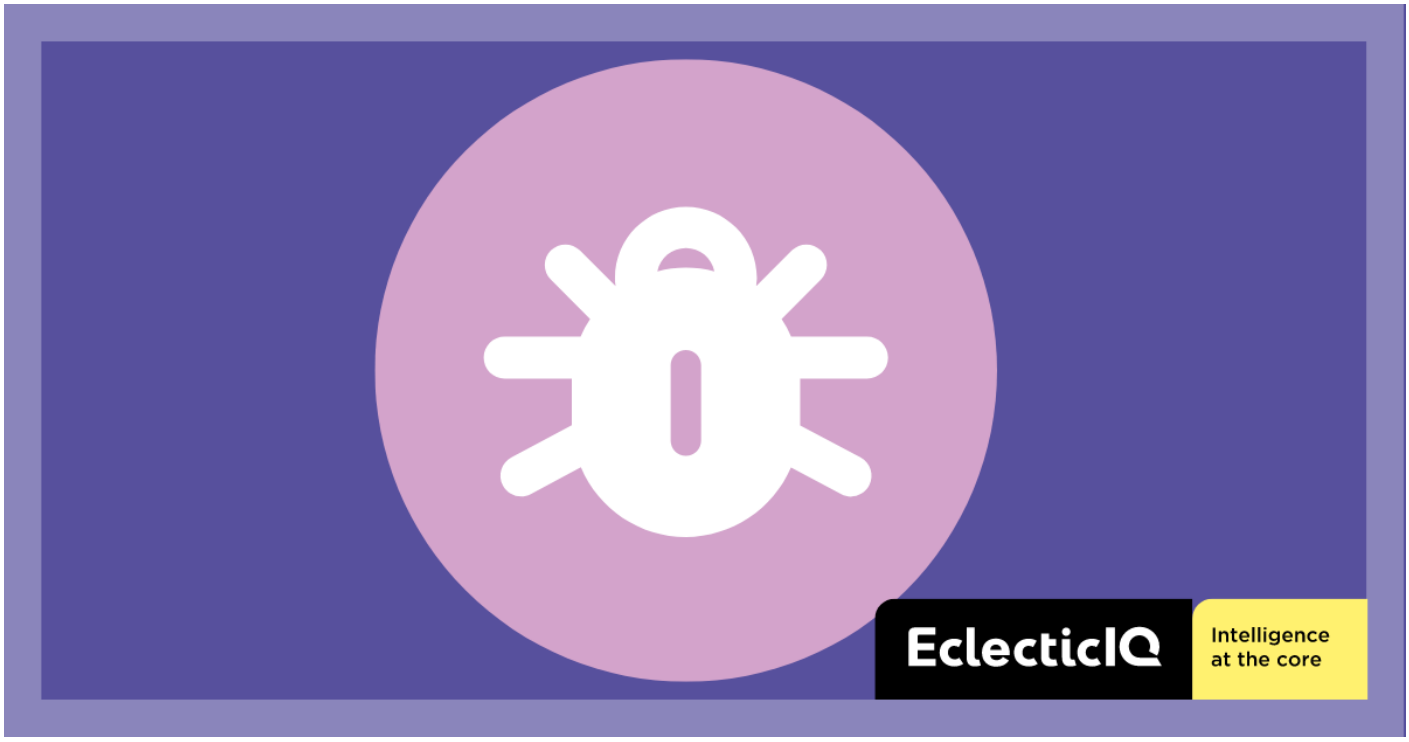
Mustang Panda APT Group Uses European Commission-Themed Lure to Deliver PlugX Malware



EXECUTIVE SUMMARY

- Since at least 2019, the Mustang Panda threat actor group has targeted government and public sector organizations across Asia and Europe [3] with long-term cyberespionage campaigns in line with strategic interests of the Chinese government.
- In November 2022, Mustang Panda shifted from using archive files to using malicious optical disc image (ISO) files containing a shortcut (LNK) file to deliver the modified version of PlugX malware. This switch increases the evasion against anti-malware solutions [2].
- The Mustang Panda APT group loads the PlugX malware in the memory of legitimate software by employing a four-stage infection chain which leverages malicious shortcut (LNK) files, triggering execution via dynamic-link library (DLL) search-order-hijacking.

PLUGX MALWARE EXECUTION FLOW

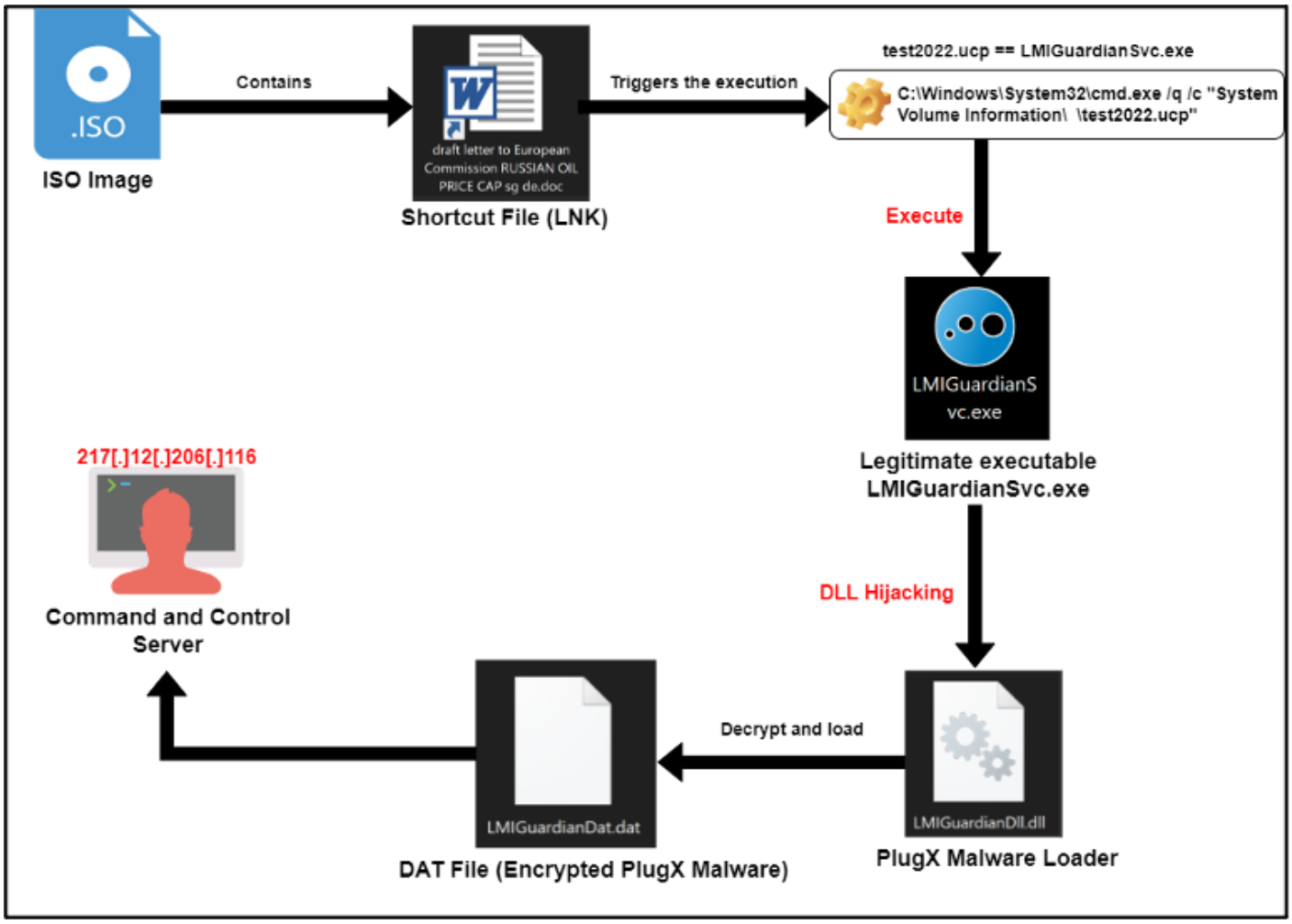


Figure 1 – Execution flow of PlugX malware.

