

BlueFox Stealer enters the arena

blog.sekoia.io/bluefox-information-stealer-traffer-maas/

2 November 2022



Log in

Whoops! You have to login to access the Reading Center functionalities!

[Forgot password?](#)

Search the site...

- All categories
- [Blogpost](#)
- [Blogpost](#)

Reset

[Blogpost](#)

BlueFox Stealer: a newcomer designed for traffers teams



Read it later Remove

8 minutes reading

*This blog post on BlueFox Stealer is an extract of the “**FLINT 2022-053 – BlueFox Stealer: a newcomer designed for traffers teams**” report ([SEKOIA.IO Flash Intelligence](#)) sent to our clients on October 20, 2022.*

Table of contents

- [Introduction](#)
- [Conclusion](#)
- [Technical Details & IoCs](#)
- [MITRE ATT&CK TTPs](#)
- [External References](#)

Introduction

In 2022, **information stealers** are one of the **most challenging threats** for both companies and individuals. Cybercriminal threat actors distribute these malware to **steal sensitive information** from infected hosts, which are then **sold on underground marketplaces**, **exploited for fraud** (Business Email Compromise, E-Shop, Bank, Cryptocurrency theft), or **leveraged in “Big Game Hunting” operations**.

Malware developers take advantage of a growing demand for MaaS (Malware-as-a-Service) within the cybercrime ecosystem to sell their newly implemented or rebranded information stealers. They use various underground forums, as well as Telegram channels to advertise, manage financial transactions, and offer technical support. SEKOIA.IO **monitor cybercrime forums to discover emerging malware**, among other threats.

In early September 2022, through our Dark Web monitoring routine we identified a **newly advertised malware dubbed BlueFox Stealer v2**, and sold as a MaaS. Based on the ads promoting it, the BlueFox developer implemented a stealer tailored to the needs of traffers teams (including wide stealing capabilities, performance, efficiency, adapted to traffers context).

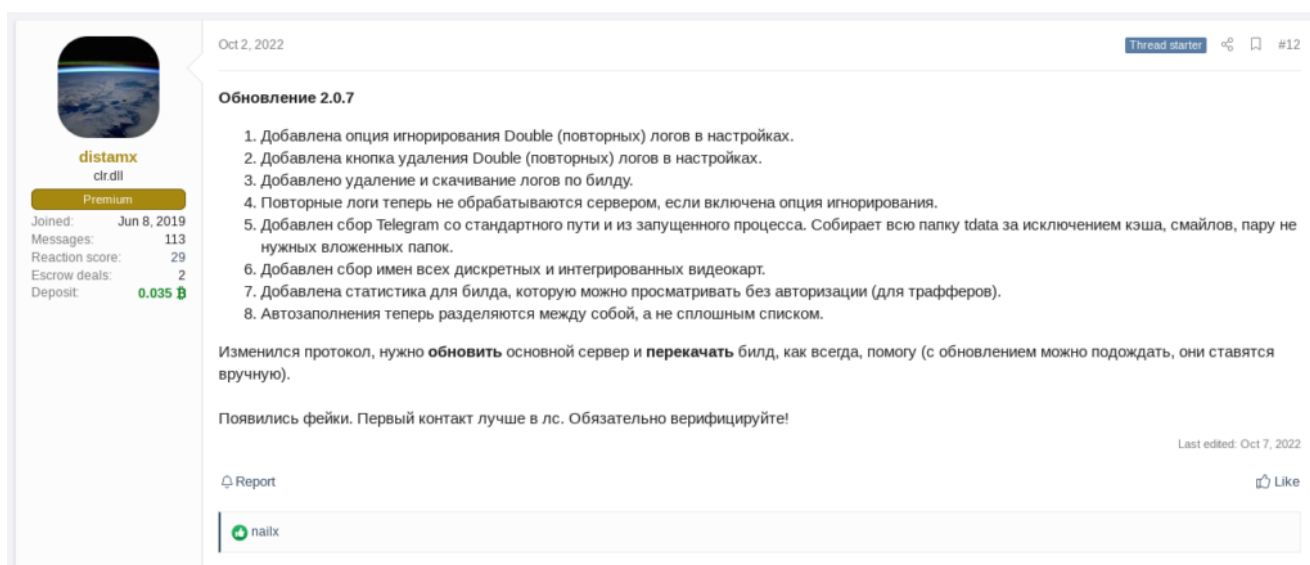
Based on this information, SEKOIA.IO assess that **BlueFox Stealer is possibly to be added to the malware arsenal of traffers teams**, similarly to Redline, Vidar, Raccoon Stealer v2, Aurora Stealer or Erbium Stealer, to be distributed at a large scale. This FLINT goes back to the emergence of BlueFox on cybercrime forums and presents a technical overview of it.

