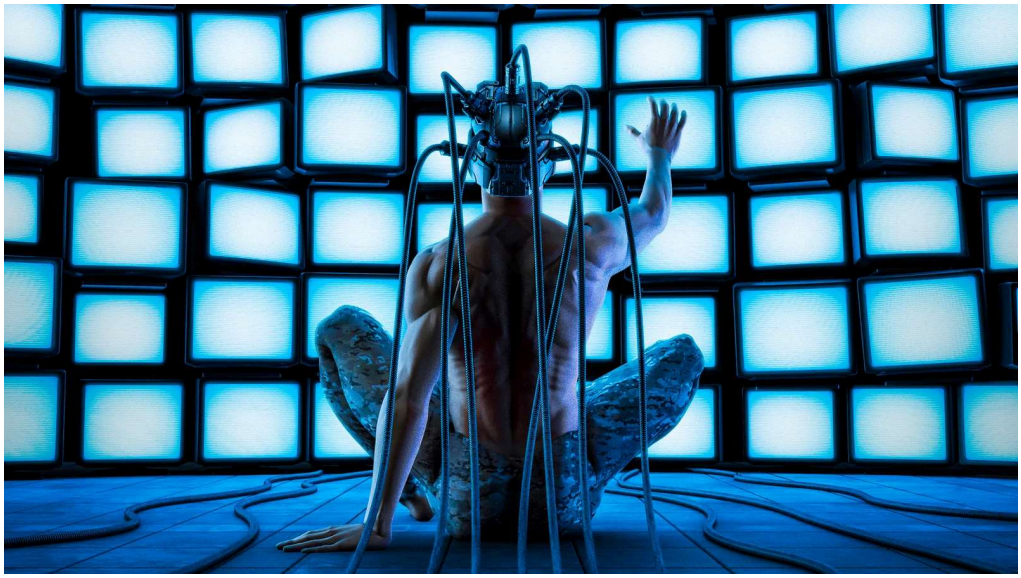
Hacker spins up 1 million virtual servers to illegally mine crypto

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** January 13, 2024 10:09 AM 4



A 29-year-old man in Ukraine was arrested this week for using hacked accounts to create 1 million virtual servers used to mine $2 million in cryptocurrency.

As announced today by Europol (https://www.europol.europa.eu/media-press/newsroom/news/cryptojacker-arrested-in-ukraine-over-eur-1.8-million-mining-scheme), the suspect is believed to be the mastermind behind a large-scale cryptojacking scheme that involves hijacking cloud computing resources for crypto-mining.

By using the computing resources of others' servers to mine cryptocurrency, the cybercriminals can profit at the expense of the compromised organizations, whose CPU and GPU performance is degraded by the mining.

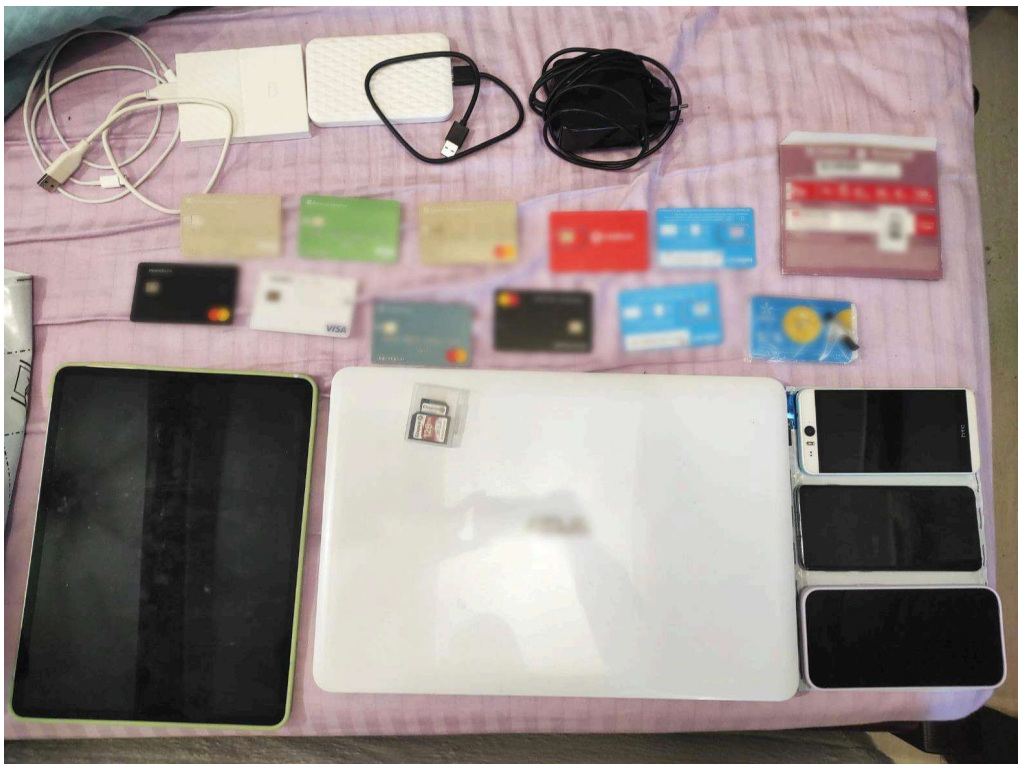
For on-premise compromises, the damage extends to having to pay for increased power usage, commonly generated by miners.

A 2022 report from Sysdig (https://www.bleepingcomputer.com/news/security/cryptominers-hijack-53-worth-of-system-resources-to-earn-1/) estimated the damage from cryptojacking to be about $53 for every $1 worth of Monero (XMR) the cybercriminals mine on hijacked devices.

Europol says they first learned of the cryptojacking attack in January 2023 from a cloud service provider who was investigating compromised cloud accounts on their platform.

Europol, the Ukrainian police, and the cloud provider worked together to develop operation intelligence that could be used to track down and identify the hacker.

The police say they arrested the hacker on January 9th, when they seized computer equipment, bank and SIM cards, electronic media, and other evidence of illegal activity.



Items seized during the suspect's arrest

Source: cyberpolice.gov.ua

A separate report by the Ukrainian cyberpolice (https://cyberpolice.gov.ua/news/zavdav-providnij-svitovij-kompaniyi-sotni-miljoniv-zbytkiv-kiberpolicziya-ta-slidchi-naczpolu-vykryly-xakera-2238/) explains that the suspect has been active since 2021 when he used automated tools to brute force the passwords of 1,500 accounts of a subsidiary of one of the world's largest e-commerce entities.

Europol and Ukraine have not identified the e-commerce company or its subsidiary.

The threat actor then used these accounts to gain access to administrative privileges, which were used to create more than one million virtual computers for use in the cryptomining scheme.

The Ukrainian authorities confirmed that the suspect was using TON cryptocurrency wallets to move the illegal proceeds, with transactions equal to roughly $2 million.

The arrested individual now faces criminal charges under Part 5 of Art. 361 (unauthorized interference in the work of information, electronic communication, electronic communication networks) of the Criminal Code of Ukraine.

Mitigating the risk

Threat actors commonly target cloud services to hijack computing resources for illegal cryptocurrency mining.

Methods to defend against cryptojacking attacks include monitoring for unusual activity like unexpected spikes in resource usage, implementing endpoint protection and intrusion detection systems, and limiting administrative privileges and access to critical resources only to those needing them.

Cryptojackers often exploit documented flaws in cloud platforms to achieve an initial compromise. So, regularly applying the available security updates on all software is crucial to protecting systems against external threats.

Finally, all administrative accounts should have 2FA enabled in case their credentials are stolen.