NETWITNESS

FIRSTWATCH

INTSUM REPORT

14 Oct – 8 Nov 2024

MONTHLY INTELLIGENCE SUMMARIES (INTSUM) WILL REPORT ON THE MOST NOTEWORTHY RANSOMWARE ATTACKS, WIDELY EXPLOITED VULNERABILITIES AND THE LATEST IN DATA PRIVACY AND SECURITY POLICY NEWS TO PROVIDE A VALUABLE SNAPSHOT AND BRIEF SYNOPSIS OF THE CURRENT THREAT LANDSCAPE

NETWITNESS
FIRSTWATCH

Iranian Hackers Act as Brokers Selling Critical Infrastructure Access

In mid-October 2024, a comprehensive alert co-authored by various agencies—including the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), Canada's Communications Security Establishment (CSE), the Australian Federal Police (AFP), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)—issued a warning regarding Iranian hackers targeting critical infrastructure organizations. These cyber actors are focused on collecting credentials and network data, which they may subsequently sell on cybercriminal forums to facilitate further attacks.

The agencies assess that these Iranian hackers are functioning as initial access brokers. Utilizing brute-force techniques, they are infiltrating organizations across diverse sectors, including healthcare and public health, government, information technology, engineering, and energy.

Since October 2023, these threat actors have employed strategies such as brute-force attacks, password spraying, and multi-factor authentication (MFA) fatigue, commonly referred to as "push bombing." These methods enable them to compromise user accounts and gain access to targeted organizations. The advisory outlines the sophisticated tactics

Iranian Hackers Act as Brokers Selling Critical Infrastructure Access (cont.)

used by Iranian hackers to infiltrate networks and collect data, which may lead to additional access points.

Upon gaining access to an account, these actors typically attempt to register their devices within the organization's MFA system, thereby compiling data for further exploitation. The advisory also highlights Iranian hackers' use of less-defined methods to secure initial access to Microsoft 365, Azure, and Citrix environments.

In a preceding advisory issued in August, the US government cautioned about an Iranian state-sponsored threat actor that has successfully gained initial access to networks of various organizations across the United States.

NetWitness Takeaways:

The joint advisory recommends that organizations review authentication logs for failed logins on valid accounts and expand the search to multiple accounts.

If a threat actor leverages compromised credentials on virtual infrastructures, organizations should look for the so-called 'impossible logins' with changed usernames, user agents, or IP addresses that do not match the user's typical geographic location.

Iranian Hackers Act as Brokers Selling Critical Infrastructure Access (cont.)

Another sign of a potential intrusion attempt is the use of the same IP for multiple accounts or the use of IPs from different locations with a frequency that would not permit the user to travel the distance.

Additionally, the agencies recommend:

- Look for MFA registrations with MFA in unexpected locales or from unfamiliar devices
- Look for processes and program execution command-line arguments that may indicate credential dumping, especially attempts to access or copy the ntds.dit file from a domain controller
- Check for suspicious privileged account use after resetting passwords or applying user account mitigations
- Investigate unusual activity in typically dormant accounts
- Scan for unusual user agent strings, such as strings not typically associated with normal user activity, which may indicate bot activity

NETWITNESS
FIRSTWATCH

Russia-Linked Hackers Attack Japan's Government and Ports

On October 14th, two pro-Russian hacking groups have initiated distributed denial-of-service (DDoS) attacks targeting Japanese logistics and shipbuilding firms, as well as government and political entities. Experts suggest that these actions are designed to exert pressure on the Japanese government, particularly in light of Japan's recent increase in defense spending and military exercises conducted in partnership with regional allies.

The two pro-Russian cyber groups, NoName057(16) and the Russian Cyber Army Team, carried out the attacks. More than half of these attacks were directed at logistics, shipbuilding, and manufacturing sectors. Notably, NoName057(16) has gained infamy for its attacks on Ukrainian and European targets since Russia's invasion of Ukraine.

The hackers indicated that their focus on Japan is a direct response to an upcoming significant joint military exercise between Japan and the US scheduled for later this month, set to occur in proximity to Russia’s borders. In response, Russia has issued warnings about taking "adequate countermeasures" against this exercise.

Russia-Linked Hackers Attack Japan's Government and Ports (cont.)

NetWitness Takeaways:

- Detecting abnormal traffic spikes, particularly to a single IP or range of IPs, is crucial in identifying DDoS attacks. Packet inspection and traffic pattern analysis can reveal unusual volumes of traffic associated with botnet activity.
- Since NoName057(16) and Russian Cyber Army Team have regional focus, organizations should consider limiting traffic from certain countries or IP ranges if they aren't part of their usual traffic sources. Geofencing and regional access controls can reduce risk exposure to targeted DDoS attacks.
- Implementing traffic filtering, particularly rate limiting at the firewall or application level, helps manage high volumes and prevent excessive requests from impacting server performance.
- Actively updating firewall rules with blacklisted botnet IPs, identified through threat intelligence, can preemptively block traffic from known malicious sources.

Akira Ransomware Resurfaces: Victims Targeted After Extortion Attempt

In early August 2024, a significant uptick in ransomware attacks leveraging Fog and Akira was observed, predominantly initiated through compromised SonicWall SSL VPN accounts. These attacks affected a range of industries, suggesting an opportunistic targeting strategy rather than a focus on specific sectors.

