NETWITNESS

FIRSTWATCH

INTSUM REPORT

16 Sep – 11 Oct 2024

FROM THE OFFICE OF FIRSTWATCH CINO

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

FBI Says It Recently Dismantled A Second Major China-Linked Botnet

The takedown of a botnet known as Raptor Train resulted from a collaborative effort by the FBI, the US Attorney's Office for the Western District of Pennsylvania, the National Security Cyber Section of the Justice Department's National Security Division, French authorities, Lumen Technologies, and Black Lotus Labs. A state-sponsored hacking group from the People's Republic of China (PRC), operating under the names Integrity Technology Group or Flax Typhoon, managed this botnet.

They targeted various connected and Internet of Things (IoT) devices, including routers, cameras, video recorders, and storage devices, using them to conduct malicious cyber activities. This group had previously targeted government agencies, critical manufacturing, and information technology organizations in Taiwan and other countries, as well as US and foreign universities, corporations, government organizations, and media organizations.

Black Lotus Labs discovered this network's activities targeting U.S. and Taiwanese entities in the military, government, higher education, telecommunications, defense industrial base (DIB), and information technology (IT) sectors. The botnet also possibly attempted to exploit Atlassian Confluence servers and Ivanti Connect Secure appliances from nodes associated with it.

FROM THE OFFICE OF FIRSTWATCH CINO

FBI Says It Recently Dismantled A Second Major China-Linked Botnet (cont.)

In June 2023, the Raptor Train botnet peaked with over 60,000 compromised devices. Since then, it has conscripted more than 200,000 SOHO routers, NVR/DVR devices, network-attached storage (NAS) servers, and IP cameras, becoming one of the largest Chinese state-sponsored IoT botnets discovered to date. The recent scale of device exploitation suggests that hundreds of thousands of devices have fallen victim to this network since its inception in May 2020.

When the hackers tried to transfer their bots to new servers and launched a DDoS attack, the FBI and its partners successfully mitigated the attack and pinpointed the new infrastructure. Realizing they faced the FBI and its partners, the hackers eventually gave up their efforts.

NetWitness Takeaways:

- Organizations must keep their IoT firmware up to date to close out the vulnerabilities.
- Isolating IoT devices from sensitive systems can help prevent deeper compromises.
- Regular reboots can help clear infection as the botnets are not persistent.
- Continuous monitoring of IoT devices, looking for unusual encrypted traffic on unusual ports should be done to avoid such attacks.

FROM THE OFFICE OF FIRSTWATCH CINO

FBI Says It Recently Dismantled A Second Major China-Linked Botnet (cont.)

MITRE ATT&CK Techniques:

- **T1071**: Application Layer Protocol
- **T1095**: Non-Application Layer Protocol
- **T1021**: Remote Services
- **T1203**: Exploitation of Client Execution
- **T1078**: Valid Accounts
- **T1568.001**: Dynamic Resolution: Fast Flux DNS
- **T1078**: Use of Valid Accounts

FROM THE OFFICE OF FIRSTWATCH CINO

Perfctl Malware: A Stealthy Threat Targeting Linux Servers

The Perfctl malware, recently discovered by Aqua Security researchers, is a sophisticated strain targeting Linux servers. Its primary purpose is to mine cryptocurrency and engage in proxy jacking, exploiting server resources while evading detection. By taking advantage of server vulnerabilities, particularly Apache RocketMQ and Polkit (CVE-2021-4043), Perfctl infects systems and maintains persistence. Once inside, it uses advanced techniques like process masquerading, rootkits, and file-less attacks to operate stealthily. Its name mimics legitimate Linux system processes, further helping it avoid raising suspicion.

The malware follows a structured attack chain, beginning with exploiting misconfigurations and known vulnerabilities. It delivers its main payload, a cryptocurrency miner, via a shell script that downloads and executes files like httpd in the /tmp directory before deleting them to mask its presence. The malware also drops rootkits, modified system utilities, and proxyjacking software, ensuring ongoing system control and resource exploitation. Perfctl's ability to hide processes, manipulate monitoring tools, and use encrypted Tor traffic makes it difficult to detect and remove, posing a significant risk to Linux-based infrastructures.

FROM THE OFFICE OF FIRSTWATCH CINO

Perfctl Malware: A Stealthy Threat Targeting Linux Servers (cont.)

