JOINT NEWS RELEASE BY SINGAPORE POLICE FORCE AND CYBER SECURITY AGENCY OF SINGAPORE

JOINT ADVISORY ON THE DISTRIBUTION OF RANSOMWARE "MAGNIBER" THROUGH FAKE WINDOWS OPERATING SYSTEM (OS) UPDATES

The Police and the Cyber Security Agency of Singapore (CSA) would like to alert the public on a ransomware variant known as "Magniber" distributed through fake Windows OS updates that results in the encryption of data in the victims' device(s).

2 Ransomware is a type of malware designed to encrypt files on a device till a ransom is paid to decrypt the files. In recent weeks, the Police and CSA have observed incidents where data on victims' devices were encrypted with the "Magniber" ransomware after victims download and install programs masquerading as Windows OS updates. A ransom note would be displayed to demand for payment in the form of cryptocurrencies such as Bitcoin if the victims would like to regain access to their data.

3 Early reports of the "Magniber" ransomware variant indicated that the ransomware was spreading through vulnerabilities in Internet Explorer. In late 2021 to early 2022, it started to spread through other Internet browsers such as Microsoft Edge and Chrome. There are now reports that the ransomware may be distributed through websites offering pirated or cracked software, i.e. warez and cracked sites. Inadvertent downloads and installation of such malware could possibly expose victims to the following risks:

a) Encryption of users' data and demand for ransom to decrypt the data;
b) Theft and subsequent misuse of personal data such as details of their bank accounts / credit cards, social media accounts, photos and videos stored in

devices. Attackers can also use such data to access the victims' financial and social media accounts to steal money and/or impersonate victims to commit credit card frauds, scams and extortion using information such as the photos and videos obtained;

c) Allowing attackers to gain remote control of their devices, resulting in the loss of data and/or control over devices;

d) Slowdown of the devices' performance due to possible unauthorised processes invoked by the malware infection (e.g. crypto-jacking).

4 Members of the public are advised to follow the steps below to ensure that their devices are adequately protected against malware:

a) Ensure that your mobile phones, computers and other devices are updated regularly with the latest OS versions and install anti-virus applications that can detect and remove malware;

b) Download files, including applications and updates, directly from official and verified sources as this ensures that the downloaded files are free from malware or viruses;

c) Backup your data regularly in a separate system and keep it offline to retain access to your data in the event of a ransomware incident. Such data backups can be done using an external hard disk that is disconnected from your devices or in the cloud;

d) Avoid clicking on pop-up ads or opening files or email attachments from unknown senders.

5 In the event that you have fallen prey to a ransomware, members of the public are advised to take the following steps:

a) Lodge a police report immediately to receive assistance from the relevant authorities;

