Vidar Stealer Exploiting Various Platforms - ASEC

By ATCP

Published: 2022-12-12 · Archived: 2026-04-05 19:05:16 UTC

Vidar Malware is one of the active Infostealers, and its distribution has been significantly increasing. Its characteristics include the use of famous platforms such as Telegram and Mastodon as an intermediary C2.

The link below is a post about a case where malicious behaviors were performed using Mastodon.

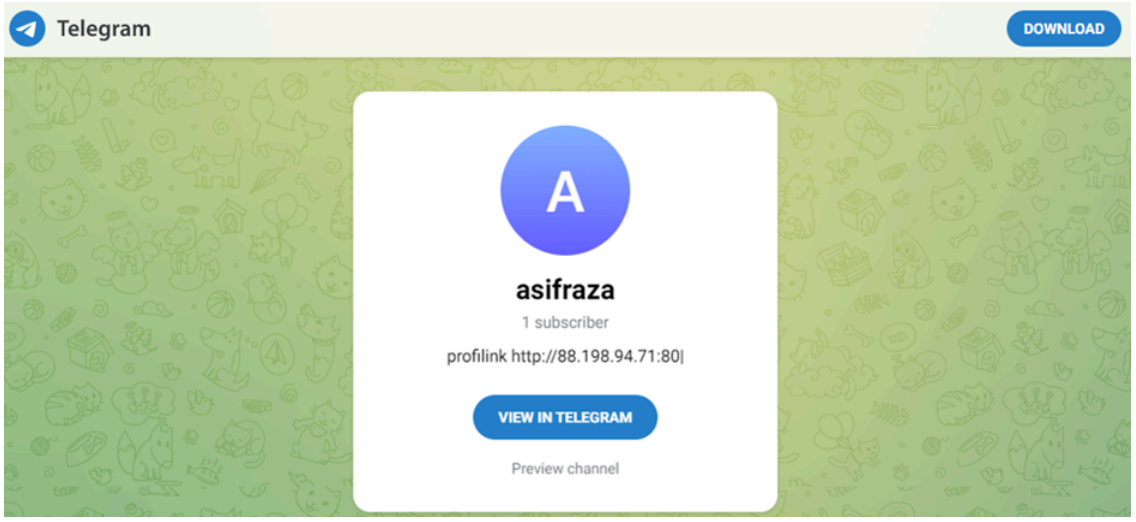
Even afterward, Vidar saw continuous version updates while actively being distributed. In the recent samples in circulation, various other platforms such as Steam and TikTok were used aside from Telegram and Mastodon. In this blog post, we aim to cover the details of these cases.

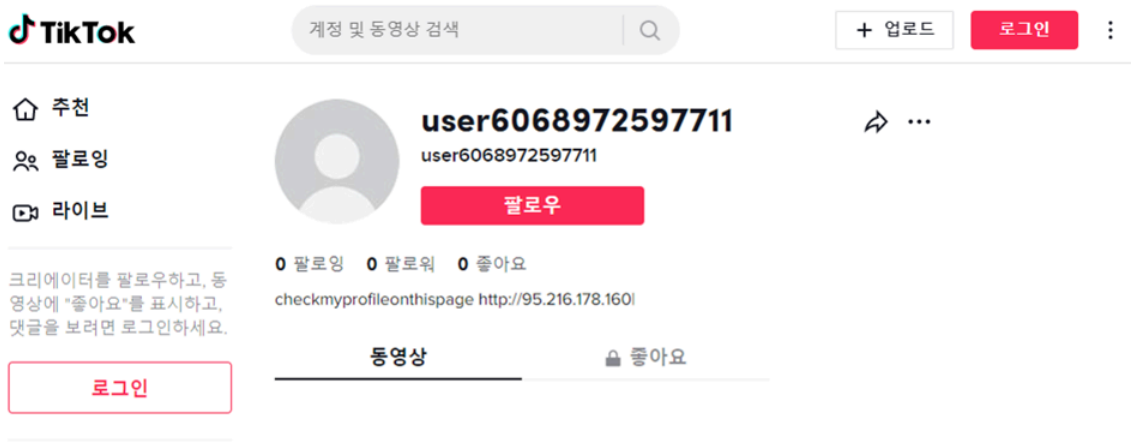
When a user creates an account on an online platform, a unique account page that can be accessed by anyone is generated. Threat actors write identifying characters and the C2 address in parts of this page.