The emergence of BlueFox Stealer on forums

Another stealer designed for traffers teams

BlueFox Stealer's first version appeared on Russian-speaking underground forums (XSS, BHF and DarkNet forums) in December 2021, and it was advertised by a threat actor going by the handle *distamx*. The lack of interactions on its publications may suggest that the project did not work as expected, for unknown reasons.

On 2 September 2022, the user *distamx* published a new post announcing version 2 of BlueFox Stealer on the XSS forum. This time, the publication resulted in more activity, including technical and business inquiries, positive feedback, as well as the release and changelogs of multiple updates (versions 2.0.4 to 2.0.7) by the alleged developer.



Oct 2, 2022 Thread starter 🔊 📄 #12

Обновление 2.0.7

1. Добавлена опция игнорирования Double (повторных) логов в настройках.
2. Добавлена кнопка удаления Double (повторных) логов в настройках.
3. Добавлено удаление и скачивание логов по билду.
4. Повторные логи теперь не обрабатываются сервером, если включена опция игнорирования.
5. Добавлен сбор Telegram со стандартного пути и из запущенного процесса. Собирает всю папку tdata за исключением кэша, смайлов, пару не нужных вложенных папок.
6. Добавлен сбор имен всех дискретных и интегрированных видеокарт.
7. Добавлена статистика для билда, которую можно просматривать без авторизации (для трафферов).
8. Автозаполнения теперь разделяются между собой, а не сплошным списком.

Изменился протокол, нужно **обновить** основной сервер и **перекачать** билд, как всегда, помогу (с обновлением можно подождать, они ставятся вручную).

Появились фейки. Первый контакт лучше в лс. Обязательно верифицируйте!

Last edited: Oct 7, 2022

Report Like

naix

Figure 1. Changelog of the BlueFox Stealer version 2.0.7 published on the XSS forum

Translated from Russian:

(...) 7. Added stats for build, which can be viewed without authorization (for traffers). (...)

Among notable changes, the malware developer added an interesting feature to the administration panel of the BlueFox Stealer version 2.0.7 to allow traffers teams to operate the malware builds internally. Thus, traffers teams distributing the BlueFox Stealer have statistics related to each trafter (also named worker) and can give it access – making the integration of the BlueFox Stealer easier into the traffers teams resources. In other words, each trafter of the team can monitor statistics related to the distribution of their build on a non-authenticated webpage, and therefore have an assessment of the impact of their work.

SEKOIA.IO observed that efforts towards facilitating the integration of stealers in the traffers teams' activities became common for infostealer developers. A second example is Lumma (aka LummaC) Stealer, another emerging malware advertised on Russian-speaking forums

and sold as MaaS since August 2022. On 3 October 2022, its author *Shamel* published an update intended for the traffers teams, integrating a similar feature to display statistics by trafter.

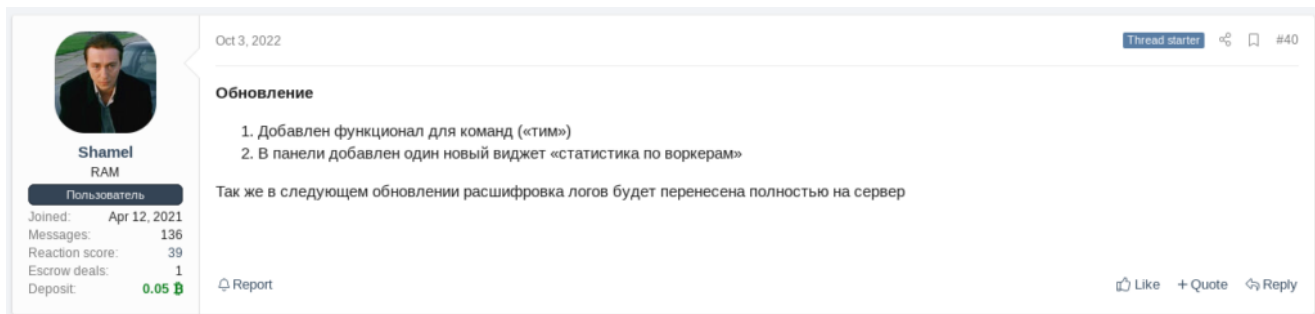


Figure 2. Changelog of the LummaC published on the XSS forum

Translated from Russian:

Update 1. Added functionality for teams 2. Added one new widget in the panel – “statistics by Workers”. (...)