On September 6, 2024, SonicWall issued a report indicating the potential exploitation of CVE-2024-40766, although no definitive link was established to the ongoing investigations. It is noteworthy that all affected devices were operating on outdated firmware, emphasizing the urgent need for regular updates and vigilant external log monitoring.

Since August, there has been a marked trend towards the involvement of SonicWall devices in ransomware incidents, with 30 recorded cases featuring Akira and Fog payloads. Akira was utilized in approximately 75% of these instances. The timeline from initial access to ransom demand exhibited considerable variation, ranging from as little as 1.5 to 2 hours to nearly 10 hours.

Analysis revealed that all compromised SSL VPN accounts were local to the SonicWall devices and generally employed default configurations. Attackers focused on a wide array of data, encompassing both general and sensitive information,

Akira Ransomware Resurfaces: Victims Targeted After Extortion Attempt (cont.)

with data exfiltration extending up to 30 months for certain types of information.

To mitigate these vulnerabilities, organizations must prioritize the timely updating of firmware on network appliances, closely monitor for unusual VPN login attempts, maintain secure off-site backups, and remain alert to suspicious activities post-compromise. Given the rapid execution of ransom demands in these incidents, adopting swift and proactive defense measures is crucial.

NetWitness Takeaways:

- Monitor for unusual or newly created file extensions like ".akira," which the ransomware appends to encrypted files.
- Watch for unusual outbound connections or data flows, especially those directed to unrecognized IPs or involving large data transfers.
- Monitor for suspicious registry modifications or unknown processes attempting to access critical files and directories.
- Deploy honeypots to detect early signs of ransomware activity, such as attempts to access or modify files in decoy directories.

Akira Ransomware Resurfaces: Victims Targeted After Extortion Attempt (cont.)

NetWitness Takeaways (cont.)

MITRE ATT&CK Techniques:

- **T1566.001** - Phishing: Spearphishing Attachment
- **T1068** - Exploitation for Privilege Escalation
- **T1543.002** - Create or Modify System Process: Windows Service
- **T1055** - Process Injection
- **T1027** - Obfuscated Files or Information
- **T1070** - Indicator Removal on Host
- **T1083** - File and Directory Discovery
- **T1016** - System Network Configuration Discovery
- **T1021** - Remote Services
- **T1074** - Data Staged
- **T1567.002** - Exfiltration Over Web Service
- **T1041** - Exfiltration Over C2 Channel
- **T1486** - Data Encrypted for Impact
- **T1489** - Service Stop
- **T1490** - Inhibit System Recovery

Akira Ransomware Resurfaces: Victims Targeted After Extortion Attempt (cont.)

Indicators of Compromise (IoCs)

•3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c
•5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5
•7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488
•678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
•8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50
•1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc
•d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959
•6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
•9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163
•1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296

New Fortinet Zero-Day Exploited for Months Before Patch

CVE-2024-47575, known as FortiJump, is a critical vulnerability rated 9.8 that affects FortiManager and FortiManager Cloud versions. Disclosed on October 22, it has been classified as a zero-day vulnerability with at least 50 potentially compromised FortiManager devices identified across various industries, with exploitation traceable back to June 27th.

This vulnerability is separate from CVE-2024-23113, which impacts FortiGate devices. Mandiant has linked the mass exploitation of FortiManager appliances to a new threat cluster, referred to as UNC5820. The vulnerability allows unauthenticated attackers to execute commands on servers using the "FortiGate to FortiManager Protocol" (FGFM) API, facilitating unauthorized management of FortiGate devices.

Fortinet has provided additional information in its advisory for CVE-2024-47575 (FG-IR-24-423), including mitigation and recovery methods. The advisory also contains further indicators of compromise (IOCs), such as other IP addresses used by the attackers and log entries for detecting a compromised FortiManager server

New Fortinet Zero-Day Exploited for Months Before Patch (cont.)

NetWitness Takeaways:

- **Unauthorized Device Registrations:** Look for unexpected devices being registered. Especially look for **"Unregistered device localhost add succeeded"** and **"Edited device settings (SN FMG-VMTMXXXXXX)"** on vulnerable versions of FortiManager.
- **System Process/Setting Changes:** Monitor for modifications to system settings or processes.
- **Suspicious Commands:** Detect unexpected commands executed by the fgfmsd daemon.
- **Config File Access/Exfiltration:** Watch for access modifications to large configuration files.
- **Non-standard Ports/Protocols:** Check for unusual ports and protocols, especially for data exfiltration.
- **Unexpected Device Connections:** Watch for unfamiliar devices connecting to FortiManager.
- **Obfuscated Traffic:** Look for encrypted or encoded payloads that don't match regular traffic.

Indicators of Compromise (IoCs):

- 45[.]32.41.202
- 104[.]238.141.143
- 158[.]247.199.37
- 45[.]32.63.2
- 195[.]85.114.78

New Fortinet Zero-Day Exploited for Months Before Patch (cont.)

- 80[.]66.196.199
- 198[.]199.122.22
- 172[.]232.167.68

MITRE ATT&CK Techniques:

- **T1190** - Exploitation of Remote Services
- **T1059** - Command and Scripting Interpreter`
- **T1543** - Create or Modify System Process
- **T1548** - Abuse Elevation Control Mechanism
- **T1027** - Obfuscated Files or Information
- **T1552** - Unsecured Credentials
- **T1082** - System Information Discovery
- **T1602** - Data from Configuration Repository
- **T1048** - Exfiltration Over Alternative Protocol