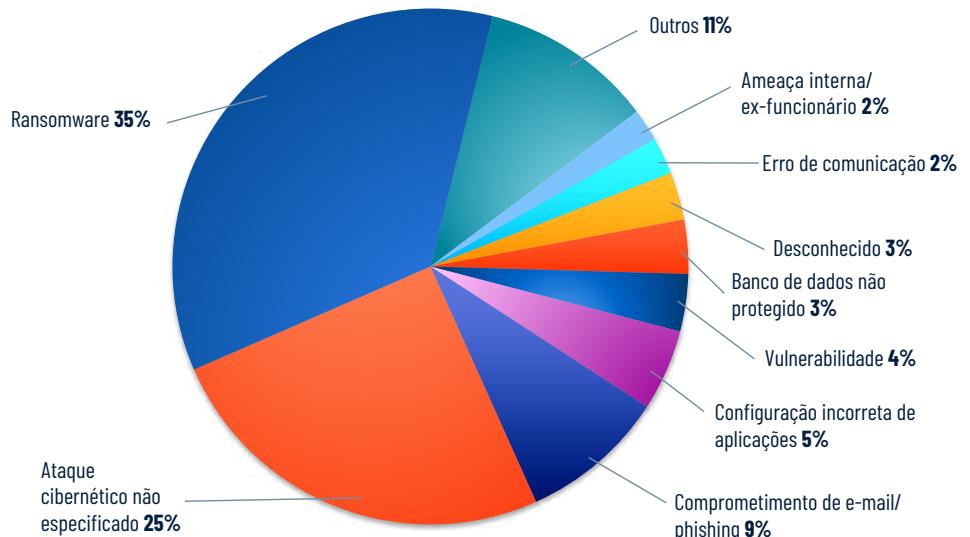
Mais de 2,2 bilhões de registros foram expostos em 2022

PONTO DE DADOS	2021	2022
Registros expostos no total	40.000.000.000	2.296.941.687
Total de arquivos expostos	1.800.000.000	389.127.450
Total de dados expostos	260 Terabytes	257 Terabytes

Região	Registros expostos no total	% do total
Ásia-Pacífico (APAC)	1.561.990.339	68,00%
América do Norte (NAM)	405.954.391	17,67%
Europa, Oriente Médio e África (EMEA)	305.994.856	13,32%
Desconhecido/Global	22.540.901	0,98%
América Latina (LATAM)	461.200	0,02%
Total	2.296.941.687	

Mais de dois terços (68%) dos registros expostos originaram-se em organizações localizadas na Ásia-Pacífico (APAC). Organizações da América do Norte (NAM) e da Europa, no Oriente Médio e na África (EMEA) representaram um total de 31% dos registros expostos. Em alguns casos, a região de uma organização não estava clara, então categorizamos esses eventos de violação como "Desconhecido/Global". Por fim, as ocorrências de violação na América Latina (LATAM) representaram apenas 0,02% dos registros expostos. Nós presumimos que essa grande diferença tenha mais a ver com os diferentes requisitos de comunicação de violações entre os países da LATAM e da NAM, da APAC e da EMEA, do que uma diferença considerável nas atividades de invasores nas diferentes regiões.

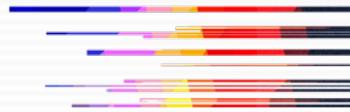
Violações de 2022 por causa raiz



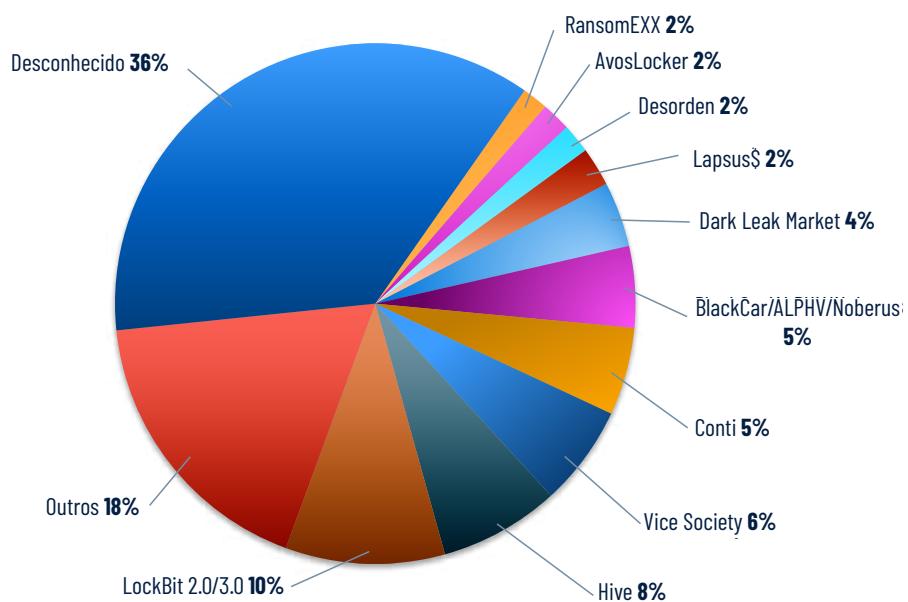
Em 2022, o ransomware continuou sendo a causa raiz mais comum de violações nas organizações, representando 35,4% de todas as ocorrências de violação. Houve uma pequena queda em relação a 2021, quando o ransomware representou 38% de todas as ocorrências de violação.

Ocorrências de ransomware como percentual de todas as ocorrências de violação

2022	2021	2020
35,4%	38%	35%



Ataques de ransomware/extorsão em 2022



Ao analisarmos todas as ocorrências de violação vinculadas a ataques de ransomware ou extorsão, classificamos quase metade (36,4%) como "Desconhecido", pois não conseguimos identificar nenhum detalhe específico sobre o grupo de ransomware ou extorsão responsável por esses ataques. Também tentamos fazer referência cruzada desses ataques com sites de vazamento de dados na dark web associados a grupos de ransomware e extorsão, mas não conseguimos vinculá-los a um grupo específico. Como não há requisitos de comunicação para ataques de ransomware, esses tipos de detalhe costumam ser desprezados.

Fora da categoria "Desconhecido", o grupo de ransomware LockBit dominou os ataques de ransomware em 2022, representando 9,9% das ocorrências de violação de ransomware analisadas. O LockBit foi autopromovido de 2.0 para 3.0, então esse número inclui ambas as iterações. Outros grupos da lista incluem o grupo de ransomware Hive (7,5%), Vice Society (6,3%) e BlackCat/ALPHV (5,1%). Outros, que compreendem 37 outros grupos, foram coletivamente responsáveis por 17,8% dos incidentes de ransomware/extorsão restantes em 2022.

Apesar de o notório grupo de ransomware Conti ter fechado as portas em maio de 2022, ele foi responsável por 5,5% das ocorrências de violação de ransomware analisadas. Para mais informações sobre o Conti, consulte a seção anterior sobre ransomware.

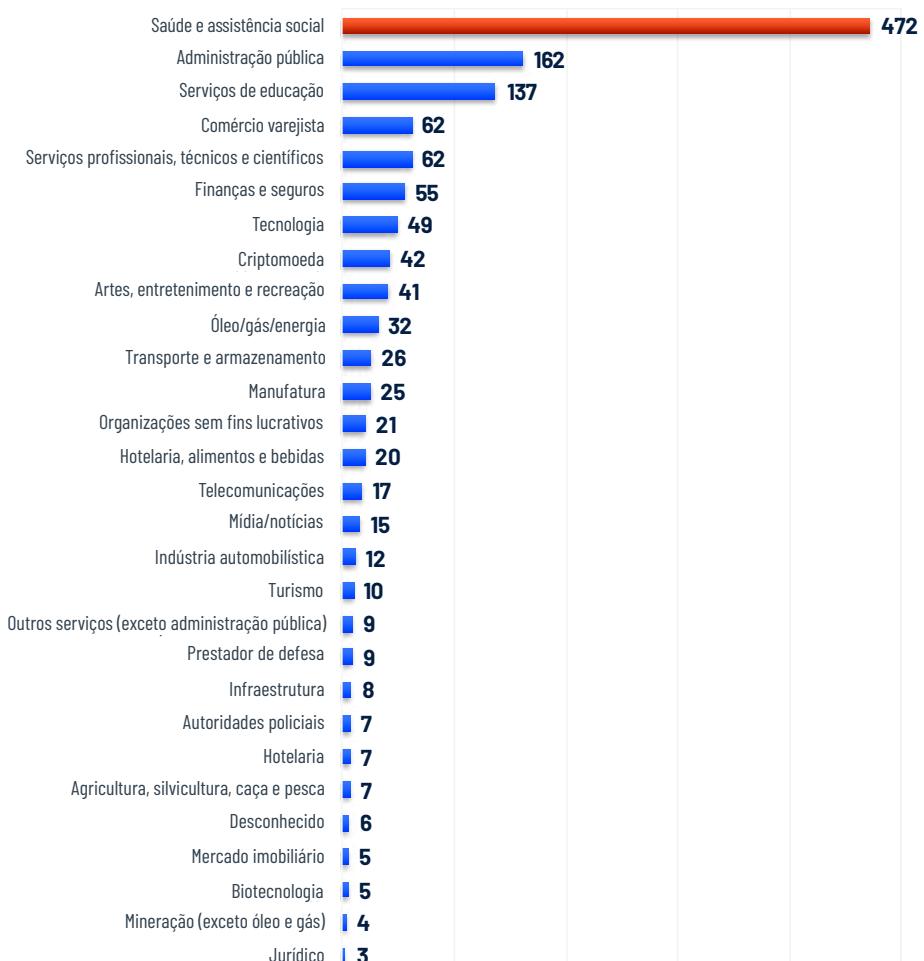
Ataques cibernéticos não especificados são a causa raiz de um quarto das ocorrências de violação

Em 2022, foi introduzida uma nova categoria chamada "ataque cibernético não especificado", como um termo geral para ocorrências de violação que não especificavam um tipo de causa raiz, mas se referiam globalmente à ocorrência de violação como um ataque cibernético ou incidente cibernético. Essa categoria representou 25,2% de todas as ocorrências em 2022. Na maioria das vezes, apesar de chamar essas ocorrências de ataque cibernético, muitas entidades afetadas não prestaram mais esclarecimentos sobre os incidentes.

**Em 2022,
o setor de
saúde foi
o principal
alvo de
ataques de
ransomware,
com 472
violações.**

O comprometimento de e-mail, que inclui ataques de phishing, representou 9,1% das ocorrências de violação em 2022, enquanto 5,1% foram decorrentes de configurações incorretas de aplicações, que muitas vezes incluem instâncias de armazenamento em nuvem mal configuradas, como Amazon Simple Storage Service (S3), Google Cloud Storage Buckets e Azure Blob Storage.

