ADVISORY FOR ICM SECTORS

Phishing email delivers Lumma Stealer

Report published on: Oct 31, 2024

Executive Summary

ISG-CERT investigated an incident which started from Spearphishing link targeting employees of an organisation in Singapore. After the malware is installed, suspicious code execution occurs on the system which eventually delivers Lumma Stealer (aka LummaC2) information stealer. When a system is infected, Lumma Stealer can steal data including cookies, browsing histories, cryptocurrencies and keystrokes. Additionally, it can create backdoors, disable protective software, and download additional malware. [1]

Background

Since December 2022, Lumma Stealer has been sold as a Malware-as-a-Service (MaaS) in underground forums and delivered often via phishing campaigns[2]. The malware is known to use malicious CAPTCHA pages hosted on Content Delivery Networks (CDNs) to scam targets into clicking through the "verification" process triggering the initial malware download. Completing the steps triggers the execution of a PowerShell command that fetches and executes content from a TXT file. The content of the TXT file contains additional commands to download the Lumma Stealer. When the zip file is extracted and executed, Lumma Stealer will begin to establish connections with attacker-controlled domains. [1]

In a recent active Lumma Stealer campaign, Qualys Threat Research Unit (TRU) researchers observed threat actors advancing its tactics to exploit legitimate software to deliver the malware. Users were redirected to fake CAPTCHA sites by bad actors exploiting legitimate software of public-facing applications. As the user completes steps to verify that they are not a robot, a PowerShell script is triggered. Instead of fetching a TXT file, the attack uses a fileless technique mshta.exe to execute the malicious JavaScript payload, which decrypts an AES-encrypted payload to download Lumma Stealer. An obfuscated bat script is used to check for anti-virus processes such as Webroot Antivirus Component, Quick Heal Antivirus component and Bitfender. Process hollowing was also employed to evade detection and gather sensitive data (e.g. cryptocurrency, passwords) and exfiltrated via Command and Control (C2) servers leveraging Cloudflare. [3]

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Use application control tools like AppLocker or Windows Defender Application Control to restrict the execution of mshta.exe unless explicitly needed.
- Limit the use of PowerShell for administrative tasks only and monitor its use to prevent unauthorized scripts from being executed.
- Continue employee awareness to stress the importance of safe browsing practices, highlighting the need to avoid browsing malicious websites which might lead to a fake CAPTCHA page.
- Monitor network traffic for unusual or suspicious connections, especially to newly registered or uncommon domains.
- Scan the provided IOCs against your organisation CII and enterprise environment.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

Indicators of Compromise

IOCs originating from IMDA's investigations

Indicators	Type
188[.]130.206.243	IP Address
46[.]8.232.106	IP Address
46[.]8.236.61	IP Address
91[.]212.166.91	IP Address
93[.]185.159.253	IP Address
185[.]121.233.152:17289	IP Address
condifendteu[.]sbs	Domains
ehticsprocw[.]sbs	Domains
drawwyobstacw[.]sbs	Domains
vennurviot[.]sbs	Domains
enlargkiw[.]sbs	Domains
resinedyw[.]sbs	Domains
mathcucom[.]sbs	Domains
allocatinow[.]sbs	Domains
sergei-esenin[.]com	Domains
clearancek[.]site	Domains
studennotediw[.]store	Domains
dissapoiznw[.]store	Domains
eaglepawnoy[.]store	Domains
mobbipenju[.]store	Domains
spirittunek[.]store	Domains
bathdoomgaz[.]store	Domains
licendfilteo[.]site	Domains
48748de5330d0e64fa9e52bb73ba664ead933909fca374ae811c228f17fac256	MD5
21bb3d4342fd0cd06dffe5542e92393c06365ae5d5274caa942abf24a0ce259b	MD5
56968c8822210a87b1ec5db39dde881941ce22c0a72c01bee3d0dd5c278c9d6a	MD5
798b775e23824c6d9c1d207f30d56aac4c3ae50f986c5d3ac36eaa0e9198bfcc	MD5
48748de5330d0e64fa9e52bb73ba664ead933909fca374ae811c228f17fac256	MD5
5b0b157c71e65906d0d398fd0e1c58ac3104d0dd49dbd14198ffbcf43db6a640	MD5
c052369f476b624913e8aec1a3ba729d30b5d5f145c4c5c58d64f7d09cfa54b5	MD5

IOCs originating from open source[1]

