Hackers fork open-source reverse tunneling tool for persistence

bleepingcomputer.com/news/security/hackers-fork-open-source-reverse-tunneling-tool-for-persistence/

Bill Toulas

By
Bill Toulas

- March 9, 2022
- 01:24 PM
- 0

Security experts have spotted an interesting case of a suspected ransomware attack that employed custom-made tools typically used by APT (advanced persistent threat) groups.

Although no concrete connection between groups has been uncovered, the operational tactics, targeting scope, and malware customization capabilities signify a potential connection.

As detailed in a report sent to Bleeping Computer by Security Joes, the threat actors observed in an attack against one of its clients in the gambling/gaming industry where a mix of custom-made and readily available open-source tools were used.

The most notable cases are a modified version of Ligolo, a reverse tunneling utility that's freely available for pentesters on GitHub, and a custom tool to dump credentials from LSASS.

Attack in the wild

According to the incident responders at Security Joes, the attack unfolded on a weekend evening and followed a rapid development, showcasing the actors' skills and "red teaming" knowledge.

The initial access came through compromised employee SSL-VPN credentials, followed by admin scans and RDP brute-force, and then credential harvesting efforts.

The subsequent steps involved accessing additional machines with high privileges, the deployment of a custom proxy tunneling for secure communications, and finally, the dropping of Cobalt Strike.

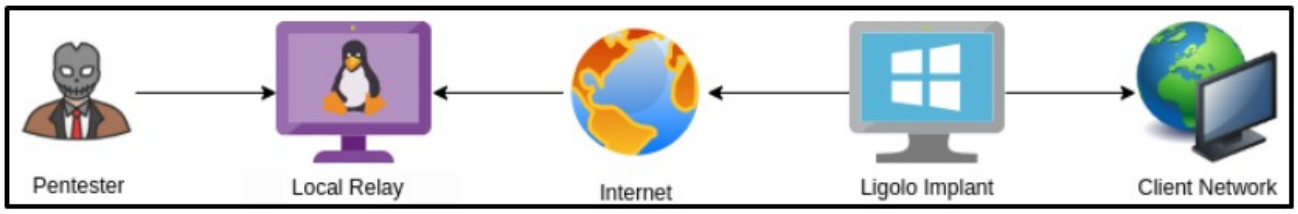
Although the threat actors never had the chance to proceed any further in this particular case, Security Joes believes the next step would be to deploy a ransomware payload, as the methods followed match those of typical ransomware gang operations.

However, this part hasn't been confirmed as the responders stopped the execution of the payload before the infiltrators were ready to deploy anything on the compromised network.

Custom tools

The threat actors used several off-the-shelve open-source tools commonly used by numerous adversaries, like Mimikatz, SoftPerfect, and Cobalt Strike.

One notable differentiation is the deployment of ‘Sockbot’, a GoLang-written utility based on the Ligolo open-source reverse tunneling tool.



Operation of the Ligolo tool *(GitHub)*

The hackers modified Ligolo with meaningful additions that removed the need to use command-line parameters and included several execution checks to avoid running multiple instances.

As a researcher of Security Joes told Bleeping Computer, a customized Ligolo isn't a common sight in the arsenal of any threat actors, apart from the Iranian state-sponsored MuddyWater hacking group, who is the only threat group known to modify it.

The reason for this rarity is that Ligolo isn't suitable for malicious deployment, so to make it fit intrusion operations, coding skills are required.

> "Comparing the new variant (Sockbot) to the original source code available online, the threat actors added several execution checks to avoid multiple instances running at the same time, defined the value of the Local Relay as a hard-coded string to avoid the need of passing command line parameters when executing the attack and set the persistence via a scheduled task." - Security Joes

Another case of particular interest is ‘lsassDumper’, a custom tool also written in GoLang, used by the actors for automatic exfiltration from the LSASS process to the “transfer.sh” service.

Security Joes claims this is the first time lsassDumper has been spotted in the wild, which again demonstrates the particular threat actor's capacity and sophistication.

```
local_2d0 = "[+] Start uploading %s to transfer.sh\n\n";
local_2c8 = (char *)0x27;
local_2c0 = (undefined **)local_238;
local_2b8 = (undefined **)0x1;
local_2b0 = (undefined **)0x1;
FUN_004e6750();
local_148 = ZEXT816(0);
local_138 = ZEXT816(0);
local_128 = ZEXT816(0);
FUN_004642ac();
local_138 = CONCAT88(local_138._8_8_,local_118);
FUN_0044f470();
```

lsassDumper code snippet *(Security Joes)*

Also, direct dumping of credentials from LSASS is another typical method of ransomware gangs, so it's another element that backs this hypothesis.

Finally, the network infiltrators used ADFind for network reconnaissance, a freely available tool that adversaries use to gather information from the Active Directory, also very common in the ransomware space.

"Based on the behavior, the tools seen in this intrusion and the targeted sectors, we concluded that the attackers behind this operation are tightly related to a Russian-speaking ransomware gang, which is taking tools used by other groups and adding their personal signature to them." - concludes the report from Security Joes.

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

Hackers use Conti's leaked ransomware to attack Russian companies

- APT
- Cyberattack
- Ligolo
- Ransomware
- Russian

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

You may also like: