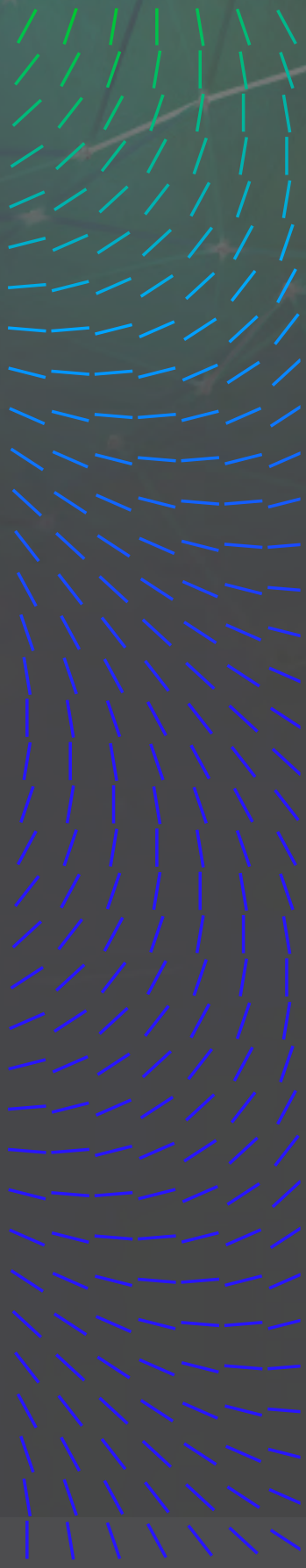
Apresentado por

Trellix ADVANCED RESEARCH CENTER

RELATÓRIO SOBRE AMEAÇAS

Fevereiro de 2023

SUMÁRIO



VISÃO GERAL DAS AMEAÇAS NO 4° TRIMESTRE DE 2022

Os perpetradores de ameaças continuaram sendo adversários formidáveis nos últimos meses de 2022 e o Trellix Advanced Research Center respondeu a isso acrescentando ainda mais recursos de inteligência sobre ameaças à nossa equipe de centenas de analistas e pesquisadores de segurança de elite.

"Em outras palavras: levamos nossa inteligência sobre ameaças a um novo patamar. Para trazer tranquilidade ao caos das suas operações de segurança, com uma segurança mais simples. Para melhorar os resultados da sua segurança com menos estresse. As ameaças continuam evoluindo. E você também pode evoluir."

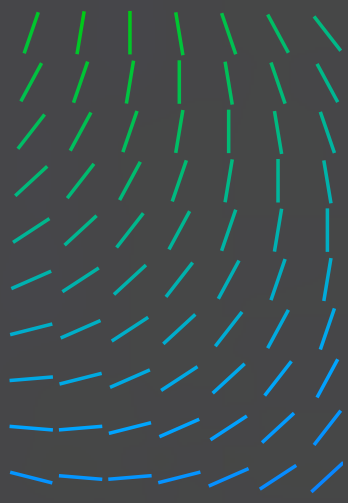
Neste relatório nós compartilhamos nossa seleção líder do setor de quais perpetradores de ameaças, famílias, campanhas e técnicas favoritas predominaram durante o trimestre passado. E mais. Também expandimos nossas fontes para extrair dados de sites de vazamentos de ransomware e relatórios do setor de segurança. E conforme os recursos da Trellix crescem, o mesmo acontece com as categorias de pesquisa de ameaças, inclusive conteúdos novos sobre segurança de rede, incidentes de nuvem, incidentes de endpoint e operações de segurança.

Desde nosso último relatório sobre ameaças, o Trellix Advanced Research Center esteve envolvido em pesquisas e descobertas no mundo todo, inclusive o link de Gamaredon, os ataques cibernéticos em intensidade muito maior contra a Ucrânia no 4° trimestre, a correção de 61.000 projetos de código aberto vulneráveis e a divulgação de insights sobre as novidades em ataques do ano novo com suas Previsões sobre ameaças em 2023.

A visão geral a seguir obtida desses aperfeiçoamentos do relatório sobre ameaças é um exemplo de como o Trellix Advanced Research Center trabalha para que clientes e o setor de segurança consigam produzir resultados melhores contra as ameaças:

Ransomware

- Pesquisa reveladora sobre a importância do LockBit 3.0 como grupo de ransomware mais impactante do quarto trimestre



- O predomínio continuado do ransomware em todo o mundo, especialmente nos Estados Unidos
- Setores visados pelo ransomware, inclusive os de serviços e bens industriais

Estados-nações

- Estados-nações visando setores, como governamental e de transportes e logística
- Empresas sediadas nos Estados Unidos e afetadas pela atividade de estados-nações

Aproveitamento da funcionalidade existente (LOLBIN)

- Insights mais detalhados sobre o Cobalt Strike à solta, graças à metodologia de caça do Trellix Advanced Research Center
- O grande número de servidores Cobalt Strike Team hospedados em provedores de nuvem chineses
- Shell de comandos do Windows representando quase metade dos 10 binários de sistema operacional mais utilizados nas campanhas referidas

Perpetradores de ameaças

- China, Coreia do Norte e Rússia no topo da lista de países com mais perpetradores de ameaças

Tendências da segurança de e-mail

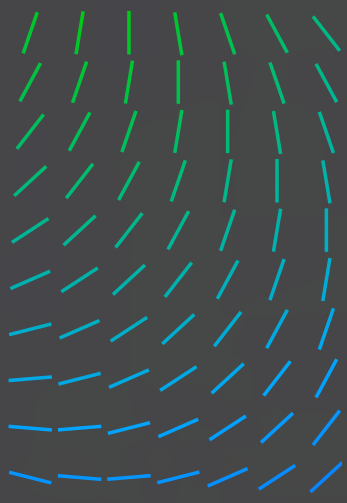
- O volume consideravelmente maior de e-mails maliciosos em países árabes observados durante a copa do mundo de futebol
- Insights sobre campanhas de phishing e vishing, inclusive técnicas de impostura, e temas de empresas conhecidas utilizados por vishing

Segurança de rede

- Os ataques, WebShells, ferramentas e técnicas mais impactantes, significativos e relevantes do trimestre

Telemetria de operações de segurança fornecida pela Trellix XDR

- Alertas de segurança, explorações, fontes de logs e técnicas MITRE ATT&CK predominantes
- Incidentes de nuvem
- Técnicas e detecções para Azure, AWS e GCP
- Principais técnicas e detecções



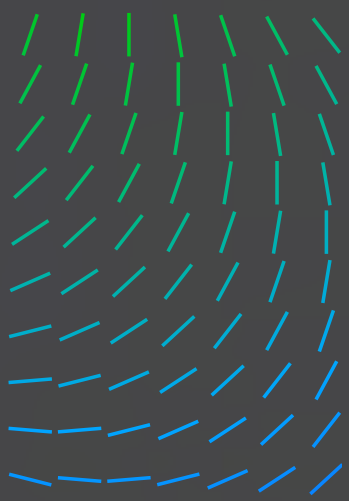
CARTA DO NOSSO CHEFE DE INTELIGÊNCIA SOBRE AMEAÇAS

Nossa equipe do Advanced Research Center está entusiasmada por compartilhar os dados preliminares do Relatório sobre ameaças do quarto trimestre de 2022, encerrando o ano. Você verá que o relatório continua evoluindo, com a inclusão de novos dados de nossa matriz de sensores de produtos, juntamente com insights de outras fontes de dados, como sites de vazamentos de ransomware e nosso rastreamento de infraestruturas na Internet. Na Trellix, continuamos determinados em nossa missão de proteger nossos clientes contra o mal porque os perpetradores de ameaças e suas motivações nunca dão trégua e se tornam mais multifacetados. A necessidade de inteligência global sobre ameaças cresce enquanto as perspectivas geopolíticas e econômicas continuam complicadas, com um nível de incerteza maior.

Em escala global, a incerteza econômica criada pela guerra na Ucrânia provocou um choque de preços de energia que não se via desde os anos 70 e que está afetando duramente a economia mundial. A volta da guerra à Europa também serviu como alerta para aqueles que questionavam a abordagem de segurança e defesa da União Europeia e sua capacidade de defender seus interesses, particularmente no espaço cibernético. A administração dos EUA também reconheceu a necessidade de lidar com questões de competição geoestratégica, proteger infraestruturas críticas e combater a interferência e a manipulação de informações por estrangeiros. SolarWinds, Hafnium, Ukraine e outros eventos deram azo a ações bipartidárias da administração e do congresso em relação a financiamento e novos padrões de segurança baseados significativamente nos compromissos e no trabalho de governos anteriores dos EUA. Então, como essa incerteza está afetando a segurança cibernética de nossas empresas, nossas instituições públicas e privadas e nossos valores democráticos?

No trimestre passado, nossa equipe viu o uso ativo do espaço cibernético nas áreas de espionagem, guerra e desinformação por governos de países, a serviço de ambições políticas, econômicas e territoriais. A guerra na Ucrânia também provocou o surgimento de novas formas de ataques cibernéticos e os hacktivistas ficaram mais experientes e mais determinados a adulterar sites, vazar informações e executar ataques de DDoS. Enquanto isso, as formas tradicionais de ataque cibernético continuam. Golpes de engenharia social para enganar e induzir pessoas a divulgar informações confidenciais ou pessoais, como é o caso do phishing, continuam comuns.

O ransomware continuou a afligir muitas organizações no mundo todo. Tal como observamos durante a pandemia de COVID-19, os criminosos cibernéticos foram rápidos em se aproveitar de um momento de crise e incerteza. Conforme o cenário de ameaças evolui, o mesmo acontece



com nossa pesquisa. Nossa missão é manter o foco em sempre aprimorar a eficácia de nossos produtos e oferecer inteligência decisiva às partes interessadas para assegurar que possam proteger o que mais importa. Neste relatório você verá o quão importante é o trabalho que fazemos para cada membro do Trellix Advanced Research Center. Não há um pesquisador ou especialista em nossa equipe que não aborde com empenho e dedicação cada um dos projetos que realizamos.

Diga-nos o que você acha deste relatório estendido e, se houver alguma área na qual você ache que nossa equipe deve se aprofundar, fale comigo ou com nossa equipe @TrellixARC no Twitter. Esperamos vê-lo na RSA de São Francisco em abril.

John Fokker
Chefe de inteligência sobre ameaças

METODOLOGIA

Os sistemas de back-end da Trellix fornecem a telemetria que utilizamos como fonte de dados para nossos relatórios trimestrais de ameaças. Nós combinamos nossa telemetria com inteligência de fontes abertas sobre ameaças e nossas próprias investigações sobre ameaças predominantes, como ransomware, atividades de estados-nações etc.

Quando falamos em telemetria, referimo-nos a detecções, e não a infecções. Uma detecção é registrada quando um arquivo, URL, endereço IP ou outro indicador é detectado por um de nossos produtos e relatado para nós.