Indicators	Type	Description
hxxps[:]//trick-troll[.]b-cdn[.]net/happy-check.html	URL	
hxxps[:]//dangafile[.]b-cdn[.]net/getcaptchanorm5.html	URL	
hxxps[:]//finalstepgo[.]com/uploads/il4.txt	URL	
hxxps[:]//finalstepgo[.]com/uploads/trr22.txt	URL	
hxxps[:]//finalstepgo[.]com/uploads/tr10.txt	URL	
hxxps[:]//finalstepgo[.]com/uploads/il22.txt	URL	

hxxps[:]//finalstepgo[.]com/uploads/il22.zip	URL	
hxxps[:]/185[.]255[.]122[.]133/uploads/il22.zip	URL	
hxxps[:]//winrar01[.]b-cdn[.]net/win.txt	URL	
hxxps[:]//winrar01[.]b-cdn[.]net/winrar.zip	URL	
hxxps[:]//winscp[.]b-cdn[.]net/scp.txt	URL	
hxxps[:]//get-zip[.]b-cdn[.]net/n41.txt	URL	
hxxps[:]//view41[.]b-cdn[.]net/n41.txt	URL	
hxxps[:]//down41[.]b-cdn[.]net/norm41.zip	URL	
hxxps[:]//fetchinglinknow[.]b-cdn[.]net/service/n5.txt	URL	
hxxps[:]//fetchinglinknow[.]b-cdn[.]net/norm5.zip	URL	
hxxps[:]//best-received[.]b-cdn[.]net/built-in/store-of/the-sys/kbsn2.txt	URL	
hxxps[:]//xilz222[.]b-cdn[.]net/xil222.zip	URL	
finalstepgo[.]com (hosted on 185[.]255[.]122[.]133)	Domains	
finalsteptogo[.]com	Domains	
finalstagetogo[.]com	Domains	
finalstepgetshere[.]com	Domains	
winrar01[.]b-cdn[.]net	Domains	
get-zip[.]b-cdn[.]net	Domains	
view41[.]b-cdn[.]net	Domains	
down41[.]b-cdn[.]net	Domains	
xilx222[.]b-cdn[.]net	Domains	
fetchinglinknow[.]b-cdn[.]net	Domains	
best-received[.]b-cdn[.]net	Domains	
wintx41[.]b-cdn[.]net	Domains	
trick-troll[.]b-cdn[.]net	Domains	
8d41789382f08d76ad65330318a0421d904b4eb5efe9d9f39de3397d70351b07	SHA256	fake CAPTCHA passing-page2.html
5c081145b490e95e7778caa7feda13f793532bd533b61ccbd24d8e3ef2474071	SHA256	fake CAPTCHA getcaptchanorm5.html
d8039aae9940f1f9a19849a16839713aa1d424382882ba48b04750dcfa037091	SHA256	fake CAPTCHA captcha-pass-request.html
fc42b118e6e5a88b3c5a84992c776bf558a4170cf83efd83135f16a79aad5899	SHA256	Lumma Stealer n41.txt
b23bce1cd04539b8c8cdd010b9a28045c44c80b5fc1d35fb5a57a00a6e7473fd	SHA256	Lumma Stealer n41.txt
411bda155e792174cb893e9cad2aa534916a180c33527bf24fab0ae979609306	SHA256	Lumma Stealer n41.txt
184b6a800c6fc568f6c8e20a3619fb4856823ddc1d530a64812993a7044f237c	SHA256	Lumma Stealer il22.txt
bc58a6105f2296c2ddc58bc4ffc1c7eca4293ef4e70fe940030373743 8f50220	SHA256	Lumma Stealer il22.zip
b37a3eb131e059e65899a9aaca83f20dfd533b22bda146395fc0789aff01bc0b	SHA256	Lumma Stealer n5.txt
ed7d9b23dcaffd9f24527e095374a2f635659debd20c55e876e556cc091028f9	SHA256	Lumma Stealer scp.txt
abdb34d71b74553c4bcabd6066b2a0e2f4c9be963ee78249a892b5f18519f6ec	SHA256	Lumma Stealer Accel.exe

ee891252b44186f18938e7ae4826b396eeb91939dee0a184091db164445f1098	SHA256	Lumma Stealer cknoqrf4.zip / norm41.zip
406078cc2412404c3d007637632550f289ba1209971a016e7a5c222002355650	SHA256	Lumma Stealer norm5.zip

MITRE ATT&CK Tactics and Techniques

Tactic	Technique	Technique Name
Initial Access	T1566	Phishing
Initial Access	T1189	Drive-by Compromise
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Execution	T1204.001	User Execution: Malicious Link
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Command and Control	T1105	Ingress Tool Transfer
Defense Evasion	T1055.012	Process Injection: Process Hallowing
Defense Evasion	T1218.005	System Binary Proxy Execution: Mshta
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1112	Modify Registry
Defense Evasion	T1564.003	Hide Artifacts: Hidden Window
Exfiltration	T10141	Exfiltration Over C2 Channel

References

1. **^** Closed Source: Cisco AEGIS
2. **^** Anomali Cyber Watch: Lumma Stealer Waits for Human Mouse Movements, LitterDrifter USB Worm Spreads beyond Ukraine, and More
3. **^** “Unmasking Lumma Stealer: Analyzing Deceptive Tactics with Fake CAPTCHA”