CERT-UA

Archived: 2026-04-05 14:00:30 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, керуючись пп.1 п.2 ст.8 Закону України "Про основні засади забезпечення кібербезпеки України", вжито заходів з виявлення та реагування на кібератаку в інформаційно-комунікаційній системі одного з державних органів України.

З'ясовано, що 18.04.2023 та 20.04.2023 на електронну адресу відомства начебто з офіційної поштової скриньки Посольства Таджикистану в Україні (вірогідно, в результаті компрометації останньої) надіслано електронні листи, перший з яких містив додаток у вигляді документу з макросом, а другий - посилання на той самий документ.

У випадку завантаження документу та активації макросу на ЕОМ буде створено та відкрито DOCX-файл "SvcRestartTaskLogon", який також містить макрос, що забезпечить створення ще одного файлу з макросом "WsSwapAssessmentTask". Призначенням останнього є створення файлу "SoftwareProtectionPlatform", що класифіковано як HATVIBE, а також запланованого завдання для його запуску. HATVIBE представлено у вигляді кодованого VBScript-файлу (VBE), який функціонально забезпечує можливість завантаження та запуску інших файлів.

В процесі комп'ютерно-технічого дослідження визначено, що 25.04.2023 за невстановлених обставин (вірогідно, за допомогою HATVIBE) на ЕОМ створено додаткові програми: кейлогер LOGPIE (забезпечує збереження у файл значень натискань на клавіатуру та вмісту буферу обміну) та бекдор CHERRYSPY (забезпечує виконання Python-коду, отриманого з серверу управління). Згадані файли розроблено з використанням мови програмування Python та захищено за допомогою утиліти PyArmor. При цьому модуль "pytransform", в якому реалізовано механізми шифрування та обфускації коду, додатково захищено за допомогою Themida. Слід додати, що для пошуку та ексфільтрації файлів, в тому числі результатів роботи кейлогеру LOGPIE (розширення файлу: ".~tmp"), використовується шкідлива програма STILLARCH (приклад розширень файлів: ".doc",".docx",".rtf",".xlsx",".xls",".pdf",".ppt",".pptx",".~tm",".bmp",".rar",".jpg",".odt",".p12",".heic",".enc",".jpeg",".tiff",".tif",".zip",".crf",".enc",".cr",

Додаткове вивчення інфраструктури та пов'язаних файлів дозволили зробити висновок про те, що серед об'єктів заінтересованості групи є організації з Монголії, Казахстану, Киргизстану, Ізраїлю, Індії.

Зауважимо, що згадана активність здійснюється з метою шпигунства та відстежується з 2021 року за ідентифікатором UAC-0063.

З метою зменшення поверхні атаки рекомендуємо для облікових записів користувачів обмежити можливіть виконання "mshta.exe", запуску Windows Script Host ("wscript.exe", "cscript.exe") та інтерпретатору Python.

Індикатори кіберзагроз

Файли:

