W1 Feb| EN | Story of the week: Stealers on the Darkweb

By Hyunmin Suh

Published: 2021-02-03 · Archived: 2026-04-05 18:19:25 UTC

Co-author: Minjei Cho, Researcher at

Before deep dive into credential/info stealers in the dark web, let's have a look at the term.

- Credential/Info Stealer — malware that is collecting credential information such as login information saved in browser. It is often associated with Remote Access Tools (RATs) & Botnets.

Much has been discussed about the stealers and the market interlinked with the dark web and surface web, but there aren't many simple and easy-to-understand diagram in accordance with the supply chain how this malicious ecosystem works from the dark web to the surface web. To help you better understand, we've attempted to divide the system into five stages based on what we observed.

1. Sellers of the stealer

AZORult was known to be the one of the most notorious stealer, but the author has stopped its maintenance in 2018. However, the source code of AZORult is still shared and modified by independents which claims to be the latest version.

Besides AZORult, there are two other famously mentioned stealers,
Vidar stealer and **Raccoon stealer**.

Vidar stealer is sold on a Russian speaking hacking forum and has operated since Nov, 2018. The price of Vidar ranges from $130~$750 depending on the usage period. Vidar is written in C++ and it searches wide range of following data:

- All popular browsers of different bit sizes (passwords, cookies, autofill)
- Wallets of cryptocurrencies
- CC — Card data other than CVV
- Files
- Telegram authorization (Windows)
- Browser history (Last 10,000 entries from a specific browser)
- FTP, WINSCP, MAIL

Raccoon, also found on a Russian speaking hacking forum, has operated since April, 2019. The price ranges from $75~$200 depending on the duration which has a similar pricing scheme to Vidar, and other stealers in general. It

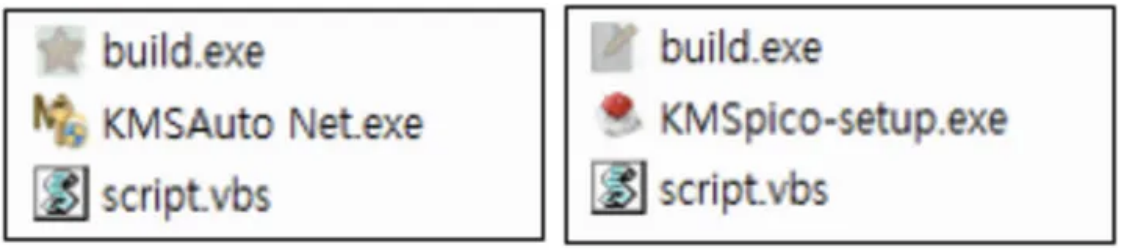
is written in C/C++ and it works on 32/64-bit systems without dependencies on .NET framework. Features include:

- Information found in popular browsers (passwords, cookies, autofill)
- IP
- Geographical information
- Credit Card
- Wallets of cryptocurrencies
- System Information

2. Distribution method

There are various attempts to lure victims to click on a risk link, like targeting high-traffic torrent, redirecting a site hosted with the malicious payloads or disguising it as an installer file. In the case of South Korea, Vidar is distributed as an installer file disguised as KMSAuto which is used for Windows genuine product validation. https://asec.ahnlab.com/en/17633/

