مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Earth Baku Threat Campaign

Tracking #:432316143

Date:13-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

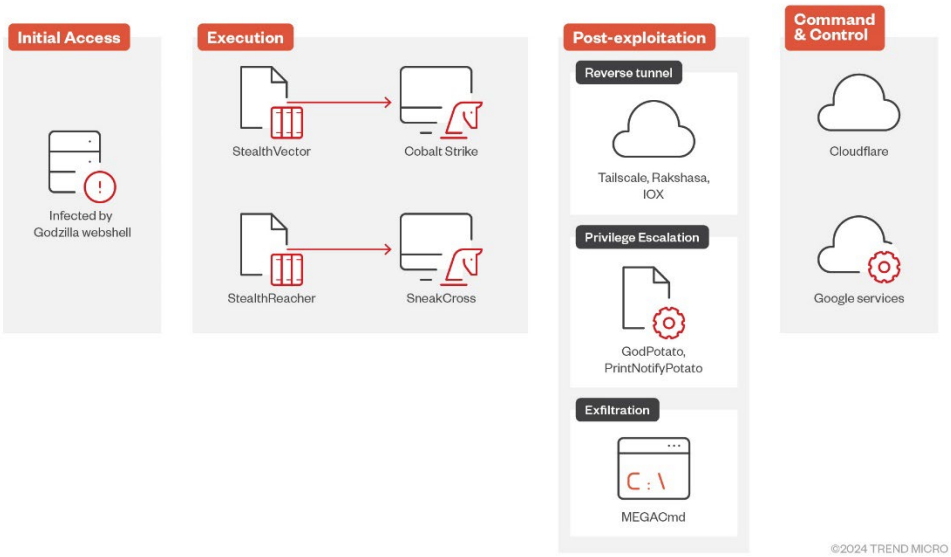
The UAE Cyber Security Council has observed Earth Baku has evolved into a formidable APT actor, expanding its operations beyond the Indo-Pacific to target critical infrastructure in Europe, the Middle East, and Africa.

TECHNICAL DETAILS:

Earth Baku (a threat actor associated with APT41) expanding its operations beyond the Indo-Pacific to target critical infrastructure in Europe, the Middle East, and Africa targeting countries like Italy, Germany, UAE, and Qatar, with suspected threat activity in Georgia and Romania. This sophisticated group leverages advanced techniques and tools to compromise systems and exfiltrate sensitive data.

Key Findings:

- **Expanded Target Regions**: Earth Baku's geographic scope has significantly widened, posing a global threat.
- **Advanced TTPs:** The group has refined its tactics, employing sophisticated malware and evasion techniques.
- **Public-Facing Applications as Entry Points**: IIS servers are being exploited as initial access vectors.
- **Destructive Malware Arsena**l: StealthVector, StealthReacher, and SneakCross are key components of the attack chain.
- **Data Exfiltration**: MEGAcmd is used to steal and transfer sensitive information.
- **Persistence Mechanisms**: Reverse tunnels and VPN services are employed to maintain persistent access.
- **Potential Impact:**The targeting of government, media, telecom, technology, healthcare, and education sectors highlights the critical nature of the threat. Successful attacks can lead to data breaches, financial loss, reputational damage, and disruption of essential services.



The infection vector of recent campaigns

INDICATORS OF COMPROMISE:

Attached File

RECOMMENDATIONS:

- Robust Network Security: Implement firewalls, intrusion detection/prevention systems, and web application firewalls to protect against attacks targeting public-facing applications.
- Employee Awareness: Educate employees about phishing, social engineering, and other cyber threats to prevent initial access.
- Regular Updates and Patching: Keep operating systems, applications, and software up-to-date with the latest security patches.
- Incident Response Planning: Develop and test a comprehensive incident response plan to minimize damage in case of a breach.
- Data Protection: Implement robust data protection measures, including encryption, access controls, and regular backups.

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.trendmicro.com/en_us/research/24/h/earth-baku-latest-campaign.html?&web_view=true