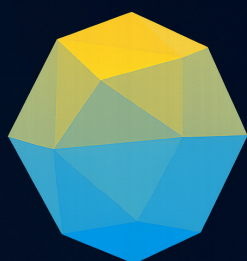

Relatório de Inteligência - RIT-001

Lumma Stealer Analysis

João Pedro Rosa Cezarino

September 15, 2025



**Threat
Intelligence**

Sumário

1	Introdução	2
2	Sumário	3
3	Pontos Chave	4
4	Detalhes da Ameaça	5
5	Diamond Model	6
5.1	Adversary	6
5.2	Infrastructure	6
5.3	Capability	6
5.4	Victim	7
6	Modus Operandi	8
7	Vítimas	10
8	Análise do Hash Encontrado	11
8.1	Classificação e Detecções	11
8.2	Infraestrutura Observada	11
8.3	Indicadores de Comportamento	12
9	Técnicas, Táticas e Procedimentos (TTPs)	13
10	Artifacts	14
10.0.1	Endpoint Artifacts	14
10.0.2	Network Artifacts	14
10.0.3	Malware Hashes	15
10.0.4	Vulnerabilities	15
11	Detecção	16
12	Recomendações	17
13	Conclusão	18
14	Referências	19

1 Introdução

- **ID:** RIT-001
- **Prioridade:** High
- **Autor:** João Pedro Rosa Cezarino
- **Título:** Lumma Stealer Analysis
- **Nível de Confiabilidade:** B2 - Usually reliable and Probably true.
- **Classificação da Informação:** TLP:GREEN

Este Relatório de Inteligência descreve as principais informações sobre a ameaça **Lumma Stealer** e tem como objetivo auxiliar na tomada de decisão dos riscos cibernéticos. A análise teve início a partir da investigação do hash **65eb366739361b97fb68c0ac4b9fbaad2ac26e0c30a21ef0ad0a756177e22e94**, identificado em diferentes fontes de Threat Intelligence, que serviu como ponto de partida para a correlação de indicadores, TTPs e infraestrutura adversária.

2 Sumário

O **Lumma Stealer**, também conhecido como **LummaC2**, é um malware do tipo Infostealer, identificado desde 2022, que opera sob um modelo de Malware-as-a-Service (MaaS). Desde Janeiro deste ano, observou-se um crescimento exponencial e uma sofisticação operacional, tornando-o um dos infostealers mais dominantes no mercado.

A relevância deste relatório reside na necessidade de compreender as diversas Táticas, Técnicas e Procedimentos (TTPs) empregadas pelo Lumma Stealer, que incluem o uso de sites falsos de CAPTCHA (ClickFix), malvertising e a exploração de plataformas legítimas para distribuição. Tornando-o um risco persistente para organizações em todos os Setores.

Suas capacidades visam o roubo de credenciais de navegadores, carteiras de criptomoedas e outros dados sensíveis e, portanto, a análise aprofundada da cadeia de infecção deste malware é crucial para fortalecer as defesas e proteger as organizações contra esta ameaça.

3 Pontos Chave

- Infostealer oferecido como MaaS desde 2022, focado em roubo de credenciais, cookies, carteiras de criptomoedas e tokens 2FA.
- Abusa de engenharia social (ex.: técnica **ClickFix** e sites falsos com CAPTCHAs), além de malvertising, phishing e software pirata.
- Atuação global, com forte presença na Europa, Américas e Ásia. Tem servido como ponto de acesso inicial para grupos de ransomware.
- Usa binários legítimos (LOLBINS), injeção de processos e técnicas de ofuscação para evitar detecção.
- Rede de C2 descentralizada, com uso de serviços como Cloudflare, Telegram e até Steam para comunicação.
- Mesmo após operações de derrubada, atores tendem a se reorganizar, mostrando alta resiliência no ecossistema de cibercrime.
- Adotar MFA resistente a phishing, Reforçar controles de endpoint, Treinar usuários contra phishing/engenharia social e Restringir a utilização de LOL-BINs estão entre as recomendações de proteção.

