National Computer Board

CERT-MU

# CERT-MU Security Alert

Date of Issue: 07 March 2022

## WhisperGate or IssacWiper or HermeticWiper : Destructive Malware Targeting Organizations

### 1. Description

Cybersecurity researchers have discovered various destructive malicious programs which are being exploited in the wild and targeting organisations. These malware have been dubbed as WhisperGate, IssacWiper and HermeticWiper malware. Destructive malware can present a direct threat to an organization's daily operations, impacting the availability of critical assets and data. Recently, the WhisperGate and HermeticWiper, two destructive malware strains were seen in attacks against organizations in Ukraine. According to security researchers, further disruptive cyberattacks against organizations in Ukraine are likely to occur and may unintentionally spill over to organisations in other countries. Organisations should therefore increase vigilance and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event.

### 2. Technical Details

a) **WhisperGate** is a form of wiper malware that masquerades as ransomware and targets a system master boot record for destruction rather than encrypting files. The malware, first discovered by the Microsoft Threat Intelligence Center and was used in multiple cyberattacks against Ukrainian organisations. WhisperGate has two stages that corrupts a system's master boot record, displays a fake ransomware note, and encrypts files based on certain file extensions. Although a ransomware message is displayed during the attack, Microsoft highlighted that the targeted data is destroyed, and is not recoverable even if a ransom is paid.

b) **HermeticWiper**, another strain of disruptive wiper malware, was used to target Ukrainian organisations shortly before the launch of a Russian invasion. Discovered by ESET security firm, the malware renders computers inoperable. These attacks were observed targeting hundreds of computers in the region, came just hours after a series of distributed denial-of-service (DDoS) attacks knocked several important websites in the country offline. As per security researchers, the ransomware component (HermeticRansom) was added to the HermeticWiper to divert attention away from the destructive wiper eating away at another part of a network. HermeticWiper uses four drivers from the EaseUS Partition Master for its operations. It disables Windows' Volume Shadow Copy Service before wiping data, then wipes evidence of itself from disks.

c) **IssacWiper** is another data wiper malware that was observed deployed against an unnamed Ukrainian government network, a day after destructive cyber-attacks struck multiple entities in the country preceding the start of Russia's military invasion. The IssacWiper was detected on organisations that was not affected by the HermeticWiper. It is suspected that the attackers leveraged tools like Impacket and RemCom, a remote access software, for the lateral movement and malware distribution. As per security researchers, IsaacWiper shares no code-level overlaps with HermeticWiper and is substantially less sophisticated, even as it sets out to enumerate all the physical and logical drives before proceeding to carry out its file wiping operations.

## 3. Mitigations - Best Practices for Handling Destructive Malware

This section is focused on the threat of malware using enterprise-scale distributed propagation methods and provides recommended guidance and considerations for an organisation to address as part of their network architecture, security baseline, continuous monitoring, and incident response practices.

CERT-MU urges all organizations to implement the following recommendations to increase their cyber resilience against this threat:

### Potential Distribution Vectors

Destructive malware may use popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from websites, and virus-infected files downloaded from peer-to-peer connections. Malware seeks to exploit existing vulnerabilities on systems for quiet and easy access.

The malware has the capability to target a large scope of systems and can execute across multiple systems throughout a network. As a result, it is important for organizations to assess their

environment for atypical channels for malware delivery and/or propagation throughout their systems. Systems to assess include:

- Enterprise applications – particularly those that have the capability to directly interface with and impact multiple hosts and endpoints. Common examples include:
- Patch management systems,
- Asset management systems,
- Remote assistance software (typically used by the corporate help desk),
- Antivirus (AV) software,
- Systems assigned to system and network administrative personnel,
- Centralized backup servers, and
- Centralized file shares.

**Here are few simple yet effective steps that will help you mitigate Wiper malware and safeguard your infrastructure:**

- Impart Knowledge: Educate users about useful defense practices. Users should be well aware of the email etiquette and vigilant surfing practices. Teach them to identify suspicious websites, infected links, phishing emails, URL abnormalities, etc. Diligent use of the computer system along with the internet will prevent Wiper from getting a foothold of your system along with the data stored on it.

- Regularly patch your system and related software: Operating system updates not only include additional features and functionality but also comprises security patches against system voids and vulnerabilities. Keeping an up-to-date device adds a security layer to your device.

- Use Powerful Malware Protection: Using a powerful and most recent malware protection suite will guard you against malicious attacks.

- Monitor changes: Keep your eyes open to any uncommon changes in your device.

## 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