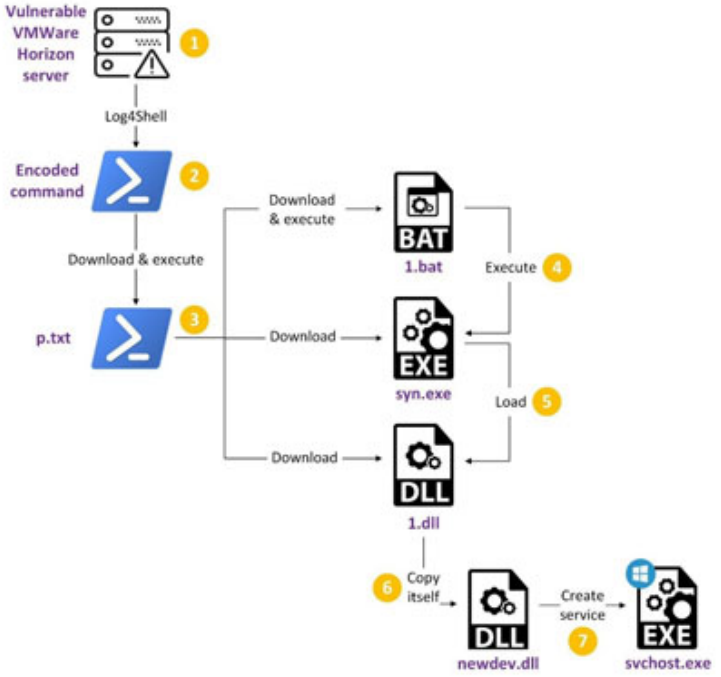
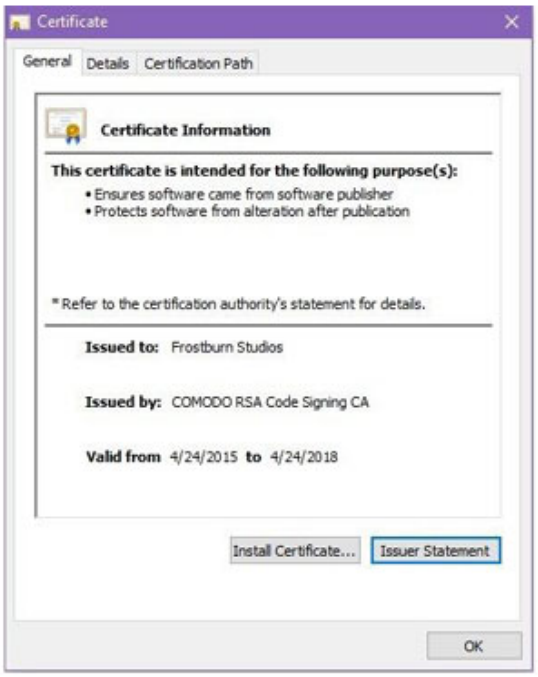
Chinese Hackers Target VMware Horizon Servers with Log4Shell to Deploy Rootkit

thehackernews.com/2022/04/chinese-hackers-target-vmware-horizon.html

April 1, 2022





A Chinese advanced persistent threat tracked as Deep Panda has been observed exploiting the Log4Shell vulnerability in VMware Horizon servers to deploy a backdoor and a novel rootkit on infected machines with the goal of stealing sensitive data.

"The nature of targeting was opportunistic insofar that multiple infections in several countries and various sectors occurred on the same dates," said Rotem Sde-Or and Eliran Voronovitch, researchers with Fortinet's FortiGuard Labs, in a report released this week. "The victims belong to the financial, academic, cosmetics, and travel industries."

Deep Panda, also known by the monikers Shell Crew, KungFu Kittens, and Bronze Firestone, is said to have been active since at least 2010, with recent attacks "targeting legal firms for data exfiltration and technology providers for command-and-control infrastructure building," according to Secureworks.

Cybersecurity firm CrowdStrike, which assigned the panda-themed name to the threat cluster all the way back in July 2014, called it "one of the most advanced Chinese nation-state cyber intrusion groups."

The latest set of attacks documented by Fortinet shows that the infection procedure involved the exploitation of the Log4j remote code execution flaw (aka Log4Shell) in vulnerable VMware Horizon servers to spawn a chain of intermediate stages, ultimately leading to the deployment of a backdoor dubbed Milestone ("1.dll").

Based on the leaked source code of the infamous Gh0st RAT but with notable differences in the command-and-control (C2) communication mechanism employed, Milestone is also designed to send information about the current sessions on the system to the remote server.

Also detected during the attacks is a kernel rootkit called "Fire Chili" that's digitally signed with stolen certificates from game development companies, enabling it to evade detection by security software and conceal malicious file operations, processes, registry key additions, and network connections.

