COMPUTER SECURITY BULLETIN

Risk/Impact Rating: SERIOUS

< RANSOMWARE >

Description:

Ransomware is a type of malware that infects computer systems, restricting users' access to the infected systems.

It holds your PC or files for "ransom" and often spread through phishing emails that contain malicious attachments or through drive-by downloading.

Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

Two types of ransomware:

1. Lockscreen ransomware - **locks the victim out of the operating system**, making it impossible to access the desktop and any apps or files. The files are not encrypted in this case, but the attackers still ask for a "ransom" to unlock the infected computer.

2. Encryption ransomware - designed to block system files and demand payment to provide the victim with the key that can decrypt the blocked content.

Ransomware not only targets home users; businesses can also become infected with it, leading to negative consequences, including:

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information.

In addition, decrypting files does not mean the malware infection itself has been removed.

Recommendations / Solutions / How To's:

For PNP Personnel

- Employ a data back-up and recovery plan for all critical information regularly;
- Keep your software up-to-date;
- Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing;
- Use a reputable security suite;
- Do not follow unsolicited Web links in emails;
- Show hidden file extensions;
- Disconnect from WiFi or unplug from the network immediately; and
- Contact the customer care number for your country/region.

For Key officers and Technical Staff

- Restrict users' ability (permissions) to install and run unwanted software applications;
- Avoid enabling macros from email attachments;
- Filter EXEs in email;
- Disable files running from AppData/LocalAppData folders;
- Disable RDP (Remote Desktop Protocol);
- Check to see if a decryptor is available;
- Use system Restore to get back to a known-clean state; and
- Set the BIOS clock back.

References:

https://www.us-cert.gov/ncas/alerts/TA16-250A

https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

http://www.welivesecurity.com/2016/10/10/ransomware-expert-advice-keep-safe-secure/