مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Underground Team Ransomware

Tracking #:432315951

Date:13-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Underground Team ransomware group displaying new tactics, techniques, and procedures (TTPs), leading to the deployment of their ransomware variant and exfiltration of sensitive information.

TECHNICAL DETAILS:

The Underground ransomware is the successor of the Industrial Spy ransomware and was deployed by a threat actor called Storm-0978. The malware stops a target service, deletes the Volume Shadow Copies, and clears all Windows event logs.

- Delivery: Spam campaigns with malicious attachments or exploit unpatched vulnerabilities in software to gain initial access. Used Multiple phishing attempts that directed users to a fake Microsoft login page to capture credentials.

- Encryption: Team Underground utilises a custom-made ransomware executable built with Microsoft Visual C/C++ and designed for 64-bit systems. The ransomware encrypts victim files and unlike many strains, doesn't alter filenames or extensions.

- Exfiltration: Team Underground claims to steal data during the attack process. Their ransom note mentions exfiltrating sensitive information like financial records, employee data, and confidential agreements.

- Ransom Note: Team Underground's ransom note, titled "!readme!!!.txt", stands out for offering more than just a decryption key in exchange for a ransom payment.

Indicators of Compromise

IPs
79.141.173[.]210
Hashes
059175be5681a633190cd9631e2975f6
0a08d9b027457da99725968eb4566eb836a7d503219ad5690f851caecabce93d
d4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666
URLs
hxxp://47glxkuxyayqrvugfumgsblrdagvrah7gttfscgzn56eyss5wg3uvmqd.onion hxxp://undgrddapc4reaunnrdrmnagvdelqfvmgycuvilgwb5uxm25sxawaoqd.onion hxxp://ehehqyhw3iev2vfso4vqs7kcrzltfebe5vbimq62p2ja7pslczs3q6qd.onion/auth/login

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 Underground ransomware.
- 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.