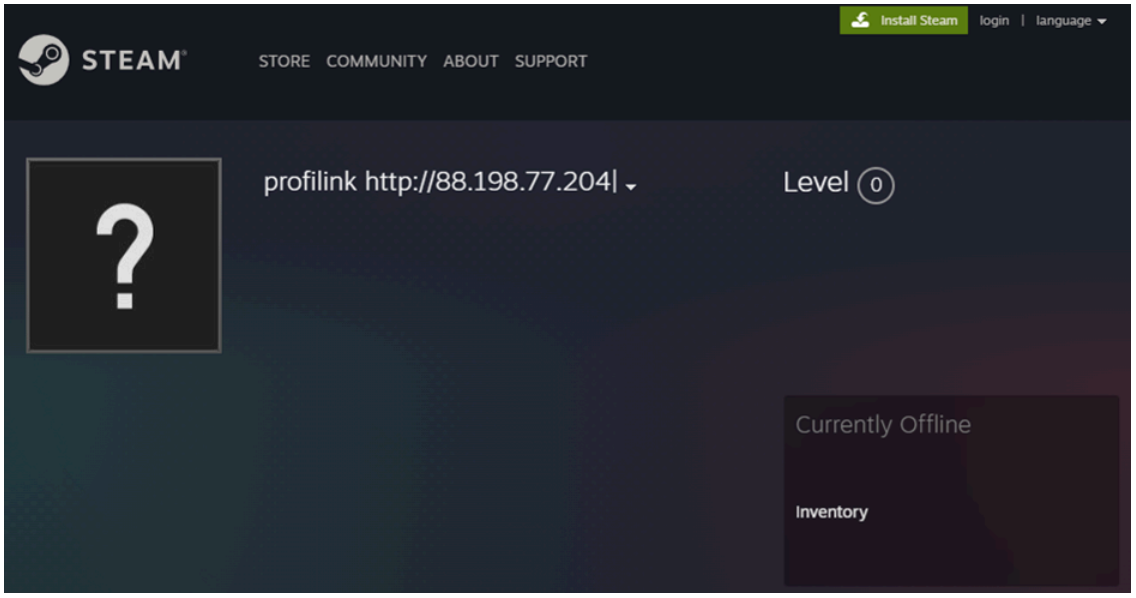
When the malware is executed, it accesses the threat actor’s account page to search for the identifier string and find the C2 address. Then, it performs malicious behaviors while communicating with this C2 server.

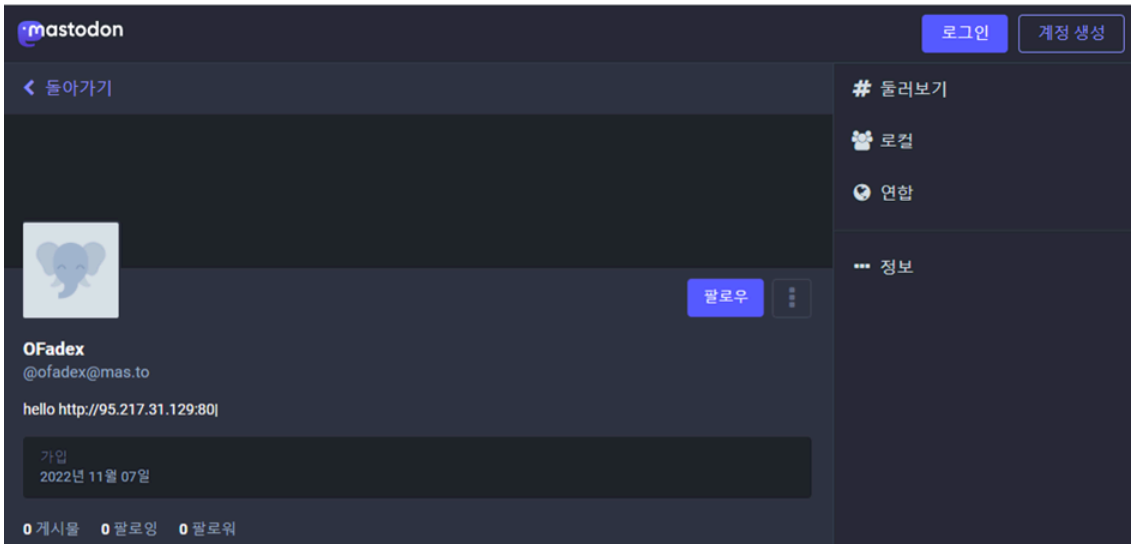
Such public platform URLs are difficult to block with security solutions. Even if the threat actor’s C2 server is blocked, opening a new C2 server and editing the account page will allow all previously distributed malware to communicate with the new C2 server.