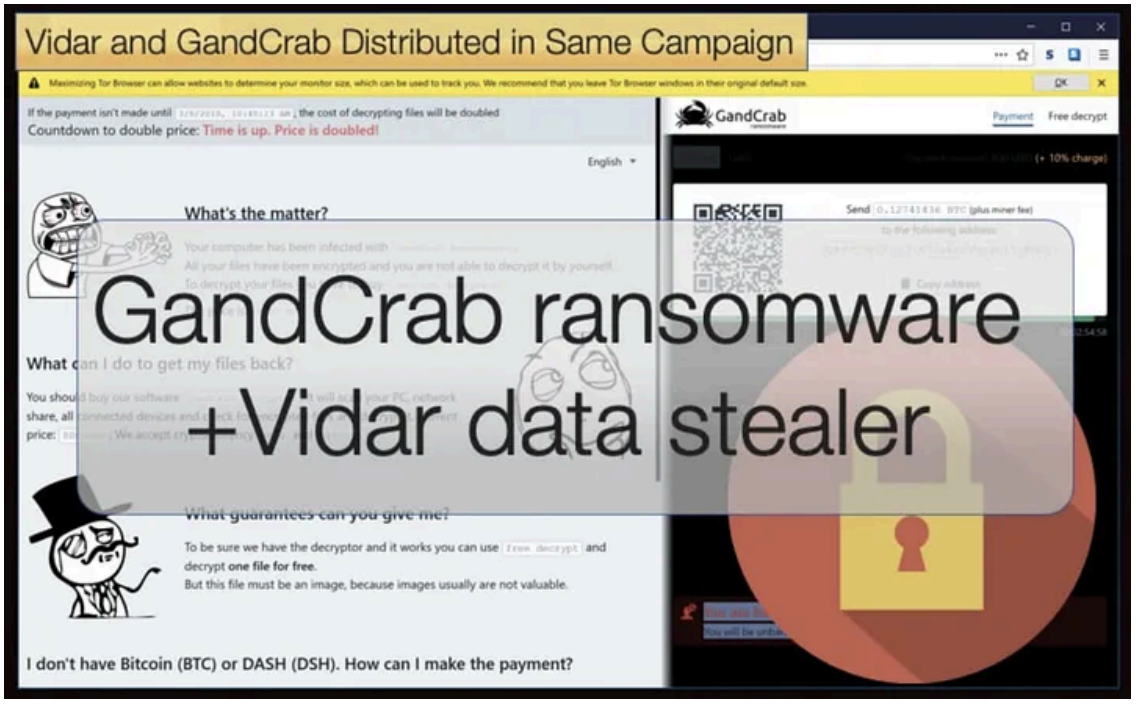
Press enter or click to view image in full size



Vidar disguised as KMSauto authentication tool, source: ASEC Blog

Stealer can also be distributed within a ransomware campaign. PC risk published an article that Vidar was once used with Gandcrab campaign (2019) that the stealer took a role of downloading additional forms of malware which showed it was more capable than just an info stealer. https://www.pcrisk.com/internet-threat-news/14270-vidar-and-gandcrab-distributed-in-same-campaign

Press enter or click to view image in full size



Vidar and GandCrab distributed in the same campaign, source: pcrisk.com

Later on, it appeared in a new spam campaign along with Nemty Special Edition Ransomware targeting South Korean in May 2020. https://asec.ahnlab.com/ko/1316/

Inside the attachment of the fake job application email, two executable files exist in a compressed format (.zip) shown in picture below.

Press enter or click to view image in full size

Two executable files compressed in attachment of the fake job application email, source: ASEC blog

Both executables are disguised as Nemty and Vidar. While Nemty ransomware focusing on encrypting user files, Vidar is used to exfiltrate credential information in this instance.

3. Exploring the details of stealers

Let’s have a look at the details of stealers, main functions and how they work.

Main functions of stealers

Main functions of stealers can vary depending on developers; however, most of stealers we observed share common functions as below.

#Collect Browser Information

- Passwords
- Saved Logins / Autofills
- Payment Methods
- Cookies

#Copying Files

- Copy all files from a certain directory
- Copy files
- Specific Apps or Software files (Bitcoin wallet, Telegram, etc)

