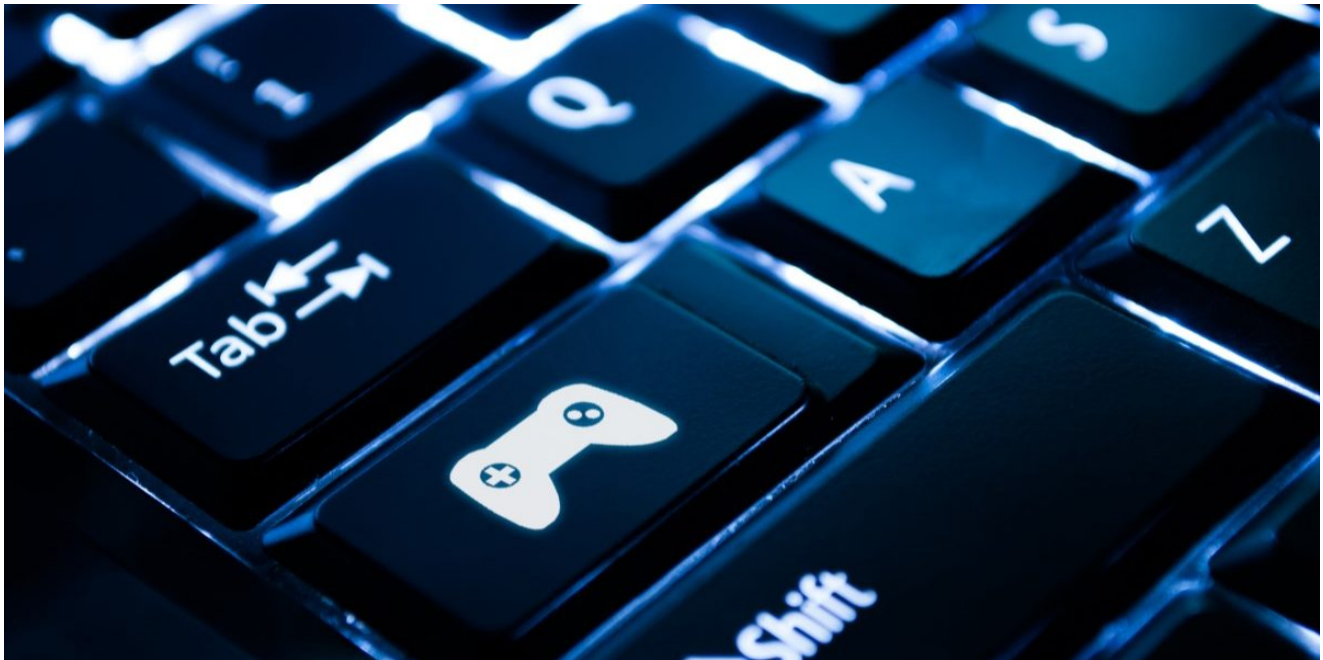





BloodyStealer and gaming assets for sale

SL securelist.com/bloodystealer-and-gaming-assets-for-sale/104319/



Authors

-  [Leonid Bezvershenko](#)
-  [Dmitry Galov](#)
-  [Marc Rivero](#)