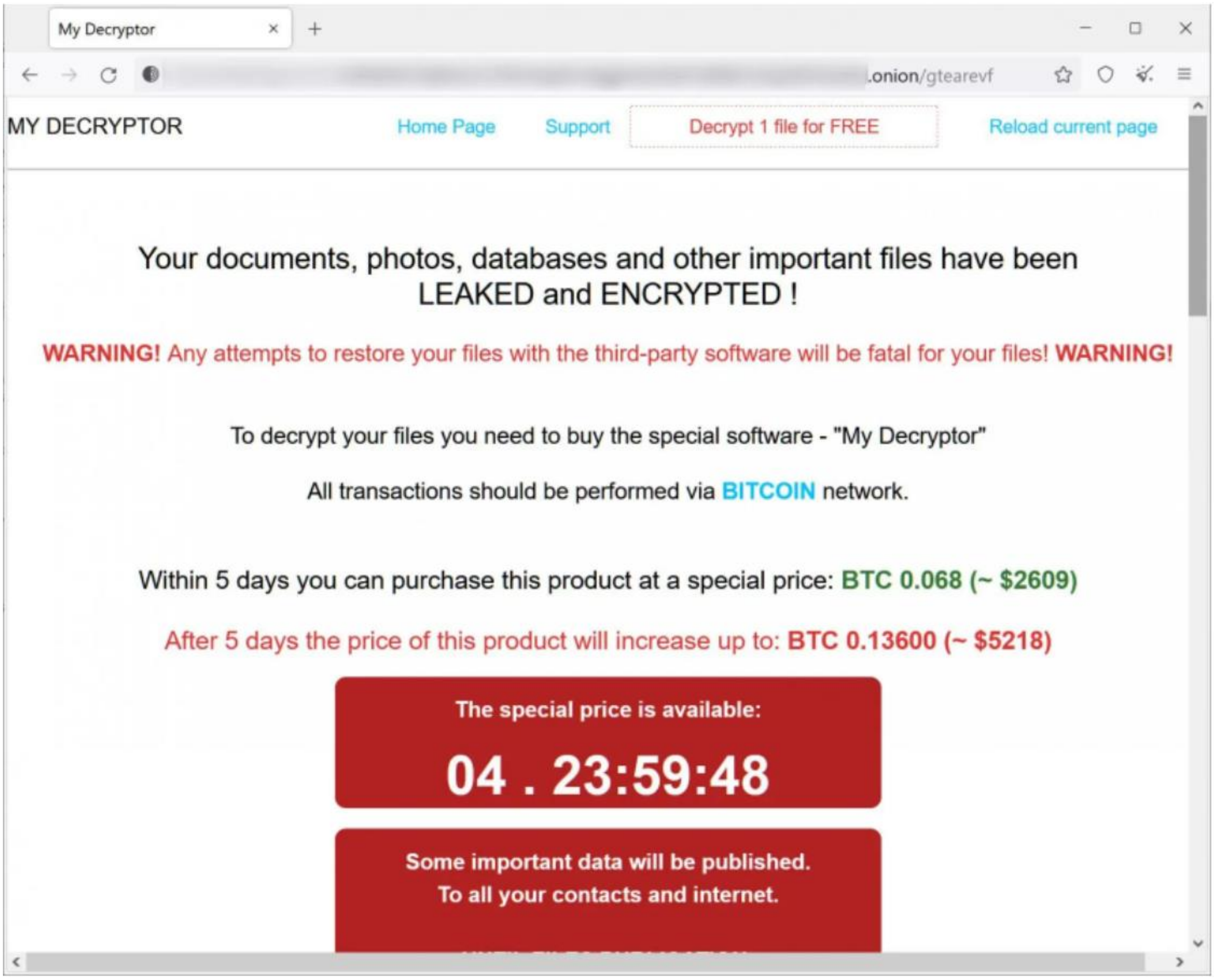
b) We do not recommend paying the ransom as demanded by the attacker as it does not guarantee that your data would be decrypted and encourages the attacker to continue their criminal activities and target more victims;

c) Visit the “No More Ransom” website (https://www.nomoreransom.org) to check if there are available decryptors.

6 To find out more about ransomware and how preventive steps can be taken to protect your systems and data, members of public may wish to refer to CSA’s SingCERT advisory at https://www.csa.gov.sg/alerts-advisories/Advisories/2021/ad-2021-009.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY OF SINGAPORE
14 MAY 2022 @ 5PM

Annex A



Your documents, photos, databases and other important files have been LEAKED and ENCRYPTED !

WARNING! Any attempts to restore your files with the third-party software will be fatal for your files! **WARNING!**

To decrypt your files you need to buy the special software - "My Decryptor"

All transactions should be performed via **BITCOIN** network.

Within 5 days you can purchase this product at a special price: **BTC 0.068 (~ $2609)**

After 5 days the price of this product will increase up to: **BTC 0.13600 (~ $5218)**

The special price is available:

04 . 23:59:48

Some important data will be published.
To all your contacts and internet.

Screenshot of “Magniber” ransomware locking victim’s computer
Source: www.bleepingcomputer.com