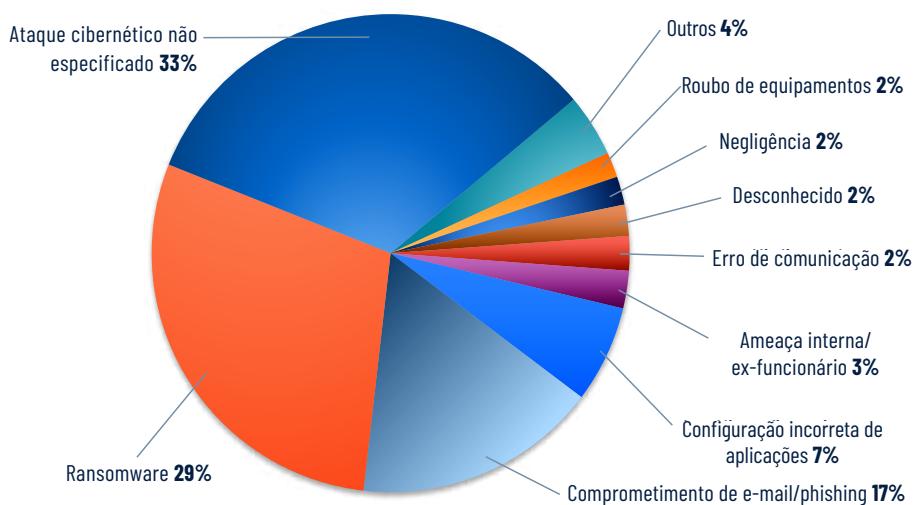
Violações de 2022 por setor



Sem nenhuma surpresa, as áreas de saúde e assistência social continuam tendo a maior quantidade de violações, representando 35,4% de todas as ocorrências analisadas – um aumento acentuado em relação a 2021, em que 24% das violações foram atribuídas à área da saúde.

A administração pública, que inclui governos e municípios, desbancou a educação para o segundo lugar em 2022, representando 12,1% das ocorrências de violação. A área de serviços educacionais ficou em terceiro lugar em 2022, representando 10,3% das ocorrências de violação.

Violações no setor de saúde em 2022 por causa raiz

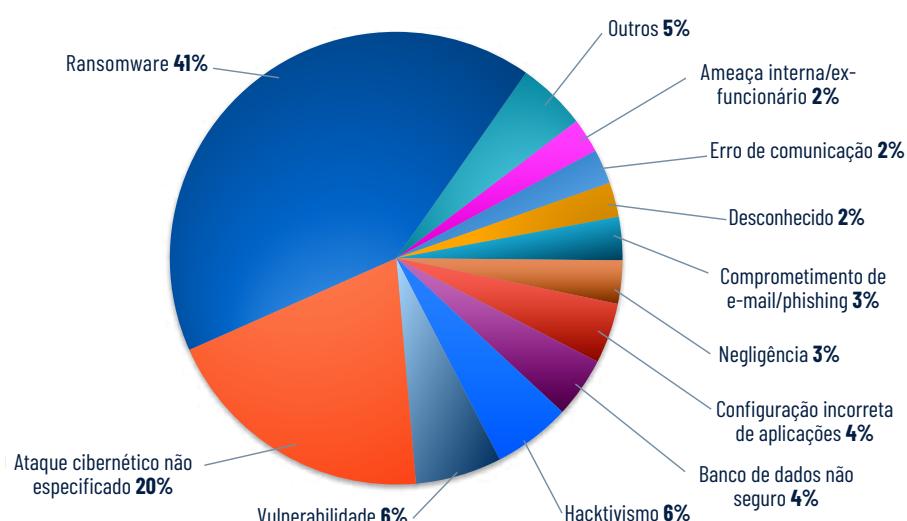


Quase um terço de todas as ocorrências de violação na área da saúde rastreadas em 2022 foram atribuídas a ataques cibernéticos não especificados, seguidos por ransomware em quase 29,2%. Isso representa uma redução de 7% em relação a 2021, quando o ransomware representou 36,2% das violações na área da saúde. Em 2022, 16,5% das violações na área de saúde resultaram de comprometimento de e-mail/phishing.

Por que a saúde é o setor mais afetado?

A área da saúde permanece no topo da nossa lista de ocorrências de violação a cada ano, em parte devido aos [requisitos de relatórios do Departamento de Saúde e Serviços Humanos dos EUA](#) e a regra de notificação de violação da Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) (45 CFR §§ 164.400-414). Além disso, as entidades americanas deverão fazer um comunicado à mídia se uma ocorrência de violação afetar mais de 500 pessoas. Se os padrões de comunicação de violação fossem adotados no mundo todo e fossem tão rigorosos quanto as regras da HIPAA, talvez tivéssemos muito mais informações sobre o nível de exposição das informações de identificação pessoal.

Violações na administração pública em 2022 por causa raiz

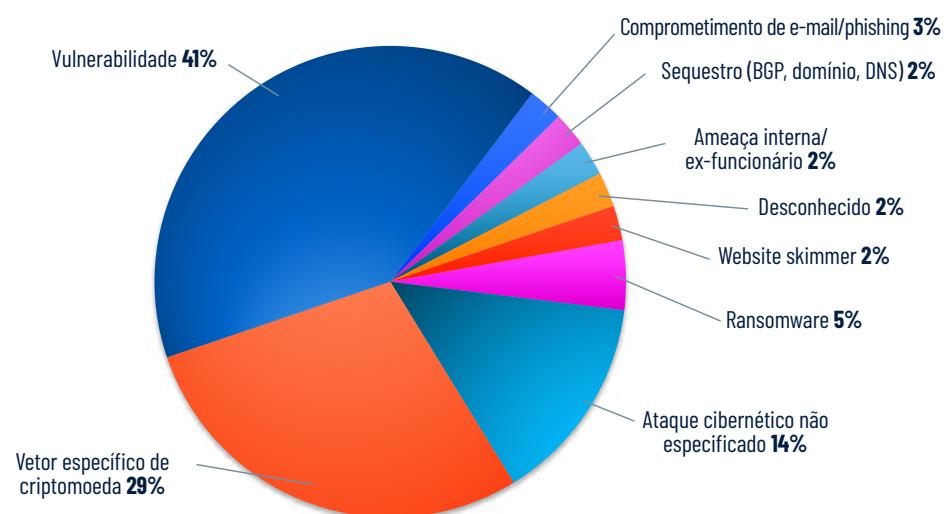


Os ataques de ransomware foram responsáveis por 41,4% de todas as ocorrências de violação na administração pública. Mais notavelmente, em 2022, observamos um esforço conjunto em direção a várias entidades de administração pública na LATAM, incluindo Costa Rica, Brasil e México. O hacktivismo também foi responsável por 5,6% das ocorrências de violação na administração pública, com impressionantes 89% afetando órgãos na LATAM.

Ataques de criptomoedas resultaram no roubo de US\$ 2,4 bilhões

Em 2022, houve pelo menos 42 ocorrências de violação vinculadas ao setor de criptomoedas, incluindo ataques contra entidades em finanças descentralizadas (DeFi), um setor em si que não é administrado por uma entidade ou corporação central e é regido por um código no blockchain conhecido como smart contracts.

Violações de criptomoedas em 2022 por causa raiz



Mais de dois terços (69,1%) das ocorrências de violação no espaço das criptomoedas resultaram de vulnerabilidades ou de uma causa raiz que chamamos de "vetor específico de criptomoeda", que inclui elementos exclusivos desse espaço, como **ataques de empréstimo instantâneo** e **manipulação de oráculo de preço**. Mais de US\$ 1,2 bilhão roubados em ocorrências de violação de criptomoedas foram atribuídos a essas duas causas raiz.

Violações de criptomoedas em 2022 por causa raiz	Fundos roubados
Vulnerabilidade	US\$ 766.460.000
Comprometimento de e-mail/phishing	US\$ 625.000.000
Vetor específico de criptomoeda	US\$ 531.530.000
Ataque cibernético não especificado	US\$ 204.400.000
Desconhecido	US\$ 160.000.000
Website skimmer	US\$ 120.000.000
Sequestro (BGP, domínio, DNS)	US\$ 235.000
Total	US\$ 2.407.625.000

A maior ocorrência de violação de criptomoeda em 2022 foi um ataque contra a Sky Mavis, desenvolvedora do jogo de criptomoeda conhecido como Axie Infinity. Os invasores [usaram ofertas de emprego falsas no LinkedIn para roubar US\\$ 625 milhões da Ronin Bridge](#).

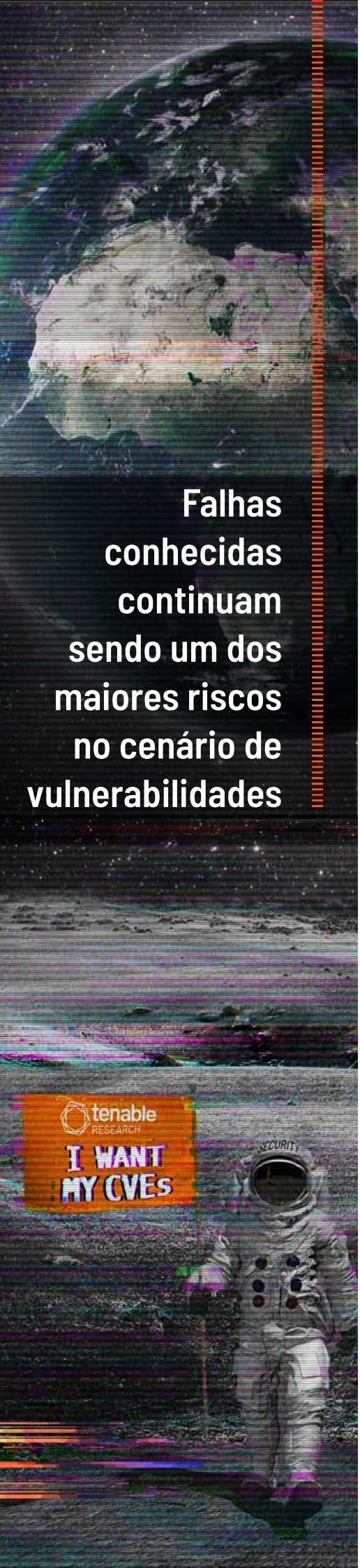
Entidade afetada	Fundos roubados
1. Sky Mavis (Ronin)	US\$ 625.000.000
2. Wormhole Bridge (Solana/Ethereum)	US\$ 320.000.000
3. Bitmart	US\$ 200.000.000
4. Beanstalk	US\$ 182.000.000
5. Winternmute	US\$ 160.000.000
6. Nomad	US\$ 156.000.000
7. Badger DAO	US\$ 120.000.000
8. Binance Bridge (BSC Chain)	US\$ 110.000.000
9. Horizon Ethereum Bridge	US\$ 100.000.000
10. Mango Markets	US\$ 100.000.000

Observação: aqui, os valores em dólares representam o valor no momento da ocorrência das violações. Em decorrência da flutuação de preços das diferentes criptomoedas, esses números podem ser citados de forma diferente pelas fontes de notícias.

Para os criminosos cibernéticos, além do ransomware, violações direcionadas ao espaço de criptomoedas provavelmente serão os empreendimentos mais rentáveis.

Como entender as tendências em ataques cibernéticos por meio dos dados de violação

Nossa análise não é uma lista completa de todas as violações que podem ter ocorrido durante o período informado. Nós observamos que as violações podem não ser divulgadas até anos depois da ocorrência ou da descoberta, e algumas organizações afetadas podem nunca chegar a divulgá-las publicamente. Portanto, suspeitamos que os números verdadeiros das violações provavelmente sejam muito maiores do que os relatados. No entanto, acreditamos que ainda seja prático analisar as violações que foram relatadas publicamente para entender melhor as tendências sob a perspectiva de região e setor, ao mesmo tempo em que nos aprofundamos nas causas raiz mais comuns das violações.