Part 2 of gaming-related cyberthreat report

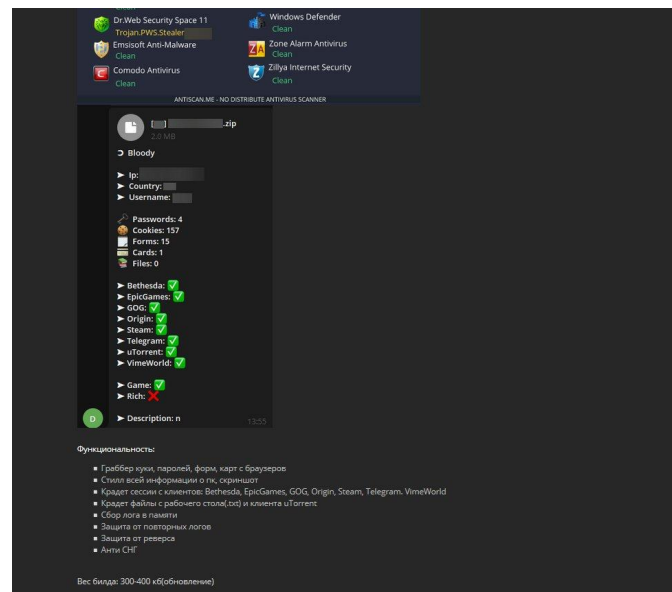
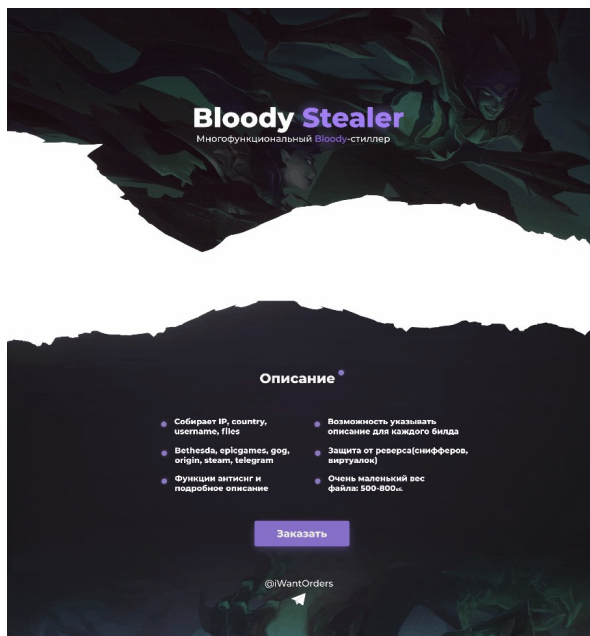
Earlier this year, we [covered the threats related to gaming](#), and looked at the changes from 2020 and the first half of 2021 in mobile and PC games as well as various phishing schemes that capitalize on video games. Many of the threats faced by gamers are associated with loss of personal data, and particularly, accounts with various gaming services.

This tendency is not unique to PC or mobile games or to the gaming industry as a whole. Nevertheless, as games offer users plenty of in-game goodies and even feature their own currencies, gaming accounts are of particular interest to cybercriminals.

In this report, we take a closer look at threats linked to loss of accounts with popular video game digital distribution services, such as Steam and Origin. We also explore the kind of game-related data that ends up on the black market and the prices.

Background

In March 2021, we noticed an advertisement for malware named “BloodyStealer” on a Russian-speaking underground forum. According to the ad, BloodyStealer was a malicious stealer capable of fetching session data and passwords, and cookie exfiltration, and protected against reverse engineering and malware analysis in general. A buyer can use Telegram channels as well as traditional web panels for communication with the C&C. The author offered potential customers to get in touch via Telegram. The price of BloodyStealer is 700 RUB (less than \$10) for one month or 3000 RUB (approx. \$40) for lifetime.



The BloodyStealer ad (Source: <https://twitter.com/3xp0rtblog>)

The ad highlights the following features of BloodyStealer (translated from Russian as is):

- *Grabber for cookies, passwords, forms, bank cards from browsers*
- *Stealer for all information about the PC and screenshots*
- *Steals sessions from the following clients: Bethesda, Epic Games, GOG, Origin, Steam, Telegram, VimeWorld*
- *Steals files from the desktop (.txt) and the uTorrent client*
- *Collects logs from the memory*
- *Duplicate logging protection*

- *Reverse engineering protection*
- *Not functional in the CIS*

What caught our attention is BloodyStealer's capability to fetch information related to computer games installed on an infected system. BloodyStealer targets major online gaming platforms, such as Steam, Epic Games Store, EA Origin, etc.

At the time of our investigation, the forum thread related to BloodyStealer was publicly unavailable, but the analysis of visible information on the forum revealed that discussions relating to BloodyStealer still continued in private channels. This, along with the fact that visible stealer activity had been observed since its release, suggested that the threat actor behind BloodyStealer had decided to offer its product only to VIP members of underground forums.

Kaspersky products detect the threat as Trojan-Spy.MSIL.Stealer.gen. For additional technical information about BloodyStealer (malicious techniques, YARA rules, etc.), please contact financialintel@kaspersky.com.

