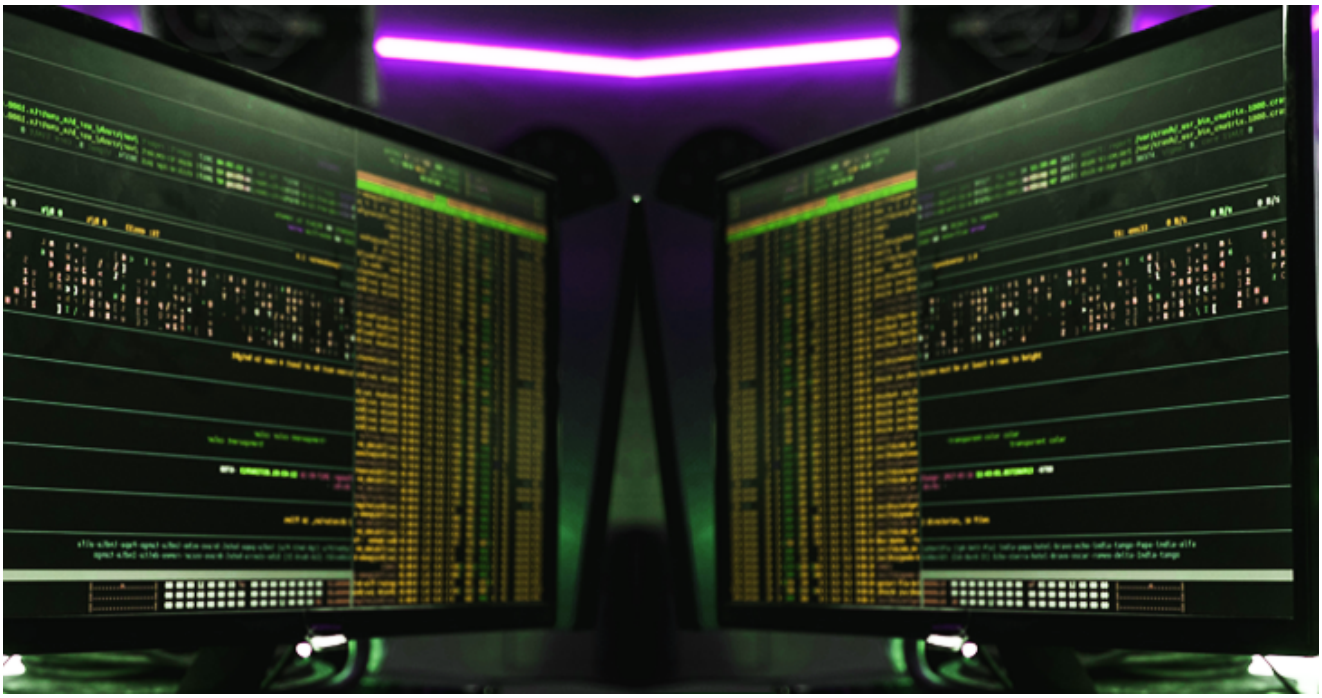
Chinese Hackers Exploited Recent Fortinet Flaw as 0-Day to Drop Malware

thehackernews.com/2023/01/new-chinese-malware-spotted-exploiting.html

January 20, 2023



A suspected China-nexus threat actor exploited a recently patched vulnerability in Fortinet FortiOS SSL-VPN as a zero-day in attacks targeting a European government entity and a managed service provider (MSP) located in Africa.

Telemetry evidence gathered by Google-owned Mandiant indicates that the exploitation occurred as early as October 2022, at least nearly two months before fixes were released.

"This incident continues China's pattern of exploiting internet facing devices, specifically those used for managed security purposes (e.g., firewalls, IPS\IDS appliances etc.)," Mandiant researchers said in a technical report.

The attacks entailed the use of a sophisticated backdoor dubbed **BOLDMOVE**, a Linux variant of which is specifically designed to run on Fortinet's FortiGate firewalls.

The intrusion vector in question relates to the exploitation of CVE-2022-42475, a heap-based buffer overflow vulnerability in FortiOS SSL-VPN that could result in unauthenticated remote code execution via specifically crafted requests.

Earlier this month, Fortinet disclosed that unknown hacking groups have capitalized on the shortcoming to target governments and other large organizations with a generic Linux implant capable of delivering additional payloads and executing commands sent by a remote server.

The latest findings from Mandiant indicate that the threat actor managed to abuse the vulnerability as a zero-day to its advantage and breach targeted networks for espionage operations.

"With BOLDMOVE, the attackers not only developed an exploit, but malware that shows an in-depth understanding of systems, services, logging, and undocumented proprietary formats," the threat intelligence firm said.

The malware, written in C, is said to have both Windows and Linux flavors, with the latter capable of reading data from a file format that's proprietary to Fortinet. Metadata analysis of the Windows variants of the backdoor shows that they were compiled as far back as 2021, although no samples have been detected in the wild.

BOLDMOVE is designed to carry out a system survey and is capable of receiving commands from a command-and-control (C2) server that in turn allows attackers to perform file operations, spawn a remote shell, and relay traffic via the infected host.

An extended Linux sample of the malware comes with extra features to disable and manipulate logging features in an attempt to avoid detection, corroborating Fortinet's report.

"The exploitation of zero-day vulnerabilities in networking devices, followed by the installation of custom implants, is consistent with previous Chinese exploitation of networking devices," Mandiant noted.