NetWitness Takeaways:
To counter Perfctl, organizations should focus on both detection and prevention. Monitoring for unusual CPU spikes, employing rootkit detection tools, and analyzing network traffic is critical to identifying infections. Prevention strategies include:

- Patching vulnerabilities.
- Restricting file execution.
- Implementing role-based access control (RBAC).
- Segmenting networks to minimize lateral movement by attackers.

These steps and regular security updates can strengthen defenses and mitigate the risks posed by the increasingly sophisticated Perfctl malware.
Using EDR solutions that focus on Linux systems and containers help detect anomalies at the endpoint level.

MITRE ATT&CK Techniques:

- **T1059.004** – Command and Scripting Interpreter: Unix Shell
- **T1036** – Masquerading
- **T1105** – Ingress Tool Transfer
- **T1543** – Create or Modify System Process
- **T1071.001** – Application Layer Protocol: Web Protocols
- **T1496** – Resource Hijacking
- **T1564** – Hide Artifacts
- **T1204** – User Execution

FROM THE OFFICE OF FIRSTWATCH CINO

Threat Actors Target the Middle East Using Fake Palo Alto GlobalProtect Tool

Threat actors are currently directing malware at Middle Eastern organizations, presenting it as the legitimate Palo Alto GlobalProtect Tool. This malware can potentially seize data and initiate remote PowerShell commands to further penetrate internal networks.

Palo Alto GlobalProtect is a legitimate security solution provided by Palo Alto Networks. It delivers secure VPN access with support for multi-factor authentication and is extensively utilized by organizations to guarantee secure access to private network resources for remote employees, contractors, and partners.

The exploitation of Palo Alto GlobalProtect as bait suggests that the attackers are focusing on high-value corporate entities employing enterprise software rather than adopting a random user approach.

An integral feature of this malware is its deployment of a command-and-control (C&C) infrastructure connecting to a recently registered URL ("sharjahconnect"). This URL, designed to mimic a corporate VPN portal, is a clear sign of the attackers' deceptive tactics, necessitating heightened vigilance to prevent the malware's network infiltration and sustained access.

FROM THE OFFICE OF FIRSTWATCH CINO

Threat Actors Target the Middle East Using Fake Palo Alto GlobalProtect Tool (cont.)

Furthermore, the malware leverages the Interactsh project for beaconing purposes. This project serves as a tool for penetration testers to validate the success of their exploits. The malware initiates connections to hostnames within the Interactsh's oast[.]fun domain. It is noteworthy that other threat actors, such as APT28, have also been observed exploiting this resource. In this case, the threat actor responsible for the malware has utilized these connections to monitor the progress of targets across diverse stages of the infection chain.

This C#-authored malware possesses diverse functionalities, comprising the execution of remote PowerShell commands, downloading and executing additional payloads, and exfiltrating specific files from the compromised machine. These capabilities underscore the potential for substantial harm and disruption within targeted organizations.

As we scrutinize the technical aspects and broader implications of this threat, cybersecurity professionals must remain well-informed and vigilant. A comprehensive understanding of the complexities associated with such advanced attacks is vital for formulating effective defense mechanisms and mitigating potential risks to critical infrastructure and sensitive data.

Threat Actors Target the Middle East Using Fake Palo Alto GlobalProtect Tool (cont.)

NetWitness Takeaways:

Organizations should monitor the unusual use of remote PowerShell commands. NetWitness offers a wide variety of application rules that detect such activity.
The following rules can be downloaded from NetWitness LIVE to help detection:

- Runs PowerShell with a hidden window
- Runs PowerShell downloading content
- Runs PowerShell defining function
- Runs PowerShell using encoded command
- Runs PowerShell with long arguments
- Runs PowerShell decoding base64 string
- Runs PowerShell commands on the remote computer
- Disables Windows Defender using Powershell

MITRE ATT&CK Techniques:

- **T1071.001** - Application Layer Protocol: Web Protocols
- **T1059.001** - Command and Scripting Interpreter: PowerShell
- **T1027** - Obfuscated Files or Information
- **T1105** - Ingress Tool Transfer
- **T1566.002** - Phishing: Spearphishing Link
- **T1055** - Process Injection
- **T1218.011** - System Binary Proxy Execution: Rundll32
- **T1497** - Virtualization/Sandbox Evasion

FROM THE OFFICE OF FIRSTWATCH CINO

China-Linked CeranaKeeper Targeting Southeast Asian Organizations with Data Exfiltration (cont.)