Estamos cientes, por exemplo, de um número crescente de organizações que estão usando estruturas de teste de eficácia que distribuem amostras de malware reais. Tal uso aparece como uma detecção, mas certamente não é uma infecção.

O processo de análise e filtragem de falsos positivos na telemetria está em constante desenvolvimento, o que pode resultar em novas categorias de ameaças, em comparação com as edições anteriores.

Novas categorias de ameaças também serão acrescentadas conforme mais equipes de organização da Trellix contribuírem para este relatório trimestral.

A privacidade de nossos clientes é fundamental. Ela é importante no que se refere à telemetria e ao mapeamento com os setores e países de nossos clientes. A base de clientes difere conforme o país e os números podem mostrar aumentos que exijam análises mais detalhadas dos dados.

Um exemplo: o setor de telecomunicações frequentemente se destaca em nossos dados. Isso não significa, necessariamente, que esse setor é altamente visado. O setor de telecomunicações também inclui provedores de serviços de Internet, os quais possuem espaços de endereços IP que podem ser comprados por empresas. O que isso significa? Denúncias associadas ao espaço de endereços IP do provedor aparecem como detecções de telecomunicações, mas podem ser de clientes do provedor que operam em um setor diferente.

RANSOMWARE NO 4° TRIMESTRE DE 2022

Nesta seção oferecemos os vários insights que coletamos sobre atividade de grupos de ransomware. Essas informações são coletadas de várias fontes para proporcionar uma imagem melhor do cenário de ameaças, reduzir o viés da observação e nos ajudar a determinar qual família de ransomware foi a mais impactante no quarto trimestre de 2022. A primeira fonte é quantitativa e retrata estatísticas de campanhas de ransomware extraídas da correlação entre IOCs de ransomware e a telemetria dos clientes da Trellix. A segunda é qualitativa e mostra a análise dos vários relatórios publicados pelo setor de segurança, selecionados, triados e analisados pelo grupo Threat Intelligence. Por último, a terceira fonte é uma nova categoria que consiste no conjunto de relatórios de vítimas de ransomware extraídos de vários "sites de vazamentos" de grupos de ransomware, normalizados, aprimorados e finalmente analisados para proporcionar uma versão anonimizada dos resultados.

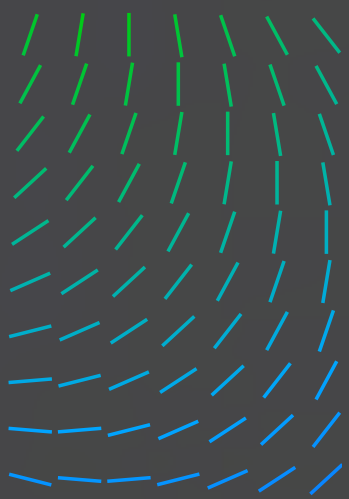
Ao oferecer esses diferentes pontos de vista, buscamos oferecer muitas peças do quebra-cabeça em que consiste o cenário de ameaças atual. Nenhum deles é suficiente devido às próprias limitações. Ninguém tem acesso a todos os logs de todos os sistemas conectados à Internet, nem todos os incidentes de segurança são relatados e nem todas as vítimas são extorquidas e incluídas nos sites de vazamentos. Porém, a combinação dos diversos pontos de vista pode resultar em uma compreensão melhor das várias ameaças, além de reduzir nossos próprios pontos cegos.

Um julgamento informado é o que conseguimos com a combinação de dados quantitativos e qualitativos das fontes, levando em consideração possíveis desvantagens e pontos cegos.

Destaques de ransomware no 4° trimestre de 2022

Grupo de ransomware mais impactante no 4° trimestre: LockBit 3.0

Por meio da observação das várias fontes da Trellix, podemos concluir que o LockBit 3.0 foi o grupo de ransomware mais impactante no quarto trimestre de 2022. A posição significativa do LockBit 3.0 baseia-se nas seguintes características:



3° O LockBit 3.0 ficou em terceiro lugar entre os grupos de ransomware predominantes no trimestre, segundo a análise da telemetria de ransomware obtida pelos sensores globais da Trellix.

2° O LockBit 3.0 ficou em segundo lugar – juntamente com o ransomware Cuba – entre os grupos de ransomware mais denunciados pelo setor de segurança, conforme análises das várias campanhas coletadas pelo grupo Threat Intelligence.

1° O site de vazamentos do LockBit 3.0 relatou o maior número de vítimas entre os grupos de ransomware no trimestre. Isso torna o LockBit o mais ávido por pressionar suas vítimas citando-as e expondo-as.

Veja a seguir mais categorias e descobertas sobre o LockBit no quarto trimestre de 2022:

SETORES AFETADOS PELO LOCKBIT 3.0 NO 4° TRIMESTRE DE 2022

29%

O setor de serviços e bens industriais foi o mais afetados pelo LockBit 3.0 no 4° trimestre de 2022, segundo o site de vazamentos das vítimas do LockBit 3.0.

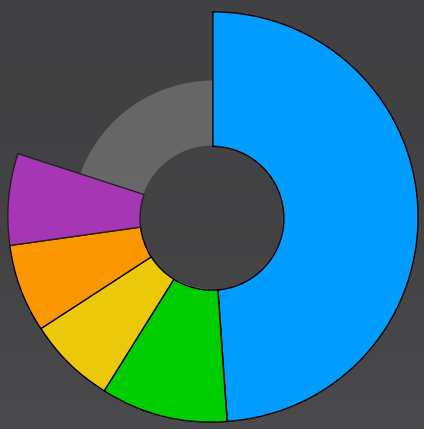
- Serviços e bens industriais
- Varejo
- Tecnologia
- Saúde
- Construção civil e materiais
- Artigos pessoais e para o lar
- Governo

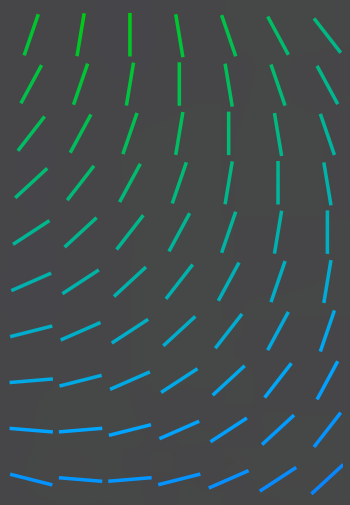
PAÍSES DAS EMPRESAS AFETADAS PELO LOCKBIT 3.0 NO 4° TRIMESTRE DE 2022

49%

As empresas dos Estados Unidos foram as mais afetadas (49%) pelo LockBit 3.0 no 4° trimestre de 2022, seguidas por empresas do Reino Unido, segundo o site de vazamentos de vítimas do LockBit 3.0.

- Estados Unidos
- Reino Unido
- Canadá
- França
- Brasil





Ferramentas e explorações do LockBit 3.0

VULNERABILIDADES NOTORIAMENTE EXPLORADAS PELO LOCKBIT 3.0

CVE-2018-13379
CVE-2020-0787
CVE-2021-20028
CVE-2021-34473
CVE-2021-34523

FERRAMENTAS MALICIOSAS USADAS PELO LOCKBIT 3.0

Amadey	Hakops
Blister	Neshta
BloodHound	SocGholish
Cobalt Strike	StealBit
Grabff	WinPEAS

FERRAMENTAS NÃO MALICIOSAS UTILIZADAS PELO LOCKBIT 3.0

BCDEdit	MiniDump	NSIS	Schtasks.exe
Cmd	MpCmdRun.exe	PCHunter	VSSAdmin
Fltmc.exe	Mshta	PowerShell	wevtutil
Fsutil	Mstsc	Process Monitor	WMIC
GMER	Netsh	Rundll32	RCLONE
MEGASYNC	Nltest		

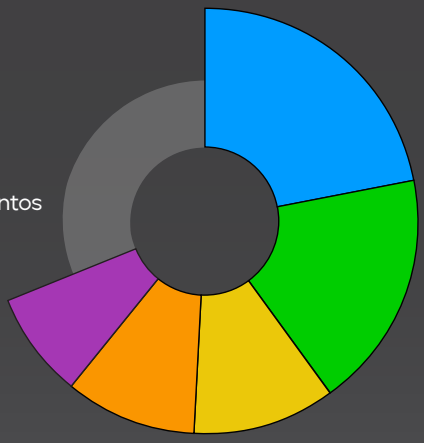
Ransomware pela ótica de nossa telemetria

As estatísticas seguintes baseiam-se em correlações entre nossa telemetria e nossa base de conhecimentos de inteligência sobre ameaças. Após uma fase de análise, identificamos um conjunto de campanhas com base em dados ao longo do período de tempo selecionado e extraímos suas características. As estatísticas exibidas são das campanhas, e não propriamente das detecções. Nossa telemetria global mostrou indicadores de comprometimento (IoCs) pertencentes a várias campanhas de diversos grupos de ransomware. As famílias de ransomware seguintes, com suas respectivas técnicas e ferramentas, representam as famílias mais comuns nas campanhas identificadas. Da mesma forma, os países e setores seguintes constituem os mais afetados pelas campanhas identificadas.

FAMÍLIAS DE RANSOMWARE MAIS COMUNS NO 4° TRIMESTRE DE 2022

22%

Cuba foi a família de ransomware mais predominante no 4° trimestre de 2022. Zeppelin foi frequentemente usada pela Vice Society. Leia mais sobre os vazamentos de comunicações do Yanluowang.



- Cuba
- Hive
- LockBit
- Zeppelin
- Yanluowang

FERRAMENTAS MALICIOSAS MAIS FREQUENTEMENTE USADAS POR GRUPOS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

41%

Cobalt Strike foi a ferramenta maliciosa mais frequentemente usada por grupos de ransomware no 4° trimestre de 2022.

1.	Cobalt Strike	41%
2.	Mimikatz	23%
3.	BURNTCIGAR	13%
4.	VMProtect	12%
5.	POORTRY	11%

TÉCNICAS MITRE-ATT&CK MAIS OBSERVADAS EM USO POR GRUPOS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

1.	Dados criptografados para maior impacto	17%
2.	Descoberta de informações do sistema	11%
3.	PowerShell	10%
4.	Transferência de ferramenta de ingresso	10%
5.	Shell de comandos do Windows	9%

FERRAMENTAS NÃO MALICIOSAS MAIS FREQUENTEMENTE USADAS POR GRUPOS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

21%

Cmd foi a ferramenta não maliciosa mais frequentemente usada por grupos de ransomware no 4° trimestre de 2022.