BloodyStealer technical details

Anti-analysis

During our research, we were able to identify several anti-analysis methods that were used to complicate reverse engineering and analysis of BloodyStealer, including the usage of packers and anti-debugging techniques. As the stealer is sold on the underground market, every customer can protect their sample with a packer of their choice or include it into a multistage infection chain. We had been monitoring BloodyStealer since its announcement, so we were able to notice that the majority of the BloodyStealer samples were protected with a commercial solution named "AgileNet".

While analyzing samples discovered in the wild, we found that some of them were protected not only with AgileNet but also with other, very popular, protection tools for the .NET environment, such as Confuser.

Victim identification, communication with the C&C and data exfiltration

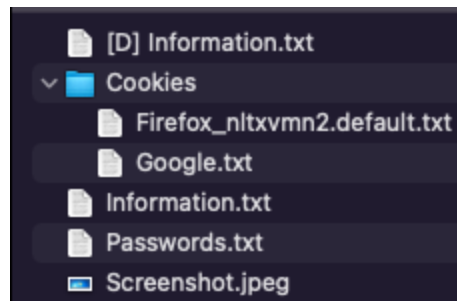
BloodyStealer is capable of assigning a unique identifier to every infected victim. The identifier is created by extracting data, such as the GUID and serial number (SID) of the system. This information is extracted at runtime. Besides this identification, BloodyStealer extracts the public IP address of the C&C by requesting the information from the domain [whatleaks\[.\]com](http://whatleaks[.]com).

```
GET / HTTP/1.1
Host: whatleaks.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Sat, 29 May 2021 20:55:43 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

The request used to get the public IP

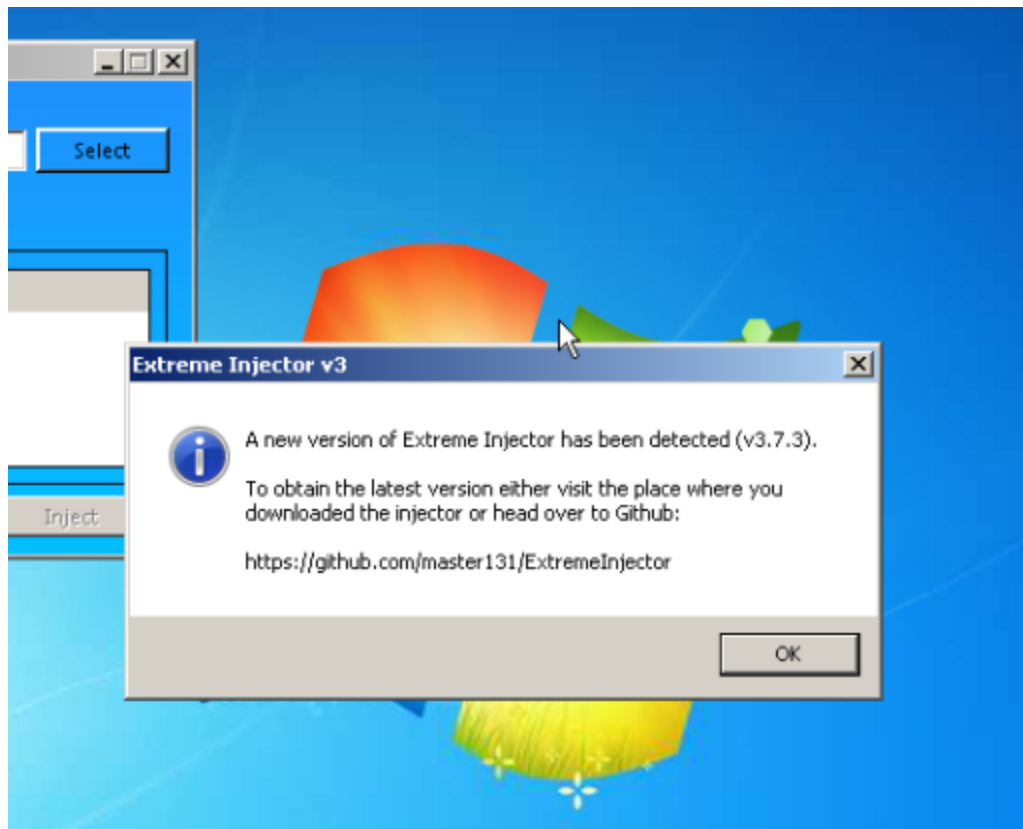
After assigning a UID to the victim and getting the C&C IP address, BloodyStealer extracts various data from the infected machine, creates a POST request with information about the exfiltrated data, and sends it to the malicious C&C. The data itself is sent to the configured C&C server later as a non-protected ZIP archive and has the structure shown below.



The IP address configured in the infected system is used as the name of the ZIP archive.

BloodyStealer as part of a multistage infection chain

In our analysis of BloodyStealer samples, we found out how various threat actors who had acquired this product decided to use the stealer as a part of other malware execution chains, for example, KeyBase or Agent Tesla. The criminals who combined the stealer component with other malware families also protected BloodyStealer with other packers, such as Themida.

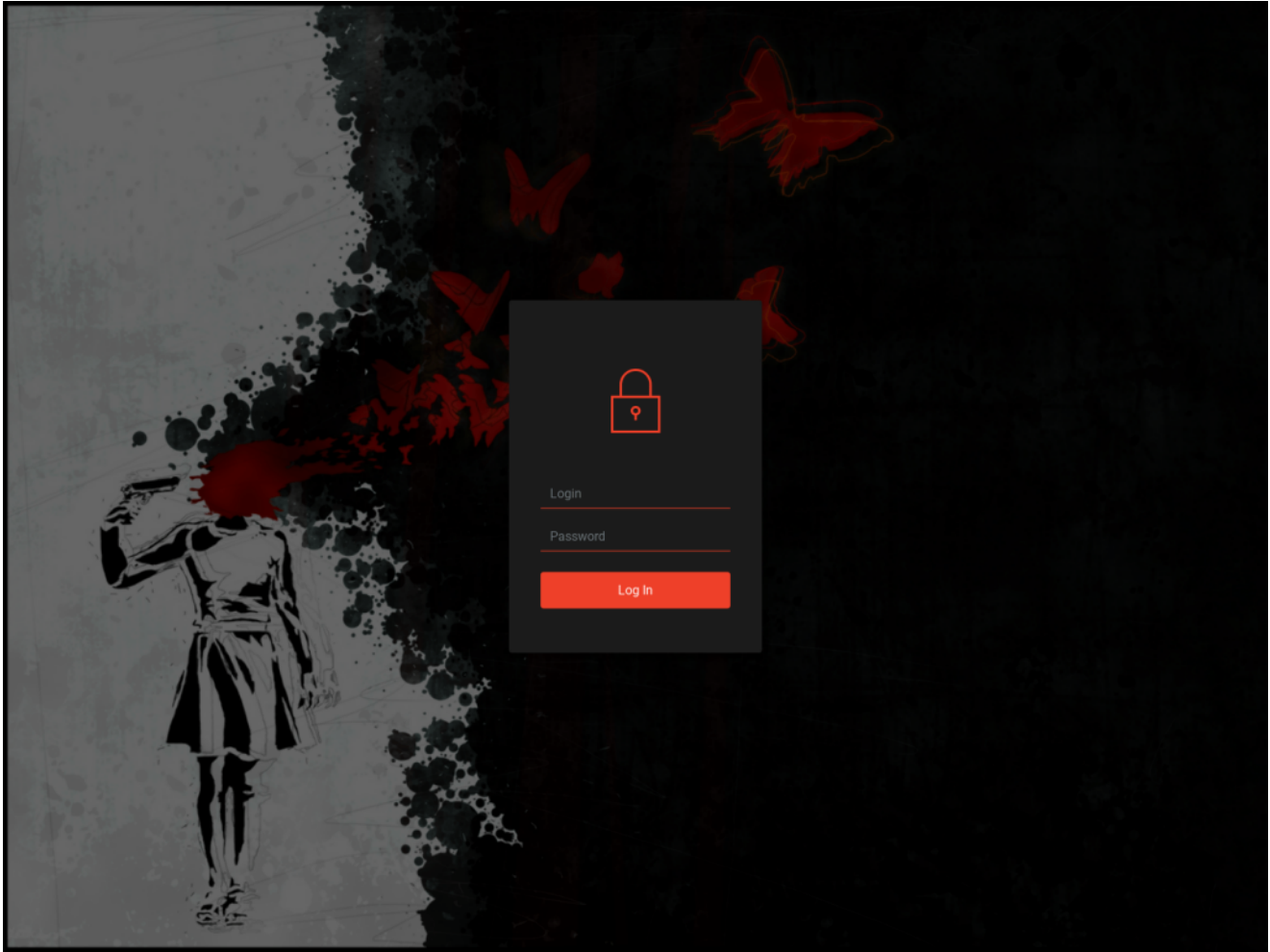


BloodyStealer as used alongside other malware families or hacking tools

