2easy: Logs Marketplace on the Rise

KELA Cyber Intelligence Center

As part of KELA's continuous monitoring of communities and markets in the cybercrime underground, KELA identified a rise in the activity of a relatively new market of stolen user information, called "2easy". The market is an automated platform where different actors sell "logs" – data and browser-saved information harvested from machines (bots) all over the world infected with information-stealing malware. Currently, the market offers information stolen from almost 600,000 bots.

Based on analysis of the data collected by KELA's systems from this market, as of December 2021, the market hosts 18 sellers offering their infostealer logs for sale. Investigation of these sellers' activities in the cybercrime underground, as well as feedback about the market posted to dark web sources, indicates that the market has a certain recognition among cybercriminals that deal with stolen credentials; they provide mostly positive feedback. As such, KELA assesses that credentials sold in 2easy are generally valid and may present a direct threat to organizations. KELA's analysis of the market finds that RedLine information stealing malware is the most popular choice for the market's vendors – with over 50% of the machines offered for sale on the market being infected with RedLine.

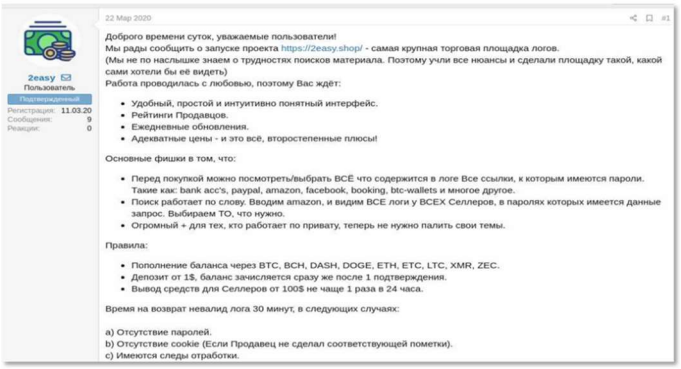
The Market: Background, Prices, and Features

KELA identified that 2easy's administrators have been advertising the market in various Russian-speaking hacking forums since March 2020. Based on the claims of the actors behind 2easy, the market is operating from 2019, though only in 2021 it has started to significantly grow. Domain registration records support the claimed operations start date – it was registered in the end of 2018 and is currently hosted by a Ukrainian provider that is also advertised in cybercrime communities.

In 2021, updates were also implemented by 2easy developers. While in July 2020 the market offered access to logs harvested from 28,000 bots, it currently boasts logs from almost 600,000 bots.

Compared to prices on two other infamous markets, Genesis and Russian Market, 2easy lists relatively cheap bots – with most of them having prices below USD 5.

On Genesis, during the past year, most of the bots were offered for USD 5-25, and on Russian Market – for USD 10-15.

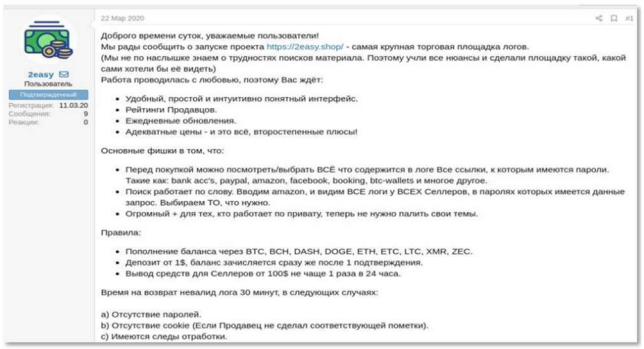


One of the first advertisements of 2easy botnet market, posted on a Russian-speaking cybercrime forum Dublikat

The market's GUI enables its users to:

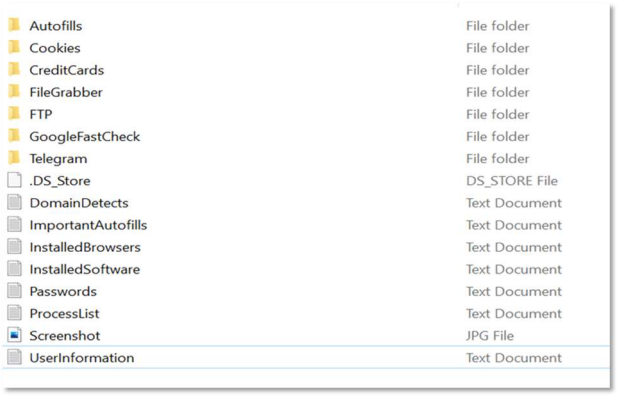
- View all URLs to which the infected machines logged in.
- Search URLs of interest.
- Browse through a list of infected machines from which credentials to said website were stolen.
- Check the seller's rating.
- Review tags assigned by sellers, which most times include the date the machine was infected and sometimes additional notes from the seller.
- Acquire credentials to selected targets.