First Stage: PlugX Malware Delivered by ISO Image

In the first stage of the infection chain, EclecticIQ researchers assess that the malware was almost certainly delivered by a malicious email with an ISO image attachment. The ISO image contains a shortcut (LNK) file, but it decoyed as a DOC file called “draft letter to European Commission RUSSIAN OIL PRICE CAP sg de.doc”.

The malicious LNK file contains a command line argument that can be executed by user execution to start the PlugX malware execution chain.

The command line argument of “draft letter to European Commission RUSSIAN OIL PRICE CAP sg de.doc” is shown below:

```
C:\Windows\System32\cmd.exe /q /c "System Volume Information\  \test2022.ucp"
```

The test2022.ucp portion of the command line argument is a renamed legitimate software which is originally called LMIGuardianSvc.exe. This executable is abused to perform DLL hijacking and to load the initial PlugX loader called LMIGuardianDll.dll. The legitimate and malicious executables are placed on the same file path (System Volume Information) to perform DLL Hijacking.

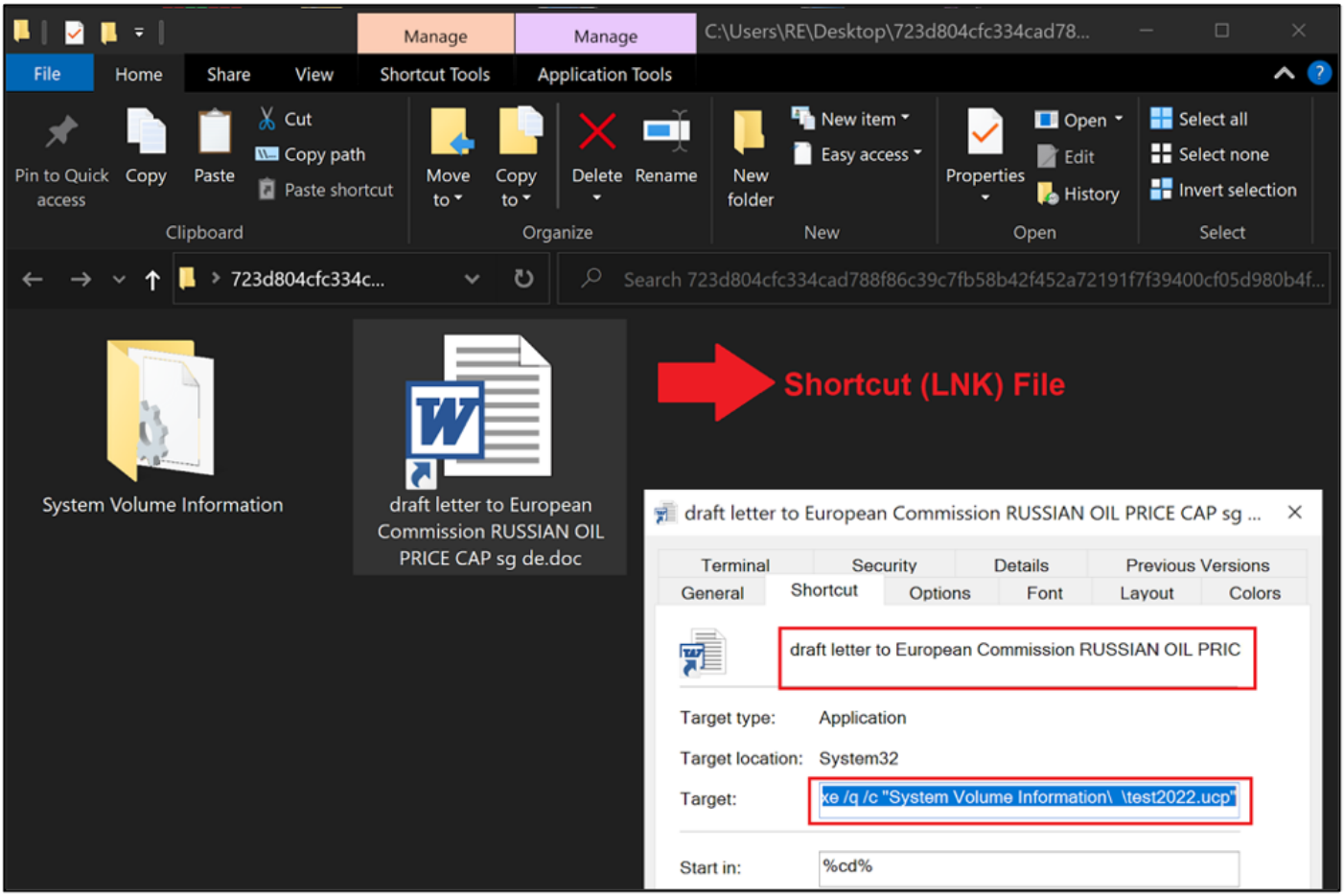


Figure 2 – Command line argument of malicious shortcut (LNK) file.

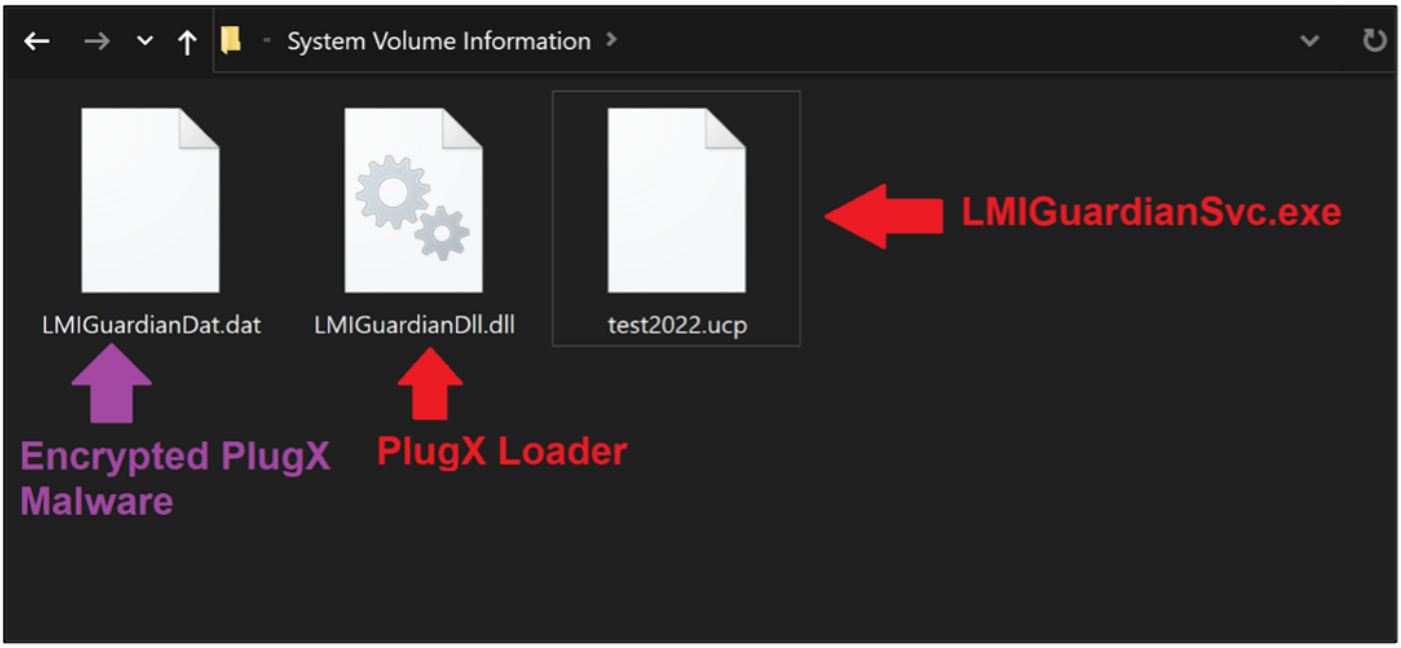


Figure 3 -PlugX malware loader execution file path.

Second Stage: DLL Hijacking Execution Chain to Load PlugX Malware

When a victim clicks on the shortcut file, it executes the command line argument mentioned in first stage, which is a technique called DLL hijacking (after the execution of LMIGuardianSvc.exe, it loads LMIGuardianDll.dll aka PlugX loader automatically). Upon execution of the PlugX loader a Microsoft Office Word document opens. The document is named “draft letter to European Commission RUSSIAN OIL

PRICE CAP sg de.docx". This is a decoy document to trick the user into thinking there is no malicious activity.

One example of the Word document can be seen in the image below:

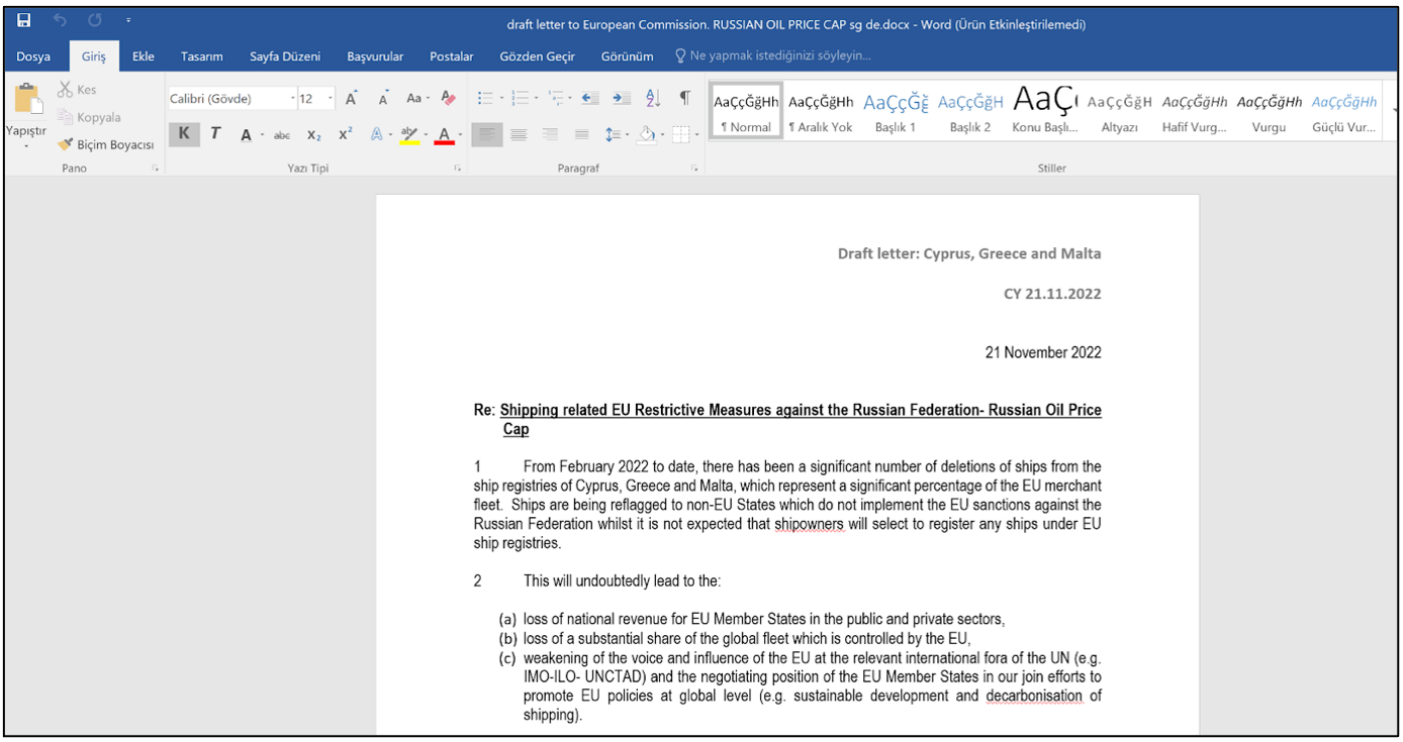


Figure 4 – A decoy Word document is used for social engineering. The victim sees a real Word document open after clicking on a shortcut (LNK) file that has a Word document icon.

The process tree below shows the execution of the legitimate application LMIGuardianSvc.exe, which is executed twice under a new directory (\AppData\Roaming\SamsungDriver) created by the malware and used for persistence access on infected device.

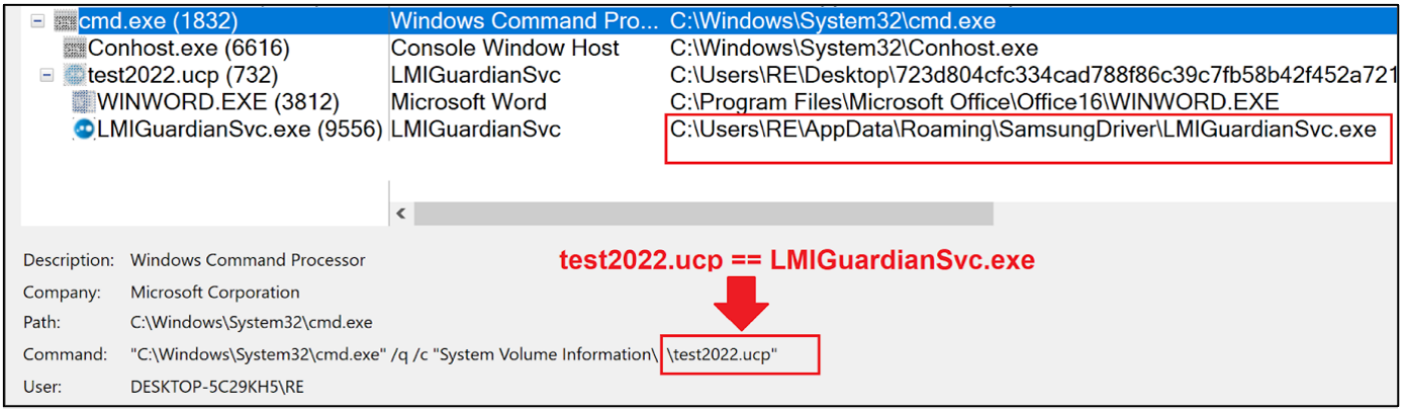


Figure 5 – Captured process tree during the execution of malicious shortcut (LNK) file which masquerades as a word document.

