Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

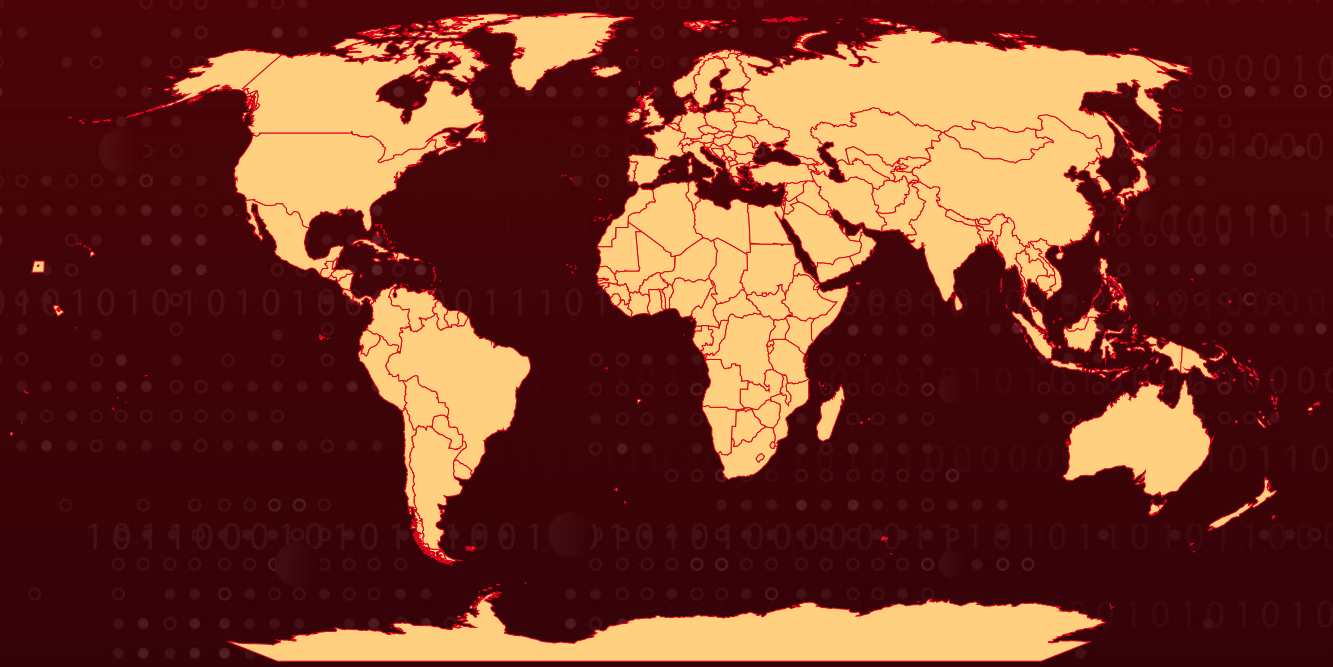
Malware-as-a-Service in Action: Lumma Stealer's Expanding Attack Methods

Date of Publication	Admiralty Code	TA Number
February 18, 2025	A1	TA2025046

Summary

Active Since: February 2025
Targeted Countries: Worldwide
Malware: Lumma Stealer
Targeted Industries: Education, Academia, Corporate, Business, Government, Legal, Healthcare, Pharmaceuticals, Financial, Banking, Engineering, Manufacturing, Technology, Blockchain, Media, and Journalism
Affected Platform: Windows
Attack: A sophisticated, ongoing malware campaign involving Lumma Stealer is exploiting compromised educational institutions to distribute malicious PDF-themed LNK files. These files trigger a multi-stage infection, stealing credentials, browser data, and cryptocurrency information. Targeting industries like finance and healthcare, the attackers use Steam profiles for command-and-control operations, evading detection. This campaign highlights the increasing risks of phishing and social engineering tactics, urging organizations to enhance cybersecurity through awareness training, endpoint protection, and network monitoring.