36379daf7ee88e10a395958cacf6f7c0	fdc59293e2ed95e72e11d627c733a7e4234f1b428737147c6ee34f02d92a92eb	SvcRe
482406314bdb06a44fcdd53f67ddcaf1	1d2cfdafdf0ab4a2f17befb94c3b84ff24b96a18fb4ab8d69f225407f7d38952	WsSwa
10cab7f70c3b094f2d47e425e42a6013	9e2dfe15eae41295f59b1d4775f37aa0c5bb5e43883903ff07b803865b1ae33e	Softw
5f2d5eb1c13bf0aeaddc1986f44a2444	c517b4e59f1998fdd05dd00b08dfbbdb98f961a6466aa84b7fcafec26b2bbfe2	slmgr
e9076cc28cfeb8912c844b2fddad0066	ab4f206a4b383dba4e6c659404561a50c31d4b771ec23e57b242cadbb7df88ae	WinTi
ccc4c2174641daab7a623535869df715	afbf4a1ada282a9bf85d8f390df304e4506646627ee4837710291b526eb31840	pytra
774606fd7c7fe7e2bdfe4fc190c7472f	5429935c3446dd1eda1930af9d249e5b0a1e6193c67e000ab072ffeb9db23f66	help.p
5ffd5424cda3878ea3974ec91a0b6920	e0a59595fbfe3f9465c265888ee6a42039d0fea3838b467b2f9c4d4a7c0f0401	pytra
89f15568bc19cc38caa8fd7efca977af	d2005b2b3a6bfe22477fb9ad965c0473fc525602333f939eb5db17878e31d078	Diags
c273cdfcfd808efa49ec0ed4f1c976e0	d2a0e6e5bdd66332fca965dad6126c1d6ef956e3782c431f1f41e99f45926331	diags
70e4305af8b00d04d95fba1f9ade222d	75395359af2d61b2434d68fbee12ebc9947c4d113ca8363dd060caab76077474	Diags
14a8aad94b915831fc1d3a8e7e00a5df	70d8e503fd199de816815b88e82fe70802955437cdc3785cbd0d34e0343ce5f1	drive
(Історичні дані)		
ea7b4922e6f6a121ba4dbdf5d883f22c	6db96476ce30ebc6218aac12d9c9f814254ac9d10b4bbbc53cdc1df666f4b7a7	BCEM
8c5ba061fec025fd37f1d9ca9029f9ba	d42dfb13b49125aa0ba80482319a1654cafa8a9ee6d63c09c82b3a3ec7fdaee2	BCEM
bac64cabd0f50f34be91e91d41031482	c66cba6b9e4ad7b0178123f379f021622ffda9c9d70fed9a3d00fe041fe501b1	2022-(
6c61cda823e4174113a0f08a3ba7a689	7fe6db9438e5dadfd2b333f77fab14c956d57ddfded2aa58c3b13cad94b16bfa	Тайва

Хостові:

```
%PROGRAMDATA%\scripts\SoftwareProtectionPlatform
%PROGRAMDATA%\scripts\WsSwapAssessmentTask
%PROGRAMDATA%\scripts\SvcRestartTaskLogon
%PROGRAMDATA%\Drivers\slmgr.vbe
%WINDIR%\System32\Tasks\drivers\slmgr
%WINDIR%\System32\Tasks\Management\WManSvc
%WINDIR%\System32\Tasks\Application\SynchronizeTime
%WINDIR%\System32\Tasks\SoftwareProtectionPlatform
%WINDIR%\System32\mshta.exe %PROGRAMDATA%\scripts\SoftwareProtectionPlatform
%PROGRAMDATA%\Temp\load
%PROGRAMDATA%\Python\Tools\scripts\
%PROGRAMDATA%\Python\pythonw.exe %PROGRAMDATA%\Python\Tools\scripts\help.py 10 20
%PROGRAMDATA%\Python\pythonw.exe %LOCALAPPDATA%\Diagnostics\%SID%\1dbe1327-516b-f17a-3977-5v54adb8642b\WinTim
%PROGRAMDATA%\Python\Tools\scripts\help.py
%PROGRAMDATA%\Python\Tools\scripts\pytransform.pyd
%LOCALAPPDATA%\Diagnostics\%SID%\1dbe1327-516b-f17a-3977-5v54adb8642b\WinTime.py
%LOCALAPPDATA%\Diagnostics\%SID%\1dbe1327-516b-f17a-3977-5v54adb8642b\pytransform.pyd
%LOCALAPPDATA%\Diagnostics\%SID%\1cbe6654-466b-4d53-8303-2e86ab6db8a7\
```

Мережеві:

```
hxxp://206.166.251[.]216/connect.php
hxxp://84.32.188[.]123/hftqlbgtg.php
hxxps://diagnostic-resolver[.]com/
hxxps://ms-webdav-miniredir[.]com/getdata.php
hxxps://ms-webdav-miniredir[.]com/takeanwser.php
hxxps://ms-webdav-miniredir[.]com/connection.php
206.166.251[.]216 (@blnwx[.]com; NL)
185.203.117[.]6 (@vpsag[.]com; BG)
79.124.60[.]180 (@4vendeta[.]com; BG)
84.32.188[.]123 (@cherryservers[.]com; NL)
172.104.62[.]59 (@linode[.]com; SG)
diagnostic-resolver[.]com (@namecheap[.]com; 2023-01-13)
net-certificate[.]services (@namecheap[.]com; 2022-01-28)
ms-webdav-miniredir[.]com (@namecheap[.]com; 2023-03-09)
```