**Falhas
conhecidas
continuam
sendo um dos
maiores riscos
no cenário de
vulnerabilidades**

Conclusão

Com o nosso exame do cenário de vulnerabilidades e ameaças de 2022, ficam as seguintes lições:

Abordar as vulnerabilidades conhecidas é o que se pode fazer de mais eficaz agora. Parecemos um disco quebrado? Sim. Demos o mesmo aviso em 2020 e em 2021 e, mesmo assim, dois anos depois, essas falhas continuam sendo um dos maiores riscos no cenário de vulnerabilidades. Vulnerabilidades sem patches oferecem aos invasores a maneira mais econômica e direta de obter acesso inicial ou elevar privilégios nas organizações. Não espere, identifique o quanto antes os ativos do seu ambiente que estão expostos às vulnerabilidades mencionadas neste relatório.

Ignore o alarde e foque na avaliação do seu ambiente. O incidente da SolarWinds em 2020 e a vulnerabilidade Log4Shell em 2021 causaram um impacto duradouro na forma como o setor reage aos problemas da cadeia de suprimentos. Pesquisadores, jornalistas e, por extensão, executivos e diretores estão preocupados, esperando o "próximo Log4Shell". Em vez de focar na "marca" de uma vulnerabilidade ou nos rumores que a cercam, as organizações precisam deixar de especular e examinar os detalhes específicos das vulnerabilidades, quando disponíveis, para avaliar o verdadeiro possível impacto. O segredo para proteger suas redes é a capacidade de avaliar rapidamente cada faceta do ambiente para identificar todos os ativos e avaliar sua base de código.

Os ataques de ransomware não desaceleraram, então nossos esforços para contê-los também não devem desacelerar. Os relatos da morte iminente do ransomware foram muito exagerados. O ransomware, em si, é um empreendimento lucrativo para os diversos participantes do ecossistema, e não podemos julgar a atividade do ransomware com base apenas nas entradas dos sites de vazamento de dados. O Active Directory é o segredo dos eventos de violação de ransomware de maior sucesso; portanto, as organizações precisam fortalecer os ambientes do AD contra ataques de ransomware.

Configurações incorretas e erros humanos continuam a representar riscos significativos na nuvem. Com guias de práticas recomendadas, dicas de fortalecimento etc. divulgados por CSPs, organizações governamentais e fornecedores, cabe aos usuários de produtos de nuvem e contêiner seguir e acompanhar esses recursos. Erros humanos na configuração e na implementação, mais do que vulnerabilidades, representam alguns dos maiores riscos na nuvem. As organizações que migram para a nuvem precisam examinar continuamente seus contêineres e scripts de implementação para assegurar que suas implementações atendam e superem os limites de segurança. Para mitigar esses riscos, recomendamos que as equipes de segurança adotem soluções de gerenciamento da postura de segurança na nuvem (CSPM). O CSPM estabelece uma configuração segura de linha de base e design para ativos na nuvem. Ao começar com uma linha de base segura como alicerce, a organização pode abordar preventivamente as preocupações com o gerenciamento de usuários e acesso e garantir que a conformidade regulatória seja mantida com a criação de novos serviços e ambientes.



Como a Tenable pode ajudar

A Tenable lançou modelos de verificação para o Tenable One, o Tenable.io Vulnerability Management, o Tenable.sc, o Nessus Expert e o Nessus Professional, que são pré-configurados para permitir uma verificação rápida das vulnerabilidades discutidas neste relatório. Além disso, clientes do Tenable One e do Tenable.io Vulnerability Management têm um novo painel e novos widgets na biblioteca de widgets, e usuários do Tenable.sc também têm um novo painel cobrindo a Retrospectiva do cenário de ameaças de 2022.

Sobre a equipe de resposta de segurança da Tenable

A Tenable Research procura destacar-se no ciclo de gerenciamento de vulnerabilidades. Nossa equipe de resposta de segurança (SRT) monitora feeds de vulnerabilidade e threat intel para garantir que as equipes de pesquisa possam oferecer cobertura de sensor para os nossos produtos o mais rápido possível. A SRT também trabalha para investigar detalhes técnicos e publicações de autores, posts de blogs e comunicados adicionais para garantir que as partes interessadas estejam totalmente informadas sobre os riscos e as ameaças mais recentes. A SRT apresenta análises das vulnerabilidades mais recentes no blog da Tenable.

A Tenable Research lançou mais de 180 mil plug-ins e lidera o setor em cobertura de CVEs. A equipe está focada em trabalhos diversos que formam os pilares do gerenciamento de vulnerabilidades: criação de plug-ins para detecção de vulnerabilidades e ativos, desenvolvimento de verificações de auditoria e conformidade e melhoria da automação do VM.

Sobre os autores:

[Scott Caveza](#), Senior Manager, Research

[Satnam Narang](#), Senior Staff Research Engineer

[Ciarán Walsh](#), Associate Research Engineer

Créditos adicionais:

[Susan Nunziata](#), Senior Director of Editorial & Content

[Juan Perez](#), Senior Content Marketing Manager

Sobre a Tenable

A Tenable® é a empresa de Exposure Management. Mais de 40 mil organizações no mundo todo contam com a Tenable para entender e reduzir o risco cibernético. Como criadora do Nessus®, a Tenable aproveita sua experiência em vulnerabilidades para oferecer a primeira plataforma capaz de visualizar e proteger qualquer ativo digital em qualquer plataforma computacional. Entre os clientes da Tenable, estão mais de 60% das empresas Fortune 500, mais de 40% das empresas Global 2.000 e agências governamentais de grande porte. Saiba mais em pt-br.tenable.com.

SEÇÃO 3

Um olhar mais atento sobre as principais vulnerabilidades de 2022



VULNERABILIDADE DE DIA ZERO



EXPLORADA



VULNERABILIDADE NOMEADA



VULNERABILIDADE ANTERIOR A 2022



NUVEM



RELEVANTE

Adobe



A [CVE-2022-24086](#) é uma vulnerabilidade de validação de entrada imprópria que pode levar à execução remota de código (RCE) por um invasor não autenticado. A Adobe estava ciente da exploração limitada no mundo real direcionada aos comerciantes do Adobe Commerce no momento em que o patch foi lançado.



A [CVE-2022-24087](#) é uma vulnerabilidade de validação de entrada imprópria que pode levar à RCE por um invasor não autenticado. Como a CVE-2022-24086, a CVE-2022-24087 parece não ter sido explorado no mundo real.



Amazon Web Services



A [CVE-2022-0070](#) e a [CVE-2022-0071](#) são vulnerabilidades no Apache Log4j Hot Patch Service produzido pela Amazon Web Services, causadas pela capacidade de execução de comandos com privilégios desnecessários.



SEM-ID-CVE: uma vulnerabilidade XML External Entity (XXE) encontrada no serviço AWS CloudFormation. Quando explorada, a vulnerabilidade permite que os invasores obtenham primitivas de divulgação de arquivos e credenciais, que podem ser usadas para vazar arquivos confidenciais em máquinas vulneráveis.

Nome: BreakingFormation



SEM-ID-CVE: uma vulnerabilidade de divulgação de informações no AWS Glue. Quando a vulnerabilidade é explorada, o invasor consegue acessar credenciais de contas de serviço da AWS, obtendo acesso completo à API de serviço interno. Combinando essa exploração com uma configuração incorreta na API, os invasores conseguem aumentar os privilégios para acesso irrestrito a todos os recursos da região.

Nome: Superglue



Apache



A [CVE-2021-31805](#) é uma vulnerabilidade de avaliação forçada de Object-Graph Navigation Language (OGNL) no Apache Struts que pode levar à RCE. Esta é uma correção secundária para a CVE-2020-17530, pois o patch inicial estava incompleto.



A [CVE-2021-44228](#) é uma vulnerabilidade de RCE no Apache Log4j 2. Um invasor remoto não autenticado poderia explorar essa falha enviando uma solicitação especialmente criada para um servidor que executa uma versão vulnerável do log4j. A solicitação elaborada usa uma injeção de Java Naming and Directory Interface (JNDI) por meio de uma variedade de serviços, incluindo:

- Protocolo LDAP (Lightweight Directory Access Protocol);
- LDAP seguro;
- Invocação de método remoto;
- Serviço de nome de domínio.

Se o servidor vulnerável usar o Log4j para registrar as solicitações, a exploração solicitará uma carga maliciosa sobre JNDI por meio de um dos serviços acima de um servidor controlado pelo invasor. O sucesso dessa exploração poderia resultar em RCE.

Nome: Log4Shell



A [CVE-2021-44521](#) é uma vulnerabilidade de injeção de código no Apache Cassandra. Para explorar essa vulnerabilidade, alguns requisitos de configuração não padrão são necessários. O sucesso dessa exploração permitiria que o invasor escapasse da área restrita e conseguisse a RCE.



A [CVE-2022-42889](#) é uma vulnerabilidade de avaliação de script perigosa nos interpoladores padrão na classe Apache Commons Text StringSubstitutor. Um invasor pode explorar essa vulnerabilidade passando uma string especialmente criada com dados não confiáveis, geralmente por meio de um campo de entrada de usuário, que é interpolado pela classe StringSubstitutor. O sucesso dessa exploração resultaria na execução de código arbitrário ou faria com que uma aplicação efetuasse uma pesquisa arbitrária em um servidor remoto controlado pelo invasor.

Nome: Text4Shell



Apple



A [CVE-2021-1789](#) é uma vulnerabilidade de confusão de tipo do iOS, do iPadOS, do macOS, do tvOS e do watchOS. Um dispositivo vulnerável que acessa ou processa uma página Web especialmente criada pode conceder privilégios arbitrários de execução de código a um invasor. De acordo com o Threat Analysis Group (TAG) do Google, essa vulnerabilidade foi [explorada no mundo real como parte de uma cadeia de ataques](#) que incluía a CVE-2021-30869.



A [CVE-2021-30869](#) é uma vulnerabilidade de confusão de tipo do iOS, do iPadOS e do macOS. Uma aplicação mal-intencionada com código de exploração pode obter execução arbitrária de código com privilégios de kernel.



Apple (continuação)>>

A [CVE-2022-22587](#) é um problema de corrupção de memória no IOMobileFrameBuffer do macOS, do iOS e do iPadOS. Uma aplicação mal-intencionada pode explorar a falha para obter execução arbitrária de código com privilégios de kernel.



A [CVE-2022-22588](#) é um problema de depleção de recursos do iOS e do iPadOS. O invasor pode explorar essa vulnerabilidade quando um dispositivo iOS ou iPadOS tenta processar um acessório com nome malicioso HomeKit. O sucesso dessa exploração poderia resultar em uma condição de negação de serviço (DoS).

Nome: doorLock



A [CVE-2022-22594](#) é um problema de origem cruzada na API IndexDB para o WebKit Storage. A exploração dessa falha permitiria que um site rastreasse informações confidenciais do usuário.



