2easy now a significant dark web marketplace for stolen data

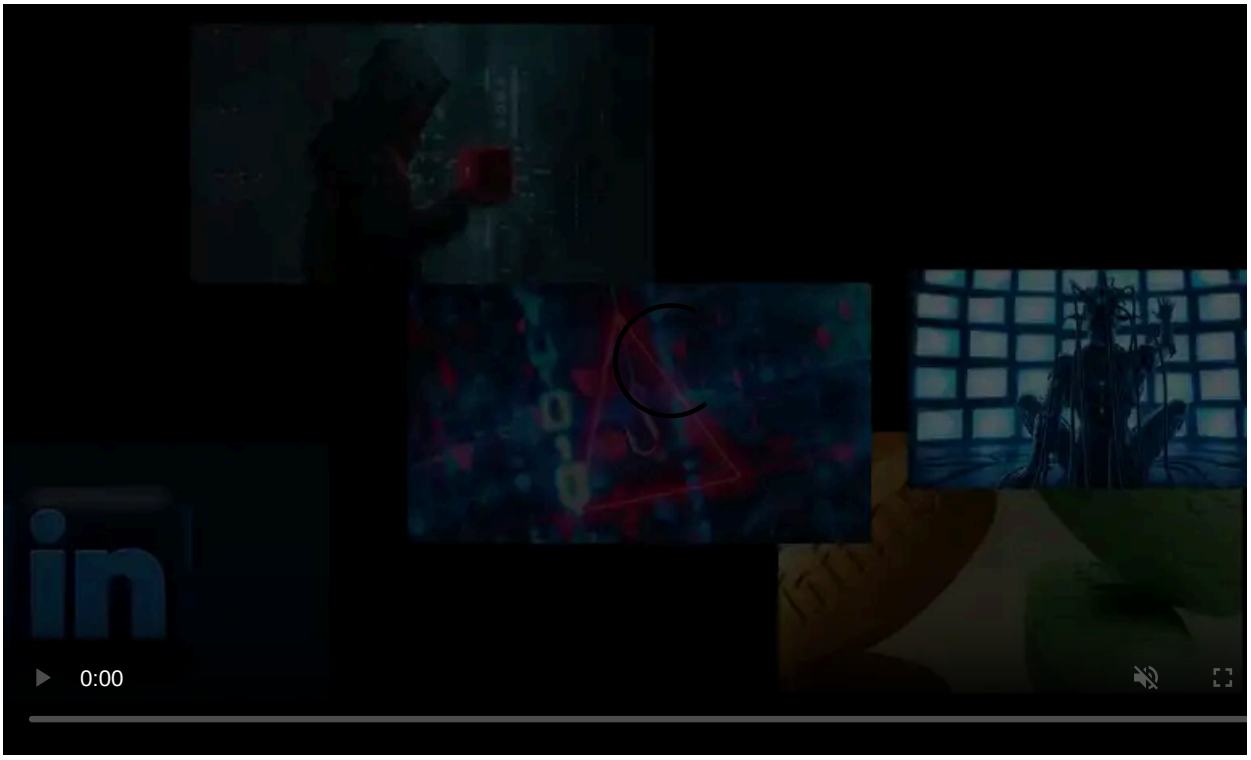
By Bill Toulas

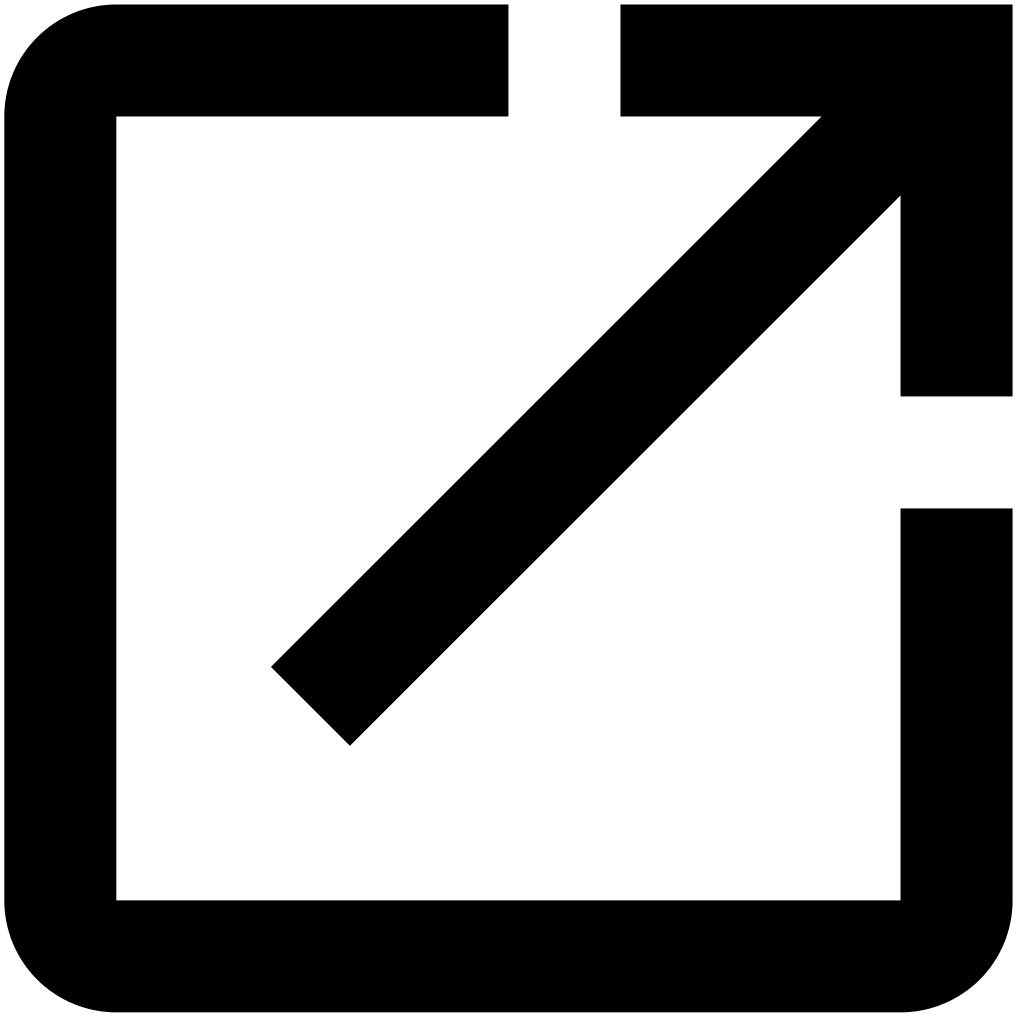
Published: 2021-12-21 · Archived: 2026-04-05 18:27:17 UTC

A dark web marketplace named '2easy' is becoming a significant player in the sale of stolen data "Logs" harvested from roughly 600,000 devices infected with information-stealing malware.

"Logs" are archives of data stolen from compromised web browsers or systems using malware, and their most important aspect is that they commonly include account credentials, cookies, and saved credit cards.

