REvil Ransomware Can Now Reboot Infected Devices

By Akshaya Asokan

Business Continuity Management / Disaster Recovery , Fraud Management & Cybercrime , Governance & Risk Management

MalwareHunterTeam Finds Updated Capabilities (asokan_akshaya) • March 24, 2021

The REvil ransomware gang has added a new malware capability that enables the attackers to reboot an infected device after encryption, security researchers at MalwareHunterTeam report.

See Also: On Demand | Ransomware in 2025: Evolving Threats, Exploited Vulnerabilities, and a Unified Defense Strategy

In a recent tweet, the researchers note that REvil operators have added to the ransomware two new command lines called 'AstraZeneca' and 'Franceisshit' in Windows Safe Mode, which is used to access the Windows devices' startup setting screen.

"'AstraZeneca' is used to run the ransomware sample itself in the safe mode, and 'Franceisshit' is used to run a command in the safe mode to make the PC run in normal mode after the next reboot," MalwareHunterTeam tweeted.

Emsisoft threat analyst Brett Callow told ISMG: “While not unique, the approach is certainly unusual. The most likely reason for REvil introducing this functionality is that it may enable their ransomware to avoid detection by

some security products," as these capabilities enable the attackers to encrypt the files in Windows Safe Mode.

"Causing a Windows computer to reboot in safe mode can disable software, potentially even antivirus or anti-ransomware software, that is working to keep your computer safe," says Erich Kron, security awareness advocate at the security firm KnowBe4. "This would then allow the attackers to make changes that may otherwise not be allowed in normal running mode."

Organizations can help prevent malicious actions by monitoring computers for unexpected reboot activities and by having effective data loss prevention controls in place, Kron says. "Because REvil primarily uses compromised RDP sessions and email phishing for distribution, organizations need to ensure that any internet-accessible RDP instances are secured, preferably with a form of multifactor authentication, and that their employees are stepped through high-quality security awareness training that can help them spot and report phishing attacks."

REvil Activity

REvil, also known as Sodinokibi and Sodin, first appeared in April 2019. The gang behind the ransomware has been tied to several high-profile attacks, such as the May 2020 attacks against celebrity law firm Grubman Shire Meiselas and Sacks and an April 2020 attack on Travelex, a London-based currency exchange that paid a ransom of $2.3 million to regain access to its data.

Recently, the gang reportedly targeted Taiwanese PC-maker Acer by apparently targeting the unpatched ProxyLogon flaw in an on-premises version of Microsoft Exchange server (see: *Acer Reportedly Targeted by Ransomware Gang*).

The REvil gang has continually upgraded its malware and changed its extortion tactics. It now often targets larger organizations in search of much bigger payoffs, publicly names and shames victims through its dedicated leak site and targets victims who have cyber insurance (see: *Charm Offensive: Ransomware Gangs 'Tell All' in Interviews*).

Spike in REvil Attacks

Security researchers have attributed the recent spike in REvil attacks to the gang's growing number of affiliates under its ransomware-as-a-service model (see: *Ransomware: As GandCrab Retires, Sodinokibi Rises*).

A 2019 report by security firm McAfee uncovered at least 41 active affiliates. In another report, McAfee noted that to infect victims, REvil affiliates mainly used remote desktop protocol brute-forcing, phishing, malicious script injection and hacking into IT solutions provided by managed service providers (see: *Ransomware Gangs' Not-So-Secret Attack Vector: RDP Exploits*).