4 Detalhes da Ameaça

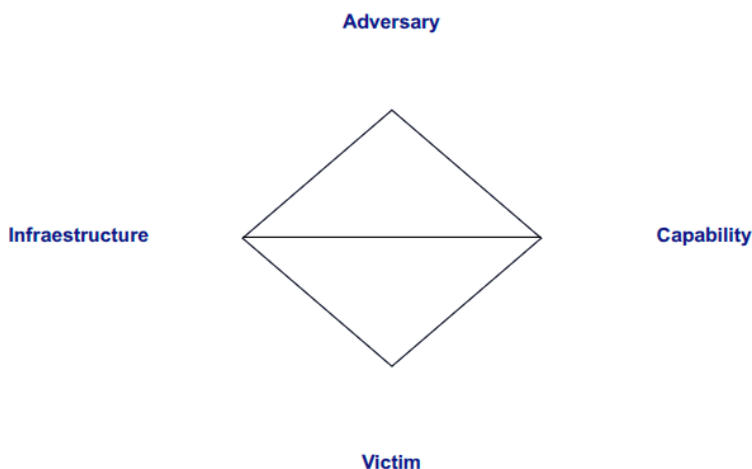
A função principal do Lumma Stealer é exfiltrar uma vasta variedade de dados sensíveis de máquinas de vítimas. O malware é escrito numa combinação de C++ e ASM, e é continuamente atualizado com funcionalidades avançadas para evadir a deteção e maximizar o roubo de dados. O seu modelo MaaS permite que afiliados personalizem e implementem o malware facilmente.

Os principais tipos de dados visados incluem:

- **Credenciais de Navegador:** Nomes de usuário, senhas, cookies e dados de preenchimento automático de mais de 10 navegadores web principais, incluindo Chrome, Firefox e Edge.
- **Carteiras de Criptomoeda:** Dados de numerosas aplicações de carteira de criptomoeda e extensões de navegador, como MetaMask, Electrum e Exodus.
- **Tokens de Autenticação de Dois Fatores (2FA):** Informações de extensões 2FA, como Authenticator, potencialmente permitindo que os atacantes contornem a autenticação multifator.
- **Informações do Sistema:** Dados detalhados sobre a máquina comprometida, incluindo informações da CPU, versão do SO, localidade do sistema e aplicações instaladas.
- **Dados de Aplicações:** Credenciais e dados de várias aplicações, incluindo clientes FTP, clientes de e-mail e aplicações de mensagens como Telegram, bem como AnyDesk ou KeePass.
- **Documentos Genéricos:** Ficheiros encontrados em perfis de usuários e outros diretórios comuns, especialmente aqueles com extensões .pdf, .docx ou .rtf.

O malware emprega uma cadeia de execução multi-estágio, frequentemente “fileless”, utilizando scripts PowerShell ofuscados e Binários “Living Off the Land” (LOLBINS) como mshta.exe para evadir a deteção. O Lumma Stealer é conhecido por usar “Binary Padding” (adição de dados inúteis para aumentar o tamanho do ficheiro e dificultar a análise) e “Indirect Control Flow” (cálculo dinâmico de endereços de salto) como técnicas de ofuscação. Observou-se também, que o Lumma Stealer pode usar “process hollowing” para injetar a sua carga maliciosa em processos legítimos do sistema como msbuild.exe, regasm.exe, regsvcs.exe e explorer.exe, disfarçando sua execução.

5 Diamond Model



5.1 Adversary

- **País:** Rússia.
- **Motivação:** Ganho financeiro (Malware-as-a-Service).
- **Plataformas utilizadas:** Fóruns clandestinos (RAMP, XSS) e Telegram.

5.2 Infrastructure

- **Entrega de payloads:** Bitbucket, GitHub e S3/CDN.
- **Servidores C2:** Diversos TLDs (.cyou, .shop, .biz, .xyz, .icu, .store, .click, etc.).
- **Hospedagem:** Cloudflare.
- **Serviços auxiliares:** FileZilla Servers, perfis falsos em plataformas legítimas.

5.3 Capability

- **Distribuição:** Phishing, malvertising, ClickFix e cracks de software.
- **Coleta de dados:** Credenciais de navegadores, cookies, carteiras de criptomoedas, tokens 2FA, informações de sistema, clipboard e dados financeiros.
- **Exfiltração:** Exfiltração via C2, bots Telegram.
- **Evasão:**
 - Uso de LOLBINs (mshta.exe, regasm.exe, msbuild.exe).
 - Injeção de processos (process hollowing).
 - Ofuscação avançada (control-flow, binary padding).

- Bypass AMSI, técnicas anti-sandbox/debug.
- Uso de AI/ML para evitar detecção e restaurar cookies expirados.

