Relatório de Inteligência - RIT-001

Lumma Stealer Analysis

João Pedro Rosa Cezarino

September 10, 2025

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.
- **Information Sensitivity:** TLP:GREEN

Este Relatório de Inteligência descreve as principais informações e atualizações sobre a ameaça Lumma Stealer e tem como objetivo auxiliar na tomada de decisão dos riscos cibernéticos.

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

- Browser Credentials: Usernames, passwords, cookies, and autofill data from over 10 major web browsers.
- Cryptocurrency Wallets: Data from numerous cryptocurrency wallet applications and browser extensions.
- Two-Factor Authentication (2FA) Tokens: Information from 2FA extensions, potentially allowing attackers to bypass multi-factor authentication.
- System Information: Detailed information about the compromised machine, including hardware, OS version, and IP address.
- Application Data: Credentials and data from various applications, including FTP clients and messaging apps like Telegram.

4 Detalhes da Ameaça

The primary function of Lumma Stealer is to harvest and exfiltrate a wide variety of sensitive data from victim machines. The malware is written in C and is continuously updated with advanced features to evade detection and maximize data theft. Its MaaS model allows affiliates to customize and deploy the malware easily. The primary types of data targeted include:

- Browser Credentials: Usernames, passwords, cookies, and autofill data from over 10 major web browsers.
- Cryptocurrency Wallets: Data from numerous cryptocurrency wallet applications and browser extensions.
- Two-Factor Authentication (2FA) Tokens: Information from 2FA extensions, potentially allowing attackers to bypass multi-factor authentication.
- System Information: Detailed information about the compromised machine, including hardware, OS version, and IP address.
- Application Data: Credentials and data from various applications, including FTP clients and messaging apps like Telegram.

The malware employs a multi-stage, often fileless, execution chain using obfuscated PowerShell scripts and Living Off the Land Binaries (LOLBINs) like mshta.exe to evade detection. A particularly effective delivery method is the “ClickFix” technique, where victims are tricked by fake CAPTCHA pages into pasting and executing malicious commands in the Windows Run dialog, bypassing browser-based security controls. Data is exfiltrated via HTTP POST requests to a resilient and frequently changing Command and Control (C2) infrastructure.

5 Capabilities, Adversary Infrastructure & Victim

- Credential harvesting (browsers, crypto wallets, extensions)
- System reconnaissance (hostname, hardware ID, geolocation)
- Exfiltration via Telegram bots & C2 servers
- MaaS infrastructure with tiered subscription models

6 Perfil da Ameaça

The threat actor “Shamel” (also known as “Lumma”) is a Russian-speaking developer responsible for creating and maintaining the Lumma Stealer. The malware has been advertised on Russian-language underground forums since August 2022. Shamel operates a Malware-as-a-Service (MaaS) business, selling subscriptions to the stealer via Telegram and a dedicated website. This model allows a broad range of cybercriminals, from low-skilled individuals to sophisticated groups like the ransomware operator Octo Tempest, to use the malware for initial access and data theft. Subscription tiers range from approximately $250 per month to $20,000 for access to the source code, making it a commercially successful and widely distributed threat.

