CERT-UA

Archived: 2026-04-05 20:32:46 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA досліджено кібератаку угрупування UAC-0063, здійснену 08.07.2024 по відношенню до однієї з українських науково-дослідних установ з використанням шкідливих програм HATVIBE та CHERRYSPY.

На етапі первинного ураження зловмисник, маючи доступ до облікового запису електронної пошти співробітника установи, здійснив відправку копії нещодавно відправленого листа десяткам адресатів (включаючи самого відправника), замінивши оригінальний документ-вкладення іншим документом, в який було вбудовано макрос.

У випадку відкриття DOCX-документу та активації макросу на ЕОМ буде створено та відкрито ще один документ (DOC) з макросом, який, у свою чергу, забезпечить створення на ЕОМ закодованого HTA-файлу шкідливої програми HATVIBE "RecordsService", а також, файлу запланованого завдання "C:\Windows\System32\Tasks\vManage\StandaloneService", призначеного для запуску останньої.

Використовуючи створену технічну можливість прихованого віддаленого управління ЕОМ, на комп'ютер в каталог "C:\ProgramData\Python" згодом завантажено Python-інтерпретатор та файл шкідливої програми CHERRYSPY, який, на відміну від попередньої версії, обфускованої за допомогою pyArmor, скомпільовано в .pyd (DLL) файл.

Зазначимо, що активність, яка відстежується за ідентифікатором UAC-0063, з середнім рівнем впевненості асоційовано з діяльністю угрупування APT28 (UAC-0001), яке має безпосереднє відношення до ГУ ГШ ЗС РФ. При цьому, на Virustotal виявлено DOCX-документ (MD5: 33c3e4599ad678133905e6c1589c12d2) з аналогічним макросом, який було завантажено з Вірменії 16.07.2024, контент-приманка якого містить (спотворений) текст, адресований Управлінню оборонної політики Міністерства оборони Республіки Вірменія від імені Управління міжнародного військового співробітництва Міністерства оборони Киргизької Республіки.

Слід додати, що в червні 2024 року зафіксовано числені випадки встановлення бекдору HATVIBE шляхом експлуатації вразливості (вірогідно, CVE-2024-23692) в програмному продукті HFS HTTP File Server (https://www.rejetto.com/hfs/), що свідчить про застосування угрупуванням UAC-0063 різних векторів первинної компрометації.

Реалізація кібератаки стала можливою у зв'язку з систематичним нехтуванням організацією типовими для поточного ландшафту кіберзагроз рекомендаціями, зокрема:

- відсутність двохфакторної автентифікації для облікових записів електронної пошти;
- членство облікового запису користувача в групі "Administrators";

- відсутність політик для блокування можливості запуску макросів, mshta.exe, а також інших програм (зокрема, інтерпретатору Python).

Кожен керівник та системний адміністратор (адміністратор безпеки), який допускає кібератаки, засоби, тактики, техніки і процедури реалізації яких неодноразово публічно описані, сприяє досягенню ворогом поставлених цілей.

Індикатори кіберзагроз

Файли:

```
197e86b76a41f154b64e092f7cc3b306    6c439e62fb404e9095392878ef32ffce18ce6155a1510f4005409243401e8caf
81cdcda59c86f8aa636810e4a085d673    f9baa77117f5a058461e859efc67c8ce1ac205d1536326e01a030ab22295af5b
7a2a8c002a5e22c6231885e1ccf82bd1    593ca6d639f7c3e99db768b318b765e7585496debfde553dc1df03f5894012e3
7f865b65a82dcb18385644e0fd894727    259619899c60aa46df4f83558606813c79927c141bbf4b21bbf07b21b40e7ac1
33c3e4599ad678133905e6c1589c12d2    e6daa00e095948acfc176d71c5bf667a0403e5259653ea5ac8950aee13180ae0
d618720afd0ee49601f7933c414ffbb5    bcdbe035001af9d2cc173e975fa0b13b133e613b7d9b6e90df86672f9057e19b
8e1b29046c7f5bd1ddd4f549e2555592    f4ada2b858c84da8b53c08ce4579f8b5b5df25e0d0f17ee0b48e10c87c338d23
d84043b72bdceb92b2d60c2725bd674f    93322be0785556e627d2b09832c18e39c115e6a6fbff64b1e590e1ddcf8f6a43
34ced721349626ce81c11693b9243c19    a171e9c413518750806ae094e32f15791d4193229cc598642760af536cf6551d
d0c3b49e788600ff3967f784eb5de973    332d9db35daa83c5ad226b9bf50e992713bc6a69c9ecd52a1223b81e992bc725
8159abd281783e0ae601afce3b7d23b1    48a30083f115ca0d359afc175cf942367207a73fdda28778e2b264534cf21830
```