1.	Cmd	21%
2.	PowerShell	14%
3.	Net	10%
4.	Reg	8%
5.	PsExec	8%

PAÍSES MAIS AFETADOS POR GRUPOS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

29%

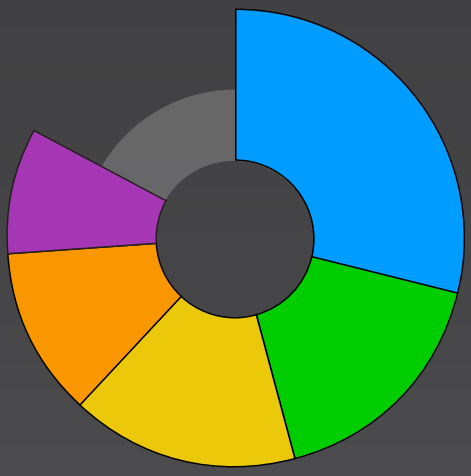
Os Estados Unidos foram o país mais afetado por grupos de ransomware no 4° trimestre de 2022, segundo a telemetria da Trellix.

- Estados Unidos
- China
- Catar
- Japão
- Indonésia

SETORES MAIS AFETADOS POR GRUPOS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

29%

O setor de terceirização e hospedagem foi o mais afetado por grupos de ransomware no 4° trimestre de 2022, segundo a telemetria da Trellix. Isso se correlaciona com o tamanho médio das organizações das vítimas listadas nos sites de vazamentos de ransomware, pois tais organizações não costumam ter um bloco de IPs próprio e dependem de provedores de hospedagem.



- Terceirização e hospedagem
- Bancário/financeiro/ gestão de patrimônio
- Governo
- Atacado
- Farmacêutico

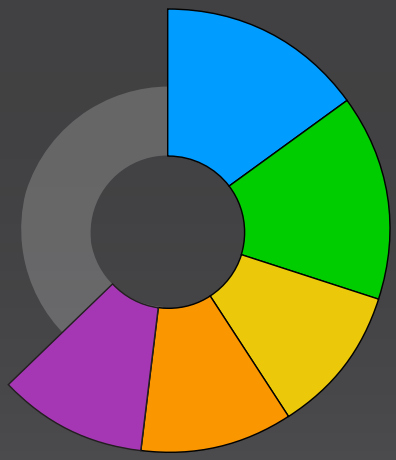
Ransomware relatado pelo setor de segurança

As estatísticas seguintes baseiam-se em relatórios públicos, bem como em pesquisas internas. Observe que nem todos os incidentes de ransomware são relatados. Muitas famílias de ransomware já estão ativas há bastante tempo e, naturalmente, têm menos destaque que famílias novas em trimestres específicos. Com base nesses critérios, tais métricas são uma indicação das famílias de ransomware que o setor de segurança considerou mais impactante e relevante no trimestre.

FAMÍLIAS DE RANSOMWARE MAIS RELATADAS NO 4° TRIMESTRE DE 2022

15%

Black Basta e Magniber foram as famílias de ransomware mais relatadas no 4° trimestre de 2022 segundo relatórios do setor de segurança.



- Black Basta
- Magniber
- Cuba
- LockBit
- Quantum

PRINCIPAIS TÉCNICAS DE ATAQUE DE FAMÍLIAS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

19%

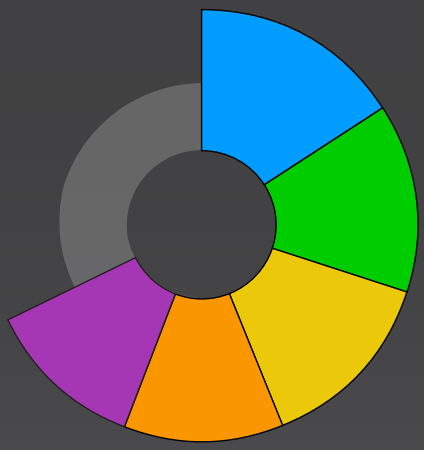
A técnica de ataque de dados criptografados para maior impacto foi a mais relatada em uso por famílias de ransomware no 4° trimestre de 2022, segundo relatórios do setor de segurança.

1.	Dados criptografados para maior impacto	19%
2.	Shell de comandos do Windows	11%
3.	Descoberta de informações do sistema	10%
4.	Transferência de ferramenta de ingresso	10%
5.	PowerShell	10%

PRINCIPAIS SETORES VISADOS POR FAMÍLIAS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

16%

O setor de saúde foi o mais visado pelas famílias de ransomware no 4° trimestre de 2022, segundo relatórios do setor de segurança.



- Saúde
- Finanças
- Governo
- Manufatura
- Transportes

PAÍSES MAIS VISADOS POR FAMÍLIAS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

19%

Os Estados Unidos foram o país mais visado por famílias de ransomware no 4° trimestre de 2022, segundo relatórios do setor de segurança.

- Estados Unidos
- Alemanha
- Brasil
- Argentina
- Canadá
- Índia
- Holanda
- Coreia do Sul
- Suíça
- Reino Unido

CVES UTILIZADAS POR FAMÍLIAS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

1.	CVE-2021-31207	16%
	CVE-2021-34474	16%
	CVE-2021-34523	16%
2.	CVE-2021-34527	13%
3.	CVE-2021-26855	9%
	CVE-2021-27065	9%

FERRAMENTAS MALICIOSAS USADAS POR FAMÍLIAS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

44%

Cobalt Strike foi a ferramenta maliciosa mais usada pelas famílias de ransomware relatadas no 4° trimestre de 2022, segundo relatórios do setor de segurança.

1.	Cobalt Strike	44%
2.	QakBot	13%
3.	IcedID	9%
4.	BURNTCIGAR	7%
5.	Carbanak SystemBC	7% 7%

FERRAMENTAS NÃO MALICIOSAS USADAS POR FAMÍLIAS DE RANSOMWARE NO 4° TRIMESTRE DE 2022

21%

PowerShell foi a ferramenta não maliciosa mais usada pelas famílias de ransomware relatadas no 4° trimestre de 2022, segundo relatórios do setor de segurança.

1.	PowerShell	21%
2.	Cmd	18%
3.	Rundll32	11%
4.	VSSAdmin	10%
5.	WMIC	9%

Relatórios de vítimas de "sites de vazamentos" de ransomware no 4° trimestre de 2022

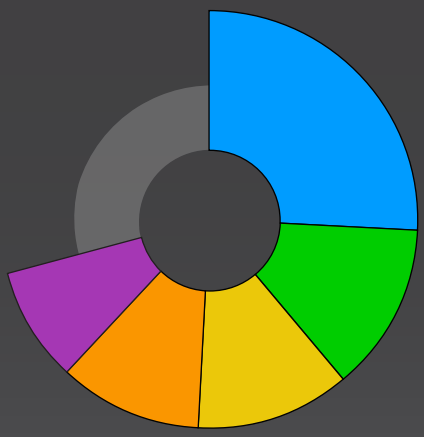
Os dados desta seção foram compilados extraindo-se informações em "sites de vazamentos" de vários grupos de ransomware. Os grupos de ransomware extorquem suas vítimas publicando informações sobre elas nesses sites. Quando as negociações chegam a um impasse ou as vítimas se recusam a pagar o resgate no prazo determinado pelo grupo de ransomware, este libera informações roubadas das vítimas. Nós utilizamos a ferramenta de código aberto RansomLook para coletar as várias postagens, processamos internamente os dados para normalizar e enriquecer os resultados e, com isso, oferecer uma versão anonimizada da análise de vitimologia.

É importante observar que nem todas as vítimas de ransomware são expostas nos respectivos sites de vazamentos. Muitas vítimas pagam o resgate e não são expostas. Essas métricas são uma indicação de vítimas extorquidas por grupos de ransomware ou que sofreram retaliação, não devendo ser confundidas com a quantidade total de vítimas.

GRUPOS DE RANSOMWARE QUE MAIS FIZERAM VÍTIMAS NO 4° TRIMESTRE DE 2022

26%

O LockBit 3.0 representou 26% dos 10 principais grupos de ransomware, responsáveis pelo maior número de vítimas em seus respectivos sites de vazamentos, no 4° trimestre de 2022.

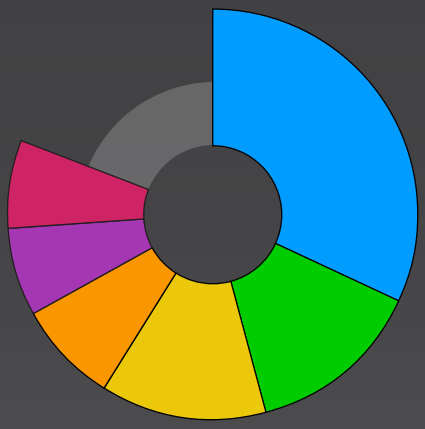


- LockBit 3.0
- ALPHV
- Royal
- Black Basta
- Cuba

SETORES AFETADOS POR GRUPOS DE RANSOMWARE SEGUNDO SITES DE VAZAMENTOS NO 4° TRIMESTRE DE 2022

32%

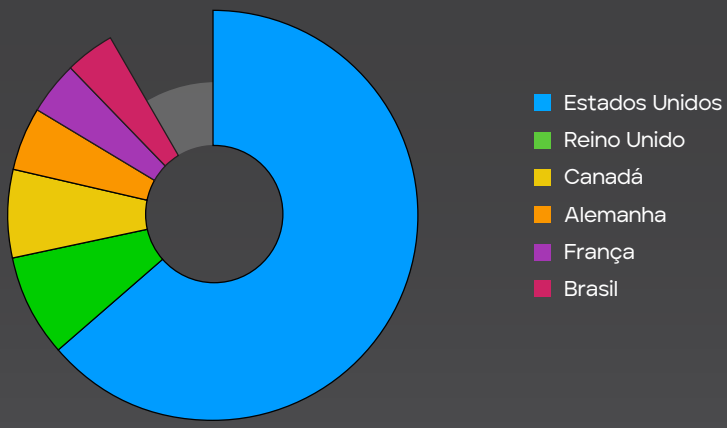
O setor de serviços e bens industriais foi o mais afetado por grupos de ransomware segundo seus sites de vazamentos no 4° trimestre de 2022. Serviços e bens industriais abrangem todos os produtos materiais e serviços não tangíveis, utilizados principalmente em construção civil e manufatura.



- Serviços e bens industriais
- Varejo
- Tecnologia
- Contrução civil e materiais
- Saúde
- Governo

PAÍSES DAS EMPRESAS AFETADAS POR GRUPOS DE RANSOMWARE SEGUNDO SITES DE VAZAMENTOS NO 4° TRIMESTRE DE 2022

63% das 10 principais empresas relatadas por vários grupos de ransomware em seus respectivos sites de vazamentos no 4° trimestre de 2022 são sediadas nos Estados Unidos, seguidas por Reino Unido (8%) e Canadá (7%).



