# Relatório de Inteligência - RIT-001

Lumma Stealer Analysis

João Pedro Rosa Cezarino

September 12, 2025

Threat Intelligence

## Summary

# 1 Introdução

- **Report ID:** RIT-001
- **Date:** 09/09/2025
- **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 `65eb366739361b97fb68c0ac4b9fbaad2ac26e0` 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, 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 criptomoeda e outros dados sensíveis e, portanto, a análise aprofundada da cadeia de infeção deste malware é crucial para fortalecer as defesas e proteger as organizações contra esta ameaça.

## 3 Pontos Chave

- **O que é**: Infostealer oferecido como MaaS desde 2022, focado em roubo de credenciais, cookies, carteiras de criptomoedas e tokens 2FA.
- **Disseminação**: Abusa de engenharia social (ex.: técnica ClickFix e sites falsos com CAPTCHAs), além de malvertising, phishing e software pirata.
- **Escopo e Alvos**: Atuação global, com forte presença na Europa, Américas e Ásia. Tem servido como ponto de acesso inicial para grupos de ransomware.
- **Evasão**: Usa binários legítimos (LOLBINs), injeção de processos e técnicas de ofuscação para evitar detecção; consegue burlar o AMSI.
- **Infraestrutura**: Rede de C2 resiliente e descentralizada, com uso de serviços como Cloudflare, Telegram e até Steam para comunicação.
- **Persistência**: Mesmo após operações de derrubada, atores tendem a se reorganizar, mostrando alta resiliência no ecossistema de cibercrime.
- **Recomendações**:
  - Adotar MFA resistente a phishing.
  - Reforçar controles de endpoint (EDR em modo bloqueio).
  - Treinar usuários contra phishing/engenharia social.
  - Restringir LOLBINs para perfis não técnicos.
  - Bloquear tráfego para TLDs/domínios maliciosos conhecidos.

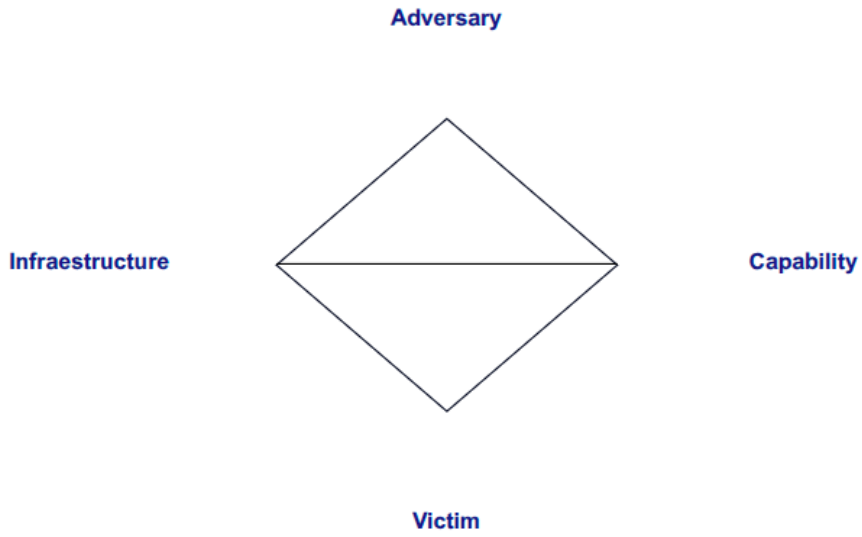
# 4 Detalhes da Ameaça

A função principal do Lumma Stealer é recolher e 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 utilizador, 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 de Utilizador: Ficheiros encontrados em perfis de utilizador 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. Também pode usar “Dispatcher Blocks” para controlar dinamicamente a execução. Observou-se 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 a execução

# 5 Diamond Model




## 5.1 Adversary

- **País**: Rússia
- **Motivação**: Ganho financeiro (Malware-as-a-Service)
- **Persona**: Shamel (desenvolvedor e operador principal)
- **Plataformas utilizadas**: Fóruns clandestinos (RAMP, XSS), Telegram, Gitbook, usrlink.io
- **Atores consumidores**: Stargazers Network, UNC5537, UNC4536, Water Hydra APT
- **Perfil**: Operador experiente, com foco em monetização e persistência no ecossistema de cibercrime

## 5.2 Infrastructure

- **Entrega de payloads**: Bitbucket, GitHub, S3/CDN, arquivos `.lnk` duplos, paste services (ex.: `nentry.co`)
- **Servidores C2**: Diversos TLDs (.cyou, .shop, .biz, .xyz, .icu, .store, .click, etc.)

