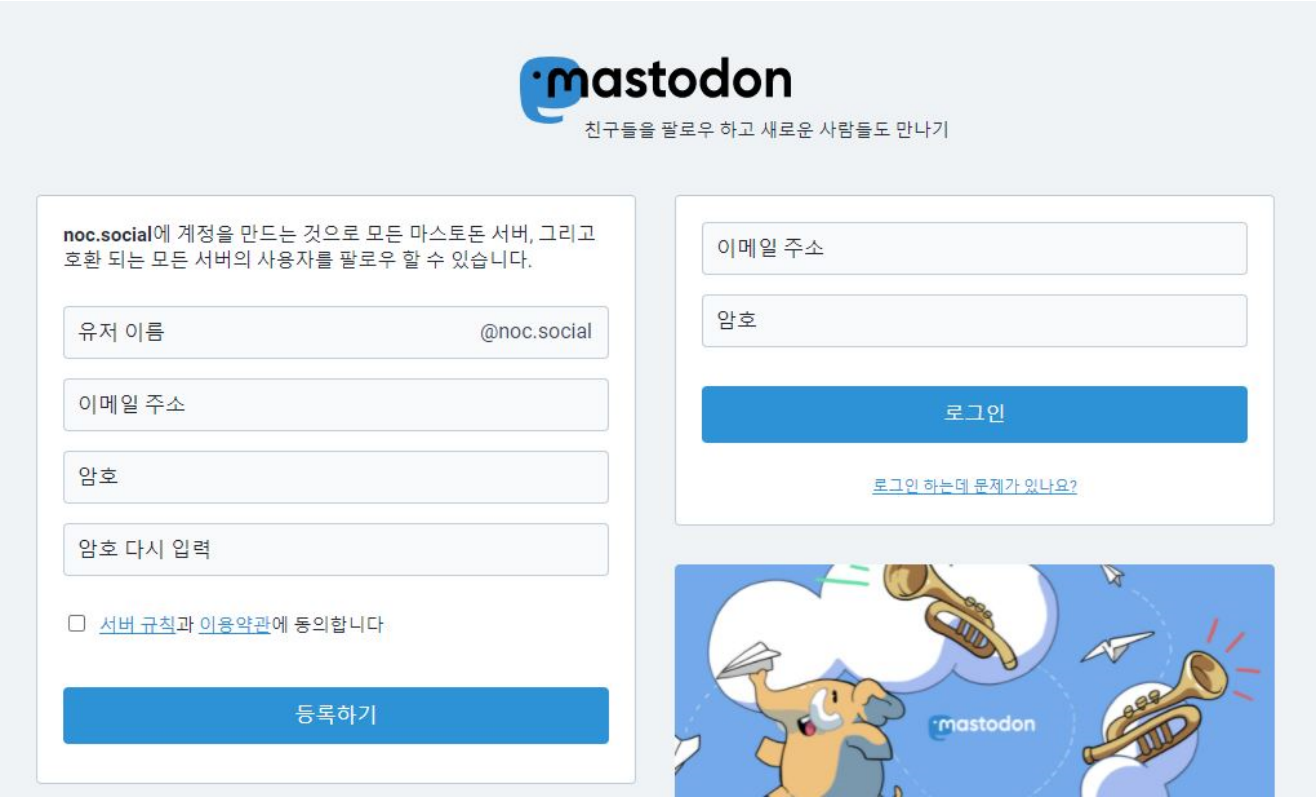
Vidar Exploiting Social Media Platform (Mastodon)

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.