Based on the price that BloodyStealer is fetching on the underground market, we can expect that it will be used in combination with other popular malware families.

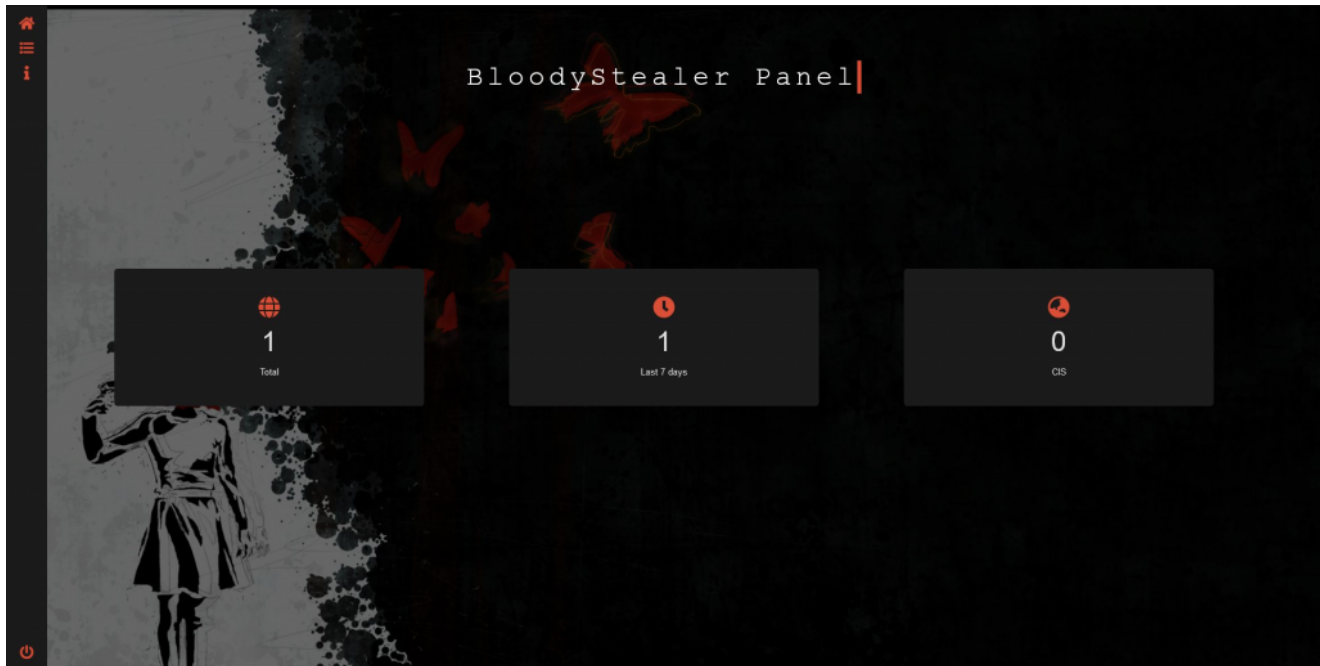
Command and Control

As mentioned above, BloodyStealer sends all exfiltrated data to a C&C server. Cybercriminals can access the data by using Telegram or via a web panel. The collected data can then be sold to other cybercriminals, who in turn will try to monetize it.



BloodyStealer C&C login page (Source: <https://twitter.com/3xp0rtblog>)

When a criminal is logged in to the C&C web panel, they will see a basic dashboard with victim-related statistics.



BloodyStealer stats dashboard (Source: <https://twitter.com/3xp0rtblog>)

While pivoting through the structure used for allocating the content panel, we were able to identify the second C&C server located at

`hxxp://gwrq23445b235245ner.mcdi[r.]me/4/654/login.php`

Both C&C servers are placed behind Cloudflare, which hides their original IPs and provides a layer of protection against DDoS and web attacks.

Victimology

BloodyStealer is still quite new on the market when compared to other existent malware tools; however, by analyzing available telemetry data, we have found detections of BloodyStealer in Europe, Latin America and the APAC region. At the time of the investigation, we observed that BloodyStealer mostly affected home users.

Next links in the chain: darknet markets

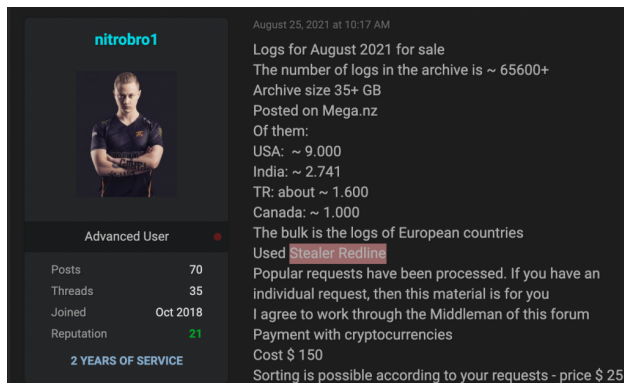
Unfortunately, BloodyStealer is just one example of stealers targeting gamers. With many more in use, cybercriminals gather a significant number of game-related logs, login credentials, and other data, spurring a well-developed supply and demand chain for stolen credentials on the dark web. In this section, we will dig deeper into the dark gaming market and look at the types of game-related items available there.

Our experts, who specialize in understanding what goes on on the dark web, conducted research on the current state of user data as a commodity on these platforms to find out what kind of personal data is in demand, what it is used for, and how much it costs. For the

purposes of this report, we analyzed active offers on twelve international darknet forums and marketplaces that use English or Russian.

Wholesale deals

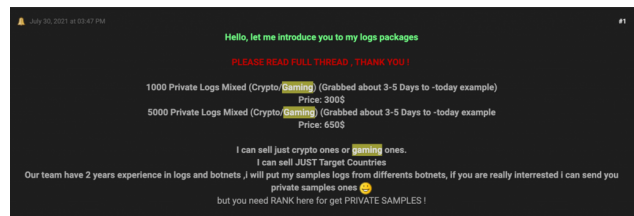
Dark web sellers provide a broad variety of goods, sold both wholesale and retail. Specifically, one of the most popular wholesale products is logs.



nitrobro1
August 25, 2021 at 10:17 AM

Logs for August 2021 for sale
The number of logs in the archive is ~ 65600+
Archive size 35+ GB
Posted on Mega.nz
