مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

UNC1860 Targeting Government and Telecommunications Sectors

Tracking #:432316318

Date:23-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed UNC1860, an Iranian threat actor presents a significant threat to organizations in the Middle East, particularly in the governmental and telecommunications sectors.

TECHNICAL DETAILS:

UNC1860 is an advanced Iranian threat actor known for its sophisticated tooling and passive backdoors, which enable it to gain persistent access to high-priority networks, particularly in the government and telecommunications sectors in the Middle East. The group's activities include scanning for vulnerabilities, targeting VPN servers, and using custom malware controllers like TEMPLEPLAY and VIROGREEN to facilitate remote access and control of victim networks. UNC1860's malware, such as STAYSHANTE and SASHEYAWAY, is designed to evade detection and provide a strong foothold for further operations. The group's use of passive implants and web shells, along with its collaboration with other Iranian-based threat actors like APT34, indicates its role in espionage and network attack operations.

UNC1860's Tactics, Techniques, and Procedures (TTPs):

Initial Access:

- Exploitation of vulnerable internet-facing servers, particularly those with exposed SharePoint vulnerabilities (CVE-2019-0604).
- Deployment of web shells and droppers (e.g., STAYSHANTE and SASHEYAWAY) to gain initial foothold.

Persistence:

- Use of passive implants (e.g., TEMPLEDOOR, FACEFACE, SPARKLOAD) designed to evade detection and maintain long-term access.
- Repurposing of legitimate software components, such as the Windows kernel driver from Sheed AV, to protect malicious files from modification.

Privilege Escalation:

- Exploitation of vulnerabilities to gain higher privileges within the compromised network.
- Use of custom utilities (e.g., TEMPLELOCK) to manipulate and control the Windows Event Log service.

Defense Evasion:

- Employing custom Base64 encoding/decoding and XOR encryption/decryption libraries to bypass security tools.
- Use of HTTPS-encrypted traffic to conceal command and control (C&C) communications.

Lateral Movement:

- Utilizing network scanning tools to identify additional targets within the compromised network.
- Exploiting credentials and email addresses across multiple domains to expand access.

Command and Control (C&C):

- Use of GUI-operated malware controllers (e.g., TEMPLEPLAY, VIROGREEN) to facilitate remote access and control.
- Employing proxy servers and volatile sources to obfuscate C&C traffic and make detection more difficult.

Collaboration with Other Threat Actors:

- UNC1860 has been observed collaborating with other Iranian-based threat actors, such as APT34, suggesting a role in assisting with lateral movement and providing initial access for destructive and disruptive operations.

Indicators of Compromise:
Attached File.

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- Regularly update and patch systems to protect against known vulnerabilities.
- Implement multi-factor authentication (MFA) to enhance account security.
- Conduct regular security audits and vulnerability assessments.
- Use advanced security solutions that can detect and block passive implants and web shells.
- Monitor for unusual outbound traffic and encrypted communications that may indicate C&C activity.

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://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks/