مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Desert Dexter Malware Campaign Targeting Middle Eastern and North African Countries

Tracking #:432316939

Date:07-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers has identified an ongoing malicious campaign, attributed to the threat actor Desert Dexter, targeting individuals and organizations across the Middle East and North Africa (MENA) region.

TECHNICAL DETAILS:

Security researchers has identified an ongoing malicious campaign, attributed to the threat actor Desert Dexter, targeting individuals and organizations across the Middle East and North Africa (MENA) region. The campaign, active since September 2024, leverages social media platforms, particularly Facebook, and Telegram channels to distribute a modified version of AsyncRAT. The malware is designed to steal sensitive information, including cryptocurrency wallet data, and establish persistence on infected systems.

The attackers exploit the region's geopolitical climate by posting fake news and advertisements that lure victims into downloading malicious files. These files are hosted on legitimate file-sharing services or Telegram channels disguised as reputable media outlets.

Attack Methodology

1. **Initial Infection Vector**
   - Attackers create fake news channels and temporary accounts on Facebook* to post advertisements containing links to malicious files.
   - The ads often reference leaked reports or geopolitical developments to entice users into clicking.
   - Links redirect to file-sharing services (e.g., Files.fm) or Telegram channels hosting RAR archives containing malicious scripts.
2. **Malware Delivery**
   - The RAR archives contain BAT or JS files that execute PowerShell scripts to download and run the AsyncRAT payload.
   - The PowerShell script terminates processes that could interfere with the malware, deletes specific file types, and establishes persistence by modifying registry keys.
3. **Malware Functionality**
   - The modified AsyncRAT variant collects system information, including hardware IDs, IP addresses, and installed antivirus software, and sends it to a Telegram bot controlled by the attackers.
   - It scans for cryptocurrency wallet extensions and applications, such as MetaMask, Binance Wallet, and Ledger Live, to steal sensitive data.
   - The malware includes a basic keylogger that logs keystrokes and active processes.
4. **Persistence and Evasion**
   - The malware replaces the user startup folder in the registry to ensure it runs at system startup.
   - It uses a custom reflective loader to inject code into .NET processes, making detection more difficult.

5. **Network Infrastructure**

- The attackers use Dynamic DNS (DDNS) domains with IP addresses belonging to VPN services, making attribution challenging.
- The infrastructure includes semantically similar domain names and IP addresses from the same VPN provider.

Indicators of Compromise:
Attached File

RECOMMENDATIONS:

1. **Enhance Social Media Vigilance**
   - Educate employees and users about the risks of clicking on links or downloading files from unverified social media posts, especially those related to geopolitical news.
   - Implement strict policies for accessing social media platforms on corporate devices.
2. **Strengthen Endpoint Security**
   - Deploy advanced endpoint detection and response (EDR) solutions to identify and block malicious scripts, such as PowerShell and Batch files.
   - Regularly update antivirus software and ensure it is configured to detect and quarantine AsyncRAT and similar remote access trojans (RATs).
3. **Monitor and Block IOCs**
   - Use the provided IOCs to block malicious domains, IP addresses, and file hashes across your network.
   - Implement network traffic monitoring to detect connections to suspicious VPN services and Telegram bots.
4. **Restrict PowerShell Usage**
   - Limit the use of PowerShell to authorized personnel and enable logging to monitor for unusual script execution.
   - Disable PowerShell v2 and other deprecated versions that are often exploited by attackers.
5. **Conduct Regular Security Audits**
   - Perform periodic reviews of system configurations, registry entries, and startup folders to identify unauthorized changes.
   - Use threat intelligence feeds to stay informed about emerging threats in the MENA region.
6. **Implement Multi-Factor Authentication (MFA)**
   - Require MFA for accessing sensitive systems and applications, particularly those related to cryptocurrency wallets and financial transactions.
7. **Educate Users on Phishing Tactics**
   - Train employees to recognize phishing attempts, including fake news posts and malicious advertisements on social media.

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://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/desert-dexter-attacks-on-middle-eastern-countries