7 Modus Operandi

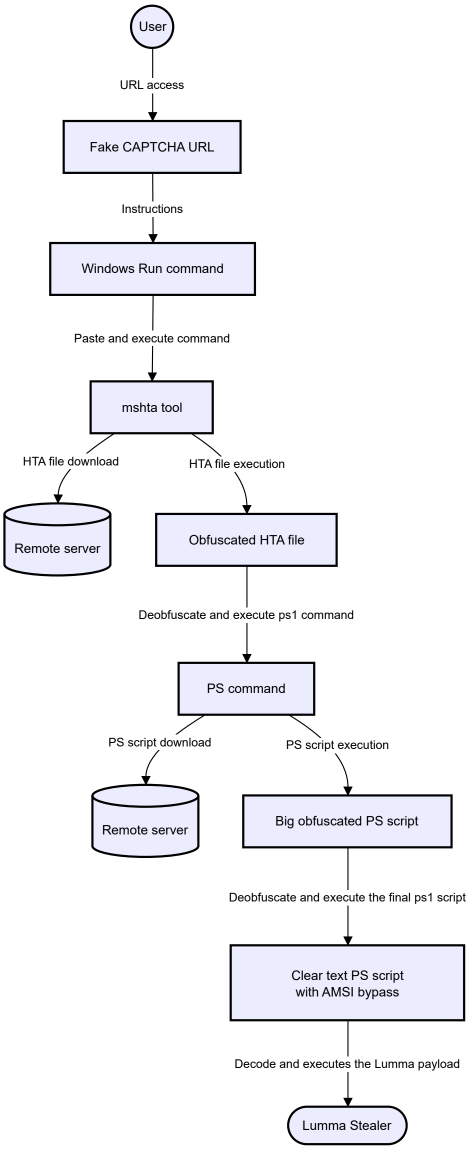

Figure 1: Lumma stealer infection chain

8 Análise do Hash Encontrado

65eb366739361b97fb68c0ac4b9fbaad2ac26e0c30a21ef0ad0a756177e22e94

9 Vítimas

O grupo RansomHouse tem como alvo principal países como Estados Unidos, Europa e Ásia. Os 10 principais setores mais afetados pelo RansomHouse de 1º de janeiro de 2023 a 22 de maio de 2024 foram os setores: farmacêuticos, tecnológicos, assistência médica, serviços de suporte empresarial e aeroespacial.

10 Recomendações

1. **User Awareness Training**: Educate employees to recognize phishing, malvertising, and social engineering tactics like the “ClickFix” fake CAPTCHA. Emphasize caution against downloading software from untrusted sources or executing commands from websites.
2. **Endpoint Detection and Response (EDR)**: Deploy and configure an EDR solution to monitor for anomalous process behavior, such as mshta.exe spawning PowerShell, or unauthorized processes accessing browser credential stores.
3. **Restrict Script Execution**: Use application control policies to restrict the execution of PowerShell and other scripting languages for users who do not require them for their job functions.
4. **Network Filtering**: Block connections to known malicious domains and newly registered domains (NRDs), which are frequently used for C2 infrastructure. Use DNS filtering and web gateways to prevent access to malware distribution sites.
5. **Credential Hygiene**: Encourage the use of password managers instead of saving credentials in browsers. Enforce Multi-Factor Authentication (MFA) across all critical services to mitigate the impact of stolen credentials.
6. **Regular Software Updates**: Keep operating systems, browsers, and other software patched and up-to-date to protect against vulnerabilities that could be exploited in multi-stage attacks.

11 Conclusão

The Lumma Stealer represents a mature and resilient threat within the cybercrime ecosystem, amplified by its accessible MaaS model. Its reliance on sophisticated social engineering and evasive execution techniques makes it a danger that bypasses traditional signature-based defenses. Organizations must adopt a multi-layered security posture that combines advanced technical controls with robust user education to effectively mitigate the risk of credential theft and subsequent network compromise.

