

MADCAT RANSOMWARE – A Multidimensional Crime

Analysis description:

On 31/10/2023 on the breachforums[.]is forum, a user named: Plessy published a post announcing the sale of 246,000 passport scans, originating from Poland.

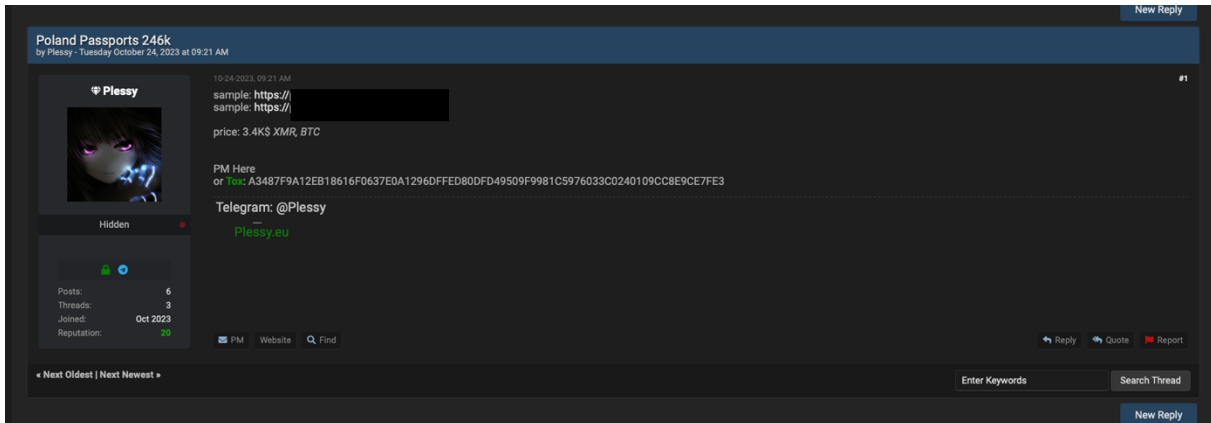


Figure 1

For the entirety of this illegal collection, Plessy is demanding a sum of \$3,400, preferring payment in cryptocurrencies such as Monero (XMR) or Bitcoin (BTC).

As proof of the authenticity of his offer, Plessy published links to passport samples he claims to have in his possession.

In addition, the said user declares having other bases for sale With documents:

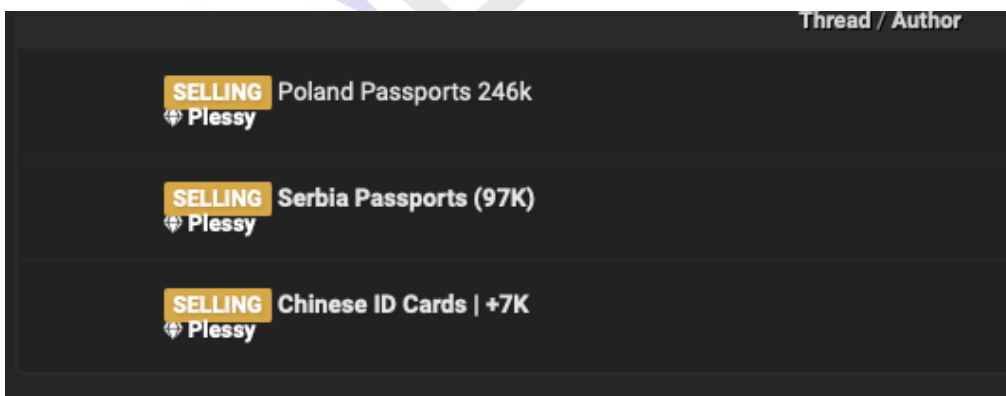
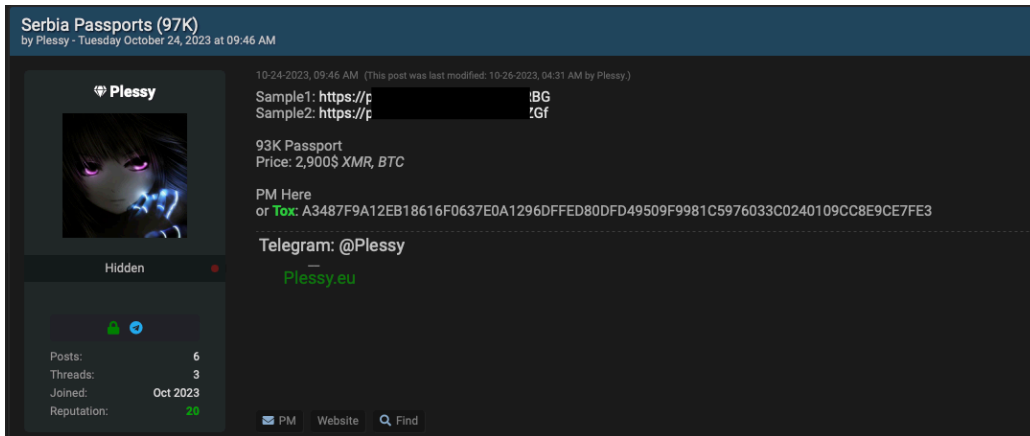


