

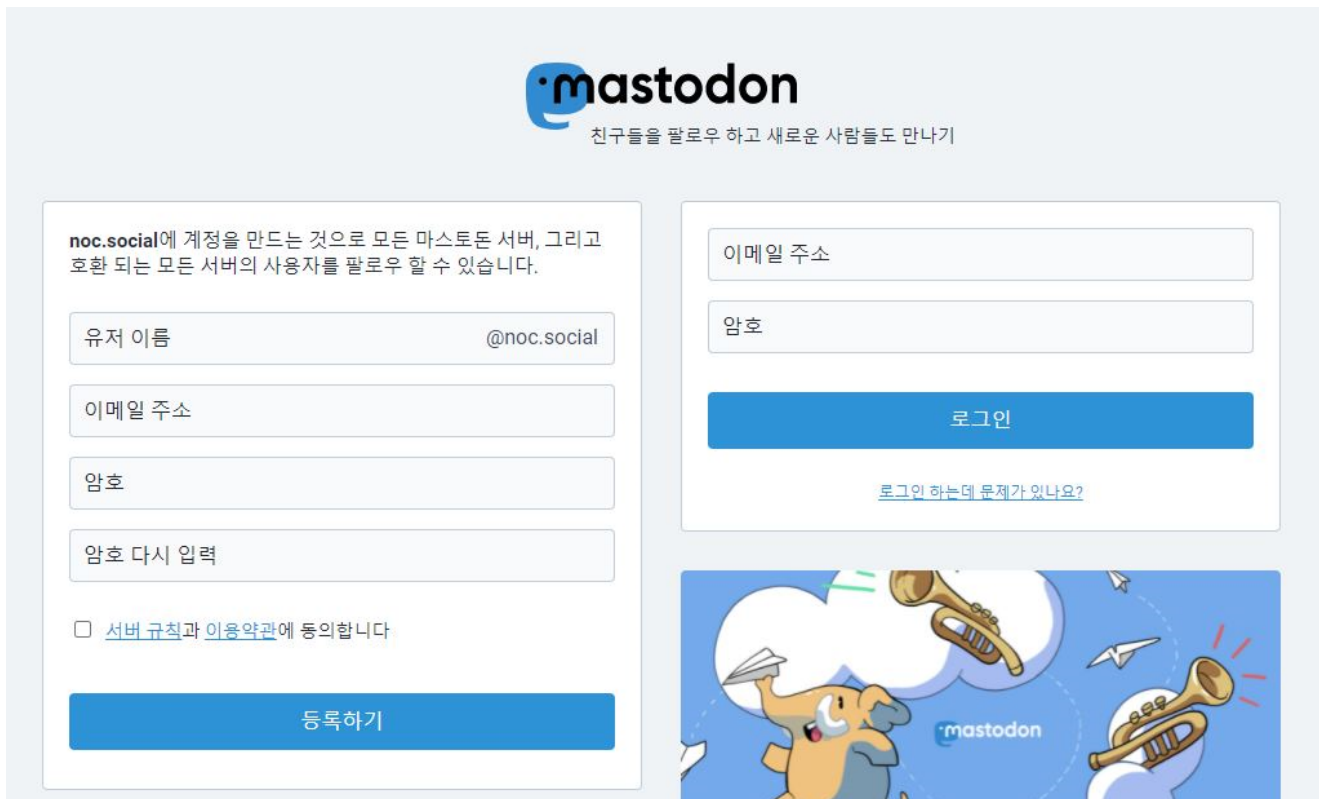
Vidar Exploiting Social Media Platform (Mastodon)

ASEC asec.ahnlab.com/en/30875/

January 26, 2022



The ASEC analysis team has recently discovered that Vidar is exploiting a social media platform named Mastodon to create C&C server addresses.



