Communicating WNCRY

What is it and what happened?

- WannaCry is Malware, specifically, Ransomware
- *“malicious software which covertly encrypts your files – preventing you from accessing them – then demands payment for their safe recovery. Like most tactics employed in cyberattacks, ransomware attacks can occur after clicking on a phishing link or visiting a compromised website.”*
- However, WannaCry ransomware deviates from the traditional ransomware definition by including a component that is able to find vulnerable systems on a local network and spread that way as well. This type of malicious software behavior is called a “**worm**”
- Because **WannaCry combines two extremely destructive capabilities**, it has been far more disruptive and destructive than previous cases of ransomware that we’ve seen over the past 18-24 months.

How does a company protect/mitigate the risk

- **Immediate Steps:**
- Ensure MS-17-010 patch is installed on every Windows system, including Windows XP
- Disable SMBv1, an older version of the SMB protocol, and block port 445 at the perimeter, but test first since this may cause some business interruption. Generally, the SMB protocol does not need to be exposed externally, and is only used internally.
- Ensure your security program has an understanding of what ports, protocols and services are required for your business to operate, and disable any that are not, especially port 445
- Whitelist the WNCRY “kill switch” domains
  - *www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
    *www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
  - (remove square brackets [] when whitelisting)

How does a company protect/mitigate the risk

- **Secondary Steps:**
- Search our network for files with the .wncry extension to find any encrypted drives that must be recovered from back ups
- Configure your SIEM or IDS to look for SMB scanning of port 445 in volume. This will also help to determine if your organization was attacked

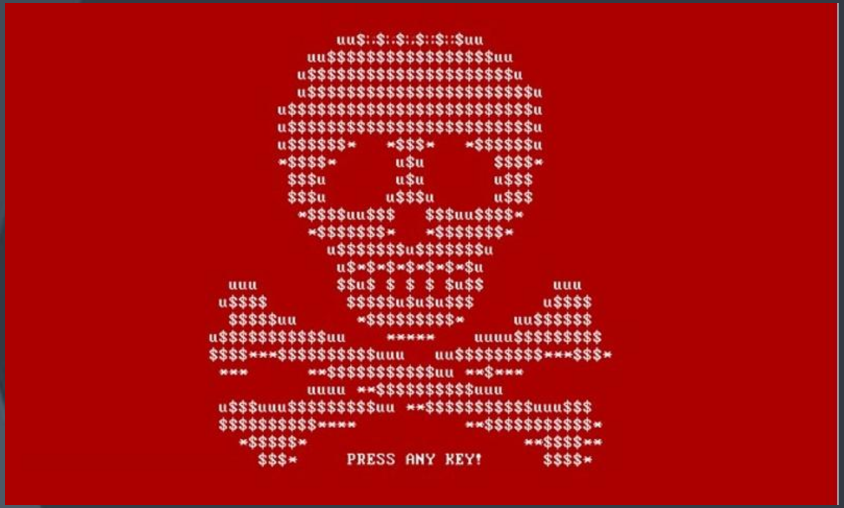
How does a company protect/mitigate the risk

- **Best Practices to Reduce Risk:**
- Implement an ongoing vulnerability management process cycle to identify, prioritize and remediate vulnerabilities, including system configuration, as a cornerstone of your Security Program
- Segment your networks to stop the spread of infections.
- Assess data protection, back-up and restoration to ensure that if your data becomes compromised or corrupted, it is easily recoverable. This attack, at a data level, is responded to just like a massive data corruption issue.
- Follow a standard framework or guideline such as the CIS Critical Security Controls. They are basic to network hygiene.

What implications does this have for our security program

- This should be used as a teaching tool to implement process rigor and heighten the importance of detection and response. In this case unless prevention was 100% flawlessly executed, organizations were affected. Security programs require focus on all of prevention, detection and response, as well as people, processes and technology. There is no one vendor solution that can plan for outbreaks like this.

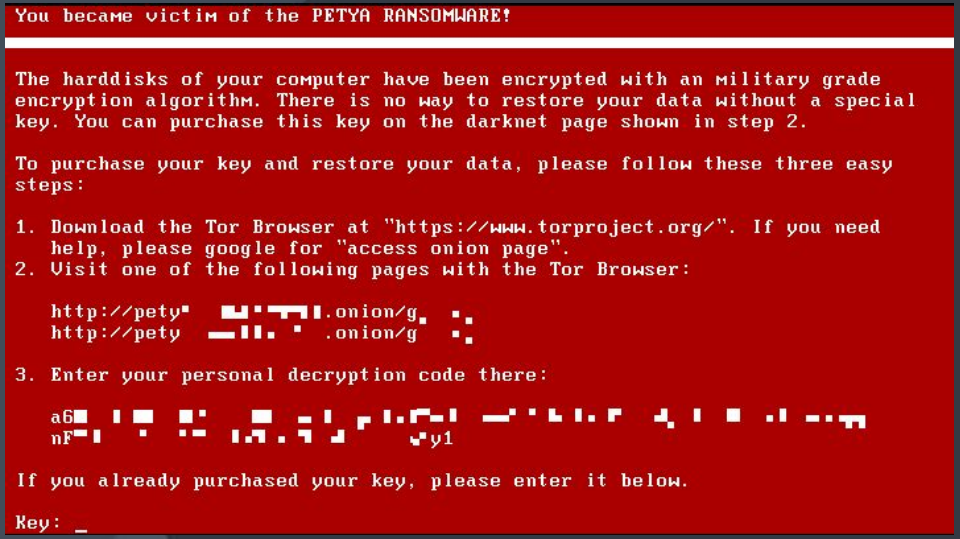
Petya virus



PRESS ANY KEY!

ASCII art of a skull and crossbones is displayed as part of the payload on the original version of Petya

Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system.



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://pety[redacted].onion/g[redacted]
   http://pety[redacted].onion/g[redacted]

3. Enter your personal decryption code there:

   a6[redacted]
   nF[redacted]y1

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

Key: _
```

Info screen of the original version of Petya

On 27 June 2017, a major global cyberattack began (Ukrainian companies were among the first to state they were being attacked), utilizing a new variant of Petya. On that day, Kaspersky Lab reported infections in France, Germany, Italy, Poland, the United Kingdom, and the United States, but that the majority of infections targeted Russia and Ukraine, where more than 80 companies initially were attacked, including the National Bank of Ukraine. Also during the attack initiated on 27 June 2017, the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline. Several Ukrainian ministries, banks and metro systems were also affected.