Figure 2

Passports - Serbia:



Serbia Passports (97K)
by Plessey - Tuesday October 24, 2023 at 09:46 AM

10-24-2023, 09:46 AM (This post was last modified: 10-26-2023, 04:31 AM by Plessey)

Sample1: <https://p> IBG
Sample2: <https://p> ZGf

93K Passport
Price: 2,900\$ XMR, BTC

PM Here
or **Tox:** A3487F9A12EB18616F0637E0A1296DFFED80DFD49509F9981C5976033C0240109CC8E9CE7FE3

Telegram: @Plessey
[Plessey.eu](https://www.plessey.eu)

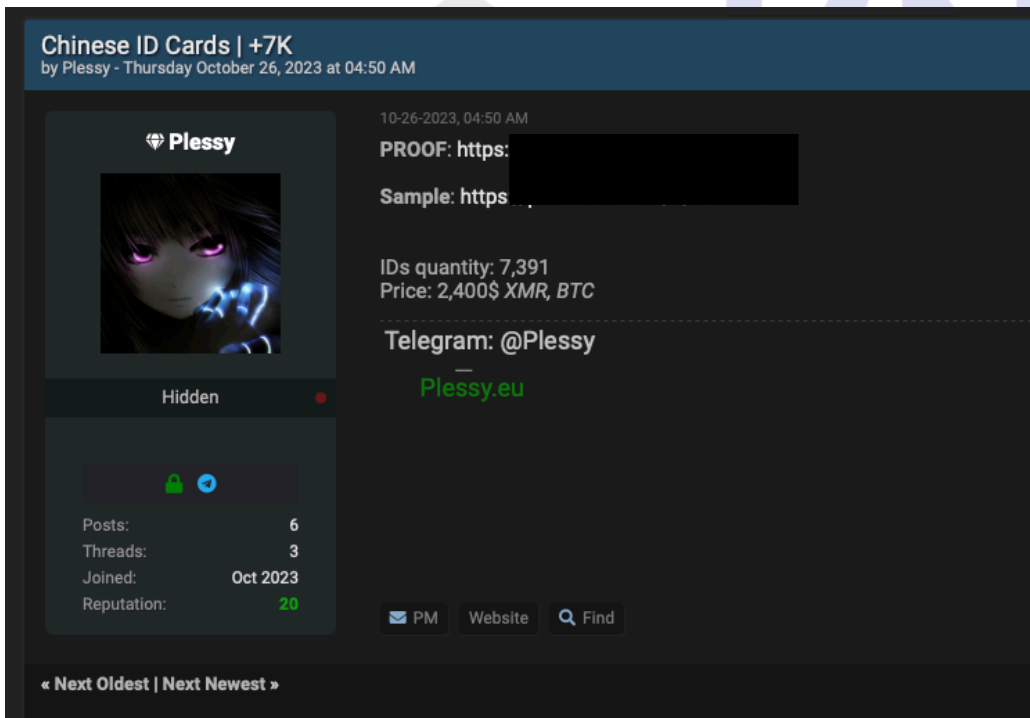
Hidden

Posts: 6
Threads: 3
Joined: Oct 2023
Reputation: 28

PM Website Find

Figure 3

ID Cards - China:



