Antivirus software being disabled by new threat

by Lyle Adriano10 Feb 2020

Cybersecurity experts are cautioning computer users to be wary of a new ransomware that exploits the vulnerabilities of affected devices.UK-based cybersecurity firm Sophos found that the attackers behind two recent cyber cases involving the malware “RobbinHood” had a unique way of skirting around antivirus software to ensure the ransomware caused the most damage to the infected systems.The hackers’ strategy is as follows:First, the cyber attackers gain access to the victim’s network.

Then the hackers install a Gigabyte hardware driver, GDRV.SYS, on the device.

The ransomware actors then exploit a vulnerability in the GDRV.SYS driver to gain kernel access, then utilize the access to temporarily disable the Windows OS driver signature enforcement.

Afterwards, the hackers install a malicious kernel driver named RBNL.SYS. This allows them to disable or stop antivirus and other security products.

Once the way has been cleared of any security roadblocks, the hackers then execute the RobbinHood ransomware.

ZDNet reported that this antivirus bypassing technique works on Windows 7, Windows 8, and Windows 10.Gigabyte had claimed two years ago that its products were not affected by any exploit – even after security researchers who discovered the weakness publicly disclosed details of the vulnerability to raise awareness.

ZDNet said that information from the researchers, particularly their proof-of-concept code which reproduces the vulnerability, was used by the RobbinHood attackers.Public pressure eventually got to Gigabyte to address the issue, but rather than release a patch to fix the exploit, the company chose to discontinue the driver.

However, Sophos found that despite the driver no longer being in use, it can still be exploited among those who still have a copy.“Verisign, whose code signing mechanism was used to digitally sign the driver, has not revoked the signing certificate, so the Authenticode signature remains valid,” the security firm said.