← Go to listing page

FIN6 group goes from compromising PoS systems to deploying ransomware

Threat Actors April 09, 2019 Cyware Hacker News

- The group was observed to deploy ransomware such as Ryuk and LockerGoga on compromised networks that did not contain any payment data.
- Just like its PoS exploits, FIN6 relied on Windows' Remote Desktop Protocol (RDP) to move laterally across affected networks.

FIN6, which is one of the sophisticated cybercriminal groups, has now moved to deploy ransomware in its attacks. This recent development was uncovered by security firm FireEye when it analyzed a cyber attack performed on an engineering industry. It was found that FIN6 installed ransomware on systems that did not have any payment data on them.

The big picture

- In the attack analyzed by FireEye, FIN6 employed two different techniques after using Windows' RDP to laterally move across the networks. This movement enabled FIN6 to then inject LockerGoga and Ryuk ransomware.
- The first technique involved executing an encoded command through PowerShell. The command downloaded a Cobalt Strike payload, which in turn was configured to drop a malicious payload onto the systems. This payload remains unknown as of now.
- The second technique involved the use of a Windows Service created by Metasploit, that was used to communicate with a C2 server for dropping additional payloads into compromised systems. This would allow FIN6 to escalate privileges in the system.

Worth noting

FireEye suggested that the group's shift to ransomware might be the next method in its extortion related operations. "As the frequency of these intrusions deploying ransomware has increased, the cadence of activity traditionally attributed to FIN6—intrusions targeting point-of-sale (POS) environments, deploying TRINITY malware and sharing other key characteristics—has declined. Given that, FIN6 may have evolved as a whole to focus on these extortive intrusions," the researchers stated in their blog.

As always, advanced cybercriminal groups like FIN6 are continuously evolving to evade security measures and subvert large-scale networks for monetary purposes.

Lateral Movement Techniques | LockerGoga | Trinity | FireEye | Ryuk ransomware

Publisher
Cyware

← PREVIOUS
Zero-day flaw leaves TP-Link routers open to remote att ...
Malware and Vulnerabilities

→ NEXT
Anubis Android trojan spotted stealing PayPal credentia ...
Malware and Vulnerabilities