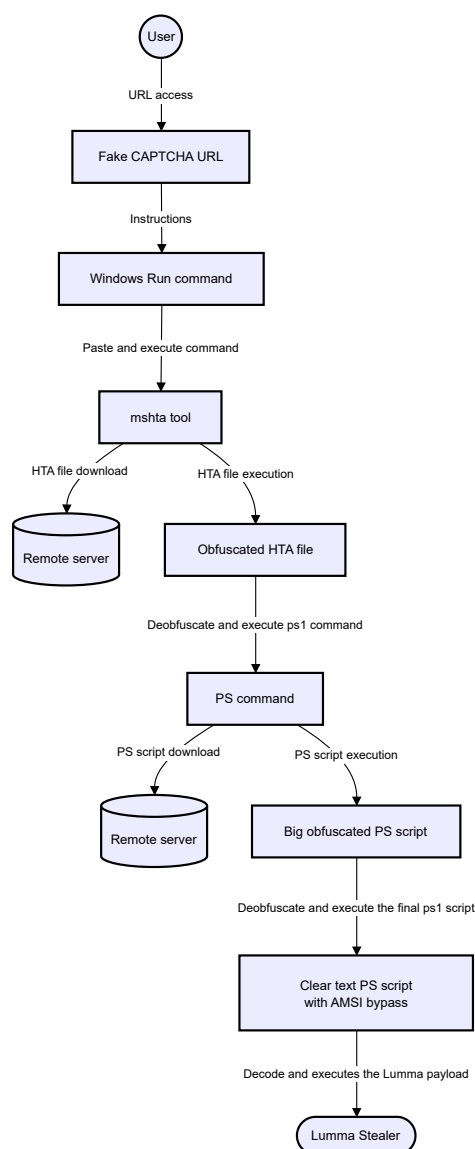
5.4 Victim

- **Regiões afetadas:** Europa, Américas (EUA, Brasil, Argentina, Colômbia), Ásia (Índia, Japão, Sudeste Asiático).
- **Setores principais:** Financeiro, Tecnologia, Saúde, Educação, Transporte e Manufatura.
- **Perfis visados:** Usuários domésticos e empresas exploradas por ransomware via acesso inicial.
- **Impacto:** Roubo de credenciais, movimentação lateral e suporte a operações de ransomware.

6 Modus Operandi

A cadeia de infecção do Lumma Stealer segue um fluxo bem definido de engenharia social e execução em múltiplos estágios, com forte uso de scripts ofuscados e abuso de ferramentas nativas do Windows (LOLBINS) para contornar mecanismos de defesa.

- **Estágio 1:** Página Falsa com CAPTCHA A vítima acessa um site malicioso (via phishing, malvertising ou links manipulados) que exibe um CAPTCHA falso. O usuário é instruído a copiar e colar um comando na caixa “Executar” do Windows, acreditando tratar-se de uma etapa de verificação legítima.
- **Estágio 2:** Execução Inicial via Windows Run + MSHTA O comando acionado pela vítima invoca o mshta.exe, um utilitário legítimo do Windows, que baixa e executa um ficheiro HTA ofuscado hospedado em um servidor remoto. Essa etapa serve como loader inicial para a cadeia de infecção.
- **Estágio 3:** PowerShell Obfuscado O HTA decompila e executa um comando PowerShell, também ofuscado. Esse PowerShell baixa um script PS1 maior e fortemente ofuscado, que contém mecanismos de bypass para evitar a detecção por antivírus.
- **Estágio 4:** Desofuscação e Execução da Carga Final O script PowerShell baixa e executa outro PS1 em texto claro, que finalmente decodifica e executa a carga útil do Lumma Stealer. Nesta fase, o malware já está implantado no sistema, pronto para roubar credenciais, carteiras de criptomoeda e outros dados sensíveis.

**Figure 1:** Lumma stealer infection chain

7 Vítimas

O Lumma Stealer apresenta uma distribuição global significativa, com **maior concentração de infecções na Europa, América do Norte e América do Sul**, especialmente no Brasil e nos Estados Unidos. O malware também mostra presença relevante em países da Ásia (como Índia, Japão e Sudeste Asiático), além de pontos de infecção na Oceania.

