CERT-UA

Archived: 2026-04-05 15:10:10 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA у взаємодії з Центром кібернетичної безпеки інформаційно-телекомунікаційних систем військової частини А0334 (ЦКБ ІТС в/ч А0334) вжито заходів з дослідження цілеспрямованої кібератаки, що полягала у спробі ураження шкідливим програмним забезпеченням ЕОМ представників Сил оборони України.

Так, 22.02.2024 невстановленою особою за допомогою месенджеру Signal серед декількох військовослужбовців розповсюджено XLS-документ "1_ф_5.39-2024.xlsm" з повідомленням про, нібито, проблеми з формуванням звітності. Окрім легітимного макросу, згаданий документ містив додатковий програмний VBA-код, який забезпечував запуск PowerShell-команди, призначеної для завантаження, декодування та виконання PowerShell-сценарію "mob2002.data".

Завантажений з Github PowerShell-скрипт здійснює модифікацію реєстру операційної системи, зокрема:

- запис основного пейлоаду в base64-кодованому вигляді в гілку "HKEY_CURRENT_USER\SOFTWARE\Microsoft\XboxCache" (значення: "db1".."db27")
- запис декодеру-лаунчеру в base64-кодованому вигляді в гілку "HKEY_CURRENT_USER\SOFTWARE \Microsoft\XboxCache" (значення: "db")
- створення ключа 'xbox' в гілці автозапуску 'Run' зі значенням у вигляді PowerShell-команди "cmd /c start /min "" powershell -windowStyle hidden -c(powershell -windowStyle hidden -enC(gpv -Name 'db' -Path 'HKCU:\SOFTWARE\Microsoft\XboxCache'))", що призначена для запуску декодера, який забезпечить виконання основного пейлоаду

Зазначений вище основний пейлоад, після декодування, містить черговий PowerShell-скрипт, який здійснить GZIP-декомпресію та запуск шкідливої програми COOKBOX.

COOKBOX - PowerShell-сценарій, що реалізує функціонал завантаження та виконання PowerShell-командлетів. Для кожної ураженої ЕОМ обчислюється унікальний ідентифікатор з використанням криптографічних перетворень (хеш-функцій SHA256/MD5) на основі комбінації значень імені комп'ютера та серійного номеру диску, який, під час взаємодії з сервером управління, передається в заголовку "X-Cookie" HTTP-запитів. Персистентність бекдору забезпечується відповідним ключем в гілці Run реєстру операційної системи (ОС), який створюється на етапі первинного ураження стороннім PowerShell-скриптом (в т.ч., COOKBOX deployer'ом). Зазвичай, в програмному коді використовуються елементи обфускації: chr-кодування символів, заміна символів (replace()), base64-перетворення, GZIP-компресія.

Для функціонування інфраструктури серверів управління використовуються сервіси динамічного DNS (наприклад, gotdns.ch, myftp.biz) та Cloudflare Workers.

Описана активність здійснюється, щонайменше, з осені 2023 року, має точковий характер та відстежується за ідентифікатором UAC-0149.

З огляду на типовість тактик, технік та процедур, успішна реалізація описаної загрози можлива у відношенні тих ЕОМ, на яких системними адміністраторами (адміністраторами безпеки) ще й досі не налаштовано елементарні безпекові політики, зокрема, блокування спроб запуску утиліт cmd.exe, powershell.exe, mshta.exe, w(c)script.exe, hh.exe та інших як в цілому, так і за умови, якщо батьківським є процес однієї з програм Microsoft Office (наприклад, EXCEL.EXE).

Зауважимо, що в одному з випадків ураженню ЕОМ вдалося запобігти завдяки завчасно інстальованій типовій для ЗСУ технології захисту (EDR), про необхідність невідкладного встановлення якої було неодноразово наголошено CERT-UA.

Найбільш актуальна та вичерпна інформація щодо порядку захисту ІКС Сил оборони України, в т.ч, стосовно згаданих технологій, може бути отримана в ЦКБ ІТС в/ч А0334.

