Executive Summary

Once again, a ransomware attack, dubbed "Petya-like", has been launched against weary organizations trying to keep up with their patch management processes.

Like WannaCry, "Petya-like's" goal is to encrypt, but instead of encrypting exfiltrated payload, the attack attempts to overwrite the Master Boot Record for encrypting the device's Master File Table. Essentially, "Petya-like" is a device-level denial-of-service attack where the victim will have to pay a ransom to recover their file table and device resources.

"Petya-like" takes advantage of leaked exploits, like WannaCry, using strong encryption and a modular architecture. Petya-like's initial vector was a Word document (according to Ukrainian resources), and its spread mechanism is through either one of the leaked NSA exploits, or the use of PsExec with administrative credentials.

This document provides an overview of the "Petya-like" attack.

Table of Contents:

- The "Petya-like" Ransomware Attack Biopsy 4
- Attack Flowchart 6
- Summary and What To Do Now 13
The "Petya-like" Ransomware Attack Biopsy

1. The original entrance vector to the organization was an MS-WORD document (according to online data regarding this attack), but this can, and will, change to any one of many initial attack vectors.

2. The malware will attempt to spread in the organization using the following methods:
   
   a. The NSA exploits that were provided by ShadowBrokers a few months ago will allow the malware to propagate to other EPs in the local Network.

   b. If the entry-point EP user has admin privileges (on their EP or on any other EP), then LSASS will be scanned for relevant tokens, which will allow it to propagate into other EPs. With the relevant token, it will access Target_EP_IP and write the malicious DLL to the target-EPs admin$ share. A service will be created remotely on the target-EP, which will execute the malware (using rundll32.exe).

3. Per-EP malware potential damage. Overwrite the Master Boot Record (MBR), then encrypt sensitive user files.

The above means:

1. That even if an organization downloads the latest Microsoft patches to protect against NSA leaked exploits, the malware will still try and may succeed to penetrate EPs by using method 2.b above.

2. That it only takes a single vulnerable EP (to the above mentioned vectors) in an organization to allow the malware to damage the entire environment.
Petya's initial vector was MS-Word (according to Ukrainian sources). Its spread mechanism is through either one of the NSA exploits, or using PsExec with administrative credentials.

The initial DLL is loaded using Rundll32.exe, with the command-line arguments in the following structure: Rundll32.exe petyawrap.dll #1 60 [Note that the argument 60 is optional]

At first, the binary checks for the existence of C:\Windows\<dll name>. If this exists, the DLL will not proceed. Otherwise, execution proceeds as normal:
Creating a dummy file (e.g. "perfc") will not help as the attackers are easily capable (using the same variant) of rendering this defense ineffective.

Example of the malware’s action when the file exists:

(Notice: the file’s name is 'petyawrap,' not "perfc").

The ransomware now overwrites the MBR with its own code:

Uses a named pipe for inter-process communication. (As we will see later one of the binaries is given this named pipe’s full-path as a commandline argument):

A scheduled task is created to restart the endpoint after one hour:
Network adapters are enumerated, netbios attempts (port 139) to retrieve the remote endpoint’s computer-name are made, along with probing for SMB (port 445) - in order to expand using exploits leaked from the NSA:

This binary is a tool used to read LSASS.exe’s memory and attain administrative privileges.

The process extracts PsExec (names it “dllhost.dat”) to the local machine from its resources:
The final line in this image shows the “CreateThread” method used to invoke the attempt to infect other machines by writing the malicious DLL to `\<ENDPOINT-IP>\admin$\<dllname>`. `admin$` is a known share in windows environments for administrators. This thread also attempts to execute the malicious code as a service using the administrative privileges it acquired from reading LSASS.exe’s memory:

Using PsExec to execute on a remote machine:

