CERT-UA

Archived: 2026-04-02 12:12:45 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA отримано інформацію щодо здійснення спроби ураження шкідливим програмним забезпеченням ЕОМ представника Сил оборони України.

З'ясовано, що засобами месенджеру Signal під виглядом необхідності надання документів для заміщення посади в Департаменті операцій з підтримки миру ООН невстановленою особою надіслано файл "Супровід.rar". Згаданий архів містить експлойт для вразливості у програмному забезпеченні WinRAR (CVE-2023-38831).

У випадку відкриття архіву та успішної експлуатації вразливості буде виконано CMD-файл "супровід.pdf .cmd", що, серед іншого, призведе до відкриття документу-приманки "DPO_SEC23-1_OMA_P-3_16-ENG.pdf" та запуску PowerShell-скриптів, що класифіковано як шкідливу програму COOKBOX (детальна інформація в публікації від 24.02.2024 https://cert.gov.ua/article/6277849).

Зауважимо, що для забезпечення функціонування серверу управління COOKBOX використовується сервіс динамічного DNS NoIP. За сприяння останніх відповідне доменне ім'я було заблоковане.

Користувачів ЕОМ просимо бути пильними та критично ставитися до будь-яких спроб спонукання до відкриття файлів чи переходу за посиланням, в тому числі тих, що надходять через мессенджери. За найменшої підозри подібні повідомлення, посилання та файли надавати для аналізу до відповідних підрозділів і/або CERT-UA.

Системним адміністраторам наполегливо рекомендуємо заборонити можливість запуску користувачами утиліт на кшталт powershell.exe, wscript.exe, csript.exe, mshta.exe та інших, для чого доцільно застосувати штатні механізми операційної системи (SRP, AppLocker, налаштування реєстру).

Індикатори кіберзагроз

Файли:

```
2fec3ab587e6b5533b4c6b3c11dd357a    d8ccaef116cada9c558f9e912d5cf7ef2978082611e677f6f55ca233f47a2f68
cc1732ce2d2cd79dc85893fdc3b7d143    6652b46987350e831678d7a33a70bce94c8c9cca137f0bb0efbbd0c07279cbb6
ba1859659089253621e5a65181ea94cd    8f8abfa6717ad2043a295d16b5aeeac3e7084b7994f6eec8351e18a9a3c59997
1e857958a3c7f909ee1370c66d71adfd    56b569912a6e1c4c08e5612c0ef5ddf9f238b1d708621b89963b47b31e45cde1
```

Мережеві:

```
Mozilla/5.0(Windows NT 10.0;Win64;x64;rv:109.0)Gecko/20100101 Firefox/116.0
hXXp://netman.servehttp[.]com
hXXp://worker-misty-mouse-6ac7.aky15825.workers[.]dev/
netman.servehttp[.]com
worker-misty-mouse-6ac7.aky15825.workers[.]dev
```

Хостові:

```
HKCU:\Environment\XBoxD1
HKCU:\Environment\XBoxD2
HKCU:\Environment\XBoxD3
HKCU:\Environment\XBoxD4
HKCU:\Environment\XBoxD5
HKCU:\Environment\XBoxD6
HKCU:\Environment\XBoxD7
HKCU:\Environment\XBoxD8
HKCU:\Environment\XBoxD9
HKCU:\Environment\XBoxD10
HKCU:\Environment\XBoxD11
HKCU:\Environment\XBoxD12
HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\XBoxCache
cmd /c start /min "" powershell -windowStyle hidden -c(powershell -windowStyle hidden -enC $env:XBox
```

Графічні зображення

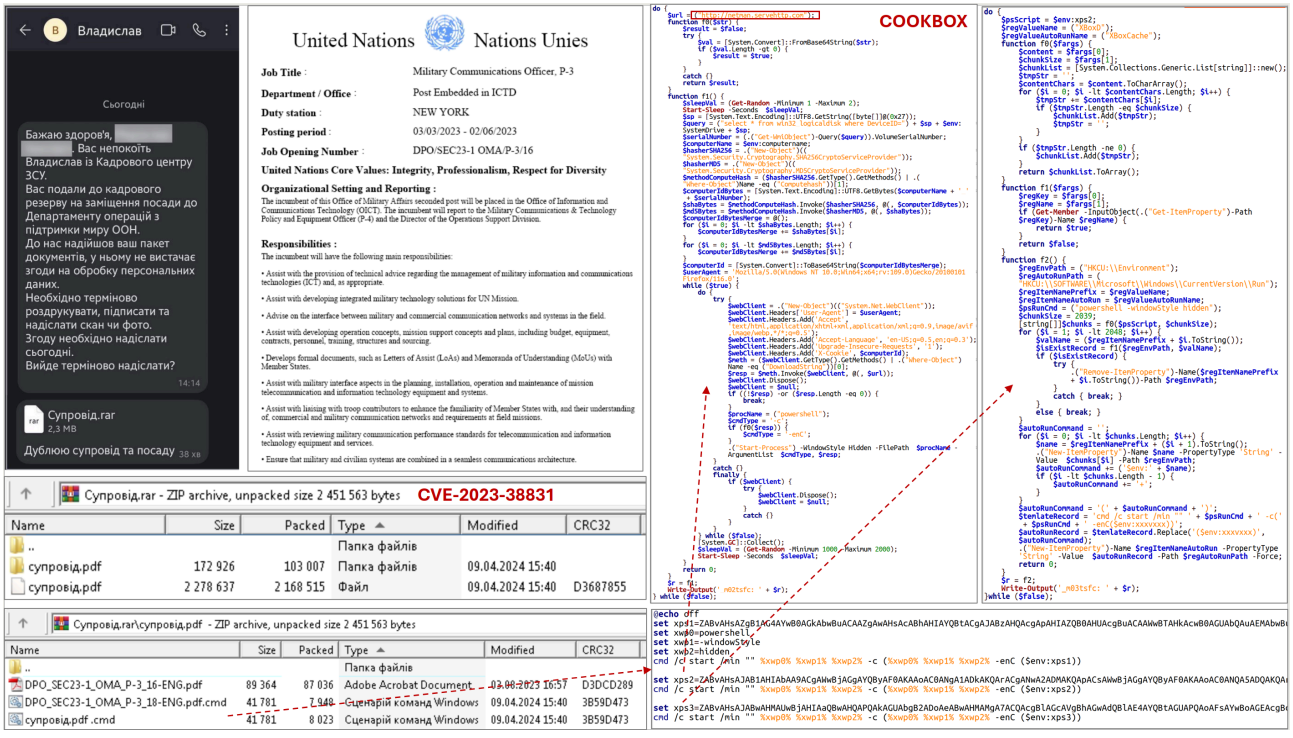

Рис.1 Приклад ланцюга ураження

Source: https://cert.gov.ua/article/6278620