HIGHGATE
SYSTEMS

PETYA RANSOMWARE OUTBREAK

Many organizations in Europe and the US have been crippled by a ransomware attack known as "Petya". The malicious software has spread through large firms including the advertiser WPP, food company Mondelez, French construction materials company Saint-Gobain and Russian steel and oil firms Evraz and Rosneft, legal firm DLA Piper, Danish shipping and transport firm Maersk and now targeting government and financial institutions, leading to PCs and data being locked up and held for ransom.

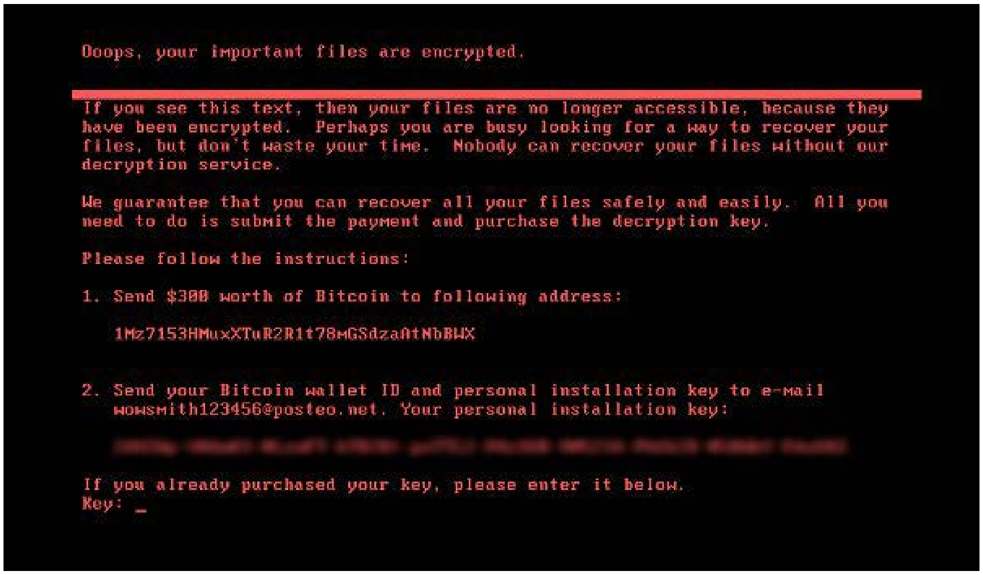
It's the second major global ransomware attack in the past two months. In early May, Britain's National Health Service (NHS) was among the organizations infected by WannaCry, which used a vulnerability first revealed to the public as part of a leaked stash of NSA-related documents released online in April by a hacker group calling itself the Shadow Brokers.

Petya has been in existence since 2016. A new strain of the Petya ransomware started propagating on June 27, 2017. It differs from typical ransomware as it doesn't just encrypt files, it also overwrites and encrypts the master boot record (MBR).

The ***MEDoc accounting software*** is used to drop and install Petya into organizations' networks. Once in the network it uses two methods to spread.

One of the ways in which Petya propagates itself is by exploiting the MS17-010 vulnerability, also known as ***EternalBlue***. It also spreads by acquiring user names and passwords and spreading across network shares. Petya is primarily impacting organizations in Europe.

Latest outbreak attack recorded, asks for 300Bitcoins which is equal to US $75000/- to provide the decryption key.



```
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:

   [redacted]

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

MICROSOFT PATCH

Microsoft has released its update patch in order to combat the Petya outburst, link is as follows.
http://www.catalog.update.microsoft.com/Search.aspx?q=MS17-010

Author of Original Petya Ransomware Publishes MASTER DECRYPTION KEY

The author of the original Petya ransomware — a person/group going by the name of Janus Cybercrime Solutions — has released the master decryption key of all past Petya versions.

This key can decrypt all ransomware families’ part of the Petya family except NotPetya.
“Here is our secp192k1 privatekey: **38dd46801ce61883433048d6d8c6ab8be18654a2695b4723**
We used ECIES (with AES-256-ECB) Scheme to encrypt the decryption password into the "Personal Code" which is BASE58 encoded”

BEST PRACTICES TO AVOID PETYA

- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world.
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.
- If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.
- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

Disclaimer: The above article presents a set of best practices but is not intended to be a replacement to any other professional advice, tool or recommendations provided by your technical department and makes no claims to its effectiveness.