#Send System Information

- OS version
- Username
- IP Address

#Account theft in various applications

Get Hyunmin Suh’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

#Screenshot

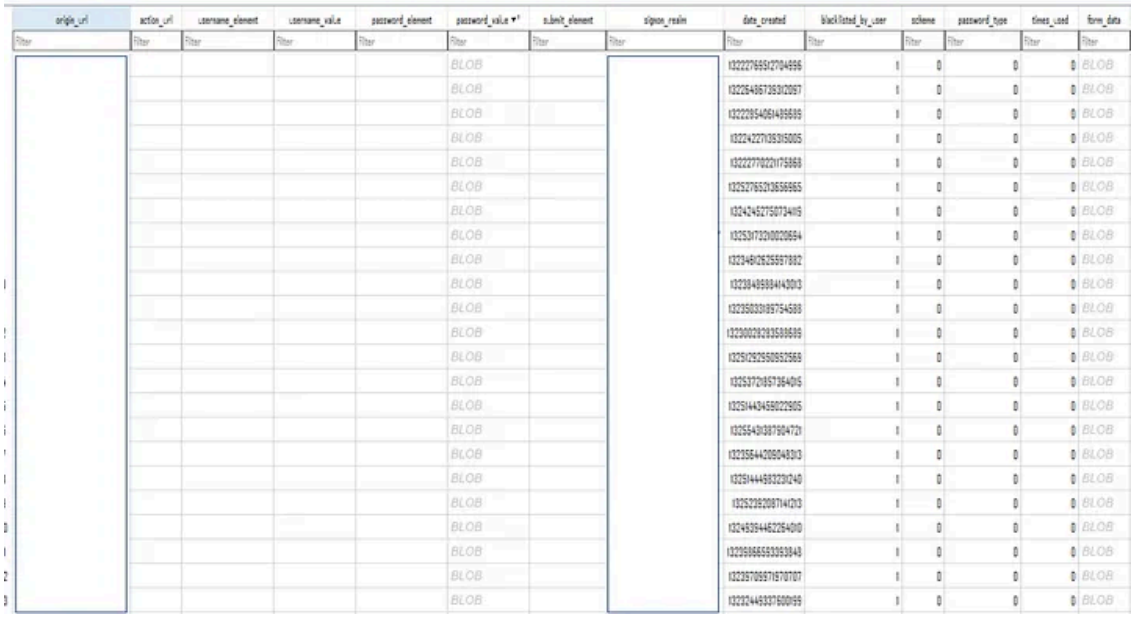
#Additional Malware Download

How Stealers Steal Data

Chrome and other browsers based on the Chromium engine (Opera, Yandex, etc.) store sensitive data in the same location in general.

Stealer can steal information stored in the browser by performing decryption with the user's authority. In the case of Chrome, the credential information is normally encrypted and stored in SQLite format if the user chooses the option to save the login information. If the user revisits the site, chrome browser will decrypt the information stored in the SQLite database with user's authority which the malware can do the same.

Press enter or click to view image in full size



Example of Imported Login Data of Chrome Browser to SQLite

4. Stolen Information evidenced in DDW (Deep, Dark Web)

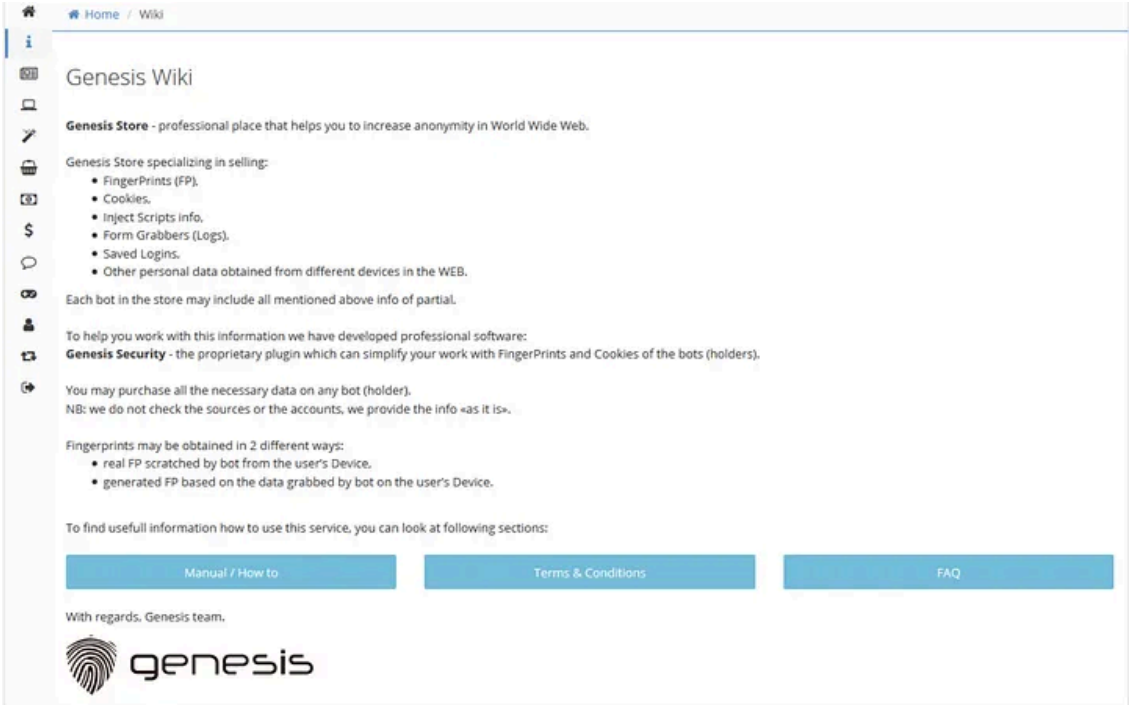
Information obtained fraudulently by stealers are often observed in three areas.