However, unlike other botnet markets KELA monitors, very little information about the victim is available prior to the purchase (e.g., no redacted IP address or OS version).



2easy's homepage

When a bot is purchased, a buyer receives an archived (zipped) file containing folders and files with stolen data and information about the bot: saved credentials and credit cards, a list of installed browsers and software, a list of processes, user information, some files, and more. The type of data the buyer gets depends on the capabilities of infostealers used; different malware strains may be focused on stealing various types of data.

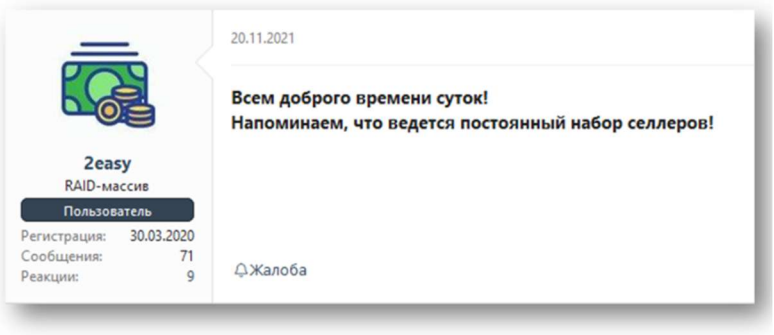


Folder with information from a bot compromised by RedLine as received from "2easy"

As other markets of this kind, 2easy offers an option to refund purchases if they are of bad quality – namely they do not contain passwords and cookies (if it was not specified prior to the purchase). Purchases can also be refunded if there are traces that these logs have been previously used by other cybercriminals, which is apparently a measure to prevent reselling of logs from other markets or providers on 2easy.

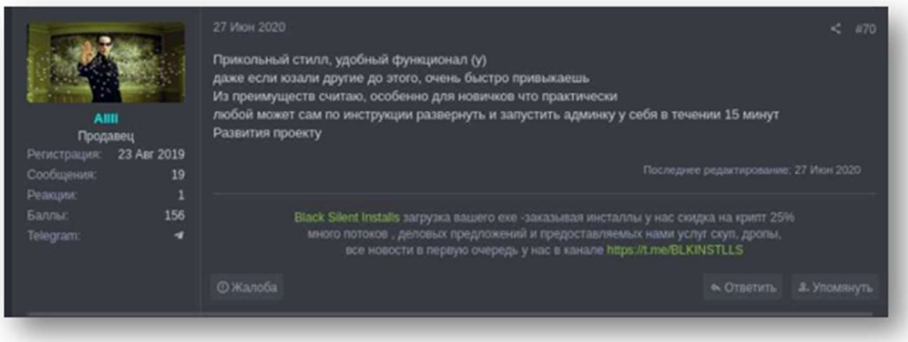
The Sellers and their Malware

2easy frequently advertises an opportunity to join the market as a seller. Based on 350,000 bots that were processed by KELA's systems for this analysis, the market has 18 sellers, with the top 4 sellers offering almost 94% of all bots listed on the market. Moreover, the most active actor named DarkSeller sells logs harvested from almost 60% of all 2easy bots.



Un *A representative of 2easy claims the market constantly recruits Sellers*

Analyzing the data collected by KELA's threat intelligence platform from the market, a unique piece of information was identified that makes it evident that 50% of the detected bots included information stolen by the RedLine infostealer. However, only 5 of the sellers use it exclusively, while 4 others appear to leverage other malware as well. For example, DarkSeller was also seen using Raccoon, another public stealer popular among cybercriminals.



