Chinese APT Hackers Attack Windows Users via FakeNarrator Malware to Implant PcShare Backdoor

gbhackers.com/fakenarrator-malware

BALAJI N September 26, 2019

Chinese APT hackers launching a FakeNarrator malware to attack technology companies using windows computers and implant modified version of open-source PcShare backdoor.

Threat actors loaded this open-source software in victims machine with the help of legitimate NVIDIA application and also deploy the FakeNarrator screen reader application to replace the Windows built-in Narrator, a free screen reader in Microsoft Windows nad bypass the Windows “Easy access” feature.

The malware campaign mainly targeting the tech companies that located in south-east Asia successful attack could allow attackers to gain complete control of the targetted system and take the remote desktop access without any sort of credentials.

Attackers customize the Chinese based opensource backdoor PcShare for their operation and used the backdoor as the main foothold on the victim’s machine.

They included various features in the backdoor including command-and-control (C&C) encryption and proxy bypass functionality and they’re removed some of the unused functionality which they feel not necessary for this campaign.

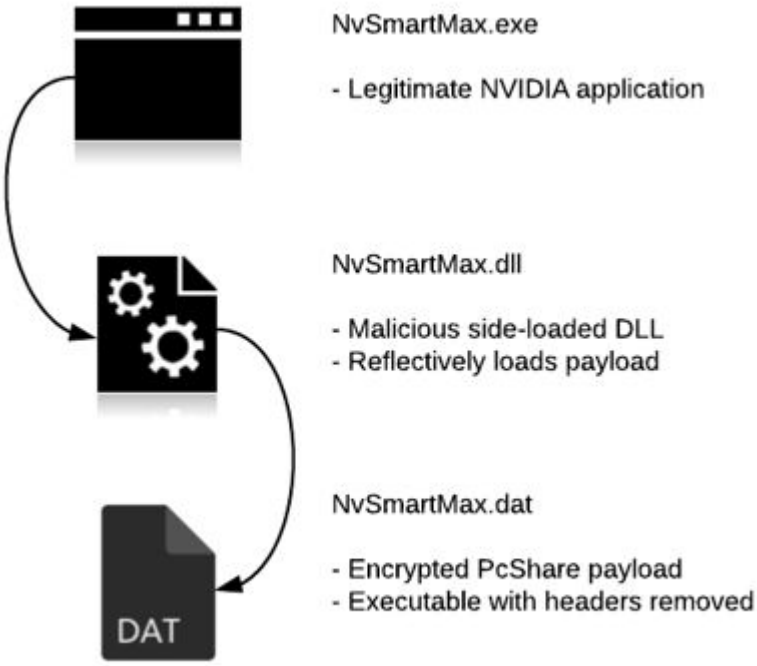
PcShare Backdoor Infection Process

Once the attacker gains access to the victim’s machine, they start deploying the post-exploitation tools which have been developed with the help of publicly available source code that can be accessed via the Chinese programming portal.

Threat actors use one of the post-exploitation tool called bespoke Trojan to abusing the Microsoft Accessibility Features to gain SYSTEM-level access on the compromised machine.

Here the FakeNarrator comes into play, attacker Trojanize the Narrator executable to gain the SYSTEM-level access and maintain the persistence.

According to cylance research ” The campaign is characterized by a fair level of stealthiness as the threat actor made a concerted effort to avoid detection. The use of DLL side-loading technique together with a bespoke loader utilizing memory injection ensures that the main backdoor binary is never dropped to the disk.”



Loader overview

Also, the malware using an anti-sandbox technique to evade the detection by antivirus solutions and protected its command and control server communication.

Researchers also find the PcShare backdoor similarities with Tropic Trooper which is actively targeting government institutions and heavy industry companies in Taiwan and the Philippines.

The backdoor is capable of performing some of following remote administration abilities:

- List, create, rename, delete files and directories
- List and kill processes
- Edit registry keys and values
- List and manipulate services
- Enumerate and control windows
- Execute binaries
- Download additional files from the C&C or provided URL
- Upload files to the C&C
- Spawn command-line shell
- Navigate to URLs
- Display message boxes
- Reboot or shut down the system

“Once the FakeNarrator is enabled at the logon screen via “Ease of Access”, the malware will be executed by winlogon.exe with SYSTEM privileges. Typing the attacker’s defined password will allow the attacker to spawn any executable, also running under the SYSTEM account, at the logon screen” Cylance researchers said.

Its leads to gain the persistence shell on the compromised windows machine without having the valid credentials.

IOCs

SHA256

```
c5226bfd53d789a895559e8bcbedc4ecdde543e54a427b1cb4e5d7ef90756daa
 1899b3d59a9dc693d45410965c40c464224160bbef596f51d35fda099d609744
 bd345155aa4baa392c3469b9893a4751c2372ae4923cf05872bcdc159b9596f8
 49b86ae6231d44dfc2ff4ad777ea544ae534eb40bd0209defffec1eb1fe66b34
 0022508fd02bb23c3a2c4f5de0906df506a2fcabc3e841365b60ba4dd8920e0c
```