Chinese ID Cards | +7K
by Plessey - Thursday October 26, 2023 at 04:50 AM

10-26-2023, 04:50 AM

PROOF: <https://> [REDACTED]

Sample: <https://> [REDACTED]

IDs quantity: 7,391
Price: 2,400\$ XMR, BTC

Telegram: @Plessey
[Plessey.eu](https://www.plessey.eu)

Hidden

Posts: 6
Threads: 3
Joined: Oct 2023
Reputation: 20

PM Website Find

« Next Oldest | Next Newest »

Figure 4

Analysis of user profile 'Plessy' on Breachforums

Account Establishment Date: October 23, 2023.

Forum Activity:

Plessy has shown limited activity outside of his own threads. He has been spotted participating in two discussions: one about the QiCard data leak in Iraq, and the other about the security incident at the eKosova service.

Details of his activities can be followed at the link:

[https://breachforums\[.\]is/search.php?action=results&sid=8b986392ea7dd81c124be0561efcdc0b](https://breachforums[.]is/search.php?action=results&sid=8b986392ea7dd81c124be0561efcdc0b).

Contact Methods Provided by Plessy:

Telegram: @Plessy

Website: Plessy[.]eu

Tox (Secure Messaging):

A3487F9A12EB18616F0637E0A1296DFFED80DFD49509F9981C5976033C0240109CC8E9CE7FE3

Telegram:

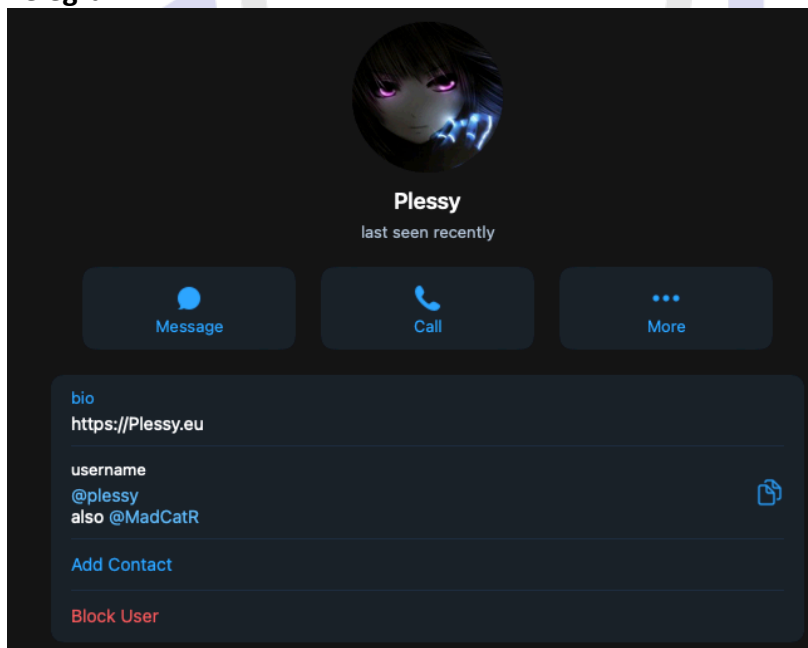


Figure 3 Telegram @plessy

The biographies in Telegram messenger were excerpted:

- website address: plessy[.]eu
- usernames: @plessy and @MadCatR

When searching for the **@MadCatR** account, we can find the related channel:

