CERT-UA

Archived: 2026-04-05 20:31:29 UTC

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA від суб’єкту координації отримано інформацію щодо розповсюдження, начебто, від імені Національної поліції України, електронних листів, із вкладеннями у вигляді захищених паролем DOCX-документів, наприклад «Повідомлення про вчинення злочину (Білоус Олексій Сергійович).docx» або «Повідомлення про вчинення злочину.docx».

Згадані документи містять вбудовані об’єкти, активація яких призведе до створення і запуску на комп’ютері Javascript-файлу, наприклад «GSU207@POLICE.GOV.UA - Повідомлення (2).js». Останній, за допомогою powershell здійснить підключення до сервісу Discord та завантажить і виконає EXE-файл, що призведе до ураження комп’ютера жертви шкідливою програмою OutSteel (дата компіляції: 30.01.2022) .

Активність асоційовано з діяльністю групи UAC-0056.

Індикатори компрометації

Файли:

```
4d01975268c215fc26ed79ebd17ec22d    Повідомлення про вчинення злочину (Білоус Олексій Сергії
12ed130045b2e731bc66c9261c88efaa    GSU207@POLICE.GOV.UA - Повідомлення (2).js
22c1d43016cb2b8b9e5e5e9895526354    Повідомлення про вчинення злочину .docx
0e3c3fe6167485807c4d36a904dfcae1    GSU207@POLICE.GOV.UA - Повідомлення (17).js
259f06fcdb971f606d239b3178110981    putty.exe
ccc3750d9270d1e8c95649d91f94033b    putty.dmp.exe (OutSteel)
5fa2c64ed3e9944030b6fd9f3d3d7102    puttyjejfrwu.exe
57a10dad336f1a6cb206dca7ddd3fcaf    AutoIt.exe (OutSteel)
ab2a92e0fc5a6f63336e442f34089f16    1406.exe (SaintBot)
af9a60ea728985f492119ebf713e0716    load4849kd30.exe (SaintBot)
247165c7d96bf443b6a7360a44b7dcfb    f0d.exe
cd8915c63f3134425aa7c851f5f1e645    f1d.exe
```

Мережеві:

```
hxxps://cdn.discordapp[.]com/attachments/932413459872747544/938291977735266344/putty.exe
hxxps://cdn.discordapp[.]com/attachments/932413459872747544/938317934026170408/puttyjejfrwu.exe
hxxp://185.244.41[.]109:8080/upld/
hxxp://eumr[.]site/load74h74830.exe
185.244.41[.]109
```

```
eumr[.]site
mariaparsons10811@gmail[.]com
```

Хостові:

```
%PUBLIC%\GoogleChromeUpdate.exe
%USERPROFILE%\Documents\.exe
%TEMP%\GSU207@POLICE.GOV.UA - Повідомлення (2).js
%TEMP%\rmm.bat
%TEMP%\svjhost.exe
```

Процеси:

```
1       powershell.exe "%USERPROFILE%\Documents\.exe"
11      powershell.exe "%USERPROFILE%\Documents\.exe"
3       powershell.exe <IP-адреса>:443
22      powershell.exe cdn.discordapp[.]com
1       wscript.exe powershell.exe "%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe" [Ne
1       WINWORD.EXE wscript.exe "%SYSTEMROOT%\System32\WScript.exe" "%TEMP%\GSU207@POLICE.GOV.UA - П
```

Додаткова інформація

Рекомендуємо заблокувати доступ до сервісів в мережі Інтернет, використання яких не є необхідним і/або може створювати додаткові ризики (наприклад, Discord).

Звертаємо увагу на коректність налаштування політик безпеки і засобів захисту комп’ютера, а саме:

- заборонити процесам програм MS Office (зокрема, WINWORD.EXE) запускати потенційно небезпечні програми, в даному випадку – wscript.exe (Sysmon EventID: 1);
- контролювати мережеві з’єднання (Sysmon EventID: 3,22) потенційно небезпечних програм (powershell.exe тощо)

Графічні зображення

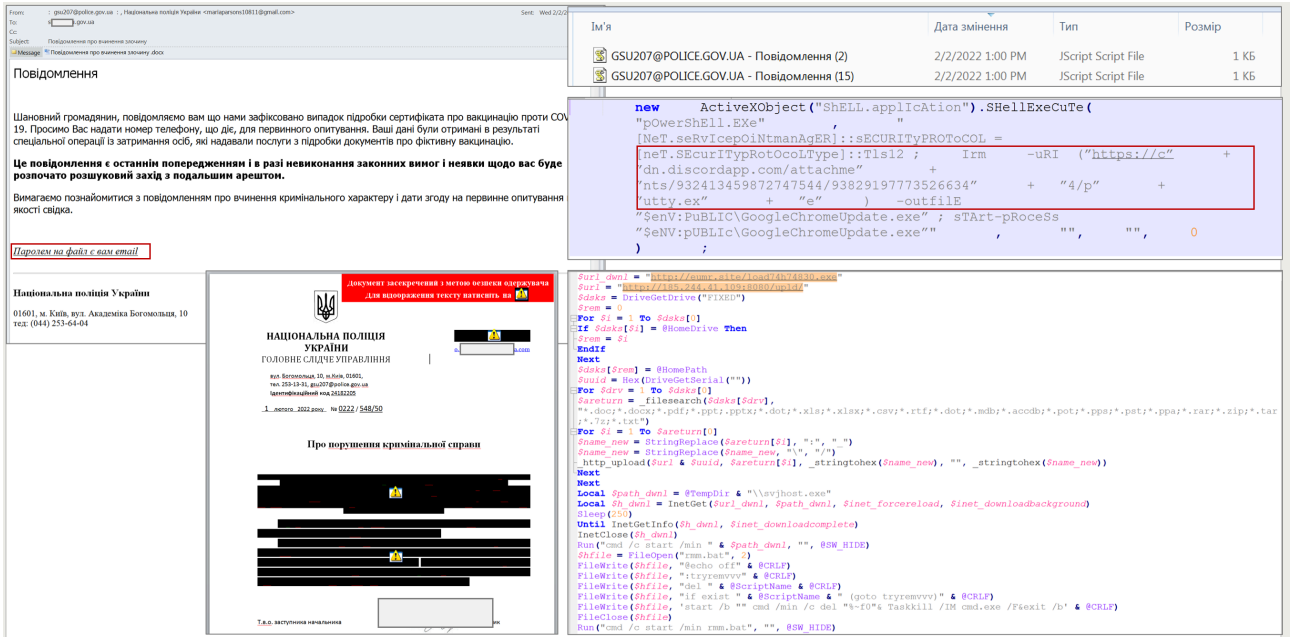

Рис. 1 Приклад електронного листа та шкідливого документу

Source: https://cert.gov.ua/article/18419