Мережеві:

```
hXXp://trust-certificate[.]net/setup.php
hXXp://trust-certificate[.]net/tmp/379.zip
hXXps://enrollmentdm[.]com:443
trust-certificate[.]net   2024-07-09  @namecheap.com
enrollmentdm[.]com    2024-05-13  @namecheap.com
185.158.248[.]198 RO  @m247.com
193.124.65[.]97   RU  @mtw.ru
45.136.198[.]184
5.45.70[.]178
hXXp://45.136.198[.]184/connect.php
hXXp://45.136.198[.]184/input.php
hXXp://45.136.198[.]184/output.php
hXXp://5.45.70[.]178/RemoteAssistanceSvc.hta
```

```
http://trust-certificate.net/setup.php
http://trust-certificate.net/tmp/379.zip
https://enrollmentdm.com:443
trust-certificate.net  2024-07-09 @namecheap.com
enrollmentdm.com  2024-05-13 @namecheap.com
185.158.248.198 RO @m247.com
```

```
193.124.65.97  RU @mtw.ru
45.136.198.184
5.45.70.178
http://45.136.198.184/connect.php
http://45.136.198.184/input.php
http://45.136.198.184/output.php
http://5.45.70.178/RemoteAssistanceSvc.hta
```

Хостові:

```
%TMP%\punkt-1-07-10-24-na-zasid.doc.doc
%TMP%\punkt-1-07-10-24-na-zasid.docx.doc
%PROGRAMDATA%\Python\DLLs
%PROGRAMDATA%\Python\Lib
%PROGRAMDATA%\Python\Scripts
%PROGRAMDATA%\Python\include
%PROGRAMDATA%\Python\pip_update.cp37-win32.pyd
%PROGRAMDATA%\Python\pip_update.pyd
%PROGRAMDATA%\Python\python.exe
%PROGRAMDATA%\Python\pythonw.exe
%PROGRAMDATA%\Python\pythonw.exe -m pip_update.pyd 20 30
%PROGRAMDATA%\scripts
%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\0Q0UYOEK\379[1].zip
%LOCALAPPDATA%\records\RecordsService
C:\HFS\RemoteAssistanceSvc.hta
C:\temp\AccessProtection.hta
C:\temp\RemoteAssistanceSvc.hta
C:\Windows\System32\Tasks\Python\UpdateService
C:\Windows\System32\Tasks\vManage\StandaloneService
\Python\UpdateService
\vManage\StandaloneService
C:\Windows\System32\mshta.exe %LOCALAPPDATA%\records\RecordsService
```