A [CVE-2022-22620](#) é um problema da vulnerabilidade "use-after-free" que afeta o macOS, o iOS e o iPadOS. Um site malicioso pode ser usado para obtenção da execução de código arbitrário. A Apple sabia da exploração dessa falha no mundo real no momento em que o patch foi lançado.



A [CVE-2022-22674](#) é um problema de leitura fora dos limites no driver de gráficos da Intel para macOS. O invasor pode explorar essa vulnerabilidade para ler memória do kernel.



A [CVE-2022-22675](#) é uma vulnerabilidade de gravação fora dos limites no AppleAVD do macOS e do watchOS que foi explorada no mundo real. O invasor pode explorar essa vulnerabilidade usando uma aplicação criada especialmente para ler a memória do kernel.



A [CVE-2022-32893](#) é um problema de gravação fora dos limites no mecanismo de navegador Web WebKit da Apple no iOS, no iPadOS e no macOS. O invasor pode explorar essa vulnerabilidade ao usar engenharia social em um alvo que acessa um site com conteúdo Web mal-intencionado. O sucesso dessa exploração poderia resultar na execução de códigos arbitrários.



A [CVE-2022-32894](#) e a [CVE-2022-32917](#) são problemas de gravação fora dos limites no kernel do iOS, do iPadOS e do macOS. O invasor pode explorar essa falha convencendo a vítima a abrir uma aplicação criada especialmente com código malicioso. O sucesso dessa exploração poderia resultar na execução de códigos arbitrários com privilégios de kernel.



A [CVE-2022-42827](#) é uma vulnerabilidade de gravação fora dos limites que afeta o kernel do iOS e do iPadOS, podendo permitir a execução arbitrária de código com privilégios de kernel.



Apple (continuação)>>

A [CVE-2022-42856](#) é uma vulnerabilidade de confusão de tipos no mecanismo de navegador Web WebKit da Apple no macOS, no iOS, no iPadOS, no tvOS e no Safari. O invasor pode explorar essa vulnerabilidade ao usar engenharia social em um alvo que acessa um site com conteúdo Web mal-intencionado. O sucesso dessa exploração poderia resultar na execução de códigos arbitrários.



Arm



A [CVE-2022-23960](#) é uma vulnerabilidade de especulação de cache em que o código malicioso usa o histórico de ramificação compartilhado para influenciar ramificações imprevistas no hardware da vítima. Essa técnica pode ser usada para provocar a alocação do cache, permitindo que o invasor acesse dados que não deveriam poder ser acessados.

Nome: Spectre-BHB



Atlassian



A [CVE-2022-26134](#) é uma vulnerabilidade de injeção de OGNL no Atlassian Confluence Server and Data Center. Um invasor remoto e não autenticado poderia explorar essa vulnerabilidade com o envio de uma solicitação HTTP específica para uma instância vulnerável do Confluence Server ou do Data Center. O sucesso dessa exploração resultaria na execução de códigos arbitrários.



A [CVE-2022-26136](#) é uma vulnerabilidade arbitrária de desvio de filtro de servlet em vários produtos da Atlassian. Um invasor remoto e não autenticado poderia explorar essa vulnerabilidade com o envio de uma solicitação HTTP específica para se desviar de vários filtros de servlet usados por aplicações próprias e de terceiros.



A [CVE-2022-26137](#) é uma vulnerabilidade de invocação de filtro de servlet em vários produtos da Atlassian. Um invasor remoto e não autenticado poderia explorar essa vulnerabilidade com o envio de uma solicitação HTTP específica para se desviar do filtro de servlet usado para responder a solicitações de compartilhamento de recursos entre origens (CORS).



A [CVE-2022-26138](#) é uma vulnerabilidade de senha codificada na aplicação Questions for Confluence para o Confluence Server e o Confluence Data Center. A aplicação cria uma conta de usuário padrão com privilégios elevados. Um invasor com conhecimento da senha codificada poderia explorar a falha para obter acesso ao Confluence e acessar todas as páginas às quais o grupo "confluence-users" tenha acesso.



VULNERABILIDADE NOMEADA



VULNERABILIDADE ANTERIOR A 2022



NUVEM



RELEVANTE

Cisco



A [CVE-2020-3153](#) é uma vulnerabilidade de caminho de pesquisa descontrolada no Cisco AnyConnect Secure Mobility Client for Windows. Um invasor local autenticado com credenciais válidas do Windows poderia explorar essa vulnerabilidade usando um arquivo mal-intencionado copiado em um diretório do sistema. O sucesso dessa exploração permitiria que o invasor copiasse os arquivos mal-intencionados em locais no sistema Windows com privilégios no nível do sistema.



A [CVE-2020-3433](#) é uma vulnerabilidade de sequestro de DLL no Cisco AnyConnect Secure Mobility Client for Windows. Um invasor local autenticado com credenciais válidas do Windows poderia explorar essa vulnerabilidade por meio de uma mensagem IPC criada especialmente para o processo do AnyConnect. O sucesso dessa exploração concederia privilégios de execução de código arbitrário como SYSTEM.



A [CVE-2022-20624](#) é uma vulnerabilidade DoS no recurso Cisco Fabric Services over IP (CFSoIP) encontrado no software NX-OS da Cisco. Um invasor remoto não autenticado poderia explorar essa falha enviando pacotes CFSoIP criados especialmente para um dispositivo vulnerável. O sucesso dessa exploração resultaria em uma condição DoS.



A [CVE-2022-20821](#) é uma vulnerabilidade de porta aberta no monitor de paciente remoto de verificação de integridade do software Cisco IOS XR. Um invasor remoto não autenticado poderia explorar a falha conectando-se à instância do Redis pela porta aberta e gravando no banco de dados da memória ou no sistema de arquivos do contêiner e extraíndo as informações do banco de dados.



Citrix



A [CVE-2019-19781](#) é uma vulnerabilidade de travessia de diretórios do produto Citrix Application Delivery Controller (ADC) and Gateway. Um invasor remoto não autenticado poderia explorar a vulnerabilidade ao enviar uma solicitação criada especialmente com uma sequência de caracteres de travessia de diretórios para o endpoint vulnerável da Citrix. O sucesso da exploração garantiria ao invasor a capacidade de executar um código arbitrário. Ela foi apresentada como uma das cinco principais vulnerabilidades na Retrospectiva do cenário de ameaças de 2020.



A [CVE-2022-27510](#) é uma vulnerabilidade de desvio de autenticação do Citrix ADC and Gateway; recebeu uma pontuação CVSSv3 de 9,8 e foi identificada como crítica. No seu boletim, a Citrix observou que essa vulnerabilidade afeta equipamentos que ativam a funcionalidade da rede privada virtual da camada de soquete seguro (SSL VPN) ou que são usados como um proxy de arquitetura de computação independente com autenticação. Vulnerabilidades de desvio de autenticação como esta podem ser exploradas pelo invasor como um vetor de acesso inicial a uma rede.



Citrix (continuação)>>

A [CVE-2022-27518](#) é uma vulnerabilidade de RCE que afeta o Citrix ADC ou o Citrix Gateway quando configurada como um provedor de serviços (SP) Security Assertion Markup Language (SAML) ou um provedor de identidade SAML (IdP). A vulnerabilidade é classificada como crítica e pode ser explorada por um invasor remoto não autenticado para execução de código arbitrário. A CVE-2022-27518 recebeu uma pontuação CVSSv3 de 9,8.



F5



A [CVE-2020-5902](#) é uma vulnerabilidade crítica de travessia de diretórios na interface do usuário de gerenciamento de tráfego (TMUI) da linha de produtos BIG-IP, que inclui uma série de soluções baseadas em software e hardware. Um invasor remoto não autenticado poderia enviar uma solicitação criada especialmente para um dispositivo BIG-IP vulnerável contendo uma sequência de caracteres de travessia de diretórios (por exemplo, “..;/”) para explorar a vulnerabilidade. O sucesso da exploração daria ao invasor a capacidade de executar comandos arbitrários do sistema, criar ou excluir arquivos ou desabilitar serviços no host vulnerável. Ela foi apresentada como uma das cinco principais vulnerabilidades na Retrospectiva do cenário de ameaças de 2020.



A [CVE-2022-1388](#) é uma vulnerabilidade de desvio de autenticação no componente REST da API iControl do BIG-IP que recebeu uma pontuação CVSSv3 de 9,8. A API REST iControl é usada para o gerenciamento e a configuração de dispositivos BIG-IP. A CVE-2022-1388 poderia ser explorada por um invasor não autenticado com acesso via rede à porta de gerenciamento ou aos endereços IP próprios de dispositivos que usam o BIG-IP. A exploração permitiria que o invasor executasse comandos arbitrários do sistema, criasse e excluisse arquivos e desabilitasse serviços.



Fortinet



A [CVE-2018-13379](#) é uma vulnerabilidade de divulgação de informações não autenticadas em SSL VPNs do FortiOS. Essa vulnerabilidade de leitura arbitrária de arquivos permite que invasores leiam o conteúdo de um arquivo de sessão que contém um nome de usuário e uma senha em texto simples. Isso é feito por meio do envio de uma solicitação especialmente criada para a SSL VPN vulnerável do FortiOS. Os invasores poderiam então utilizar essas informações para autenticar a SSL VPN.



A [CVE-2022-40684](#) é uma vulnerabilidade crítica de desvio de autenticação que recebeu uma pontuação CVSSv3 de 9,6. Ao enviar solicitações HTTP ou HTTPS especialmente criadas para um alvo vulnerável, um invasor remoto com acesso à interface de gerenciamento poderia executar operações de administrador.



Fortinet (continuação) >>

A [CVE-2022-42475](#) é um estouro de buffer baseado em heap em várias versões do FortiOS, que recebeu uma pontuação CVSSv3 de 9,3. Um invasor remoto e não autenticado poderia explorar essa vulnerabilidade com uma solicitação específica e obter execução de código.



Google

Google

A [CVE-2021-22600](#) e a [CVE-2021-39793](#) são vulnerabilidades de elevação de privilégios (EoP) no Google's Upstream Kernel for Android e receberam a pontuação de severidade "Moderada". De acordo com o Google, essas vulnerabilidades estão sob exploração limitada e direcionada.



A [CVE-2022-0609](#) é uma vulnerabilidade "use-after-free" no mecanismo de animação do Google Chrome. Ela foi relatada pelo grupo de análise de ameaças do Google e já foi explorada no mundo real.



A [CVE-2022-1096](#) é uma vulnerabilidade de confusão de tipos no mecanismo V8 do Google Chrome. Ela foi relatada anonimamente e já foi explorada no mundo real.



A [CVE-2022-1364](#) é uma vulnerabilidade de confusão de tipos no mecanismo V8 do Google Chrome. Ela foi relatada pelo grupo de análise de ameaças do Google e já foi explorada no mundo real.



A [CVE-2022-2294](#) é uma vulnerabilidade de estouro de buffer baseada em heap no componente Web Real-Time Communications (WebRTC) do Chromium.



A [CVE-2022-2856](#) é uma vulnerabilidade de validação de entrada imprópria no Google Chrome. Essa vulnerabilidade foi relatada pelo grupo de análise de ameaças do Google e já foi explorada no mundo real.