Entre os setores mais afetados, destacam-se: - **Serviços Financeiros e Bancários - Tecnologia e Software - Saúde - Educação - Energia e Manufatura**

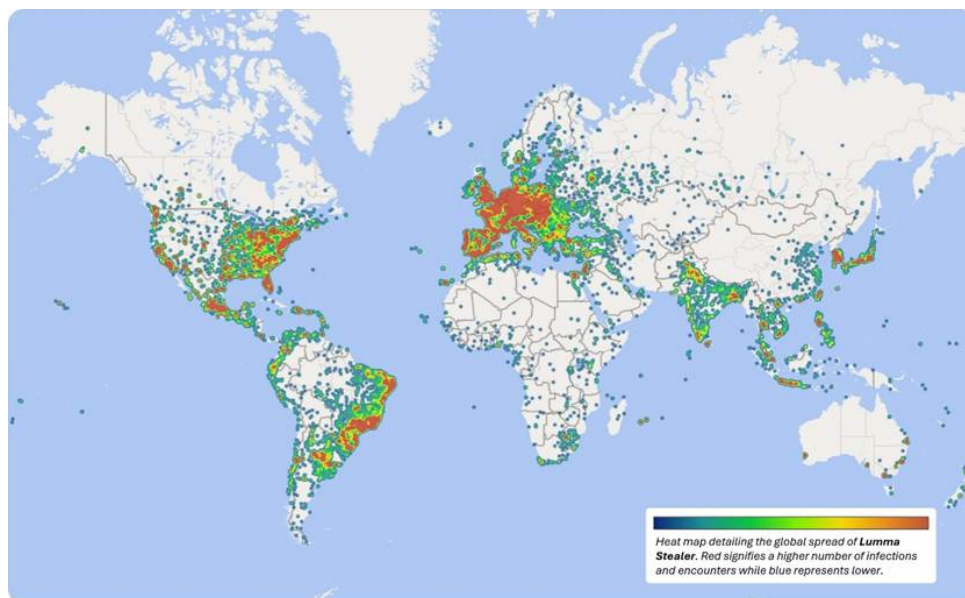


Figure 2: Mapa global de infecções atribuídas ao Lumma Stealer. Fonte: Microsoft

8 Análise do Hash Encontrado

Segue abaixo um breve compilado dos itens encontrados a partir da investigação do hash **65eb366739361b97fb68c0ac4b9fbaad2ac26e0c30a21ef0ad0a756177e22e94**.

- **MD5:** 45435e186d4136209f9af26548ae6a32
- **SHA-1:** 211d4f56edfa632a76d3a03c69898dcd2fb95259
- **Nome original:** Vertan.exe
- **Tamanho:** 1.18 MB
- **Tipo:** PE32+ Executable (Win64, console) - compilado em 2025-06-23 com Microsoft Visual C/C++.
- **Seções notáveis:**
 - .text de alta entropia (6.85) sugerindo ofuscação.
 - Presença de .gxf, uma seção incomum indicando potencial técnica anti-análise.
- **Primeira vez visto:** 23/06/2025
- **Última análise:** 05/08/2025

8.1 Classificação e Detecções

- **Detecção AV (VirusTotal):** 58/72 mecanismos classificaram como malicioso.
- **Principais nomes:** Trojan.Win.Crypt, TrojanPSW:Win64/Lumma, Spyware.Lumma.
- **Sandboxes externas:**
 - **Joe Sandbox:** LummaC Stealer (score 100/100).
 - **VMRay:** Injector, Spyware - evidência de exfiltração de credenciais.
 - **ANY.RUN:** execução maliciosa com conexões a múltiplos C2, tags telegram, lumma, stealer.
 - **MalwareBazaar:** classificado como Malware/LummaStealer.

8.2 Infraestrutura Observada

- **Domínios contatados:**
 - swenku.xyz/gaok, baviip.xyz/twiw, ropyj.xyz/zadf.
 - Domínios legítimos (MSN, Akamai) usados para **living-off-the-land**.
- **Endereços IP:**
 - 144.172.115.212 (US) - 14/95 engines detectaram.
 - 149.154.167.99 (GB) - vinculado ao Telegram C2.
 - Outros IPs Microsoft/Akamai possivelmente usados para camuflagem.
- **Canais de exfiltração:**

- Telegram bot.
- Conexão com domínios recém-registrados.

8.3 Indicadores de Comportamento

- **Persistência:** uso de Run Keys (HKCU\Software\Microsoft\Windows\Run).
- **Evasão:** process hollowing, uso de LOLBINs (mshta.exe, regasm.exe, explorer.exe).
- **Entrega:** arquivos .lnk duplos, pacotes hospedados em repositórios públicos.
- **Dropper:** criação de até **50 arquivos** adicionais em %Temp% durante execução.

