Neighboring Wi-Fi networks exploited in APT28 attack

Newly discovered nearest neighbor targeting, or the compromise of neighboring Wi-Fi networks, had been leveraged by Russian state-backed threat operation APT28 also known as Fancy Bear, Sofacy, Forest Blizzard, and Gruesome Larch to remotely infiltrate the enterprise Wi-Fi network of a U.S. organization working with Ukraine more than two years ago, reports BleepingComputer.

After unsuccessfully exploiting the targeted organization's Wi-Fi credentials obtained via password spraying attacks due to multi-factor authentication, APT28 resorted to breaching other entities in close proximity before discovering a device within range of the original target, according to a Volexity analysis. Researchers also noted attackers' exploitation of a remote desktop connection to facilitate lateral network movement and data exfiltration. "Volexity further determined that GruesomeLarch was actively targeting Organization A in order to collect data from individuals with expertise on and projects actively involving Ukraine," said Volexity researchers, who noted the findings to emphasize the importance of more robust protections for corporate Wi-Fi networks.

Quelle:	Cyber Security Monitor Worldwide vom 26.11.2024
Ressort:	Cyber Security
Dokumentnummer:	460991134