UAE warns public about growing threat of destructive 'wiper' cyberattacks

Tracking ID#: PCS-03-1426

Date: 14-03-2026

Disclaimer: This is a shared security advisory service; hence, it can be communicated to a single dedicated point of contact. We would highly appreciate it if you assigned them to your organisation's concerned asset/technology owner. Please use it as applicable to your environment

Date: 14-03-2026

Summary:

The **UAE Cybersecurity Council** has warned about the growing threat of **wiper malware**, a type of malicious software designed to erase or damage data and disrupt digital systems rather than steal information. These attacks can delete files, corrupt operating systems, or overwrite critical disk structures, potentially causing systems to stop functioning and making recovery extremely difficult. The council noted that such cyberattacks can significantly impact both individuals and organizations, resulting in loss of personal data, service disruptions, operational delays, financial losses, and reputational damage. Some variants of wiper malware can spread rapidly across networks, infecting multiple systems within a short period and potentially disrupting critical sectors such as energy, logistics, and digital infrastructure. Wiper malware is considered a highly destructive category of malicious software because its primary objective is to permanently destroy data and disable system functionality rather than generate financial gain. After gaining access to a device or network, the malware may execute destructive actions such as deleting files, corrupting operating system components, or damaging key disk structures required for system operation. In many cases, the malware targets elements such as the **Master Boot Record (MBR)** or other essential file system components, preventing affected machines from starting normally. Due to its destructive nature, successful wiper attacks can result in large-scale system outages, prolonged operational disruptions, costly system rebuilding efforts, and long-term service interruptions. Such attacks are often linked to geopolitical conflicts or state-sponsored cyber operations aimed at disrupting critical infrastructure and causing widespread operational impact.

Target:

Applicable to all users.

Recommendation and mitigations:

- **Regularly update systems and software**- Install security updates and patches to fix known vulnerabilities that attackers may exploit.
- **Be cautious with links and attachments-** Avoid opening links or downloading files from unknown or suspicious sources, which are common infection methods.
- **Maintain secure backups**- Keep separate (offline or isolated) backups of important data so systems can be restored if files are wiped.
- **Test backups regularly**- Ensure backups work and can be used during recovery.
- **Create cyber incident response plans -** Organizations should have a clear plan for responding to cyber incidents to reduce downtime and damage.
- **Increase cybersecurity awareness-** Educate users and staff about modern cyber threats and safe digital practices.

References:

UAE warns public about growing threat of destructive 'wiper' cyberattacks