Графічні зображення

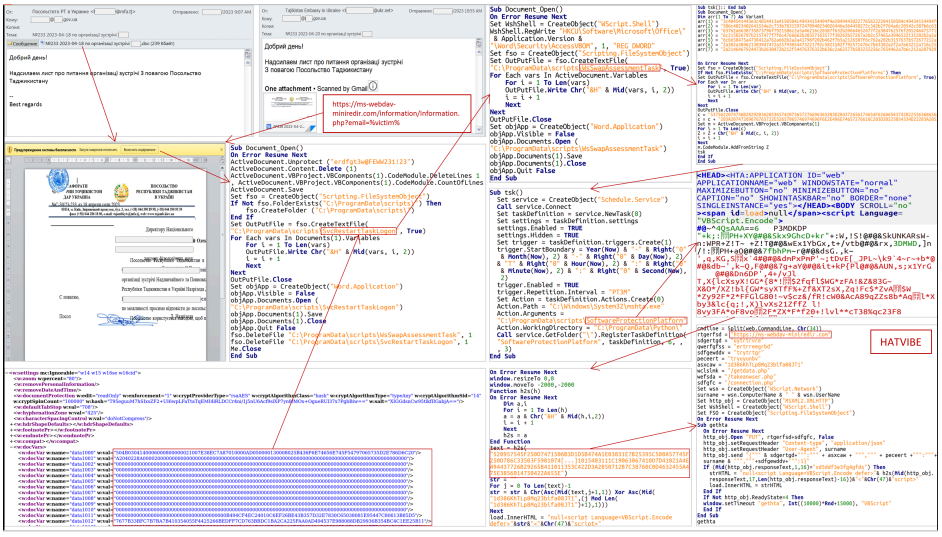

Рис.1 Приклад ланцюга первинного ураження

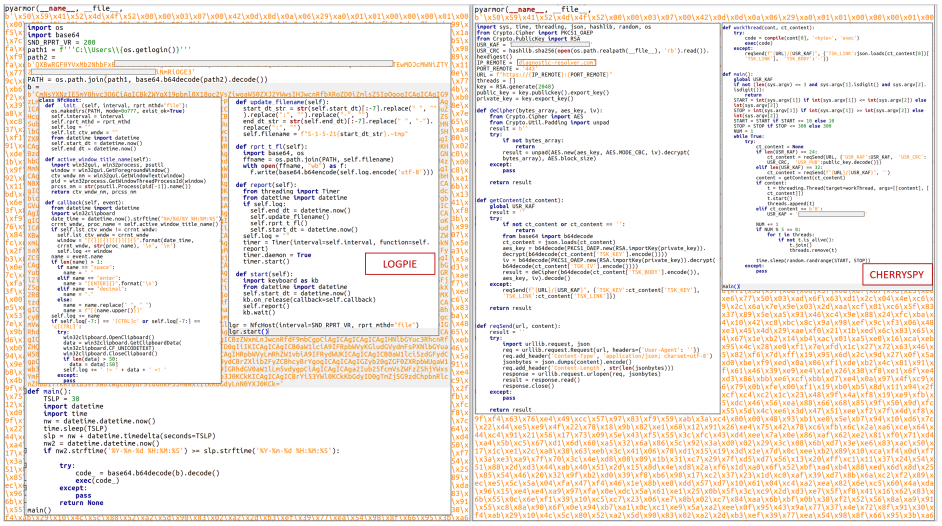

Рис.2 Приклад вихідного коду LOGPIE та CHERRYSPY

Посилання

[1] https://www.bitdefender.com/blog/businessinsights/deep-dive-into-downex-espionage-operation-in-central-asia/
