Cyber Security Incident Learning:

WHAT WE KNOW

- Current information indicates that the perpetrator/s/malicious actor/s gained unauthorized access to the computer network by compromising an internet facing web server.
- Once the perpetrator/malicious actor/s accessed the network, the perpetrator/s/malicious actor/s pivoted to an end user device through an RDP connection, by using a poorly protected shared privileged account. A fake OneDrive stand alone update program was installed by the malicious actor/s.
- This is how the malicious actor installed several surveillance and credential harvesting tools on the various workstations, and used these tools to move laterally on the network.
- The malicious actor/s then activated malicious ransomware on other servers on the network, which in turn disabled these servers.
- The IM team noticed the service disruption, and upon further investigation identified the ransomware.
- To contain further spread of the ransomware the IM team responded preemptively by shutting down the network and services.

What are the learnings for implementation?

HOW DID THIS HAPPEN?

Based on available information, a number of control failures led to the security breach. Poor perimeter protection and detection capabilities, ineffective configuration and software lifecycle management, inadequate account and password controls, and lack of event and alert monitoring capabilities led to unencumbered access to the internal network and services.

WHAT WAS THE OBJECTIVE OF THE Malicious Actor/s?

Based on the activation of the ransomware the Malicious Actor's motive was most likely extortion, but gaining and stealing personal information of various individual users associated with the affected servers, in an attempt to obtain internet banking information to steal money from users' bank accounts.