ESTATÍSTICAS SOBRE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

Esta seção oferece insights que coletamos sobre atividade de grupos ligados a estados-nações. Essas informações são coletadas de várias fontes para criar uma imagem melhor do cenário de ameaças e reduzir o viés da observação. Primeiramente, apresentamos as estatísticas extraídas da correlação entre IOCs de grupos ligados a estados-nações e a telemetria dos clientes da Trellix. Em seguida, oferecemos insights de vários relatórios publicados pelo setor de segurança, os quais são selecionados, triados e analisados pelo grupo Threat Intelligence.

Estatísticas sobre estados-nações no 4° trimestre de 2022

- Estados Unidos e Alemanha tiveram aumentos significativos em ataques de estados-nações.
- China e Vietnã tiveram destaque em ataques de estados-nações no quarto trimestre.

Estatísticas de estados-nações pela ótica de nossa telemetria global

As estatísticas seguintes baseiam-se em correlações entre nossa telemetria e nossa base de conhecimentos de inteligência sobre ameaças. Após uma fase de análise, identificamos um conjunto de campanhas com base em dados ao longo do período de tempo selecionado e extraímos suas características. As estatísticas exibidas são das campanhas, e não propriamente das detecções. Devido a

várias agregações de logs, ao uso de estruturas de simulação de ameaças por nossos clientes e a correlações de alto nível com a base de conhecimentos de inteligência sobre ameaças, os dados são filtrados manualmente para satisfazer os critérios desejados.

Nossa telemetria global mostrou indicadores de comprometimento (IoCs) relacionados a várias campanhas de grupos de ameaças persistentes avançadas (APT). Os países dos perpetradores de ameaças seguintes, bem como suas técnicas e ferramentas, constituem os mais comuns nas campanhas identificadas. Da mesma forma, os dados sobre países e setores representam os mais afetados pelas campanhas identificadas.

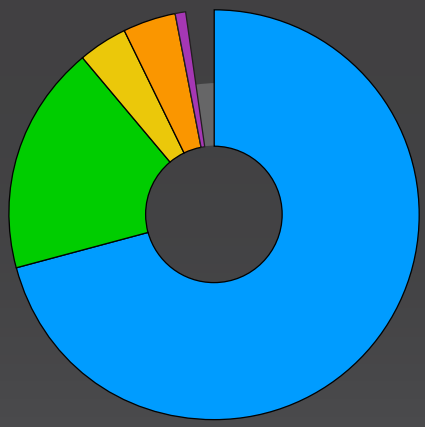
Insights da telemetria de estados-nações

PAÍSES DOS PERPETRADORES DE AMEAÇAS MAIS COMUNS POR TRÁS DE ATIVIDADES DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

71%

A China foi o mais frequente país de origem de perpetradores de ameaças por trás de atividades de estados-nações no 4° trimestre de 2022.

- China
- Coreia do Norte
- Rússia
- Irã
- Líbano

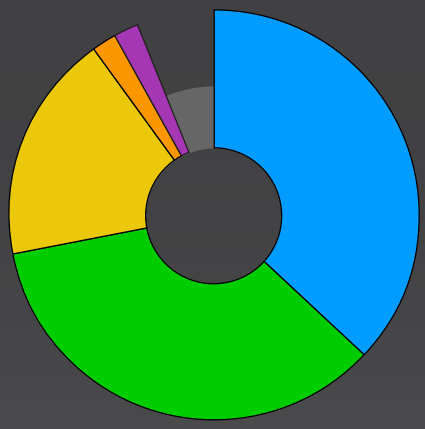


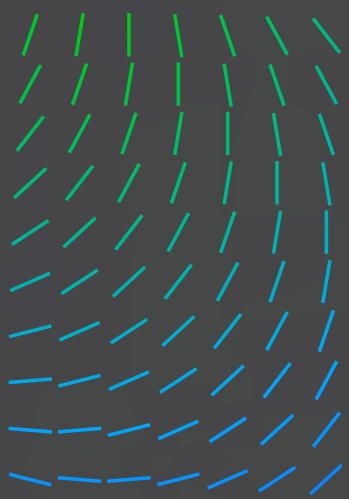
GRUPOS DE PERPETRADORES DE AMEAÇAS PREDOMINANTES NO 4° TRIMESTRE DE 2022

37%

Mustang Panda foi o grupo de perpetradores de ameaças predominante no 4° trimestre de 2022, segundo telemetria de estados-nações.

- Mustang Panda
- UNC4191
- Lazarus
- MuddyWater
- Kimsuky





TÉCNICAS MITRE ATT&CK MAIS COMUNS EM ATIVIDADES DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

1.	Carregamento lateral de DLL	14%
2.	Rundll32	13%
3.	Arquivos ou informações ocultadas	12%
4.	Shell de comandos do Windows	11%
5.	Chaves de execução do Registro / pasta de inicialização	10%

FERRAMENTAS MALICIOSAS MAIS FREQUENTEMENTE USADAS EM ATIVIDADES DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

1.	PlugX	24%
2.	BLUEHAZE	23%
3.	DARKDEW	23%
4.	MISTCLOAK	23%
5.	Cavalo de Troia de acesso remoto JSX	2%

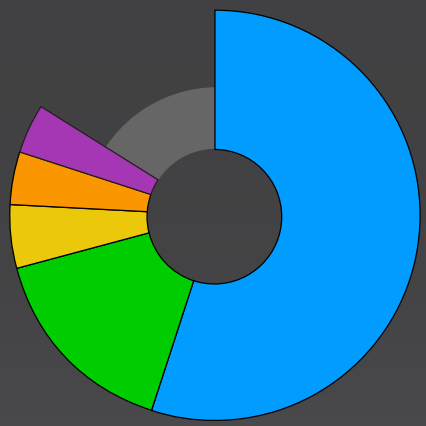
FERRAMENTAS NÃO MALICIOSAS MAIS FREQUENTEMENTE USADAS EM ATIVIDADES DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

1.	Rundll32	22%
2.	Cmd	19%
3.	Reg	17%
4.	Ncat	12%
5.	Regsvr32	6%

PAÍSES MAIS AFETADOS POR ATIVIDADES DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

55%

Os Estados Unidos foram o país mais afetado por atividades de estados-nações no 4° trimestre de 2022.

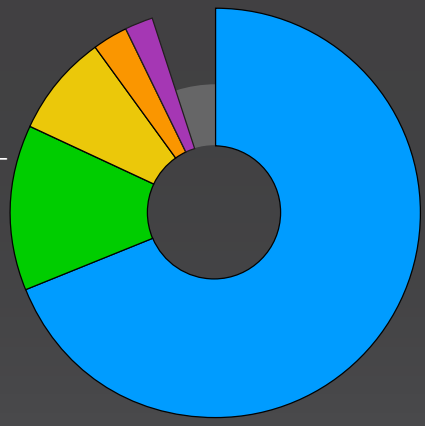


- Estados Unidos
- Vietnã
- Índia
- Alemanha
- China

SETORES MAIS AFETADOS POR ATIVIDADES DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

69%

O setor de transportes e logística foi o mais afetado por atividades de estados-nações no 4° trimestre de 2022.



- Transportes e logística
- Energia/Petróleo e gás
- Atacado
- Varejo
- Bancário/financeiro/ gestão de patrimônio

Incidentes de estados-nações, segundo relatórios públicos no 4° trimestre de 2022

Essas estatísticas baseiam-se em relatórios públicos e em pesquisas internas – e não em telemetria de logs de clientes. Observe que nem todos os incidentes de estados-nações são relatados. Muitas campanhas utilizam as mesmas ferramentas, táticas e procedimentos (TTPs) já conhecidos e menos sujeitos a serem mencionados em relatórios. O setor tende a se concentrar em campanhas mais novas nas quais um perpetrador tente algo novo ou cometa um erro. Essas métricas são uma indicação do que o setor considerou esclarecedor e relevante durante o quarto trimestre de 2022.

PAÍSES DOS PERPETRADORES DE AMEAÇAS MAIS RELATADOS EM CAMPANHAS DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

37%

das campanhas de estados-nações relatadas publicamente no 4° trimestre de 2022 originaram-se na China.

1.	China	37%
2.	Coreia do Norte	24%
3.	Irã	1%
4.	Rússia	1%
5.	Índia	1%

PERPETRADORES DE AMEAÇAS MAIS COMUNS POR TRÁS DE ATIVIDADES DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

33%

Lazarus foi o perpetrador de ameaças mais predominante por trás de atividades de estados-nações no 4° trimestre de 2022.

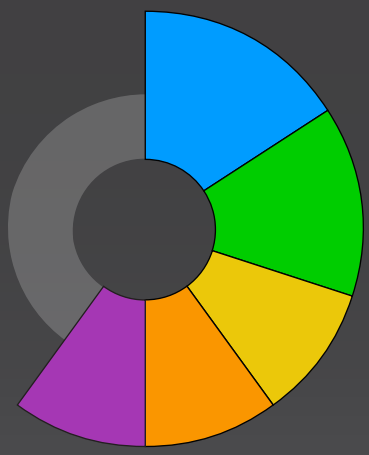
1.	Lazarus	33%
2.	Mustang Panda	17%
3.	APT34 APT37 APT41 COLDRIVER Patchwork Polonium SideWinder Winnti Group	1% cada

PAÍSES MAIS VISADOS POR CAMPANHAS DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

16%

Os Estados Unidos foram o país mais visado por campanhas de estados-nações no 4° trimestre de 2022.

- Estados Unidos
- Reino Unido
- Paquistão
- Rússia
- Ucrânia

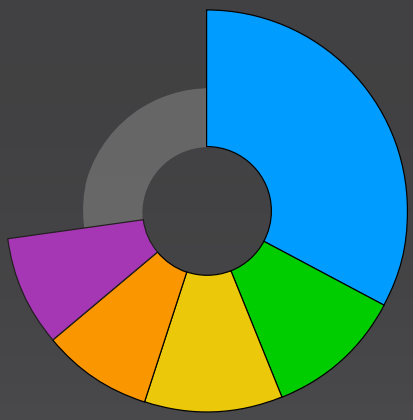


SETORES MAIS VISADOS POR CAMPANHAS DE ESTADOS-NAÇÕES RELATADAS NO 4° TRIMESTRE DE 2022

33%

O setor governamental foi o mais visado por campanhas de estados-nações no 4° trimestre de 2022, seguido pelos setores militar (11%) e de telecomunicações (11%).