1) Botnet Market

Genesis Market is known to be the biggest dark web market specialty in followings:

- FingerPrints(FP)
- Cookies
- Inject Scripts info
- Form Grabbers (Logs)
- Saved Logins
- Other personal data obtained from different devices in the web

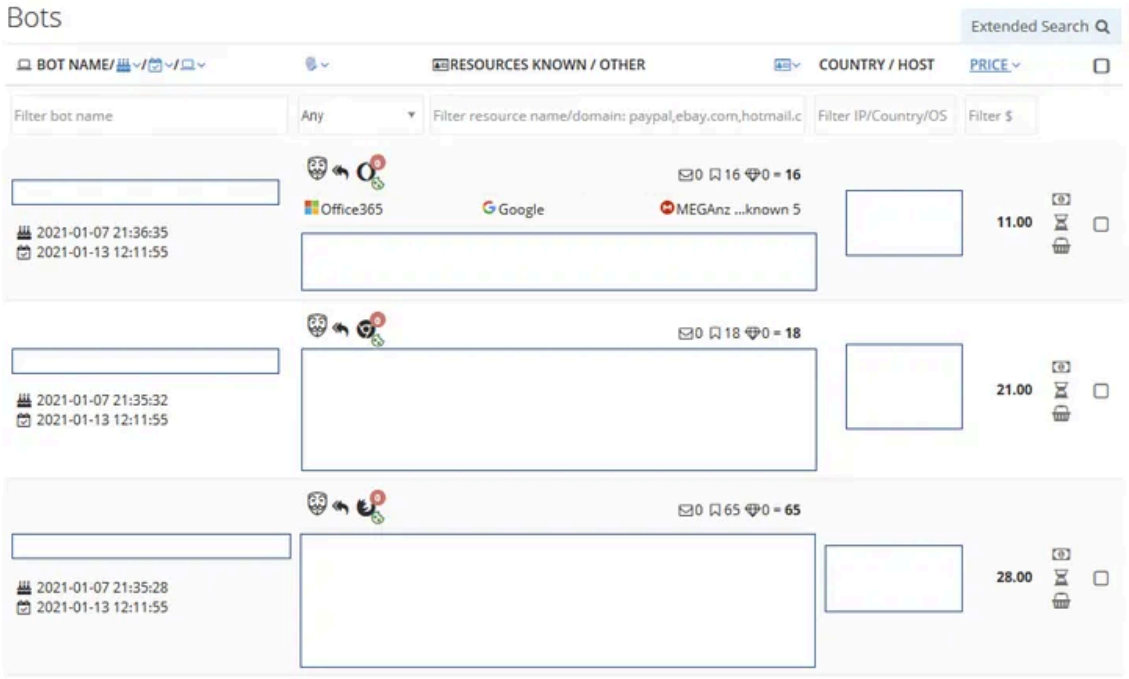
Press enter or click to view image in full size



Main page of genesis market

Bots are sold in following format:

Press enter or click to view image in full size



The price of each product seems to fluctuate substantially depending on the importance of cookies and its quantity. The average price of product usually positioned from $10~$30 as seen in the above picture. However, if the number of cookies is sufficient and its information is highly relevant to financial accounts, the price may take up to $350.

Press enter or click to view image in full size

2) Carding forum

A perfect example of carding site is ‘Joker’s stash’ but the operator of Joker’s stash claims to leave for a retirement a month after the domain seizure taken by FBI and Interpol. https://threatpost.com/jokers-stash-carding-site-taken-down/162548/

Despite the absence of Joker’s Stash, there are still flooding number of carding sites in Russian speaking forums selling credit card information. There can be many other techniques to obtain credit card information from the victim’s device, and stealers will do such a thing to collect all the credit card information viciously to be dumped and sold on carding forums.

3) Hacking forum

The stealers’ logs are not just sold in the carding forums and botnet markets but they are often shared in closed Russian speaking hacking forums. The below picture is posted this early week 1st of February, 2021, titled ‘858 LOGS MIX WORLDWIDE FOR FREE 2020’. These logs are often shared without compensations, and the size of logs files can range from couple of MBs to tens of GBs.