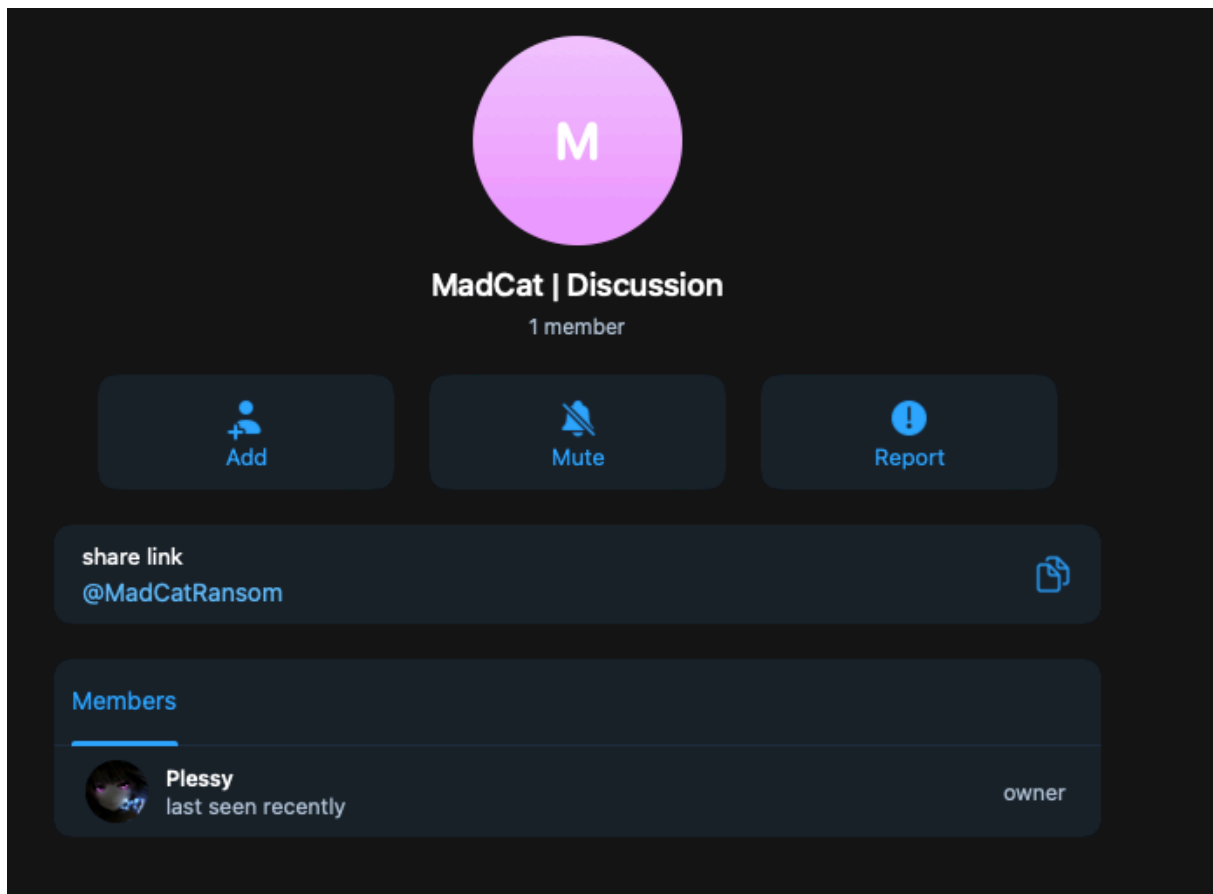


Figure 4 MadCatRansom channel

The channel is **@MadCatRansom**, where the only user is user **@Plessy**. The name of the channel itself suggests that it may be a **Ransomware** group.

