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

CERT-MU Security Alert

Date of Issue: 18 October 2022

New Prestige Ransomware Targets Organizations in Transport and Logistics Sectors

Severity Level: High

Affected sectors: Transport and Logistics

Description:

According to a Microsoft research and analysis, a new ransomware dubbed as "Prestige" is currently being used to target transportation and logistics organizations. Countries such Ukraine and Poland has already been targeted. The strain of ransomware was firstly identified in the wild on October 11, 2022. Attackers were seen deploying the ransomware payloads across their victims' enterprise networks.

According to Microsoft Threat Intelligence, the malicious activities shares victimology with recent Russian state-aligned activity, specifically on affected geographies and countries, and overlaps with previous victims of the FoxBlade malware (also known as HermeticWiper).

Technical Information

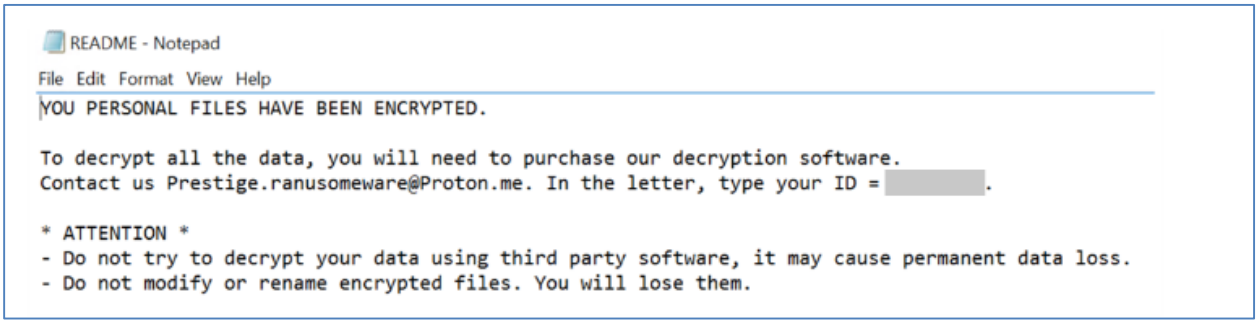
Microsoft Threat Intelligence highlights the following three methods used for Prestige ransomware deployment:

Method 1: The ransomware payload is copied to the ADMIN$ share of a remote system, and Impacket is used to remotely create a Windows Scheduled Task on target systems to execute the payload.

Method 2: The ransomware payload is copied to the ADMIN$ share of a remote system, and Impacket is used to remotely invoke an encoded PowerShell command on target systems to execute the payload.

Method 3: The ransomware payload is copied to an Active Directory Domain Controller and deployed to systems using the Default Domain Group Policy Object.

Once deployed, Prestige ransomware payloads will drop ransom notes named "README.txt" in the root directory of each drive it encrypts.



It encrypts files based on extensions matching a predefined list and adds the *.enc* extension at the end of the files' names after encryption. It uses the CryptoPP C++ library to AES-encrypt each matching file on compromised systems, and it will delete the backup catalog and all volume shadow copies to hinder recovery efforts.

Indicators of Compromise

The following IOCs were identified during the investigation. Users are advised to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems.

Indicator	Type	Description
5dd1ca0d471dee41eb3ea0b6ea117810f228354fc3b7b47400a812573d40d91d	SHA-256	Prestige ransomware payload
5fc44c7342b84f50f24758e39c8848b2f0991e8817ef5465844f5f2ff6085a57	SHA-256	Prestige ransomware payload
6cff0bbd62efe99f381e5cc0c4182b0fb7a9a34e4be9ce68ee6b0d0ea3eee39c	SHA-256	Prestige ransomware payload
a32bbc5df4195de63ea06feb46cd6b55	Import hash	Unique PE Import Hash shared by ransomware payloads
C:\Users\Public\README	File path	File path of the ransom note

Workarounds

To prevent or mitigate such the Prestige Ransomware attack, users are advised to adopt the following security measures:

- Block process creations originating from PSExec and WMI commands to stop lateral movement utilizing the WMIexec component of Impacket.
- Enable Tamper protection to prevent attacks from stopping or interfering with Microsoft Defender.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity, including VPNs.

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
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org