- **Hospedagem**: Cloudflare, Steam Profiles para resolução de domínios, Dynadot & Namecheap (out/2024)

- **Serviços auxiliares**: FileZilla Servers, perfis falsos em plataformas legítimas

### 5.3 Capability

- **Distribuição**: Phishing, malvertising, ClickFix, cracks de software, e-mails maliciosos

- **Coleta de dados**: Credenciais de navegadores, cookies, carteiras de criptomoedas, tokens 2FA, informações de sistema, clipboard e dados financeiros

- **Exfiltração**: HTTP/HTTPS POST para C2 dinâmicos, bots Telegram, SOCKS5 manager, decriptação server-side

- **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, Manufatura

- **Perfis visados**: Usuários domésticos (gamers, entusiastas de software/IA, OnlyFans users), empresas exploradas por ransomware via acesso inicial

- **Impacto**: Roubo de credenciais, movimentação lateral, suporte a operações de ransomware (Akira, RansomHub, Hellcat)

# 6 Modus Operandi

A cadeia de infeção do Lumma Stealer frequentemente começa quando a vítima visita um site que a redireciona para uma página falsa de CAPTCHA. A vetor de ataque inicial pode ser e-mails de phishing ou malvertising. Uma vez na página falsa de CAPTCHA, o utilizador é instruído a realizar uma sequência de ações que leva à execução da próxima fase da cadeia de infeção. Um método de entrega particularmente eficaz é a técnica "ClickFix", onde as vítimas são enganadas por páginas falsas de CAPTCHA para colar e executar comandos maliciosos na caixa de diálogo "Executar" do Windows, contornando os controlos de segurança baseados no navegador. Esta técnica de engenharia social exibe mensagens de erro falsas para enganar os utilizadores a executar comandos maliciosos nos seus próprios sistemas. Os comandos geralmente descarregam e executam o Lumma diretamente na memória, usando codificação Base64 e cadeias de entrega furtivas.

A cadeia de infeção pode incluir: - Estágio 1: Link de Confirmação de Reserva Falsa que Leva à Verificação de CAPTCHA Falsa: A vítima visita um site, possivelmente através de um e-mail de phishing. O link redireciona para uma página que contém um documento borrado do booking.com, com um CAPTCHA falso que exige que o utilizador clique na caixa "Não sou um robô". - Estágio 2: Script PHP Obfuscado: Copia Script PowerShell para a Área de Transferência: O código-fonte da página revela um script JS que carrega um comando de um script PHP ofuscado e encriptado com ROT13. Após a desencriptação, o script JS copia um comando Base64 para a área de transferência da vítima. - Estágio 3: Mecanismo de Download da Carga Útil: O código Base64 desencriptado, a ser colado na caixa "Executar" do Windows, invoca um script PowerShell codificado em Base64. Este script descarrega um ficheiro para o diretório Temp e executa-o. As amostras do Lumma Stealer nesta fase são significativamente maiores, até 350% (de 2MB para 9MB), e são disfarçadas de instaladores legítimos para evitar a deteção. - Estágio 4: Carga Útil do Lumma Stealer: O ficheiro da carga útil do Lumma Stealer muda ao longo do tempo. As amostras recolhidas utilizam "Binary Padding" e "Indirect Control Flow" para dificultar a análise e a deteção por ferramentas de segurança. O malware também pode empregar a técnica "Heaven's Gate", que envolve saltos para segmentos de código de 64 bits para executar chamadas de sistema, antes de regressar ao código de 32 bits.

