CYBER THREAT INTELLIGENCE ANALYSIS

THREAT INTELLIGENCE ASSESSMENT ON LUMMA INFORMATION STEALER

DOCUMENT PREPARED
BY ELLEN HALLAM
SENIOR THREAT INTELLIGENCE ANALYST

CREATED: 24TH OCTOBER 2023

LUMMA INFORMATION STEALER

SUMMARY:

The Lumma Information Stealer, also known as Lumma Stealer or LummaC2, is a type of Malware-as-a-Service (MaaS) that has been advertised and sold on numerous dark web forums since 2022.

Lumma Stealer specialises in gathering and exfiltrating sensitive data, such as login credentials and bank details, from affected devices. It primarily targets cryptocurrency wallets, browser extensions, and two-factor authentication (2FA), before ultimately stealing sensitive information from compromised machines. The malware has been observed being distributed through drive-by-downloads, masquerading as browser updates, and through deceptive sites offering game downloads and software cracks.

It can obtain system and installed program data from compromised devices, alongside sensitive information such as cookies, usernames and passwords, credit card numbers, connection history, and cryptocurrency wallet data.

OBSERVATION:

Typically, Lumma has been distributed disguised as cracked or fake popular software like VLC or ChatGPT. Recently though, threat actors have also delivered the malware through emails containing payloads in the form of attachments or links impersonating well-known companies. The malware is proliferated using phishing and social engineering techniques. Malicious software is typically presented as, or bundled with, ordinary software/media. The most common distribution methods include drive-by (stealthy/deceptive) downloads, online scams, spam emails and messages, dubious download channels (e.g., unofficial and freeware websites, Peer-to-Peer sharing networks, etc.), illegal program activation ("cracking") tools, and fake updates. Virulent files can be Microsoft Office and PDF documents, archives (RAR, SIP, etc.), executables (.exe, .run, etc.) and JavaScript. When a malicious file is executed, run, or otherwise opened - the infection chain is initiated.

Lumma is known to target Windows operating systems from Windows 7 to 11 and at least 10 different browsers including Google Chrome, Microsoft Edge, and Mozilla Firefox. It has also been observed targeting crypto wallets like Binance and Ethereum, as well as crypto wallet and 2FA browser extensions like Metamask and Authenticator respectively. Data from applications such as AnyDesk or KeePass can also be exfiltrated by the malware.

Lumma Information Stealer has been an emerging threat since early 2023, joining the list of info stealers that have been on the rise, including Vidar and Racoon. It was developed by a threat actor known as “Shamel”, under the alias "Lumma" and has been sold in underground (dark web) forums since December 2022. The number of sightings of this malware being distributed on dark web forums is on the rise, and thus far, more than a dozen command-and-control (C2) servers have been observed in the wild. Between January and April 2023, multiple instances of Lumma stealer activity were observed and investigated across the customer base.

ANALYST ASSESSMENT:

The Malware-as-a-Service (MaaS) model continues to provide would-be threat actors with an inexpensive and relatively straightforward way to carry out sophisticated cyber-attacks. There has been an increase in the popularity and usage of information stealing malware in underground markets and it is *highly likely* this is a trend which will continue over the next 6 months. It is *almost certain* the malware will continue to become more damaging, and that it’s stealing capabilities, simple administration, execution and above all, ability to remain undetected will ensure that its popularity continues. It is also *likely* that users with limited technical knowledge will continue to use it, as evidenced by threat actors offering subscription-based access, rather than the usual single payment methodology. There is a *realistic possibility* that, depending on the sensitivity of the stolen data, cyber criminals could potentially use it for blackmail purposes and demand a ransom under threat of publication. Likewise, criminals can abuse communication/social platforms to steal the victim's identity and ask their

contacts/friends for loans, which can also be used to spread the malware (by sharing malicious files/links). Finance-related accounts will *almost certainly* be used to make fraudulent transactions or online purchases.

ISSUE CORRECTION:

For Individuals:

1. Update systems, applications and software to the latest version and download the latest security patches.
2. Install anti-virus/anti-malware software and keep the software (and its definition files) updated. Perform a scan of the systems and networks regularly and scan all received files.
3. Avoid Suspicious Downloads: Always source downloads from official and verified channels. Utilise legitimate developers' functions/tools for activation and updates, avoiding illegal activation tools and fake updaters that could harbour malware.

For Organisations:

1. Disable all ports and protocols that are not essential for business purposes.
2. Isolate devices that use legacy operating systems if organisations are unable to update these devices.
3. Limit privileged access to authorised personnel to reduce the risk of privileged account abuse or compromise.
4. Regularly monitor all user accounts and disable inactive accounts.
5. Closely monitor inbound and outbound network traffic for suspicious communications or data transmissions.
6. Enforce password updates for account owners that may have their credentials leaked.
7. Implement regular training to educate employees about the different types of phishing attacks, common phishing techniques and how to identify and respond to suspicious emails, links, and attachments.
8. Regular Backups: Conduct regular backup practices and keep those backups offline or in a separate network.
9. Use Reliable Antivirus Software: Scan and protect devices from malicious threats.
10. Employee Training: If you're part of an organisation, ensure that employees are trained to spot and avoid social engineering scams.
11. Monitor Network Connections and Review System Logs to Quickly Detect a Potential Intrusion
12. Enable logging of system events to facilitate investigation of suspicious events or issues.
13. Use an Effective Endpoint Detection and Response (EDR) Solution at end-users' devices for continuous monitoring, detecting and responding of cyber threats.

Caveat:

This is based on current, limited knowledge, which should be further investigated and checked, before being applied to your systems.

SOURCES:

1. Defending Against Lumma Information Stealer Malware (csa.gov.sg)
2. Everything you need to know about the LummaC2 stealer: leveraging IDA Python and Unicorn to deobfuscate Windows API hashing - Outpost24
3. Lumma Stealer - Malware removal instructions (updated) (pcrisk.com)
4. The Rise of the Lumma Info-Stealer | Darktrace Blog
5. How Organisations and Their Employees Can Stay Ahead of Cybersecurity Threats (csa.gov.sg)

Annex 1:

The Probability Yardstick

To quantify language, we use the Probability Yardstick, from the Professional Head of Intelligence Assessment. It is a tool used by the UK Government to standardise the way we describe probability and has been used to ensure consistency across the different thematic areas and threats when providing assessments on how *likely* something is to occur. The yardstick is included for clarity.

Professional Head of Intelligence Assessment

Probability Yardstick

Probability range	Judgement terms	Fraction range
> 0 - ≤ ≈5%	***Remote chance***	> 0 - ≤ ≈1/20
≈10% - ≈20%	***Highly unlikely***	≈1/10 - ≈1/5
≈25% - ≈35%	***Unlikely***	≈1/4 - ≈1/3
≈40% - < 50%	***Realistic possibility***	≈2/5 - < 1/2
≈55% - ≈75%	***Likely*** or ***Probably***	≈5/9 - ≈3/4
≈80% - ≈90%	***Highly likely***	≈4/5 - ≈9/10
≥ ≈95% - < 100%	***Almost certain***	≥ ≈19/20 - < 1

≈ approximately ≥ is more than or equal to ≤ is less than or equal to > is more than < is less than

Source Evaluation:

We also assess our sources using the below matrix, but rarely disclose our source, to protect the integrity of the source. We assess sources on how reliable they are, how they accessed the intelligence, and we then decide if this intelligence can be shared. The table shown to the illustrates this.

Source Evaluation	Intelligence Evaluation	Handling Conditions
1 - Reliable	A - Known directly to the source	P – Lawful sharing permitted
	B - Known indirectly to the source but corroborated	
2 - Untested	C - Known indirectly to the source	C - Lawful sharing permitted with conditions
	D - Not known	
3 – Not reliable	E - Suspected to be false	

Confidence Levels:

High Confidence	High confidence generally indicates judgements based on high-quality information, and/or the nature of the issue makes it possible to render a solid judgment. A “high confidence” judgment is not a fact or a certainty, however, and still carries a risk of being wrong.
Moderate Confidence	Moderate confidence generally means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence
Low Confidence	Low confidence generally means questionable or implausible information was used, the information is too fragmented or poorly corroborated to make solid analytic inferences, or significant concerns or problems with sources existed