Trellix | ABC Co.

RELATÓRIO DA ADVANCED THREAT RESEARCH

JAN/2022

Este relatório da equipe Advanced Threat Research é oferecido a você por cortesia de nosso parceiro.

RELATÓRIO

Trellix

RELATÓRIO DA ADVANCED THREAT RESEARCH

JAN/2022

RELATÓRIO

SUMÁRIO

03 CARTA DE NOSSO CIENTISTA-CHEFE

04 LOG4J

04 Log4j: a memória que sabia demais
04 Cronologia da Log4j
05 Ataque Log4j
05 Defesas da equipe ATR da Trellix contra a Log4j

06 RANSOMWARE

07 Resposta governamental a ameaças de ransomware
07 Detecções de famílias de ransomware

08 TÉCNICAS DE PADRÃO DE ATAQUE

08 Perpetradores de ameaças de APT
09 Ferramentas de APT

10 ADVANCED THREAT RESEARCH

10 Ameaças de ferramentas de ATR

11 AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

11 Países e continentes: T3 2021
11 Setores dos ataques: T3 2021
11 Vetores de ataque: T3 2021

12 APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE: T3 2021

12 Binários nativos do sistema operacional
13 Ferramentas administrativas

13 BUG REPORT

13 Insetos no para-brisa
14 Um momento de reflexão
14 Cupins

15 PESQUISAS E DADOS ADICIONAIS DO 3° TRIMESTRE DE 2021

15 Ransomware: Setores dos clientes, países dos clientes e técnicas MITRE ATT&CK
16 Técnicas de padrão de ataque (APT): Setores dos clientes, países dos clientes e técnicas MITRE ATT&CK
18 Advanced Threat Research (ATR): Setores dos clientes, países dos clientes e técnicas MITRE ATT&CK

20 RECURSOS

20 Twitter

No primeiro relatório de ameaças de nossa nova empresa, destacamos a questão Log4j que dominou não apenas as manchetes, mas também o foco de defensores e equipes de segurança corporativas.

Redação e pesquisa

Alfred Alvarado
Christiaan Beek
John Fokker
Douglas McKee
Tim Polzer
Steve Povolny
Raj Samani
Leandro Velasco

CARTA DE NOSSO CIENTISTA-CHEFE

Seja bem-vindo ao nosso novo relatório de ameaças e à nossa nova empresa.

Ao avaliarmos as perspectivas deste novo ano, precisamos reconhecer um cenário de ameaças que nos deixou a todos exaustos em decorrência de um fim de ano particularmente desafiador em 2021. No primeiro relatório de ameaças de nossa nova empresa, destacamos a questão Log4j que dominou não apenas as manchetes, mas também o foco de defensores e equipes de segurança corporativas. Também fazemos uma retrospectiva do terceiro e quarto trimestres de 2021, mas primeiramente vamos detalhar a variedade de recursos que disponibilizamos para ajudar você a combater a Log4j.

Fundamentalmente, conforme surgem mais detalhes sobre a ameaça Log4j, é imperativo conectar-se à nossa pesquisa e a nossos recursos atualizados para obter ajuda. Além do status do produto, nós monitoramos continuamente a presença de qualquer campanha ativa que aproveite essa vulnerabilidade e detalhamos o status de cobertura para as novas cargas virais.

Quando surgiram detalhes da vulnerabilidade Log4j, nós respondemos muito rapidamente disponibilizando assinaturas baseadas em rede e um relatório sobre a vulnerabilidade. Logo em seguida fornecemos ativos adicionais, detalhados neste relatório.

Para saber mais sobre a atividade atual da ameaça Log4j, bem como de outras ameaças predominantes, consulte nosso indispensável dashboard de ameaças.

Além disso, o blog Threat Labs da Trellix, onde você encontra nosso conteúdo mais recente sobre ameaças, vídeos e links para o boletim de segurança.

Naturalmente, a Log4j não é a única ameaça contra a segurança da sua empresa. Este relatório também destaca o espectro e a perturbação do ransomware e outras ameaças e ataques predominantes observados à solta.

Feliz 2022 e seja bem-vindo a uma nova empresa.

— Raj Samani
Associado e cientista-chefe

Twitter: @Raj_Samani

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

Seguindo o que está se tornando uma tradição ameaçadora, a nova vulnerabilidade Log4j, que afeta a amplamente utilizada biblioteca Log4j, foi lançada logo antes das festas de fim de ano. Descrita como a mais grave falha de segurança cibernética em décadas, ela colocou a Trellix e o setor de segurança cibernética para trabalhar intensamente no quarto trimestre de 2021. A vulnerabilidade Log4j ameaçava ter um impacto potencialmente devastador sobre qualquer produto que tivesse integrado a biblioteca Log4j em seus aplicativos e sites, incluindo produtos e serviços Apple iCloud, Steam, armazenamento do Samsung Cloud e muitos outros.

Nossa equipe vem acompanhando a Log4j de perto desde sua descoberta. Nós lançamos uma assinatura de rede KB95088 para usuários que utilizam Network Security Platform (NSP). A assinatura detecta tentativas de explorar CVE-2021-44228 via LDAP.
Essa assinatura pode ser expandida para incluir outros protocolos e serviços e assinaturas adicionais podem ser lançadas para complementar a cobertura.

