MITRE-ID: G0104

Name: Sharpshooter

Country: Unknown

Description:

This group of APT has been replaced as Operation Sharpshooter.

Operation Sharpshooter was a global cyber espionage campaign that targeted nuclear, defense, government, energy, and financial companies, with many located in Germany, Turkey, the United Kingdom, and the United States. Security researchers noted the campaign shared many similarities with previous Lazarus Group operations, including fake job recruitment lures and shared malware code.

TTPs:

Resource Development:

* the threat actors staged malicious files on Dropbox and other websites.
* the threat actors used the Rising Sun modular backdoor

Initial Access and Execution:

* the first stage downloader resolved various Windows libraries and APIs
* the threat actors relied on victims executing malicious Microsoft Word or PDF files.

Persistence:

* a first-stage downloader installed Rising Sun to %Startup%\mssync.exe on a compromised host.

Privilege Escalation:

* threat actors leveraged embedded shellcode to inject a downloader into the memory of Word.

Defense Evasion:

* threat actors installed Rising Sun in the Startup folder and disguised it as mssync.exe.

Command and control:

* additional payloads were downloaded after a target was infected with a first-stage downloader.
* the threat actors used the ExpressVPN service to hide their location.

Reference:

https://attack.mitre.org/campaigns/C0013/