Encrypted shellcode named LMIGuardianDat.dat contains PlugX malware:

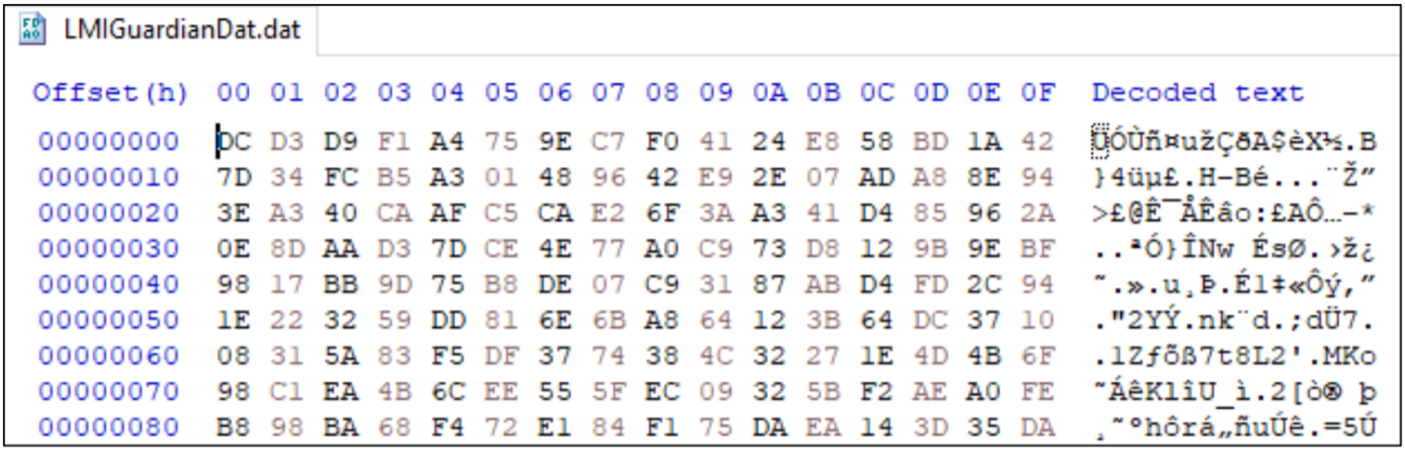


Figure 6 - Encrypted PlugX shellcode in Hex editor.

The PlugX Malware loader decrypts and loads the encrypted shellcode (LMIGuardianDat.dat) inside the LMIGuardianSvc.exe. Injected memory space can be extracted to perform further analysis of decrypted PlugX Malware.

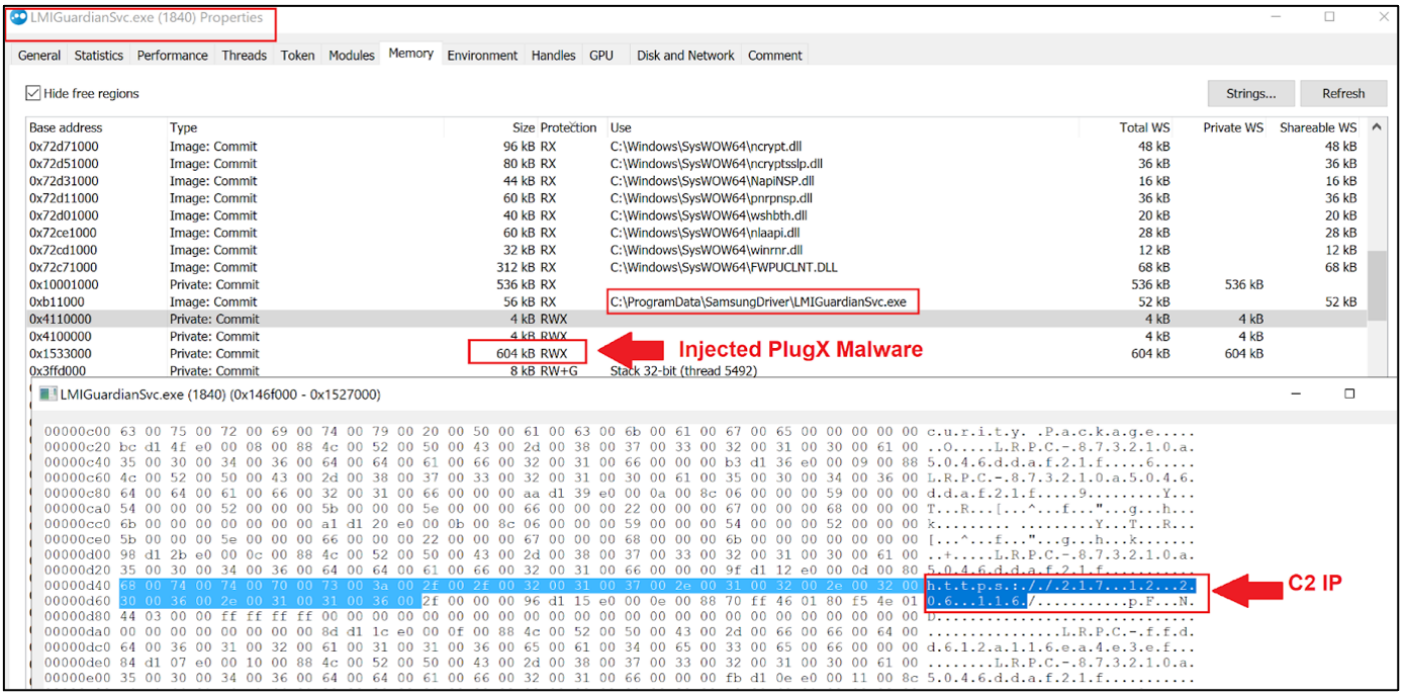


Figure 7 – Memory map of LMIGuardianSvc.exe.

LMIGuardianDLL.dll (PlugX Loader) decrypts the LMIGuardianDAT.dat and loads it in memory of the legitimate process.

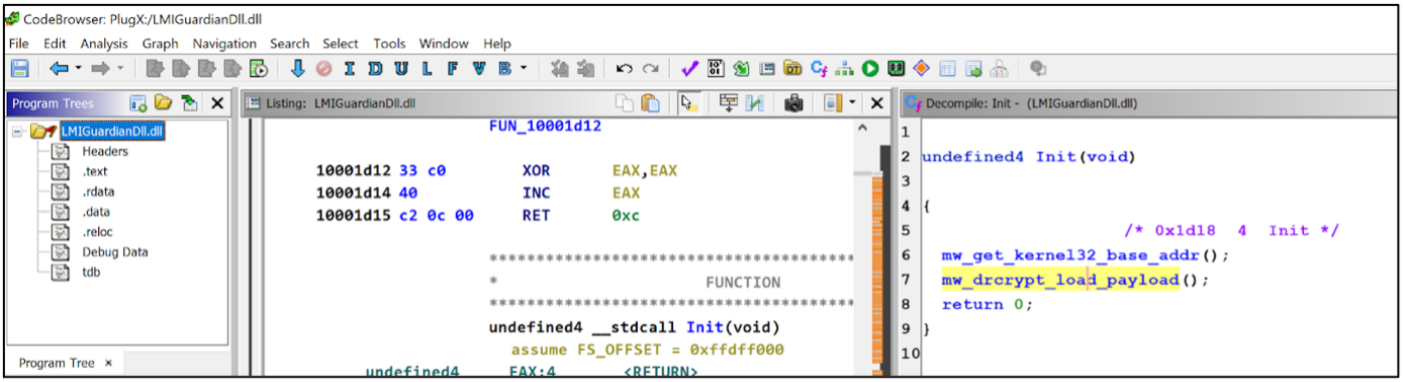


Figure 8 – Decompiled PlugX loader contains decryption function.

During static analysis, EclecticIQ analysts identified that the PlugX malware loader used a simple XOR algorithm to decrypt the LMIGuardianDAT.dat (XOR encrypted PlugX shellcode) to avoid signature-based detection from antimalware solutions.

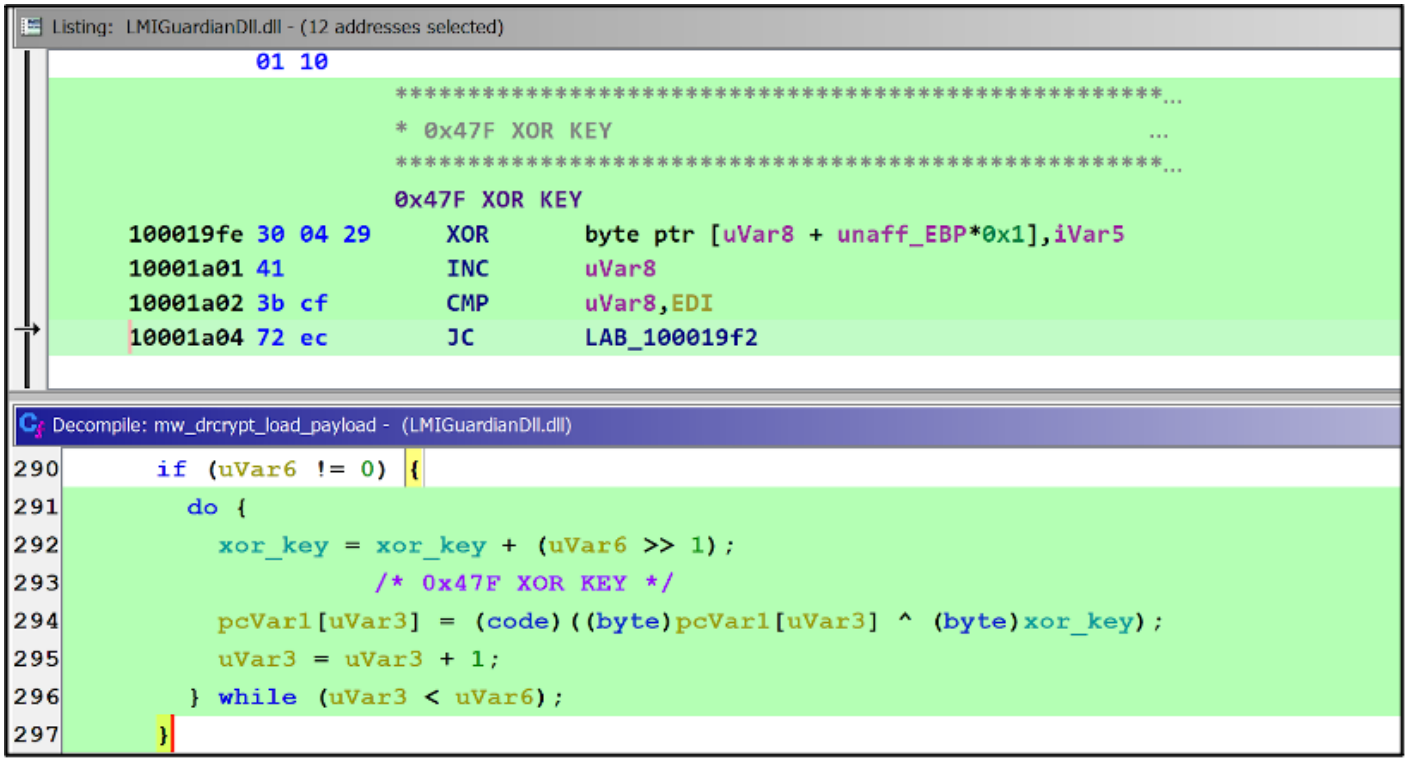


Figure 9 – XOR key is stored statically to perform decryption during execution time of PlugX loader.

PlugX loader used a static XOR key “0x47F”, to decrypt the PlugX shellcode. The below image shows a Python script being used to decrypt the LMIGuardianDAT.dat.

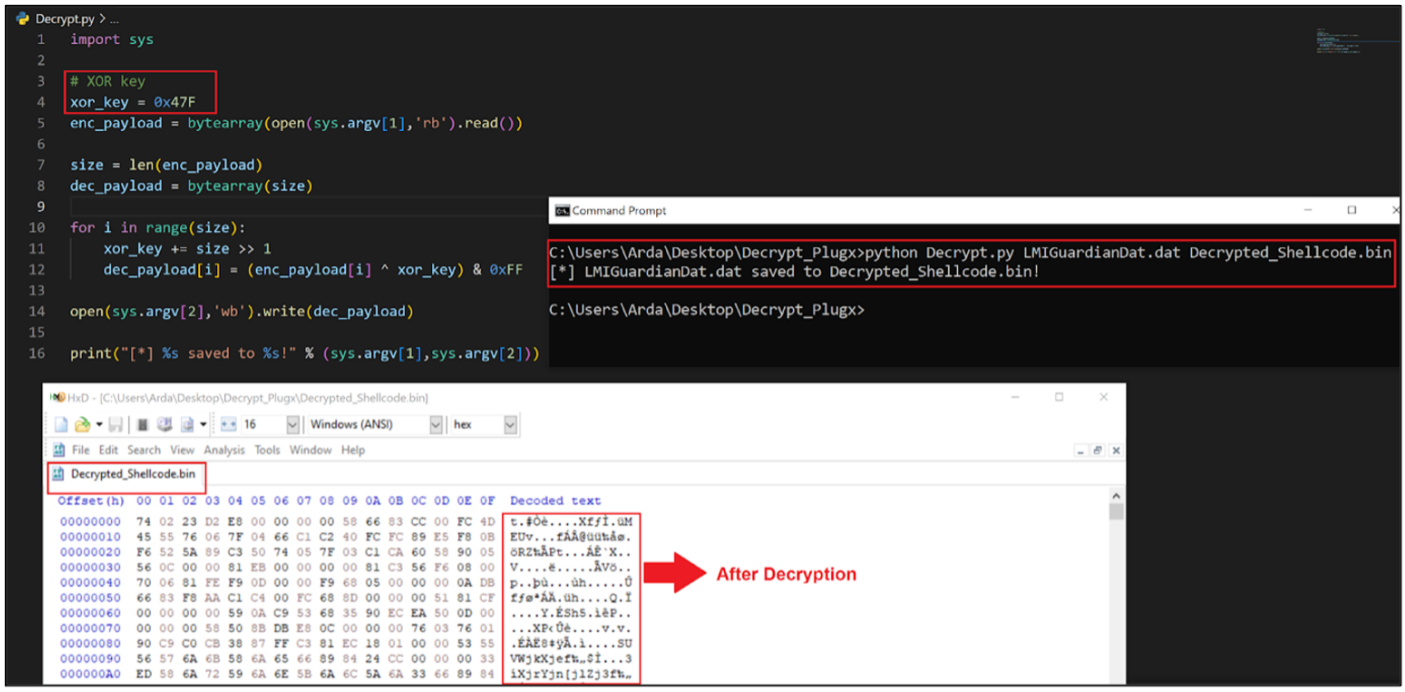


Figure 10 – Decrypted PlugX shellcode.

Once the PlugX malware has been executed in-memory, the C2 config is decrypted. The C2 IP address 217[.]12[.]206[.]116 and the campaign ID of “test2022” are seen in the figures below:

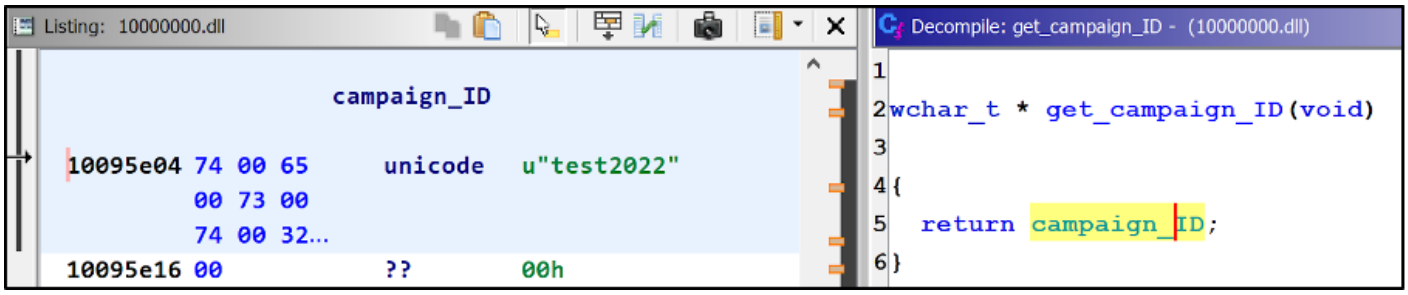


Figure 11 – Decompiled PlugX malware contains campaign ID as a fingerprint of the attack to categorize the victims.

