مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

APT Campaign Targeting UAE Organizations

Tracking #:432316197

Date:29-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a group of Iran-based cyber threat actors that are actively targeting UAE organizations across various sectors, including education, finance, healthcare, defense, and local government.

TECHNICAL DETAILS:

Security researchers have warned that a group of Iran-based cyber threat actors is actively targeting organizations in various sectors, including education, finance, healthcare, defense, and local government, across multiple countries, including the United Arab Emirates.These actors conduct computer network exploitation activity, as well as collaborate with ransomware affiliates to deploy ransomware.

This group is known in the private sector by the names Pioneer Kitten, Fox Kitten, UNC757, Parisite, RUBIDIUM, and Lemon Sandstorm. The actors also refer to themselves by the moniker Br0k3r, and as of 2024, they have been operating under the moniker “xplfinder” in their channels.

Observed Tactics, Techniques, and Procedures:

The Iranian cyber actors' initial intrusions rely upon exploits of remote external services on internet-facing assets to gain initial access to victim networks. As of July 2024, they have been observed scanning IP addresses hosting Check Point Security Gateways, probing for devices potentially vulnerable to CVE-2024-24919.In April 2024, they conducted mass scanning of IP addresses hosting Palo Alto Networks PAN-OS and GlobalProtect VPN devices, likely probing for devices vulnerable to CVE-2024-3400.

Following exploitation of vulnerable devices, the actors use techniques such as:

- Capturing login credentials using webshells on compromised Netscaler devices [T1505.003][T1056]
- Creating accounts on victim networks with names like "sqladmin$," "adfsservice," "IIS_Admin," "iis-admin," and "John McCain" [T1136.001]
- Deploying a malicious backdoor version.dll in the C:\Windows\ADFS\ directory [T1505.003]
- Using a scheduled task to load malware through installed backdoors[T1053]

Execution, Privilege Escalation, and Defense Evasion:

- The actor uses compromised credentials to access other applications and infrastructure within the victim network, indicating a focus on lateral movement and privilege escalation (T1078.003, T1078.002).
- Disabling antivirus and security software, and lowering PowerShell policies, are techniques used to evade defenses and create a more permissive environment for executing malicious activities (T1562.001, T1562.010).
- Attempting to allowlist the actor's tools by entering security exemption tickets suggests an effort to maintain persistence and avoid detection.

Discovery:

- Exporting system registry hives and network firewall configurations, along with exfiltrating account usernames, configuration files, and logs, are methods used to gather

detailed information about the network and its users, which can be used for further exploitation (T1012, T1482).

Command and Control:

- Installing the AnyDesk remote access program provides a backup access method, ensuring persistent access to the compromised network (T1219).
- Enabling Windows PowerShell Web Access and using tunneling tools like Ligolo and NGROK facilitate remote command execution and data exfiltration, respectively (T1059.001, T1572).

Exfiltration and Impact:

- Collaborating with ransomware affiliates (including NoEscape, Ransomhouse, and ALPHV [aka BlackCat]) in exchange for a percentage of the ransom payments by providing affiliates with access to victim networks, and conducting separate malicious activities, such as stealing sensitive data, indicate a multi-faceted approach to monetizing the breach, including ransom demands and espionage (T1657, TA0010).

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- Apply patches and/or mitigations for CVE-2024-3400, CVE-2022-1388, CVE-2019-19781, and CVE-2023-3519
- Monitor outbound web requests to files.catbox[.]moe and *.ngrok[.]io, as these domains are known to be associated with the threat actors.
- Search for Unusual Activity: Look for unusual login attempts, new accounts with unusual usernames, or anomalous network traffic.
- **Advanced Endpoint Protection**: Employ advanced security solutions to detect and block malicious scripts. Ensure these tools are updated frequently.
- **Enable Multi-Factor Authentication (MFA)**: Implement MFA to add an additional layer of security, reducing the impact of compromised credentials.
- **Incident Response Plan**: Develop and regularly update an incident response plan to ensure swift action against potential malware infections.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.cisa.gov/sites/default/files/2024-08/aa24-241a-iran-based-cyber-actors-enabling-ransomware-attacks-on-us-organizations_0.pdf

- Attached File :