National Computer Board

CERT-MU

CERT-MU Security Alert

Emotet Malware Can Shut Down Entire Network By Overheating PCs

Issue Date: 09 April 2020

Description

Emotet is one of the notorious malware wreaking havoc across industries by hacking systems. In the latest attack, the malware was able to spread through the entire network of an organisation and shut it down by overheating computers. The malware penetrated the organisation through phishing and propagated via network shares and legacy protocols. Consequently, Emotet was able to shut down the organisation's core services.

The virus avoided detection by antivirus solutions through regular updates from an attacker controlled command and control (C2) infrastructure and spread through the company's systems, causing network outages and shutting down essential services.

Affected Systems:

- Microsoft systems

Attack Methodology

- Phishing email with attachment was sent to an employee.
- Employee clicked on the attachment.
- Emotet malware managed to evade all detection systems as it is regularly controlled by the attacker's command and control (C2C) server.
- Employees' credentials were extracted by the phishing email attachment.
- The Emotet payload was delivered and executed.

- Other employees and external contacts were targeted.
- Credentials were stolen and more systems were affected.
- The malware took over the control of the entire network by gaining access to the admin account.
- All the PCs connected to the network started experiencing overheating, freezing, abrupt shutdowns and reboot due to Blue Screen of Death.
- Emotet malware also chugged all the bandwidth thus slowing down the internet connection of the network.

CERT-MU advises all organisations using Microsoft systems to be vigilant and recommends users to deploy email filtering tools to avoid potential phishing attacks and multi-factor authorization to evade illegal access to the system.

Report Cyber Incidents

Let us unite together for a Safe Mauritian cyberspace during this crisis situation.

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
National Computer Board
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu
MAUCORS: http://maucors.govmu.org