مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Ransomware: Black Basta

Tracking #:432315845

Date:13-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed Black Basta, a ransomware threat actively targeting critical infrastructure sectors, including healthcare.

TECHNICAL DETAILS:

Black Basta is considered a ransomware-as-a-service (RaaS) variant and was first identified in April 2022. As of May 2024, Black Basta affiliates have impacted over 500 organizations globally. Black Basta affiliates use common initial access techniques—such as phishing and exploiting known vulnerabilities—and then employ a double-extortion model, both encrypting systems and exfiltrating data.

Black Basta affiliates primarily use spearphishing [T1566] to obtain initial access, and have also exploited ConnectWise vulnerability CVE-2024-1709 [T1190] starting in February 2024.They use tools such as SoftPerfect network scanner, BITSAdmin, PsExec, and Remote Desktop Protocol (RDP) for lateral movement and reconnaissance. Affiliates use credential scraping tools like Mimikatz for privilege escalation, and have exploited vulnerabilities like ZeroLogon, NoPac, and PrintNightmare. RClone is used to exfiltrate data prior to encryption using a ChaCha20 algorithm with an RSA-4096 public key Vssadmin.exe is used to delete volume shadow copies to inhibit system recovery.

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Implement strong password policies: Enforce complex passwords with minimum length requirements and regular password changes
- Enable multi-factor authentication (MFA): MFA adds an extra layer of security by requiring a second verification factor beyond a username and password.
- Organizations should promptly install updates for operating systems, software, and firmware to mitigate vulnerabilities exploited by Black Basta.
- Secure Remote Access: Apply security measures to secure remote access software and make backups of critical systems to enable recovery in case of an attack.

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/2024-05/aa24-131a-joint-csa-stopransomware-black-basta_0.pdf