Threat Hunting Guide Template

Threat Hunting Guide: [LummaC2]

1. Overview

- **Threat Name:** [LummaC2]
- **Aliases:** [LummaStealer, Shamel]
- **Category:** [Malware (Stealware) works as a MaaS (malware as a service), easy to deploy and buy**,** built using C++ and highly customizable]
- **Targeted Sectors:** [Financial institutions and handling high value transactions, 2FA browser extensions, system credentials]
- **Geographic Focus:** [North America, Europe, South America] originates from Russia
- **First Seen:** [August 2022 - Today]
- **Last Known Activity:** [Active]
- **Known Malware Families Utilized:** QBot and Pinkslipbot (variants)

2. Threat Description

- **Summary:** [Info stealing malware that has gained traction as a MaaS model. Recent campaigns leverage fake GitHub repositories to distribute SmartLoader, which then delivers Lumma Stealer as a secondary payload. This malware gathers sensitive data from infected devices, including banking credentials and cryptocurrency wallet details. Can be bought through Dark Web forums and telegram channels. Initial access is often achieved through phishing emails or through compromised legitimate websites that redirect users to malicious GitHub links or encourage downloads of cracked software. It has been observed injecting itself into legitimate processes using techniques such as thread execution hijacking. One of its highlights is its adaptation to evolving cybersecurity challenges and threats associated with AI- driven cyber crime. Has 3 subscription options that offers variety of features such as a command and control panel, which allows criminals to monitor and manage the malware's activities on compromised machines.]
- **Tactics, Techniques, and Procedures (TTPs):** [T1027.001 (Obfuscated Filer or Information), T1055 (Process Injection), T1059 (Command and Scripting Interpreter)

Credential access, Discovery, Defense Evasion, Persistence, Collection, C2] The Top Ten MITRE ATT&CK Techniques

- **Notable Campaigns:** [ClearFake]
- **Distribution Methods:**
    - **Fake Software:** One of the most prevalent methods used to distribute the malware. Users will download fake applications which contain the malware and infect the systems via a zip file.
    - **Phishing Emails:** Cybercriminals craft emails that look like the can be from legit sources such as banks, e-commerce platforms, or social media networks, which contain false links to login in to your account.
    - **Discord Messages:** In few cases, Lumma Operators have targeted users through discord to try to persuade them to download fake executables (social engineering)

3. Indicators of Compromise (IOCs)

- **File Hashes:**
    - **SHA 256**
        - 277d7f450268aeb4e7fe942f70a9df63aa429d703e9400370f0621a438e918bf
        - f37c412bd47fc18d4c153664b116ea18c7d251eb8cdd0af8f130010958a93353
        - beb2dbeb0987697f1c440958bb1c54754958b47eb4def4db40a4a71d3a9a5b3f
        - d323f2034ee22ad7b02394182f3d52456b3fb3a37bc0d1cea888c5a482c88a26
        - 1cd1a6c8b63ce8cf1ac0de34237bcbdac46f8c613536c7f1e7ad0091420def25
        - f930a52a2107da4907876576 29a889c86714dd2fa9dbd7a18ac31866811ec6e9
        - 1e391c6e0d52e8ae9babcee62cf692635f35e6a88de1fd264a04f501b31b67a1
        - b833c19e1c47e6110ac74e5144a328dbb2bd2fca519b3bf211b32730f0f9b9f4

    - ♣ 3f58ce78300acd111096a6460f57d607790497a21d59712a4da368c714c344e6
    - ♣ 49a7efd8296089d8f30b3eb592b13dc8d9f85e7f9091b0e2653f1ceed77482dc
  -