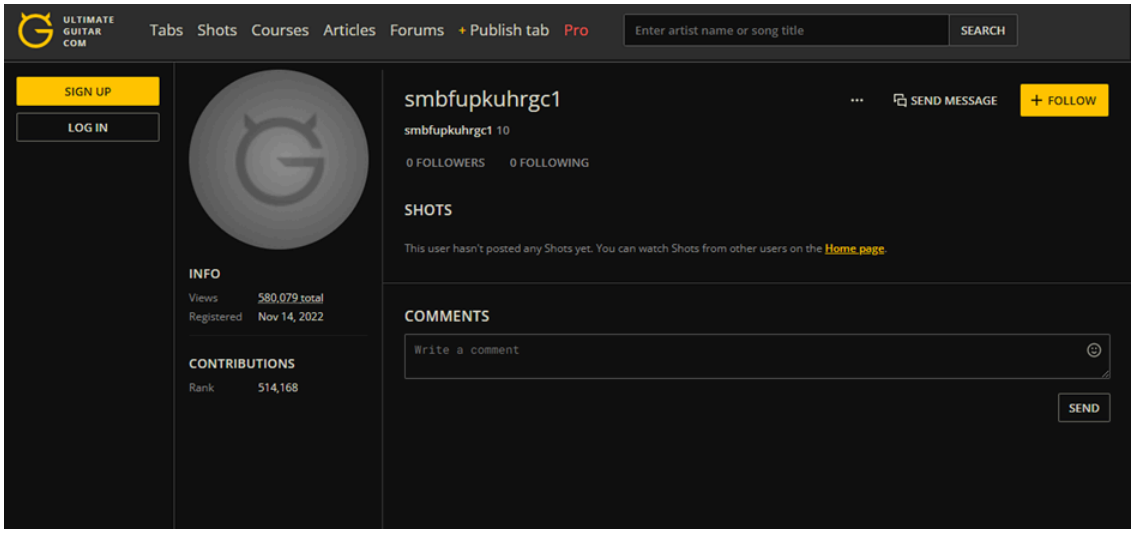
The exploited services share a common trait, which is the fact that it is comparatively easy to create an account on these platforms. The following is a page that was recently abused by Vidar.




TikTok
계정 및 동영상 검색
+ 업로드
로그인
추천
팔로잉
라이브
크리에이터를 팔로우하고, 동영상에 "좋아요"를 표시하고, 댓글을 보려면 로그인하세요.
로그인
user6068972597711
user6068972597711
팔로우
0 팔로잉 0 팔로워 0 좋아요
checkmyprofileonthispage http://95.216.178.160
동영상
좋아요


Install Steam
login | language
STEAM
STORE COMMUNITY ABOUT SUPPORT
profilink http://88.198.77.204
Level 0
Currently Offline
Inventory


mastodon
로그인
계정 생성
돌아가기
둘러보기
로컬
연합
정보
팔로우
OFadex
@ofadex@mas.to
hello http://95.217.31.129:80
가입
2022년 11월 07일
0 게시물 0 팔로잉 0 팔로워



The last screenshot is the threat actor's account on Ultimate Guitar. Multiple samples exploiting this platform have been collected, but unfortunately, we could not secure a screenshot with the actual C2 information. The C2 address connected during the collection was 116.202.2[.]1/1707.

Upon execution, the strings used in its behaviors are decrypted. While it is in a simple XOR format, there are multiple garbage codes that execute string-modifying functions with the dummy text "Lorum ipsum" as the argument. The strings and functions used differ slightly with each sample. This is deemed to be for the purpose of implementing changes to the read-only data area or making it difficult to find the string that identifies the malware on the process memory.