Attack Regions



Attack Details

#1 An active campaign is distributing Lumma Stealer, an information-stealing malware offered as Malware-as-a-Service (MaaS). The attackers use malicious LNK files disguised as PDFs to infect victims, primarily targeting industries such as finance, healthcare, and technology, where access to sensitive information is highly valuable.

#2 To enhance credibility and evade detection, attackers leverage compromised networks of educational institutions. By using these trusted networks, they can distribute malware more widely while minimizing suspicion. This tactic helps them bypass security measures that might otherwise flag their activities.

#3 The attack begins when a victim downloads a malicious LNK file disguised as a PDF from a compromised website. When executed, the LNK file triggers a PowerShell script via WMIC, which then launches Mshta.exe to download and execute a JavaScript payload. This script, in turn, retrieves and executes Lumma Stealer on the victim's system.

#4 Once installed, Lumma Stealer attempts to connect to command and control (C2) servers to exfiltrate stolen data. If the primary C2 servers are inaccessible, the malware employs an alternative method by leveraging Steam profiles as a covert communication channel. It uses a Caesar cipher to decrypt C2 domains, making detection and mitigation more challenging.

#5 In recent months, hackers exploited fake CAPTCHA verification pages to spread Lumma Stealer globally, targeting multiple industries. This technique tricked users into executing the malware under the guise of verifying their identity.

#6 This campaign demonstrates the increasing use of unconventional platforms for malware communication and control. It also underscores the growing risks of phishing and social engineering tactics in modern cyberattacks, reinforcing the need for stronger cybersecurity awareness and defenses. In recent months, Lumma Stealer has been observed using new distribution tactics.

Recommendations

Strengthen Email and File Scanning: Configure email gateways and endpoint security solutions to detect and block malicious LNK files and other suspicious attachments. Employ robust sandboxing and anti-phishing solutions to identify threats before they reach end users.

Implement Strong Access Controls: Restrict user privileges and limit administrative rights, ensuring that only essential personnel have access to critical systems. Enable multi-factor authentication (MFA) for all critical logins to reduce the impact of compromised credentials.

Implement Advanced Endpoint Protection: Deploy Next-Generation Antivirus (NGAV) and Endpoint Detection and Response (EDR) solutions to detect and block malicious scripts and payloads. Configure behavior-based threat detection to identify abnormal activities, such as unexpected PowerShell or Mshta.exe executions. Enforce application whitelisting to block unauthorized script execution.

Secure Cloud and Social Media Platforms: Monitor for malicious content on YouTube and other platforms that attackers might use to spread malware. Implement two-factor authentication (2FA) and strict access controls on cloud services to prevent account compromise. Regularly audit social media and cloud accounts for signs of unauthorized activity.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0005 Defense Evasion	TA0006 Credential Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0040 Impact	T1490 Inhibit System Recovery

T1059 Command and Scripting Interpreter	T1204 User Execution	T1047 Windows Management Instrumentation	T1547.001 Registry Run Keys / Startup Folder
T1547 Boot or Logon Autostart Execution	T1204.002 Malicious File	T1218.011 Rundll32	T1218 System Binary Proxy Execution
T1027 Obfuscated Files or Information	T1036.003 Rename System Utilities	T1036 Masquerading	T1564.003 Hidden Window
T1564 Hide Artifacts	T1012 Query Registry	T1082 System Information Discovery	T1021.002 SMB/Windows Admin Shares
T1021 Remote Services	T1114 Email Collection	T1560 Archive Collected Data	T1071 Application Layer Protocol
T1041 Exfiltration Over C2 Channel	T1489 Service Stop		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	BB2E14BB962873722F1FD132FF66C4AFD2F7DC9B6891C746D697443C0007426A, e15c6ecb32402f981c06f3d8c48f7e3a5a36d0810aa8c2fb8da0be053b95a8e2, 40b80287ba2af16daaf8e74a9465a0b876ab39f68c7ba6405cfcb41601eeec15
URLs	hxxps[:]//80[.]76[.]51[.]231/Kompass-4[.]1[.]2[.]exe, hxxps[:]//80[.]76[.]51[.]231/Samarik, hxxp[:]//87[.]120[.]115[.]240/Downloads/254-zebar-school-for-children-that-tej-pro-order-abad-rural[.]pdf[.]lnk

