

# Diving into the underground market of Stealer Logs

---

Apurv Singh Gautam  
ASG\_Sc0rpi0n

# About Me

- Threat Researcher 
- TA @ StationX
- Cybersecurity @ Georgia Tech (Go Jackets) 
- Presented at conferences



- Hobbies
  - Hiking
  - Lockpicking
  - Gaming/Streaming

- Twitter - @ASG\_Sc0rpi0n
- Website – [apurvsinghgautam.me](http://apurvsinghgautam.me)

# AGENDA

- Stealers: Introduction
- Stealer Logs
- Underground Market Analysis
- Market beyond Stealer Logs
- Protection for consumers/business
- Conclusion

---

## **. Stealers: Introduction**

## What are Stealers?

- Trojan
- Steal username, password, cookies, autofills, etc.
- Used for initial access

## Stealers over Time

- Zeus (2006)
- Koobface (2008)
- Currently most botnets have stealer capability
- Examples – TrickBot, Emotet, LokiBot, etc.

## • Current Market of Stealers •

Top Stealers	
Agent Tesla	Oski
Formbook	Bloody
RedLine	AZORult
Raccoon	Loki
Mars	CopperStealer
Vidar	KPOT

- Widely known stealers – AZORult, Vidar, Raccoon, RedLine





## Infection Methods

- Phishing, torrents, pirated software, compromised websites, etc.
- Leverage anti-evasion techniques
- Rely on Wrappers/Packers/Cryptors



# Capability of Stealers

- Keylogging
- Hooking into browsers and other applications
- Utilizing Web Injection scripts



---

## . Stealer Logs

## Types of Logs Generated

- Browser Cookies
- Browser Autofills
- Crypto Wallets
- Steam/Discord Tokens
- Login Details
- Payment Details

## Example of Stealer Logs

```
Autofills
Cookies
CreditCards
Discord
FileGrabber
Steam
Telegram
Wallets
DomainDetects.txt
ImportantAutofills.txt
InstalledBrowsers.txt
InstalledSoftware.txt
Passwords.txt
Screenshot.jpg
UserInformation.txt
```

```
Autofills
├── Google_[Chrome]_Default.txt
├── Microsoft_[Edge]_Default.txt
└── Opera_GX_Unknown.txt
Cookies
├── Google_[Chrome]_Default_Extension.txt
├── Google_[Chrome]_Profile_1.txt
├── Microsoft_[Edge]_Default_Network.txt
└── Opera_GX_Unknown_Network.txt
CreditCards
├── Google_[Chrome]_Default.txt
Discord
├── Tokens.txt
FileGrabber
├── da.txt
Steam
├── DialogConfig.vdf
├── DialogConfigOverlay_1920×1080.vdf
├── config.vdf
├── libraryfolders.vdf
├── loginusers.vdf
Telegram
├── DB50A020D36CB65Cs
├── Profile_1
├── key_data
├── prefix
├── settings
├── shortcuts-custom.json
├── shortcuts-default.json
├── usertag
Wallets
├── Exodus
├── exodus.conf.json
├── market-history-cache.json
└── window-state.json
```

## Example of Stealer Logs

```
URL: https://accounts.google.com/signin/v2/challenge/pwd
Username: [REDACTED]
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
URL: android:
tify.music/
Username: [REDACTED]
Password: [REDACTED]
Application: Google_[Chrome]_Default
=====
```

```
address-ui-widgets-enterAddressFullName: [REDACTED]
address-ui-widgets-streetName: [REDACTED]
address-ui-widgets-buildingNumber: [REDACTED]
address-ui-widgets-neighborhood: [REDACTED]
address-ui-widgets-enterAddressCity: [REDACTED]
email-or-phone: [REDACTED]@gmail.com
LoginForm[email]: [REDACTED]@gmail.com
firstName: [REDACTED]
emailaddress: [REDACTED]@gmail.com
```

File: Tokens.txt


MTY [REDACTED] ZfAc

---

# **Underground Market Analysis**



# Stealers Landscape



Feb 19, 2020


WHEN PURCHASING THROUGH THE PM OF THE FORUM OR THE GUARANTOR OF THE FORUM 20% DISCOUNT FOR ALL TYPES OF SERVICES

Write only and only here <https://t.me/NEWREDLINE> and require confirmation through the PM of the forum

I would like to present you a stealer designed for convenient work with logs. Collects the most requested information for work in all areas. The program was written taking into account all the wishes of people professionally involved in the field of carding.