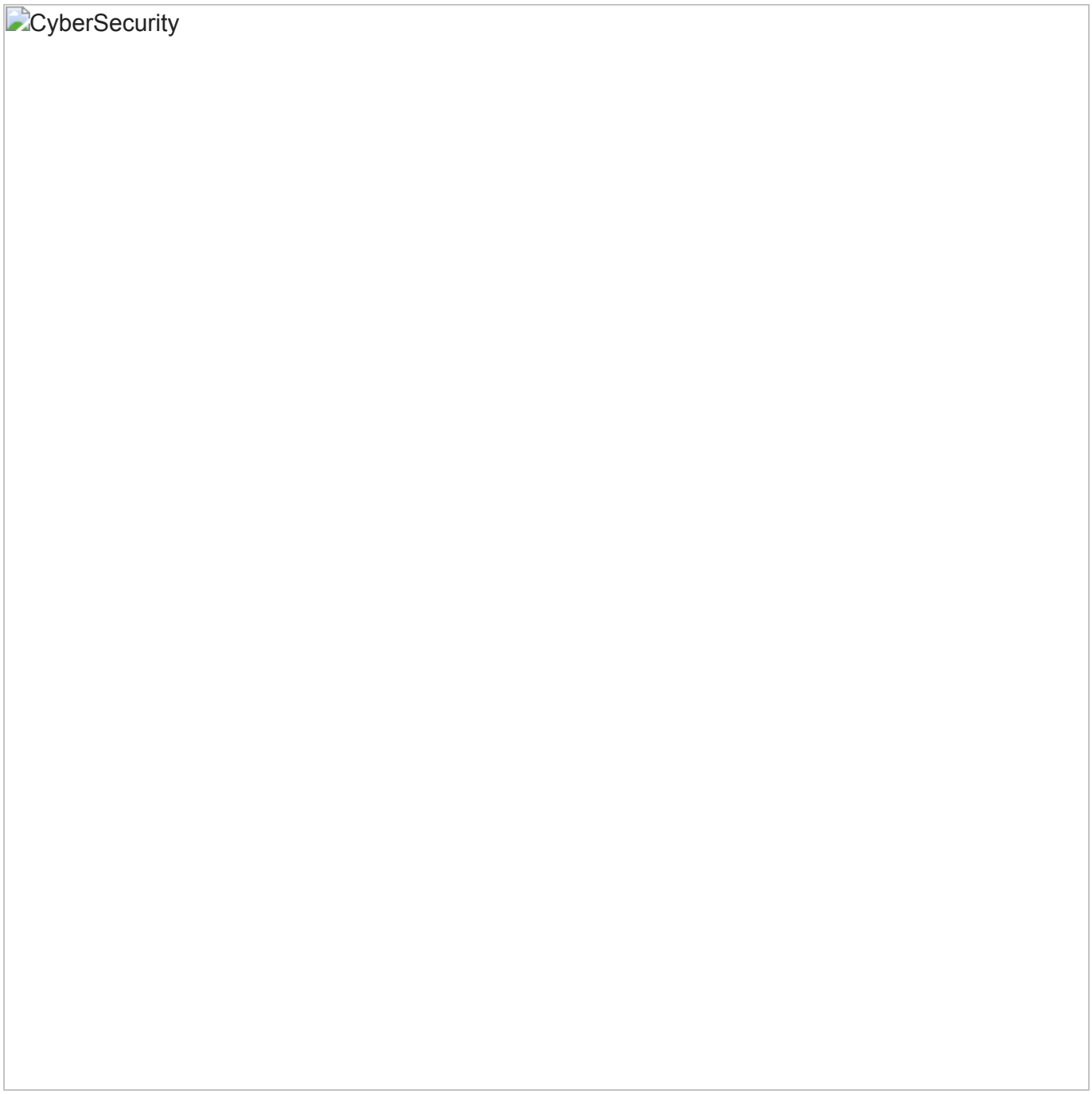
IOCTL	Action	Description
0xF3060000	Hide file	Add a path to global file list
0xF3060004	Stop hiding file	Remove a path from global file list
0xF3060008	Hide\protect process	Add a file path or PID to global process list
0xF306000C	Stop hiding\protecting process	Remove a file path or PID from global process list
0xF3060010	Hide registry key	Add a key to global registry list
0xF3060014	Stop hiding registry key	Remove a key from global registry list
0xF3060018	Hide network connections	Add a file path or port number to global network list
0xF306001C	Stop hiding network connections	Remove a file path or port number from global network list

This is achieved by means of ioctl (input/output control) system calls to hide the driver rootkit's registry key, the Milestone backdoor files, and the loader file and process used to launch the implant.

Fortinet's attribution to Deep Panda stems from overlaps between Milestone and Infoadmin RAT, a remote access trojan used by the sophisticated hacking collective in the early 2010s, with additional clues pointing to tactical similarities to that of the Winnti group.

This is backed by the use of compromised digital signatures belonging to gaming companies, a target of choice for Winnti, as well as a C2 domain (gnisoft[.]com), which has been previously linked to the Chinese state-sponsored actor as of May 2020.

"The reason these tools are linked to two different groups is unclear at this time," the researchers said. "It's possible that the groups' developers shared resources, such as stolen certificates and C2 infrastructure, with each other. This may explain why the samples were only signed several hours after being compiled."



The disclosure adds to a long list of hacking groups that have weaponized the Log4Shell vulnerability to strike VMware's virtualization platform.

In December 2021, CrowdStrike described an unsuccessful campaign undertaken by an adversary dubbed Aquatic Panda that leveraged the flaw to perform various post-exploitation operations, including reconnaissance and credential harvesting on targeted systems.

Since then, multiple groups have joined the fray, including the Iranian TunnelVision group, which was observed actively exploiting the Log4j logging library defect to compromise unpatched VMware Horizon servers with ransomware.

Most recently, cybersecurity company Sophos highlighted a slew of attacks against vulnerable Horizon servers that have been ongoing since January and have been mounted by threat actors to illicitly mine cryptocurrency, install PowerShell-based reverse shells, or to deploy Atera agents to remotely deliver additional payloads.

"Attempts to compromise Horizon servers are among the more targeted exploits of Log4Shell vulnerabilities because of their nature," Sophos researchers said, adding "platforms such as Horizon are particularly attractive targets to all types of malicious actors because they are widespread and can (if still vulnerable) easily found and exploited with well-tested tools."