Website:

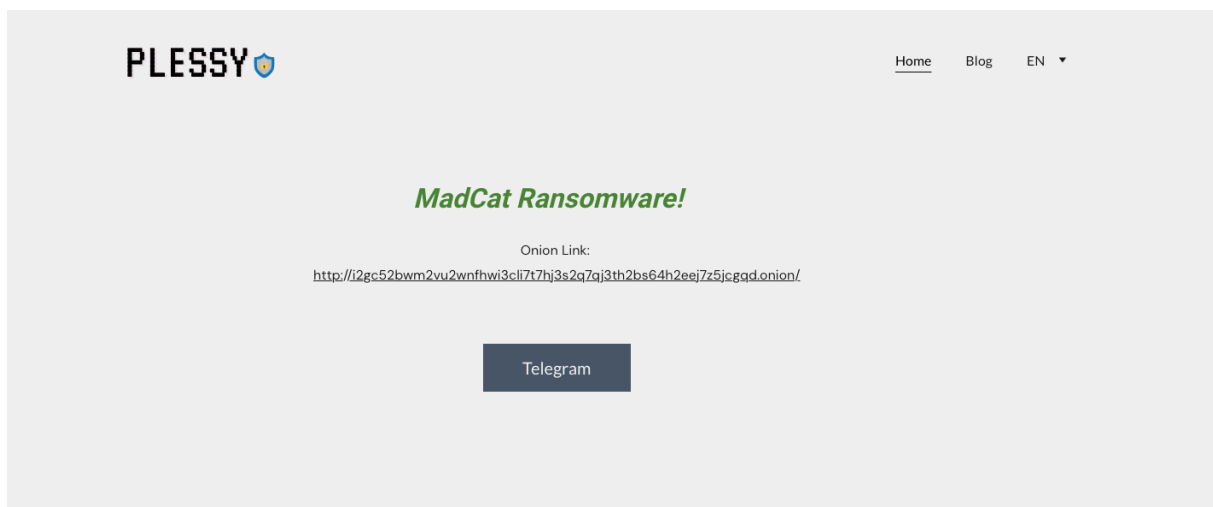


Figure 5 Website plessy[.]eu

The plessy[.]eu home page has a URL link that redirects to a page on the TOR network at the address:

hxxp://i2gc52bwm2vu2wnohwi3cli7t7hj3y2q7qj3th2bs64h2eej7z5jcgqd[.]onion.

In addition, on the same page, under the Telegram icon, there is a link to the profile of user **@shinyenigma** on the Telegram platform:

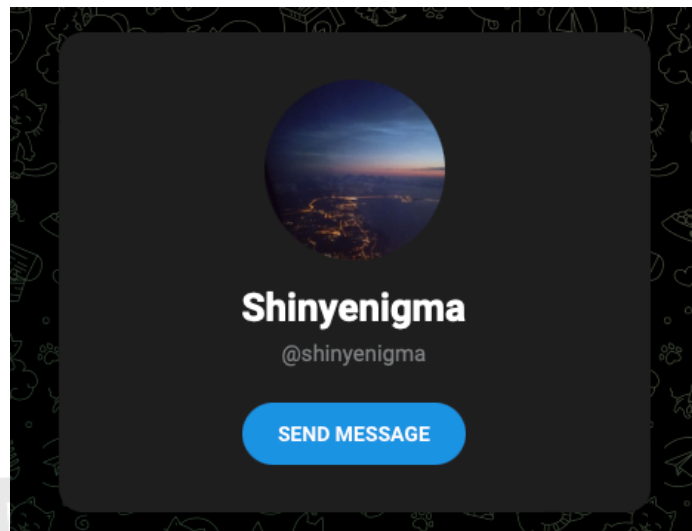


Figure 6 @shinyenigma

The Plessy[.]eu website was built using a website builder:
Hostinger Website Builder:

```
    }  
  }, s({  
    type: "element",  
    tagName: "meta",  
    properties: {  
      name: "generator",  
      content: "Hostinger Website builder"  
    }  
  })  
}
```

Figure 7 Source code for plessy[.]eu website

Meta-name sourced from the Plessy website:

Explore the dark secrets of Mr.Plessy, the mastermind behind MadCat Ransomware and other projects. Join us on an exciting journey into the world of cybercrime. Stay tuned for more

On the subpage Blog - date of entry 26.10.2023 (hxxps://plessy[.]eu/hackers-resources-and-tools0) there is a logo with the content: MADCAT Ransomware.