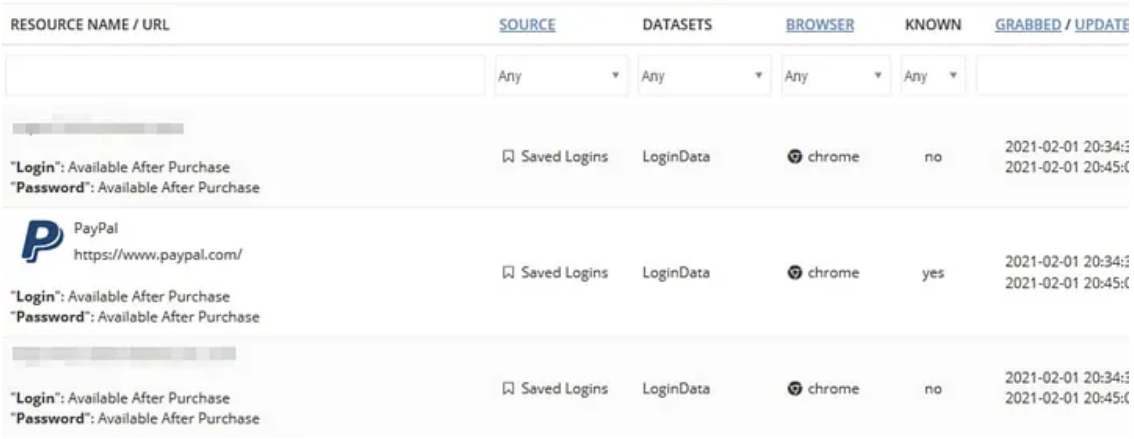
Press enter or click to view image in full size

5. Where to use?

Based on our research, there are three assumptions of buying and sharing stealer logs.

1. **Finding any financial related accounts such as paypal login information in order to get a fraudulent access to the account.**

   Press enter or click to view image in full size



RESOURCE NAME / URL	SOURCE	DATASETS	BROWSER	KNOWN	GRABBED / UPDATE
	Any	Any	Any	Any	
"Login": Available After Purchase "Password": Available After Purchase	Saved Logins	LoginData	chrome	no	2021-02-01 20:34: 2021-02-01 20:45:(
PayPal https://www.paypal.com/ "Login": Available After Purchase "Password": Available After Purchase	Saved Logins	LoginData	chrome	yes	2021-02-01 20:34: 2021-02-01 20:45:(
"Login": Available After Purchase "Password": Available After Purchase	Saved Logins	LoginData	chrome	no	2021-02-01 20:34: 2021-02-01 20:45:(

In Genesis market, it is not hard to find a Paypal login information which stored in the chrome browser. Detail information can be seen after purchasing the product.

A picture below is a sample of pay account found in the stealer logs which was shared on an Russian speaking hacking forum.

Press enter or click to view image in full size

It may require many tries to find an account with big valid budgets, but the activity of sharing botnet/stealers logs doesn’t seem to decrease.

2. Stealing corporate login information of the victim trying to access to its corporate portal remotely

We have observed many urls that are seem to be corporate related accounts such as azure or aws, cloud-like accounts.

Adversary favours the accounts named ‘administrator’ OR ‘admin’ will likely be attempted with brute force attack.

3. Information gathering at a national level

In Genesis market, there is a dashboard showing the list of current bots per country and how many have been added. Since the bots are classified with the country code, adversary or the ‘client’ can have an intuitive view of victims by country. In this sense, the information can be efficiently collected if the user is targeting specific country or language.

Available Bots

COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
219	+547	+3353	+39093	354059
Groupped by				
US	+80	+434	+5484	14311
IT	+66	+372	+4583	48896
ES	+45	+370	+3945	32711
FR	+40	+258	+3280	36603
RO	+23	+196	+2420	15047
PL	+32	+220	+2410	12126
AR	+50	+228	+2218	10018
CL	+17	+131	+1552	4559
PT	+33	+186	+1545	21188
HU	+18	+119	+1269	8072
CA	+10	+60	+1212	2908
GR	+10	+99	+1135	4988
NL	+16	+91	+1065	7014
NP	+13	+64	+942	4892
BE	+15	+79	+855	6330
AU	+10	+48	+692	3423
BG	+7	+57	+630	3721
SK	+6	+53	+531	2310
HR	+11	+53	+525	2118

Source: https://medium.com/s2wlab/w1-feb-en-story-of-the-week-stealers-on-the-darkweb-49945a31601d