A [CVE-2022-3075](#) é uma vulnerabilidade de validação de dados insuficiente no sistema Mojo IPC do Google Chrome. A vulnerabilidade foi relatada por um pesquisador anônimo e sua exploração no mundo real foi confirmada.



Google (continuação) >>

A [CVE-2022-3723](#) é uma vulnerabilidade de confusão de tipos no mecanismo V8 do Google Chrome. Ela foi relatada por pesquisadores do Avast e já foi explorada no mundo real.



A [CVE-2022-4135](#) é uma vulnerabilidade de estouro de buffer de heap na GPU do Google Chrome. Ela foi relatada pelo grupo de análise de ameaças do Google e já foi explorada no mundo real.



A [CVE-2022-4262](#) é uma vulnerabilidade de confusão de tipos no mecanismo V8 do Google Chrome. Ela foi relatada pelo grupo de análise de ameaças do Google e já foi explorada no mundo real.



Magnitude Simba

A [CVE-2022-29972](#) é uma validação imprópria da vulnerabilidade do token de autenticação nos drivers Magnitude Simba Amazon Redshift ODBC e JDBC. Um invasor local e autenticado poderia explorar essa vulnerabilidade para executar comandos remotos.

Nome: SynLapse



Microsoft

A [CVE-2017-11882](#) é uma vulnerabilidade de corrupção de memória no componente Equation Editor do Microsoft Office que pode levar à RCE e recebeu uma pontuação CVSSv3 de 7,8. Ela foi explorada em ataques por diversos agentes de ameaças e está incorporada em alguns dos principais tipos de malware.



A [CVE-2018-0798](#) é uma vulnerabilidade de corrupção de memória no componente Equation Editor do Microsoft Office que pode levar à RCE e recebeu uma pontuação CVSSv3 de 8,8. A exploração pode permitir a execução arbitrária de código no contexto de um usuário que interagiu com um arquivo ou site específico criado.



A [CVE-2018-0802](#) é uma vulnerabilidade de corrupção de memória no componente Equation Editor do Microsoft Office que pode levar à RCE e recebeu uma pontuação CVSSv3 de 8,6. A exploração pode permitir a execução arbitrária de código no contexto de um usuário que interagiu com um arquivo ou site específico criado.



VULNERABILIDADE DE DIA ZERO



EXPLORADA



VULNERABILIDADE NOMEADA



VULNERABILIDADE ANTERIOR A 2022



NUVEM



RELEVANTE

Microsoft (continuação)>>

A [CVE-2020-0688](#), é uma vulnerabilidade de chave de validação decorrente da geração de chaves de criptografia estáticas que pode levar à RCE. A vulnerabilidade foi relatada à Iniciativa de vulnerabilidades de dia zero, e depois foi divulgada para a Microsoft. Logo após a vulnerabilidade ser divulgada em 2020, começaram a surgir relatos de que agentes de ameaças estavam utilizando a falha no mundo real.



A [CVE-2020-1472](#) é uma vulnerabilidade de EoP no Netlogon Remote Protocol da Microsoft. Esse protocolo é utilizado para manter relacionamentos de controladores de domínio (DC) dentro e entre domínios. O MS-NRPC também é usado essencialmente para gerenciar mudanças de conta para DCs, como senhas. Essa vulnerabilidade existe por causa de uma falha em como o MS-NRPC implementa a criptografia AES-CFB8. Por ser uma falha local de escalonamento de privilégio, o invasor precisa estar na mesma rede local que o alvo. O Active Directory é um alvo bem preocupante do Zerologon. Caso um invasor consiga explorá-lo no AD, seria possível imitar qualquer máquina na rede, redefinir a senha de administrador do controlador de domínio ou lançar ataques de ransomware contra toda a rede.

Nome: Zerologon



A [CVE-2021-26855](#) é uma vulnerabilidade de falsificação de solicitação do lado do servidor (SSRF) apelidada de ProxyLogon pela Orange Tsai, a pesquisadora creditada pela descoberta. Um invasor remoto não autenticado poderia explorar essa falha com o envio de uma solicitação HTTP específica para um servidor Exchange que aceite conexões não confiáveis na porta 443. Com o sucesso da exploração dessa falha, o invasor conseguaria autenticar o servidor Exchange visado. Ela foi apresentada como uma das cinco principais vulnerabilidades na Retrospectiva do cenário de ameaças de 2021.

Nome: ProxyLogon



A [CVE-2021-26857](#) é uma vulnerabilidade de desserialização não segura. Mais especificamente, a falha fica no Serviço de Unificação de Mensagens do Exchange, que habilita a funcionalidade de correio de voz, além de outros recursos. Para explorar essa falha, um invasor teria que estar autenticado no servidor vulnerável do Exchange Server com privilégios de administrador, possivelmente com a exploração de outra vulnerabilidade. Com o sucesso dessa exploração, o invasor teria privilégios de execução de código arbitrário como SYSTEM.



A [CVE-2021-26858](#) e a [CVE-2021-27065](#) são vulnerabilidades de gravação arbitrária de arquivos. Essas falhas são pós-autenticação, o que significa que um invasor precisaria autenticar o Exchange Server vulnerável primeiro, para depois poder explorá-lo. Isso poderia ser feito com a exploração da CVE-2021-26855 ou com a utilização de credenciais roubadas de administrador. Assim que estiver autenticado, o invasor poderá gravar arbitrariamente em qualquer caminho do servidor vulnerável.



A [CVE-2021-34473](#), uma vulnerabilidade de RCE, a [CVE-2021-34523](#), uma vulnerabilidade de EoP e a [CVE-2021-31207](#), um desvio de recurso, constituem a cadeia de vulnerabilidades chamada ProxyShell. Com o encadeamento dessas vulnerabilidades, um invasor poderia executar comandos arbitrários em servidores vulneráveis do Exchange na porta 443.

Nome: ProxyShell



Microsoft (continuação)>>

A [CVE-2021-36942](#) é uma vulnerabilidade de falsificação de autoridade de segurança local (LSA) do Windows que recebeu patches em agosto e esteve relacionada ao ataque de retransmissão do PetitPotam NTLM, divulgado por Gilles Lionel. A exploração poderia ser usada para forçar controladores de domínio a autenticar um destino controlado pelo invasor. Grupos de ransomware exploraram esse ataque cerca de um mês após a sua divulgação, e o patch para a CVE-2021-36942 apenas corrigiu o problema parcialmente. A Microsoft publicou orientações gerais para a mitigação do problema **contra ataques de retransmissão do NTLM**. O ransomware LockFile encadeou vulnerabilidades no Microsoft Exchange com a PetitPotam para tomar controle de controladores de domínio.

Nome: PetitPotam



A [CVE-2021-40444](#) é uma vulnerabilidade de RCE na plataforma MSHTML (Trident) da Microsoft, o mecanismo de navegador exclusivo da Microsoft. Para explorar essa vulnerabilidade, um invasor teria que criar um documento específico no Microsoft Office contendo um controle malicioso do ActiveX e usar técnicas de engenharia social para convencer um alvo a abrir o documento. O impacto dessa vulnerabilidade é mais significativo quando o alvo possui privilégios de administrador.



A [CVE-2022-21836](#) é uma vulnerabilidade de falsificação que afeta os certificados do Windows e recebeu uma pontuação CVSSv3 de 7,8. O invasor poderia utilizar certificados comprometidos para desviar da verificação binária da tabela binária da plataforma Windows. Embora a exploração seja classificada como menos provável, a Microsoft afirma que a falha foi divulgada publicamente. Os certificados comprometidos conhecidos pela Microsoft foram adicionados à lista de bloqueio do driver do kernel do Windows, e a Microsoft oferece orientações adicionais no seu comunicado de segurança.



A [CVE-2022-21839](#) é uma vulnerabilidade de consumo descontrolado de recursos na lista de controle de acesso discricionário de rastreamento de eventos do Windows. Um invasor local poderia explorar essa vulnerabilidade para causar uma condição DoS.



A [CVE-2022-21874](#) é uma RCE na API Windows Security Center que recebeu uma pontuação CVSSv3 de 7,8. Essa vulnerabilidade requer interação do usuário para ser explorada, e o vetor de ataque é local.



A [CVE-2022-21882](#) é uma vulnerabilidade de EoP no driver do sistema Win32k. Um invasor local e autenticado poderia explorar essa vulnerabilidade para elevar privilégios.



A [CVE-2022-21907](#) é uma vulnerabilidade de RCE no componente de serviços de informações da Internet nos seguintes sistemas operacionais da Microsoft: Windows 10, Windows Server 2022 e Windows Server 2019. A vulnerabilidade pode ser explorada com o envio de uma solicitação HTTP criada especialmente para um alvo vulnerável, gerando um DoS que pode ser encadeado com outras vulnerabilidades que levam à RCE.



Microsoft (continuação)>>

A [CVE-2022-21919](#) é uma vulnerabilidade de EoP no serviço de perfis de usuário do Windows. Para explorar essa vulnerabilidade, o invasor precisaria estabelecer uma posição no sistema vulnerável por meio de engenharia social, outra exploração ou um malware. O sucesso da exploração daria ao invasor privilégios elevados no sistema vulnerável.



A [CVE-2022-21971](#) é uma vulnerabilidade de RCE no tempo de execução do Windows. O invasor poderia explorar essa vulnerabilidade convencendo o alvo a abrir um arquivo de documento criado especialmente com código malicioso. O sucesso dessa exploração concederia ao invasor privilégios de execução de código arbitrário.



A [CVE-2022-21989](#) é uma vulnerabilidade de EoP no kernel do Windows. De acordo com a classificação do índice de explorabilidade da Microsoft, essa vulnerabilidade tem mais possibilidade de ser explorada. O comunicado observou que o invasor precisa executar ações adicionais antes de explorar essa vulnerabilidade, o que é evidente pela classificação "Alta" na "Complexidade do ataque" da pontuação CVSSv3 de 7,8.



A [CVE-2022-21990](#) é uma vulnerabilidade de RCE no cliente de desktop remoto da Microsoft. Para explorar a falha, o invasor precisaria convencer um usuário a se conectar a um servidor de desktop remoto controlado por ele.



A [CVE-2022-22047](#) é uma vulnerabilidade EoP no subsistema de tempo de execução do servidor cliente do Windows. É provável que esse tipo de vulnerabilidade tenha sido usado como parte da atividade pós-comprometimento, depois que o invasor obteve acesso ao sistema-alvo e executou uma aplicação específica.



A [CVE-2022-22713](#) é uma vulnerabilidade de DoS que afeta o Windows Hyper-V. De acordo com a descrição da Microsoft, para a vulnerabilidade ser explorada, o invasor precisa vencer uma condição de corrida, recebendo uma classificação de alta complexidade e uma pontuação CVSSv3 de 5,6. Ela foi divulgada publicamente antes de haver um patch disponível.



A [CVE-2022-24459](#) é uma vulnerabilidade de EoP que afeta o serviço de fax e digitalização do Windows. A vulnerabilidade tem uma pontuação CVSSv3 de 7,8 e pode ser explorada por um invasor local autenticado. Embora não houvesse tanta preocupação com a severidade e os requisitos de exploração, essa vulnerabilidade foi divulgada publicamente.



A [CVE-2022-24512](#) é uma vulnerabilidade de RCE no Microsoft .NET e no Visual Studio. De acordo com a Microsoft, a exploração dessa falha exige que "o usuário acione a carga útil na aplicação".