A newly identified threat actor has emerged, linked to a series of data exfiltration attacks targeting a Thai governmental institution. ESET designates this group as CeranaKeeper, which utilizes tools previously associated with the Mustang Panda actor, illustrating a sophisticated approach in its operations.

CeranaKeeper continuously enhances its backdoor capabilities to avoid detection and employs a diverse array of methods for extensive data extraction. The group is known to exploit widely-used, legitimate cloud and file-sharing services, such as Dropbox and OneDrive, to implement its customized backdoors and extraction tools.

In addition to Thailand, CeranaKeeper has directed its efforts towards other nations, including Myanmar, the Philippines, Japan, and Taiwan, all of which have increasingly drawn the attention of state-sponsored Chinese threat actors in recent years.

In mid-2023, CeranaKeeper successfully infiltrated Thai government systems through a brute-force attack against a local area network domain control server. This breach enabled them to gain initial access, facilitating further penetration into the network. The compromised machines

FROM THE OFFICE OF FIRSTWATCH CINO

China-Linked CeranaKeeper Targeting Southeast Asian Organizations with Data Exfiltration (cont.)

were subsequently converted into proxies and update servers, housing updates for their backdoor operations.

The CeranaKeeper actors demonstrate a commitment to refining their toolset and rapidly adapting to sustain their stealth. Their primary objective appears to be long-term espionage, as evidenced by the substantial volume of data harvested during their intrusion, a characteristic hallmark of this group.

NetWitness Takeaways:
The following rules can be downloaded from NetWitness LIVE to help detect this threat actor.

CeranaKeeper uses malicious BAT and PowerShell scripts. Monitoring encoded PowerShell commands can help detect their activity. The rule below identifies such executions.

- Runs Powershell Using Encoded Command

CeranaKeeper dumps credentials from LSASS to gain access to systems. Monitor for attempts to dump credentials from LSASS or memory. The following rules help detect unusual LSASS credential dumps.

- Powershell Opens LSASS Process

FROM THE OFFICE OF FIRSTWATCH CINO

China-Linked CeranaKeeper Targeting Southeast Asian Organizations with Data Exfiltration (cont.)

- Unexpected lsass.exe Parent
- Procdump Dumps Lsass
- Process Enumeration Followed by Dumping LSASS

Specific Activities to Monitor:

- Web shells or unusual system processes running on critical systems.
- Use of legitimate cloud platforms for maintaining access.
- Privilege Escalation: Suspicious process creation or credential dumping activity targeting LSASS or SAM.
- Anomalous outbound traffic to cloud storage platforms like Dropbox, OneDrive, or GitHub, especially from non-typical sources.
- Unusual uploads or outbound traffic spikes to cloud storage platforms, particularly outside of normal working hours.
- CeranaKeeper is known to use cloud services like Dropbox, OneDrive, and GitHub for C2 and data exfiltration. Monitoring network traffic for unusual or anomalous connections to these services, especially from critical servers, is crucial.
- Look for outbound encrypted traffic, especially when it's tied to cloud services or occurs outside normal usage patterns.
- Monitor for large uploads or unusual amounts of data transferred to these services, particularly from servers or workstations that do not typically interact with these platforms.

FROM THE OFFICE OF FIRSTWATCH CINO

China-Linked CeranaKeeper Targeting Southeast Asian Organizations with Data Exfiltration (cont.)

.

- CeranaKeeper uses web shells to maintain access to compromised servers. Monitoring web server logs for abnormal POST requests, file uploads, or command executions on web servers is essential to catch this activity.

MITRE ATT&CK Techniques:

- **T1110 -** Brute Force
- **T1059 -** Command and Scripting Interpreter
- **T1218 -** Signed Binary Proxy Execution
- **T1505 -** Server Software Component
- **T1543 -** Create or Modify System Process
- **T1078 -** Valid Accounts
- **T1027 -** Obfuscated Files or Information
- **T1036 -** Masquerading
- **T1003 -** Credential Dumping
- **T1071 -** Application Layer Protocol
- **T1573 -** Encrypted Channel
- **T1567 -** Exfiltration Over Web Services

FROM THE OFFICE OF FIRSTWATCH CINO