Графічні зображення

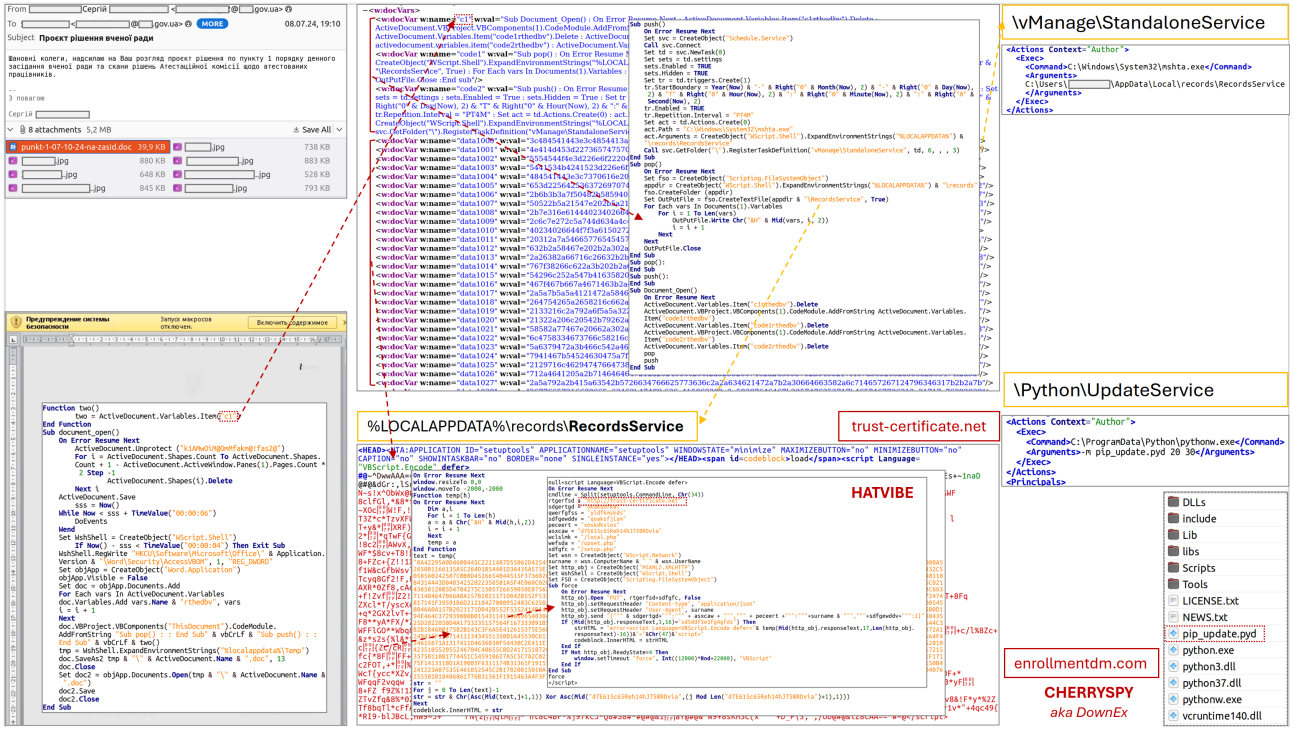
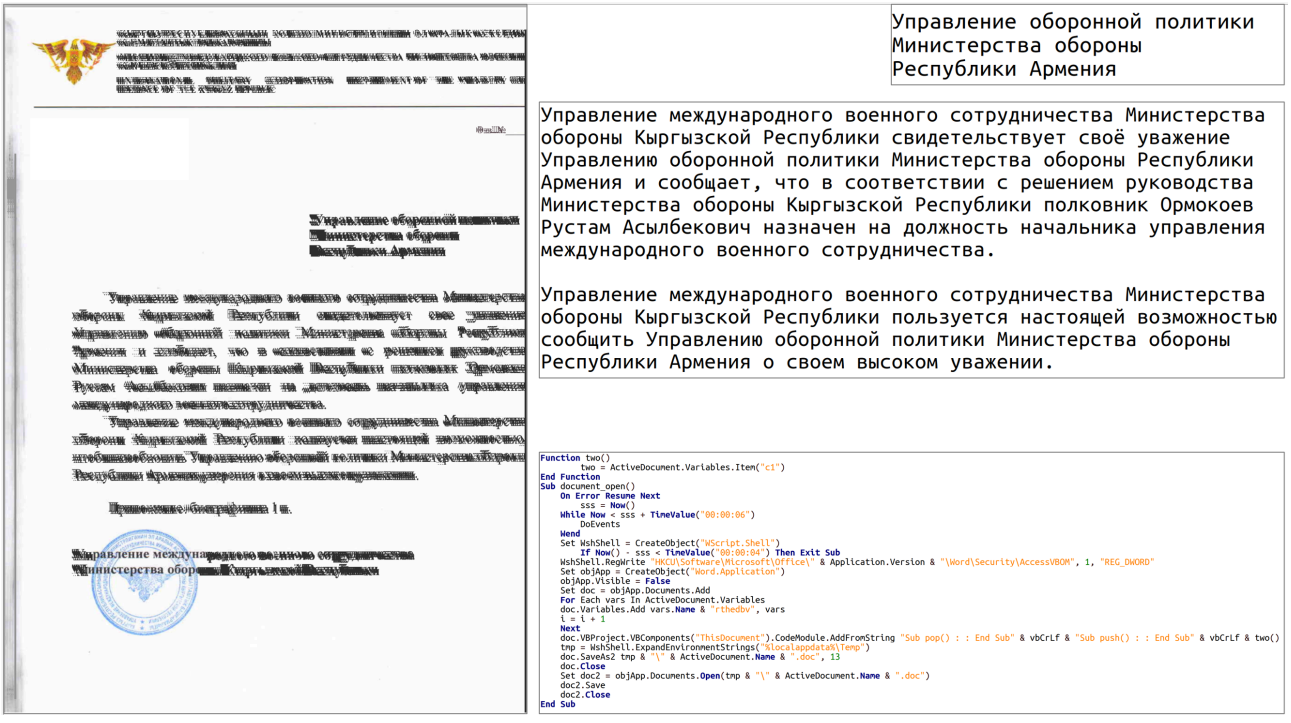