Lastly, find the logical drives to encrypt (filesystem drives):

```
The encryption process:

The following is a list of file extensions that will be encrypted by this malware:

- 3ds
- .7z
- .accdb
- .ai
- .asp
- .aspx
- .avhd
- .back
- .bak
- .c
- .cfg
- .conf
- .cpp
- .cs
- .ctl
- .dbf
- .disk
- .djvu
- .doc
- .docx
- .dwg
- .eml
- .fdb
- .gz
- .h
- .hdd
- .kdbx
- .mail
- .mdb
- .msg
- .nrg
- .ora
- .ost
- .ova
- .ovf
- .pdf
- .php
- .pmf
- .ppt
- .pptx
- .pst
- .pvi
- .py
- .pyc
- .rar
- .rtf
- .sln
- .sql
- .tar
- .vbox
- .vbs
- .vcb
- .vdi
- .vfd
- .vmc
- .vmdk
- .vmsd
- .vmx
- .vsdx
- .vsv
- .work
- .xls
- .x
- .cfg

Once one hour passes, the scheduled task should initiate a shutdown process to the machine and the disk encryption initiates:

Repairing file system on C:

The type of the file system is NTFS.

One of your disks contains errors and needs to be repaired. This process may take several hours to complete. It is strongly recommended to let it complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!

CHRESDK is repairing sector 22016 of 248000 (0%)

NYOTRON
Securing the world
Once the MFT encryption process completes it presents the user with the following screen for the decryption key:

```
Doops, 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:
   1Mz7153HMuWXTuRZ1t7BmG5dzaAIWdBB4w

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
   rMC926-8jkmD7-R6MNW-ww5XH-CtVWQ-rZd1J-s-rUq2o-c5Bx7h-LBv4bM-WhtLeNh

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

A view from the PARANOID Management Environment (PME) that shows that PARANOID successfully prevents the attack:
A view from the machine shows that the malicious process is terminated:

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Start Time</th>
<th>Access</th>
<th>Directory Path</th>
<th>Operation</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Users\App Data\Local\Microsoft\Windows\Explorer\thumbcache_x64.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Users\App Data\Local\Microsoft\Windows\Explorer_thumbcache_32.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Users\App Data\Local\Microsoft\Windows\Explorer\thumbcache_x64.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Users\App Data\Local\Microsoft\Windows\Explorer\thumbcache_32.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Users\App Data\Local\Microsoft\Windows\Explorer\thumbcache_x64.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Users\App Data\Local\Microsoft\Windows\Explorer\thumbcache_32.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Users\App Data\Local\Microsoft\Windows\Explorer\thumbcache_x64.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Users\App Data\Local\Microsoft\Windows\Explorer\thumbcache_32.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Windows\Prefetch\AppLaunch.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Windows\Prefetch\AppLaunch.db</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Windows</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\AppData</td>
<td>1940</td>
<td>SUCCESS</td>
<td></td>
<td>SUCCESS</td>
<td></td>
</tr>
<tr>
<td>C:\Program Files\Nyotron\Logs\Events\2111.6605.0_2017-10-28-2.log</td>
<td>1940</td>
<td>ACCESS DENIED</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Process exits upon failure. No damage is done.
Summary and What To Do Now

Nyotron’s senior security scientists recommend defending against this type of attack by first ensuring that all operating system patches including service packs, hotfixes and special security updates are current.

Nyotron highly recommends selecting a deterministic malware defense system that ignores your patch update status and protects you from damage: data manipulation, encryption, and exfiltration regardless of operating system status.

Threat-agnostic solutions offer protection and near zero exposure to damage. These solutions can quickly identify and stop today's known, known-unknown attacks like the 'Petya-like' ransomware, and the more dangerous unknown-unknown attacks expected in the days ahead.

About Nyotron

Nyotron is a privately held cybersecurity company that has developed a disruptive Threat-Agnostic Defense™ technology to cope with the biggest challenge of today’s digital era - the unknown threat. PARANOID is designed to prevent targeted and advanced national-level cyber-attacks on high-profile enterprises, and it does so without any previous knowledge about the threat or its methodologies. Based on a unique last-line-of-defense approach, the company’s technology is designed to protect enterprise data and critical assets by mitigating threats that are able to outsmart all security layers. Nyotron’s customer base includes all major industries.