Cronologia da Log4j

Segue uma cronologia breve da Log4j e de nossa pesquisa:

- **9 de dezembro** – A vulnerabilidade Log4j (CVE-2021-44228) foi lançada no Twitter, juntamente com uma PoC no Github para a biblioteca de logging Apache Log4j. O bug foi divulgado originalmente à Apache em 24 de novembro.
- **10 de dezembro** – Steve Povolny e Douglas McKee fizeram uma postagem de blog sobre a Log4j, com uma visão geral de suas descobertas iniciais. Nosso objetivo, a princípio, era determinar a facilidade de exploração utilizando-se a PoC pública, a qual reproduzimos e confirmamos. Isso foi feito utilizando-se o contêiner público Docker e uma arquitetura de cliente-servidor que usava tanto LDAP quanto RMI, bem como marshalsec, para explorar a versão 2.14.1 da Log4j.
- **14 de dezembro** – A vulnerabilidade da versão 1.2 da Log4j a ataques semelhantes por meio do componente JMSAppender foi confirmada e a CVE-2021-4104 foi emitida.
- **18 de dezembro** – Uma nova vulnerabilidade de negação de serviço (DOS) CVE-2021-45105 foi descoberta, afetando as versões 2.0-alpha1 a 2.16.0 da Log4j.

Consulte nossas postagens no blog Trellix Threat Labs e o dashboard de ameaças para ter acesso a nossas pesquisas mais recentes sobre como se defender contra a Log4j. Nossa equipe coleta e analisa informações de múltiplas fontes, abertas e fechadas, antes de divulgar relatórios de inteligência.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

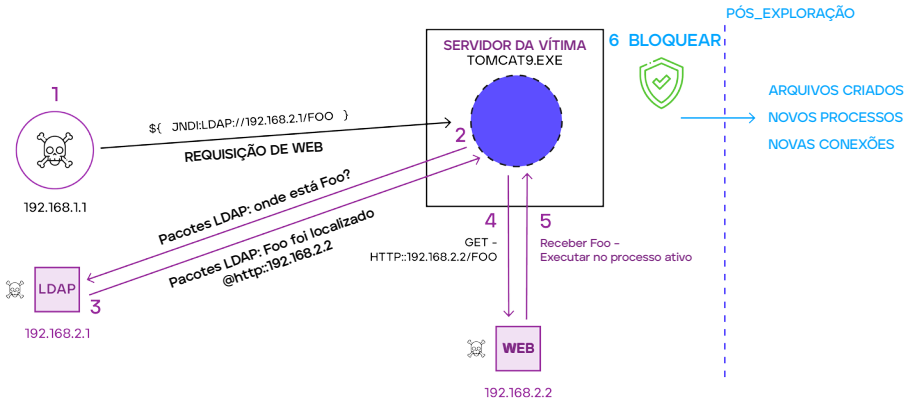
MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

Ataque Log4j

Nossa equipe rapidamente pesquisou e descreveu o que acontece na execução de um ataque Log4j comum baseado na Web:

FLUXO DE EXECUÇÃO DA LOG4J



- Etapa 1 – Um atacante envia uma sequência de caracteres específica para o servidor Web que está hospedando o aplicativo vulnerável. Essa sequência, como vimos, pode ser ocultada para contornar assinaturas baseadas em rede.
- Etapa 2 – O aplicativo reverte a ocultação da sequência de caracteres e a carrega na memória. Em seguida, o aplicativo inicia uma conexão LDAP para solicitar o endereço da localização da classe maliciosa.
- Etapa 3 – O servidor LDAP controlado pelo atacante responde com a localização do arquivo da classe maliciosa indicando o endereço URL HTTP no qual ele está hospedado.
- Etapa 4 – O aplicativo vulnerável inicia o download do arquivo da classe maliciosa.
- Etapa 5 – O aplicativo vulnerável carrega e executa o arquivo da classe maliciosa da etapa 4.

Defesas da equipe ATR da Trellix contra a Log4j

Para proteger um ambiente contra ataques como o da Log4j, uma estratégia em camadas, composta de segurança de rede aliada a varreduras de memória nos endpoints visados, permite que os defensores detectem e previnam efetivamente o fluxo de execução do ataque contra sistemas vulneráveis expostos através de vetores de rede. As reações Expert Rules (Regras de especialistas) e Custom Scan (Varredura personalizada) do ENS foram desenvolvidas para dar aos defensores essas capacidades, para que possam aplicar contramedidas precisas nessas ameaças emergentes.

O CISA.gov também oferece um mecanismo de varredura de Log4j para ajudar organizações a identificar serviços Web potencialmente vulneráveis afetados pelas vulnerabilidades Log4j.

