Cert.to Advisory

Tonga National Computer Emergency Response Team

Threat Name/Title: Petya/NotPetya/Petna

Original Issue Date: 28th June 2017

Updated: 29th June 2017

Severity Rating: High

Description:
Further to the advisory sent out yesterday, this serves as an update with information received to date. We will also try to simplify the advisory and at the same provide the attached updated technical advisory.

The new ransomware campaign now also referred to as NotPetya (originally reported as Petya) is affecting Microsoft Windows devices globally.

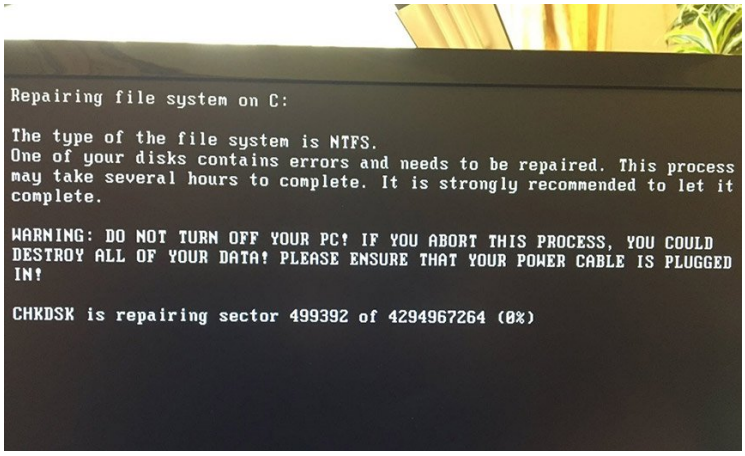
To protect your organisation, it's critical to ensure that the software on all devices is fully up to date.

In many ways, this ransomware is behaving similarly to WannaCry Ransomware — it infects unupdated Windows devices by exploiting a software vulnerability. If Petya infects a device, it will encrypt the hard drive, demanding a ransom is paid to regain access to the device.

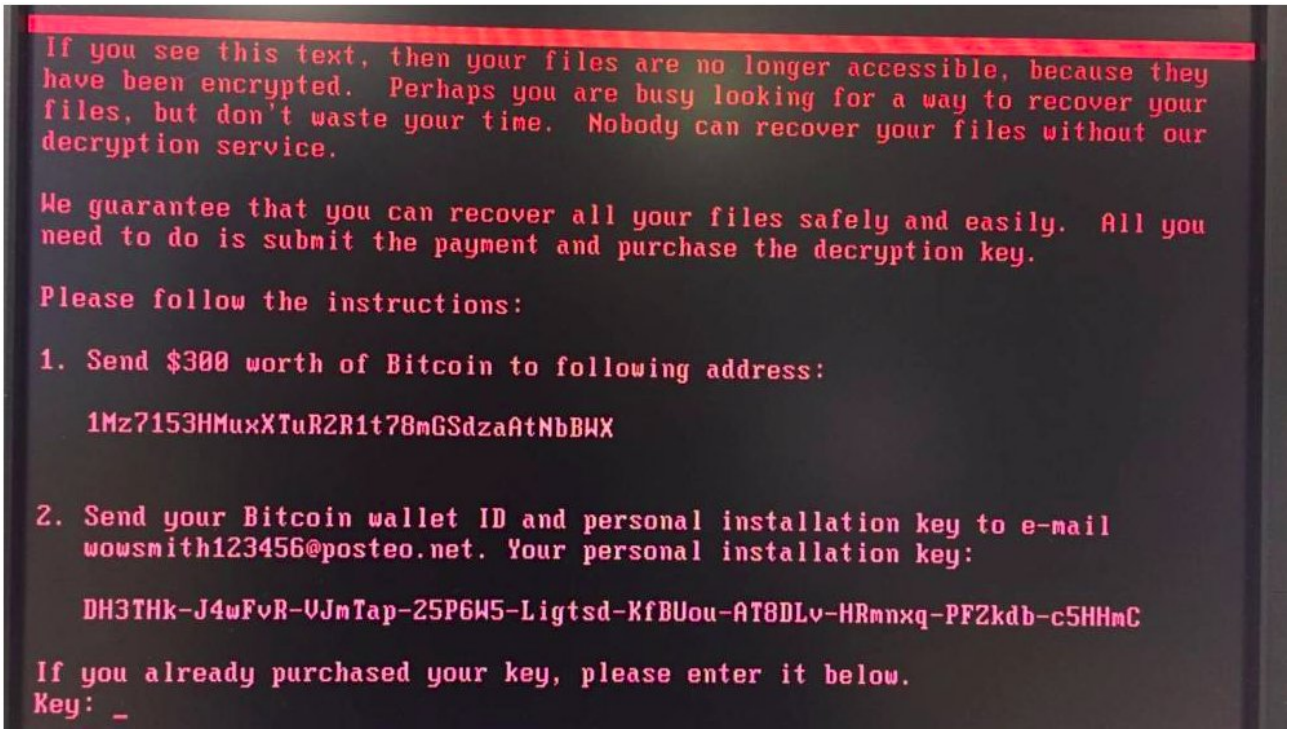
A point of difference that this ransomware has from WannaCry is that once a single computer in you computer network is infected, the program looks for other computers on the network and infects them as well — even when they're fully up to date.

cert.to strongly recommends that the ransom is not paid, under any circumstances. At least one email address used to communicate with the attackers has been taken down, and subsequent email addresses are likely to be taken down as well. In this case, this means that you will not be able to recover your files, even if the ransom is paid.

What to do if you're hit by the ransomware?
This is an example of what you may see if Petya is attempting to encrypt your files:



If you see the above, turn your device off, and don't turn it on again — an IT Specialist may be able to recover your files. If you turn your device back on again and NotPetya encrypts your data, there may be no way to recover it. When this has happened, you'll see something like this on your screen:



What to do to prevent?

In priority order, these are the technical steps that *cert.to* recommends you take immediately to protect your network.

1. Ensure all Windows systems in your network is updated. In this case, it's particularly important to apply the MS17-010 Microsoft patch. *cert.to* recommends that you apply all security updates to all systems and software.
2. Make sure you've backed up your system and data and if possible have stored your files securely outside your network.
3. Make sure that firewalls and anti-virus software is installed, up-to-date, and fully operational.
4. Be careful when opening emails and clicking on links. These emails could be from anyone, including an email address you're familiar with.
5. Ensure staff are aware of this campaign. Remind them to be vigilant about links and attachments contained in incoming emails.
6. There is also a "*vaccine*" similar to a "*kill switch*" that can be applied to ensure that ransomware does not encrypt your data. This would require assistance from your IT Staff and instructions can be obtained from here: https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/

If you need further information, please contact the Tonga National CERT as below:

Tonga National CERT
Ministry of MEIDECC
Sanft Building
Nuku'alofa
Tel: 2378
email: cert@cert.to, web: www.cert.to

References:

https://www.cert.govt.nz/businesses-and-individuals/recent-threats/notpetya-targeting-microsoft-windows-computers