CERT-UA

Archived: 2026-04-02 11:14:02 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA 21.02.2023 зафіксовано масове розповсюдження електронних листів начебто від імені Печерського районного суду міста Києва з темою "Печерський районний суд міста Києва" та додатком у вигляді RAR-архіву "електронний судовий запит № 7836071.rar".

Архів містить текстовий документ "код доступу 3527 .txt" та захищений паролем RAR-архів "електронний судовий запит № 7836071.rar", в якому знаходиться виконуваний файл "електронний судовий запит № 7836071.pdf.exe" розміром 688МБ з підробленим цифровим підписом.

Запуск EXE-файлу призведе до встановлення на комп'ютері жертви програми для віддаленого контролю та спостереження Remcos.

Зауважимо, що один з електронних листів містить заголовок "Received: from [91.228.10[.]77] (port=56344 helo=109x194x3x7.static-customer.bryansk.ertelecom[.]ru)"; при цьому, зазначена IP-адреса була застосована 13.02.2023 під час розсилання шкідливих електронних листів з темою "RE: Критичне оновлення безпеки" (MD5: 8fe5572d2683360d3483ad32e8bad9a1) та додатком у вигляді програми для віддаленого управління Remote Utilities (https://cert.gov.ua/article/3863542; CERT-UA#5961).

Виходячи з викладеного, вважаємо за можливе поєднати UAC-0050 та UAC-0096 в одну групу та продовжити відстеження активності за ідентифікатором UAC-0050.

Звертаємо увагу на той факт, що після успішного ураження комп'ютерів зловмисники здійснюють ексфільтрацію автентифікаційних даних, а також використовують інфіковану ЕОМ для розвідки локальної обчислювальної мережі та подальшого розвитку атаки на інформаційно-комунікаційну систему організації.

Індикатори компрометації

Файли:

```
6d4eccbdf2de6a8d251dd5d290472be8    8872d6afaa790c755ce42823549fa80f6594c9296d0f8fcc8dde5b0839d63c1b
399327a4dd1ac365f99f6e77c6089897    eb07ad9ca3b06aee903d38512cf1157dd3b38f9fcbe919593af37d53c1f17a83
90bc4319fc2bcf2d49d97e37fb99ea78    ee4a2d34012f5ea2b2d1c6c60f322a5a36c31748700aa6ae73d1a7fa875dfed1
099870d8fb21d5e9673711117ec4ff3e    86146b1265de8425e9c0960ba06464d2dfec7a0c803eaa31af29a7682700fa68
fcc95f2d4edad0ff682f190406b35ff0    5b9ec22aef059dc09bf82d694934e52d7cbfd8fd696b4c4e68ac10d7280d31d6
```

Хостові:

```
%PROGRAMDATA%\word\wos.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\word
```