12 Diamond Model

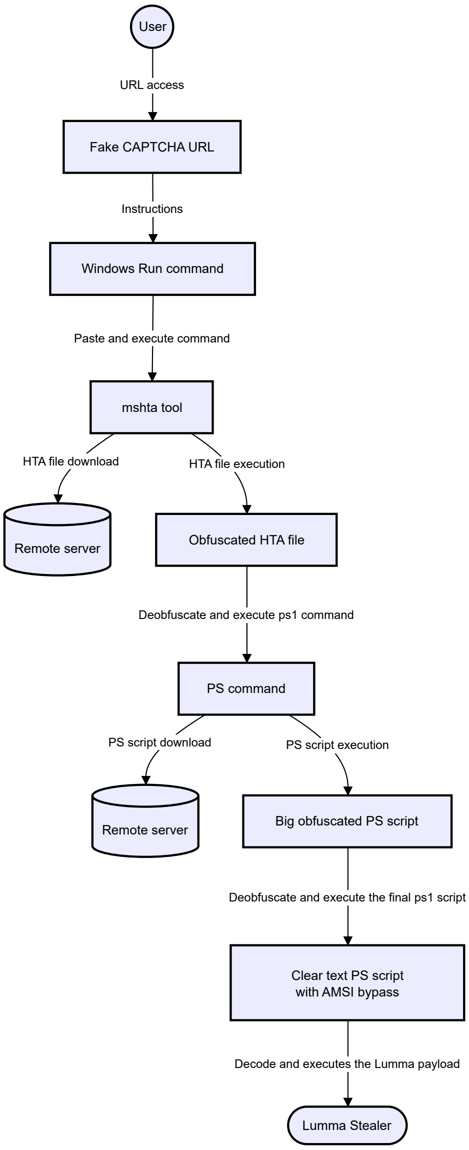

Figure 2: Lumma stealer infection chain

13 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

14 Artifacts

14.0.1 Endpoint Artifacts

Type	Description	Tactic
Registry Key	`HKCU\Software\Microsoft\Windows\Run` [67]	Persistence [T1547.001]
File Drop	`%AppData%\Roaming\lumma\` [67]	Execution, Persistence [T1059]
File Drop	Arquivos `.accde`, `.bat`, `.a3x` no `%AppData%\Local\Temp\` [68-71]	Execution, Defense Evasion [T1059, T1027]
Process Injection	Injeção em `msbuild.exe`, `regasm.exe`, `regsvcs.exe`, `explorer.exe` [40]	Defense Evasion [T1055]

14.0.2 Network Artifacts

Type	Description	Kill Chain Stage
HTTP POST	Exfiltração de dados para C2 com URIs como `/c2sock` e User-Agent `TeslaBrowser/5.5` [44, 67]	C2, Exfiltration [T1041, T1071.001]
Telegram API	Bot usado para uploads de credenciais [43, 67]	C2 [T1102.002]
C2 URLs (Exemplos)	`hxxps://payment-confirmation.82736[.]store/pgg46`, `hxxps://booking[.]procedeed-verific[.]com/goo_pdf` [72] `hxxps://h3.errantrefrainundocked.shop/riii2.aspx` [33] `hxxps://dogalmedical[.]org`, `hxxps://t[.]me/lolypop343` [73]	C2 [T1071.001]

14.0.3 Malware Hashes

Type	File Hash	Description	Kill Chain Stage
SHA256	65eb366739361b97fb68c0ac4b9fba6d2ac26e0c30a21ef0ad0a756177e22e94 (Exemplo Lumma Stealer v4) [67]	Installation, C2 [T1547, T1071]	
SHA256	7b3bd767ff532b3593[illegible]a6494257d (Exemplo Lumma Stealer) [74]	Installation, C2 [T1547, T1071]	
SHA1	e32145901e539b4d3322efa4485dca56cf521ce5 (Arquivo Compactado de campanha Forcepoint) [73]	Delivery [T1566]	
SHA1	ec69088d1409444de6 (Payload EXE de campanha Forcepoint) [73]	Installation [T1547]	
SHA1	2c8ec98431a788f18f1865c7d742deb741a927b3 (Script AutoIT .a3x de campanha Forcepoint) [73]	Execution [T1059.003]	

14.0.4 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 #	CVSS Score	Patch Available (Y/N)	Remediation	Date Reported	Patch Applied (Y/N/N/A)
CVE-2021-40444	8.8	S	Bloquear controles ActiveX, aplicar patch MS [67]	2021-09-07	N/A

14.0.5 Detection & Response

Tactic (MITRE ATT&CK)	Technique (MITRE ATT&CK)	Procedure	D3FEND Control	Rule / Query Name	Type	Description	Reference
Credential Access [TA0006]	T1555.003 Credential from Web Browsers	Coleta de credenciais de navegadores [75]	Credential Hardening [D3-CH]	Lumma_Browser_IOC [75]	Sigma	Detecta acesso anormal a arquivos de navegador [75]	MITRE ATT&CK
Persisten	T1547.00 Registry Run Keys / Startup Folder	Persistên via chave de registro Run [75]	Registry Monitoring [D3-RM]	Lumma_F [75]	Sigma	Alerta quando uma chave Run suspeita é criada [75]	Sysmon Logs
Exfiltration [TA0010]	T1041: Exfiltration Over C2 Channel	Exfiltração via C2 HTTPS [75]	Network Segmentation [D3-NS]	Lumma_HTTP_Exfil [75]	Sigma	Detecta exfiltração anômala POST HTTPS [75]	Suricata Rule

