CERT-UA

Archived: 2026-04-05 14:10:57 UTC

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA отримано інформацію щодо масового розповсюдження електронних листів з темою "Нова програма для запису в журналі." серед громадян України та вітчизняних організацій. Текст електронного листа містить повідомлення, начебто, від Міністерства освіти та науки України щодо "електронних навчальних журналів", а також посилання на "програму" та пароль на архів.

У разі відкриття архіву та запуску EXE-файлу, комп'ютер буде уражено шкідливою програмою, яку, за сукупністю ознак (незважачи на деякі відмінності), класифіковано як MarsStealer.

MarsStelaer - шкідлива програма-стілер, розроблена з використанням мов програмування C/ASM. Основний функціонал - збір інформації про комп'ютер, викрадення аутентифікаційних даних з Інтернет-браузерів, плагінів крипто-гаманців, програм багатофакторної аутентифікації, викрадення файлів, а також завантаження і запуск виконуваних файлів і виготовлення знімку екрану.

Шкідлива програма продається на тематичних форумах. Вірогідно, після призупинки продажів стілера Racoon, використовуватиметься як альтернатива. Зауважимо, що заявлений функціонал, який передбачає уникнення випадків застосування стілера у відношенні "країн СНД", відключено шляхом патчингу викликів відповідних функцій.

Виявлена активність відстежується за ідентифікатором UAC-0041 як діяльність однієї з груп, що мають на меті викрадення автентифікацйних даних користувачів.

Індикатори компрометації

Файли:

```
50dc32d384eddc6142d98dba4b383952    e9022b65a0f367bebb6862dd17f084a662d7adb50076c1c364df0e074888656c
eac2f01715ff167bf3e155fad36e5b0d    f67ff70f862cdcb001763c69e88434d335b185a216e2944698f20807df28bdf2
67dde33620bb01c74f9189f5e03d6528    e65231f304e78ce51dc77728f883c41465b9c8a5457cc2b22fc362f48521017a
b5129b33d2181343b31bd64ec340a599    afa0662aa8eac0e607a9ffc85aa0bdfc570198dcb82dccdb40d0a459e12769dc
```

Мережеві:

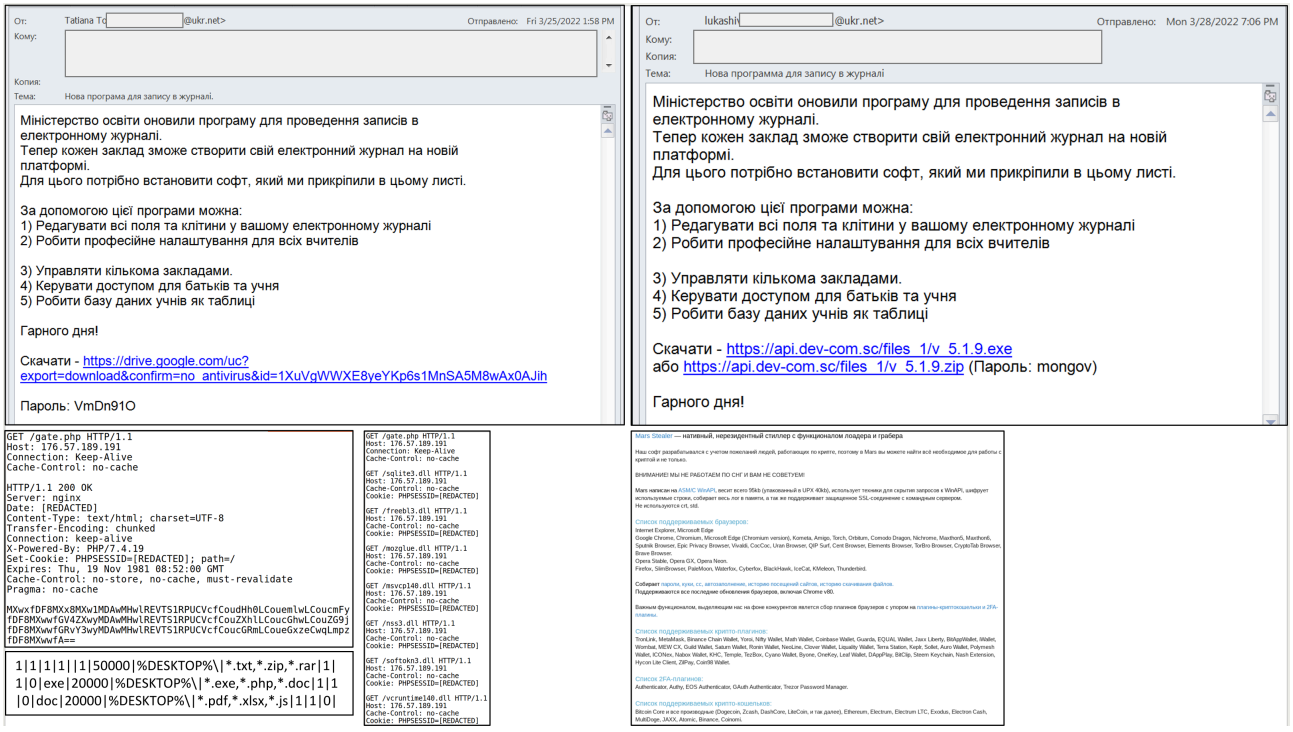
```
hXXps://drive.google[.]com/uc?export=download&confirm=no_antivirus&id=1XuVgWWXE8yeYKp6s1MnSA5M8wAx0A
hXXps://api.dev-com[.]sc/files_1/v_5.1.9.exe
hXXps://api.dev-com[.]sc/files_1/v_5.1.9.zip
hXXp://176[.]57.189.191/gate[.]php
hXXp://176[.]57.189.191/mozglue[.]dll
```

```
hXXp://176[.]57.189.191/vcruntime140[.]dll
hXXp://176[.]57.189.191/nss3[.]dll
hXXp://176[.]57.189.191/msvcp140[.]dll
hXXp://176[.]57.189.191/freebl3[.]dll
hXXp://176[.]57.189.191/sqlite3[.]dll
hXXp://176[.]57.189.191/softokn3[.]dll
api.dev-com[.]sc
dev-com[.]sc (2022-03-24)
176[.]57.189.191
95[.]111.231.126
```

Хостові:

```
C:\ProgramData\sqlite3.dll
C:\ProgramData\freebl3.dll
C:\ProgramData\mozglue.dll
C:\ProgramData\msvcp140.dll
C:\ProgramData\nss3.dll
C:\ProgramData\softokn3.dll
C:\ProgramData\vcruntime140.dll
```

Графічні зображення



Source: https://cert.gov.ua/article/38606