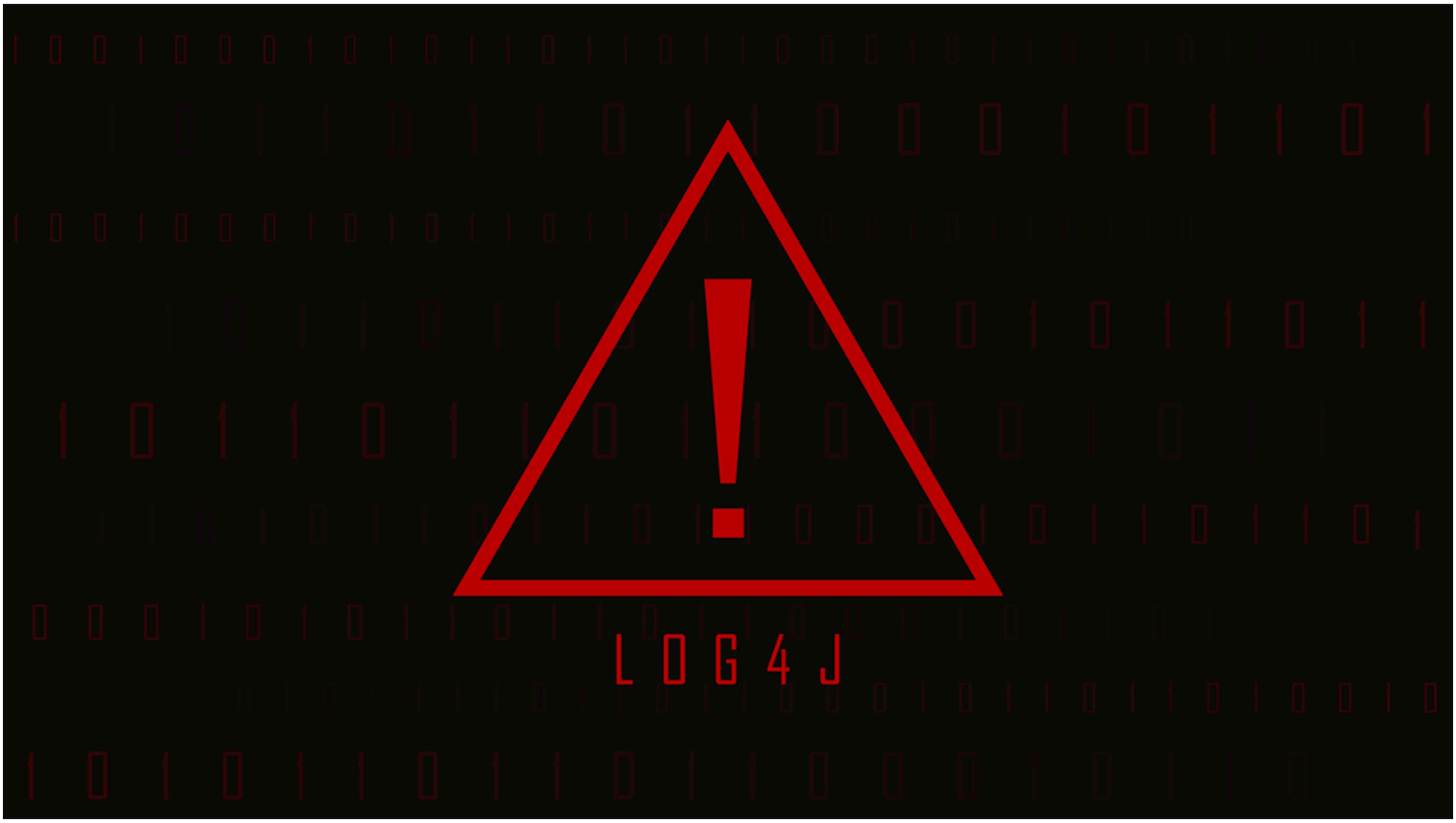
The Daily Swig
Cybersecurity news and views

VMware Horizon under attack as China-based ransomware group targets Log4j vulnerability

Adam Bannister 11 January 2022 at 15:21 UTC
Updated: 11 January 2022 at 15:26 UTC

Log4j Ransomware Microsoft

Microsoft says cybercrime group is attempting to deploy NightSky ransomware



A China-based ransomware operator has for the past week been actively exploiting the Log4j vulnerability in VMware Horizon, the desktop and app virtualization platform, Microsoft has warned.

