مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Wiper Malware Campaign Targeting Multiple Sectors

Tracking #:432318719

Date:04-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a destructive wiper malware campaign targeting multiple sectors across the region. This malware is designed to irreversibly delete data and render systems inoperable, causing significant operational disruption, and some organizations have already been impacted, indicating that the campaign is active and ongoing.

TECHNICAL DETAILS:

Wiper malware is a type of malicious software designed to delete or destroy data on computers and networks. Unlike ransomware, which demands payment, wiper malware's goal is purely destructive: it erases files, disables systems, and often destroys backups, making recovery difficult or impossible.

Threat Details

- **Malware Type:** Wiper (data destruction)
- **Primary Objective:** Permanent data erasure and system disruption
- **Target Scope:** Multiple sectors (including government, energy, finance, telecom, and critical infrastructure)
- **Impact Observed:**
  - System crashes and boot failures
  - Deletion of critical files and backups
  - Network-wide propagation in some incidents

Initial Access & Propagation (Observed Patterns)

The attackers are believed to be leveraging:

- Phishing emails with malicious attachments or links
- Compromised credentials (including VPN access)
- Exploitation of unpatched vulnerabilities
- Lateral movement via:
  - Remote administration tools
  - SMB shares and domain privileges

Indicators of Compromise (IOCs)

Organizations should monitor for:

- Unexpected system reboots or failure to boot
- Sudden deletion or corruption of files
- Unauthorized use of admin credentials
- Suspicious PowerShell or command-line activity
- Unusual outbound network traffic

RECOMMENDATIONS:

- **Strengthen Access Controls**
  - Enforce multi-factor authentication (MFA) on all remote access
  - Review and restrict privileged accounts
  - Disable unused or dormant accounts
- **Patch and Harden Systems**
  - Apply critical security patches immediately
  - Prioritize internet-facing systems

- Disable unnecessary services and ports
- **Network Segmentation**
  - Limit lateral movement by segmenting networks
  - Isolate critical systems from general user networks
- **Backup Strategy**
  - Ensure offline, immutable backups are in place
  - Regularly test backup restoration procedures
- **Monitoring & Detection**
  - Increase logging and monitoring across endpoints and networks
  - Deploy or update EDR/XDR solutions
  - Alert on suspicious administrative activity
- **Awareness & Training**
  - Educate staff about phishing, suspicious downloads, and unsafe links.
  - Encourage reporting of unusual system activity immediately.
- **If compromise is suspected:**
  - Immediately isolate affected systems from the network
  - Do not power off systems abruptly (preserve forensic evidence if possible)
  - Activate incident response procedures
  - Notify internal security teams
- If compromised, conduct a deep dive assessment to ensure the security of the environment with one of the CSC approved provider and provide the incident report as soon with necessary information.

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.