CARTA DE NOSSO CIENTISTA-CHEFE
LOG4J: A MEMÓRIA QUE SABIA DEMAIS
RANSOMWARE
TÉCNICAS DE PADRÃO DE ATAQUE
ADVANCED THREAT RESEARCH
AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES
APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE
BUG REPORT
MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK
RECURSOS

RANSOMWARE

No terceiro trimestre de 2021, grupos de ransomware de alto perfil desapareceram, reapareceram, reinventaram-se e até tentaram mudar de nome, mas continuaram relevantes e predominantes como uma ameaça popular e potencialmente devastadora contra um leque cada vez maior de setores.

Muito embora a atividade de ransomware tenha sido denunciada e banida em diversos fóruns de criminosos cibernéticos no segundo trimestre de 2021, nossa equipe observou atividade entre os mesmos perpetradores de ameaças em vários fóruns, sob nomes alternativos.

Trellix contribui para prisões por ransomware e confisco de pagamentos de resgate

Em dezembro de 2021, a Trellix forneceu pesquisas que auxiliaram o FBI e a Europol na prisão de afiliados do REvil e no confisco de US$ 2 milhões em pagamentos de rasgate.

As tendências e campanhas de ransomware de maior destaque no terceiro trimestre de 2021 foram:

- BlackMatter – Essa ameaça de ransomware, descoberta perto do fim de julho de 2021, começou com um grupo forte de ataques que ameaçaram revelar dados pertencentes à empresa estadunidense de cadeia de fornecimento de produtos agrícolas New Cooperative. A New Cooperative relatou que suas capacidades de gerenciamento de cadeia de fornecimento e agendamento de alimentação de animais foram bloqueadas e estimou que 40% da produção de grãos nos EUA poderia ter sido prejudicada. Embora o BlackMatter tenha alegado utilizar as melhores partes de outros exemplares de malware, como GandCrab, LockBit e DarkSide, duvidamos muito que a campanha tenha sido administrada por um grupo novo de desenvolvedores. O malware BlackMatter tem muita coisa em comum com o malware DarkSide associado ao ataque contra a Colonial Pipeline.
- Nós divulgamos nossa convicção de que o grupo Groove está associado ao grupo Babuk, seja como ex-afiliado ou subgrupo.
- O grupo REvil/Sodinokibi assumiu a responsabilidade por infectar mais de um milhão de usuários por meio de um ataque de ransomware contra o provedor de software de serviços gerenciados Kaseya VSA. O pedido de resgate de US$ 70 milhões da Revil é o maior valor de resgate conhecido publicamente até hoje. Os resultados do ataque incluíram o fechamento forçado de centenas de supermercados por vários dias.
- O LockBit 2.0 surgiu em julho de 2021 e, eventualmente, listou mais de 200 vítimas em seu site de vazamento de dados.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

Resposta governamental a ameaças de ransomware

No terceiro trimestre, o governo dos EUA iniciou uma campanha proativa para reduzir o predomínio do ransomware com o lançamento da central StopRansomware.gov, oferecendo prêmios de até US$ 10 milhões por informações que identificassem ou localizassem perpetradores de ameaças patrocinados por governos e envolvidos em atividades cibernéticas contra infraestruturas críticas dos EUA.

Para saber mais sobre como esses exemplos de ransomware e novas campanhas podem ameaçar empresas nos próximos meses, leia as previsões de ameaças da Trellix para 2022.

Pesquisa de ransomware da Trellix

Para ajudar as empresas a compreender e a se defender melhor contra ataques de ransomware no cenário vigente, nossa equipe apresenta pesquisas e descobertas sobre o predomínio de uma ampla variedade de ameaças de ransomware, incluindo famílias, técnicas, países, setores e vetores.