Portanto, após a análise, conclui-se que o hash corresponde a uma amostra confirmada do **Lumma Stealer**, demonstrando forte capacidade de coleta de credenciais, uso do Telegram para exfiltração e uso de infraestrutura baseada em domínios descartáveis. O volume de detecções por diferentes AVs, aliado às observações em múltiplos sandboxes (Joe Sandbox, VMRay, ANY.RUN), validam a classificação como ameaça **crítica e persistente**, frequentemente utilizada como vetor de **acesso inicial para grupos de ransomware**.

9 Técnicas, Táticas e Procedimentos (TTPs)

Fase	Tática	Técnica	Procedimento	D3FEND
S1 Recon.	-	-	Temas/apps populares usados como isca	-
S2 Weapon.	Resource Dev.	Malware Dev (T1587.001)	Afiliado empacota Lumma com <i>crypters</i> /packers para evasão	-
S3 Delivery	Initial Access	Phishing: Link (T1566.002)	Links maliciosos (e-mail, malvertising, YouTube/GitHub)	D3-URLA
S4 Exploit.	Initial Access	User Exec: Malicious File (T1204.002)	Execução por usuário/ClickFix	D3-EFA
S5 Install.	Exec / Def. Ev.	PowerShell (T1059.001); Mshta (T1218.005); Obf. File (T1027)	Scripts ofuscados; abuso do LOLBIN mshta.exe	D3-PSA / D3-LONA
S6 C2	Command & Control	Web Protocols (T1071.001); File Sharing (T1071.004)	C2 via HTTP(S) POST; uso de Telegram API para exfiltração	D3-OTF
S7 Actions	Credential Access	Browser Creds (T1555.003)	Roubo de cookies/senhas/-tokens em navegadores	D3-FPA

10 Artifacts

10.0.1 Endpoint Artifacts

Tipo	Descrição	MITRE TTP's
Chave de Registo	HKCU\Software\Microsoft\Windows\Run	Persistência - T1547.001
Ficheiro Caído	%AppData%\Roaming\lumma\client.exe	Execução, Persistência - T1059
Ficheiro Caído	%AppData%\Local\Temp*.accde	Execução, Evasão - T1059, T1027
Ficheiro Caído	%AppData%\Local\Temp\Mars.accde.bat	Script batch para gerar executáveis
Ficheiro Caído	%AppData%\Local\Temp\Alexander.com	Executável AutoIT compilado
Ficheiro Caído	%AppData%\Local\Temp\o.a3x	Script AutoIT compilado

10.0.2 Network Artifacts

Tipo	Descrição
User-Agent	TeslaBrowser/5.5
Domínio C2	swenku[.]xyz
Domínio C2	baviip[.]xyz
Domínio C2	ropyj[.]xyz
Domínio C2	dogalmedical[.]org
URL Maliciosa	hxxps://payment-confirmation.82736[.]store/pgg46

Tipo	Descrição
URL Mali- ciosa	hxxps://booking[.]proceede-verific[.]com/goo_pdf
URL Mali- ciosa	.robazumuxi.com
URL Mali- ciosa	.berapt-medii.com

10.0.3 Malware Hashes

Tipo	Hash do Arquivo	Descrição
SHA256	65eb366739361b97fb68c0ac4b9fbaad2ac26e0c30a21ef0ad0a756177e22e94	Lumma Stealer v4
SHA256	7b3bd767ff532b3593e28085940646f145b9f32f2ae97dfa7cdd652a6494257d	Lumma Stealer variante
SHA256	ba09a680cc482c7004f3c1936f66f5c9305df04315e950119fb8b013b6e08f13	Amostra analisada (Ver-tan.exe)
SHA1	ec69088d1409444de60c3c6aba5021194839d7ba	Executável Lumma
SHA1	2c8ec98431a788f18f1865cc7d742deb741a927b3	Script AutoIT .a3x
SHA1	d7cd79911d2fbb575777b26ecf32da109d65291f	Script .bat
SHA256	bfdffcee5951982691af1678f899b39b851b6fd3167d3354c62385fb9b7eac02	Lumma Stealer - família