Microsoft (continuação)>>

A [CVE-2022-24521](#) é uma vulnerabilidade de EoP do driver do sistema de arquivos de log comuns do Windows. Um invasor que já tenha obtido acesso a um sistema vulnerável pode explorar essa vulnerabilidade executando uma aplicação específica. O sucesso da exploração daria ao invasor a capacidade de executar processos em um contexto elevado.



A [CVE-2022-26809](#) é uma vulnerabilidade de RCE crítica no tempo de execução da chamada de procedimento remoto (RPC). Um invasor remoto e não autenticado poderia explorar essa vulnerabilidade com o envio de uma chamada RPC específica para um host.



A [CVE-2022-26904](#) é uma vulnerabilidade de EoP no serviço de perfis de usuário do Windows. A complexidade do ataque a essa falha é considerada alta porque exige que o invasor vença uma condição de corrida. O sucesso da exploração permitiria que o invasor obtivesse acesso privilegiado a uma conta com menos privilégios.



A [CVE-2022-26923](#) é uma vulnerabilidade de EoP nos serviços de certificado do Microsoft Active Directory (AD CS). Um invasor com poucos privilégios em um sistema vulnerável com o AD CS em execução pode explorá-la executando um script específico. O sucesso da exploração permitiria que o invasor passasse de um usuário com poucos privilégios a um administrador de domínio.



A [CVE-2022-26925](#) é uma vulnerabilidade de falsificação no Windows LSA que já foi explorada no mundo real. Um invasor não autenticado pode forçar os controladores de domínio a autenticar um servidor controlador do invasor usando NTLM.



A [CVE-2022-30137](#) é uma vulnerabilidade de EoP no Microsoft Azure Service Fabric for Linux. Um invasor local e autenticado poderia explorar a vulnerabilidade para elevar privilégios e obter privilégios de raiz em um nó. O sucesso da exploração poderia talvez resultar no comprometimento de todos os nós de um cluster.

Nome: FabricScape



A [CVE-2022-30190](#) é uma vulnerabilidade de RCE no Microsoft Windows Support Diagnostic Tool (MSDT) que afeta várias versões do Microsoft Office, incluindo versões do Office 2019 e 2021 com patches aplicados. A vulnerabilidade existe devido à forma como o Microsoft Windows Support Diagnostic Tool (MSDT) é chamado usando o protocolo de URL de determinadas aplicações. Graças à maneira como essa vulnerabilidade é explorada, a Microsoft lista o vetor de ataque como "local", mas o invasor que utiliza essa falha provavelmente seria remoto.

Nome: Follina



Microsoft (continuação) >>

A [CVE-2022-30216](#) é uma vulnerabilidade de coerção de autenticação no Microsoft Windows Server decorrente de um erro "off-by-one" encontrado em um procedimento do retorno de chamada de segurança. De acordo com os pesquisadores, o invasor pode explorar essa vulnerabilidade combinando-a com um ataque de retransmissão do New Technology LAN Manager (NTLM) contra o AD CS.



A [CVE-2022-33675](#) é uma vulnerabilidade de EoP no Microsoft Azure Site Recovery Suite. A causa da vulnerabilidade são permissões incorretas em uma das pastas de instalação do software. O invasor pode utilizar essa vulnerabilidade sequestrando DLLs armazenadas nessa pasta, levando à execução de código mal-intencionado com privilégios SYSTEM.



A [CVE-2022-34713](#) é uma vulnerabilidade de RCE no MSDT. O invasor poderia explorar essa falha usando engenharia social para convencer um alvo a abrir um documento malicioso ou abrir um link que faz download de um arquivo malicioso. Ela foi divulgada pela primeira vez pelo pesquisador Imre Rad em janeiro de 2020. Após a descoberta da vulnerabilidade Follina (CVE-2022-30190), a Microsoft reavaliou a descoberta de Imre e corrigiu a falha.

Nome: DogWalk



A [CVE-2022-37969](#) é uma vulnerabilidade de EoP do driver do sistema de arquivos de log comuns do Windows. De acordo com a Microsoft, essa vulnerabilidade já foi explorada no mundo real e foi divulgada publicamente antes da disponibilização de um patch. Por ser uma vulnerabilidade pós-exploração, ela pode ser explorada depois que o invasor obtém acesso ao sistema-alvo vulnerável por outros meios, incluindo a exploração de outra vulnerabilidade ou via engenharia social.



A [CVE-2022-37981](#) é uma vulnerabilidade de DoS no serviço de log de eventos do Microsoft Windows. De acordo com a Microsoft, a disponibilidade está definida como baixa nessa falha pois, embora o desempenho possa ser interrompido e/ou reduzido, o comunicado do fornecedor observou que o invasor "não pode negar totalmente o serviço".

Nome: OverLog



A [CVE-2022-41033](#) é uma vulnerabilidade de EoP no serviço de sistema de eventos Windows COM+, que permite notificações de eventos do sistema para serviços de componentes COM+. Um invasor autenticado poderia explorar essa vulnerabilidade para elevar privilégios em um sistema vulnerável e obter privilégios SYSTEM.



A [CVE-2022-41040](#) é uma vulnerabilidade de SSRF no Microsoft Exchange Server. Um invasor autenticado poderia explorar essa vulnerabilidade utilizando credenciais roubadas em qualquer conta de usuário do Exchange Server.

Nome: ProxyNotShell



Microsoft (continuação)>>

A [CVE-2022-41043](#) é uma vulnerabilidade de divulgação de informações no Microsoft Office for Mac. A exploração dessa falha exige que o invasor obtenha acesso local ao host vulnerável. Ela foi divulgada publicamente antes de haver um patch disponível.



A [CVE-2022-41073](#) é uma vulnerabilidade de EoP que afeta o serviço de spooler de impressão do Windows. A vulnerabilidade tem uma pontuação CVSSv3 de 7,8 e a descoberta foi creditada ao Microsoft Threat Intelligence Center. Essa falha já foi explorada no mundo real, de acordo com a Microsoft, e pode permitir que um usuário com poucos privilégios obtenha privilégios de nível SYSTEM.



A [CVE-2022-41082](#) é uma vulnerabilidade de RCE. Um invasor autenticado poderia explorar essa vulnerabilidade utilizando credenciais roubadas em qualquer conta de usuário do Exchange Server. Ela pode ser encadeada com a CVE-2022-41040.

Nome: ProxyNotShell



A [CVE-2022-41091](#) é uma vulnerabilidade de desvio de recursos de segurança que afeta o Windows Mark of the Web (MoTW). O MoTW é um recurso de segurança usado para marcar arquivos baixados da Internet e impedir que eles executem certas ações. Os arquivos sinalizados com o MoTW seriam abertos no modo de exibição protegido no Microsoft Office. Um banner de aviso de segurança é exibido aos usuários, solicitando que confirmem se o documento é confiável ao selecionar "Habilitar conteúdo". Um agente mal-intencionado poderia criar um arquivo para desviar o MoTW, "resultando em uma perda limitada de integridade e disponibilidade dos recursos de segurança, como o modo de exibição protegido".



A [CVE-2022-41125](#) é uma vulnerabilidade de EoP no serviço de isolamento de chaves do Windows Cryptography Next Generation (CNG) usado para operações e suporte de criptografia do Windows. Com uma pontuação CVSSv3 de 7,8, o sucesso da exploração permitiria que o invasor obtivesse privilégios SYSTEM.



A [CVE-2022-41128](#) é uma vulnerabilidade crítica que afeta a linguagem de script JScript9 nos sistemas operacionais Windows e pode ser usada para lançar malware em um alvo direcionando o usuário para um site malicioso que explora o ponto fraco.



A [CVE-2022-44698](#) é uma vulnerabilidade de desvio de recursos de segurança no sistema operacional Windows. Essa vulnerabilidade do MoTW impede que downloads especialmente criados sejam marcados como originários da web, o que afeta a integridade e a disponibilidade dos recursos de segurança que utilizam a marcação MoTW. O sucesso da exploração impede que o SmartScreen faça uma verificação de reputação no arquivo baixado, o que pode fazer com que um arquivo executável malicioso conhecido não alerte os usuários de que o arquivo pode ser malicioso.



Microsoft (continuação)>>

SEM-ID-CVE: uma vulnerabilidade crítica entre contas foi descoberta no serviço de automação do Azure. Essa vulnerabilidade não recebeu um identificador de CVE. Um usuário não autorizado poderia enviar uma solicitação criada especialmente para um endpoint de identidade especial e obter tokens pertencentes a outros usuários/organizações.

Nome: AutoWarp



SEM-ID-CVE: uma vulnerabilidade de desvio de autenticação entre contas por meio de um certificado forjado foi descoberta no mecanismo PostgreSQL do Microsoft Azure. Quando encadeada com uma vulnerabilidade de escalonamento de privilégios, o invasor pode obter acesso não autorizado para ler os bancos de dados PostgreSQL de outros clientes.

Nome: #ExtraReplica



SEM-ID-CVE: uma vulnerabilidade de escalonamento de privilégios foi descoberta no mecanismo PostgreSQL do Microsoft Azure. Quando encadeada com uma vulnerabilidade de desvio de autenticação entre contas, o invasor pode obter acesso não autorizado para ler os bancos de dados PostgreSQL de outros clientes.

Nome: #ExtraReplica



Mitel



A [CVE-2022-29499](#) é uma vulnerabilidade de validação de entrada imprópria no MiVoice Connect, um componente do Mitel Service Appliance. Um invasor remoto não autenticado poderia explorar essa vulnerabilidade para obter privilégios de RCE no contexto do Service Appliance.



Mozilla



A [CVE-2022-26485](#) é uma vulnerabilidade "use-after-free" no Mozilla Firefox na forma como os parâmetros são processados por meio de Extensible Stylesheet Language Transformations (XSLT). Na remoção de um parâmetro XSLT durante o processamento, o resultado é um "use-after-free" que pode ser explorado. O Mozilla diz ter recebido relatos de que essa falha já foi explorada no mundo real.



A [CVE-2022-26486](#) é uma vulnerabilidade "use-after-free" na estrutura WebGPU IPC do Mozilla Firefox. "Use-after-free" e escape de área restrita são possíveis quando a estrutura recebe uma mensagem inesperada. O Mozilla diz ter recebido relatos de que essa falha já foi explorada no mundo real.





Nooie

SEM-ID-CVE: as babás eletrônicas Nooie contêm várias vulnerabilidades, incluindo o vazamento de informações de transporte de telemetria da fila de mensagens não autenticadas, uma vulnerabilidade de acesso não autorizado no protocolo de transmissão em tempo real e a falta de uma política de controle de acesso para um bucket da AWS. Essas três vulnerabilidades não receberam um identificador CVE, mas permitem que o invasor externo acesse a câmera da babá eletrônica ou cause mais comprometimentos no dispositivo vulnerável por meio da execução de código malicioso.



A [CVE-2022-24295](#) é uma vulnerabilidade de injeção de comando no Okta Advanced Server Access Client for Windows. O sucesso da exploração dessa vulnerabilidade poderia conceder privilégios de RCE ao invasor.