- **Malicious Domains & URLs:**
  - [Domains: gservice-node.io , millyscroqwp.shop , caffegclasiqwp.shop , locatedblsoqp.shop , evoliutwoqm.shop , condedqpwqm.shop , traineiwnqo.shop , votteryloeq.shop , stamppreewntnq.shop , stagedchheiqwo.shop , pushjellysingeywus.shop , mealplayerpreceodsju.shop , suitcaseacanehalk.shop , entitlementappwo.shop , democraticseekysiwo.shop , economicscreateojsu.shop , absentconvicsjawun.shop , bordersoarmanusjuw.shop , wifeplasterbakewis.shop , deicedosmzj.shop ,]
  - [URL's: http://185.99.133.246/c2sock , http://195.123.226.91/c2sock , http://gstatic-node.io/c2sock , http://winhttp.dll/c2sock , http://82.117.255.80/c2sock , http://aloowforest.xyz/c2sock , http://speedtestip.xyz/c2sock , http://stoppublick.xyz/c2sock , http://many-verses.xyz/c2sock , http://worldofpoetry.xyz/c2sock , http://crazypictures.xyz/c2sock , http://skicloud-my.xyz/c2sock , http://solopodvip-my.xyz/c2sock , http://clonecloud-my.xyz/c2sock , http://2flowers-my.xyz/c2sock , http://vipcloud-my.xyz/c2sock , http://agustfreeday-my.xyz/c2sock , http://gservice-node.io/c2sock , http://195.123.227.138/c2sock , http://flowers-my.xyz/c2sock , hxxps://heroic-genie-2b372e.netlify.app/please-verify-z.html , hxxps://sdkjhfdskjnck.s3[.]amazonaws.com/human-verify-system.html , hxxps://newvideozones.click/veri.html , https://keennylrwmqlw.shop/api
  -

- **IP Addresses:**
  - [195.123.226.91 , 94.158.244.69 , 185.99.133.246 , 144.76.173.247 , 195.123.226.167 , 195.123.227.138 , 82.117.255.80 , 77.73.134.68 , 217.12.206.230 , 82.118.23.50 , 45.9.74.78]

  - C2IP Addresses: 144.76.173.247 , 45.9.74.78 , 77.73.134.68 , 82.117.255.127 , 82.118.23.50 , 5.4.32.5 , 2.5.4.62 , 4.52.5.4 , 72.5.4.82 , 3.3.3.3
- **Registry Modifications:**
  - [Key locations and values modified]
- **File Paths & Artifacts:**
  - [Suspicious file locations and names]
- **Command and Control (C2) Servers:**
  - [195[.]123[.]226[.]91] outpost24.com
- **Malicious Email Indicators:**
  - [Subject lines, senders, attachment names]
- **Other Notable Indicators**
  - [Other data (ex: specific configuration setting change)]

4. Indicators of Attack (IOAs)

- **Behavioral Indicators:**
  - Causes unexpected system behavior, such as unusual network traffic patterns, high CPU usage, and unexplained system slowdowns.
  - May exhibit suspicious patterns like frequent connections to unknown IP addresses, especially those associated with C2 servers.
- **Persistence Mechanisms:**
  - Uses scheduled tasks to maintain persistence on infected systems
  - Establishes communication with C2 servers via HTTP POST requests.
  - Malicious youtube links
  - Unusual registry modifications: used to maintain persistence and disable security software
- **Privilege Escalation Techniques:**
  - Code injection into Windows processes to gain higher level permissions
  - Obfuscation (making data or code difficult to understand)
  - Fake CAPTCHA pages
- **Lateral Movement Methods:**
  - Credential dumping: extracting credentials from compromised systems to access other systems within the network

    - Using hashed credentials to authenticate to other systems without needing the password
    - Using PsExec to execute processes on remote systems
- **Data Exfiltration Indicators:**
    - Unusual outbound traffic
    - Changes to system files or presence of new files that could be used to exfiltrate data
    - Processes that are usually not part of you systems normal operations, especially those consuming network resources
    - Suspicious network connections, C2 servers may be involved encrypting information

5. Threat Hunting Queries

You may find Yara and Sigma rules online which you should convert to CrowdStrike queries, Sentinel queries, or Splunk queries. If the detection pertains to an endpoint, then a CrowdStrike query is appropriate. If the detection pertains to network logs which would not be on an endpoint, then a Sentinel query is appropriate.

