مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Ransomware Campaign: RA World

Tracking #:432315712

Date:19-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a ransomware campaign known as RA World – actively targeting Windows users globally.

TECHNICAL DETAILS:

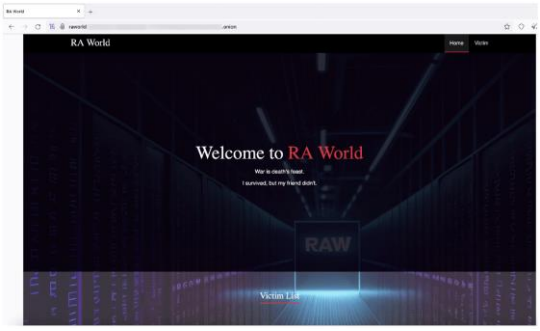
RA World is a ransomware strain that encrypts a victim's files, rendering them inaccessible. Additionally, it steals sensitive data and threatens to leak it if a ransom is not paid. This ransomware also takes steps to prevent data recovery, such as disabling backups and deleting shadow copies.

RA World Characteristics:

Encryption: Appends the .RAWLD extension to encrypted files.
Data Theft: Steals sensitive data and threatens to publish it online.
Recovery Obstruction: Disables backups and deletes shadow copies.
Ransom Demand: Delivers a ransom note with contact information for payment instructions.
Leak Sites: Operates on both TOR and non-TOR websites for stolen data publication.
Infection Vectors:

RA World can infiltrate systems through various means, including:

Phishing emails: Malicious emails containing infected attachments or links.
Exploiting software vulnerabilities: Targeting unpatched software on a victim's machine.
Remote Desktop Protocol (RDP) attacks: Unauthorized access gained through weak RDP configurations.
Victims: RA World has targeted a variety of organizations, highlighting the need for vigilance across all sectors.



The RA World ransomware's TOR site

INDICATORS OF COMPROMISE(IoCs):

File Indicators (Hashes SHA256)
4866d6994c2f8b4dadfaabc2e2b81bd86c12f68fdf0da13d41d7b0e30bea0801
51da3acc6c7089bd0f1df9d9902e183db0d1342552404c3c1b898b168399b0bc
31ac190b45cc32c04c2415761c7f152153e16750516df0ce0761ca28300dd6a4
9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de

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.
- Regular Backups: Implement a robust backup routine with backups stored offline and regularly tested for recoverability.
- Software Updates: Maintain up-to-date software on all devices to patch vulnerabilities.
- User Education: Train employees on identifying phishing attempts and cyber threats.
- Endpoint Security: Utilize endpoint detection and response (EDR) solutions to monitor systems for suspicious activity.
- Network Segmentation: Segment your network to minimize the impact of a potential breach.
- Multi-Factor Authentication (MFA): Enforce MFA on all critical systems and accounts.
- Incident Response Plan: Develop a plan for responding to a ransomware attack, including data recovery and communication protocols.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings (e.g. IOCs, TTPs...etc).

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

REFERENCES:

1. https://www.fortinet.com/blog/threat-research/ransomware-roundup-ra-world