Індикатори кіберзагроз

Файли:

```
9654451a766b27fb9e678d47094d7dd7    894cd78af8e3ccf3bd19515bb2b60434012fcdaad896d9fde9d49eaa98866eef
32091993b1a864ec259429880d4c2809    5b2cbeec241ea3ce083e2adab5878f8ea982084f9a7674714cd4627f118c182d
0ff0c9228a98dd55a4ab51ade7bfe10e    9309c2833242182b592d253fcb19c15c625425f614bdd614d1ffbb54f5c25f9a
df167cd8a13e75585c5aecb6e57a4326    d80526421527f63d3b7fdf60b980b31871526c905f9d6d0f4f3c1073b42773ba
3d33bcef89039dba97ef243cc193d8a7    1f2057b60a31708fb397c6b27539d8643ae0e8d87cb26cb0256411da14d98c67
f4efa1840c2fb39ebf8d6b1325617b3c    383023689bb2af75da5337ae864dd430086e2d7d7855a65b25f7682c344e082b
a32eebda67c5de1402b539e4ae51a37b    e3b916c2bd7c09a9ecb3737be615b8f4560f1bde495506e3ff67b839a65054b9
6854d326b3756b92708b5658b2a3313a    f0b356b8485b2656da8ae4ecd13b64166da3c446bc0be124aad216b8688aa618
5d9ab0fba328c0fb07f1ee1794c702ef    fd791cae012145402c8fb903fbe29a91f56cd1c0a3e98203241701dc5f456d83
c2a31573662e0b608f8c83016490822c    3293f76da5fa85d4a2b76a0eab30f11e4d61b81e8b4ad14efffa027d8d5f8aee
52ee3c6259c5aa85ece1037f7d76fd73    7bf2288b72775b7dc4b992d17b5dcbc0d6d6a6b1a049c3ec725b1d1f299bb88a
c4055568bcedad91df2ac5616395a823    c630b95cee017b3d2536074ead8278e5415a3e6ff9dc21cd88c59d5d3a11c6dc
ba1f2511fc30423bdbb183fe33f3dd0f    181210f8f9c779c26da1d9b2075bde0127302ee0e3fca38c9a83f5b1dd8e5d3b
```

Хостові:

```
HKEY_CURRENT_USER\Environment\XBoxD
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\'xbox'
HKEY_CURRENT_USER\SOFTWARE\Microsoft\XboxCache
HKEY_CURRENT_USER\SOFTWARE\Microsoft\XboxCache\'db'
cmd /c start /min "" powershell -windowStyle hidden -c(powershell -windowStyle hidden -enC(gpv -Name
C:\Windows\System32\cmd.exe /c start /min "" powershell -windowStyle hidden -c (powershell -windowSt
```

Мережеві:

hXXps://shorturl[.]at/uvcpv
hXXps://github[.]com/kekpelmeshek/testdatasearch/raw/main/mob2002.data
hXXps://raw.githubusercontent[.]com/kekpelmeshek/testdatasearch/main/mob2002.data
hXXp://array.myftp[.]biz
hXXp://bom02.gotdns[.]ch
hXXp://worker-test-6f41.idv64828.workers[.]dev
array.myftp[.]biz
bom02.gotdns[.]ch
worker-test-6f41.idv64828.workers[.]dev
34.199.8.144 (DDNS IP)