Of them:
USA: ~ 9,000
India: ~ 2,741
TR: about ~ 1,600
Canada: ~ 1,000
The bulk is the logs of European countries
Used [Stealer Redline](#)
Popular requests have been processed. If you have an individual request, then this material is for you
I agree to work through the Middleman of this forum
Payment with cryptocurrencies
Cost \$ 150
Sorting is possible according to your requests - price \$ 25

Advanced User
Posts 70
Threads 35
Joined Oct 2018
Reputation 21
2 YEARS OF SERVICE



July 26, 2021 at 03:47 PM #1

Hello, let me introduce you to my logs packages
PLEASE READ FULL THREAD - THANK YOU!

1000 Private Logs Mixed (Crypto/[Banning](#)) (Grabbed about 3-5 Days to -today example)
Price: 300\$
5000 Private Logs Mixed (Crypto/[Banning](#)) (Grabbed about 3-5 Days to -today example)
Price: 650\$

I can sell just crypto ones or [Banning](#) ones.
I can sell JUST Target Countries
Our team have 2 years experience in logs and botnets. I will put my samples logs from different botnets, if you are really interested I can send you private samples ones 😊
but you need RANK here for get PRIVATE SAMPLES!

In these examples, cybercriminals offer logs: an archive containing more than 65,000 logs for 150\$ and packages with 1,000 private logs for 300\$

Logs are credentials that are needed for accessing an account. These typically take the form of saved browser cookies, information about server logins, screenshots of the desktop, etc. They are the key for accessing victims' accounts. Logs might be outdated, contain only old game sessions or even have no account-related data. That is why they need to be checked before use. In the chain of log sales, there are several roles.

Firstly, there are people who steal logs with the help of botnets or phishing schemes. These are the **operators**. The operators might have thousands of collected logs in their clouds, but this whole data stream needs to be validated. To process the logs, the cybercriminal needs to check whether the login and password combination is still relevant, how many days have passed since the last password or email change (that is, whether the victim has found out that the account was stolen) and check the balance. The fraudsters might do it on their own, but this may prove quite time-consuming with thousands of logs to go through. For this, there are log **checkers**: cybercriminals who own special tools for processing logs. The software collects statistics about processed logs, and the checker gets a share of the profits: typically, 40%.

It is possible to purchase logs per unit and process them manually or purchase in bulk and process with the help of specialized services. The average price per log is 34¢; the price per 100 logs is \$17.83.