2easy launched in 2018 and has experienced rapid growth since last year when it only sold data from 28,000 infected devices and was considered a minor player.


0:00



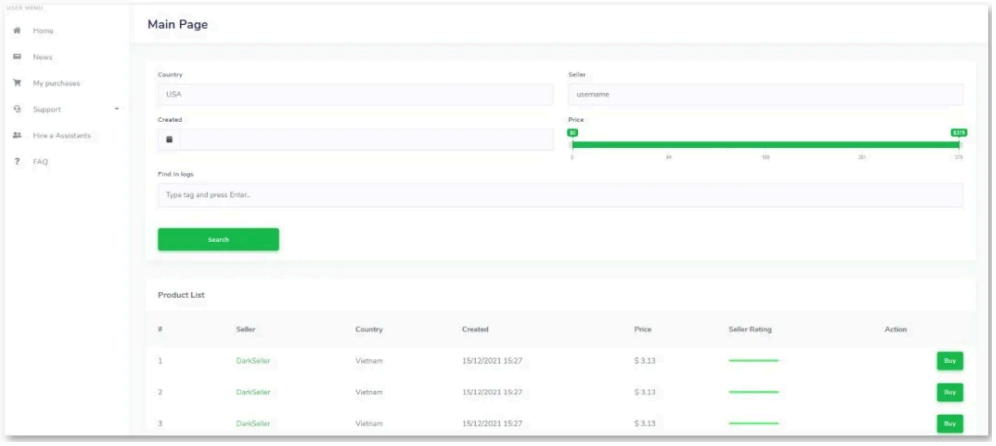
Based on an analysis by researchers at Israeli dark web intelligence firm KELA, the sudden growth is attributed to the market's platform development and the consistent quality of the offerings that have resulted in favorable reviews in the cybercrime community.