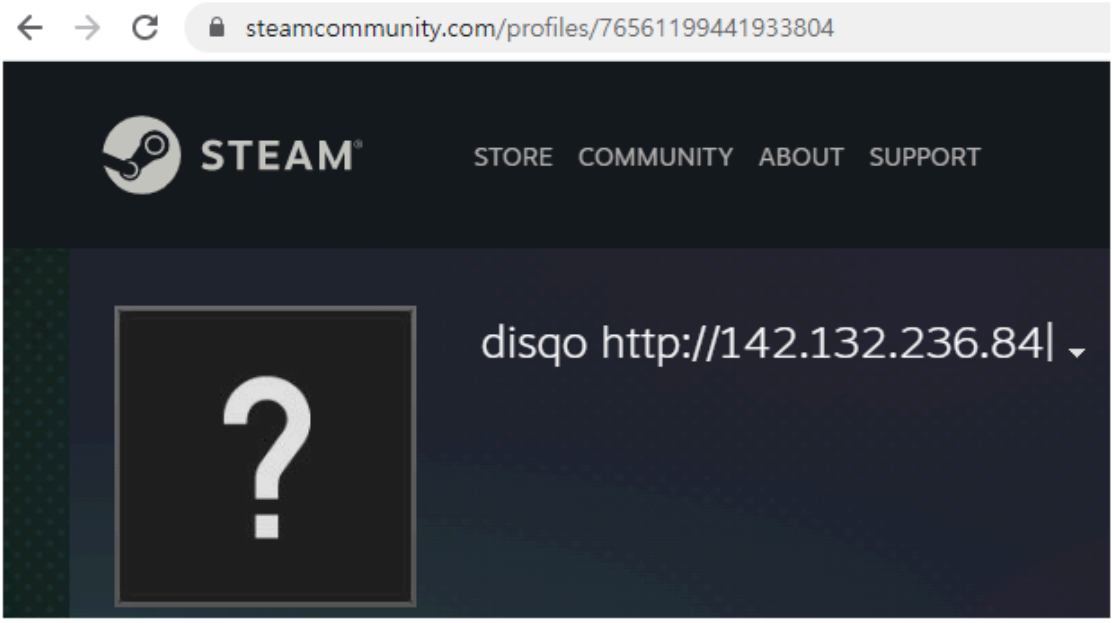
```
strcat(
  Str1,
  "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. ");
strcat(
  Str2,
  "Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.");
strcmp(Str1, Str2);
strcmp(Str1, Str2);
strcmp(Str1, Str2);
strcmp(Str1, Str2);
v9 = LocalAlloc(0x40u, a1 + 1);
```

```
wcscat(
  Destination,
  L"Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it is pain");
wcslen(Destination);
wcslen(Destination);
wcslen(Destination);
wcslen(Destination);
v7 = LocalAlloc(0x40u, a1 + 1);
```

The computer name and username are checked. If they are found to be "HAL9TH" and "JohnDoe" respectively, the malware ceases to function and shuts down immediately. These are the names known to be used by Windows Defender Emulator, and this code seems to serve the purpose of bypassing this feature.

```
CALL get_pc_name                          [123.get_pc_name
MOV ECX,DWORD PTR DS:[13970F8]            ASCII "HAL9TH"
MOV EDX,EAX
CALL string_cmp                           [123.string_cmp
TEST EAX,EAX
JNZ SHORT 0135CCFA
CALL get_user_name                        [123.get_user_name
MOV ECX,DWORD PTR DS:[1397260]            ASCII "JohnDoe"
MOV EDX,EAX
CALL string_cmp                           [123.string_cmp
TEST EAX,EAX
JNZ SHORT 0135CCFA
PUSH EAX                                  [ExitCode
CALL DWORD PTR DS:[1397444]               [KERNEL32.ExitProcess
RETN
```