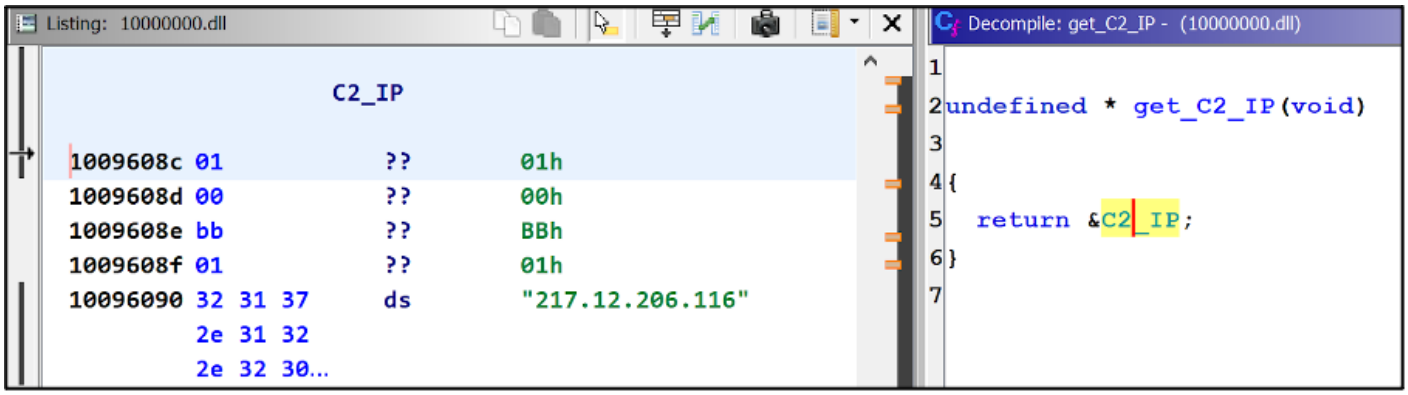


Figure 12 - Decompiled PlugX malware contains command and control (C2) IP address as static.

Third Stage: Registry Run Key Persistence

Mustang Panda abuses Windows registry run keys to gain persistence on the infected system. On Windows operating systems the run registry keys execute the specified program when a user logs on to the device.

The PlugX malware created a new run key called as LMIGuardian Update, shown in the image below.

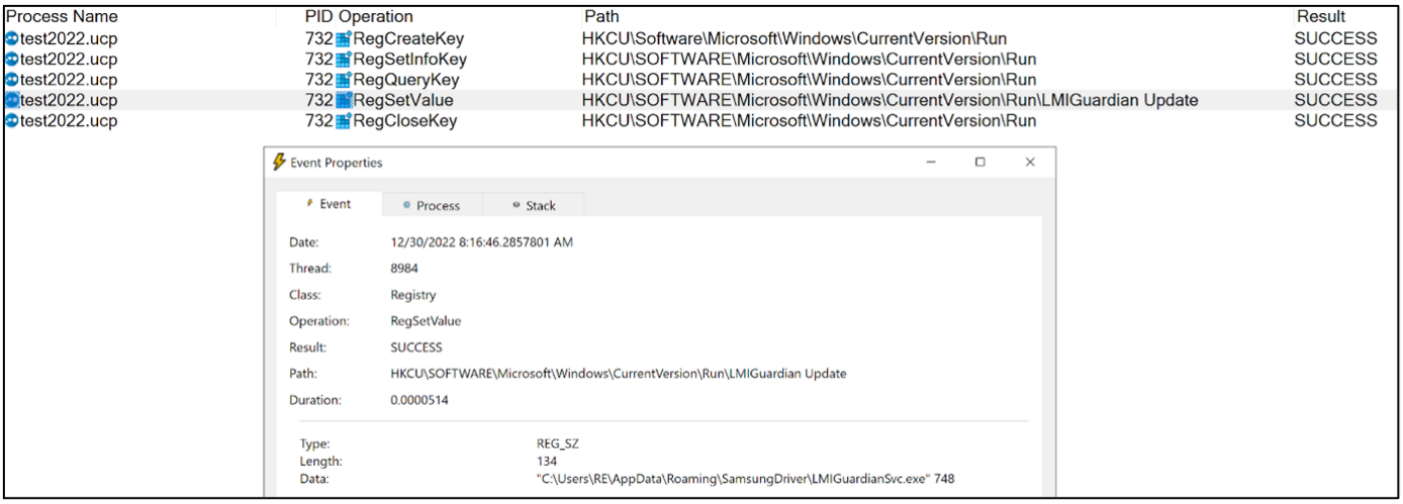


Figure 13 – Persistence established by malware after writing a new Run key.

Every logon will cause the Windows registry run key to execute the LMIGuardianSvc.exe, triggering the DLL Hijacking that leads to PlugX malware execution.

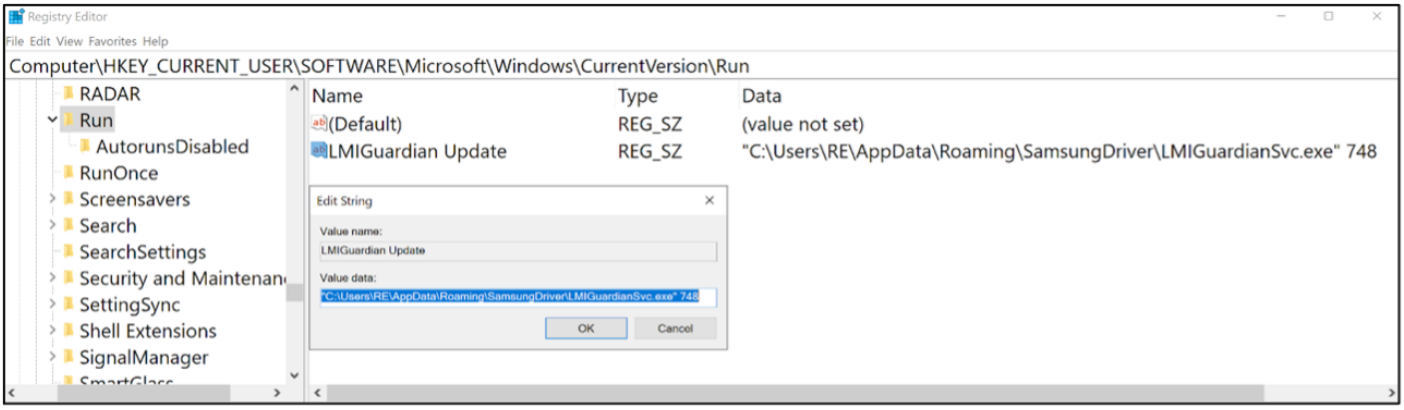


Figure 14 – Written registry key.