- Governo
- Militar
- Telecomunicações
- Energia
- Financeiro



FERRAMENTAS MALICIOSAS MAIS POPULARES USADAS EM CAMPANHAS DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

1.	PlugX	22%
2.	Cobalt Strike	17%
3.	Metasploit	13%
4.	BlindingCan	9%
5.	Scanbox ShadowPad ZeroCleare	9% cada

FERRAMENTAS NÃO MALICIOSAS MAIS POPULARES USADAS EM CAMPANHAS DE ESTADOS-NAÇÕES NO 4° TRIMESTRE DE 2022

1.	Cmd	32%
2.	Rundll32	20%
3.	PowerShell	14%
4.	Reg	8%
5.	Schtasks.exe	7%

TÉCNICAS MITRE ATT&CK MAIS POPULARES USADAS EM CAMPANHAS DE ESTADOS-NAÇÕES RELATADAS NO 4° TRIMESTRE DE 2022

1.	Transferência de ferramenta de ingresso	13%
2.	Descoberta de informações do sistema	13%
3.	Arquivos ou informações ocultadas	12%
4.	Protocolos da Web	11%
5.	Decodificação/decifração de arquivos ou informações	11%

VULNERABILIDADES OBSERVADAS SENDO EXPLORADAS EM CAMPANHAS DE ESTADOS-NAÇÕES RELATADAS NO 4° TRIMESTRE DE 2022

CVE-2017-11882
CVE-2021-44228
CVE-2018-0802
CVE-2021-26855
CVE-2021-27065
CVE-2021-34473
CVE-2021-34523
CVE-2015-2545
CVE-2017-0144
CVE-2018-0798
CVE-2018-8581
CVE-2019-0604
CVE-2019-0708
CVE-2019-16098
CVE-2020-0688
CVE-2020-1380
CVE-2020-1472
CVE-2020-17141
CVE-2020-17143
CVE-2021-21551
CVE-2021-26606
CVE-2021-26857
CVE-2021-26858
CVE-2021-28480
CVE-2021-28481
CVE-2021-28482
CVE-2021-28483
CVE-2021-31196
CVE-2021-31207
CVE-2021-40444
CVE-2021-45046
CVE-2021-45105
CVE-2022-1040
CVE-2022-30190
CVE-2022-41128

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE (LOLBIN) E FERRAMENTAS DE TERCEIROS NO 4° TRIMESTRE DE 2022

Observações e rastreamento realizados através de nossa plataforma Trellix Insights Global Threat Intelligence reuniram a seguinte inteligência e visibilidade sobre o cenário de ameaças no 4° trimestre de 2022:

DESTAQUES DO LOLBIN NO 4° TRIMESTRE DE 2022

- O aproveitamento da funcionalidade existente continua a desempenhar um papel relevante nas fases de acesso inicial, execução, descoberta, persistência e impacto.

- Dados do 4° trimestre de 2022 mostram uma tendência continuada de técnicas de comando e script executadas por meio do Windows Command Shell ou do PowerShell como as mais frequentemente utilizadas.
- O uso por criminosos cibernéticos é predominante entre perpetradores de ameaças, inclusive por experientes APTs, grupos com motivação financeira e hacktivistas.

Os recém-chegados, as iniciativas isoladas e os jovens criadores de scripts que esbarram no cenário de ameaças também estão utilizando os binários já presentes em estruturas de exploração populares em suas tentativas de não serem notados ao hackear alguém ou explorar uma vulnerabilidade.

O aproveitamento da funcionalidade existente continua sendo utilizado para realizar tarefas nefastas nas fases de acesso inicial, execução, descoberta, persistência e impacto. Em dados coletados ao longo do quarto trimestre de 2022, podemos ver uma tendência continuada de técnicas de comando e script executadas por meio do shell de comandos do Windows ou do PowerShell como as mais frequentemente utilizadas.

BINÁRIOS DE SISTEMA OPERACIONAL PREDOMINANTES NO 4° TRIMESTRE DE 2022

47%

O shell de comandos do Windows representou 47% - quase metade – dos 10 binários de sistema operacional predominantes no quarto trimestre de 2022, seguido pelo PowerShell (32%) e pelo Rundl32 (27%).

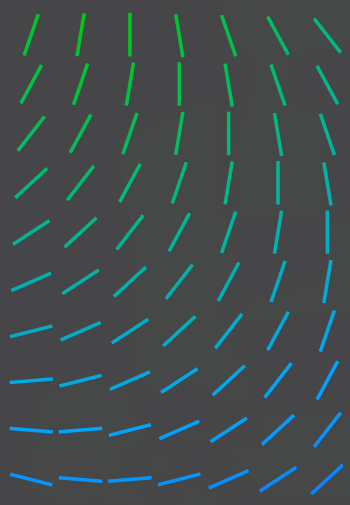
1.	Shell de comandos do Windows	47%
2.	PowerShell	32%
3.	Rundl32	27%
4.	Schtasks	23%
5.	WMI	21%

O uso por criminosos cibernéticos é predominante entre perpetradores de ameaças, inclusive por experientes ameaças persistentes avançadas, grupos com motivação financeira e hacktivistas "woke".

Os eventos processados através de nossa plataforma Trellix Insights nos quais perpetradores de ameaças utilizam binários do Windows levou ao desenvolvimento de malware adicional, seja um ladrão de senhas, um cavalo de Troia para acesso remoto ou ransomware. Binários como MSHTA, WMI ou WScript podem ter sido executados para obtenção de cargas virais adicionais de recursos controlados pelo atacante.

PRINCIPAIS FERRAMENTAS DE TERCEIROS NO 4° TRIMESTRE DE 2022

1.	Ferramentas de acesso remoto	58%
2.	Transferência de arquivos	22%
3.	Ferramentas de exploração de postagens	20%
4.	Descoberta de rede	16%
5.	Descoberta de AD	10%



Ferramentas de controle e acesso remoto estão consistentemente entre as ferramentas mais frequentemente aproveitadas por perpetradores de ameaças, mas as ferramentas utilizadas pelos profissionais de segurança continuam sendo aproveitadas para fins maliciosos. Os perpetradores de ameaças podem utilizá-las para manter ativos seus "beacons", automatizar exfiltrações ou coletar e compactar as informações visadas.

Entre ferramentas gratuitas e de código aberto, os empacotadores de software são aproveitados por perpetradores de ameaças para criar pacotes de software legítimo com conteúdo malicioso ou para acondicionar malware com o intuito de contornar mecanismos de detecção ou análise.

INSIGHTS SOBRE O COBALT STRIKE NO 4° TRIMESTRE DE 2022

O grupo Threat Intelligence do Trellix Advanced Research Center monitora a utilização de servidores Cobalt Strike Team (Cobalt Strike C2s) na Internet combinando metodologias de caça de infraestruturas e cargas virais. Apresentamos aqui insights de destaque identificados durante a análise dos beacons do Cobalt Strike coletados:

15% LICENÇAS DE AVALIAÇÃO DO COBALT STRIKE

Apenas 15% dos beacons do Cobalt Strike identificados na Internet tinham uma licença de avaliação do Cobalt Strike. Essa versão do Cobalt Strike inclui a maioria dos recursos conhecidos dessa estrutura de exploração de postagens. No entanto, ela acrescenta "indícios" e remove a criptografia em trânsito para tornar a carga viral mais fácil de detectar com produtos de segurança.

87% RUNDLL32.EXE

Rundll32.exe, processo padrão utilizado para sessões de disseminação e execução de trabalhos pós-exploração, foi encontrado em 87% dos beacons identificados.

5% CABEÇALHO HTTP DE HOST

Pelo menos 5% dos beacons do Cobalt Strike observados utilizaram o cabeçalho HTTP de host, uma opção que facilita o "fronting" de domínio com o Cobalt Strike. Fronting de domínio é uma técnica que se aproveita de redes de entrega de conteúdo (CDNs) que hospedam múltiplos domínios. Os atacantes ocultam uma solicitação HTTPS para um site malicioso dentro de uma conexão TLS para um site legítimo.

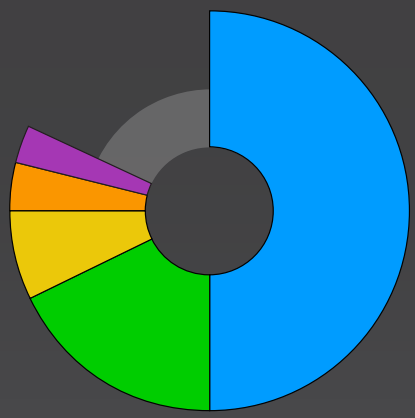
22% BEACONS DE DNS

Beacons de DNS representaram 22% dos beacons do Cobalt Strike identificados. Esse tipo de carga viral comunica-se de volta com o servidor Cobalt Strike Team do atacante, que é o servidor oficial do domínio, por meio de consultas DNS para esconder sua atividade.

PAÍSES QUE MAIS HOSPEDAM SERVIDORES COBALT STRIKE TEAM NO 4° TRIMESTRE DE 2022

50%

Metade dos servidores Cobalt Strike Team detectados no quarto trimestre de 2022 foram hospedados na China, o que se deve, principalmente, ao volume de hospedagem em nuvem disponível na China.



- China
- Estados Unidos
- Hong Kong
- Rússia
- Holanda

GOOTLOADER NO 4° TRIMESTRE DE 2022

Gootloader é um malware modular cujo nome pode ocasionalmente se referir a um outro malware identificado como "GootKit" ou "GootKit Loader". Os atuais recursos modulares do malware Gootloader estão sendo utilizados para distribuir cargas de malware adicionais, inclusive REvil, Kronos, Cobalt Strike e Icedid.

Em eventos recentes, o Gootloader foi visto utilizando otimização de mecanismos de pesquisa (SEO) para levar usuários incautos a sites falsos ou comprometidos utilizados para hospedar um arquivo compactado contendo como carga um arquivo JS (JavaScript). Contudo, essa técnica exige que o usuário incauto abra o arquivo e execute o conteúdo, o qual por sua vez executa o código JS malicioso por meio do Windows Scripting Host. Ao ser executado, o Gootloader inicia comunicações de comando e controle e busca malware adicional.

O Gootloader é um malware como serviço (MaaS) oferecido a assinantes, o que permite aos perpetradores de ameaças carregar várias cargas virais adicionais, e isso faz com que o Gootloader constitua uma ameaça significativa a ambientes corporativos.

Com nosso rastreador interno de Gootloader, identificamos uma variante recente, encontrada na Internet em 18 de novembro de 2022, e testemunhamos variantes antigas saindo de cena em 13 de novembro de 2022. As modificações na variante mais recente consistem em:

- Remoção da funcionalidade de manipulação do Registro
- Aumento das solicitações de rede remota para 10 URLs em vez de três

- Capacidade de chamar scripts PowerShell diretamente via CScript
- Persistência para cada login de usuário.

Nosso processo de rastreamento do Gootloader

A nova variante do Gootloader evoluiu utilizando múltiplas camadas de ocultação. Cada estágio sucessivo após a descompactação utiliza variáveis carregadas do estágio anterior, o que torna a análise mais difícil. As amostras coletadas como resultado de nossos esforços de caça YARA são fornecidas a um analisador estático de JavaScript e PowerShell para extrair IOCs como servidores de comando e controle (C&C ou C2) remotos e assinaturas de identificação exclusivas. Esses IOCs podem ser utilizados para identificar e rastrear instâncias específicas do Gootloader na Internet.