As amostras analisadas pela Netskope mostraram o uso de uma ferramenta de código aberto para contornar a Windows Antimalware Scan Interface (AMSI), removendo a string "AmsiScanBuffer" da memória do módulo "clr.dll", evitando que a carga final seja verificada pelo AMSI.

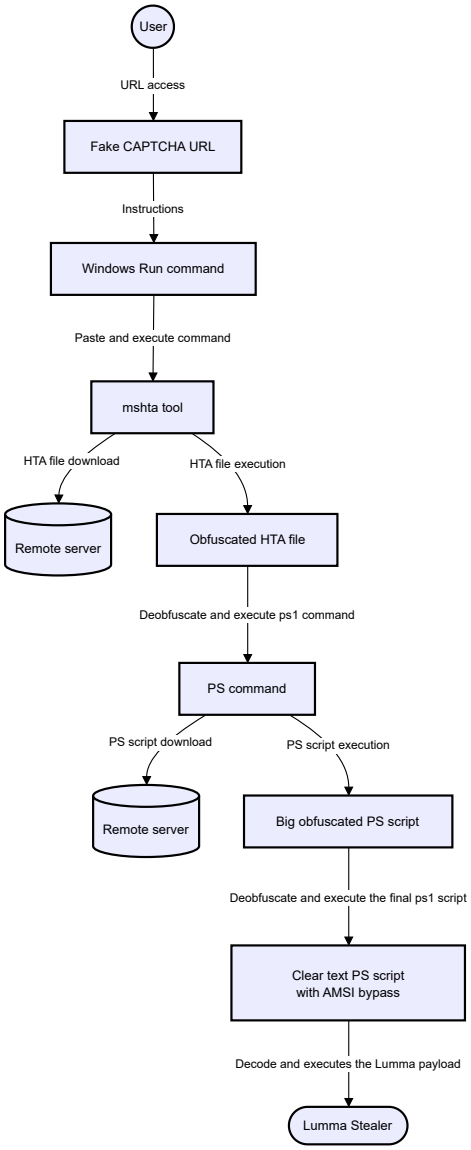



**Figure 1:** Lumma stealer infection chain

# 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**

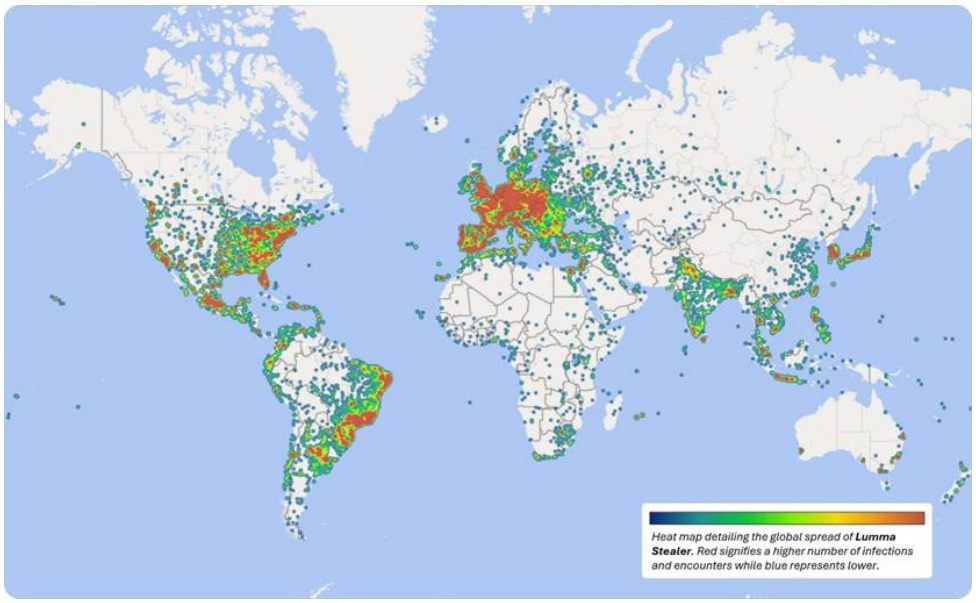



**Figure 2:** Mapa global de infecções atribuídas ao Lumma Stealer. Fonte: [Microsoft](https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/)

