Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 15 June 2022

Phobos Ransomware: A threat to the Healthcare Service Providers

Severity Level: High

Impact: File Encryption and Data Exfiltration

Description:

As per the cyber threat intelligence gathered by CERT-MU's Security Operations Centre (SOC), it was found that a new ransomware strain known as Phobos Ransomware is in circulation and is targeting healthcare service providers. This ransomware has targeted healthcare service providers, with victims in to other countries such the United States, Seychelles, Portugal, Brazil, Indonesia, Germany, Romania, and Japan.

CERT-MU advises organisations, especially the healthcare service providers to watch out this ransomware and take precautionary measures to avoid becoming victims.

Technical Information:

The ransomware is based on the Dharma malware that first appeared at the beginning of 2019. It spreads into several systems via compromised Remote Desktop Protocol (RDP) connections. Moreover, this malware does not use any UAC bypass methods. Unlike other cybercrime gangs that go after big hunts, Phobos creators go after smaller firms that do not have sufficient funding to pay massive ransoms. Its perpetrators demand a little ransom payment, which appeals to victims and enhances the chances of payment. The average Phobos ransom payment in July 2021 was $54,700.

Indicators of Compromise (IOSs)

MD5

c3ccde9c3fab53d5c749b2186e997bdc

c75d77ce6144a284bcec84022a5d1166

SHA-256

c21de9109580e03f0fc0a71c10bfe2923927eb0dfe748bea47d550f1fe7f1715
161c471b0aaaf0d7c1f0267ebb837e10fb8c5edfe09b0d00bf2472820f413713

SHA1

b494a696f4edbbd3831163dfd0f1b5efc134d068
72c38863c4367096388766250c70437e84883bde

Workarounds

- Monitor your network and block any threat indicators such as suspicious traffic, unusual logins, repeated attempts of unauthorized applications or increased in escalated privileges.
- Search for the above indicators of compromise and block them.
- Ensure you have an updated data backup.

Report Cyber Incidents

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)
Ministry of Information Technology, Communication and Innovation
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org