Em seguida, os IOCs do Gootloader extraídos são processados consultando-se o banco de dados da equipe de reputação de URLs da Trellix para identificar quais são maliciosos, quais são domínios legítimos potencialmente comprometidos e quais são domínios legítimos utilizados para chamar atenção e prejudicar a análise.

Insights da telemetria do Gootloader

As estatísticas exibidas são as das campanhas identificadas pela correlação entre os IOCs extraídos e os logs de nossos clientes, e não as detecções em si. No caso do Gootloader, a maioria das detecções baseia-se em ocorrências do domínio. Como o Gootloader utiliza domínios como isca, as estatísticas mostradas devem ser interpretadas como maliciosas com um nível médio de confiança.

PAÍSES MAIS ATINGIDOS PELO GOOTLOADER NO 4° TRIMESTRE DE 2022

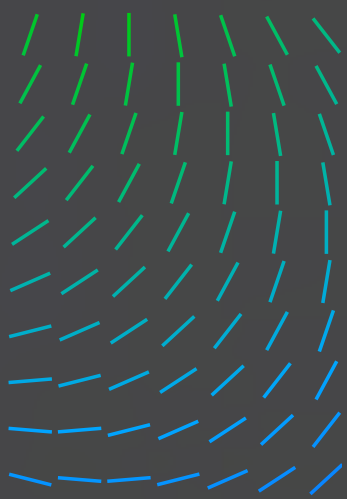
37%

Os Estados Unidos foram o país mais atingido pelo Gootloader no 4° trimestre de 2022.

1.	Estados Unidos	37%
2.	Itália	19%
3.	Índia	11%
4.	Indonésia	9%
5.	França	5%

TÉCNICAS MITRE ATT&CK MAIS POPULARES UTILIZADAS PELO GOOTLOADER NO 4° TRIMESTRE DE 2022

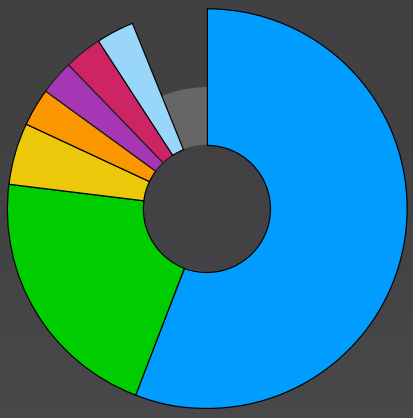
1. Decodificação/ decifração de arquivos ou informações
2. JavaScript
3. Arquivos ou informações ocultados
4. PowerShell
5. Esvaziamento de processos



SETORES MAIS VISADOS PELO GOOTLOADER NO 4° TRIMESTRE DE 2022

56%

O setor de telecomunicações foi o mais visado pelo Gootloader no 4° trimestre de 2022.



Técnicas MITRE ATT&CK mais populares utilizadas pelo Gootloader no 4° trimestre de 2022

Decodificação/decifração de arquivos ou informações

JavaScript

Arquivos ou informações ocultados

PowerShell

Esvaziamento de processos

Carregamento reflexivo de código

Chaves de execução do Registro / pasta de inicialização

Rundll32

Tarefa agendada

INTELIGÊNCIA SOBRE VULNERABILIDADES NO 4° TRIMESTRE DE 2022

Nosso dashboard de vulnerabilidades concentra as análises das mais recentes vulnerabilidades de grande impacto. A análise e a triagem são realizadas pelos especialistas do setor em vulnerabilidades do Trellix Advanced Research Center. Esses pesquisadores, especializados em engenharia reversa e análise de vulnerabilidades, monitoram continuamente as vulnerabilidades mais recentes e como os perpetradores de ameaças as estão utilizando em seus ataques para oferecer orientações sobre remediação. Essas recomendações concisas e altamente técnicas de especialistas permitem que você separe o joio do trigo e se concentre nas vulnerabilidades mais impactantes que podem afetar a sua organização, possibilitando uma reação rápida.

DESTAQUES DA INTELIGÊNCIA SOBRE VULNERABILIDADES NO 4° TRIMESTRE DE 2022

41% O Lanner foi responsável por 41% dos fornecedores e produtos vulneráveis e afetados por CVEs exclusivas no 4° trimestre de 2022.

29% A versão de firmware IAC-AST2500A 1.10.0 foi a CVE mais relatada das utilizadas por produtos no 4° trimestre de 2022.

CVES, FORNECEDORES E PRODUTOS VULNERÁVEIS MAIS IMPACTANTES NO 4° TRIMESTRE DE 2022

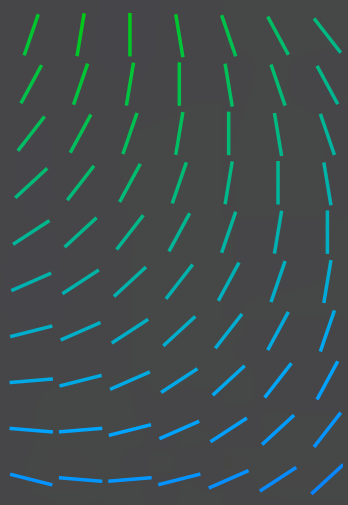
1.	Lanner	41%
2.	Microsoft	19%
3.	BOA	15%
4.	Oracle	8%
5.	Apple Chrome Citrix Fortinet Linux	5% cada

CVES RELATADAS POR PRODUTOS NO 4° TRIMESTRE DE 2022

29%

A versão de firmware IAC-AST2500A 1.10.0 foi a CVE mais relatada das utilizadas por produtos no 4° trimestre de 2022, seguida por servidor BOA (10%), IAC-AST2500A (6%) e Exchange (6%).

Produtos das CVEs relatadas	CVEs exclusivas
IAC-AST2500A, versão de firmware 1.10.0	9
Servidor BOA	3
Exchange	3
IAC-AST2500A	2
tvOS	1
iPadOS	1
iOS	1
Windows	1
Safari	1
SQLite até 3.40.0 (inclusive)	1
Oracle Access Manager, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0	1
MacOS	1
Linux Kernel anterior a 5.15.61	1
Internet Explorer	1



Produtos das CVEs relatadas	CVEs exclusivas
FortiOS (sslvpnd)	1
Citrix ADC/Citrix Gateway	1
Chrome, versões anteriores a 108.0.5359.94/.95	1
Servidor BOA, Boa 0.94.13	1

CVES RELATADAS NO 4° TRIMESTRE DE 2022

CVE-2022-1786
CVE-2022-26134
CVE-2022-27510
CVE-2022-27518
CVE-2022-31685
CVE-2022-32917
CVE-2022-32932
CVE-2022-33679
CVE-2022-34718
CVE-2022-35737
CVE-2022-3602
CVE-2022-3786
CVE-2022-37958
CVE-2022-40684
CVE-2022-41040
CVE-2022-41080
CVE-2022-41082
CVE-2022-41128
CVE-2022-41352
CVE-2022-42468
CVE-2022-42475
CVE-2022-4262
CVE-2022-42856
CVE-2022-42889
CVE-2022-43995
CVE-2022-46908
CVE-2022-47939

TENDÊNCIAS DA SEGURANÇA DE E-MAIL NO 4° TRIMESTRE DE 2022

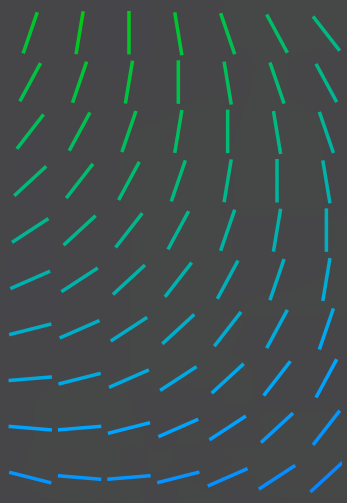
As estatísticas de segurança de e-mail baseiam-se em telemetria gerada em vários appliances de segurança de e-mail distribuídos em redes de clientes do mundo todo. Os logs de detecção são agregados e analisados para produzir as descobertas seguintes:

DESTAQUES DAS TENDÊNCIAS DE SEGURANÇA DE E-MAIL NO 4° TRIMESTRE DE 2022

100% Observou-se que o volume de e-mails maliciosos em países árabes aumentou 100% em outubro, em comparação com agosto e setembro.

40% Qakbot foi a tática de malware mais utilizada, representando 40% das campanhas que visaram países árabes.

42% O setor de telecomunicações foi o mais afetado por e-mails maliciosos no quarto trimestre de 2022, representando 42% das campanhas de e-mails maliciosos que visaram setores específicos.



87% Os e-mails de phishing com URLs maliciosos foram, por uma grande margem, o vetor de ataque predominante no quarto trimestre de 2022.

64% Os casos de impostura aumentaram 64% do terceiro para o quarto trimestre de 2022.

82% de todos os e-mails de fraude de CEO foram enviados por meio de serviços de e-mail gratuitos.

78% de todos os ataques de comprometimento de e-mail corporativo (BEC) utilizaram frases de CEO comuns.

142% Os ataques de vishing foram predominantes no quarto trimestre de 2022, aumentando 142% em relação ao terceiro trimestre de 2022.

TÁTICAS DE MALWARE DE E-MAIL PREDOMINANTES NO 4° TRIMESTRE DE 2022

40%

Qakbot foi a tática de malware de e-mail mais utilizada no 4° trimestre de 2022.

1.	Qakbot	40%
2.	Emotet	26%
3.	Formbook	26%
4.	Remcos	4%
5.	QuadAgent	4%

PRODUTOS E MARCAS MAIS VISADOS POR PHISHING DE E-MAIL NO 4° TRIMESTRE DE 2022

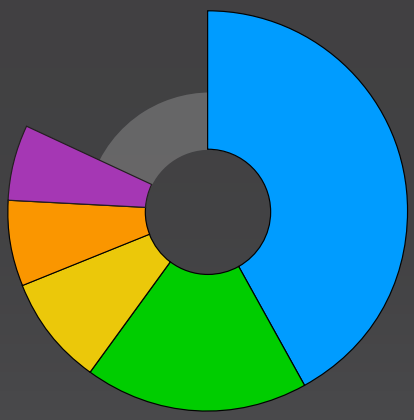
1.	Genéricos	62%
2.	Outlook	13%
3.	Microsoft	11%
4.	Ekinet	8%
5.	Cloudfare	3%

SETORES MAIS AFETADOS POR E-MAILS MALICIOSOS NO 4° TRIMESTRE DE 2022

42%

O setor de telecomunicações foi o mais afetado por e-mails maliciosos no 4° trimestre de 2022.

- Telecomunicações
- Governo
- Educação
- Finanças
- Serviços/consultoria



DESTAQUES DAS TENDÊNCIAS DE IMPOSTURA DE E-MAIL NO 4° TRIMESTRE DE 2022

82% de todos os e-mails de fraude de CEO foram enviados por meio de serviços de e-mail gratuitos.