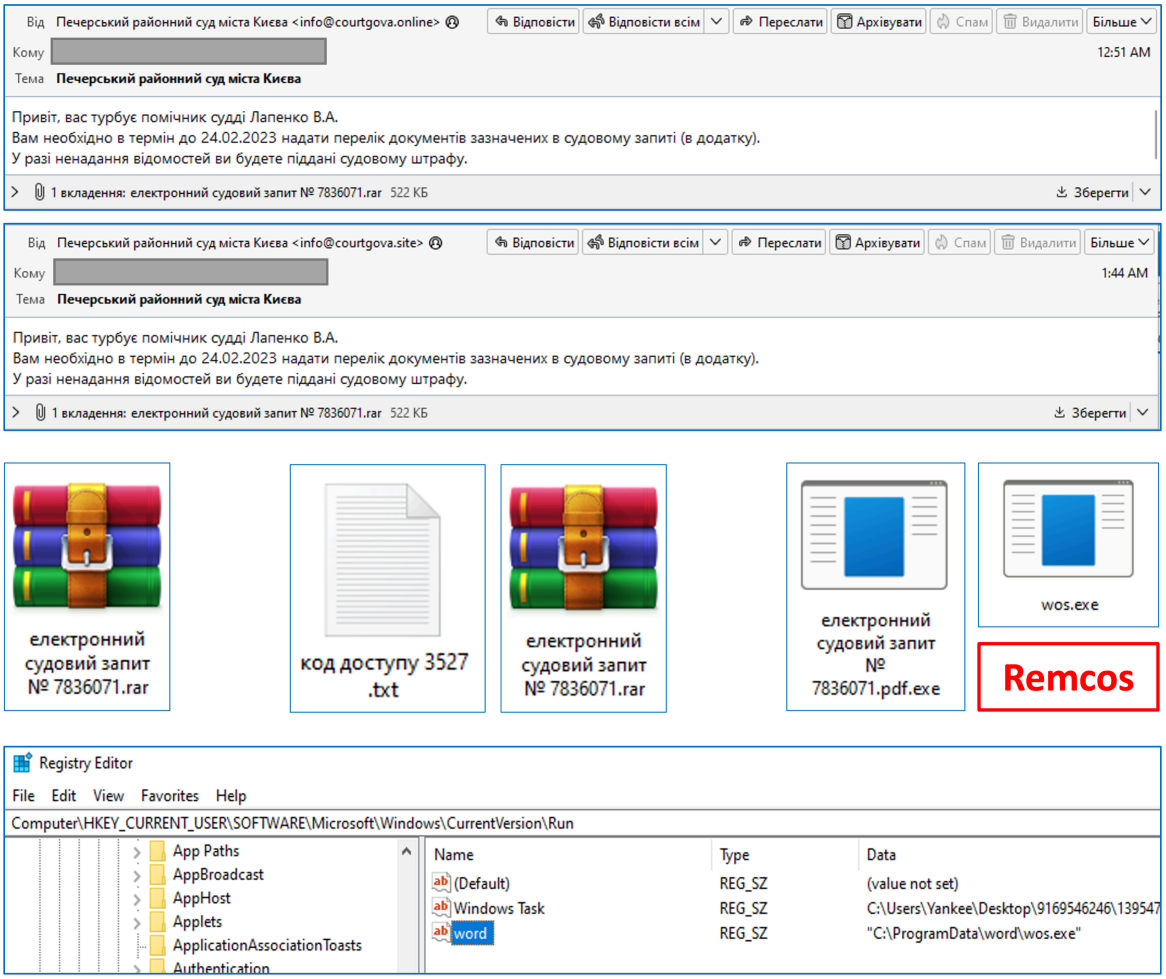
Мережеві:

```
courtgova[.]online                  2023-02-13    @publicdomainregistry.com
courtgova[.]site                    2023-02-13    @publicdomainregistry.com
courtbox[.]online                   2023-02-13    @publicdomainregistry.com
95.163.235[.]80                     RU            @reg.ru (Received)
91.228.10[.]77                      RU            @stark-industries.solutions (Received)
80.78.248[.]17                      RU            @reg.ru
80.78.248[.]200                     RU            @reg.ru
info@courtgova[.]site
info@courtgova[.]online

(Remcos C2)
77[.]91.100.6                                     @stark-industries.solutions
77[.]91.100.9
94[.]131.99.153
94[.]131.99.156
94[.]131.99.159
101[.]99.91.124                                   @shinjiru.com.my
101[.]99.91.158
101[.]99.91.170
101[.]99.91.176
101[.]99.93.104
111[.]90.148.194
217[.]69.139.209                                  @corp.mail.ru (?)
217[.]69.139.232
217[.]69.139.243
(tcp)://77[.]91.100.6:5222
(tcp)://77[.]91.100.9:5222
(tcp)://94[.]131.99.153:5222
(tcp)://94[.]131.99.156:5222
(tcp)://94[.]131.99.159:5222
(tcp)://111[.]90.148.194:5222
(tcp)://111[.]90.148.194:81
(tcp)://101[.]99.91.124:5222
(tcp)://101[.]99.91.158:5222
(tcp)://101[.]99.91.170:5222
(tcp)://101[.]99.91.176:5222
(tcp)://101[.]99.93.104:5222
(tcp)://217[.]69.139.209:5222
(tcp)://217[.]69.139.209:81
```

```
(tcp)://217[.]69.139.232:81
(tcp)://217[.]69.139.243:81
```

Графічні зображення



Source: https://cert.gov.ua/article/3931296