The malware creates a new file path which is being used by the persistence mechanism (Run key) to execute the LMIGuardianSvc.exe on this specific file path:

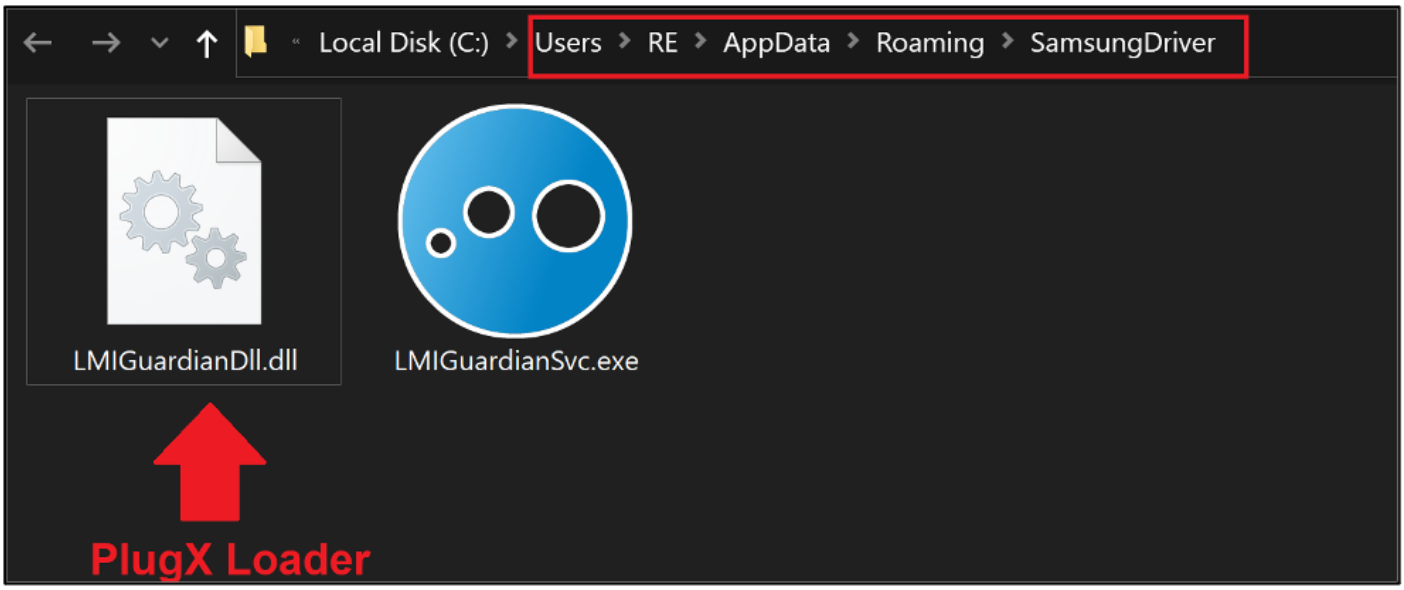


Figure 15 – New file path created for persistence execution of PlugX malware.

Fourth Stage: Command and Control Connection

After a successful execution of PlugX malware, it connects to a remote C2 server which is used to send commands to compromised systems via the PlugX malware and to receive exfiltrated data from a target network.

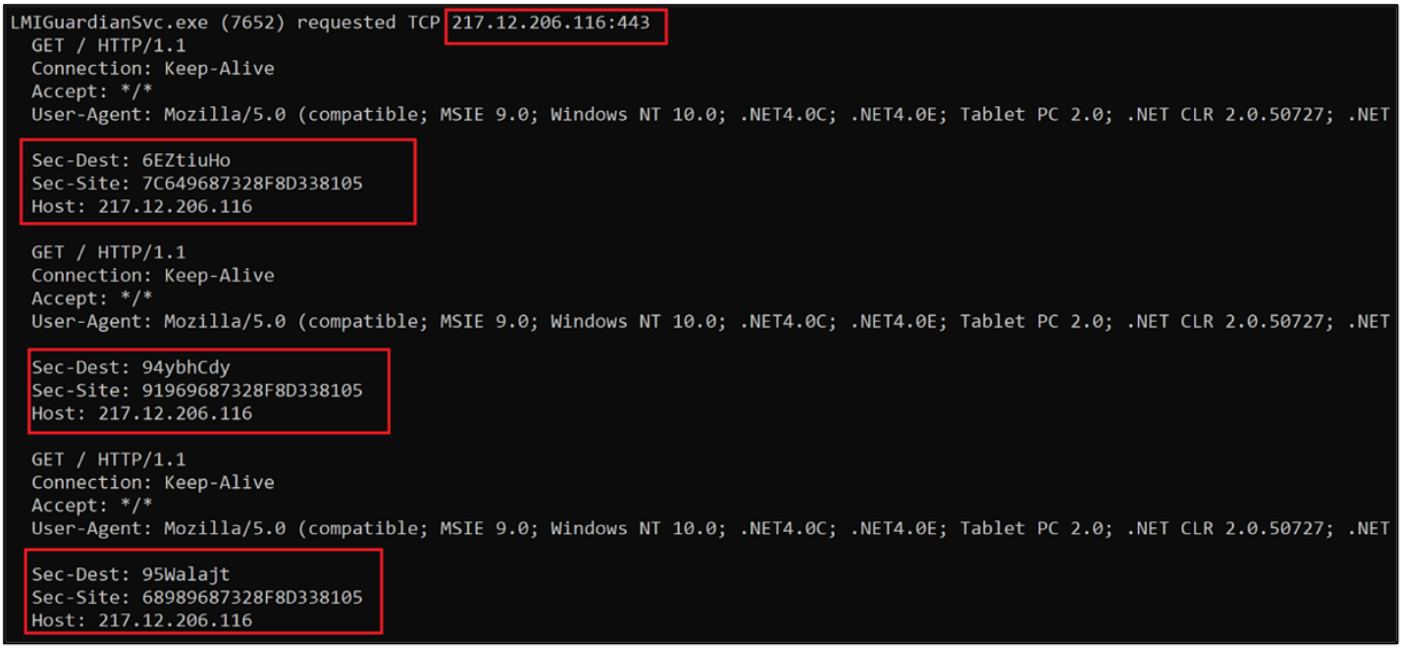


Figure 16 – Request headers and server response observed in Mustang Panda's customized PlugX variant.

Once the device is infected, an attacker can remotely execute several kinds of commands on the affected system. 'Sec-Dest' and 'Sec-Site' HTTP sections contain encrypted data of victim machine information sent to attackers.

Figure 17 - Network capture during the TCP request to remote C2 server over port 443.

The C2 IP address 217[.]12[.]206[.]116 was seen hosting another service on port 8088 with a unique SSL certificate that is itself issued to the IP address 45[.]134[.]83[.]29, which is identified as additional Mustang Panda's infrastructure, according to the BlackBerry Research & Intelligence Team [1].