Build features:

- 1) Collects from browsers:
  - a) Login and passwords
  - b) Cookies
  - c) Autofill fields



**raccoonstealer**  
RAID array  
User

Sign up: 01.04.2019  
Messages: 75  
Reaction: 29


20.05.2019

**Raccoon Stealer. We steal, You deal!**

We started in April 2019 on exploit, wwh, xss, etc.  
Over the past time, we have received a lot of good reviews and constantly try to keep the quality of our service at the level.

**Software**

- \* Native code. Our build is not a fork of products already existing on the market.
- \* Stealer is written in C/C++.
- \* Our build will give you a different tap at each spill, because Raccoon is noticed by units of antiviruses in the conditions of a dynamic test.
- \* Raccoon collects: passwords, cookies and autofill from all popular browsers (including Firefox x64), CC data, system information
- \* Almost all existing cryptocurrency desktop wallets, including the Brave browser wallet and the Metamask extension wallet.
- \* Built-in file downloader.
- \* Work on both 32 and 64-bit systems without dependencies on .NET.
- \* Output file - Native x86 executable is easy to crypto.



**blackteam007**  
(L1) cache  
Пользователь

Регистрация: 14.04.2020  
Сообщения: 921  
Реакции: 159  
Гарант сделки: 1  
Депозит: 0.0001 \$

08.04.2021


✓ Stealer "BlackGuard" ✓  
Scantime/Runtime - <https://checkzilla.io/scan/d1f23cc6-72a7-4002-8d9f-0450f9826eb7>

★ Функционал:

- 1) Сбор Passwords
- 2) Cookies
- 3) Autofill
- 4) History
- 5) Wallet:
  - 5.1) AtomicWallet
  - 5.2) BitcoinCore
  - 5.3) DashCore
  - 5.4) Electrum
  - 5.5) Ethereum
  - 5.6) Exodus
  - 5.7) LitecoinCore
  - 5.8) Monero
  - 5.9) Jaxx
  - 5.10) Zcash

20-07-2021, 03:02

**Jester Stealer - Member**



Join Date: Jul 2021

МЫ КОМАНДА ПРОГРАММИСТОВ ПИШУЩИХ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ЛЮБЫХ ЦЕЛЕЙ НАШИХ КЛИЕНТОВ И ПО ДОСТУПНЫМ ЦЕНАМ


НА ДАННЫЙ У НАС В ПРОДАЖЕ ИМЕНЕТОР:  
BOTNET, STEALER, CLIPPER, MINER

ПОМОЖИ ПРОДАЖИ ГОТОВЫХ РЕШЕНИЙ, МЫ МОЖЕМ РАЗРАБОТАТЬ ДЛЯ ВАС ПРОЕКТ ЛЮБОЙ СЛОЖНОСТИ. УЧЕНЫ ВСЕ ВАШИ ПОЖЕЛАНИЯ, НО НЕ БУДЕМ ЗАТРУГЛИВАТЬ СРОКАМИ И ЗАВЫШАТЬ ЦЕНУ. НАША КОМАНДА УЖЕ СЕЙЧАС АКТИВНО РАЗВИВАЕТСЯ И КОНКУРИРУЕТ С ДРУГИМИ ПРОДАВЦАМИ ГОТОВЫХ РЕШЕНИЙ

ДЛЯ ЧЕГО НЕ КОММЕНТАРИЙТЕ, УСПЕШНО ЗАВЕРШАЯ ПРОЦЕСС "ОТКРЫТИЯ КОНТАКТОВ" ПЕРЕД НАЧАЛОМ РАБОТЫ. НЕ ЗАБЫВАЙТЕ ПОДПИСАТЬСЯ НА НАШЕГО БОТА.



# Stealers Landscape (Contd.)



**MarsTeam**  
RUC-массов

Пользователи: 22.05.2021  
Созданные: 96  
Реакции: 34  
Получено: 1  
Донаты: 0.009 B

22.06.2021

**Mars Stealer** — нативный, нерезидентный стиллер с функционалом лоадера и грабера

Наш софт разрабатывался с учетом пожеланий людей, работающих по крипте, поэтому в Mars вы можете найти всё необходимое для работы с криптой и не только.

