Date: 18 September 2025
Notice No: FSRA/FCCP/128/2025

To*:* Senior Executive Officers (SEO) and Principal Representatives (PR) of FSRA's Authorised Persons and Recognised Bodies.

Dear SEO / PR,

Subject: Cybercrime Prevention – Protect your organisation from Malware

In alignment with the Financial & Cyber Crime Prevention (FCCP) department's commitment to safeguarding FSRA Authorised Persons (APs) and Recognised Bodies (RBs), this notice aims to raise awareness of the threat posed by Malware. Cybercrime is a major threat to firms of all sizes and a significant proportion of these crimes are facilitated through malware-infected devices that can compromise data, disrupt operations and cause financial and reputational harm.

This notice serves as a reminder to FSRA APs and RBs to remain vigilant of malware threats and ensure the implementation and maintenance of appropriate security measures to effectively mitigate associated risks.

Overview of Malware Threats

Malware is malicious software or web content that can harm an organization by:

- Rendering devices inaccessible or otherwise unusable.
- Resulting in loss, deletion or encryption of data.
- Controlling devices to facilitate further malicious activities.
- Compromising credentials and authentication information.
- Installing illegal cryptocurrency mining software.

Overview of Common Malware Types

Malware appears in various forms and generally classified into several broad categories:

- Data exfiltration and unauthorized access e.g., spyware or Trojans.
- Disruptive and damaging software e.g., viruses and worms.
- Encryption of data e.g., Ransomware.
- Intrusive or unwanted software e.g., adware or rootkits.

Infection pathways and threat vectors

Malware can infect devices in several ways. For example:

- **Drive-by downloads**: A passive infection that occurs without active user intervention. By simply visiting a compromised or malicious website can trigger malware in the background.

- **Active Downloads:** User initiated action such as downloading or installing software from the internet where the source is untrusted or unknown.

- **Infected Media Devices**: USB stick or external hard drive can store malware and infect systems when plugged in.

- **Unsecured Network Connection**: Public Wi-Fi networks lacking proper security measures can allow cybercriminals to intercept your data, steal credentials or install malware.

- **Phishing Email**: Malicious email containing harmful attachments or links.

Prevention and Mitigation Strategies

Implementing proactive measures can significantly reduce the risk of malware infections. Below is a list of recommended practices for effective prevention and mitigation but is not an exhaustive list:

- **Install Antivirus Software**: Deploy reputable antivirus solutions to detect and block malware. Anti-virus solutions are signature based. They contain a database of known malware signatures to identify infected files and applications.

- **Apply Application Whitelisting and Safe Browsing Practices:** Restrict employees from downloading third-party applications and accessing websites known to host malicious content to prevent the installation of unapproved or potentially harmful software.

- **Use Email Filtering:** Implement email filtering systems to block malicious emails and remove executable attachments.

- **Disable Remote Desktop Protocol (RDP) when it is not needed:** Limit remote access to reduce the attack surface area. If remote access is necessary, enable Multi Factor Authentication (MFA) to strengthen security and ensure only authorized personnel can connect.

- **Patch devices:** Keep all hardware and firmware up to date. Patching addresses security vulnerabilities and enhances device performance.

- **Activate Automatic Updates**: Configure operating systems, applications and firmware to update automatically whenever possible. Be aware that some updates are no longer available when products reach their end-of-life cycle.

- **Control USB Drive Usage:** Limit or block access to USB ports to prevent the inadvertent introduction of malware via infected external drives. This policy reduces the risk of untracked or malicious media being connected to computer systems.

- **Configure Firewall Rules:** Utilise built-in firewall features on endpoints to block unauthorized traffic, restrict access to certain sites or deny specific IP addresses.

- **Apply Network controls:** Network controls can filter traffic through controls that define what traffic is allowed into the network from the internet.

- **Deploy Intrusion Detection and Prevention system (IDS/IPS):** Implement IDS or IPS solutions to monitor network traffic for malicious activity. IDS systems generate alerts for suspicious patterns, requiring manual response whereas IPS can automatically block malicious traffic in real-time, offering enhanced protection.

- **Maintain Offline Backups:** Create offline backups that are kept separate from the network. Thereby, strengthening the ability to recover from malware incidents.

Firms are also reminded to adopt a 'defence in depth' approach by using layers of defence to detect malware and stop it before it causes harm.

Your vigilance and adherence to these measures are crucial for maintaining the security, integrity and stability of the ADGM and wider UAE's financial ecosystem.

For any further clarification, Authorised Persons and Recognised Bodies are required to reach out by email to fccp-cybercrimeprevention@adgm.com

Sincerely,

Financial & Cyber Crime Prevention