مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Earth Simnavaz Cyberattacks Targeting UAE and Gulf Regions

Tracking #:432316390

Date:14-10-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a recent campaign by the cyber espionage group Earth Simnavaz (APT34, OilRig) targeting critical infrastructure, particularly the energy sector, in the United Arab Emirates (UAE) and the broader Gulf region.

## TECHNICAL DETAILS:

Earth Simnavaz (also known as APT34 and OilRig), a cyber espionage group, targets organizations in the energy sector, particularly those involved in oil and gas, as well as other critical infrastructure. It is known for using sophisticated tactics, techniques, and procedures (TTPs) to gain unauthorized access to networks and exfiltrate sensitive information.

- **Attack Techniques**:
  - **Backdoor Deployment**: The group has been observed using a new backdoor that exploits Microsoft Exchange servers for credential theft.
  - **Vulnerability Exploitation**: They leverage vulnerabilities such as **CVE-2024-30088** for privilege escalation, allowing them to execute arbitrary code with elevated privileges.
  - **Custom Tools**: Earth Simnavaz utilizes a mix of customized .NET tools, PowerShell scripts, and IIS-based malware, enabling their malicious activities to blend seamlessly with normal network traffic.
- **Persistence Mechanisms**:
  - The attackers establish a persistent foothold within compromised networks, often using legitimate tools like **ngrok** to create secure tunnels for command-and-control communications.
  - They also employ techniques such as abusing dropped password filter policies to harvest credentials from domain users.
- **Data Exfiltration**:
  - Sensitive data is exfiltrated through legitimate email traffic, often using stolen credentials to send emails from compromised Exchange servers.
  - The attackers utilize a tool identified as **STEALHOOK**, which retrieves user credentials and sends them via email attachments.

**Impact**

- Successful attacks by Earth Simnavaz could result in:
  - Data breaches and exposure of sensitive information
  - Disruption of critical infrastructure operations
  - Loss of operational control for targeted organizations

## INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

## RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- **Implement a layered security approach** that includes:

  - Patching systems promptly, especially for known vulnerabilities like CVE-2024-30088.
  - Strengthening network security controls to detect and prevent unauthorized access attempts.
  - Employing advanced threat detection and response (XDR) solutions.
  - Implementing segmentation to limit the impact of breaches.
  - Regularly monitoring systems for suspicious activity.
- **Security awareness training** for employees to educate them on phishing tactics and social engineering techniques often used by APT groups.
- **Consider threat intelligence feeds** to stay updated on the latest TTPs used by Earth Simnavaz and other threat actors.

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/j/earth-simnavaz-cyberattacks-uae-gulf-regions.html