**ВНИМАНИЕ! Мы НЕ РАБОТАЕМ ПО СНГ И ВМ НЕ СОВЕТУЕМ!**

Mars написан на ASM/C WinAPI, весит всего 95kb (упакованный в UPX 40kb), использует техники для скрытия запросов к WinAPI, шифрует используемые строки, собирает весь лог в памяти, а так же поддерживает защищенное SSL-соединение с командным сервером.

Не используете crt, std.

**Список поддерживаемых браузеров:**  
Internet Explorer, Microsoft Edge  
Google Chrome, Chromium, Microsoft Edge (Chromium version), Kometa, Amigo, Torch, Orbitum, Comodo Dragon, Nichrome, Maxthon5, Maxthon6, Sputnik Browser, Epic Privacy Browser, Vivaldi, CocCoc, Uran Browser, QIP Surf, Cent Browser, Elements Browser, TorBro Browser, CryptoTab Browser, Brave Browser.  
Opera Stable, Opera GX, Opera Neon.  
Firefox, SlimBrowser, PaleMoon, Waterfox, Cyberfox, BlackHawk, IceCat, KMeleon, Thunderbird.

Собирает пароли, куки, сс, автозаполнение, историю посещений сайтов, историю скачивания файлов.  
Поддерживаются все последние обновления браузеров, включая Chrome v80.

Важным функционалом, выделяющим нас на фоне конкурентов является сбор плагинов браузеров с упором на плагины-криптокошельки и 2FA-плагины.

**Список поддерживаемых крипто-плагинов:**  
IronLink, MetaMask, Binance Chain Wallet, Yoroi, Nifty Wallet, Math Wallet, Coinbase Wallet, Guarda, EQUAL Wallet, Jaxx Liberty, BitAppWallet, iWallet, Wombat, MEW CX, Guild Wallet, Saturn Wallet, Robin Wallet, NeoLine, Clover Wallet, Liquality Wallet, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh Wallet, ICONEX, Nabox Wallet, KNC, Temple, TezBox, Cyano Wallet, Byone, OneKey, Leaf Wallet, DAppPlay, BitClip, Steem Keychain, Nash Extension, Hycon Lite Client, ZilPay, Coin98 Wallet.

**Список 2FA-плагинов:**  
Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Trezor Password Manager.

## Jester

### [EN]: Universal Exploit Builder

We are opening pre-sales of the builder.  
The builder will help you to hide any one without any problems .exe file in such extensions as: ".jar", ".bat", ".ps1", ".txt", ".png", ".mp3", ".mp4", ".pdf", ".doc", ".xls", ".ppt" and others at your request.

When you run an infected file, the virus will open secretly, as well as the file itself with which you are gluing.  
Also, with the help of a builder, you can glue ordinary ones .exe + .exe files.

## REDLINE STEALER Pro

Stealer functionality:

Collects from browsers:  
Login and passwords  
Cookies  
Autocomplete fields  
Credit cards  
Supported browsers:  
All browsers based on Chromium (even latest version of Chrome)  
All Gecko-based browsers (Mozilla, etc.)  
Data collection from FTP clients, IM clients  
File-grabber customizable by Path, Extension, Search-in-subfolders (can be configured for the necessary cold wallets, Steam, etc.)  
Settings by country. Setting up a blacklist of countries where the build will not work  
Settings for anti-duplicate logs in the panel  
Collects information about the victim's system: IP, country, city, current username, HWID, keyboard layout, screenshot, screen resolution, operating system, UAC Settings, is the current build running with administrator privileges, User-Agent, information about PC hardware (video cards, processors) and the steal of crypto

Info:  
https://t.me/REDLINESTEALERPro - Official page  
@StorBotnetProstealer - Buy Redline

Contacts:  
@StorBotnetProstealer - Support and Buy

Telegram  
REDLINE STEALER Pro  
Buy Redline Stealer Pro

VIEW CHANNEL



## REDLINESTEALER Соедините контакт

bot

What can this bot do?