# 8 Análise do Hash Encontrado

**Hash principal analisado:**
`ba09a680cc482c7004f3c1936f66f5c9305df04315e950119fb8b013b6e08f13`

- **MD5**: 45435e186d4136209f9af26548ae6a32
- **SHA-1**: 211d4f56edfa632a76d3a03c69898dcd2fb95259
- **SHA-256**: ba09a680cc482c7004f3c1936f66f5c9305df04315e950119fb8b013b6e08f13
- **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 `.gxfg` — 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, Win64:Stealer.Lrt, Spyware.Lumma
  - Fortinet: W64/GenKryptik.HUOTU
  - Kaspersky: Trojan-PSW.Win32.Lumma.mtv
- **Sandboxes externas**:

  - **Joe Sandbox**: LummaC Stealer (score 100/100) – comunicação com `t.me/vstalnasral555`, `swenku.xyz` e `baviip.xyz`
  - **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** (`t.me/vstalnasral555`)
  - HTTP(S) POST para 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

O hash analisado corresponde a uma amostra confirmada do **Lumma Stealer**, categorizada como **infostealer distribuído como MaaS**. Sua análise demonstra forte capacidade de coleta de credenciais (navegadores, carteiras cripto, tokens 2FA), uso de **Telegram para exfiltração** e ampla infraestrutura baseada em domínios descartáveis.
O volume de detecções por diferentes AVs, aliado às observações em múltiplos sandboxes (Joe Sandbox, VMRay, ANY.RUN), consolidam sua classificação como ameaça **crítica e persistente**, frequentemente utilizada como vetor de **acesso inicial para grupos de ransomware**.

# 9 Técnicas, Táticas e Procedimentos (TTPs)

| Kill Chain Stage | Tactic | Technique | Procedure (Concise) | D3FEND |
|---|---|---|---|---|
| **S1 Reconnaissance** | - | - | Identificação de softwares/temas populares para atrair vítimas | - |
| **S2 Weaponization** | - | - | Afiliado empacota carga Lumma usando crypters | - |
| **S3 Delivery** | Initial Access | Phishing (T1566.002) | Links maliciosos via e-mail, malvertising, YouTube, GitHub | D3-URLA |
| **S4 Exploitation** | Initial Access | User Execution (T1204.002) | Execução de arquivo malicioso ou ClickFix | D3-EFA |
| **S5 Installation** | Execution | PowerShell (T1059.001), Mshta (T1218.005) | Scripts ofuscados e LOLBIN mshta.exe | D3-PSA / D3-LONA |
| **S6 C2** | C2 | Web Protocols (T1071.001) | Comunicação com servidor C2 via HTTP/HTTPS POST | D3-OTF |
| **S7 Actions on Obj.** | Credential Access | Browser Creds (T1555.003) | Roubo de cookies e senhas de navegadores | D3-FPA |

# 10 Artifacts

### 10.0.1 Endpoint Artifacts

| Tipo | Descrição | Tática / Técnica MITRE | Fonte |
|---|---|---|---|
| Chave de Registo | `HKCU\Software\Microsoft\Windows\Run` | Persistência – T1547.001 | VT/Análise Sandbox |
| Ficheiro Caído | `%AppData%\Roaming\lumma\client.exe` | Execução, Persistência – T1059 | VT |
| Ficheiro Caído | `%AppData%\Local\Temp\*.accde` | Execução, Evasão – T1059, T1027 | Sandbox |
| Ficheiro Caído | `%AppData%\Local\Temp\Mars.accde.bat` | Script batch para gerar executáveis | Sandbox |
| Ficheiro Caído | `%AppData%\Local\Temp\Alexander.com` | Executável AutoIT compilado | VT / Joe Sandbox |
| Ficheiro Caído | `%AppData%\Local\Temp\o.a3x` | Script AutoIT compilado | Forcepoint IOC |
| Injeção de Processo | Injeção em `msbuild.exe`, `regasm.exe`, `regsvcs.exe`, `explorer.exe` | Evasão – T1055 | VT / Sandboxes |