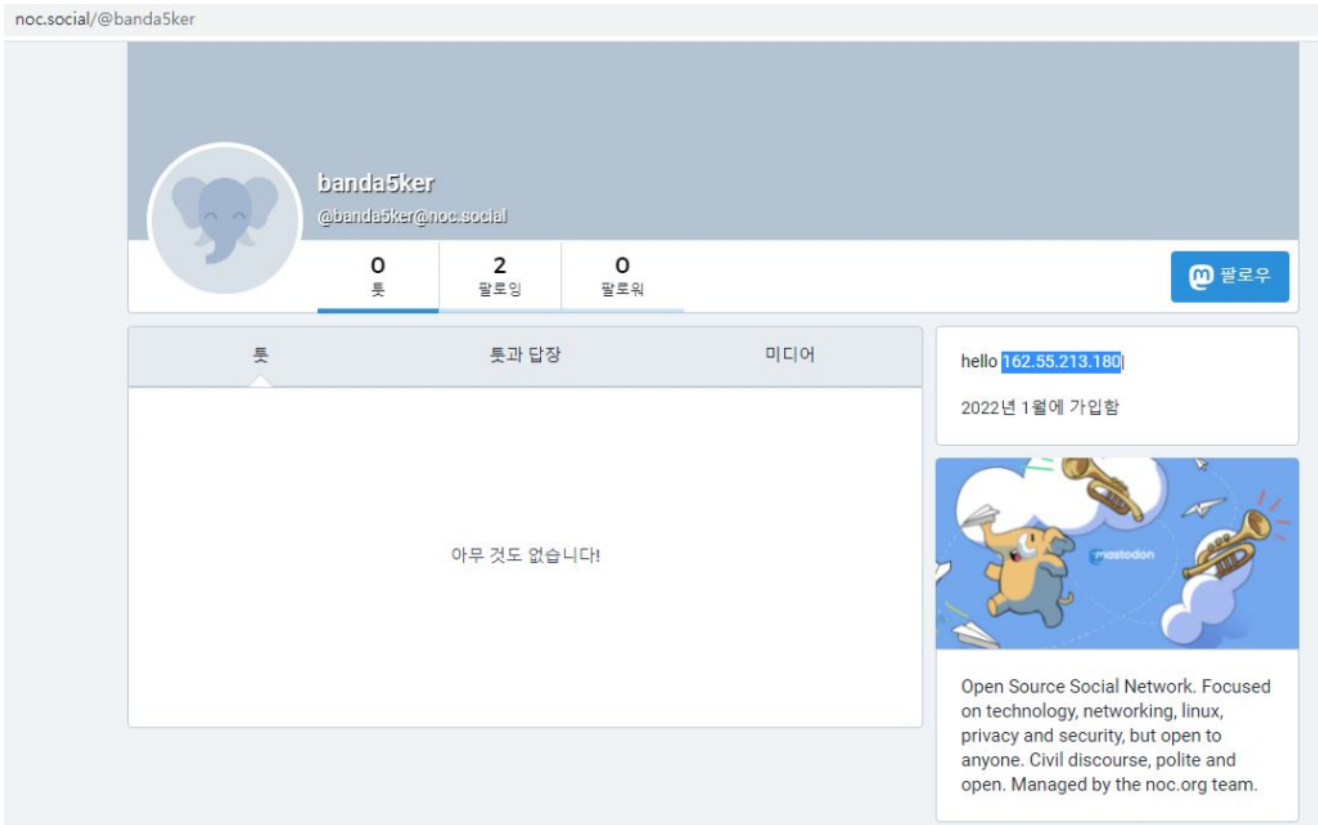
Mastodon website

Vidar is an info-stealer malware installed through spam emails and PUP, sometimes being disguised as a KMSAuto authenticator tool. It has been consistently distributed since the past, and there was a recent case of it being installed through other types of malware such as Stop ransomware. When Vidar is run, it first accesses the C&C server to receive commands and DLLs that are required to steal information before it can perform its info-stealing activities. In the past, the malware simply connected to C&C server and received commands and additional files like other malware. Yet the recent Vidar type exploits various online platforms to actually create C&C servers.

Last year, it used a game matching platform called Facelt to do so, which was discussed in one of the ASEC blog posts.

Vidar Info-Stealer Abusing Certain Game Platform

Recent Vidar cases exploit Mastodon, a social media platform. When Vidar is run, it first accesses Mastodon (noc.social website) before it tries to communicate with the C&C server. To be more specific, it is a profile page of a user named “banda5ker”.



Attacker's Mastodon profile

The profile page has the string shown below. It is the actual C&C server address of Vidar.

