

INCIDENTS WE DEALT WITH



Detected an incident?
 We are here to help!



047774003
 incident@aecert.ae

ADVISORYS OF THIS MONTH



Abuse of .MSI Windows Installer

Advanced Notification of abuse custom actions in Windows Installer .MSI to execute malicious JavaScript

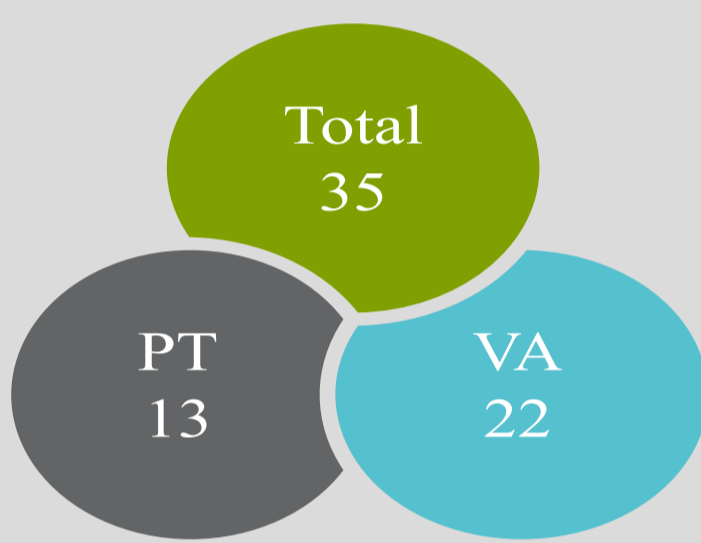


Windows Task Scheduler Zero-day

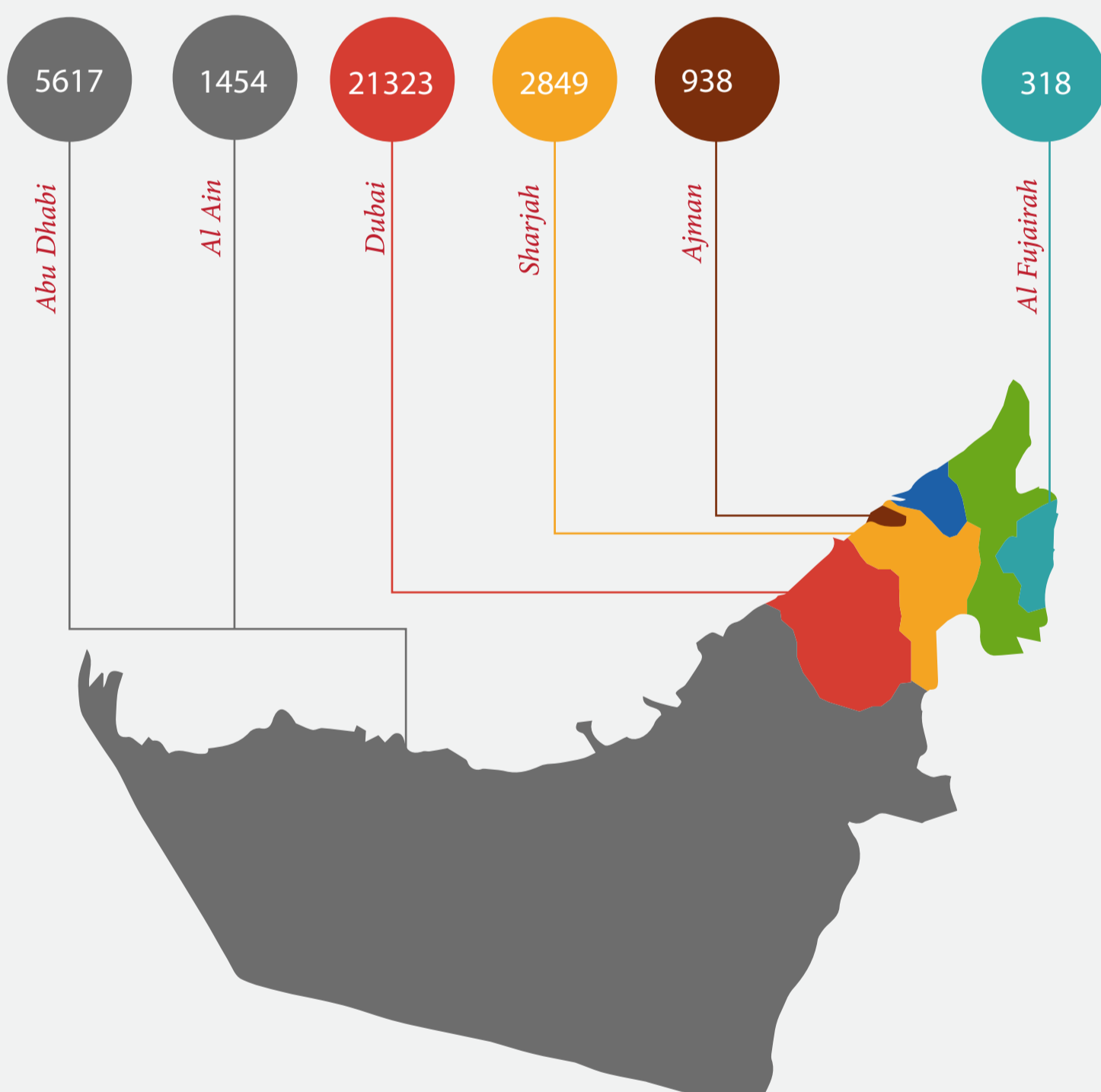
New zero-day exploit for the Windows operating system

Want to be up-to-date on the latest Malwares?
 Join our advisory list www.tr.ae/aeCERT

VULNERABILITY ASSESS AND PENETRATION TESTING STATISTICS - YEAR TO DATE



MALWARE PER EMIRATES



YOU ARE SMARTER, DON'T BE A VICTIM OF CYBER FRAUD!

Awareness tips

- Its always good to update yourself with the latest Cyber security trends
- Always keep a hard copy of your bank statement.
- Always enable the pin code auto lock in your mobile phone.
- Dont save your data and passwords in your phone in an easy way to be understand by others



You can request your own session, or join one
 Learn more through www.tr.ae/aeCERT

About aeCERT

The Computer Emergency Response Team (aeCERT) was established by Resolution 5/89 of 2008 issued by the Ministerial Council for Services. The team was established to improve the standards and practices of information security, and protect the IT infrastructure in the UAE from risks and violations, in conformity with the TRA strategy that aims at supporting and ensuring a safer cyber space for the residents of the UAE, both nationals and expatriates.