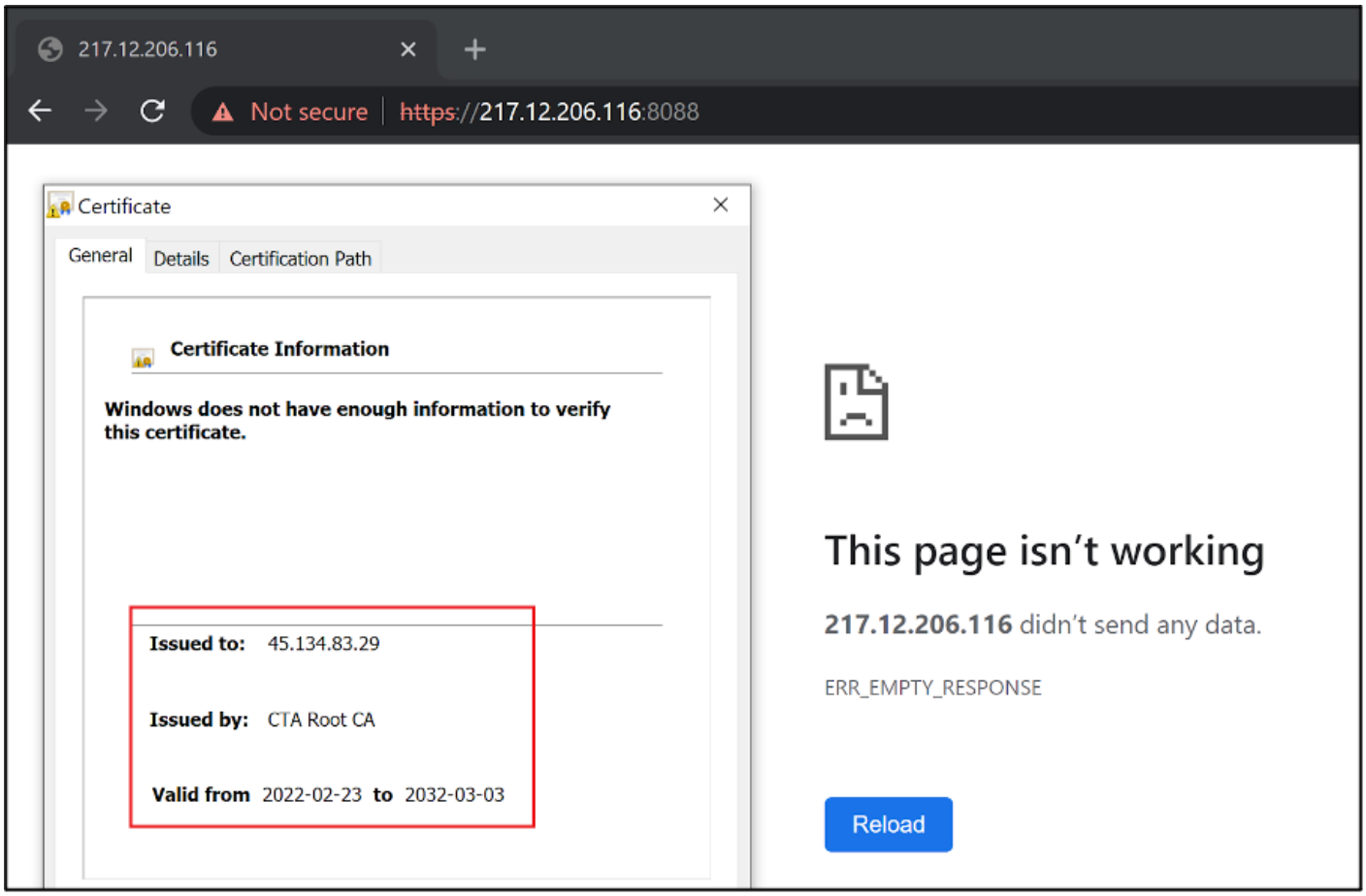


Figure 18 – Issued SSL certificate contains another IP address, which was used by Mustang Panda APT group for previous attacks. [1]

Conclusion

EclecticIQ analysts assess it is almost certain the APT group Musta Panda was responsible for this attack. Mustang Panda has leveraged PlugX malware in previous campaigns targeting the Ukraine and has used similar TTPs like DLL hijacking. The group previously used Windows shortcut (LNK) files disguised using double extensions (such as .doc.lnk) with a Microsoft Word icon and has abused registry run keys for persistence. The SSL certificated used in this attack overlaps with previous Mustang Panda activity targeting the Ukraine.

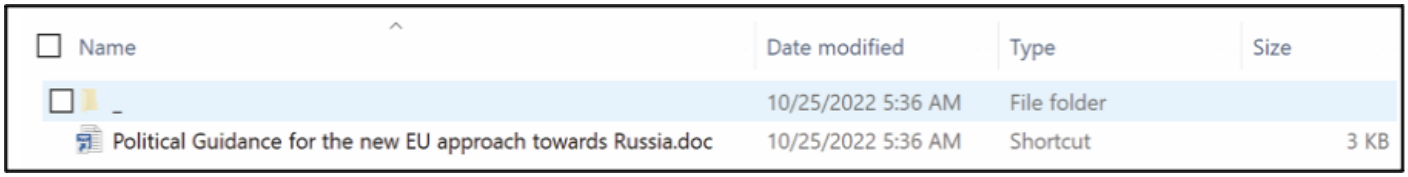


Figure 19 – Example of LNK Phishing lure used by Mustang Panda APT group in their previous attacks. [2]

EclecticIQ analysts assess it is probable the target for this lure document was a European entity. The phishing lure used in the campaign discusses the effect EU sanctions against Russia will have on the European Union. Mustang Panda has targeted European organizations before in a similar campaign in 2022-10-26 [Figure 19]. Mustang Panda APT group continues to be a highly active threat group conducting cyber operations targeting organizations across Europe [2]. EclecticIQ analysts have identified Mustang Panda operators adding new evasion techniques, like using a custom malware loader to execute

encrypted an PlugX sample for the purpose of increasing infection rates and staying under the radar while performing cyber espionage activates against victims.

EclecticIQ analysts assess that it is probable Mustang Panda will increase their activity and continue to use similar TTPs in response to geopolitical developments in Ukraine and Europe, based on an examination of the group's previous cyberespionage activity. Analysts should continue to track Mustang Panda using the TTPs and infrastructure highlighted in the report and the YARA rules provided below.

Mitigations

- Implement basic incident response and detection deployments and controls like network IDS, netflow collection, host-logging, and web proxy, alongside human monitoring of detection sources.
- Employ host-based controls.
- Filter email correspondence and monitor for malicious attachments.
- Identify critical data and implement additional network segmentation and special protections for sensitive information, such as multifactor authentication, highly restricted access, and storage systems only accessible via an internal network.
- Create alerts for disk image file types, such as ISO, and shortcut files, which have been increasingly abused by different threat actors. Furthermore, organizations should consider disabling auto-mounting of ISO or VHD files.
- Configure intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defence mechanisms in place to alert on and upon review, consider blocking connection attempts from unrecognized external IP addresses and domains.

MITRE ATT&CK

Tactic: Technique	ATT&CK Code
Execution: User Execution Malicious File	T1204
Defense Evasion: Hijack Execution Flow DLL Search Order Hijacking	T1574.001
Defense Evasion: Deobfuscate/Decode Files or Information	T1140
Defense Evasion: Masquerading Double File Extension	T1036.007
Command-and-Control: Encrypted Channel Symmetric Cryptography	T1573.001
Command-and-Control: Data Encoding Standard Encoding	T1132.001
Persistence: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001

INDICATORS OF COMPROMISE

Sample File Name(s)	SHA-256 Hash
LMIGuardianDll.dll	ee2c8909089f53aafc421d9853c01856b0a9015eba12aa0382e98417d28aef3f
LMIGuardianDat.dat	8c4926dd32204b6a666b274a78ccfb16fe84bbd7d6bc218a5310970c4c5d9450
draft letter to European Commission RUSSIAN OIL	723d804cfc334cad788f86c39c7fb58b42f452a72191f7f39400cf05d980b4f3

PRICE CAP sg de.iso	
draft letter to European Commission RUSSIAN OIL PRICE CAP sg de.doc.lnk	2c0273394cda1b07680913edd70d3438a098bb4468f16eebf2f50d060cdf4e96
LMIGuardianSvc.exe renamed (test2022.ucp)	26c855264896db95ed46e502f2d318e5f2ad25b59bdc47bd7ffe92646102ae0d

Command and Control Servers

217[.]12[.]206[.]116

45[.]134[.]83[.]29

Hunting Resources: Live Queries & Yara Rules