مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Phobos Ransomware Campaign

Tracking #:432315666

Date:04-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a ransomware called Phobos targeting various organizations globally, including critical infrastructure sectors. It encrypts victim files, rendering them inaccessible, and extorts ransom payments for decryption.

TECHNICAL DETAILS:

Phobos ransomware has been actively targeting various critical sectors, including government, education, emergency services, healthcare, and other vital infrastructure, since May 2019. Operating under the ransomware-as-a-service (RaaS) model, it has successfully extorted millions of dollars from victim organizations.

The attacks typically begin with **phishing emails** that deploy **IP scanning tools**. These tools identify vulnerable **Remote Desktop Protocol (RDP) ports**, which are then **brute-forced** for access and to gather information about the victim's network. Additionally, attackers have been observed using various tools like Bloodhound, Cobalt Strike, and SmokeLoader in conjunction with Phobos ransomware.

Linked to other malicious variants such as Backmydata, Devos, Eight, Elking, and Faust, Phobos primarily gains initial access through two methods: **phishing emails** and **exploiting vulnerable RDP ports** through brute-force attacks.

Once inside a network, the ransomware:

- Installs itself in key locations.
- Targets user files and network shares for encryption.
- Demands a ransom for decryption keys.
- Exfiltrates data from the victim's network.

Threat actors leveraging Phobos have utilized various techniques:

- **Deploying remote access tools** to establish a persistent connection within the compromised network.
- **Using spoofed email attachments** to deliver malicious payloads like the SmokeLoader backdoor, which then deploys Phobos and steals data.
- **Running legitimate executables** to deploy additional payloads with elevated privileges.
- **Modifying system firewall configurations** to bypass network defenses.
- **Utilizing Windows Startup folders and Run Registry Keys** for persistence.

Reconnaissance, credential harvesting, and discovery are often conducted using open-source tools such as Bloodhound, Sharphound, Mimikatz, NirSoft, and Remote Desktop Passview. Legitimate tools like WinSCP and Mega.io may be used for **data exfiltration** to FTP servers or cloud storage.

Phobos has been observed exhibiting additional malicious behavior:

- **Identifying and deleting data backups** to prevent recovery.
- **Encrypting all connected logical drives** on the target machine.

Extortion typically occurs via email, although some Phobos affiliates have resorted to **voice calls** and **instant messaging applications** for communication with victims. Compromised organizations have even been listed on **Tor-based sites** that also host allegedly stolen data.

INDICATORS OF COMPROMISE(IOCs):

Refer to this link here for IOCs and More information

RECOMMENDATIONS:

- Block the IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Regularly update all software, including operating systems and applications, to patch vulnerabilities.
- Implement strong authentication methods, such as multi-factor authentication (MFA), for all critical systems and applications.
- Monitor network traffic for unusual or suspicious activities using intrusion detection systems (IDS) and intrusion prevention systems (IPS).
- **Network Security:** Review and enhance network security by closing unused ports, removing unnecessary applications, and monitoring for suspicious activity.
- Implement endpoint detection and response (EDR) solutions.
- **Secure Backups:** Maintain offline, immutable backups of critical data. Regularly test restoration procedures.
- **User Awareness Training:** Educate employees on phishing, social engineering, and secure password practices.

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/news-events/cybersecurity-advisories/aa24-060a