UNC3886 Uses Fortinet, VMware 0-Days and Stealth Tactics in Long-Term Spying

Date: 20th June 2024 | Severity: High

Summary

The China-nexus cyber espionage actor linked to the zero-day exploitation of security flaws in Fortinet, Ivanti, and VMware devices has been observed utilizing multiple persistence mechanisms in order to maintain unfettered access to compromised environments. Persistence mechanisms encompassed network devices, hypervisors, and virtual machines, ensuring alternative channels remain available even if the primary layer is detected and eliminated.

Attack Vectors

- Attacks orchestrated by the adversary have leveraged zero-day flaws such as CVE-2022-41328 (Fortinet FortiOS), CVE-2022-22948 (VMware vCenter), and CVE-2023-20867 (VMware Tools) to perform various malicious actions, ranging from deploying backdoors to obtaining credentials for deeper access.
- After exploiting zero-day vulnerabilities to gain access to vCenter servers and subsequently managed ESXi servers, the actor obtained total control of guest virtual machines that shared the same ESXi server as the vCenter server. Mandiant observed the actor use two publicly available rootkits, REPTILE and MEDUSA, on the guest virtual machines to maintain access and evade detection.
- REPTILE was the rootkit of choice by UNC3886 as it was observed being deployed immediately after gaining access to compromised endpoints. REPTILE offers both the common backdoor functionality, such as command execution and file transfer capabilities, as well as stealth functionality that enables the threat actor to evasively access and control the infected endpoints via port knocking.
- UNC3886 automated the deployment of REPTILE components with shell scripts. These scripts contained similar code to the installation script responsible for building REPTILE components and configuring a persistence mechanism for the REPTILE kernel-level component.
- The threat actor was observed deploying malware, including MOPSLED and RIFLESPINE, that leverages trusted third parties like GitHub and Google Drive as C2 channels while relying on the rootkits for persistence.

Indicator of compromise

INDICATOR TYPE	INDICATORS	
IP	• 8.222.218[.]20 • 8.222.216[.]144 • 8.219.131[.]77 • 8.219.0[.]112 • 8.210.75[.]218 • 8.210.103[.]134 • 47.252.54[.]82 • 47.251.46[.]35 • 47.246.68[.]13 • 47.241.56[.]157	• 45.77.106[.]183 • 45.32.252[.]98 • 155.138.161[.]47 • 165.154.134[.]40 • 152.32.144[.]15 • 123.58.196[.]34 • 118.193.63[.]40 • 118.193.61[.]178 • 118.193.61[.]71

Recommendation

- Patch Management: Consistently apply security patches and updates to all systems, especially network devices, hypervisors, and virtualization platforms. Vulnerabilities exploited by UNC3886 often have patches available, so staying up to date is crucial.
- Network Segmentation: Isolate critical systems and sensitive data from less secure parts of the network. Implement strict access controls and segment the network to limit lateral movement in case of a breach.
- Zero Trust Architecture: Adopt a zero-trust approach, where access is granted based on strict authentication and authorization policies. Assume that internal networks are as risky as external ones and verify every request.
- Behavioral Monitoring: Deploy advanced endpoint detection and response (EDR) solutions to monitor for suspicious behavior. Look for signs of lateral movement, privilege escalation, and unusual network traffic.
- Threat Intelligence: Stay informed about UNC3886's tactics, techniques, and procedures (TTPs). Leverage threat intelligence feeds and collaborate with industry peers to share information.
- User Training: Educate employees about phishing, social engineering, and other attack vectors. Regular security awareness training helps prevent successful intrusions.
- Multi-Factor Authentication (MFA): Enable MFA for all critical accounts and services. Even if credentials are compromised, MFA adds an extra layer of security.
- Incident Response Plan: Develop and evaluate an incident response plan. Be prepared to detect, contain, and remediate any security incidents promptly.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/06/chinese-cyber-espionage-group-exploits.html
- https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations