CERT-UA

Archived: 2026-04-05 15:16:33 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, починаючи з лютого 2025 року, відстежується цільова активність, яка здійснюється з метою шпигунства у відношенні осередків розвитку інновацій у військовій сфері, військових формувань, правоохоронних органів України та органів місцевого самоврядування, особливо тих, що розташовані вздовж східного кордону країни.

Первинна компрометація забезпечується шляхом розповсюдження електронних листів із вкладеннями у вигляді XLS-документів з макросами (розширення ".xlsm"), назви/теми яких можуть стосуватися питань розмінування території, адміністративних штрафів, виробництва БПЛА, компенсації за зруйноване майно тощо. При цьому, "корисне навантаження" представлене у вигляді base64-кодованих рядків, що зберігаються в клітинках Excel-таблиці. Згаданий макрос забезпечує перетворення (декодування) base64-кодованих рядків у виконувані файли, їх збереження на комп'ютер без розширення (!) та подальший запуск.

Станом на квітень 2025 року відомо про два види програмних засобів реалізації кіберзагрози. Перший - .NET-програма, в ресурсах якої зберігається PowerShell-сценарій, що функціонально є reverse-shell'ом, запозиченим з публічного GitHub репозиторію PSSW100AVB. Другий, класифікований як GIFTEDCROOK, C/C++ програма-стілер, що, серед іншого, забезпечує отримання баз даних Інтернет-браузерів Chrome, Edge, Firefox (Cookie, історія, збережені автентифікаційні дані), їх архівування за допомогою PowerShell-командлету Compress-Archive, та подальшу ексфільтрацію до Telegram.

Описаний кластер кіберзагроз відстежується за ідентифікатором UAC-0226.

Завдяки злагодженій роботі суб'єктів кіберзахисту, зокрема, оперативному обміну інформацією, по кожному з аналогічних кіберінцидентів CERT-UA вживаються ефективні заходи реагування. У випадку виявлення ознак здійснення кібератак просимо невідкладно інформувати будь-яким з доступних засобів зв'язку.

Звертаємо увагу, що розсилання електронних листів здійснюється з використанням скомпрометованих облікових записів, в тому числі через вебінтерфейс. У цьому зв'язку системних адміністраторів просимо окремо перевірити наявність, повноту та глибину журналів поштового та вебсерверів.

Індикатори кіберзагроз

Файли:

```
(28.02.2025)
4a2ec9f72b910c0a8e3efc4c334f5bad    f8a31715840852e8ef04016b31f909123f2aa864f3850c45eb511fd1885b4037
e5f4188682e40e79800ccd165289c844    e852d254395ef04308bcde37c3ee9725ab23ca82a202e7d69028c8bee0f0d05f
```

```
1b71d870f34587e0a2717f9925086eab    a2f651d39b8d97221ad36577e9b50beabdf0ad46aec0c29b6cff624e1e2ffd0c
(26.03.2025)
333b09f8865aae5d257b6f11f2fe5d08    a02506468e632875a2c9c9c16e730b8bdc52f7450b28ee7bd8f5ac014b264e53
b3831f0bace886aaba81873edc20aba4    40e68d7240e692ef3301cfaa92a04e0af65f2d725cbfa6711c3154b627fec0f1
100cd9d907e986ba8d5fc6d0488557d9    58b38775f655498b134ce8cd52ab0aba05b710f7611e41cbdffdc3597c5d5f3d
8b694068e5088e0c32739956e28b077e    8427dc6e7da4c163d20c7f188232cf3f83c78ddb6fcad04cec84b33e0f9bdfc0
0a178f76c48c038e8bad03a62b52cfc9    78ea83bfbca85a39e59fa35c8f704873f3fdad3a5278430e75286247530042b8
671b42e854ae2ee3341456fbec7c7787    92183f89b115881535b1bf1985f3ee4b4ebf077bec8cc4de0c6c6e266da0cb87
(02.04.2025)
3394fc2ba0a976818691751aa7f86d05    0a4777725673f9f7114ddceddd80e5a72ad3a4d20fd2014d4c60e2cc1a6cefc2
d280a258704bf9155bceaf4f731988ea    7ca3f2505e1778e6de3927571ba49d27b36447e6c28a60161d55fd2254966bce
daffbfd71f8595ab6d6b8c94cc81a778    24a60e50ed8469fc31afa9abfc361291f72922430cf062bf9c4ac7e6d84b5fad
037e2ca3c97e1a5645cdc45fb0d98064    2930ad9be3fec3ede8f49cecd33505132200d9c0ce67221d0b786739f42db18a
(04.04.2025)
cffdd24742610fe5710dbc9ebd258c64    c8bb0dbc952c9dc2bbc550a300ed033ad5d2416390891ed1e800b08ad3ab5d3a
f62ea2cbd220596072010e91dd65b673    530185fac69e756fb62f23e21e7c0b0828a964b91bbf40f1d04fc2136c1b6dd1
9f6c82c240ba5ef6bb85d28c0cdf7f7f    c27cf714293c496c8fc05b330a57bcfcb6189267e2818062660de88b0f3a25cd
b63b783a9aca15726babd599d2963869    ff1be55fb5bb3b37d2e54adfbe7f4fbba4caa049fad665c8619cf0666090748a
(07.04.2025)
966373dbe28f4111f6ce47038fb343da    8a638a788adb0edb6622b16fd8783bc225470f8ff94b1bba4a94b4d8c105acef
9c03d0da190d1046583ba9fa83a8bcd3    d7a66fd37e282d4722d53d31f7ba8ecdabc2e5f6910ba15290393d9a2f371997
```

