Log4Shell attacks expand to nation-state groups from China, Iran, North Korea, and Turkey

By Catalin Cimpanu

Published: 2023-01-18 · Archived: 2026-04-05 17:24:11 UTC

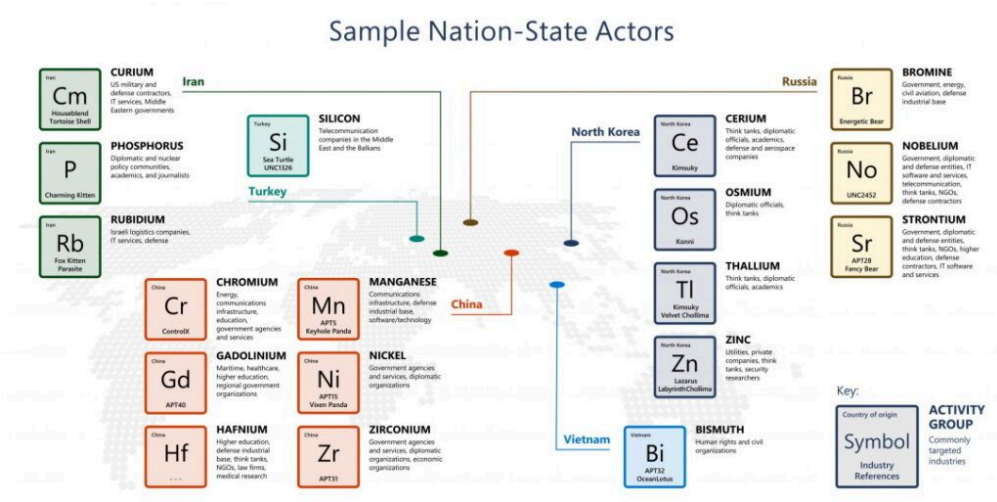
Nation-state groups from China, Iran, North Korea, and Turkey are now abusing the Log4Shell (CVE-2021-44228) vulnerability to gain access to targeted networks, Microsoft said on Tuesday.

"This activity ranges from experimentation during development, integration of the vulnerability to in-the-wild payload deployment, and exploitation against targets to achieve the actor's objectives," the company said in an update on its Log4Shell guidance blog post.

Known threat actors linked to Log4Shell attacks include Phosphorus (Iran) and Hafnium (China). Microsoft did not name the threat actors operating out of North Korea and Turkey.

"For example, MSTIC has observed PHOSPHORUS, an Iranian actor that has been deploying ransomware, acquiring and making modifications of the Log4j exploit," Microsoft said yesterday.

"In addition, HAFNIUM, a threat actor group operating out of China, has been observed utilizing the vulnerability to attack virtualization infrastructure to extend their typical targeting. In these attacks, HAFNIUM-associated systems were observed using a DNS service typically associated with testing activity to fingerprint systems," the company added.



In addition, Microsoft said it has also observed multiple threat actors who serve as initial access brokers for ransomware gangs using the Log4Shell exploit to gain a foothold on corporate networks.

These groups typically sell access to these hacked networks to ransomware gangs, and Microsoft worries that Log4Shell may contribute to a spike in ransomware attacks over the coming months.

The company's fears aren't an isolated sentiment, having also been echoed by many security experts over the past few days since the Log4Shell vulnerability came to light.

A first ransomware operation leveraging the Log4Shell exploit was spotted on Sunday.
Named Khonsari ("bloodshed" in Persian), the ransomware was categorized as a low-effort skidware that tried to frame a person of Iranian descent living in Louisiana as the attacker, providing no way for victims to recover encrypted files.

This attack was one of the several malware operations that have targeted the Log4Shell exploit and used it to spread to vulnerable systems. Over 60 variations of the Log4Shell exploit have been observed in the wild so far, and attacks have been linked to DDoS botnets, crypto-mining operations, and commodity malware like StealthLoader.

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