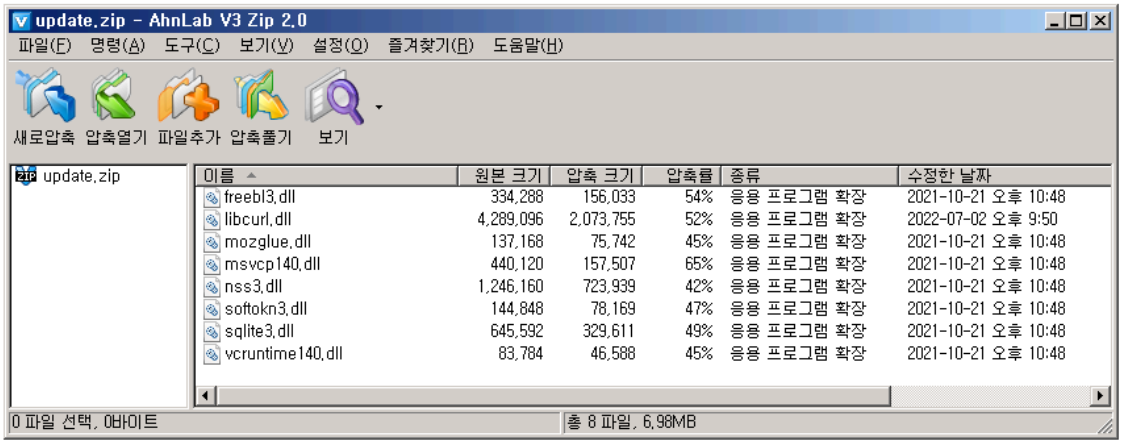
After the above preliminary processes are complete, the malware attempts to connect to the threat actor's account page to download the C2 address. Samples that are currently in distribution include two types of platform account addresses and one actual C2 server URL each. These URLs are hard-coded in the binary and connection attempts are made in order until the actual C2 address is successfully found.



The malware searches the account page's source for the identifier. The string from the character after the identifier to the character before "|" becomes the C2, and the identifier is different for each sample and is hard-coded like the C2 address. The identifier in this sample is "disqo" and the C2 address is 142.132.236.84.

```
0003E280  00 00 00 00 31 35 31 35 00 00 00 00 35 36 2E 31  ....1515....56.1
0003E290  00 00 00 00 68 74 74 70 73 3A 2F 2F 74 2E 6D 65  ....https://t.me
0003E2A0  2F 64 69 73 68 61 73 74 61 00 00 00 68 74 74 70  /dishasta...http
0003E2B0  73 3A 2F 2F 73 74 65 61 6D 63 6F 6D 6D 75 6E 69  s://steamcommuni
0003E2C0  74 79 2E 63 6F 6D 2F 70 72 6F 66 69 6C 65 73 2F  ty.com/profiles/
0003E2D0  37 36 35 36 31 31 39 39 34 34 31 39 33 33 38 30  7656119944193380
0003E2E0  34 00 00 00 68 74 74 70 3A 2F 2F 31 36 37 2E 32  4...http://167.2
0003E2F0  33 35 2E 31 35 30 2E 38 3A 38 30 00 64 69 73 71  35.150.8:80.disq
0003E300  6F 00 00 00 32 30 39 34 00 00 00 00 3B 00 00 00  o...2094....;...
```

During the initial connection to the C2 server, the information (settings) data on malicious behaviors is received, then various library files needed for these behaviors are downloaded. In the past, each file was downloaded separately, but the recently-distributed samples mostly download these files in a compressed file format before unpacking them in the memory area and using them.



The C2 response value includes the activation status of certain features, token values, the target directory, and file extensions. This shows that no drastic changes have been made to the past versions, so the previous blog post is sure to provide sufficient information regarding this. The hex value added in the middle of the function settings flag is a random token value assigned by the C2.

- https://asec.ahnlab.com/en/17633/

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 12 Dec 2022 12:44:53 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Content-Length: 105