Okta



Argo CD

A [CVE-2022-24348](#) é uma vulnerabilidade de travessia de caminho no Argo CD. Para explorar essa falha, um invasor com permissões para criar ou atualizar aplicações que podem adivinhar ou conhecer o caminho completo para um arquivo que contenha um YAML válido poderia criar um gráfico Helm malicioso para consumir YAML como arquivos de valor.



CRI-O

A [CVE-2022-0811](#) é uma vulnerabilidade no tempo de execução do contêiner CRI-O v1.19. Para que essa vulnerabilidade seja explorada, o invasor precisa ter direitos para implementar um pod em um cluster do Kubernetes. Quando explorada, ela permite a fuga do contêiner e a obtenção de acesso raiz no host, permitindo que o invasor se movimente livremente no cluster.

Nome: cr8escape



Horde Webmail

SEM-ID-CVE: o Horde Webmail contém uma vulnerabilidade de script entre sites (XSS) armazenada que não recebeu um identificador CVE. Para explorar essa falha, o invasor pode enviar um e-mail criado especialmente para um usuário usando uma versão vulnerável do Horde Webmail. Mesmo se o usuário apenas pré-visualizar o e-mail, a exploração será acionada.





Kernel do Linux

A [CVE-2021-3995](#) é uma falha na biblioteca libmount do util-linux. Quando utilizada, essa falha pode permitir a desmontagem de certos sistemas de arquivos FUSE por invasores locais sem privilégios. Os sistemas de arquivos-alvo precisam pertencer a outros usuários cujo UID seja um prefixo do UID do invasor na forma de string. A exploração dessa falha pode causar DoS em aplicações que usam esses sistemas de arquivos.



A [CVE-2021-3996](#) é uma falha na biblioteca libmount do util-linux. Quando utilizada, essa falha pode permitir a desmontagem de certos sistemas de arquivos FUSE por invasores locais sem privilégios. Os sistemas de arquivos-alvo precisam ser "word-writable" ou estar em um diretório "word-writable". A exploração dessa falha pode causar DoS em aplicações que usam esses sistemas de arquivos.



A [CVE-2021-3997](#) é uma falha de recursão incontrolável em systemd-tmpfiles. A falha pode causar um DoS quando muitos diretórios são criados em /tmp no momento da inicialização.



A [CVE-2021-3998](#) é uma falha na função realpath() do glibc que pode causar vazamento de informações ou divulgação de dados confidenciais.



A [CVE-2021-3999](#) é uma vulnerabilidade de estouro e estouro negativo de buffer "off-by-one" no glibc. Se o tamanho do buffer for 1, um invasor local poderá utilizar a vulnerabilidade para executar código arbitrário ou elevar seus privilégios.



A [CVE-2022-0185](#) é um estouro de buffer baseado em heap encontrado na funcionalidade Filesystem Context do kernel do Linux. Quando explorada, essa vulnerabilidade pode fazer com que um usuário sem privilégios escale seus privilégios.



A [CVE-2022-0492](#) é uma vulnerabilidade de autenticação imprópria no kernel do Linux que requer uma configuração específica para facilitar a exploração, podendo permitir que o invasor escape de um contêiner e aumente os privilégios.



A [CVE-2022-0847](#) é uma vulnerabilidade de inicialização imprópria no kernel do Linux. A falha está no novo pipe_buffer, que pode levar à preservação indevida de permissões.

Nome: DirtyPipe



A [CVE-2022-29799](#) é uma vulnerabilidade de travessia de diretórios encontrada na unidade networkd-dispatcher do kernel do Linux. A causa da vulnerabilidade é a falta de sanitização da função pelo networkd-dispatcher de OperationalState e AdministritiveState, levando ao escape do diretório "/etc/networkd-dispatcher".

Nome: NimbusPwn



VULNERABILIDADE NOMEADA



NUVEM



Open Source/Kernel do Linux (continuação)>>

A [CVE-2022-29800](#) é uma vulnerabilidade de condição de corrida "time-of-check-time-of-use" na unidade networkd-dispatcher do kernel do Linux. A vulnerabilidade pode ser explorada ao substituir os scripts usados pela unidade entre o momento em que são descobertos e o momento em que são executados, fazendo com que o networkd-dispatcher acredite que os scripts controlados pelo invasor pertencem à raiz.

Nome: Nimbuspwn



OpenSSL

OpenSSL

Cryptography and SSL/TLS Toolkit

A [CVE-2022-3602](#) é uma vulnerabilidade de estouro de buffer no OpenSSL causada por uma função que verifica certificados x.509. Pré-anunciada como uma vulnerabilidade crítica, essa classificação foi posteriormente rebaixada para "alta" depois que foi determinada a baixa probabilidade de RCE. Porém, a RCE ainda é possível quando explorada em ambientes incomuns.



A [CVE-2022-3786](#) é uma vulnerabilidade de estouro de buffer no OpenSSL causada por uma função que verifica certificados x.509. Como o invasor não consegue controlar dados transbordados, mas apenas o comprimento dos dados passados para a função, é improvável que essa vulnerabilidade cause RCE se explorada.



PrestaShop



PrestaShop

A [CVE-2022-31181](#) é uma vulnerabilidade de injeção de SQL no PrestaShop CMS. De acordo com os desenvolvedores, ela é usada como parte de uma "cadeia de vulnerabilidades antes desconhecida" para obter RCE nas instalações da PrestaShop.



Redis



A [CVE-2022-0543](#) é uma vulnerabilidade no Redis em distribuições específicas do Debian (Debian, Ubuntu) do Linux que usam o mecanismo Lua. O invasor pode explorar essa vulnerabilidade para escapar da área de segurança Lua e obter RCE.



WSO2



A [CVE-2022-29464](#) é uma vulnerabilidade arbitrária irrestrita de upload de arquivos em vários produtos WSO2. Um invasor remoto não autenticado poderia explorar a vulnerabilidade carregando um arquivo Jakarta Server Pages especialmente criado para um servidor vulnerável.



SQLite



A [CVE-2022-35737](#) é uma validação imprópria da vulnerabilidade do índice de matriz no SQLite. A vulnerabilidade afeta as aplicações que usam a API Library do SQLite. Ela pode ser explorada ao passar entradas de string longas (2 GB, por exemplo) para uma aplicação ou programa usando uma versão vulnerável do SQLite que usa funções printf.





Oracle

A [CVE-2020-14882](#) é uma falha de RCE não autenticada no componente de console do Oracle WebLogic Server. A Oracle descreveu a falha como facilmente explorável e atribuiu a ela uma pontuação CVSSv3 de 9,8. O sucesso da exploração permitiria que um invasor não autenticado comprometesse o servidor Oracle WebLogic por HTTP e assumisse o controle total do host.



A [CVE-2022-21500](#) é uma vulnerabilidade no Oracle E-Business Suite 12.2 que permite que um invasor não autenticado com acesso à rede acesse dados críticos. É necessária autenticação para o sucesso do ataque; porém, o usuário pode ser autor registrado.



Palo Alto Networks



A [CVE-2022-0028](#) é uma vulnerabilidade de DoS de amplificação refletida na política de filtragem de URL do PAN-OS da Palo Alto Networks em decorrência de uma configuração incorreta. O invasor pode explorar essa falha para executar um ataque de DoS que ofuscaria a origem do ataque, fazendo parecer que ele se originou de um dispositivo da Palo Alto Networks, como o PA-Series (hardware), o VM-Series (virtual) ou o firewall CN-Series (contêiner).



Plug-in do WordPress



A [CVE-2022-3180](#) é uma vulnerabilidade de escalonamento de privilégios não autenticado no plug-in premium do WordPress chamado WPGateway. Um invasor não autenticado poderia explorar essa vulnerabilidade para inserir um administrador mal-intencionado em um site vulnerável do WordPress, permitindo que ele assumisse o controle do site.



PolKit



A [CVE-2021-4034](#) é uma vulnerabilidade de EoP no pkexec do PolKit, uma ferramenta de linha de comando incluída por padrão na maioria das distribuições do Linux. O sucesso da exploração daria privilégios de raiz a um invasor local sem privilégios no sistema vulnerável.

Nome: PwnKit



A [CVE-2022-25246](#) é uma vulnerabilidade de credenciais codificadas na instalação UltraVNC dos produtos Axeda. Os produtos afetados são o Axeda Agent e o Axeda Desktop Server for Windows. Se explorada, essa vulnerabilidade pode causar RCE na máquina-alvo.

Nome: Access:7



[PTC \(continuação\)>>](#)

A [CVE-2022-25247](#) é uma vulnerabilidade de RCE encontrada no Axeda Agent e no Axeda Desktop Server for Windows. Se utilizada, o invasor consegue enviar determinados comandos para uma porta específica sem autenticação. Isso pode resultar em acesso completo ao sistema de arquivos e em RCE.

Nome: Access:7



A [CVE-2022-25248](#) é uma vulnerabilidade de divulgação de informações no serviço ERemoteServer.exe dos produtos Axeda Agent e Axeda Desktop Server for Windows. Quando um invasor se conecta a uma porta específica de um alvo que executa esses produtos, os produtos retornam o log de eventos do serviço específico associado a essa porta.

Nome: Access:7



A [CVE-2022-25249](#) é uma vulnerabilidade de travessia de diretórios no Axeda Agent e no Axeda Desktop Server for Windows. A vulnerabilidade concede a um invasor remoto e não autenticado acesso de leitura no sistema de arquivos do alvo via servidor Web.

Nome: Access:7



A [CVE-2022-25250](#) é uma vulnerabilidade de falta de autenticação para função crítica nos produtos Axeda Agent e Axeda Desktop Server for Windows. O invasor pode utilizar essa vulnerabilidade para desligar remotamente um serviço específico no alvo.

Nome: Access:7



A [CVE-2022-25251](#) é uma vulnerabilidade de falta de autenticação nos produtos Axeda Agent e Axeda Desktop Server for Windows. Essa vulnerabilidade pode permitir que o invasor envie mensagens XML a uma porta específica sem a devida autenticação e accesse e edite a configuração do programa.

Nome: Access:7



A [CVE-2022-25252](#) é uma verificação imprópria de vulnerabilidades de condições incomuns ou excepcionais nos produtos Axeda Agent e Axeda Desktop Server for Windows. Essa vulnerabilidade pode ser utilizada por um invasor não autenticado para travar o programa.

Nome: Access:7



Pulse Secure

A [CVE-2019-11510](#) é uma vulnerabilidade de divulgação arbitrária de arquivos não autenticados no Pulse Connect Secure SSL VPN, conhecido anteriormente como Juniper SSL VPN. Ela recebeu uma pontuação CVSSv3 de 10,0. Foi apresentada como uma das cinco principais vulnerabilidades na Retrospectiva do cenário de ameaças de 2020 e foi explorada por vários grupos de APT e estado-nação.



RARLAB

A [CVE-2022-30333](#) é uma vulnerabilidade de travessia de diretórios na ferramenta de extração de arquivos conhecida como UnRAR da RARLAB. O invasor pode explorar essa vulnerabilidade em instâncias vulneráveis do Zimbra Collaboration Suite ao enviar para um alvo vulnerável um e-mail específico com um anexo RAR malicioso. Não há necessidade de interação do usuário para que essa falha seja explorada, pois o Zimbra extrai o arquivo RAR malicioso, que seria processado pela biblioteca UnRAR subjacente.