Figure 8 MADCAT Ransomware logo

TOR - MADCAT Ransomware.

URL: hxxp://i2gc52bwm2vu2wnohwi3cli7t7hj3y2q7qj3th2bs64h2eej7z5jcgqd[.]onion/

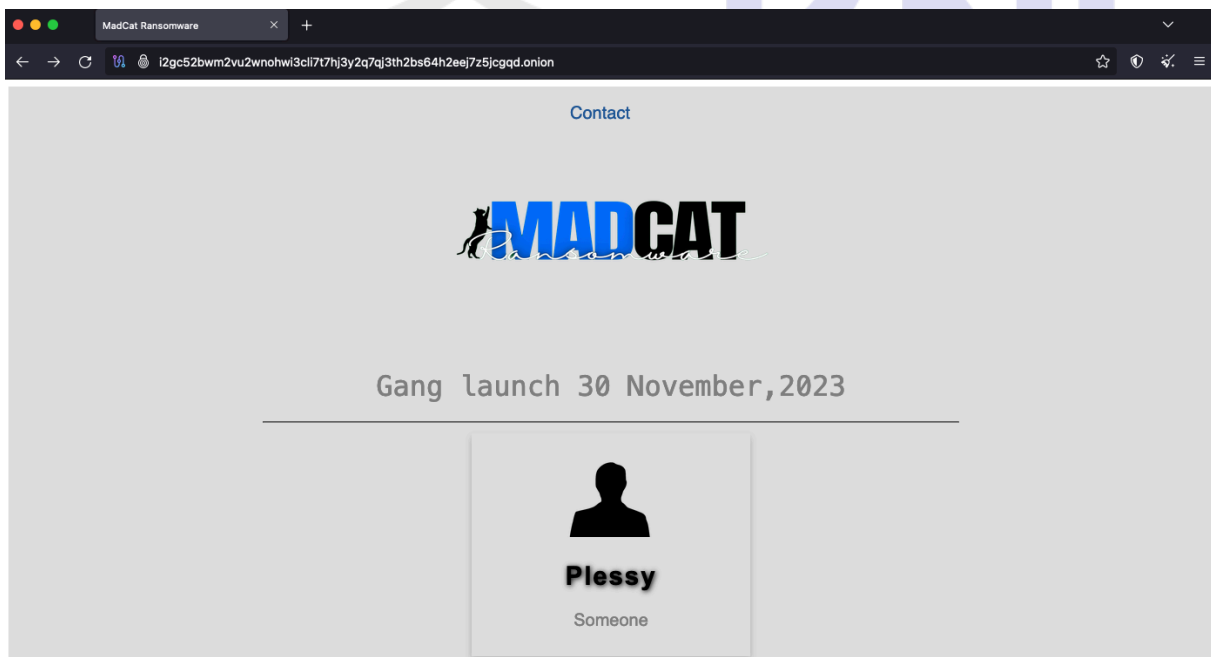


Figure 9 Home page of the MADCAT Ransomware website.

The MADCAT Ransomware logo, identical to the one seen on the plessy[.]eu website in the Blog section, appears on the main page on the TOR network. Also present is the caption: "The gang launches November 30, 2023," which may indicate that the group has not yet officially begun operations.

The person listed on this page is a user with the nickname **Plessy**, which most likely points to the same person who made the post on the breachforums forum.

In the Contact Us section of the MADCAT Ransomware website, there is brief information relating to preferred communication channels:



In addition to those seen on the Breachforums forum, you'll also find an email address: plessys@proton[.]me.

Remaining analysis:

Telegram: @shinyenigma

Looking for information about the user who was linked on plessy[.]eu, one can find a profile on Github.com with the same name (<https://github.com/Shinyenigma>).

