Security Newsletter

16 Jan 2023

Subscribe to this newsletter

Scattered Spider hackers use old Intel driver to bypass security

A financially motivated threat actor tracked as Scattered Spider was observed attempting to deploy Intel Ethernet diagnostics drivers in a BYOVD (Bring Your Own Vulnerable Driver) attack to evade detection from EDR (Endpoint Detection and Response) security products.

The BYOVD technique involves threat actors using a kernel-mode driver known to be vulnerable to exploits as part of their attacks to gain higher privileges in Windows.

Because device drivers have kernel access to the operating system, exploiting a flaw in them allows threat actors to execute code with the highest privileges in Windows.

Read More

More #News

- TikTok slapped with $5.4 million fine over cookie opt-out feature
- CircleCI's hack caused by malware stealing engineer's 2FA-backed session
- Hackers exploit Cacti critical bug to install malware, open reverse shells
- Twitter says leaked data on 200 million users was likely publicly available info

#Breach Log

- Norton Password Manager breach: nearly one million users targeted
- Deserialized web security roundup
- 251k Impacted by Data Breach at Insurance Firm Bay Bridge Administrators
- Beware: Tainted VPNs Being Used to Spread EyeSpy Surveillanceware

#Patch Time!

- Microsoft January 2023 Patch Tuesday fixes 98 flaws, 1 zero-day
- Fortinet: Govt networks targeted with now-patched SSL-VPN zero-day
- Over 100 CVEs Addressed in First Patch Tuesday of 2023

#Tech and #Tools

- Over 1,300 fake AnyDesk sites push Vidar info-stealing malware
- Microsoft: Cuba ransomware hacking Exchange servers via OWASSRF flaw
- Cisco warns of two vulnerabilities affecting end-of-life routers

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us