Detecções de famílias de ransomware

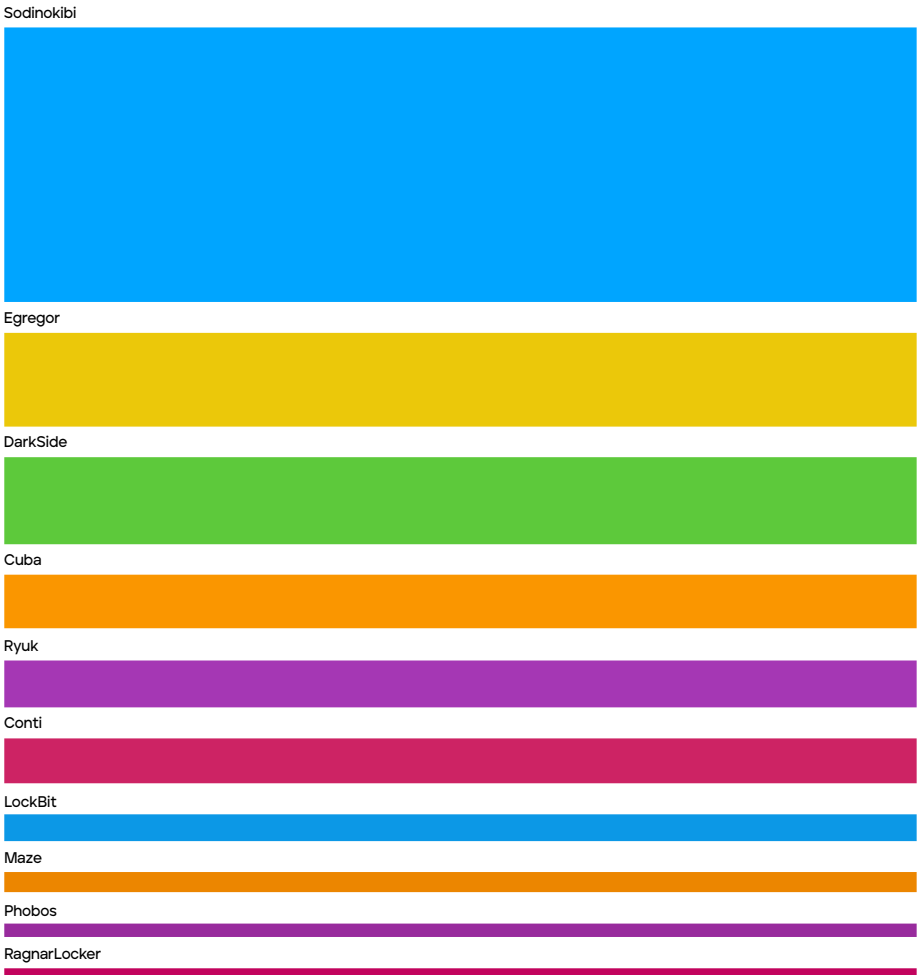


Figura 1. Sodinokibi (41%) foi a família de ransomware mais predominante das detectadas no terceiro trimestre de 2021, seguida pela DarkSide (14%) e pela Egregor (13%).

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

Veja a seguir os países dos clientes de ransomware, os setores dos clientes e as técnicas MITRE ATT&CK.

TÉCNICAS DE PADRÃO DE ATAQUE

A equipe rastreia e monitora campanhas de APT e seus indicadores e técnicas associados. A pesquisa de nossa equipe reflete perpetradores de ameaças, ferramentas, países dos clientes, setores dos clientes e técnicas MITRE ATT&CK das APT desde o terceiro trimestre de 2021.

Perpetradores de ameaças de APT



Figura 2. APT41 (24%) e APT29 (22%) foram os perpetradores de ameaças de APT mais predominantes no terceiro trimestre de 2021, tendo sido responsáveis por quase metade da atividade de APT monitorada.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

Ferramentas de APT

A equipe identificou indicadores de comprometimento pertencentes a campanhas de APT rastreadas com as seguintes ferramentas associadas. Grupos de APT são notórios por usar utilitários de sistema comuns para contornar controles de segurança e realizar suas operações:



Figura 3. Cobalt Strike (34%) foi a ferramenta de APT mais predominante detectada no terceiro trimestre de 2021, seguida por Mimikatz (27%), Net.exe (26%) e PsExec (20%). O pacote de ataque Cobalt Strike, utilizado por operativos governamentais, foi detectado em mais de um terço da atividade de APT.

Veja a seguir os países dos clientes de APT, os setores dos clientes e técnicas MITRE ATT&CK.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

ADVANCED THREAT RESEARCH

Nossa equipe rastreou as categorias das ameaças no terceiro trimestre de 2021. A pesquisa reflete percentuais de detecções por tipo de malware de ATR utilizado, países dos clientes, setores dos clientes, técnicas MITRE ATT&CK utilizadas nos ataques e setores da indústria.

