BTS INFORMATION SECURITY NEWS

Petya-Like Malware

Late June 2017 another malware was released into the international community that was labeled as a Petya variant. In previous years Petya was a ransomware that locked files from their users and asked for a fee to give them it back. The new malware that was released is not technically ransomware, but is called a wiper. It takes files from the users on their devices and deletes them. Unlike the Petya malware in the past, this one does not offer the choice of receiving any information back even when paying the hefty price that they request. Ukraine was hit by this virus in the wake of their independence day, leaving some to suggest that it was conducted by pro-Russian actors.

STOP | THINK | CONNECT™

Malware like this could damage files that are needed for the City of Portland to function. Protecting information is a responsibility we all have as employees. Follow the Stop, Think, Connect methods to reduce possibilities of an incident. Always Stop for a moment to Think about where you are going before you Connect to something.

- **Stop** - Take a moment to...
- **Think** - About your actions before you...
- **Connect** - To an unknown resource

"...the attack was aimed at disrupting… Ukraine and causing political destabilization." - Link

The original Petya ransomware made a computer unusable until a ransom was paid

Picture from BBC News: Link

Article from Arstechnica: Link

Questions to consider:

Q: Where do you keep your files?
A: Make sure to save files on OneDrive or the file server at work to keep files safe. Saving to the Desktop is not good practice.

Q: Do you read emails carefully?
A: Phishing is a huge cause of malware downloads. Make sure you visit our website, link below, to read how to identify phishing emails.

When at home

When you are at work BTS provides file shares and OneDrive to keep your files backed up in a secure place. When at home backup your most important files on a cloud service you trust, or an external hard drive. This could limit the possibilities of losing important files to a wiper malware like Petya.

This malware used the same exploit as Wanna-Cry from earlier this year. Keeping your machine up-to-date with patching will limit your exposure.

Contact Us

For questions, concerns, or feedback regarding City information security please contact BTS InfoSec at: btsinfosec@portlandoregon.gov.

For all other BTS questions, please contact the BTS Help Desk: btshelpdesk@portlandoregon.gov. x35199

Information Security Resources: https://www.portlandoregon.gov/bts/InfoSec