SIEM Queries (Sentinel Query)

- Example query to identify sample information
    - Query

EDR Queries (CrowdStrike Query)

- Example query to identify sample information
    - Query

Splunk Queries

6. Response & Mitigation Strategies

Explain how we can mitigate and respond to any of the actions we the threat actor observed performing in this guide. This may be blocking any of the IOCs we found at a device or network level. Or it could be patching systems to remediate CVEs, it could even be informing users of a potential threat if it is something we are unable to block (for example, if the threat actor is phishing users).

- Implement threat intelligence to proactively counter the threats associated with the Lumma Stealer.
- To protect the endpoints, use robust endpoint security solutions for real-time monitoring and threat detection, such as Antimalware security suit and host-based intrusion prevention system.
- Continuous monitoring of the network activity with NIDS/NIPS and using the web application firewall to filter/block suspicious activity provides comprehensive protection from compromise due to encrypted payloads.
- Configure firewalls to block outbound communication to known malicious IP addresses and domains associated with Lumma Stealer command and control servers.
- Implement behavior-based monitoring to detect unusual activity patterns, such as suspicious processes attempting to make unauthorized network connections.
- Conducting vulnerability assessment and penetration testing on the environment periodically helps in hardening the security by finding the security loopholes, followed by a remediation process.
- The use of security benchmarks to create baseline security procedures and organizational security policies is also recommended.
- Develop a comprehensive incident response plan that outlines steps to take in case of a malware infection, including isolating affected systems and notifying relevant stakeholders.
- Update security patches which can reduce the risk of potential compromise
- Conduct regular network scans to identify suspicious activity.
- Enforce the principle of least privilege for user accounts.
- Use advanced threat intelligence platforms to detect and respond to evolving threats.

7. References & Further Reading

Document sources used to craft threat hunt guide.

- **Reports from Security Vendors:** [Links to additional sources]

- **MITRE ATT&CK Mapping:** [Links to MITRE techniques used]
- **Threat Intelligence Feeds:** [Relevant sources for tracking updates]

Other Information Found:

- **Steals sensitive information from infected devices and applications.**
- **Works on clean systems and steals browsers based on Chrome and Mozilla.**
- **Targets a wide range of credentials, including browser-stored passwords, cryptocurrency wallets, and other valuable information.**
- **One tactics involves using a fake CAPTCHA page as a disguise to trick users into executing the malware.**
- LummaC2 Stealer: Windows Malware Stealing Sensitive Data
- Lumma Stealer Malware Analysis, Overview by ANY.RUN
- Malware Analysis Report on Lumma Stealer Malware
- Technical details of Software:
- **Data exfiltration:** The malware effectively gathers sensitive information from targeted applications, including login credentials, financial data, and personal details.
- **Regular updates:** LummaC2 Stealer receives automatic updates on a regular basis.
- **Data log collection:** Lumma Stealer collects detailed data logs from compromised endpoints, including information extracted from browsers and cryptocurrency wallets.
- **Loader capability:** The stealer can drop additional malware onto compromised machines, expanding its malicious capabilities and potential impact.
- Lumma is distributed via fake software, phishing emails, and discord messages.
- C2 using HTTP POST requests and supports payload delivery via Powershell, EXE, and DLL
- rf_export_technical_links_lummac2_mar_1 This is a list of ip's hash's, url, and TTp's
- Lumma Stealer Malware Thrives as Silent Push Uncovers Unique Patterns in the Infostealer's Domain Clusters - Silent Push
- Lumma Stealer: Tactics, Impact, and Defense Strategies - CYFIRMA
- LummaC2 Stealer: Windows Malware Stealing Sensitive Data