Tolyadukalis

гигабайт
●●●●



Опубликовано: 30 августа

Жалоба ↩

Всем привет, логи с января по август, все логи одного формата, никакой солянки.
Европа и юса примерно 20-30% от всего объёма.
Весь паблик отработан.
Траф биржа.

Платная регистрация

🟢 41

190 публикаций
Регистрация

продаю в 10 рук, цена за доступ 3к\$, могу продать в одни руки за 25к\$.

Доступы выдам всем одновременно когда наберется 10 человек! Продавать не спешу, если желающих купить не будет тогда не буду продавать вообще

This advertiser is offering a batch of logs for \$25,000 to one person but makes no mention of the volume of data

There are also fraudsters who have websites with a large coverage, offering to place links to malware as a way of distribution. In their ads on the darknet, these fraudsters attach traffic and download statistics to attract more customers.

Retail options

If the cybercriminal specializes in small sales (two to ten items), then the type of goods they offer on the darknet will include certain games, in-game items, and accounts with popular gaming platforms. Importantly, these products are typically offered at just 60-70% of their original price, so customers get a good deal on darknet markets. Some criminals can possess thousands of accounts and offer access to these at an enormous discount, as many of these accounts are useless: some cost nothing, and others have already been recovered by their original owners.

гигабайт

●●●●



Selling **280k** valid Gaming username and password Only **4000\$**.

Платная регистрация

🟢 11

102 публикации

Регистрация

12.06.2020

(ID: 105 235)

Деятельность

хакинг / hacking

epic	94,471
PSN	633
Steam	100,856
gog	5,665
blizzard	500
humblebundle	11,228
itch	1,202
origin	542
rockstargames	46,244
ubisoft	18,188

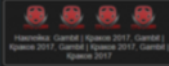
A person is offering thousands of usernames and passwords for various game platforms for just \$4000

Dark web sellers offer stolen accounts, the important selection criteria being the number of games available in the account and how long ago the account was created. Games and add-ons are not cheap, and this is where cybercriminals enter the fray, offering the same popular games at significantly lower prices. In addition to Steam, accounts on gaming platforms, such as Origin, Ubisoft Store, GOG, Battle.net, also get stolen and resold.

Всех приветствую.
Продам 3 скина.

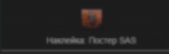
Лот 1. ★ Охотничий нож | Сажа. Износ: поношенное. Именной ярлык: есть. Стоимость в стиме 7634,68.
Цена: 5500 р.