Хостові:

```
%PROGRAMDATA%\Microsoft OneDrive Assistant\Microsoft OneDrive Assistant
%PROGRAMDATA%\Windows Service\Windows Service
%PROGRAMDATA%\Windows Telemetry\Windows Telemetry
%PROGRAMDATA%\Microsoft Runtime\Runtime
%PROGRAMDATA%\Svchost\Svchost
%PROGRAMDATA%\Microsoft ServiceHub\ServiceHub
%PROGRAMDATA%\SysAnalyzer\SysAnalyzer
%PROGRAMDATA%\FlashAssistant\FlashAssistant
%TMP%\nmpoyqv5l0ig\
%TMP%\status.zip
powershell -Command Compress-Archive -Path %TMP%\nmpoyqv5l0ig\* -DestinationPath %TMP%\status.zip
```

Мережеві:

```
149[.]102.246.110 (VPN; 2025-02-28 00:00:22+0200 - 2025-02-28 16:10:29+0200)
(tcp)://37[.]120.239.187:6501
37[.]120.239.187 (C2)

(tcp)://89[.]44.9.186:3240
89[.]44.9.186 (C2)
```

```
149.102.246.110
tcp://37.120.239.187:6501
37.120.239.187 (C2)
tcp://89.44.9.186:3240
89.44.9.186 (C2)
```