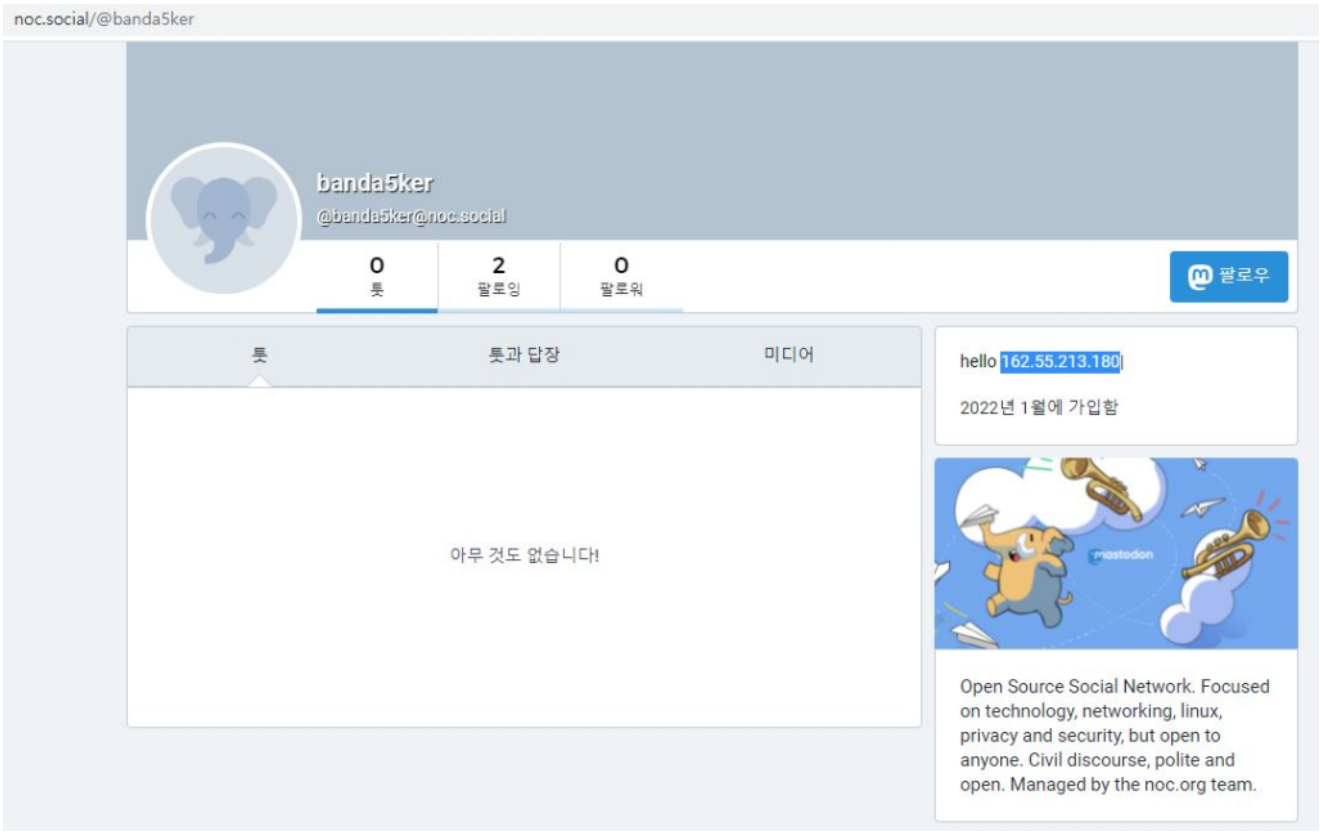
Mastodon website

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 FaceIt 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”.

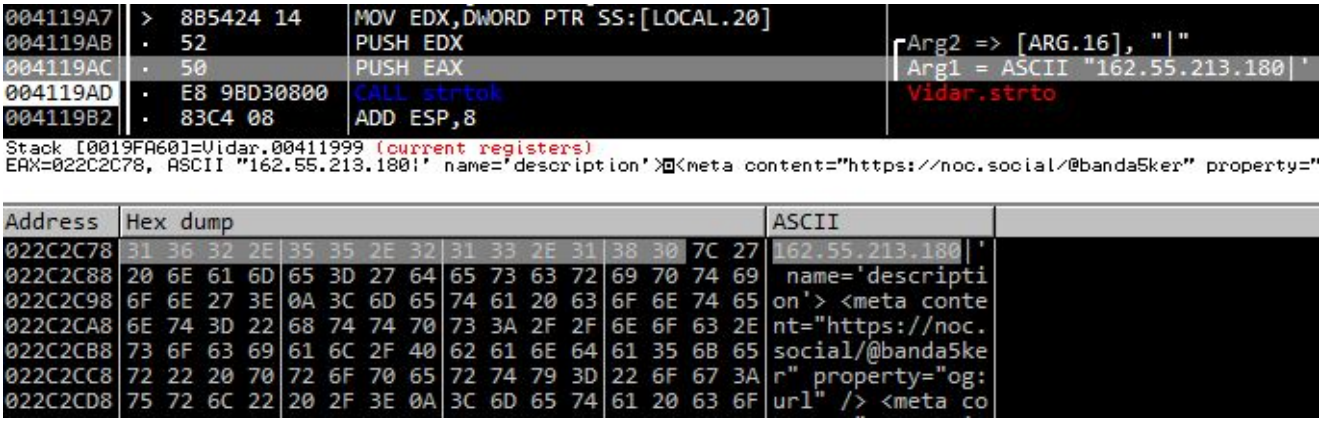


Attacker's Mastodon profile

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

"hello **162.55.213[.]180**|"

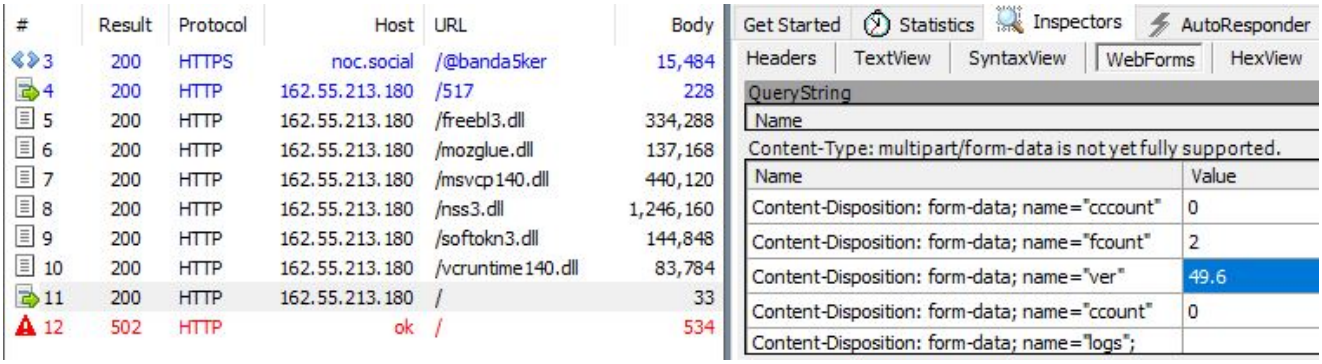
The malware downloads the web page and searches the "hello" string, parsing the C&C address existing between the separator "|".



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 FaceIt 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	/msvcp140.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

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