A look at *distamx*'s business

The business model adopted by *distamx* is a classic among MaaS operators. The BlueFox Stealer author sells its malware and the related support services for \$350 per month. Based on feedback and changelogs, *distamx* is very responsive to bug fixes and feature requests.

On 7 October 2022, *distamx* closed the sales of BlueFox Stealer v2, as the threat actor gained enough clients for work, according to its statement. We assess that the infostealer is under continuous development and the *distamx*'s workload is sufficiently high with the malware development and the customer responsiveness. It is therefore plausible that this will result in an increase of BlueFox activities in the near term if MaaS customers distribute it at large scale.

It is worth mentioning that *distamx* also advertised the malware in a Telegram channel (t.me/distamx_sup) similarly to what other MaaS operators were observed doing. BlueFox's presence on Telegram resulted in scams impersonating *distamx* to lure potential customers. SEKOIA already observed such scams, notably for Mars Stealer, Aurora Botnet, and Raccoon. These scams are common in the Russian-speaking cybercrime ecosystem, and analysts monitoring malware-related activities should be aware of this so as not to follow false leads when investigating threat actors.

Technical overview of BlueFox Stealer

Once an emerging malware appears on cybercrime forums, SEKOIA.IO analysts implement search techniques to retrieve related samples or servers, to produce actionable intelligence to our customers.

Malware sample association

A few weeks after the launch of BlueFox Stealer v2, we retrieved BlueFox-related malware samples (SHA256 are available in the [IOCs section](#)). Here are the main technical details allowing SEKOIA to confirm association of these sample to BlueFox stealer with high confidence:

BlueFox Stealer v2 features, as described in their publications	SEKOIA.IO's commentary
Update 2.04 to 2.0.7	We observed samples named <i>BlueFox2.0.4</i> , <i>BlueFox2.0.5</i> , <i>BlueFox2.0.7</i> and <i>BlueFox2.0.8</i> .
"Native x86 executable with no CRT, running .NET in memory"	The .NET sample has no dependencies.
"The size is still about 165 kb."	The stand-alone malware is 162.5KB.
"Native protocol on TCP/IP in encrypted form"	The malware communicates over TCP using a custom protocol, and data is encrypted.
"Collection ... from Chromium, Edge and Firefox-based"	The malware access data from Google Chrome, Firefox and Microsoft Edge files.
"Self-delete executable after sending log file."	Analysed sample deletes itself from the infected host using the command " <i>cmd.exe /C timeout 5 & del</i> "
"Collect PC data"	The sample reads several Windows Registry keys to fingerprint the infected host.
"... grabber to search all drives and flash drives."	The malware enumerates physical storage devices.

Table 1. Comparative table of BlueFox's features shared by distamx and the SEKOIA.IO's analysis

[Discover our CTI and XDR products](#)

Of note, this is not an exhaustive list, rather a selection of the most characteristic technical artifacts deemed relevant in our association process.

BlueFox Stealer Malware capabilities

The **BlueFox Stealer v2 capabilities** advertised by *distamx* are **those of a classic information stealer**, with a focus on cryptocurrency wallets, and file grabber and loader capabilities.

Here is an overview of its capabilities:

- Targeting of popular browsers (Chromium and Firefox based browsers: Chrome, Edge, Opera, Mozilla, etc.) to steal passwords, cookies and autocompletes;
- Targeting of almost all desktop cryptocurrency wallets and extension for cryptocurrency wallets (MetaMask, TronLink, BinanceChain, Yoroi, Coinbase, Jaxx, Ethereum, Electrum, Exodus, etc.);
- Targeting password extensions (Bitwarden, 1Password);
- File downloading and loading;
- File grabbing in all disks;
- Screenshot capturing;
- System fingerprinting.

BlueFox exfiltrates the collected data to its C2 server using socket communication via native protocol on TCP/IP in encrypted form. The malware removes itself from the infected host using the Windows command `cmd.exe /C timeout 5 & del "$PATH"`.

A dynamic analysis from the Hatching Triage sandbox of a BlueFox Stealer v2 sample is available

here: <https://tria.ge/221015-2ckbtagec3/behavioral2>.