Hello buddy, if you want buy Redline Stealer, input chat commands /start

August 10

ZK

/start 2:57 AM



Powered by © Redline 2021 | Official channel | Official chat 2:57 AM

RedLine[Month] #1 RedLine[Week] #2

RedLine[LifeTime] #3

Add balance

MyProfile

Support

# New/Private Stealers on the Market

**NoMercy v1.0.0** has been released. If you want to buy this product, DM me for further instructions  
 Price: £780 | \$10  
 Cryptocurrency: Monero ONLY

**Features:**

- 1) Execute CLI commands
  - 1.1) whoami /all
  - 1.2) arp -a
  - 1.3) ipconfig /all
  - 1.4) net view /all
  - 1.5) net share
  - 1.6) route print
  - 1.7) netstat -nao
  - 1.8) net localgroup
  - 1.9) systeminfo
- 2) Get running processes
  - 2.1) Get the window title
  - 2.2) Get the process name
  - 2.3) Get the Process ID
  - 2.4) Get the EXE path
- 3) Get public IP
- 4) Get private IP
- 5) Get M.A.C
- 6) Get HWID
- 7) Get R.A.M (in megabytes)
- 8) Get G.P.U
- 9) Get the OS version
- 10) Get installed anti-virus
- 11) Get keyboard language
- 12) Get the current clipboard
- 13) Get C.P.U

**! Major update for Typhon: v1.2.0**

**Changes:**

- Added WinSCP FTP client stealer
- Save UserInformation.txt with basic information in base dir of zip

**New features:**

- Worm, copy to any shared network or removable drive
- User agent stealer

**Next update:**

- GUI builder

DUE TO SOME PROBLEMS XMR MINER WILL BE ADDED IN V1.2.1  
 Updates will be sent to customers in 14-16 hours

Buy now by DMing - [redacted]  
 Typhon updates channel - [redacted]

---  
 Lifetime access- \$50  
 Accepted- XMR, BTC, ETH, USDT (TRC20)

**PRYNT**

Home About Us Products Contact

AI Credit Cards Botnet Logs Botnets Banks Paypal Scripts Scam Pages Tools Funks


**Prynt Stealer 1 Year License**

**LICENSE OF USE**

We don't bear the responsibility on how you use this!

[Add To Cart](#) [Buy Now - \\$700](#)

**PRODUCT INFO**



Vendor Name Admin

**[RENT] RAPOGLIFF Crypto Stealer C/C++ 28 KB**  
 By asdqwezxc, [redacted] ago in [Software] - malware, exploits, bundles, crypts

asdqwezxc  
 byte

Posted [redacted] ago (edited)

Crypto-stealer written in C/C++ for rent.  
 Focuses on crypto wallets and will move ONLY in this direction.


There are many innovations plans for the future for a better experience, we only need your support.  
 You won't need to rent a server and configure the panel, our team is responsible for all the configuration process.

**FREE & opensrc Rust Stealer**

03.07.2022

rust stealer stealer source

1 2 3 ... 8 View all



03.07.2022

Hello Community,  
 This is my 2. Rust Release here.

Some Features the Stealer has:

- Chromium Stealer:
  - edge
  - chromium
  - 7star
  - amigo
  - brave
  - centbrowser
  - chedom
  - chrome\_canary
  - coccoc
  - dragon
  - elements-browser
  - epic-privacy-browser
  - chrome
  - Amovius

Рейтинг: 23.03.2022 96  
 Просмотров: 100  
 Голосов: 2

# Stealer Logs Landscape

← [redacted] +Logs  
545 subscribers

CLOUD OF INFORMATION:

Weekly: 20-35k new logs  
Complete informative logs: cookies, authentications, sessions, victim information (hardware), Discord tokens, autofills and much more.

Our team can provide you with some screenshots from the cloud

📁 Price:

- \$ 250 / month
- \$ 850 / 6 months (SAVE 650\$)
- \$ 1500 / lifetime

📁 logs are also used for the following anti-public logs to personally check if your logs are really private.

[16.34GB] LEAKED LOGS FROM CLOUD [21000 MIXED LOGS]

[redacted]

OP [redacted]  
Hello again.