A 2easy seller called ALLLL identified by KELA as a user dubbed Allll on the BDF forum leaves positive feedback confirming his usage of the RedLine stealer: "Nice stealer, usable functionality. <…> One of the advantages, especially for the beginners, is that instructions allow everyone to deploy admin panel in 15 minutes"

KELA researched the top sellers on 2easy and identified some of them as being active or discussed as sellers on several Russian-speaking forums, such as XSS, Exploit, LolzTeam, and others.

While they did not reveal other malware used by them, some of them were seen using additional services that facilitate the theft of information.

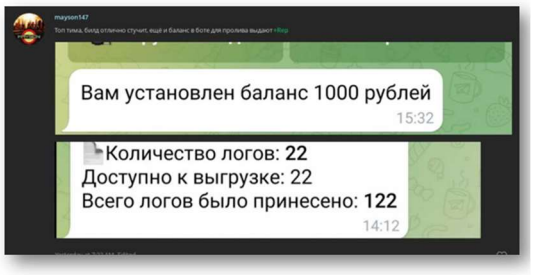
KELA researched the top sellers on 2easy and identified some of them as being active or discussed as sellers on several Russian-speaking forums, such as XSS, Exploit, LolzTeam, and others. While they did not reveal other malware used by them, some of them were seen using additional services that facilitate the theft of information.

For example, the 2easy seller Mayson_logs – identified by KELA as using the handle mayson147 on other communities – was observed using a service named “Univer City”, which apparently provides access to infostealers, as well as means to distribute them. It is not clear if “Univer City” provides some private stealers or commodity stealers, such as RedLine. Mayson_logs, in its turn, was observed using both RedLine and other infostealers as well, so both options are possible. “Univer City” also provides a way to massively distribute malicious files through disseminating malicious links via YouTube video descriptions, which may hint that Mayson_logs uses it as an initial infection vector.

Interestingly, “Univer City” appropriates logs related to Google Pay, which means that users of this service can no longer sell or leverage them. Apparently, “Univer City” uses these logs for further malicious actions. KELA is familiar with other services working on similar conditions and possibly used by some sellers of 2easy. The assessment stems from the fact that several 2easy users claim in tags that some specific type of resources (in most cases, cryptocurrency wallets) were “worked out”. This means that if credentials to such resources are contained in logs, they will not be valid, which can occur due to several reasons:

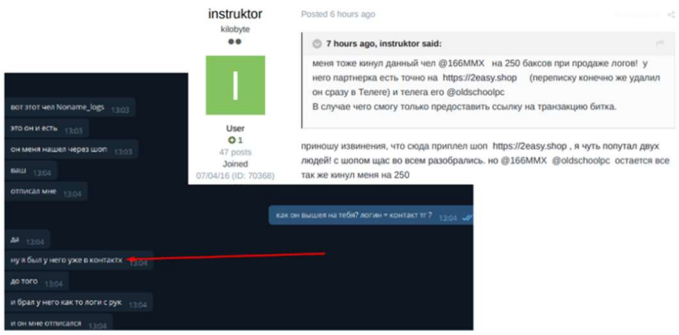
- The seller used a service similar to “Univer City” and gave away specific logs to the service.

- The seller bought the logs from another cybercriminal who had already used them.
- The seller used specific logs for his own malicious activities. For example, ALLLL was seen using a tool named StealerLogSearcher and intended for searching specific resources in stolen logs.



Mayson_logs identified as mayson147 on LolzTeam gives positive feedback to "Univer City"

As for the reputation of 2easy sellers, KELA observed scam accusations, but they proved to be inaccurate, according to the accusers themselves. For example, a user named 166MMX was accused of scam and directly associated with the market user Noname_logs. However, further investigation showed that a user who accused this actor of scamming mistakenly connected two different users.



