GOVERNMENT OF BERMUDA

The Cabinet Office

Department of Communication and Information

For immediate release

To: ALL MEDIA
Please see the media release below.

EMO: Government's Cybersecurity Working Group Warns Business Community of Petya Variant Ransomware Outbreak

Hamilton, June 27, 2017 - According to multiple sources, a new variant of Petya ransomware, also known as Petwrap, is spreading rapidly due to the same Windows SMBv1 vulnerability that the WannaCry ransomware abused. There are reports of large scale infections in the USA, and Europe. Reports of systems affected include: harbour terminals, airports, electricity grids, banks, factories, offices, insurance, and military.

Petya works very differently from other ransomware malware. Petya does not encrypt files on a targeted system one by one. Instead, it reboots victims computers and encrypts the hard drive's master file table (MFT) and renders the master boot record (MBR) inoperable. This restricts access to the full system by seizing information about file names, sizes, and location on the physical disk. Petya replaces the computer's MBR with its own malicious code that displays the ransom note and leaves computers unable to boot. It appears that Petya uses the Eternalblue NSA exploit, SMB share and lateral movement using WMIC similar to Wannacry but also spreading with a client-side attack using CVE-2017-0199.

Unlike the 2015/2016 Petya ransomware it doesn't look like there are decryption keys available.

The EMO is advising businesses to take the following precautions:

- Patch your systems for MS17-010, block SMB sharing at the firewall and disable WMIC if possible and have offline backups. If possible, block RTF (rich text) files at your e-mail gateway.
- To safeguard against any ransomware infection, you should always be suspicious of unwanted files and documents sent over an email and should never click on links inside them unless you have verified the source.
- Keep a good back-up routine in place that makes their copies to an external storage device that isn't always connected to your PC. Small busineses and home users should consider using cloud services to back up their important files. Many service providers (for example, email providers) offer a small amount of cloud storage space for free.
- Run an anti-virus security suite on your system regularly, and keep it up-to-date. Home users should turn on Windows Updates and run it.
- Always browse the Internet safely.

- Ends -