Графічні зображення

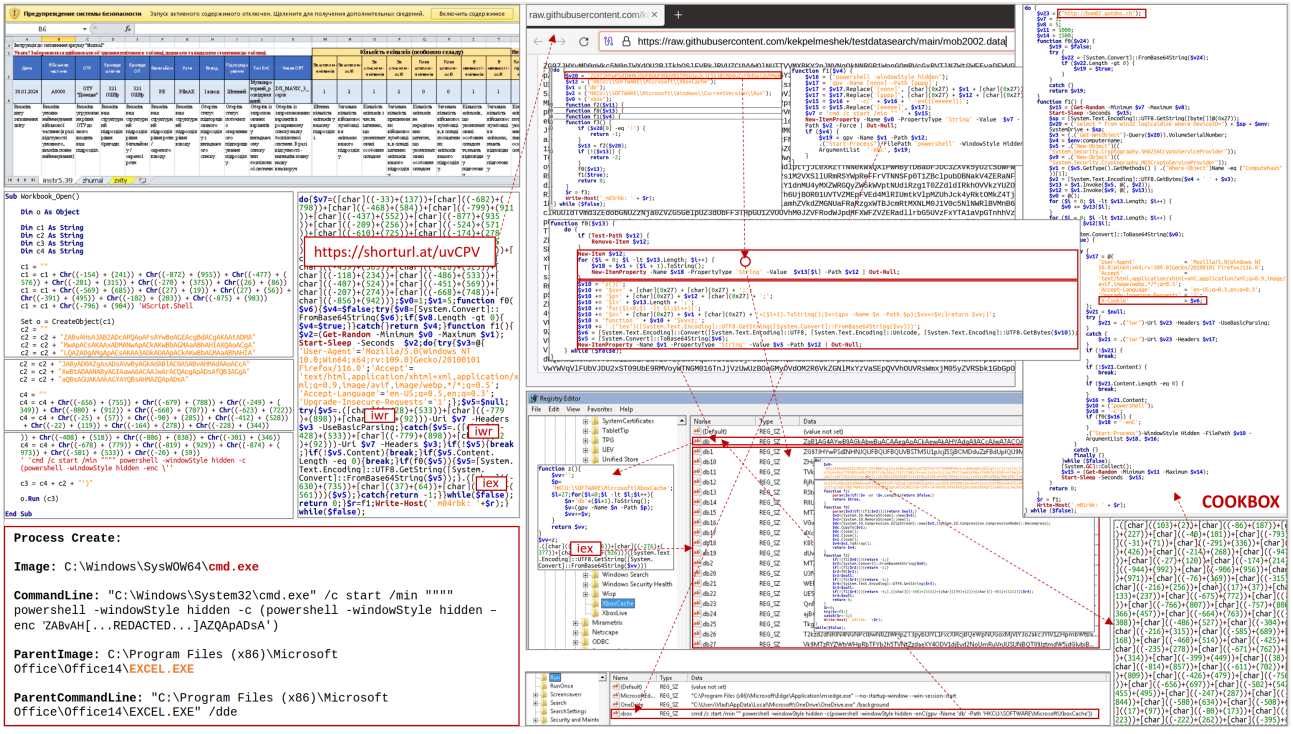

Рис.1 Ланцюг ураження

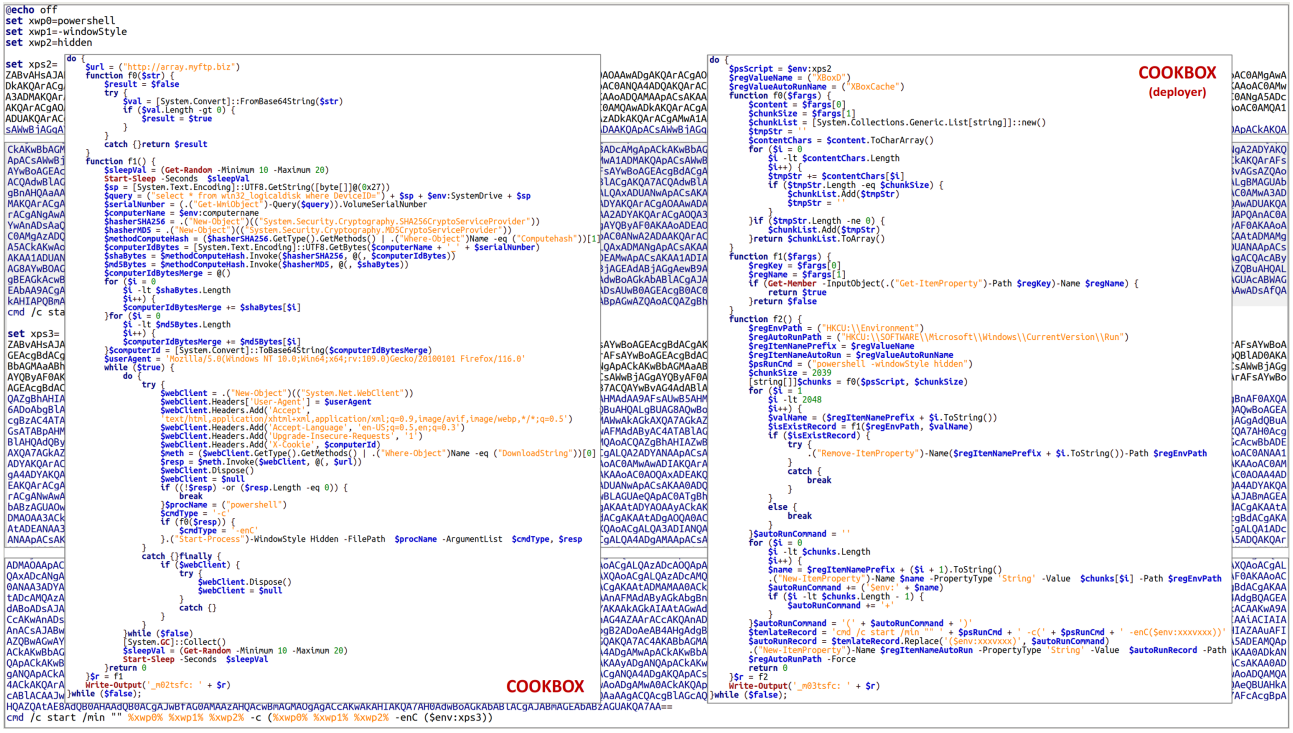

Рис.2 Приклад BAT-скрипта, що призначений для запуску COOKBOX

Source: https://cert.gov.ua/article/6277849