Cheap and valid logs

The market is fully automated, which means someone can create an account, add money to their wallets, and make purchases without interacting with the sellers directly.

The logs are made available for purchase for as low as $5 per item, roughly five times less than the average Genesis prices and three times less than the average cost of bot logs on the Russian Market.

Moreover, based on actor feedback analysis from multiple dark web forums, 2easy logs consistently offer valid credentials that provide network access to many organizations.



The 2easy homepage as seen in December 2021
Source: KELA

Besides the cost and validity, 2easy's GUI is user-friendly and powerful at the same time, enabling actors to perform the following functions on the site:

- view all URLs to which the infected machines logged in
- search URLs of interest
- browse through a list of infected machines from which credentials to said website were stolen.
- check the seller's rating
- review tags assigned by sellers, which most times include the date the machine was infected and sometimes additional notes from the seller
- acquire credentials to selected targets

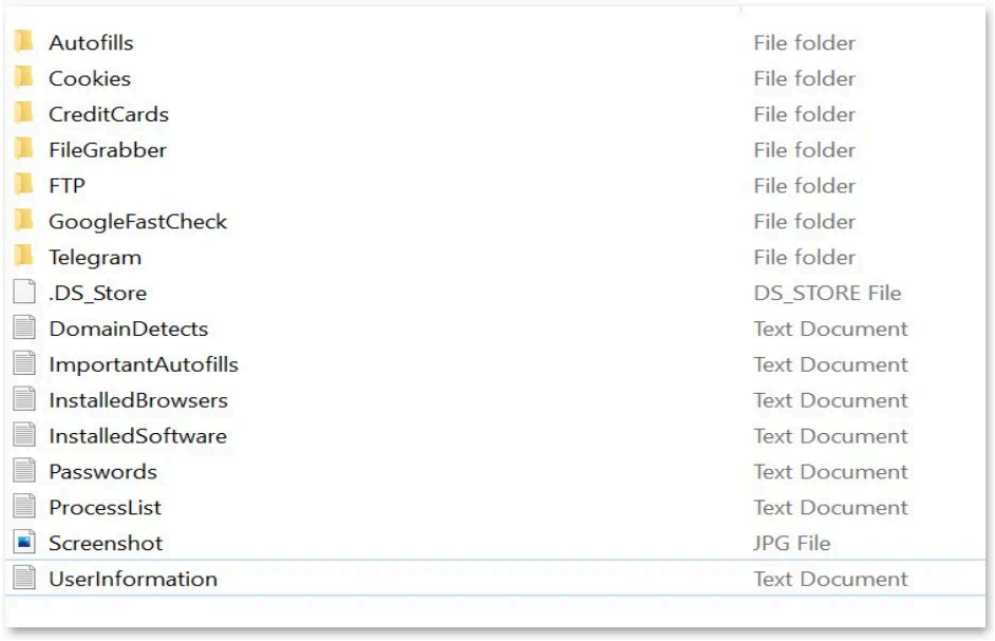
The only downside compared to other platforms is that 2easy doesn't give prospective buyers a preview of a sold item, such as the redacted IP address or OS version for the device the data was stolen.

The RedLine plague

Each item purchased on 2easy comes in an archive file containing the stolen logs from the selected bot.

The content-type depends on the info-stealing malware used for the job and its capabilities, as each strain has a different focus set.

