Chinese hacking group uses new 'Fire Chili' Windows rootkit

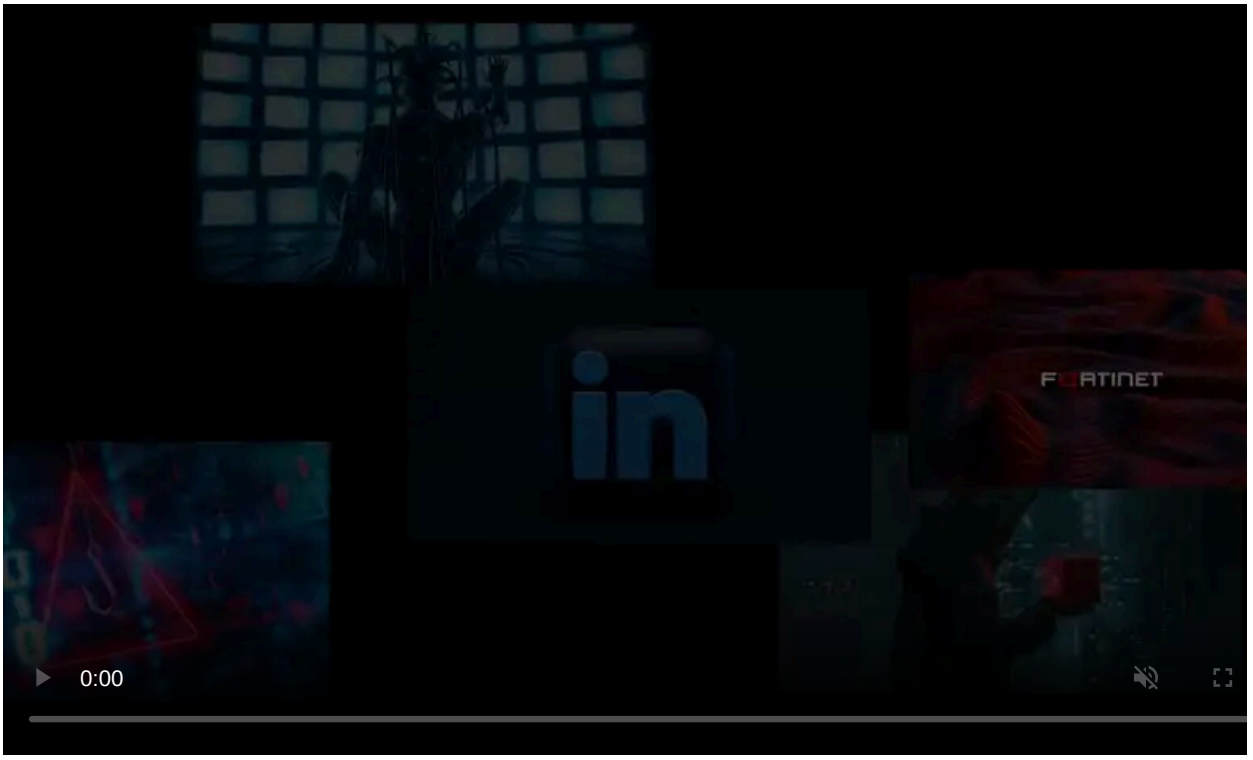
By Bill Toulas

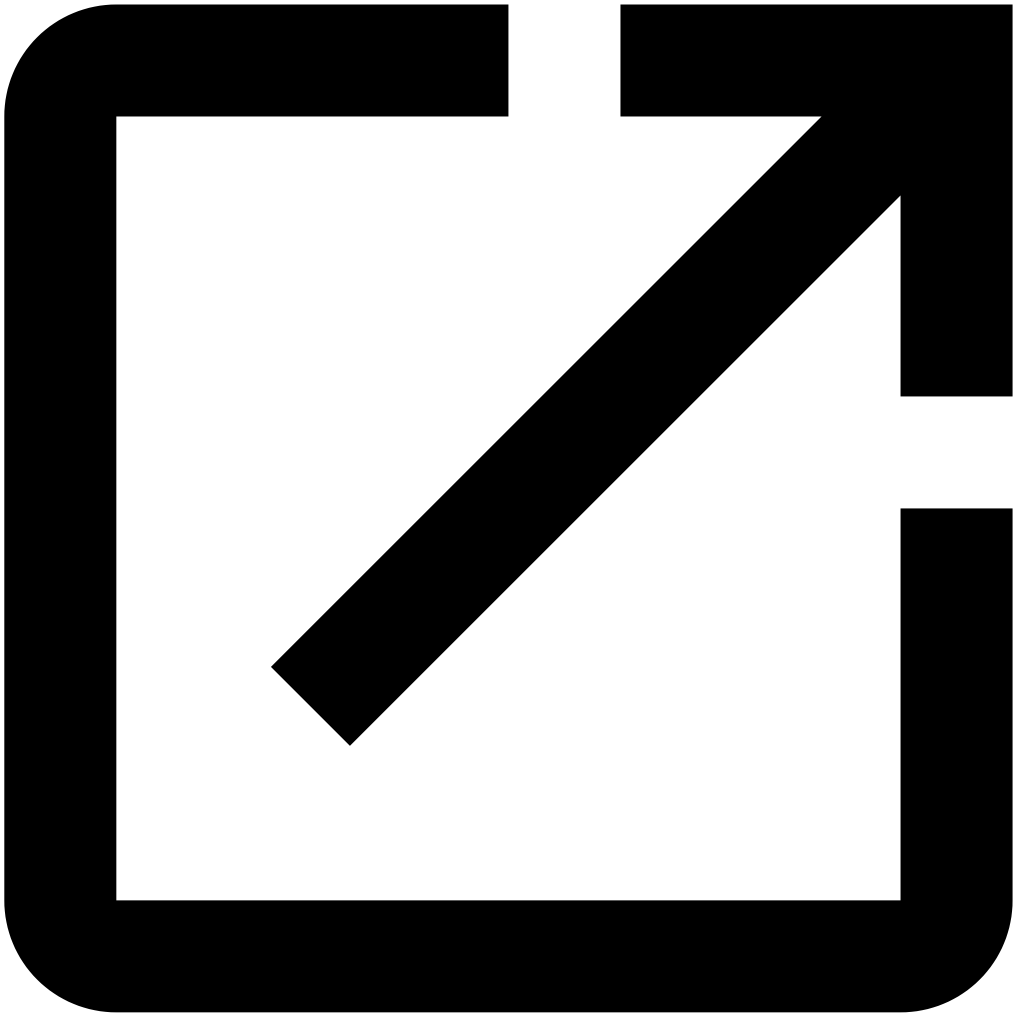
Published: 2022-03-31 · Archived: 2026-04-05 19:43:43 UTC