Лот 2. АК-47 | Красная линия. Износ: После полевых испытаний.



Стоимость в стиме 1495.
Цена: 1200 р.

Лот 3. M4A4 | Облом. Износ: После полевых испытаний. Стоимость в стиме 1023.
Цена: 800 р.

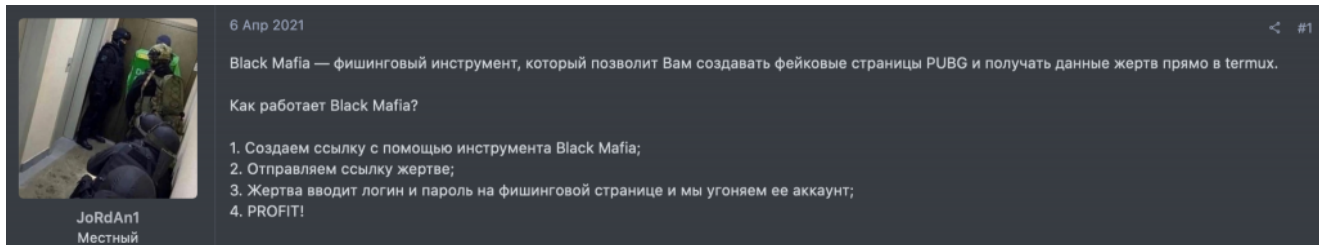


Все 3 скина отдам за 7000

A seller is offering in-game items. The original price is \$20.5, but customers can get these illegally for \$16.45.

In addition to certain games and accounts, cybercriminals also sell rare equipment from a wide range of games with a discount 30-40% off the original price. This is possible if the Steam account that owns the items has no restrictions on sending gifts to other players, e.g., no email confirmation requirement.

Some cybercriminals also sell so-called “Steam balance”. Depending on the origin, Steam balance can be “white” or “black”. White means sold from the seller’s own account. A player could get tired of the game and decide to sell their account, along with all associated in-game goodies, offering it on the black market, as Valve does not approve this kind of deals. Accounts like that can be used for illegal activity, such as fraud or money laundering as they do not – yet – look suspicious to Steam. Black balance means that the Steam accounts were obtained illegally, e.g., through phishing, social engineering or other cybercriminal techniques. Cybercriminals do their best to withdraw money by buying Steam cards, in-game items, gifts, etc., before the original owners retake control of their property with the help of the support service.



A person is outlining a scheme for stealing accounts with the help of PUBG phishing pages

Besides buying goods, darknet forum visitors can also purchase access to phishing instruments, which is a less popular offer. As you can see in the screenshot, the cybercriminal is offering a tool named “Black Mafia”. Phishing tools can even be downloaded from GitHub, after accepting the condition that these will be used for educational purposes only.

A criminal can use the tool for creating a phishing link and sending it to an unsuspecting victim. This generally follows the tried and tested flow: the victim clicks the link and inputs their credentials, which then end up in the hands of the fraudsters.

Conclusion



