Bellevue University

Cisco Router Malware Hack

Timothy Jelinek

CYBR250-T301 Intro to Cyber Threats

9/17/2023

The overview of the hacking of the Cisco routers is that it was conducted by someone who is known as APT28. The attack happened in 2021. This attack was against vulnerable Cisco routers and ones with weak SNMP community strings to perform reconnaissance on victim units. APT28 deployed malware on some of the targeted devices which obtained more information and enabled unauthenticated access by the backdoor. This is a scary situation. Cisco is a well-known, big cooperation that has routers everywhere. To know that an intelligence sector in Russia could hack your router to steal your information is something that you might not think about everyday but it becomes very real when it happens.

APT28 is the perpetrator. APT28 is known by the UK National Cyber Security Centre, the US National Security Agency, the US Cybersecurity and Infrastructure Security Agency, and the US Federal Bureau of Investigation, for being the Russian General Staff Main Intelligence Directorate(GRU)85th Special Service Centre(GTsSS) Military Intelligence Unit 26165.

Sources:

"APT28 Exploits Known Vulnerability to Carry Our Reconnaissance and Deploy Malware on Cisco Routers." CISA, cisa.gov, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108. Accessed 17 September 2023.