SAP

A [CVE-2022-22532](#) é uma vulnerabilidade de contrabando de solicitação HTTP no SAP Internet Communication Manager (ICM). A exploração não requer autenticação ou interação do usuário. Em cenários mais complexos, o invasor poderia utilizar essa falha para RCE.

Nome: ICMAD



A [CVE-2022-22533](#) é um vazamento de memória no gerenciamento de canal de memória do SAP ICM que pode resultar em DoS. O invasor pode explorar essa falha usando solicitações HTTP(S) criadas especialmente para consumir todos os recursos MPI.

Nome: ICMAD



A [CVE-2022-22536](#) é uma vulnerabilidade de dessincronização do canal de memória no SAP ICM. Um invasor remoto não autenticado poderia explorar a vulnerabilidade usando uma solicitação HTTP simples e obter controle completo do sistema.

Nome: ICMAD



SolarWinds



A [CVE-2021-35247](#) é uma vulnerabilidade de validação de entrada imprópria na tela de login Web do Serv-U. Ela foi explorada por invasores em janeiro de 2022 para propagar ataques usando as vulnerabilidades Log4j.



SonicWall



A [CVE-2021-20038](#) é uma vulnerabilidade de estouro de buffer não autenticado baseado em pilha nas variáveis de ambiente do módulo mod_cgi do servidor SMA100 Apache httpd, que pode resultar em RCE como um usuário "ninguém" no equipamento.



A [CVE-2022-22274](#) é uma vulnerabilidade de estouro de buffer baseado em pilha no SonicOS. Um invasor remoto não autenticado pode explorar essa falha para acionar um DoS e talvez obter a execução de código em produtos como firewalls da SonicWall.



Sophos



A [CVE-2022-1040](#) é uma vulnerabilidade de desvio de autenticação no User Portal e no Webadmin do Sophos Firewall. O sucesso da exploração resultaria em RCE. A Sophos relatou que essa vulnerabilidade já foi explorada no mundo real.



A [CVE-2022-3236](#) é uma vulnerabilidade de injeção de código no User Portal e no Webadmin do Sophos Firewall. Um invasor não autenticado poderia explorar esta vulnerabilidade enviando solicitações criadas especialmente para o User Portal ou o Webadmin do Sophos Firewall que pode ser acessado externamente. O sucesso da exploração permitiria RCE.



Trend Micro



A [CVE-2022-26871](#) é uma vulnerabilidade arbitrária de upload de arquivos no Trend Micro Apex Central (no local e como serviço). O sucesso da exploração poderia conceder RCE ao invasor.



A [CVE-2022-40139](#) é uma vulnerabilidade de validação imprópria na funcionalidade de "reversão" que é usada para reverter agentes Apex One para versões mais antigas. A vulnerabilidade existe porque os agentes Apex One são capazes de fazer download de componentes não verificados, podendo resultar em execução de código. Embora essa vulnerabilidade só possa ser explorada por um invasor que tenha acesso ao console administrativo do Apex One, há relatos de exploração ativa.



VMWare



A [CVE-2021-39144](#) é uma vulnerabilidade de RCE no XStream, uma biblioteca de código aberto usada para a serialização de objetos. Originalmente, essa vulnerabilidade recebeu patches na versão 1.1.18 do XStream em 22 de agosto de 2021. O VMware Cloud Foundation usa o XStream para serialização de entrada na solução Network Security Virtualization for vSphere (NSX-V). O invasor pode explorar essa vulnerabilidade mirando um endpoint não autenticado no NSX-V para obter privilégios de RCE como raiz.



A [CVE-2022-22948](#) é uma vulnerabilidade de divulgação local de informações no vCenter Server. Um invasor local autenticado com acesso de usuário com poucos privilégios a um vCenter Server vulnerável poderia explorar essa falha para obter informações confidenciais. É provável que essa vulnerabilidade seja pareada com outros bugs do VMware vCenter Server como parte de uma cadeia de ataque.



A [CVE-2022-22954](#) é uma vulnerabilidade de injeção de modelo do lado do servidor no VMware Workspace ONE Access e no Identity Manager. Um invasor não autenticado com acesso à rede poderia explorar essa vulnerabilidade com o envio de uma solicitação específica para um VMware Workspace ONE ou Identity Manager vulnerável.



A [CVE-2022-22955](#) e a [CVE-2022-22956](#) são vulnerabilidades de desvio de autenticação na estrutura OAuth 2.0 Access Control Services (ACS) do VMware Workspace ONE. Um invasor não autenticado pode enviar solicitações criadas especialmente para endpoints OAuth2.0 vulneráveis e expostos no VMware Workspace ONE para autenticação bem-sucedida na instância do Workspace ONE.



A [CVE-2022-22957](#) e a [CVE-2022-22958](#) são vulnerabilidades de RCE autenticada no VMware Workspace ONE Access, no Identity Manager e no vRealize Automation. Um invasor com acesso administrativo pode explorar essas falhas acionando a desserialização de dados não confiáveis através de um URI JDBC malicioso.



VMware (continuação)>>

A [CVE-2022-22963](#) é uma vulnerabilidade de RCE na funcionalidade de roteamento Spring Cloud Function. O invasor pode explorar essa falha com uma solicitação HTTP específica usando a linguagem de expressão Spring.



A [CVE-2022-22965](#) é uma vulnerabilidade de RCE no Spring Framework. É um desvio do patch da CVE-2010-1622. Esta vulnerabilidade tem vários pré-requisitos para exploração, inclusive que as aplicações devem executar o Java Development Kit versão 9 ou superior e usar o Apache Tomcat como o contêiner Servlet.

Nome: Spring4Shell



A [CVE-2022-22972](#) e a [CVE-2022-31656](#) são vulnerabilidades de desvio de autenticação no VMware Workspace ONE Access, no Identity Manager e no vRealize Automation que afetam usuários de domínios locais. Para explorar essa vulnerabilidade, um invasor remoto capaz de acessar a respectiva interface de usuário pode desviar a autenticação desses diferentes produtos.



A [CVE-2022-22973](#) é uma vulnerabilidade de escalonamento de privilégios local no VMware Workspace ONE Access e no Identity Manager. Para explorar essa vulnerabilidade, o invasor precisa ter acesso local às instâncias vulneráveis do Workspace ONE Access e do Identity Manager. O sucesso da exploração permitiria que o invasor obtivesse privilégios "raiz".



WatchGuard



A [CVE-2022-23176](#) é uma vulnerabilidade de escalonamento de privilégios no WatchGuard Firebox e em equipamentos XTM. Quando explorada, essa vulnerabilidade pode permitir acesso a um invasor remoto autenticado, mas sem privilégios, com uma sessão de gerenciamento privilegiada através de acesso de gerenciamento exposto. De acordo com a CISA, essa vulnerabilidade foi explorada pelo agente de ameaças russo Sandworm.



Zimbra



A [CVE-2022-24682](#) é uma vulnerabilidade XSS no recurso de calendário do Zimbra no Zimbra Collaboration Suite. O invasor pode explorar essa vulnerabilidade colocando um HTML JavaScript criado especialmente com código executável dentro dos atributos do elemento. Esse código seria injetado no documento depois de ser contido.



VULNERABILIDADE NOMEADA



VULNERABILIDADE ANTERIOR A 2022



NUVEM



RELEVANTE

A [CVE-2022-27924](#) é uma vulnerabilidade de injeção de cache de memória no Zimbra Collaboration Suite. Um invasor não autenticado poderia roubar credenciais de login envenenando as entradas de cache da rota IMAP de uma instância vulnerável do Zimbra Collaboration para obter acesso não autorizado ao servidor de e-mails de uma empresa.



A [CVE-2022-27925](#) é uma vulnerabilidade de desvio de autenticação no Zimbra Collaboration MailboxImport Servlet. Um invasor autenticado com permissões administrativas poderia explorar a falha fazendo upload de arquivos no sistema vulnerável. Pesquisadores descobriram que essa falha estava sendo utilizada como parte de uma cadeia de vulnerabilidades com a CVE-2022-37042, um desvio de patch da CVE-2022-27925. A combinação das duas falhas poderia permitir que o invasor explorasse essa falha como um invasor não autenticado, resultando em RCE.



A [CVE-2022-37042](#) é uma vulnerabilidade de desvio de autenticação no Zimbra MailboxImportServlet. O invasor pode explorar essa vulnerabilidade fazendo upload de arquivos arbitrários no sistema, que seriam extraídos por meio da funcionalidade mboximport. O sucesso da exploração resultaria em travessia de caminho e RCE.



A [CVE-2022-41352](#) é uma vulnerabilidade de RCE não corrigida no Zimbra Collaboration Suite, descoberta no mundo real graças à exploração ativa. A vulnerabilidade deve-se ao método (cpio) no qual o mecanismo antivírus do Zimbra (Amavis) verifica os e-mails recebidos. Essa vulnerabilidade CVE-2022-41352 é efetivamente idêntica à CVE-2022-30333, mas utiliza um formato de arquivo diferente. É também subproduto de uma vulnerabilidade (não corrigida) muito mais antiga, a CVE-2015-1197.



Zoho



A [CVE-2021-40539](#) é uma vulnerabilidade de desvio de autenticação na REST API no ManageEngine ADSelfService Plus. Um invasor remoto e não autenticado poderia explorar essa vulnerabilidade com o envio de uma solicitação específica para um host vulnerável. O sucesso da exploração concederia RCE ao invasor. A CVE-2021-40539 foi explorada para implementar webshells e estabelecer persistência nos ambientes-alvo.



A [CVE-2021-44077](#) é uma vulnerabilidade de RCE não autenticada no ManageEngine ServiceDesk Plus causada por uma configuração incorreta de segurança. Ela afeta implementações no local até a versão 11306.



A [CVE-2022-35405](#) é uma vulnerabilidade de RCE não autenticada no Zoho ManageEngine Password Manager Pro e PAM360. O Zoho ManageEngine Access Manager Plus também é afetado, mas o invasor precisa ser autenticado.





Zoom

A [CVE-2022-28751](#) é uma vulnerabilidade de escalonamento de privilégios local no Zoom Client para reuniões no macOS. A vulnerabilidade está presente em um problema no processo de atualização devido a um problema de validação de assinatura de pacote. Um invasor local autenticado com poucos privilégios pode explorar a vulnerabilidade para obter privilégios de raiz.



A [CVE-2022-28756](#) é uma vulnerabilidade de escalonamento de privilégios local no Zoom Client para reuniões no macOS. A vulnerabilidade está presente no processo de atualização automática do Zoom Client. Um invasor local autenticado com poucos privilégios pode explorar a vulnerabilidade para obter privilégios de raiz. A correção dessa vulnerabilidade aborda a CVE-2022-28751.



A [CVE-2022-28762](#) é uma porta de depuração mal configurada nas aplicações Zoom no Zoom Client para reuniões no macOS. Um invasor local pode explorar essa vulnerabilidade conectando-se à porta de depuração e controlando as aplicações Zoom em execução no Zoom Client.





6100 Merriweather Drive

12th Floor

Columbia, MD 21044

América do Norte: +1(410) 872-0555

América Latina: +1(443) 545-2278

pt-br.tenable.com