They slept on networks for 393 days! Chinese state hackers and the BRICK

Data: 2025-09-25 12:30:22

Autor: Inteligência Against Invaders

Redazione RHC**:25 September 2025 14:29**

According to **Google Threat Intelligence** , the China-linked espionage group **UNC5221** has carried out a *series of successful intrusions into corporate networks since March of this year,* exploiting previously unknown vulnerabilities in Ivanti products.

The attacks involved the introduction of backdoors that allowed attackers to maintain access to victims' infrastructure **for an average of 393 days.**

Experts have attributed the actions to the UNC5221 group and other related Chinese cyberespionage groups. According to the report *, UNC5221 began actively exploiting vulnerabilities in Ivanti devices as early as 2023.* Google emphasizes that this group *is not associated with Silk Typhoon (formerly Hafnium),* suspected of hacking the U.S. Treasury Department in December.

This is a financially motivated (FIN) or state-sponsored APT group, although the origin of UNC5221 clearly indicates state support. Since spring 2025, *Mandiant experts have responded to incidents related to this group across a wide range of industries, from law firms to SaaS providers and corporate outsourcing companies.* In most cases, the attackers **used a specially developed backdoor, BRICKSTORM,** implanted in devices that do not support traditional detection methods (EDR).

This allowed the attackers to slip through unnoticed: organizations' security systems simply didn't detect the malicious activity. To help identify infections, Google released *a free scanning tool that doesn't require YARA installation and is suitable for Linux and BSD-based systems* .

It looks for signatures and unique patterns in the code that are characteristic of BRICKSTORM. *Mandiant representatives emphasize that the number of infections could become significant once organizations begin mass scanning their devices:* the effects of this campaign are expected to be evident over the next one to two years.

In at least one case, state-run hackers gained access to **Ivanti Connect Secure via a zero-day vulnerability.** While Google did not specify the specific vulnerability, researchers had previously linked *UNC5221 to the active exploitation of* CVE-2023-46805 *and* CVE-2024-21887*, both of which were only publicly disclosed in January 2024.*

After penetrating the network, the attackers installed BRICKSTORM, a malware written in Go and equipped with proxy functionality (SOCKS). Although a Windows version is mentioned , Mandiant experts have not observed it directly; evidence of this modification is indirect. *Indeed, the malware*

has been detected on Linux and BSD devices, including network devices from various manufacturers.

UNC5221 **regularly attacks VMware vCenter servers and ESXi hosts,** often starting on edge devices and then using stolen credentials to penetrate deeper into the network. In one attack, BRICKSTORM was introduced into vCenter after the incident investigation began, **demonstrating the adversary's ability to adapt in real time and monitor defenders' actions** . The malware was also modified, using Garble obfuscation tools, custom wssoft libraries, and, in one case **, a timer to delay activity until a specific date.**

Additionally, in several cases, the attackers used additional malware: **BRICKSTEAL** , a *malicious Java Servlet filter for Apache Tomcat* that runs within the vCenter web interface. It intercepts HTTP Basic Auth headers, extracting login and password data, including domain credentials if the organization uses Active Directory. Installing a filter typically requires configuration changes and a server reboot, but *in this case, the attackers used a special dropper that injected code into memory without rebooting the server, further improving stealth.*

As part of the attacks, the attackers *also gained access to the email accounts of key employees: developers, system administrators, and other specialists whose activities could be of interest to Chinese economic or intelligence interests.* To do so, they exploited Microsoft's Entra ID corporate applications with mail.read or full_access_as_app privileges, allowing access to any email within the organization.

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli