Malware Campaign Targets InfoSec Community: Threat Actor Uses Fake Proof of Concept to Deliver Cobalt-Strike Beacon

blog.cyble.com/2022/05/20/malware-campaign-targets-infosec-community-threat-actor-uses-fake-proof-of-concept-to-deliver-cobalt-strike-beacon/

May 20, 2022

Recently Cyble researchers came across a post where a researcher mentioned about fake Proof of Concept (POC) of CVE-2022-26809. Upon further investigation, we discovered that it's malware disguised as an Exploit. Similarly, we found a malicious sample that appears to be a fake POC of CVE-2022-24500. Both the malicious samples were available on GitHub. Interestingly both repositories belong to the same profile, indicating the possibility that Threat Actor (TA) might be hosting a malware campaign targeting Infosec Community.

Figures 1 and 2 show the malware hosted on GitHub.

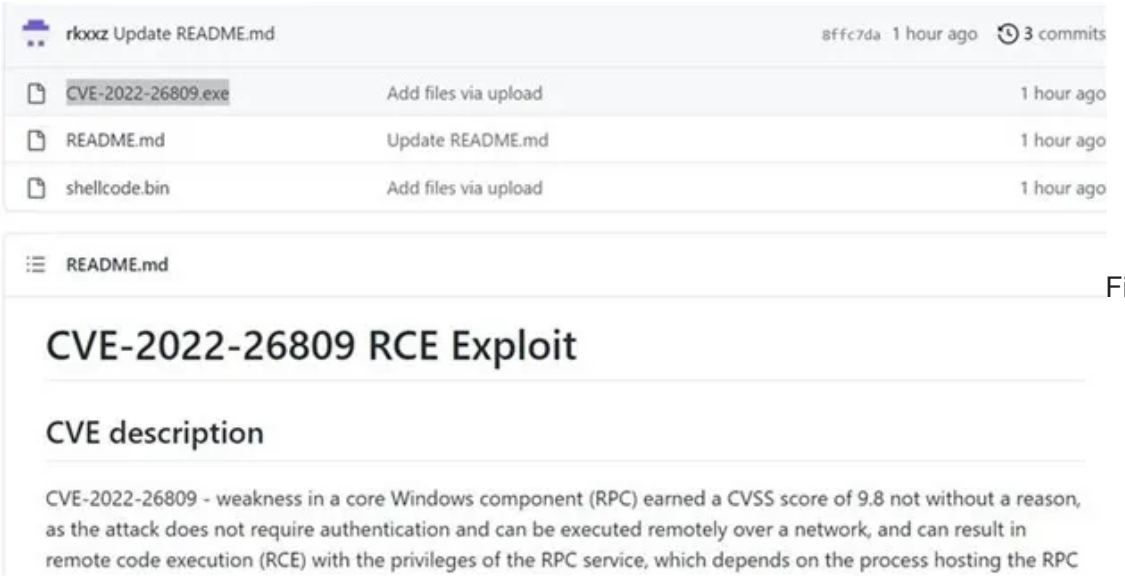

Figure 1: Exploit for CVE-2022-26809

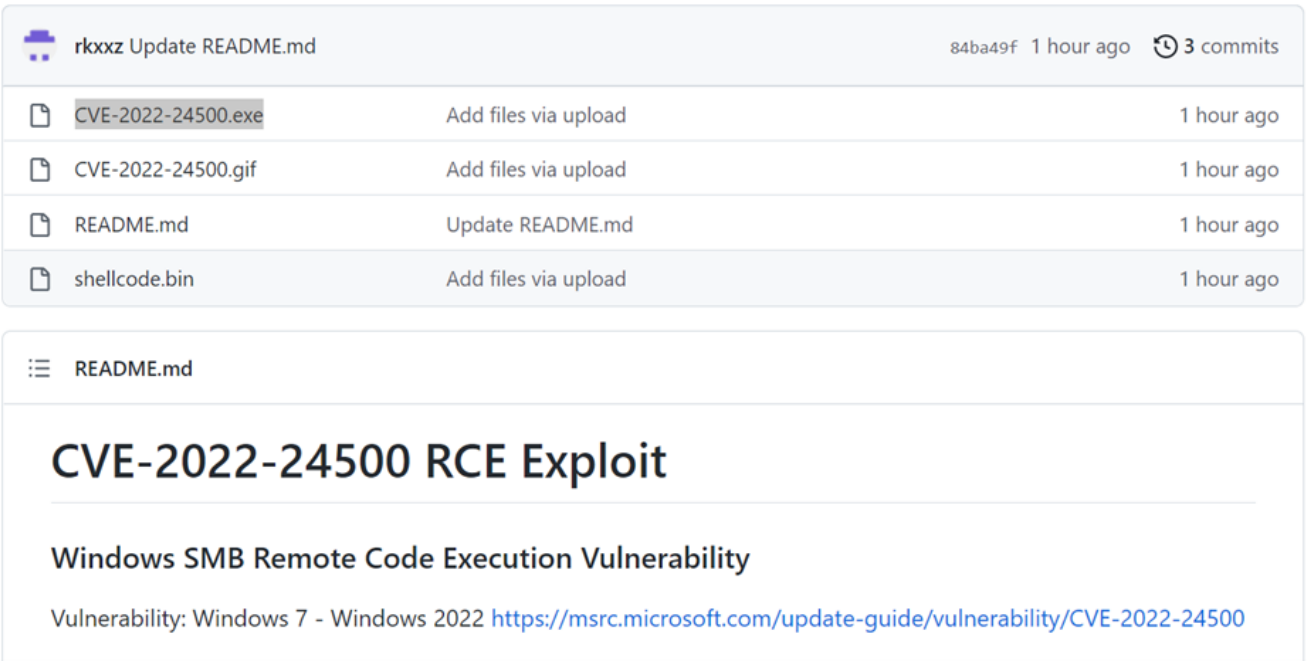

Figure 2: Exploit for CVE-2022-24500

TA used this unique technique to lure individuals into executing the malware. In the last 24 hours, TAs were also discussing these exploits on the cybercrime forum. For example, we came across a post where TAs discussed CVE-2022-24500, pointing to the fake POC GitHub repository, as shown in Figure 3.