Un usuario llamado instruktor primero asocia el usuario 166MMX con Noname_logs de 2easy, pero luego admite que se equivocó

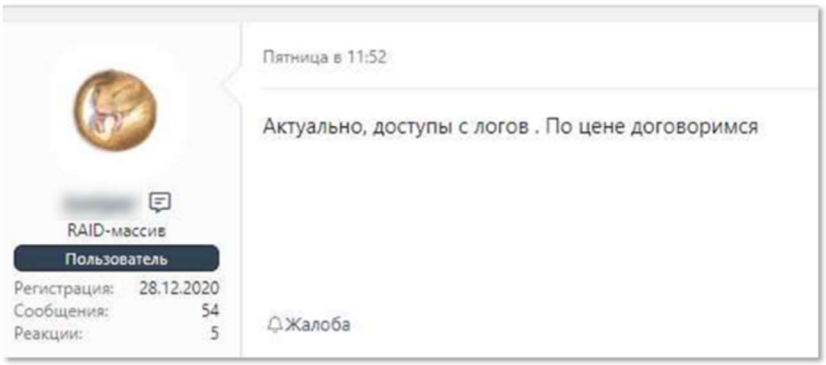
Therefore, KELA assesses that sellers on 2easy appear to be credible, albeit relatively low level, actors – using commodity infostealers and, at least in some cases, third-party services for spreading and management of their malware. KELA did not observe chatter massively accusing 2easy or its sellers of scam, though some users complained about invalid information in the logs. KELA will continue to monitor the market to further research the legitimacy of its offers.

Why is it So Important?

KELA monitors various botnet market sources, such as 2easy, which sell access to data from machines infected with information-stealing trojans such as RedLine, AZORult, Vidar, Racoon, and others. These machines contain saved credentials and personal information belonging to either employees, clients, or partners. These credentials constitute a cheap and easy-to-get possible initial entry point to an organization's network.

Such an example can be observed through the attack of Electronic Arts that was disclosed in June 2021. 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 multifactor authentication token, which enabled them to steal multiple source codes for EA games.

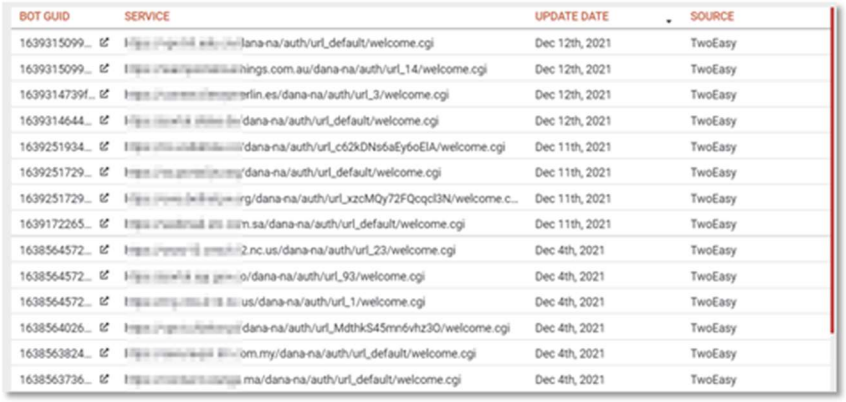
KELA also observed logs being leveraged to gain network access – a term that refers to remote access to a computer in a compromised organization. Threat actors selling these accesses are referred to as Initial Access Brokers (IABs). Some of them explicitly say they obtain network access they trade from logs.



A post from an IAB on a cybercrime forum: "relevant, accesses from logs. Will agree on a price"

When searching for network access types popular among IABs in logs traded on 2easy, KELA discovered the following results (meaning that logs contain credentials to these URLs):

- 2,480 login pages for Pulse Secure VPN
- 2,261 login pages for various VPN products
- 637 login pages for Citrix ADC (formerly NetScaler ADC)
- 499 login pages for Cisco ASA WebVPN
- 332 login pages for RDWeb
- 206 login pages for Global Protect VPN



BOT GUID	SERVICE	UPDATE DATE	SOURCE
1639315099...	lana-na/auth/url_default/welcome.cgi	Dec 12th, 2021	TwoEasy
1639315099...	hings.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 login appearances in logs from 2easy, as seen in KELA's DARKBEAST threat intelligence platform

Considering the crucial role that IABs play in the Ransomware-as-a-Service (RaaS) ecosystem, linking opportunistic attacks with targeted ones, monitoring markets as 2easy becomes crucial as it may help to interrupt this supply chain at the beginning.

Hence, if purchased by threat actors, the stolen credentials represent a considerable cyber risk to the organization, as the actors may leverage this access to perform a lateral movement to compromise multiple computers across the organization's network. This may result in various types of malicious activities, such as exfiltrating sensitive data of the organization and its clients, as well as in deploying different malware, like ransomware.