78% de todos os ataques de comprometimento de e-mail corporativo (BEC) utilizaram frases de CEO comuns.

64% foi o aumento em e-mails maliciosos fazendo-se passar por CEOs e outros líderes empresariais, do terceiro ao quarto trimestre de 2022.

Principais frases de CEO utilizadas em ataques de BEC no 4° trimestre de 2022:

"Preciso que você cuide de uma tarefa para mim imediatamente."

"Preciso que você execute uma tarefa. Por favor, informe o seu número de celular."

"Envie o seu número de celular. Preciso que você faça algo para mim agora mesmo."

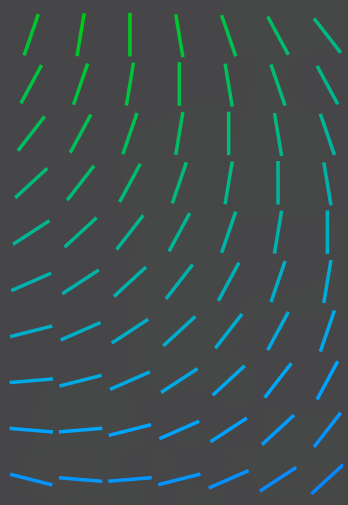
"Por favor, envie o seu número de celular e fique à espera de um texto meu. Preciso que você cuide de uma tarefa."

"Por favor, confirme o seu número de celular e fique à espera de um texto meu com instruções."

"Você recebeu meu e-mail anterior? Tenho um negócio lucrativo para você."

COMPARAÇÃO DE IMPOSTURA NO 4° TRIMESTRE DE 2022

64% Os casos de impostura aumentaram 64% do terceiro para o quarto trimestre de 2022.



INSIGHTS SOBRE CAMPANHAS DE PHISHING NO 4° TRIMESTRE DE 2022

Provedores de hospedagem de Web cada vez mais utilizados para fraudar e roubar

No quarto trimestre, observamos um aumento no uso de provedores de hospedagem de Web legítimos para fraudar usuários e roubar credenciais. Os provedores de serviços mais utilizados foram três: dweb.link, ipfs.link e translate.goog. Também observamos volumes significativos de outros domínios de provedores de serviços, como ekinet, storageapi_fleek e selcdn.ru. Os atacantes estão utilizando continuamente serviços de hospedagem novos e populares para hospedar páginas de phishing e contornar mecanismos antiphishing. Um motivo pelo qual os atacantes aumentaram seu interesse no uso de provedores de hospedagem de Web legítimos é que esses serviços não podem ser colocados em listas negras por sistemas de detecção porque seu objetivo principal é hospedar arquivos legítimos e compartilhar conteúdo.

VETORES DE ATAQUE MAIS UTILIZADOS EM E-MAILS DE PHISHING

87%

Os e-mails de phishing com URLs maliciosos foram, por uma grande margem, o vetor de ataque predominante no quarto trimestre de 2022.

1.	URL	87%
2.	Anexo	7%
3.	Cabeçalho	6%

PROVEDORES DE HOSPEDAGEM DE WEB ALTAMENTE APROVEITADOS NO 4° TRIMESTRE DE 2022

154%

Embora o Dweb tenha sido o provedor de hospedagem de Web mais aproveitado no 4° trimestre de 2022, o Google Translate apresentou o maior aumento (154%) entre o terceiro e o quarto trimestre de 2022.

1.	Dweb	81%
2.	Ipfs	17%
3.	Google Translate	10%

TÉCNICAS DE EVASÃO MAIS UTILIZADAS EM ATAQUES DE PHISHING NO 4° TRIMESTRE DE 2022

63%

A evasão baseada em redirecionamento 302 foi predominante no 4° trimestre de 2022.

- Os ataques de phishing com evasão baseada na geolocalização aumentaram significativamente no 4° trimestre.
- Ataques baseados em Captcha também aumentaram no 4° trimestre.

Vishing é uma outra forma de phishing, desenvolvida para induzir as vítimas a se conectarem com os atacantes, principalmente pelo uso de e-mails, mensagens de texto, chamadas telefônicas ou mensagens diretas de chat.

142%

Os ataques de vishing foram predominantes no quarto trimestre de 2022, aumentando 142% em relação ao terceiro trimestre de 2022.

85%

Os serviços de e-mail gratuito tornaram-se favoritos dos malfeitores que utilizam vishing. Um grande percentual de ataques de vishing que detectamos (85%) no quarto trimestre de 2022 foi enviado utilizando algum tipo de serviço de e-mail gratuito.

Norton, McAfee, Geek Squad, Amazon, e PayPal foram os temas mais populares utilizados por campanhas de vishing no quarto trimestre.

SEGURANÇA DE REDE NO 4° TRIMESTRE DE 2022

A equipe de pesquisa de rede Trellix ARC concentra-se em detectar e bloquear ataques baseados em rede que ameaçam nossos clientes. Nós inspecionamos diversas áreas da cadeia de abate, inclusive reconhecimento, comprometimento inicial, comunicações de comando e controle e ferramentas, técnicas e procedimentos (TTPs) de movimentação lateral. Nossa capacidade de aproveitar as vantagens de nossas tecnologias combinadas nos dá visibilidade para detectar melhor ameaças desconhecidas.

Técnicas MITRE ATT&CK mais populares utilizadas contra a segurança de rede no 4° trimestre de 2022

- T1083 - Descoberta de arquivos e diretórios
- T1573 - Canal criptografado
- T1020 - Exfiltração automatizada
- T1210 - Exploração de serviços remotos
- T1569 - Serviços de sistema
- T1059 - Interpretador de comandos e scripts: shell de comandos do Windows
- T1047 - Instrumentação de gerenciamento do Windows
- T1087 - Descoberta de contas
- T1059 - Interpretador de comandos e scripts
- T1190 - Exploração de aplicativos voltados ao público

Ataques mais impactantes contra serviços voltados para a Internet no 4° trimestre de 2022

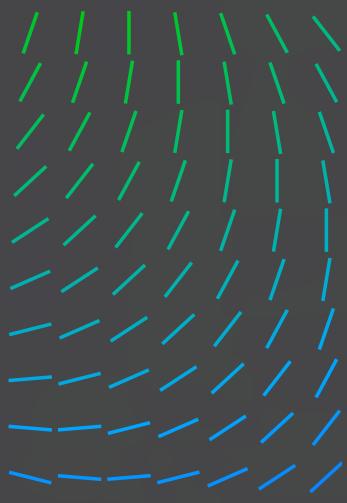
Várias varreduras de rede são realizadas todo dia para testar máquinas acessíveis pela Internet, com o objetivo de encontrar uma possível brecha no ambiente de um cliente. Explorações antigas buscam continuamente por sistemas não corrigidos.

- Detecção de tentativa de acesso a arquivo /etc/passwd
- Possível ataque via script entre sites
- Mecanismo de varredura de segurança SIPVicious
- Tráfico de mecanismo de varredura Nmap detectado
- Atividade de varredura - Shellshock, teste de servidor Web
- Execução de código remoto Bash (Shellshock) HTTP CGI (CVE-2014-6278)
- Vulnerabilidade de execução remota de código no Oracle WebLogic CVE-2020-14882
- Tentativa de travessia de diretório
- Injeção de script OGNL ConversionErrorInterceptor no Apache Struts 2
- Execução remota de código no Apache Log4j CVE-2021-44228

WebShells mais significativos utilizados como base inicial para ataques de rede no 4° trimestre de 2022

Os WebShells seguintes costumam ser utilizados em tentativas de controlar um servidor Web vulnerável.

- China Chopper WebShell
- JFolder WebShell
- ASPXSpy WebShell
- C99 WebShell
- Tux WebShell
- B374K WebShell / família RootShell



Ferramentas, técnicas e procedimentos mais relevantes, após a penetração da rede, no 4° trimestre de 2022

Os WebShells seguintes costumam ser utilizados em tentativas de controlar um servidor Web vulnerável.

Temos visto um grande volume de ferramentas, técnicas e procedimentos (TTPs) utilizados pelos atacantes durante a fase de movimentação lateral, inclusive o uso de ferramentas e vulnerabilidades antigas, como SCShell e PSExec.

- SCshell: movimentação lateral sem arquivo utilizando o gerenciador de serviços
- Chamada remota de processo do Windows WMI
- Invocação do shell de comandos via WMIEXEC por SMB
- Exploração EternalBlue detectada
- Tentativa de uso da CVE-2020-0796 no Microsoft SMBv3
- Execução remota de código no Apache Log4j CVE-2021-44228
- Enumeração remota de contas de administrador corporativo/de domínio
- Suspeita de uso remoto do PowerShell
- Suspeita de reconhecimento de rede utilizando-se WMIC
- Comando de enumeração detectado em arquivo de lote
- Atividade SMB PSEXEC

TELEMETRIA DE OPERAÇÕES DE SEGURANÇA FORNECIDA PELA TRELLIX XDR

Estas estatísticas baseiam-se em telemetria gerada por diversos sensores em nossa base de clientes. Os logs de detecção são agregados e analisados para produzir as seções seguintes:

Incidentes de segurança mais impactantes no 4° trimestre de 2022

A seção abaixo mostra os alertas de segurança mais predominantes no 4° trimestre de 2022:

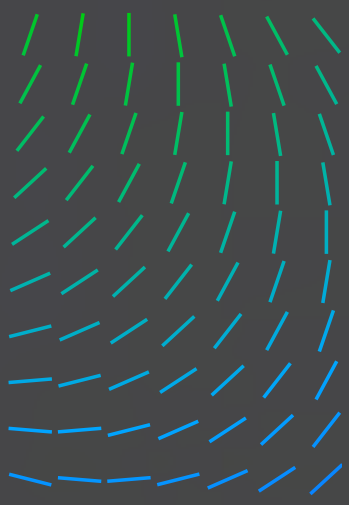
EXPLOIT - LOG4J [CVE-2021-44228]

OFFICE 365 ANALYTICS [login anormal]

OFFICE 365 [phishing permitido]

EXPLOIT - FORTINET [CVE-2022-40684]

EXPLOIT - APACHE SERVER [CVE-2021-41773 - tentativa]



WINDOWS ANALYTICS [ataque de força bruta bem-sucedido]

EXPLOIT - ATLASSIAN CONFLUENCE [CVE-2022-26134]

EXPLOIT - F5 BIG-IP [CVE-2022-1388 - tentativa]

TÉCNICAS MITRE ATT&CK MAIS UTILIZADAS NO 4° TRIMESTRE DE 2022

1.	Exploração de aplicativos acessíveis pela Internet (T1190)	29%
2.	Protocolo de camada de aplicativo: DNS (T1071.004)	14%
	Phishing (T1566)	14%
3.	Manipulação de contas (T1098.001) Força bruta (T1110) Comprometimento ao acessar (T1189) Execução pelo usuário: arquivo malicioso (T1204.002) Contas válidas: contas locais (T1078,003)	7% cada

DISTRIBUIÇÃO DAS PRINCIPAIS FONTES DE LOGS NO 4° TRIMESTRE DE 2022

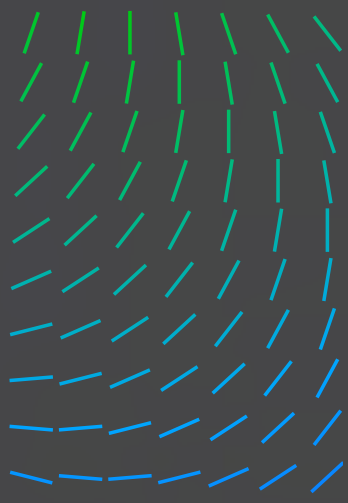
1.	Rede	40%
2.	E-mail	27%
3.	Endpoint	27%
4.	Firewall	6%

EXPLORAÇÕES OBSERVADAS NO 4° TRIMESTRE DE 2022

PRINCIPAIS EXPLORAÇÕES OBSERVADAS NO 4° TRIMESTRE DE 2022

30% Log4j foi a principal exploração observada no 4° trimestre de 2022.