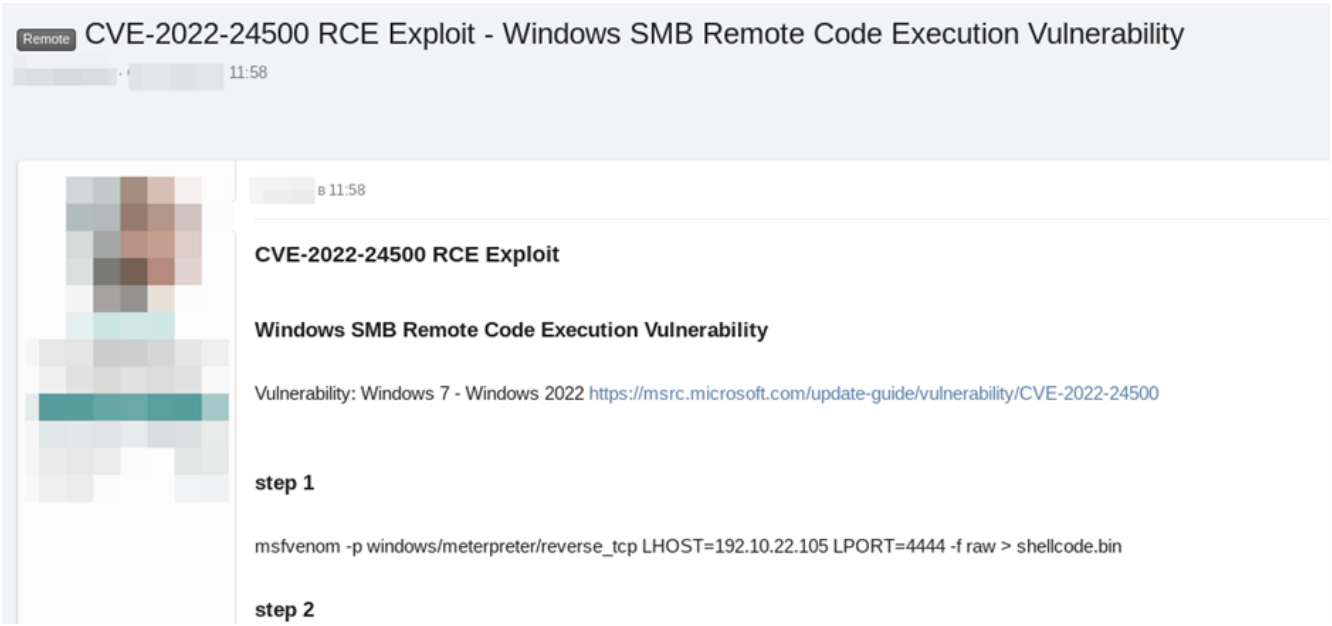

Figure 3: Post on a cybercrime forum

Technical Details:

The malware is a .Net binary packed with ConfuserEX, a free, open-source protector for .NET applications. The figure below shows the file details.

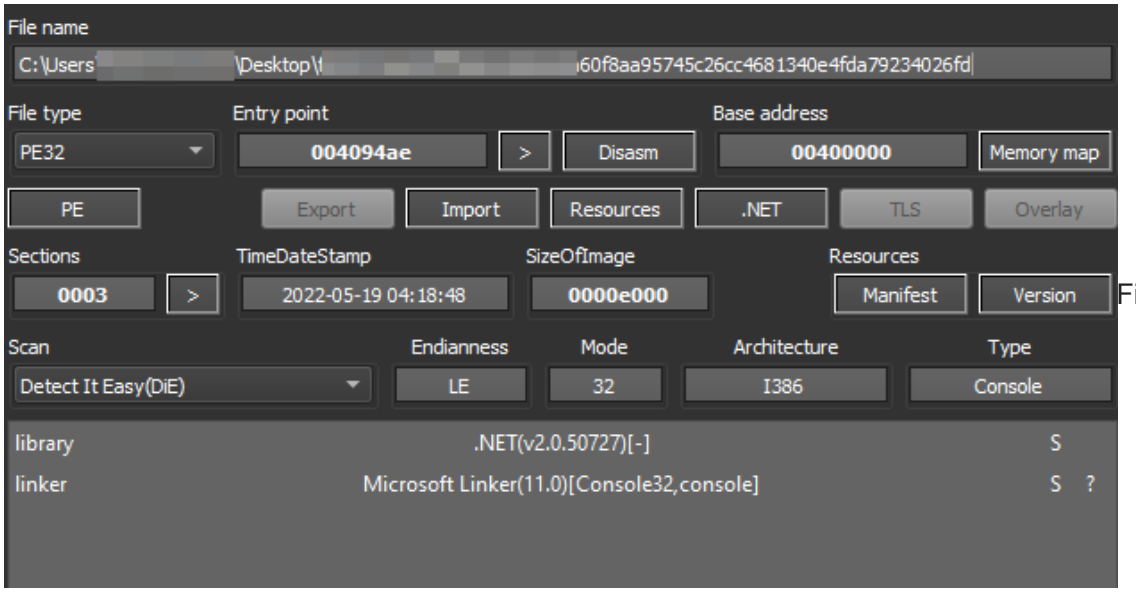

Figure 4: File details

The malware does not have any exploit code targeting the above vulnerabilities. Instead, it prints a fake message showing that it is trying to exploit and executes shellcode, as shown in Figure 5.

```
C:\                                                    >fixed.exe
CVE-2022-24500 SMB Remote Exploit
Usage: exp.exe IP Port
```

```
C:\                                                    >fixed 127.0.0.1 445
CVE-2022-24500 SMB Remote Exploit
[+] Checking... 127.0.0.1 445
[+] 127.0.0.1 445 IsOpen
[+] found low stub at phys addr 13000!
[+] PML4 at 1ad000
[+] base of HAL heap at fffff79480000000
[+] ntoskrnl entry at fffff80645792010
[+] found PML4 self-ref entry 1eb
[+] found HalpInterruptController at fffff79480001478
[+] found HalpApicRequestInterrupt at fffff80645cb3bb0
[+] load shellcode.bin
[+] built shellcode!
[+] KUSER_SHARED_DATA PTE at fffff5fbc0000000
[+] KUSER_SHARED_DATA PTE NX bit cleared!
[+] Wrote shellcode at fffff78000000a00!
[+] Try to execute shellcode!
```

Figure 5: Prints fake message

The malware uses the Sleep() function to print the messages after a small interval, to appear more legitimate. Figure 6 shows the code snippet of malware that print fake messages on execution.

