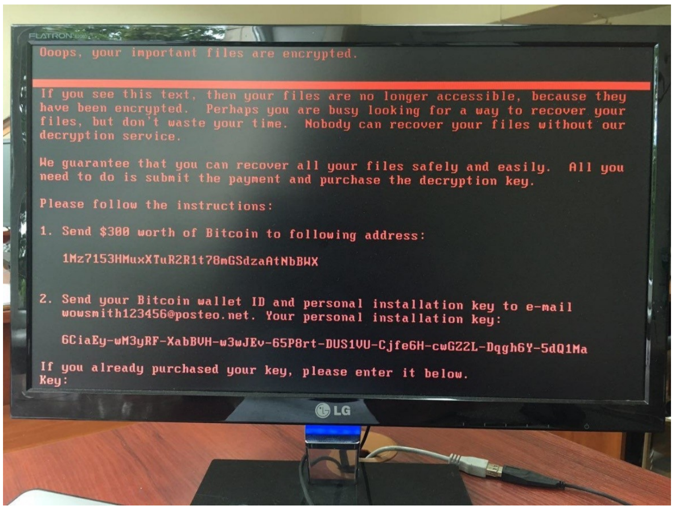
Petya Ransomware Spreads Across Europe

Written by Marco Attard
30 June 2017

A malware spectre is haunting Europe-- a strain of the malicious code dubbed Petya, first seen encrypting computers in Ukraine before spreading to Spain, Germany, the UK, the Netherlands, Israel and the US.



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   6CiaEy-wM3yRF-XabBVH-w3wJEv-65P8rt-DUS1VU-Cjfe6H-cwGZ2L-Dqgh6Y-5dQ1Ma

If you already purchased your key, please enter it below.
Key:
```

Also known as NotPetya, Petwrap or ExPetr, the malware has affected governments and industries, including shipping firms, airports, banks, a petroleum giant and even the radiation monitoring system at the Chernobyl nuclear reactor. According to Kaspersky, 50% of the malware's targets are industrial in nature, making it extremely dangerous since it can paralyse automation/control systems.

“[T]his malware campaign was not designed as a ransomware attack for financial gain,” a Kaspersky Labs blog analysis reads. “Instead, it appears it was designed as a wiper pretending to be ransomware.”

Lending support to this theory is the fact the malware generated just 3.99 BTC-- around $10300.

But what is Petya, or this variant thereof? While the malware known as Petya has existed since 2016, the version used in the current cyberattack has been modified to spread via worm. Petya/NotPetya uses the same Eternal Blue and Eternal Romance exploits as the recent WannaCry, as paired with SMB network spreading techniques allowing it to spread within organisations patched against Eternal Blue.

According to Symantec, the attack's Patient Zero is MEDoc, a tax and accounting software package widely used in Ukraine. This suggests the country was the primary target, but since Petya is a worm, it can self-propagate and spread across all computers in a network. Once it attacks, Petya shows ransom payment instructions before it starts encrypting files using a separate AES-128 encryption key for each file encrypted. In turn, the key is encrypted using an RSA-2048 public key belonging to malicious actors.

Protection against Petya involves a number of steps. First off, one must ensure the MS17-010 update is installed, the SMB v.1 service pack is disabled (or uninstalled), and the TCP 139 and 445 ports are blocked. Admins should also restrict perfc.dat file execution, crucial systems are backed up and instruct employees to be very careful when dealing with incoming emails. A properly configured malware solution should also be in use.

Go Petya Ransomware Outbreak: Here's What You Need to Know (Symantec)

Go More than 50% of Organisations Attacked by ExPetr (Petya) Cryptolocker are Industrial Companies (Kaspsersky Lab ICS CERT)