This overview demonstrates the structure of the game log and login stealing business. With the gaming industry growing, we do not expect this cybercriminal activity to wane in the future – on the opposite, this is the area in which we are likely to see more attacks as tools for targeting gamers continue to develop. BloodyStealer is a prime example of an advanced tool used by cybercriminals to penetrate the gaming market. With its efficient anti-detection techniques and attractive pricing, it is sure to be seen in combination with other malware families soon. Furthermore, with its interesting capabilities, such as extraction of browser passwords, cookies, and environment information as well as grabbing information related to online gaming platforms, BloodyStealer provides value in terms of data that can be stolen from gamers and later sold on the darknet. The overview of game-related goods sold on the darknet forums, too, confirms that this is a lucrative niche for cybercriminals. With online gaming platform accounts holding valuable in-game goods and currency, these become a juicy target. Although purchasing accounts is a gamble, as these may or may not contain goods that can be sold, cybercriminals are willing to take a bet – and are certain to find customers that are looking to save on entertainment.

To minimize the risks of losing your gaming account, follow these simple tips:

- Wherever possible, protect your accounts with two-factor authentication. For others, comb through account settings.

- A strong, reliable security solution will be a great help to you, especially if it will not slow down your computer while you are playing. At the same time, it will protect you from all possible cyberthreats. We recommend Kaspersky Total Security. It works smoothly with Steam and other gaming services.
 - It is safer to buy games on official sites only and wait for the sales – these take place fairly often and are typically tied to big holidays such as Halloween, Christmas, Saint Valentine’s Day, so you will not be sitting on your hands for long.
 - Try to avoid buying the first thing that pops up. Even during Steam’s summer sale, before forking out the dough for a little-known title, at least read some reviews of it. If something is fishy, people will probably have figured it out.
 - Beware of phishing campaigns and unfamiliar gamers contacting you. It is a good idea to double-check before clicking website links you receive via email and the extensions of files you are about to open.
 - Try not to click on any links to external sites from the game chat, and carefully check the address of any resource that requests you to enter your username and password: the page may be fake.
- Cybercrime
 - Darknet
 - Data theft
 - Gaming malware
 - Malware Descriptions
 - Social engineering
 - Trojan

Authors

- **Expert** Leonid Bezvershenko
-  Dmitry Galov
-  Marc Rivero

BloodyStealer and gaming assets for sale

Your email address will not be published. Required fields are marked *