Рис.1 Ланцюг ураження



Управление оборонной политики
Министерства обороны
Республики Армения

Управление международного военного сотрудничества Министерства обороны Кыргызской Республики свидетельствует своё уважение Управлению оборонной политики Министерства обороны Республики Армения и сообщает, что в соответствии с решением руководства Министерства обороны Кыргызской Республики полковник Ормокоев Рустам Асылбекович назначен на должность начальника управления международного военного сотрудничества.

Управление международного военного сотрудничества Министерства обороны Кыргызской Республики пользуется настоящей возможностью сообщить Управлению оборонной политики Министерства обороны Республики Армения о своем высоком уважении.

Рис.2 Приклад вмісту документу, використаного для атаки на Міністерство оборони Вірменії

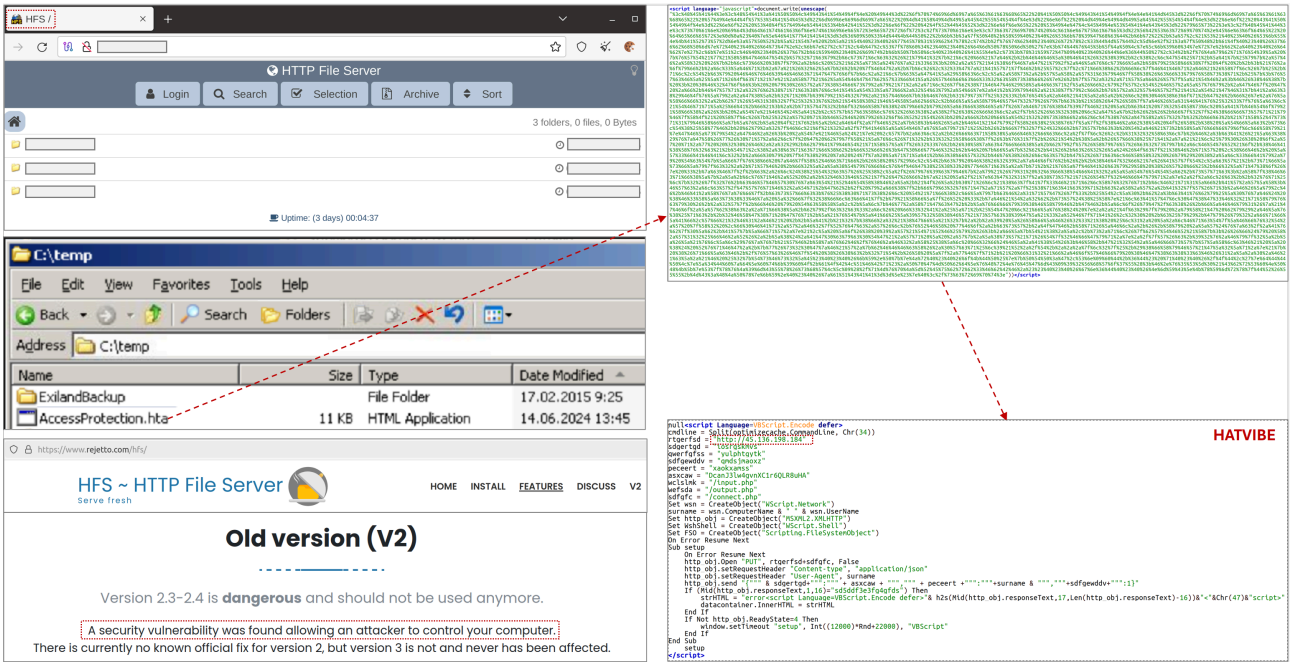


Рис.3 Приклад ураження ЕОМ з вразливою версією HFS

Source: https://cert.gov.ua/article/6280129