10.0.4 Vulnerabilities

CVE #	CVSS	Patch (S/N)	Remediation	Date Reported
CVE-2017-11882	7.8	S	Aplicar patch Microsoft Office KB2553204	2017-11-15
CVE-2021-40444	8.8	S	Bloquear controles ActiveX, aplicar patch MS	2021-09-07

11 Detecção

Tipo	Nome (com link)	Descrição
Sigma	Lumma - ClickFix (PowerShell Encoded)	Uso de PowerShell com comandos codificados/ocultos típicos do <i>ClickFix</i> .
Sigma	Lumma - Mshta Execução Remota	Execução de mshta.exe para carregar conteúdo remoto/HTA malicioso.
Sigma	Lumma - Persistência Run Key	Criação de chaves em HKCU\Software \Microsoft \Windows \Run .
Sigma	Lumma - Acesso a Bancos de Navegador	Acesso suspeito a bases de credenciais/cookies.
Sigma	Lumma - Exfiltração HTTP(S)	Tráfego POST suspeito com URIs/User-Agents maliciosos.
YARA	MAL_Lumma_Generic_v1	Strings típicas (creds, AMSI bypass) em disco/memória.
YARA	MAL_ClickFix_HTA_AutoIt	Payloads HTA/AutoIt usados em ClickFix.
YARA	MAL_Lumma_Config_IOCs	Artefatos: \%AppData\%, URIs /gate, /c2, Telegram API.

12 Recomendações

1. **Conscientização do usuário:** Educar os colaboradores para reconhecer phishing, malvertising e táticas de engenharia social como o “ClickFix”. Enfatizar a cautela ao baixar software de fontes não confiáveis ou executar comandos a partir de sites.
2. **Solução EDR (Endpoint Detection and Response):** Implementar e configurar uma solução EDR para monitorar comportamentos anômalos de processos.
3. **Restringir a execução de scripts:** Utilizar políticas de controle de aplicações para restringir o PowerShell e outras linguagens de script aos usuários que realmente precisem delas para suas funções.
4. **Filtragem de rede:** Bloquear conexões a domínios maliciosos conhecidos e a domínios recentemente registrados, frequentemente usados para infraestrutura de C2. Usar filtragem DNS e gateways web para prevenir acesso a sites de distribuição de malware.
5. **Higiene de credenciais:** Incentivar o uso de gerenciadores de senhas em vez de armazenar credenciais nos navegadores. Exigir Autenticação Multifator (MFA) em todos os serviços críticos para mitigar o impacto de credenciais roubadas.
6. **Atualizações regulares de software:** Manter sistemas operacionais, navegadores e demais softwares atualizados e com patches para proteger contra vulnerabilidades que possam ser exploradas em ataques multiestágio.
7. **Autenticação resistente a phishing:** Utilizar métodos de autenticação resistentes a phishing, como tokens FIDO ou chaves de acesso (passkeys) com Microsoft Authenticator (quando suportado).

13 Conclusão

O Lumma Stealer representa uma ameaça madura e resiliente dentro do ecossistema do cibercrime, ampliada pelo seu modelo acessível de MaaS. Sua dependência de engenharia social sofisticada e de técnicas de execução evasivas o torna um perigo capaz de contornar defesas tradicionais baseadas em assinaturas. As organizações devem adotar uma postura de segurança em múltiplas camadas que combine controles técnicos avançados com uma educação robusta dos usuários para mitigar de forma eficaz o risco de roubo de credenciais e o subsequente comprometimento da rede. É crucial utilizar ferramentas de inteligência de ameaças para identificar indicadores de comprometimento e bloquear o tráfego de saída para domínios suspeitos.

14 Referências

1. Forcepoint. [Unmasking the Lumma Stealer Campaign.](#)
2. Netskope. [Lumma Stealer: Fake CAPTCHAs & New Techniques to Evade Detection.](#)
3. Netskope Threat Labs. [LummaStealer IOCs.](#)
4. Microsoft Security. [Lumma Stealer: Breaking down the delivery techniques and capabilities of a prolific infostealer.](#)
5. Trellix. [A Deep Dive into the Latest Version of Lumma InfoStealer.](#)
6. Darktrace. [The Rise of the Lumma Info-Stealer.](#)
7. G DATA Software. [LummaStealer: Fake reCAPTCHA leads to info stealer infection.](#)
8. WithSecure Labs. [Reverse Engineering a Lumma Infection.](#)



Threat
Intelligence