Hello (WickrMe) Ransomware (CSB21-03)

February 10, 2021

Hello ransomware, also known as WickrMe ransomware, was first identified on August 2020. There are reports that the Hello ransomware has spread throughout the world, including Latin America, Asia, and North America, in just a few weeks after it resurfaced on early January 2021.

Hello ransomware uses a high-level type of cipher to encrypt data and changes their victim's files with the extension **.hello** that will look like this: **filename.docx.hello**. The virus will create a Readme text file (Readme!!!.txt) containing the ransom instruction on how or where they can message or email the threat actors for decryption.

Hello ransomware uses several deceiving tactics to enter their victim's computer. In most instances, it spreads via spam email (MalSpam campaign), malicious installers like pirated apps and freeware software's, Trojan downloader, fake software update, and malicious online advertisement.

HOW IT WORKS

Threat Actors uses MalSpam to populate Hello WickrMe Ransomware

A spam email will be sent to the victim's email containing malicious files and links

Once the victim opened and downloaded the malicious file, the ransomware will infect the victim's computer

Ransomware will encrypt victim's files

The virus will create a text file containing the ransom note and instructions on how victims can contact and decrypt their files

IMPACT

- Data can be altered, damaged, deleted, and infused with additional computer viruses.
- Interfere with the normal functioning of the computer system or prevent its utilization

MITIGATIONS

- Do not pay the ransom.
- Coordinate with IT Project Officer assigned in your office/unit.
- Remove infected computer within the network.
- Perform a full system scan in safe mode to remove any infections.

PREVENTION

- Do a regular file back-up using cloud backup and storage or an unplugged storage device.
- Consider encrypting the data on your backup.
- Update your operating system, software, and antivirus frequently.
- Ignore all emails from unknown sender. Avoid opening or downloading files attached to spam emails.
- Do not use cracked or untrusted program
- Regularly run a complete scan to check the computer for present of malware.

REFERENCE

- https://www.brucert.org.bn/advisory-hello-wickrme-ransomware