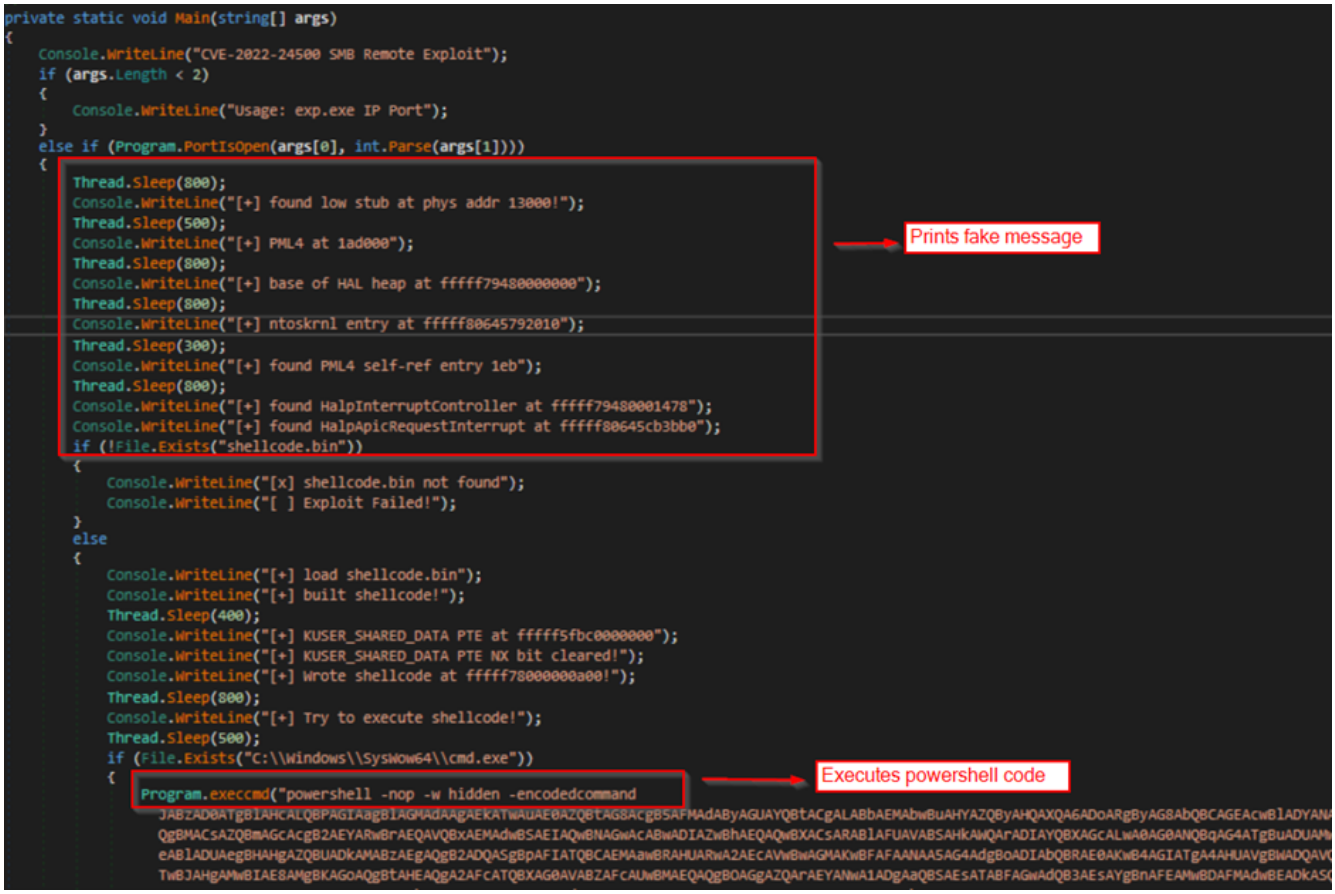

Figure 6: Unpacked Code

After printing the fake message, the malware executes the hidden PowerShell command using cmd.exe to deliver the actual payload. The below figure depicts the network communication to a command-and-control server for downloading the Cobalt-Strike Beacon.

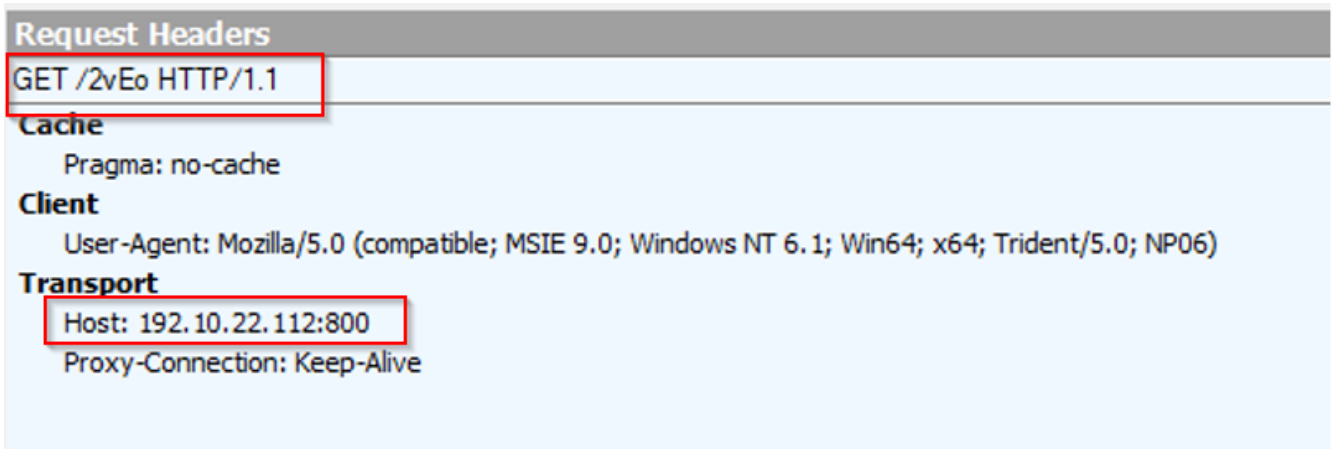

Figure 7: Network communication

The Cobalt-Strike Beacon can be used for other malicious activities such as downloading additional payloads, lateral movement, etc. This fact possibly indicates that the infosec community is also an active target of attackers.

Conclusion

TAs are adopting various techniques to carry out attacks. In this case, we witnessed how the TA used fake POCs to lure the victims into executing the malware. Usually, people working in information security or TAs use exploits to check for vulnerabilities. Hence, this malware might only target people from this community. Therefore, it becomes essential for the Infosec Community members to check the credibility of sources before downloading any proof of concept.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Avoid downloading files from unknown websites.
- Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solution on the employees' systems.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
Command and Control	T1071	Application Layer Protocol

Indicators of Compromise (IOCs)

Indicators	Indicator type	Description
192.10.22.112 45.197.132.72	**IP**	**C2**
7e0c8be0d03c75bbdc6fd286a796434a 0e2e0d26caa32840a720be7f67b49d45094861cb 6c676773700c1de750c3f8767dbce9106317396d66a004aabbdd29882435d5e0	**MD5** **SHA-1** **SHA-256**	Malicious binary
fdcf0aad080452fa14df221e74cca7d0 7431846d707140783eea466225e872f8757533e3 fa78d114e4dfff90a3e4ba8c0a60f8aa95745c26cc4681340e4fda79234026fd	**MD5** **SHA-1** **SHA-256**	Malicious Binary