140GB Log priv8 2022

[redacted]

I want to give you some series of logs ❤️  
140 GB log priv8

← [redacted]  
685 subscribers

**Pinned message #2**

🔥🔥🔥 MEGA LEAK ! 1.47 TB LOGS DOWNLOAD: <https://mega.nz>

🔥🔥🔥 Selling private cloud

- About 496,000 LOGS JUNE-AUGUST (2022 year only)
- Stealer: RedLine & Raccoon
- Price: 250 USD
- Payment: any popular crypto
- I dont sorting

uploaded: [mega.nz](https://mega.nz) separately by archives  
if you do not have [mega.nz](https://mega.nz) premium acc, after purchase I will give it for you

**MORE 1.000.000 LOGS FOR SALE APRIL-JUNE 2022**

[redacted]

I will sell a cloud with more than 1.000.000+ logs

Geo - world mix  
Log dates April - June 2022  
Jule more 90.000+ logs

The logs are hosted on Mega.nz

Base stealer - Redline

Payment exclusively in cryptocurrencies

Cloud cost \$200

Infinity

## Main Page

Country

Example - US

Created

Find in logs

Type tag and press Enter...

Search

Seller

username

Price

0%

0100

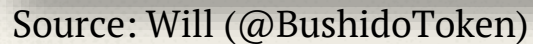
### Product List

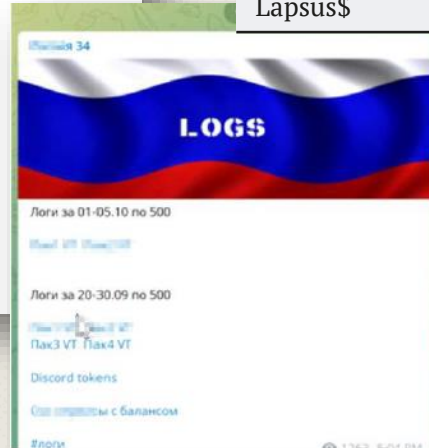
#	Seller	Country	Created	Price	Seller Rating	Action
1	DarkSeller	Burma	20/08/2022 19:48	\$ 3.9	<div></div>	<div>Buy</div>
2	DarkSeller	Burma	20/08/2022 19:48	\$ 3.9	<div></div>	<div>Buy</div>
3	DarkSeller	Burma	20/08/2022 19:48	\$ 3.9	<div></div>	<div>Buy</div>
4	DarkSeller	Burma	20/08/2022 19:48	\$ 3.9	<div></div>	<div>Buy</div>
5	DarkSeller	Burma	20/08/2022 19:48	\$ 3.9	<div></div>	<div>Buy</div>
6	DarkSeller	Burma	20/08/2022 19:48	\$ 3.9	<div></div>	<div>Buy</div>
7	DarkSeller	Burma	20/08/2022 19:48	\$ 3.9	<div></div>	<div>Buy</div>
8	DarkSeller	Burma	20/08/2022 19:48	\$ 3.9	<div></div>	<div>Buy</div>
9	DarkSeller	Burma	20/08/2022 19:48	\$ 3.9	<div></div>	<div>Buy</div>



---

# **. Market Beyond Stealer Logs**





Source: Cyble, Microsoft, Kaspersky



## Impact

- Gaining initial access to organizations
- Espionage, Data Theft, Extortion
- Ransomware

---

**. Protection for  
consumers/business**

## Protection for orgs

- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.
- Monitor any unusual endpoint behavior and network beacons to block data exfiltration by malware.
- Use the IOCs which are present on public platforms to monitor and block malware infection.
- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.

## Protection for users

- Avoid downloading pirated software from warez/torrent websites.
- The “Hack Tool” present on sites such as YouTube, torrent sites, etc., mainly contain such malware.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.

---

## **. Conclusion**

## What we discussed so far?

- Stealers and their capabilities
- Structure of stealer logs
- Underground landscape for stealers
- Market of stealer logs
- Usage of stealer logs by TAs
- Protection for users/orgs



## Resources

- Cyble - Analysis of Stealer Malware Family
- US CISA Alert (AA22-216A) – 2021 Top Malware Strains
- Microsoft – DEV-0537 (LAPSUS\$) Blog
- Kaspersky – Common TTPs of the modern Ransomware Report



# THANKS!

<Put something Cyble related>

*Any questions?*

You can contact me at:



@ASG\_Sc0rpi0n



/apurvsinghgautam



apurvsinghgautam.me