1.	Log4j (CVE-2021-44228)	30%
2.	Fortinet (CVE-2022-40684)	16%
3.	Apache Server (CVE-2021-41773)	15%
4.	Atlassian Confluence (CVE-2022-26134)	14%
5.	F5 Big-IP (CVE-2022-1388 - tentativa)	13%
6.	Microsoft Exchange (tentativa de exploração do ProxyShell)	11%



INCIDENTES DE NUVEM NO 4° TRIMESTRE DE 2022

Ataques contra infraestruturas de nuvem estão sempre em alta, pois muitas empresas estão migrando de suas infraestruturas locais. Analistas da Gartner preveem que mais de 85% das organizações terão adotado o princípio de nuvem em primeiro lugar até 2025.

Ao analisar a telemetria do quarto trimestre de 2022, observamos o seguinte:

- Detecções relacionadas ao AWS lideram o ranking, possivelmente devido ao status do AWS como líder principal no mercado de nuvem.
- O foco da maioria dos ataques foi a obtenção de acesso inicial por meio de força bruta ou "spraying" de senhas em contas válidas, o que aponta para o vetor de infecção inicial na superfície de ataque na nuvem.
- Considerando-se que a maioria das contas corporativas tem autenticação por múltiplos fatores (MFA) ativada, os ataques de força bruta bem-sucedidos levam os adversários a plataformas de MFA, resultando em um pico de detecções relacionado a MFA.

As seções abaixo descrevem brevemente os dados de telemetria de ataques baseados na nuvem contra nossa base de clientes, divididos pelos vários provedores de nuvem.

DISTRIBUIÇÃO DAS TÉCNICAS MITRE ATT&CK PARA AWS NO 4° TRIMESTRE DE 2022

1.	Contas válidas (T1078)	18%
2.	Modificação da infraestrutura de computação na nuvem (T1578)	12%
3.	Manipulação de contas (T1098)	9%
4.	Contas de nuvem (T1078.004)	8%
5.	Força bruta (T1110) Incapacitação de defesas (T1562)	6% cada

PRINCIPAIS TÉCNICAS MITRE ATT&CK PARA AZURE NO 4° TRIMESTRE DE 2022

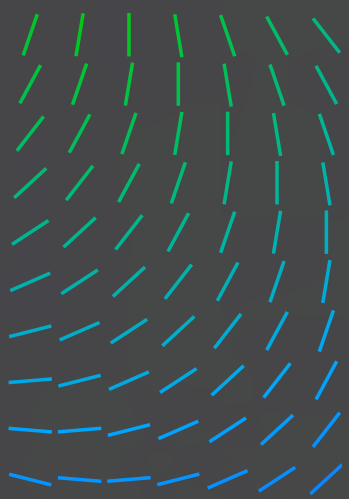
1.	Contas válidas (T1078)	23%
2.	Autenticação por múltiplos fatores (T1111)	19%
3.	Força bruta (T1110)	14%
4.	Proxy (T1090)	14%
5.	Manipulação de contas (T1098)	5%

PRINCIPAIS DETECÇÕES DE AWS POR TÉCNICAS MITRE ATT&CK NO 4° TRIMESTRE DE 2022

Técnica MITRE	Regra
Manipulação de contas (T1098)	Política de privilégio do AWS vinculada à identidade IAM AWS S3 - Política de exclusão de bucket
Contas válidas (T1078)	Login anômalo no console do AWS Analytics Utilização anômala de chave de API do AWS Analytics Comportamento anômalo de usuário do AWS GuardDuty Acesso anônimo concedido ao AWS GuardDuty
Incapacitação de defesas (T1562)	Mudanças de política do AWS CloudTrail para o CloudTrail Operação de exclusão de trilha do AWS CloudTrail
Credenciais em arquivos (T1552.001)	Alerta sobre possível roubo de chaves secretas do AWS
Modificação da infraestrutura de computação na nuvem (T1578)	Exclusão de bucket S3 pelo AWS CloudTrail Definição de permissões da ACL para bucket S3 pelo AWS CloudTrail Definição de permissões da ACL para objeto pelo AWS CloudTrail

PRINCIPAIS DETECÇÕES DE AZURE POR TÉCNICAS MITRE ATT&CK NO 4° TRIMESTRE DE 2022

Técnica MITRE ATT&CK	Regra
Contas válidas (T1078)	Inscrição arriscada no Azure AD Login no Azure de um local incomum Login no Azure por uma conta não vista em 60 dias
Força bruta (T1110)	Múltiplas falhas de autenticação no Azure Graph de ataques de força bruta contra o portal do Azure Graph da distribuição das tentativas de quebra de senha
Autenticação por múltiplos fatores (T1111)	MFA do Azure negada devido a alerta de fraude MFA do Azure negada devido a usuário bloqueado MFA do Azure negada devido a código de fraude MFA do Azure negada devido a aplicativo fraudulento
Serviços remotos externos (T1133)	Inscrição no Azure pela rede Tor
Manipulação de contas (T1098)	Redefinição incomum de senha de usuário do Azure



DISTRIBUIÇÃO DAS TÉCNICAS MITRE ATT&CK PARA GCP NO 4° TRIMESTRE DE 2022

1.	Contas válidas (T1078)	36%
2.	Execução por API (T0871)	18%
3.	Descoberta de contas (T1087.001) Manipulação de contas (T1098) Incapacitação de defesas (T1562) Modificação da infraestrutura de computação na nuvem (T1578) Serviços remotos (T1021.004)	9% cada

PRINCIPAIS DETECÇÕES DE GCP POR TÉCNICAS MITRE ATT&CK NO 4° TRIMESTRE DE 2022

Técnica MITRE ATT&CK	Regra
Contas válidas (T1078)	Criação de conta de serviço pelo GCP Atividade anômala de GCP Analytics Criação de chave de conta de serviço pelo GCP
Serviços remotos (T1021.004)	Regra de firewall do GCP permite todo tráfego em porta ssh
Manipulação de contas (T1098)	Política IAM de organização do GCP alterada
Descoberta de contas (T1087.001)	Alerta ["gcps net user"]
Transferência de dados para conta de nuvem (T1527)	Roteamento de log no GCP modificado
Modificação da infraestrutura de computação na nuvem (T1578)	Proteção contra exclusão do GCP desativada

REDAÇÃO E PESQUISA

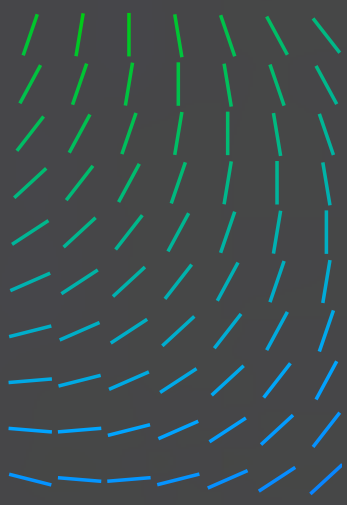
Alfred Alvarado
Henry Bernabe
Adithya Chandra
Dr. Phuc Duy Pham
Sarah Erman
John Fokker
Lennard Galang
Sparsh Jain
Daksh Kapoor
Maulik Maheta
João Marques
Tim Polzer
Srini Seethapathy
Rohan Shah
Vihar Shah
Swapnil Shashikantpa
Shyava Tripathi
Leandro Velasco

RECURSOS

Para acompanhar as ameaças mais recentes e mais impactantes identificadas pelo Trellix Advanced Research Center confira estes recursos:

TWITTER

Trellix ARC

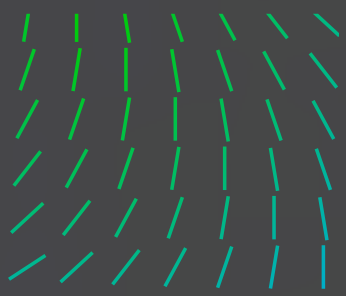


SOBRE O TRELLIX ADVANCED RESEARCH CENTER

O Trellix Advanced Research Center tem a proposta mais abrangente do setor de segurança cibernética e está na vanguarda dos métodos, tendências e perpetradores emergentes em todo o cenário de ameaças. Como parceiro preferencial de equipes de operações de segurança do mundo todo, o Trellix Advanced Research Center oferece inteligência e conteúdo de ponta para analistas de segurança, enquanto alimenta nossa plataforma de XDR.

SOBRE A TRELLIX

A Trellix é uma empresa global que está redefinindo o futuro da segurança cibernética e do trabalho abnegado. A plataforma aberta e nativa de detecção e resposta estendida (eXtended Detection and Response, XDR) ajuda as organizações confrontadas pelas ameaças mais avançadas da atualidade a ter confiança na proteção e na resiliência de suas operações. A Trellix, juntamente com um amplo ecossistema de parceiros, acelerou a inovação tecnológica através de autoaprendizagem e automação para capacitar mais de 40.000 clientes corporativos e governamentais com uma segurança viva. Mais em www.trellix.com/pt-br.



Visite Trellix.com para saber mais.

Trellix

Sobre a Trellix

A Trellix é uma empresa global que está redefinindo o futuro da segurança cibernética. A plataforma aberta e nativa de detecção e resposta estendida (eXtended Detection and Response, XDR) ajuda as organizações confrontadas pelas ameaças mais avançadas da atualidade a ter confiança na proteção e na resiliência de suas operações. Os especialistas de segurança da Trellix, juntamente com um amplo ecossistema de parceiros, aceleram a inovação tecnológica através de autoaprendizagem e automação para capacitar mais de 40.000 clientes corporativos e governamentais.

072022-05