TYPE	VALUE
Domains	tripeggyun[.]fun, processhol[.]sbs, librari-night[.]sbs, befall-sm0ker[.]sbs, p10tgrace[.]sbs, peepburry828[.]sbs, owner-vacat10n[.]sbs, 3xp3cts1aim[.]sbs, p3ar11fter[.]sbs, smiteattacker[.]org, yuriy-gagarin[.]com, vladimir-ulyanov[.]com, nikolay-romanov[.]su, aleksandr-block[.]com, misha-lomonosov[.]com, sputnik-1985[.]com, lev-tolstoi[.]com
IPv4	87[.]120[.]115[.]240, 80[.]76[.]51[.]231

References

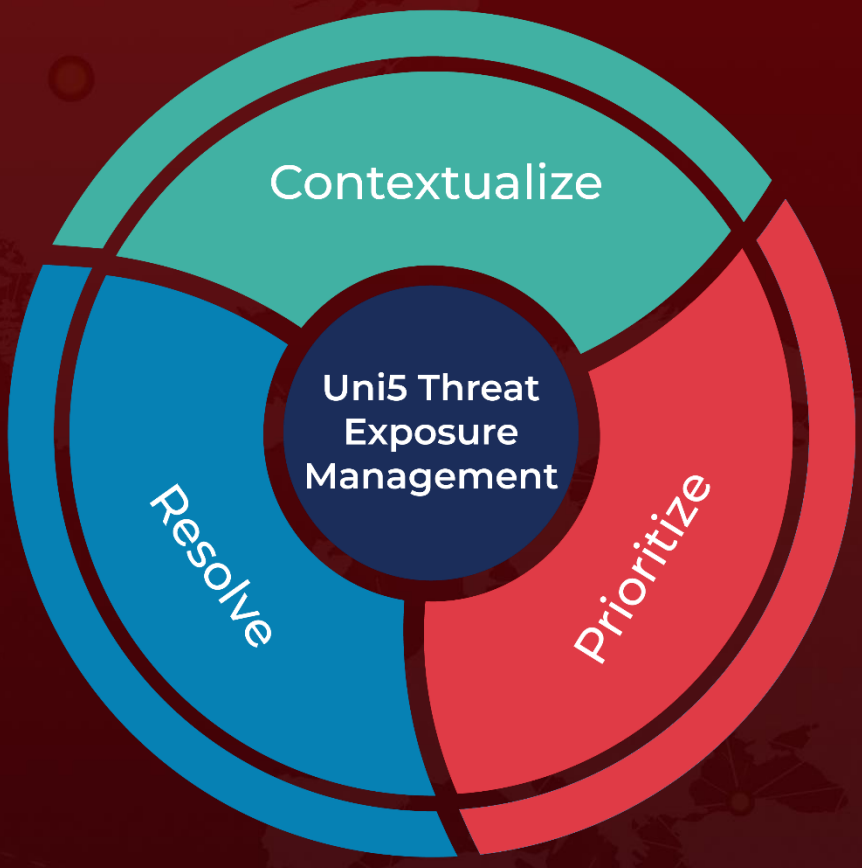
https://www.cloudsek.com/blog/lumma-stealer-chronicles-pdf-themed-campaign-using-compromised-educational-institutions-infrastructure

https://hivepro.com/threat-advisory/lumma-stealer-strikes-again-with-fake-captchas-and-advanced-evasion/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 18, 2025 • 6:30 AM

More at www.hivepro.com