Графічні зображення

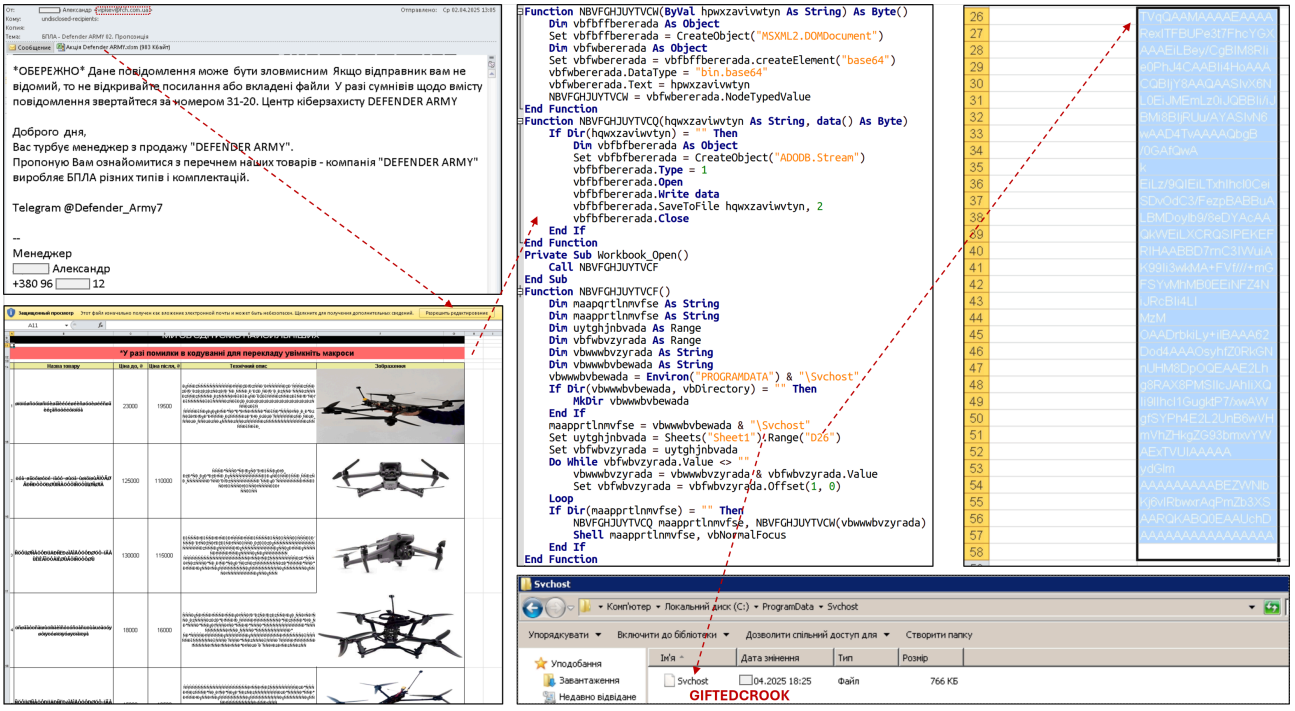

Рис.1 Приклад ланцюга ураження (GIFTEDCROOK)

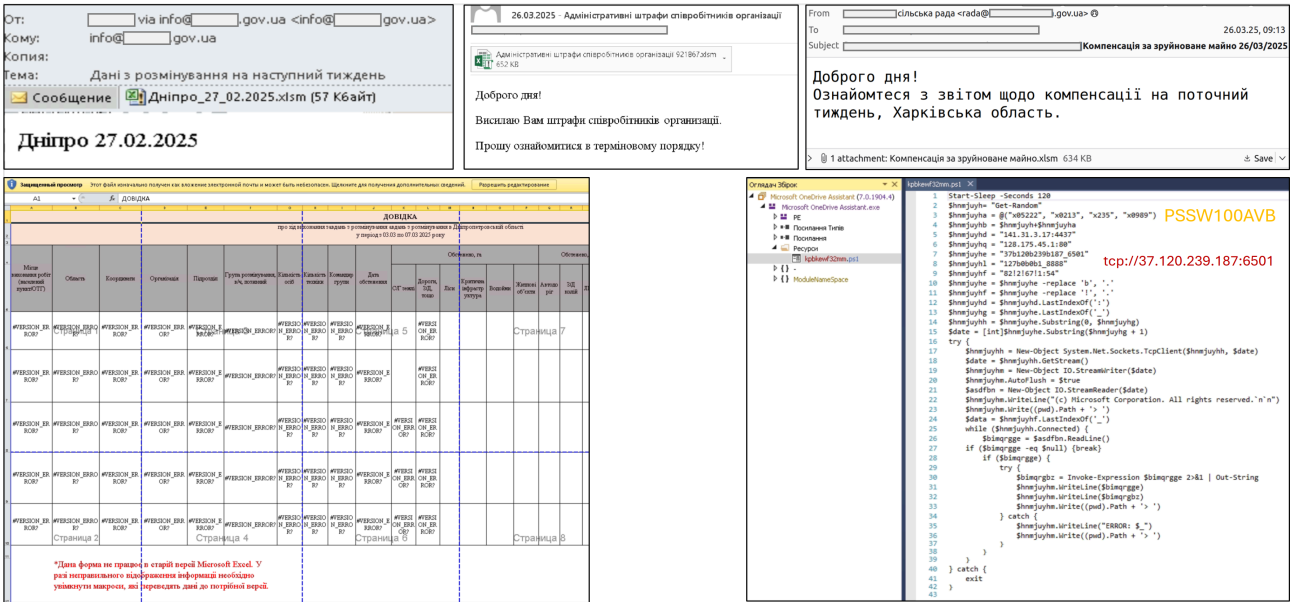

Рис.2 Приклади електронних листів та revers-shell'y

Source: https://cert.gov.ua/article/6282946