Cybercrime syndicates FIN7 linked to a spear-phishing campaign

Date: 19th April 2024 | Severity: High

Summary

A spear phishing campaign that targeted organizations in contact with the United States Securities and Exchange Commission filing. These spear phishing email messages carried an infected attachment that upon its opening started a Visual Basic script that installed a backdoor using PowerShell.

Attack Vectors

FIN7's attack started with spear-phishing emails targeting highly privileged employees in the IT department of a large U.S.-based car manufacturer. Links in the emails would take to "advanced-ip-sccanner[.]com," a typosquat of the legitimate scanner project hosted at "advanced-ip-scanner.com."

The researchers discovered that the fake site redirected to "myipscanner[.]com" (now offline). The visitor would next be taken to a Dropbox page offering a malicious executable ('WsTaskLoad.exe') disguised as the legitimate installer for Advanced IP Scanner.

Once executed, the file triggers a multi-stage process involving DLL, WAV files, and shellcode execution, leading to loading and decrypting a file named 'dmxl.bin,' which contains the Anunak backdoor payload.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• arctic-west.com • strideindustrialusa.com • fisrdteditionps.com
URL	• https://bypassociation.com/images/add?type=name

File Hash	• e0e19b748cbe5fd50a5288ec4b29f024 • 732c656660f3ac39bb2fffd243cd0c973c4c01ad695adf29ad81a6cf59a2bed0 • f93ff36c396a0e594ea18811654ce0b7a9bbad8d • b8520cf3ba6f9b3dc709823b0532117c150290bf8dd435678c48eea256052c7edb3eb 6f63e12684d811798bb07cde868d7ba3ecd
IP	• 38.180.1.17 • 109.107.171.62 • 194.156.98.73 • 62.233.57.195 • 207.174.31.206

Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Monitor the network for suspicious activity.
- Educate employees about the risks of ransomware/malware, how to identify phishing attempts, and safe online behavior.

Reference Links

- https://thehackernews.com/2024/04/fin7-cybercrime-group-targeting-us-auto.html
- https://www.bleepingcomputer.com/news/security/fin7-targets-american-automakers-it-staff-in-phishing-attacks/