EnCyb

Severity: High

Advisory Type: Threat

Destructive Wiper Malware Threat Alert Issued by UAE Authorities

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Authorities in the United Arab Emirates have issued a cybersecurity warning regarding an increase in destructive "**wiper**" malware attacks targeting individuals, organizations and critical infrastructure. These attacks are designed to permanently erase data from compromised systems, causing severe operational disruption and data loss.

Security agencies warn that threat actors may deploy wiper malware during geopolitical tensions or as part of coordinated cyber operations targeting government, energy, and enterprise sectors. Unlike ransomware, which seeks financial gain, wiper attacks aim to destroy systems and disrupt operations, making recovery significantly more difficult.

- **Active Region:** Middle East (UAE) – Potential Global Risk
- **Target Sector:** Government, Energy, Telecommunications, Finance, Critical Infrastructure
- **Severity:** High
- **Published Date:** 13 March 2026

TECHNICAL DETAILS

- **Wiper Malware Overview:** Wiper malware is designed to erase or corrupt system data, rendering operating systems and files unusable. It may overwrite the Master Boot Record (MBR), delete system files, or corrupt storage sectors.

- **Attack Vector:** Threat actors commonly deliver wiper malware through phishing emails, malicious attachments, or compromised software updates. Exploitation of vulnerabilities in internet-facing systems may also provide initial access.

- **Execution and Propagation:** Once executed, the malware begins systematic deletion or overwriting of files and disk structures. Some variants may spread laterally across networks using stolen credentials or administrative tools.

- **Evasion Techniques:** Wiper malware may disguise itself as legitimate software or ransomware. The malware may disable security services before initiating destructive actions.

INDICATORS OF COMPROMISE

TYPE	VALUES
File Hash (MD5)	4ec3c90846af6b79ee1a5188eefa3fd21f6d4cf6
File Hash (SHA256)	2d482953418daf3dd3e16bcdcd2adc4bab16a6b9b3cb190b2840d8d4ffe359b2
File Hash (SHA1)	170b69d9d1cd1c9daf528fb7a321a21ccad32982

IMPACT

- Sudden deletion or corruption of multiple files across systems
- Damage Operating Systems
- Unexpected modification of disk partitions or boot records
- Security tools or backup services being disabled
- Large volumes of disk write operations in a short time
- Spread across networks and wipe connected devices
- Systems failing to boot after suspicious activity

RECOMMENDATIONS

- Update software and systems regularly to fix vulnerabilities
- Avoid clicking suspicious links or attachments in emails or messages
- Back up important data securely and store backups separately
- Implement network segmentation to limit malware propagation.
- Endpoint protection with behavior-based detection to block wiper malware.

REFERENCES

- UAE warns public about growing threat of destructive ‘wiper’ cyberattacks
- Cybersecurity Council warns of rising threat from ‘wiper malware' | Emirates News Agency

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com