BLEEPINGCOMPUTER

Night Sky ransomware uses Log4j bug to hack VMware Horizon servers

Ionut Ilascu
January 11, 2022

The Night Sky ransomware gang has started to exploit the critical CVE-2021-44228 vulnerability in the Log4j logging library, also known as Log4Shell, to gain access to VMware Horizon systems.

The threat actor is targeting vulnerable machines exposed on the public web from domains that impersonate legitimate companies, some of them in the technology and cybersecurity sectors.

Attacks started in early January

Spotted in late December 2021 by security researcher MalwareHunterTeam, Night Sky ransomware focuses on locking enterprise networks. It has encrypted multiple victims, asking for an $800,000 ransom from one of them.

On Monday, Microsoft published a warning about a new campaign from a China-based actor it tracks as DEV-0401 to exploit the Log4Shell vulnerability on VMware Horizon systems exposed on the internet, and deploy Night Sky ransomware.

VMware Horizon is used for desktop and app virtualization in the cloud, allowing users to access them remotely through a dedicated client or a web browser.

It is also a solution for administrators for better management, security compliance, and automation across the entire fleet of virtual systems.

VMware has patched Log4Shell in Horizon products and provided workarounds for customers that could not install the new version containing the fix (2111, 7.13.1, 7.10.3). However, some companies have yet to apply the fix.

> “As early as January 4, attackers started exploiting the CVE-2021-44228 vulnerability in internet-facing systems running VMware Horizon. Our investigation shows that successful intrusions in these campaigns led to the deployment of the NightSky ransomware” Microsoft

The company adds that the group is known for deploying other ransomware families in the past, such as LockFile, AtomSilo, and Rook.

Previous attacks from this actor also exploited security issues in internet-facing systems like Confluence (CVE-2021-26084) and on-premises Exchange servers (CVE-2021-34473 - ProxyShell). It is believed that Night Sky is a continuation of the aforementioned ransomware operations.

The link with Rook ransomware has already been established. After reverse engineering the malware, Jiří Vinopal - forensic analyst at the Czech Republic CERT, discovered that Night Sky is a fork of the Rook ransomware.

Microsoft notes that Night Sky ransomware operators rely on command and control servers that impersonate domains used by legitimate companies such as cybersecurity firms Sophos, Trend Micro, technology companies Nvidia and Rogers Corporation.

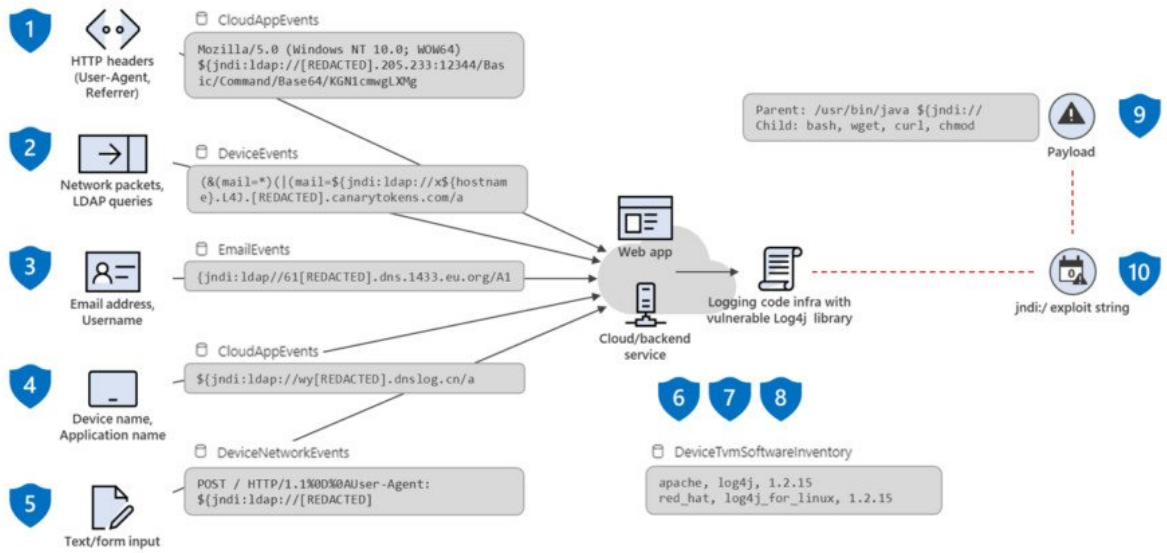
Microsoft's warning comes on the heels of another alert from UK's National Health Service (NHS) on January 5 about threat actors targeting VMware Horizon deployments with Log4Shell exploits.

Attractive attack vector

Log4Shell is an attractive attack vector for nation-state hackers and cybercriminals alike because the open-source Log4J component is present in a wide range of systems from dozens of vendors.

Exploiting the bug to achieve code execution without authentication requires minimum effort. A threat actor can initiate a callback or request to a malicious server that passes needs only visit a site or search it for a specific string to cause a server callback to a malicious location.

The security flaw can be leveraged remotely on vulnerable machines exposed on the public internet or from the local network, by a local adversary to move laterally to sensitive internal systems.



source: Microsoft

One of the first “top-tier” ransomware gangs to integrate Log4Shell in their attacks is Conti, who showed an interest in it as a potential attack avenue on December 12, just three days after the first proof-of-concept (PoC) exploit became public.

Another ransomware gang, a newcomer called Khonsari, started to leverage the exploit the very next day the PoC emerged on GitHub.

In the days following its disclosure, multiple threat actors started to leverage the Log4j bug. The first to take advantage were cryptocurrency miners, with state-backed hackers and ransomware gangs following suit.