Tactic (MITRE ATT&CK)	Technique (MITRE ATT&CK)	Procedure	D3FEND Control	Rule / Query Name	Type	Description	Reference
Executior [TA0002]	T1059.00 PowerShell	Execução de comandos PowerShell ofuscados [33]	Script Analysis [D3-SA]	Suspiciou PowerShell command line [57]	EDR Alert	Detecta comandos PowerShell suspeitos ou codificados	Microsoft Defender for Endpoint [57]
Defense Evasion [TA0005]	T1027.001 Binary Padding	Aumento do tamanho do binário para evasão [38]	Executable Code Analysis [D3-ECA]	Larger LummaStealer Samples [34]	Behavioral	Detecta executáveis Lumma incomumente grandes	G DATA [34]
Defense Evasion [TA0005]	T1027.01 Command Obfuscation	Ofuscaçã de comandos PowerShell [33]	Script Analysis [D3-SA]	Trojan:Po [76]	Antivirus	Detecção de comandos PowerShell ofuscados	Microsoft Defender Antivirus [76]
Defense Evasion [TA0005]	T1055: Process Injection	Injeção de código malicioso em processos legítimos [40]	Process Self-Modification Prevention [D3-PSMP]	Process hollowing detected [57]	EDR Alert	Detecta esvaziamento de processo e injeção de código	Microsoft Defender for Endpoint [57]

Tactic (MITRE ATT&CK)	Technique (MITRE ATT&CK)	Procedure	D3FEND Control	Rule / Query Name	Type	Description	Reference
Collection [TA0009]	T1115: Clipboard Data	Cópia de comandos maliciosos para a área de transferência [35, 50]	Clipboard Data Monitoring [D3-CDM]	ClickFix commands execution [77]	Query	Identifica execução de comandos ClickFix a partir do registro RunMRU	Microsoft Defender XDR [77]
Command and Control [TA0011]	T1071.001 Web Protocols	Comunicação C2 via HTTP/HTTPS para domínios específicos [31, 43, 44]	Traffic Filtering [D3-TF]	Suspicious Connection to TLDs or Steamcommunity API [63]	Sigma	Detecta conexões de rede para TLDs suspeitos e Steamcommunity.com	WithSecure™ Labs [63]
Command and Control [TA0011]	T1071.00 Web Protocols	Comunica inicial C2 via POST request [78]	Traffic Filtering [D3-TF]	Lumma Stealer - Possible egress POST request [78]	Sigma	Detecta solicitações POST iniciais com User Agent e URI específicos	WithSecure™ Labs [78]

Tactic (MITRE ATT&CK)	Technique (MITRE ATT&CK)	Procedure	D3FEND Control	Rule / Query Name	Type	Description	Reference
Defense Evasion [TA0005]	T1027: Obfuscated Files or Information	Uso de ofuscação de fluxo de controle indireto (Indirect Control Flow) [39]	Executable Code Analysis [D3-ECA]	Win32.Trojan-Stealer.LummaStealer (genérico) [74]	Antivirus	Detecção baseada em características de ofuscação do Lumma	G DATA [74]
Defense Evasion [TA0005]	T1027: Obfuscated Files or Information	Bypass AMSI para evitar varredura de payload [41]	Executab Code Analysis [D3-ECA]	Behavior: [76]	Antivirus	Detecção de comportamento de bypass AMSI	Microsoft Defender Antivirus [76]

15 Referências

1. Forcepoint. Unmasking the Lumma Stealer Campaign. Acessado em 10 de setembro de 2025.
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.