The Chinese hacking group Deep Panda is targeting VMware Horizon servers with the Log4Shell exploit to deploy a novel rootkit named 'Fire Chili.'

The rootkit is digitally signed using a certificate from Frostburn Studios (game developer) or one from Comodo (security software) to evade detection by AV tools.

Analysts at Fortinet who tracked Deep Panda's recent activity believe the certificates have been stolen from the mentioned software developers.


0:00



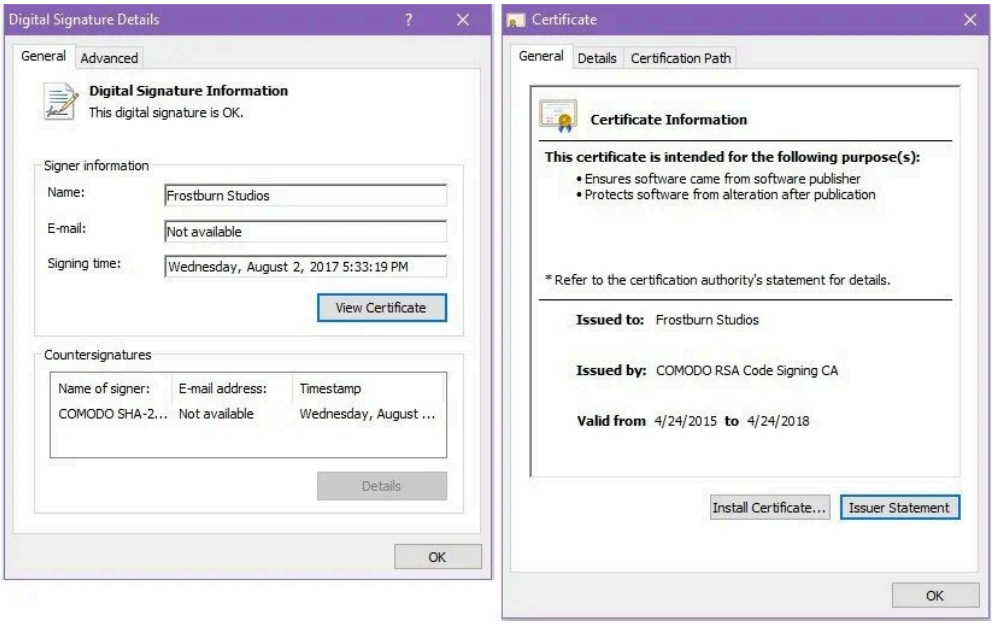
Deep Panda is a notorious Chinese APT focusing on cyber-espionage operations that has been active for many years now. The FBI had arrested one of its members back in 2017 after linking him with the exploitation of three zero-day vulnerabilities.

Fire Chili rootkit

In a recent Deep Panda campaign discovered by Fortinet, the hacking group is deploying the new 'Fire Chili' rootkit to evade detection on compromised systems.

A rootkit is malware typically installed as a driver that hooks various Windows APIs to hide the presence of other files and configuration settings in the operating system. For example, by hooking Windows programming functions, a rootkit can filter data to not display malicious file names, processes, and Registry keys APIs to Windows programs requesting the data.

In the attacks, the rootkit is signed by valid digital certificates allowing it to bypass detection by security software and load into Windows without any warnings.



Certificates stolen from legitimate companies *(Fortinet)*

Upon launch, Fire Chili performs basic system tests to ensure it's not running on a simulated environment and checks that the kernel structures and objects to be abused during operation are present.

Fortinet reports that the most recent supported operating system version for Fire Chili is Windows 10 Creators Update, released in April 2017.

The goal of the rootkit is to keep file operations, processes, registry key additions, and malicious network connections hidden from the user and any security software that could be running on the compromised machine.

For this hiding function, the malware uses IOCTLs (input/output control system calls) that are pre-populated with the malicious artifacts and can be dynamically configured.

For example, to hide malicious TCP connections from netstat, the rootkit intercepts routine IOCTL calls to the device stack, retrieves the complete list of network connections, filters out its own, and finally returns a sanitized structure.

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

IOCTLs to hide malicious artifacts *(Fortinet)*

Winnti overlaps

While looking into the latest Deep Panda campaign, Fortinet found several overlaps with Winnti, another notorious Chinese hacking group known for using digitally signed certificates.

Also, Winnti is known for persistently targeting gaming companies, so they could have stolen those certificates during one of their successful campaigns.

> "The reason these tools are linked to two different groups is unclear at this time. 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." - Fortinet

Sophisticated hacking collectives that focus on cyberespionage, and not so much for financial profit, are more likely to be backed or even coordinated by government handlers, so this overlap is hardly surprising.