Ameaças de ferramentas de ATR

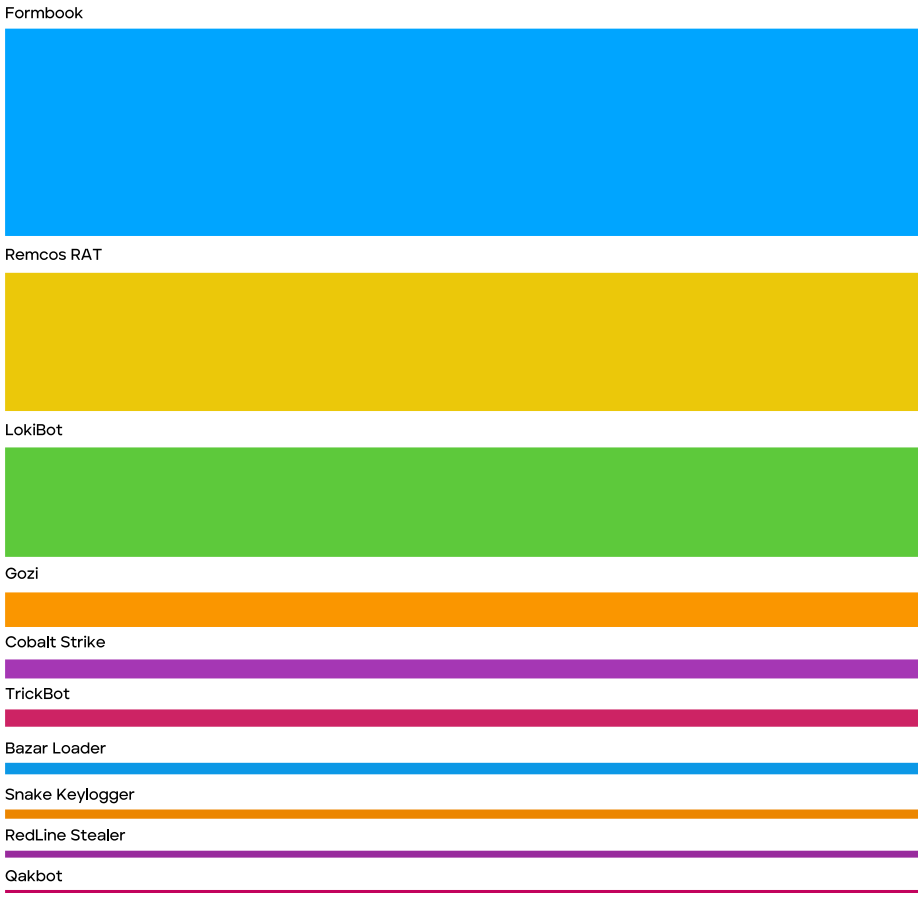


Figura 4. Formbook (36%), Remcos RAT (24%) e LokiBot (19%) foram responsáveis por quase 80% das detecções de ameaças de ferramentas de ATR no terceiro trimestre de 2021.

Veja a seguir os países dos clientes de ATR, os setores dos clientes e técnicas MITRE ATT&CK.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

Países e continentes: T3 2021

Aumentos notáveis em incidentes relatados publicamente contra países e continentes no terceiro trimestre de 2021 incluem:

- A América do Norte registrou o maior número de incidentes entre os continentes, mas teve uma redução de 12% do segundo para o terceiro trimestre de 2021.
- Os Estados Unidos tiveram o maior número de incidentes relatados no terceiro trimestre de 2021, mas os incidentes caíram 9% em relação ao segundo trimestre de 2021.
- A França registrou o maior aumento (400%) de incidentes relatados no terceiro trimestre de 2021.
- A Rússia teve a maior redução (-79%) de incidentes no terceiro trimestre de 2021 em comparação com o segundo trimestre de 2021.

Setores dos ataques: T3 2021

Dos incidentes relatados publicamente contra setores no terceiro trimestre de 2021, destacam-se:

- A categoria de diversos setores foi a mais frequentemente visada (28%), seguida pelos setores de saúde (17%) e público (15%).
- Aumentos notáveis do segundo para o terceiro trimestre de 2021 foram observados nos setores de finanças/seguros (21%) e saúde (7%).

Vetores de ataque: T3 2021

Dos incidentes relatados publicamente contra vetores no terceiro trimestre de 2021, destacamos o seguinte:

- Malware foi a técnica mais frequentemente utilizada nos incidentes relatados no terceiro trimestre de 2021, mas os incidentes de malware relatados caíram 24% em comparação com o segundo trimestre de 2021.
- Aumentos setoriais do segundo para o terceiro trimestre de 2021 incluem negação de serviço distribuída (112%) e ataque direcionado (55%).

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

Os criminosos cibernéticos utilizam as chamadas técnicas "Living off the Land" (LotL) que empregam software e funções legítimas em um sistema para realizar ações maliciosas nesse sistema. Com base nos eventos do terceiro trimestre, a Trellix identificou uma tendência nas ferramentas utilizadas por adversários que tentam continuar não sendo detectados. Embora grupos de ameaças patrocinados por governos e grandes grupos criminosos de ameaças tenham recursos para desenvolver ferramentas internamente, muitos recorrem a binários e a software instalado por administradores, que podem já estar presentes no sistema-alvo, para executar fases distintas de um ataque.

Para identificar binários nativos ou software utilizado administrativamente durante a fase de reconhecimento de um alvo de alto perfil, os adversários podem coletar informações sobre as tecnologias utilizadas a partir de anúncios de emprego, testemunhos de usuários anunciados por fornecedores ou um cúmplice dentro da empresa.

Binários nativos do sistema operacional		Comentários
PowerShell (41,53%)	T1059.001	O PowerShell é frequentemente utilizado para executar scripts e comandos de PowerShell.
Shell de comandos do Windows (CMD) (40,40%)	T1059.003	O shell de comandos do Windows é o principal utilitário de linha de comando do Windows e é frequentemente utilizado para executar arquivos e comandos em um fluxo de dados alternativo.
Rundll32 (16,96%)	T1218.011, T1564.004	Rundll32 pode ser utilizado para executar arquivos DLL locais, arquivos DLL de um compartilhamento, arquivos DLL obtidos na Internet e fluxos de dados alternativos.
WMIC (12,87%)	T1218, 1564.004	WMIC é uma interface de linha de comando para WMI que pode ser utilizada por adversários para executar comandos ou cargas virais localmente, em fluxos de dados alternativos ou em um sistema remoto.
Excel (12,30%)	T1105	Embora não seja instalado nativamente, muitos sistemas contêm software de planilhas e os adversários podem enviar para o usuário anexos contendo código malicioso ou scripts que, quando executados, podem ser utilizados para carregar cargas virais de uma localização remota.
Schtasks (11,70%)	T1053.005	Um adversário pode agendar tarefas que mantenham persistência, executem malware adicional ou realizem tarefas automatizadas.
Regsvr32 (10,53%)	T1218.010	Regsvr32 pode ser utilizado por adversários para registrar arquivos DLL, executar código malicioso e contornar listas brancas de aplicativos.
MSHTA (8,78%)	T1218.005	MSHTA pode ser utilizado por adversários para executar arquivos de JavaScript, JScript e VBScript que podem estar escondidos em arquivos HTA localmente e em fluxos de dados alternativos ou que tenham sido carregados de uma localização remota.
Certutil (4,68%)	T1105, 1564.004, T1027	Utilitário de linha de comando do Windows utilizado para obter informações sobre autoridade de certificação e para configurar serviços de certificados. Os adversários também podem utilizar o certutil para obter ferramentas e conteúdo remotos, codificar e decodificar arquivos e também acessar fluxos de dados alternativos.
Net.exe (4,68%)	T1087 e subtécnicas	Utilitário de linha de comando do Windows que permite a um adversário realizar tarefas de reconhecimento, como identificar usuários, rede e funcionalidade de serviços na máquina da vítima.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

Reg.exe *(4,10%)*	1003.002, 1564.004		Reg.exe pode ser utilizado por adversários para adicionar, modificar, excluir e exportar valores do Registro que podem ser salvos em fluxos de dados alternativos. reg.exe também pode ser utilizado para descarregar credenciais de um arquivo SAM.

Ferramentas administrativas			Comentários
Serviços remotos *(15,21%)*	T1021.001, T1021.004, T1021.005	AnyDesk ConnectWise Control RDP UltraVNC PuTTY WinSCP	Ferramentas de serviços remotos, tanto nativas do Windows quanto software de terceiros, podem ser utilizadas por adversários em conjunto com contas válidas para obter acesso a uma máquina ou infraestrutura remotamente, efetuar a implantação de ferramentas e malware, bem como vazar dados.
Utilitários de compactação *(4,68%)*	T1560.001	7-Zip WinRAR WinZip	Os adversários podem utilizar utilitários de compactação para compactar os dados coletados antes de transferi-los para fora, bem como para descompactar arquivos e executáveis.
PsExec *(4,68%)*	T1569.002		PsExec é uma ferramenta utilizada para executar comandos e programas em um sistema remoto.
BITSAdmin *(2.93%)*	T1105, T1218, T1564.004		BiTSAdmin é frequentemente utilizado para proporcionar persistência, limpar vestígios e invocar ações adicionais quando determinados critérios predefinidos são satisfeitos.
fodhelper.exe *(1,17%)*	T1548.002		Fodhelper.exe é um utilitário para Windows que pode ser utilizado por adversários para executar arquivos maliciosos com privilégios elevados na máquina da vítima.
ADFind *(0,59%)*	T1016, T1018, T1069 e subtécnicas, T1087 e subtécnicas, T1482		Utilitário de linha de comando que pode ser utilizado por adversários para descobrir informações do Active Directory, como confiabilidade de domínios, grupos de permissões, sistemas remotos e configurações de rede.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

BUG REPORT

Insetos no para-brisa

(Douglas McKee, engenheiro-chefe e pesquisador de segurança sênior, juntamente com outros blogueiros, rastreiam e analisam vulnerabilidades no relatório mensal Bug Report.)

Enquanto o mundo acelerava para chegar logo ao final de 2021, muitos "bugs" (insetos em inglês) atingiram nossos metafóricos para-brisas. Alguns saíram facilmente, enquanto outros deixaram marcas duradouras. A equipe rastreia e avalia novas vulnerabilidades (também conhecidas como bugs) todo mês, quando são lançadas, e informa o que "acha" que será de mais importância. Isso mesmo: não se trata de uma classificação OWASP ou pontuação CVSS, mas da velha impressão subjetiva baseada em anos de experiência.

Um momento de reflexão

Recapitulando os principais bugs que relatamos nos últimos meses, alguns se destacam dos demais. A Apache teve um ano difícil, com seu servidor Web (CVE-2021-41773) e o componente Log4j (CVE-2021-44228) sendo atingidos duramente por bugs impactantes. A Palo Alto também merece uma menção honrosa por um bug encontrado em seu produto GlobalProtect VPN (CVE-2021-3064), particularmente impactante durante uma pandemia global. Porém, coloquemos as coisas em perspectiva. A vulnerabilidade Log4j da Apache merece mais do que apenas o rótulo de "impactante" porque foi, indiscutivelmente, o maior bug de 2021 e, talvez, dos próximos anos. Se você vive em uma caverna e não ouviu falar sobre isso, recomendo ler nosso Bug Report de dezembro. Não se esqueça de voltar todo mês para conferir as novidades mais recentes sobre vulnerabilidades.

Então, o que faz desses bugs os piores já vistos? Basicamente, eles podem ser aproveitados remotamente, sem autenticação nas ferramentas situadas na borda da sua rede. Esses bugs podem ser o ponto de entrada inicial em uma rede, sem que o atacante tenha de "pescar" credenciais (via phishing), abrindo as portas para um ataque em escala maior.