1,1,1,1,0,989b377b6b24bb6c402a2c7443a45c68,1,1,1,1,0,Default;%DOCUMENTS%\;*.txt;50;true;movies:music:mp3;
```

The behavior changes according to the C2's settings response, but various information can be targeted for extortion, including browser data (account, password, history, cookies, etc.), cryptocurrency wallets, document files (file extensions defined by the threat actor), screenshot images, and system information.

After information collection is complete, the extorted information is compressed into a ZIP file, encoded in Base64, and transmitted to the C2 server. There is a slight difference from past versions in the process of sending the data to the C2 server.

While previous samples sent the compressed file data in plain text, recent samples send these after encoding them in Base64. Additionally, the HTTP data in transmission became simplified in the recent version. The version information of the malware was also omitted, and the malware's version can only be identified by checking the information.txt file in the compressed file or by checking the hard-coded value in the binary.

There is also a newly-added feature, where the malware receives a random token value as a reply during the initial C2 connection, when the extorted information is sent, it transmits this value as a "token." This is deemed to be for verifying the infected PC and the extorted information.

Name	Value
Content-Disposition: form-data; name="hwid"	4bc8a353-1b21-4b52-a0a7-9d20-806e6f6e6963
Content-Disposition: form-data; name="os"	Windows 7 Home Basic
Content-Disposition: form-data; name="platform"	x64
Content-Disposition: form-data; name="profile"	517
Content-Disposition: form-data; name="user"	
Content-Disposition: form-data; name="cccount"	0
Content-Disposition: form-data; name="fcount"	28
Content-Disposition: form-data; name="ver"	49.6
Content-Disposition: form-data; name="ccount"	0
Content-Disposition: form-data; name="logs"; filename="4bc8a353-1b21-4b52-a0a7-6ce56f661e714461428025.zip" Content-Type: zip	<file>

Name	Value
Content-Disposition: form-data; name="profile"	1515
Content-Disposition: form-data; name="profile_id"	2094
Content-Disposition: form-data; name="hwid"	e318d070cf7f2148772887-4bc8a353-1b21-4b52-a0a7-9d20-806e6f6e6963
Content-Disposition: form-data; name="token"	eafab50d145f7d11258801cdf860db83
Content-Disposition: form-data; name="file"	UEsDBBQAAgAIAASNjFW1tVU1VhoAALMwAAAiABEAL0Nvb2tpZXMvR29vZ2x

Out of the data stated in the extorted information files, there was also a slight change to the date format and the method of creating the HWID. According to this file, the version of the recently distributed sample is 56.1.

```
Version: 49.6

Date: Mon Dec 12 17:33:05 2022
MachineID: 4bc8a353-1b21-4b52-a0a7-6ce56f661e71
GUID: {846ee340-7039-11de-9d20-806e6f6e6963}
HWID: 4bc8a353-1b21-4b52-a0a7-9d20-806e6f6e6963

Path: C:\Users\      \Desktop\work\185cc9e866a23c5cff47d41e8834.exe
Work Dir: C:\ProgramData\9Y5UTCMFJ77095PR6DMXQX5EX

Windows: Windows 7 Home Basic [x64]
Computer Name: WIN-      OOUUR
User Name:
Display Resolution: 1440x900
Display Language: ko-KR
Keyboard Languages: 한국어(대한민국)
Local Time: 12/12/2022 17:33:5
TimeZone: UTC9
```

```
Version: 56.1

Date: 12/12/2022 17:40:50
MachineID: 4bc8a353-1b21-4b52-a0a7-6ce56f661e71
GUID: {846ee340-7039-11de-9d20-806e6f6e6963}
HWID: e318d070cf7f2148772887-4bc8a353-1b21-4b52-a0a7-9d20-806e6f6e6963

Path: C:\Users\      \Desktop\483ec112df6d0243dbb06a9414b0daf6.exe
Work Dir: In memory

Windows: Windows 7 Home Basic [x64]
Computer Name: WIN-      OOUUR
User Name:
Display Resolution: 1440x900
Display Language: ko-KR
Keyboard Languages: 한국어(대한민국)
Local Time: 12/12/2022 17:40:50
TimeZone: UTC9
```

As Vidar uses famous platforms as the intermediary C2, it has a long lifespan. A threat actor's account created six months ago is still being maintained and continuously updated. Users must practice caution because Vidar is actively being distributed under the disguise of software or cracks.

AhnLab's diagnosis for the malware as follows.

- Trojan/Win.Injection.C5318441 (2022.12.01.02)
- Infostealer/Win.Vidar.C5317169 (2022.12.13.01)
- Infostealer/Win.Vidar.C533928 (2022.11.11.01)
- Infostealer/Win.Vidar.C5308808 (2022.11.19.00)
- Infostealer/Win.Generic.C5308804 (2022.11.19.00) and more

MD5

0b9a0f37d63b0ed9ab9b662a25357962

256594282554abed80536e48f384d2e8

483ec112df6d0243dbb06a9414b0daf6

a46f7096a07285c6c3fdfdf174c8a8b0

ce1eb73f52efe56356ee21b9c4c4c6c4

Additional IOCs are available on AhnLab TIP.

URL

http[:]//mas[.]to/@ofadex

http[:]//steamcommunity[.]com/profiles/76561199436777531

http[:]//steamcommunity[.]com/profiles/76561199439929669

http[:]//steamcommunity[.]com/profiles/76561199441933804

http[:]//www[.]tiktok[.]com/@user6068972597711

Additional IOCs are available on AhnLab TIP.

FQDN

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/44554/