# Microsoft seizes web domains used by North Korean hackers

December 31 2019


Microsoft said it took over online domains used by North Korean hackers, in the fourt operation of its kind against a nation-state entity

Microsoft said Monday it obtained a court order allowing it to seize web domains used by North Korean hacking groups to launch cyberattacks on

human rights activists, researchers and others.

The US technology giant said a federal court allowed it to take control of 50 domains operated by a group dubbed Thallium, which tricked online users by fraudulently using Microsoft brands and trademarks.

"This network was used to target victims and then compromise their online accounts, infect their computers, compromise the security of their networks and steal sensitive information," said Tom Burt, Microsoft's vice president for customer security and trust.

"Based on victim information, the targets included government employees, think tanks, university staff members, members of organizations focused on world peace and human rights, and individuals that work on nuclear proliferation issues. Most targets were based in the US, as well as Japan and South Korea."

Microsoft, which had been investigating the group through its Digital Crimes Unit and Threat Intelligence Center, said the hacking group sent spoofed emails that appeared to come from Microsoft which tricked users into revealing their login credentials, a technique known as spear phishing.

"By gathering information about the targeted individuals from social media, public personnel directories from organizations the individual is involved with and other public sources, Thallium is able to craft a personalized spear-phishing email in a way that gives the email credibility to the target," Burt said.

After getting the victim's credentials, the hackers can access emails, contact lists, calendar appointments and other data and often forwards any new emails to the attackers.

The hackers also used malicious software which can access other data on a victim's computer.

An order from a US federal court in Virginia allowed Microsoft to take control of the domains, meaning "the sites can no longer be used to execute attacks," Burt said.

Microsoft said this was the fourth nation-state group it has acted against and follows similar moves against operations from China, Russia and Iran, dubbed Barium, Strontium and Phosphorus, respectively.