“Based on our analysis, the attackers are using command and control (CnC) servers that spoof legitimate domains,” said the software giant in a January 10 addition to its rolling ‘Log4Shell’ updates.

When successful, the attacks – which began "as early as January 4" – result in the deployment of the NightSky ransomware.

Catch up with the latest ransomware news and attacks

NightSky leverages the in-vogue 'double extortion' model and was identified by threat researchers from MalwareHunterTeam on January 1.

Microsoft said the ransomware group directing the Horizon attacks, which it is tracking as 'DEV-0401', has previously deployed LockFile, AtomSilo, and Rook ransomware, as well as exploited CVE-2021-26084 in Atlassian Confluence and CVE-2021-34473 in on-premises Exchange servers.

NHS warning

Microsoft's latest Log4j security alert comes after the UK's National Health Service (NHS) similarly warned of an unknown threat group attempting to gain a foothold on networks via attacks against VMware Horizon deployments running vulnerable versions of Log4j, an open source Java logging library.

In a 'medium severity' cyber alert published on January 5, the health system's digital arm, NHS Digital, said the attack "uses the Lightweight Directory Access Protocol (LDAP) to retrieve and execute a malicious Java class file that injects a web shell into the VM Blast Secure Gateway service", with a view to deploying ransomware or exfiltrating data.

In a security advisory last updated on December 23, VMWare said Horizon's HTML Access component was vulnerable to Log4Shell exploits and provided remediation and mitigation steps.

Sprawling attack surface

The Log4Shell flaw, which has spawned four patches in Log4j so far, allows cybercriminals to launch remote code execution (RCE) attacks against vulnerable systems.

The attack surface is so sprawling that bug bounty platform HackerOne had received nearly 1,700 Log4j vulnerability reports to over 400 programs less than two weeks after the bug was publicly disclosed.

RECOMMENDED Bug bounty platforms handling thousands of Log4j vulnerability reports

Microsoft has previously documented ransomware attacks on Minecraft servers via Log4Shell and access brokers compromising networks before selling access to ransomware-as-a-service affiliates.

"We have observed many existing attackers adding exploits of these vulnerabilities in their existing malware kits and tactics, from coin miners to hands-on-keyboard attacks," said Microsoft. "Organizations may not

realize their environments may already be compromised.

Microsoft recommends that customers review devices where vulnerable installations are discovered, and "assume broad availability of exploit code and scanning capabilities to be a real and present danger to their environments.

"Due to the many software and services that are impacted and given the pace of updates, this is expected to have a long tail for remediation, requiring ongoing, sustainable vigilance."

RELATED Researchers discover Log4j-like flaw in H2 database console

Log4j | Ransomware | Microsoft | Supply Chain Attacks | Bug Bounty | Vulnerabilities | Malware | China | Asia | Cloud Security | Cyber-attacks | Cybercrime | Database Security | Hacking News | Hacking Techniques | Hacking Tools | Network Security | Denial of Service | Research | Open Source Software | Secure Development | OpSec | Critical Infrastructure | Enterprise | Organizations | Industry News | Java | Healthcare | RCE | Gaming

Adam Bannister

@Ad_Nauseum74

Latest Posts

We're going teetotal – It's goodbye to The Daily Swig
PortSwigger today announces that The Daily Swig is closing down

Bug Bounty Radar
The latest bug bounty programs for March 2023

Indian gov flaws allowed creation of counterfeit driving licenses
Armed with personal data fragments, a researcher could also access 185 million citizens' PII

Related stories

Bug Bounty Radar