### 10.0.2 Network Artifacts

| Tipo | Descrição | Fase do Kill Chain | Fonte |
|---|---|---|---|
| HTTP POST | Exfiltração de dados para C2 via URIs como `/c2sock` e User-Agent `TeslaBrowser/5.5` (parâmetro `act=life`) | C2, Exfiltração – T1041, T1071.001 | VT / Forcepoint |

| Tipo | Descrição | Fase do Kill Chain | Fonte |
|---|---|---|---|
| Telegram API | Bot usado para uploads de credenciais via `t.me/vstalnasral555` e canais associados | C2 – T1102.002 | ANY.RUN / Joe Sandbox |
| Domínios C2 | `swenku[.]xyz`, `baviip[.]xyz`, `ropyj[.]xyz`, `dogalmedical[.]org`, além de TLDs descartáveis como `.shop`, `.icu`, `.store`, `.click` | C2 – T1071.001 | VT / MalwareBazaar |
| URLs Maliciosas | `hxxps://payment-confirmation.82736[.]store/pgg46`, `hxxps://booking[.]procedeed-verific[.]com/goo_pdf`, links encurtados e redirecionamentos em `.robazumuxi.com`, `.berapt-medii.com` | Entrega – T1566 | Forcepoint / VT |
| Plataformas Abusadas | Conexões legítimas para `steamcommunity.com` e `api.msn.com` utilizadas para camuflagem | C2 / Evasão – T1071 | VT / ANY.RUN |

### 10.0.3 Malware Hashes

| Tipo | Hash do Ficheiro | Descrição | Fase do Kill Chain | Fonte |
|---|---|---|---|---|
| SHA256 | 66eb366739361b97fb68c0ac4b9fbaad2ac26[illegible] | Lumma Stealer v4 | C2 – T1547, T1071 | Netskope / VT |
| SHA1 | `7b3bd767ff532b3593e28085940646f145b9` | Lumma Stealer variante | Instalação, C2 | VT |
| SHA256 | 5609a680cc482c7004f3c1936f66f5c9305df[illegible] | Amostra analisada (Vertan.exe) | Exfiltração | VT / Joe Sandbox |

| Tipo | Hash do Ficheiro | Descrição | Fase do Kill Chain | Fonte |
|---|---|---|---|---|
| SHA1 | ec69088d1409444de60c3c6aba5021194839 | Executável Lumma | Instalação | VT |
| SHA1 | 2c8ec98431a788f18f1865c7d742deb741a925b3 | Script AutoIT .a3x | Execução | Forcepoint IOC |
| SHA1 | d7cd79911d2fbb575777b26ecf32da1d0965 | Script .bat | Instalação | MalwareBazaar |
| SHA256 | b6dffcee5951982691af1678f899b39b851b6f[illegible] | Executável Lumma família | Instalação, C2 | VT |

### 10.0.4 Vulnerabilities

| CVE # | CVSS Score | Patch Available (Y/N) | Remediation | Date Reported | Patch Applied (Y/N/N/A) |
|---|---|---|---|---|---|
| CVE-2017-11882 | 7.8 | S | Aplicar patch Microsoft Office KB2553204 [67] | 2017-11-15 | N/A |
| CVE-2021-40444 | 8.8 | S | Bloquear controles ActiveX, aplicar patch MS [67] | 2021-09-07 | N/A |