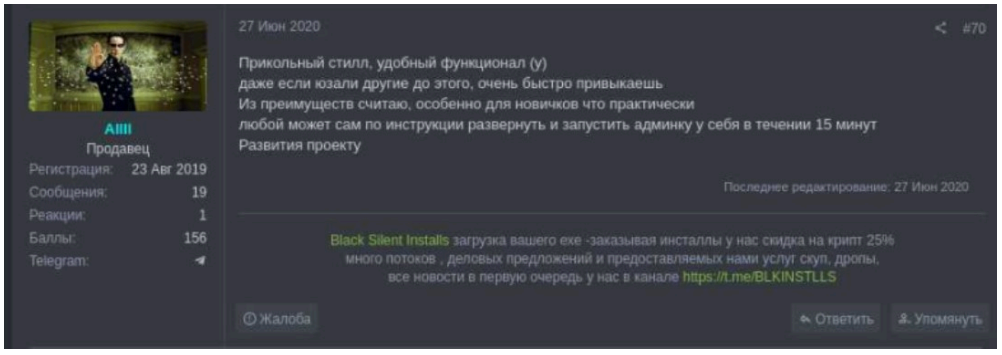
However, in 50% of the cases, the sellers use RedLine as their malware of choice, which can steal passwords, cookies, credit cards stored in web browsers, FTP credentials, and more, as shown below.



Purchased RedLine log archive contents

Source: KELA

Five out of the 18 sellers active on 2easy use RedLine exclusively, while another four use it in conjunction with other malware strains like Raccoon Stealer, Vidar, and AZORult.



A 2easy seller praising the simplicity of RedLine

Source: KELA

Why this is important

Logs containing credentials are essentially keys to doors, whether those doors lead to your online accounts, financial information, or even entry to corporate networks.

Threat actors sell this information for as little as $5 per piece, but the damage incurred to compromised entities could be counted in the millions.

"Such an example can be observed through the attack of Electronic Arts that was disclosed in June 2021," explains KELA's report

"The attack reportedly began with hackers who purchased stolen cookies sold online for just $10 and continued with hackers using those credentials to gain access to a Slack channel used by EA."

“Once in the Slack channel, those hackers successfully tricked one of EA’s employees to provide a multi-factor authentication token, which enabled them to steal multiple source codes for EA games.”

BOT GUID	SERVICE	UPDATE DATE	SOURCE
1639315099...	lana-na/auth/url_default/welcome.cgi	Dec 12th, 2021	TwoEasy
1639315099...	nings.com.au/dana-na/auth/url_14/welcome.cgi	Dec 12th, 2021	TwoEasy
1639314739f...	erlin.es/dana-na/auth/url_3/welcome.cgi	Dec 12th, 2021	TwoEasy
1639314644...	dana-na/auth/url_default/welcome.cgi	Dec 12th, 2021	TwoEasy
1639251934...	/dana-na/auth/url_c62kDNs6aEy6oEIA/welcome.cgi	Dec 11th, 2021	TwoEasy
1639251729...	/dana-na/auth/url_default/welcome.cgi	Dec 11th, 2021	TwoEasy
1639251729...	rg/dana-na/auth/url_xzcMQy72FQcqcl3N/welcome.c...	Dec 11th, 2021	TwoEasy
1639172265...	n.sa/dana-na/auth/url_default/welcome.cgi	Dec 11th, 2021	TwoEasy
1638564572...	2.nc.us/dana-na/auth/url_23/welcome.cgi	Dec 4th, 2021	TwoEasy
1638564572...	o/dana-na/auth/url_93/welcome.cgi	Dec 4th, 2021	TwoEasy
1638564572...	us/dana-na/auth/url_1/welcome.cgi	Dec 4th, 2021	TwoEasy
1638564026...	dana-na/auth/url_MdthkS45mn6vhz3O/welcome.cgi	Dec 4th, 2021	TwoEasy
1638563824...	om.my/dana-na/auth/url_default/welcome.cgi	Dec 4th, 2021	TwoEasy
1638563736...	ma/dana-na/auth/url_default/welcome.cgi	Dec 4th, 2021	TwoEasy

Pulse Secure VPN credentials available through 2easy
Source: KELA

The initial access broker market is on the rise and is directly linked to catastrophic ransomware infections, while log marketplaces like 2easy are a part of the same ecosystem.

Millions of account credentials are offered for purchase on the dark web, so appropriate security measures that treat accounts as potentially compromised are needed.

Examples of those measures include multi-factor authentication steps, frequent password rotation, and applying the principle of least privilege for all users.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