Se o seu CISO gosta de jogar roleta russa e diz que você só pode aplicar correções em um único produto, recomendamos, sem sombra de dúvida, priorizar a vulnerabilidade Log4j porque ela é de fácil execução e tem sido explorada ativamente por elementos maliciosos. Embora a falha na VPN da Palo Alto seja grave e as VPNs venham apresentando um aumento de exploração desde 2020, ela fica atrás da Log4j e de outras vulnerabilidades da Apache por afetar uma versão antiga do software de VPN e por não estar sendo explorada ativamente.

Cupins

Alguns insetos, como os cupins, podem se infiltrar através de frestas e produzir efeitos devastadores.

Um bug de ampliação de privilégios locais no Microsoft Windows Installer Service, designado como CVE-2021-41379, foi o cupim de novembro. A Microsoft divulgou que o bug exige acesso local e supostamente o corrigiu com um patch oficial, mas a estratégia saiu pela culatra quando o patch não funcionou conforme esperado.

Com um patch falho e uma PoC disponível publicamente, malfeitores não perderam tempo para compilar isso em seus roteiros, conforme visto nos Insights. Para piorar a situação, nossa equipe viu versões armamentizadas dessa exploração sendo vendidas na Dark Web.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

Países dos clientes de ransomware



Figura 5. Clientes baseados nos Estados Unidos representaram mais de um terço do total de detecções de ransomware no terceiro trimestre de 2021.

Setores dos clientes visados pelo ransomware



Figura 6. Os setores bancário/financeiro (22%), de serviços públicos (20%) e de varejo (16%) representaram quase 60% do total de detecções de ransomware contra clientes no terceiro trimestre de 2021.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

Técnicas MITRE ATT&CK do ransomware



Figura 7. Entrada de dados (2,6%), descoberta de arquivo e diretórios (2,5%) e arquivos ou informações ocultados (2,4%) foram as principais técnicas MITRE ATT&CK de ransomware detectadas no terceiro trimestre de 2021.

Países dos clientes de APT



Figura 8. As detecções de técnicas de padrão de ataque por clientes da Turquia foram responsáveis por 17% do total de detecções no terceiro trimestre de 2021, seguidas por Estados Unidos (15%) e Israel (12%).

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

Setores dos clientes de APT



Figura 9. A maioria das detecções de APT no terceiro trimestre de 2021 ocorreram no setor bancário/financeiro (37%), seguido pelos setores de serviços públicos (17%), varejo (16%) e governamental (11%).

Técnicas MITRE ATT&CK de APT

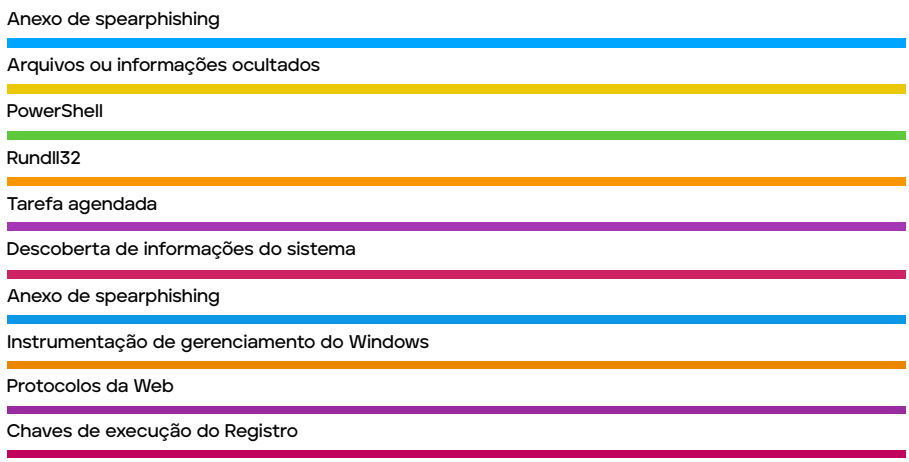


Figura 10. Anexo de spearphishing (16,8%), arquivos ou informações ocultados (16,7%) e PowerShell (16%) foram as técnicas MITRE ATT&CK de APT predominantes detectadas no terceiro trimestre de 2021.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