“hello 162.55.213[.]180|”

The malware downloads the web page and searches the “hello” string, parsing the C&C address existing between the separator “|”.

```

004119A7 |> 8B5424 14 | MOV EDX,DWORD PTR SS:[LOCAL.20]
004119AB |. 52 | PUSH EDX
004119AC |. 50 | PUSH EAX
004119AD |. E8 9BD30800 | CALL strtok
004119B2 |. 83C4 08 | ADD ESP,8
└─Arg2 => [ARG.16], "|"
└─Arg1 = ASCII "162.55.213.180"
Vidar.strto

```

Stack [0019FA60]=Vidar.00411999 (current registers)
EAX=022C2C78, ASCII "162.55.213.180|" name='description' <meta content="https://noc.social/@banda5ker" property="

| Address | Hex dump | ASCII |
|----------|---|------------------|
| 022C2C78 | 31 36 32 2E 35 35 2E 32 31 33 2E 31 38 30 7C 27 | 162.55.213.180 ' |
| 022C2C88 | 20 6E 61 6D 65 3D 27 64 65 73 63 72 69 70 74 69 | name='descripti |
| 022C2C98 | 6F 6E 27 3E 0A 3C 6D 65 74 61 20 63 6F 6E 74 65 | on'> <meta conte |
| 022C2CA8 | 6E 74 3D 22 68 74 74 70 73 3A 2F 2F 6E 6F 63 2E | nt="https://noc. |
| 022C2CB8 | 73 6F 63 69 61 6C 2F 40 62 61 6E 64 61 35 68 65 | social/@banda5ke |
| 022C2CC8 | 72 22 20 70 72 6F 70 65 72 74 79 3D 22 6F 67 3A | r" property="og: |
| 022C2CD8 | 75 72 6C 22 20 2F 3E 0A 3C 6D 65 74 61 20 63 6F | url" /> <meta co |

Routine for C&C address parsing

If the attacker edits the profile part and enters another address, the Vidar info-stealer will connect to the changed C&C server and continue to perform malicious activities. If Mastodon's attacker account is not blocked, the attacker can repeatedly edit the C&C server to make the same malware connect to different C&C servers. It is likely that the attacker is using the method to bypass network detection for the C&C address.

Vidar connects to the actual C&C servers established and receives DLL files needed for commands and info-stealing, and ultimately sends the stolen information to the C&C server. Note that Vidar's version is v49.6 (see figure of data sent below). The version of the Vidar strain which exploited Facelt was v38.6.

| # | Result | Protocol | Host | URL | Body |
|----|--------|----------|----------------|-------------------|-----------|
| 3 | 200 | HTTPS | noc.social | /@banda5ker | 15,484 |
| 4 | 200 | HTTP | 162.55.213.180 | /517 | 228 |
| 5 | 200 | HTTP | 162.55.213.180 | /freebl3.dll | 334,288 |
| 6 | 200 | HTTP | 162.55.213.180 | /mozglue.dll | 137,168 |
| 7 | 200 | HTTP | 162.55.213.180 | /msvcpl40.dll | 440,120 |
| 8 | 200 | HTTP | 162.55.213.180 | /nss3.dll | 1,246,160 |
| 9 | 200 | HTTP | 162.55.213.180 | /softokn3.dll | 144,848 |
| 10 | 200 | HTTP | 162.55.213.180 | /vcruntime140.dll | 83,784 |
| 11 | 200 | HTTP | 162.55.213.180 | / | 33 |
| 12 | 502 | HTTP | ok | / | 534 |

| Name | Value |
|---|-------|
| Content-Disposition: form-data; name="ccount" | 0 |
| Content-Disposition: form-data; name="fcount" | 2 |
| Content-Disposition: form-data; name="ver" | 49.6 |
| Content-Disposition: form-data; name="ccount" | 0 |
| Content-Disposition: form-data; name="logs" | |

Vidar's network activities of sending stolen information

The info-stealing features of Vidar are explained in the following post.

[Analysis of Info-Leaking Feature of Info-Stealer Malware Vidar](#)

AhnLab's anti-malware software, V3, detects and blocks the malware using the following aliases:

[File Detection]

– Infostealer/Win.SmokeLoader.R465643 (2022.01.19.01)

[Behavior Detection]

– Malware/MDP.Vidar.M3505

[IOC]

File

185cc9e866a23c5cff47d41e8834ffad

C&C

- hxxps://noc[.]social/@banda5ker
- hxxp://162.55.213[.]180

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:[Malware Information](#)

Tagged as:[C&C](#), [InfoStealer](#), [MASTADON](#), [vidar](#), [VidarMASTODON](#)