Conclusion

SEKOIA.IO assess that **implementing features for monitoring traffers statistics** when distributing information-stealing malware is likely to become a **must-have to be a relevant player in the cybercrime ecosystem**. Based on our observations, such capabilities are already quite common for prevalent loaders used by Pay-Per-Install services, such as SmokeLoader, PrivateLoader, and MixLoader.

To provide our customers with actionable intelligence, SEKOIA.IO analysts will continue to monitor BlueFox, emerging and prevalent infostealers; and keep an eye on the evolution of newcomers.

Technical Details & IoCs

BlueFox IoCs

BlueFox C2

The list of IoCs is available on [SEKOIA github repository](#).

IOC	Link
31.41.244[.]152:47567	app.sekoia.io

45.8.147[.]200:51425	app.sekoia.io
46.148.114[.]177:38990	app.sekoia.io
45.8.147[.]31:15100	app.sekoia.io
193.106.191[.]130:17322	app.sekoia.io
91.241.19[.]49:35767	app.sekoia.io
79.137.198[.]63:42998	app.sekoia.io
94.131.107[.]223:51176	app.sekoia.io

BlueFox samples

BlueFox2.0.8

194ef023286a19eea2c084f0d469d3427b97445b0b8fc75888d02274bf01e748
36190e8a9976de1036976ed44456ca833d7d2a7f23ed8acc707efe09fca7da9d
ca6d6555b349612637522e8506592ccaa5b0435f2a9af35aab77520cab495439
9ed0f76449bbc6d5d6db12dfc527740c072436c4379248855729321032d91bb7
82ce28407b4f0075d288470410df5af7c28e69ab44144bcf4610e6493e99e478
80bc9d060c42ada4ad5029a196293280d64257db95f223964ce7881930fab0f6
5e14e2582a02b6fe7cb28d6cad80bcddc51be2c01db097b0d292dfd575cb44a9

BlueFox2.0.7

7b7714d0bba4aa994d27130165a99d74cf627469f14ad7ba25c51ea0a1e16699
d8ca57e29b21ef3218877f43f9566f2fdbb11552f901d03234e3e9145c862392

BlueFox2.0.5

c56a00b4b8ebc12b8798e6ec7ab8e2c9815716fa40bb92488cb3e5c8a227d455

BlueFox2.0.4

186f94743c27032ff7401153a52116b4bbbf87c958dd0e2da1c0c111671c0563

BlueFox Stealer YARA rule

```

rule infostealer_win_bluefox {
  meta:
    malware = "BlueFox"
    description = "Find BlueFox Stealer v2 samples based on the specific strings
embed in the executable files"
    source = "SEKOIA.IO"
    reference = "https://blog.sekoia.io/bluefox-stealer-a-newcomer-designed-for-
traffers-teams/"
    classification = "TLP:CLEAR"

  strings:
    $str01 = "DesktopScreenshotLength" ascii
    $str02 = "SoftwareSearchesCount" ascii
    $str03 = "AutoCompleteLength" ascii
    $str04 = "DesktopSizeLength" ascii
    $str05 = "CPULength" ascii
    $str06 = "GPULength" ascii
    $str07 = "FullNameLength" ascii
    $str08 = "Asn1NssLength" ascii
    $str09 = "LoginLength" ascii
    $str10 = "BrowserCount" ascii

  condition:
    uint16(0)==0x5A4D and 9 of them
}

```

MITRE ATT&CK TTPs for BlueFox Stealer

Tactic	Technique
Execution	T1059.003 – Command and Scripting Interpreter: Windows Command Shell
Defense Evasion	T1027 – Obfuscated Files or Information
Defense Evasion	T1036 – Masquerading
Defense Evasion	T1070.004 – Indicator Removal on Host: File Deletion
Defense Evasion	T1140 – Deobfuscate/Decode Files or Information
Credential Access	T1539 – Steal Web Session Cookie
Discovery	T1012 – Query Registry
Discovery	T1082 – System Information Discovery
Discovery	T1083 – File and Directory Discovery
Discovery	T1614 – System Location Discovery

Collection	T1005 – Data from Local System
Collection	T1113 – Screen Capture
Collection	T1119 – Automated Collection
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols
Command and Control	T1105 – Ingress Tool Transfer
Command and Control	T1571 – Non-Standard Port
Exfiltration	T1041 – Exfiltration Over C2 Channel

External References

<https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem/>

Chat with our team!

Would you like to know more about our solutions? Do you want to discover our XDR and CTI products? Do you have a cybersecurity project in your organization? Make an appointment and meet us!

Contact us

You can also read other blog post :

Comments are closed.