### 10.0.5 Detecção

| Rule type | Rule Name | Concise Description | Link |
|---|---|---|---|
| Sigma | Lumma - Possível Execução ClickFix (PowerShell Encoded) | Detecta uso de PowerShell com comandos codificados e ocultos típicos da técnica ClickFix. | SigmaHQ |
| Sigma | Lumma - Mshta Execução Remota | Identifica uso do `mshta.exe` para carregar conteúdo remoto/HTA malicioso. | SigmaHQ |
| Sigma | Lumma - Persistência Run Key | Monitora criação de chaves em `HKCU\\Software\\Microsoft\\Windows\\Run` usadas para persistência. | SigmaHQ |
| Sigma | Lumma - Acesso a Bancos de Dados de Navegador | Detecta acesso suspeito a bases de credenciais/cookies de navegadores por processos anômalos. | SigmaHQ |
| Sigma | Lumma - Possível Exfiltração HTTP(S) | Regras para identificar tráfego POST suspeito com URIs e User-Agents maliciosos. | SigmaHQ |
| YARA | MAL_Lumma_Ger | Regras genéricas para detecção de amostras Lumma em disco ou memória (strings de credenciais, AMSI bypass, etc.). | YARA Docs |
| YARA | MAL_ClickFix_HTA_AutoIt | Detecta payloads ClickFix/HTA/AutoIt usados em cadeias de infecção do Lumma. | YARA Docs |
| YARA | MAL_Lumma_Cor | Procura artefatos típicos do Lumma (pastas `%AppData%`, URIs `/gate`, `/c2`, Telegram API). | YARA Docs |

# 11 Recomendações

1. Formação de Consciencialização do Utilizador: Educar os funcionários para reconhecer phishing, malvertising e táticas de engenharia social como o CAPTCHA falso "ClickFix". Enfatizar a cautela contra o download de software de fontes não confiáveis ou a execução de comandos de websites.
2. Solução EDR (Endpoint Detection and Response): Implementar e configurar uma solução EDR para monitorizar comportamentos anómalos de processos, como mshta.exe a iniciar o PowerShell, ou processos não autorizados a aceder a lojas de credenciais de navegadores.
3. Restringir a Execução de Scripts: Utilizar políticas de controlo de aplicações para restringir a execução do PowerShell e outras linguagens de script para utilizadores que não as necessitem para as suas funções.
4. Filtragem de Rede: Bloquear ligações a domínios maliciosos conhecidos e a domínios recentemente registados (NRDs), que são frequentemente utilizados para infraestruturas C2. Utilizar filtragem DNS e gateways web para prevenir o acesso a sites de distribuição de malware.
5. Higiene de Credenciais: Incentivar o uso de gestores de palavras-passe em vez de guardar credenciais em navegadores. Impor a Autenticação Multifator (MFA) em todos os serviços críticos para mitigar o impacto de credenciais roubadas.
6. Atualizações Regulares de Software: Manter os sistemas operativos, navegadores e outro software corrigidos e atualizados para proteger contra vulnerabilidades que poderiam ser exploradas em ataques multi-estágio.
7. Fortalecer a Configuração do Microsoft Defender for Endpoint: Ativar a proteção contra adulteração, a proteção de rede e a proteção web. Executar o EDR em modo de bloqueio e configurar a investigação e remediação em modo totalmente automatizado.
8. Regras de Redução da Superfície de Ataque: Ativar regras para bloquear ficheiros executáveis que não cumprem critérios de prevalência, idade ou lista de confiança, bloquear a execução de scripts potencialmente ofuscados, bloquear o lançamento de conteúdo executável descarregado por JavaScript ou VBScript, e bloquear a criação de processos originados de comandos PSExec e WMI.
9. Proteger Contra Roubo de Credenciais: Bloquear o roubo de credenciais do subsistema de autoridade de segurança local do Windows e bloquear o uso de ferramentas de sistema copiadas ou personificadas. Ativar a Proteção LSA (Local Security Authority).
10. Autenticação Resistente a Phishing: Utilizar métodos de autenticação resistentes a phishing, como FIDO Tokens ou Microsoft Authenticator com "passkey".

## 12 Conclusão

O Lumma Stealer representa uma ameaça madura e resiliente dentro do ecossistema do cibercrime, amplificada pelo seu modelo acessível de MaaS. A sua dependência de engenharia social sofisticada e técnicas de execução evasivas torna-o um perigo que contorna as defesas tradicionais baseadas em assinaturas. As organizações devem adotar uma postura de segurança em várias camadas que combine controlos técnicos avançados com uma educação robusta dos utilizadores para mitigar eficazmente o risco de roubo de credenciais e subsequente comprometimento da rede. É crucial o uso de ferramentas de inteligência de ameaças para identificar indicadores de comprometimento e bloquear o tráfego de saída para domínios suspeitos.

## 13 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