Países dos clientes de ATR

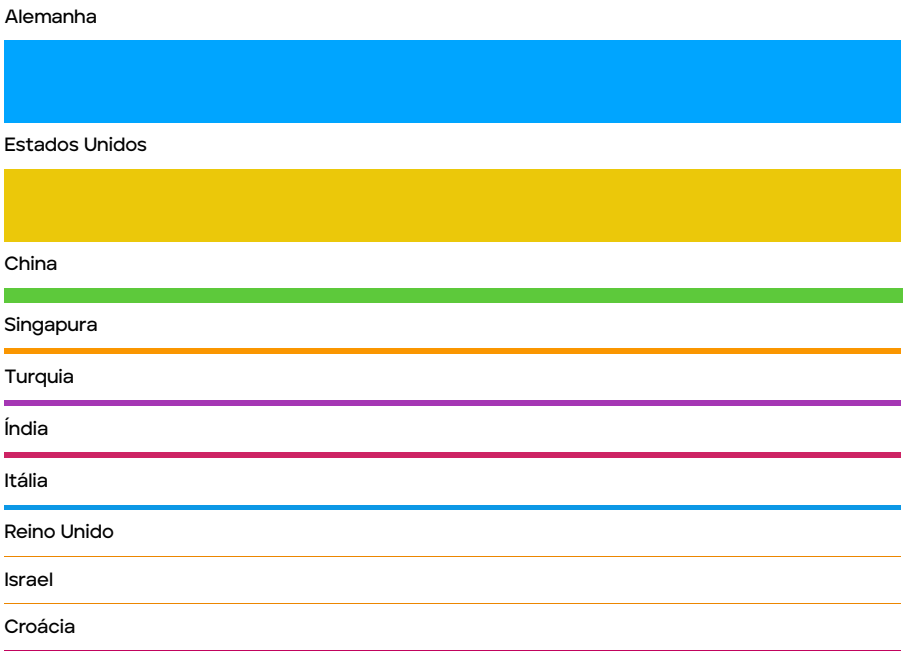


Figura 11. Mais da metade do total de ameaças por ferramentas de ATR detectadas no terceiro trimestre de 2021 foram na Alemanha (32%) e nos Estados Unidos (28%).

Setores dos clientes de ATR



Figura 12. As detecções de ATR em setores de clientes bancários/financeiros (45%) foram largamente predominantes no terceiro trimestre de 2021.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

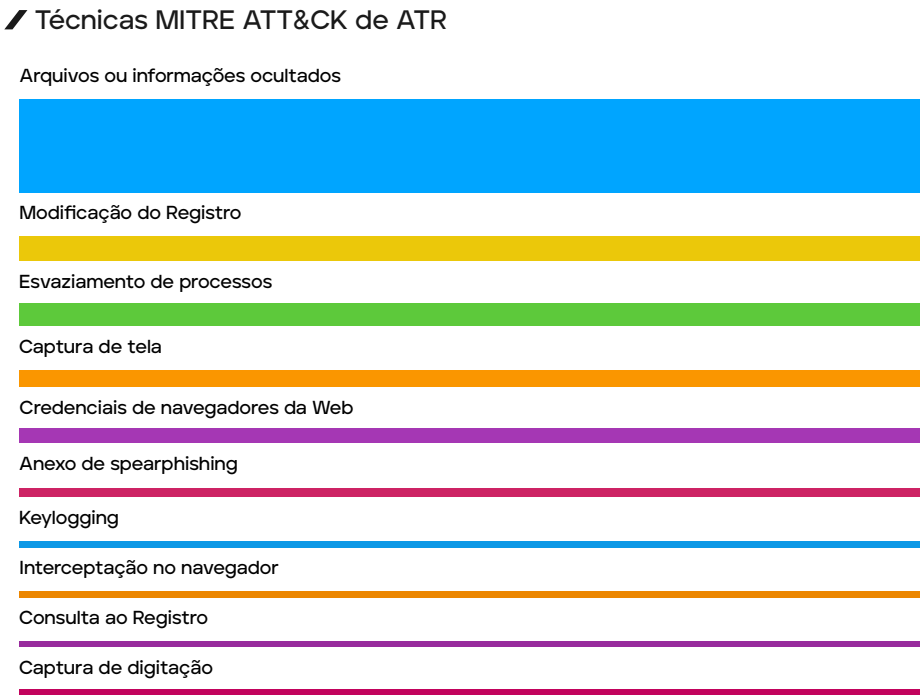


Figura 13. Arquivos ou informações ocultados chegaram a 5% de todas as detecções de técnicas MITRE ATT&CK de ATR no terceiro trimestre de 2021.

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

RECURSOS

Para acompanhar as mais recentes ameaças e pesquisas, consulte os recursos de nossa equipe:

Centro de ameaças — As ameaças mais impactantes da atualidade foram identificadas por nossa equipe.

Twitter:

Trellix Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Douglas McKee

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 ameças 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, acelera a inovação tecnológica através de autoaprendizagem e automação para capacitar mais de 40.000 clientes corporativos e governamentais. Saiba mais em www.trellix.com.

Trellix Threat Labs

Inscreva-se para receber informações sobre ameaças

CARTA DE NOSSO CIENTISTA-CHEFE

LOG4J: A MEMÓRIA QUE SABIA DEMAIS

RANSOMWARE

TÉCNICAS DE PADRÃO DE ATAQUE

ADVANCED THREAT RESEARCH

AMEAÇAS A PAÍSES, CONTINENTES, SETORES E VETORES

APROVEITAMENTO DA FUNCIONALIDADE EXISTENTE

BUG REPORT

MAIS SETORES DOS CLIENTES, PAÍSES DOS CLIENTES E TÉCNICAS MITRE ATT&CK

RECURSOS

Trellix

6220 American Center Drive,
San Jose, CA 95002

Copyright © 2022 Musarubra US LLC
JANEIRO DE 2022