The aforementioned user publishes source codes of malware (stealer, RAT) on his profile:

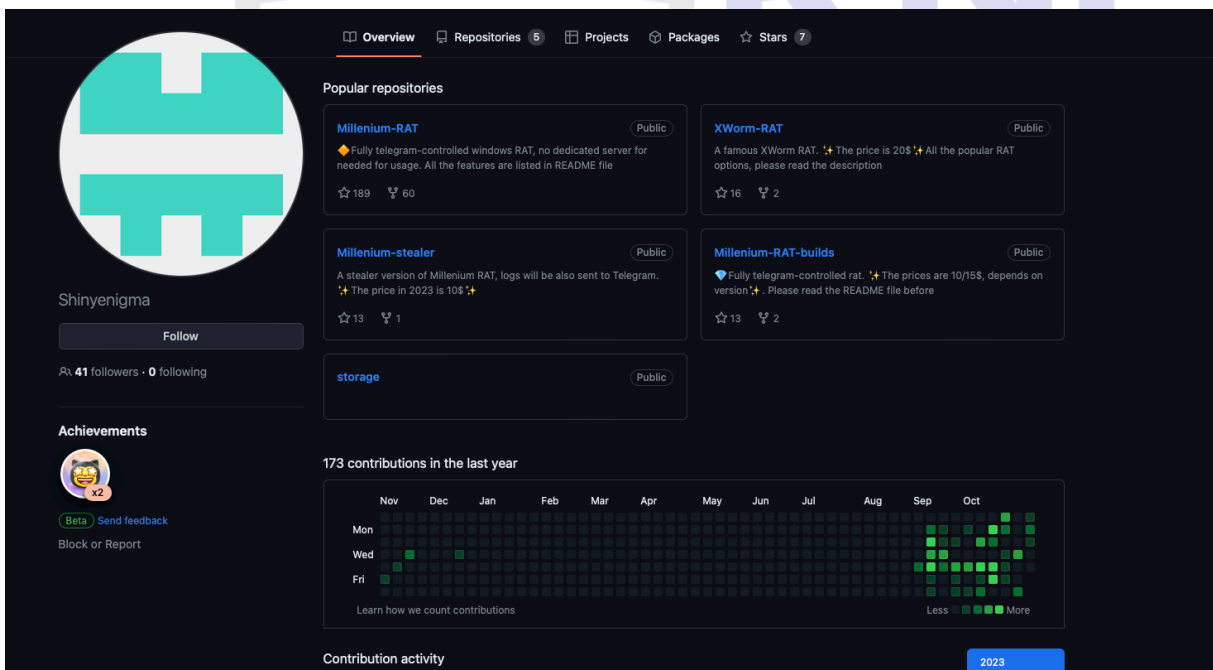


Figure 10 <https://github.com/Shinyenigma>

Ransomware and scams

On the Internet you can find notes that the Madcat ransomware group leaves its victims:

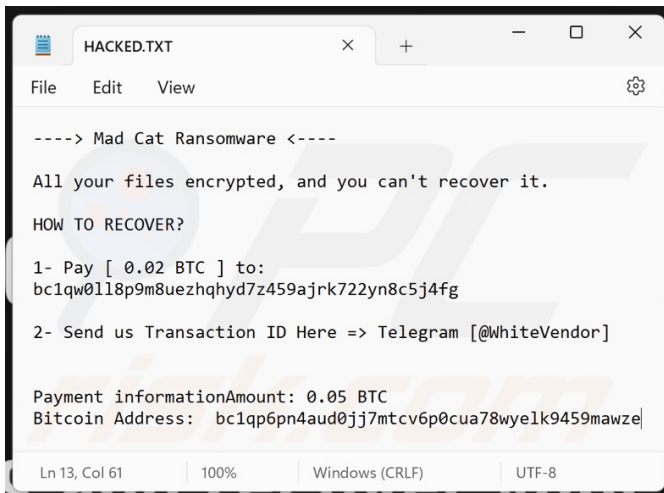


Figure 11 <https://www.pcrisk.pl/narzedzia-usuwania/12395-mad-cat-ransomware>

Note the Telegram account: **@WhiteVendor**, whose profile looks like this:

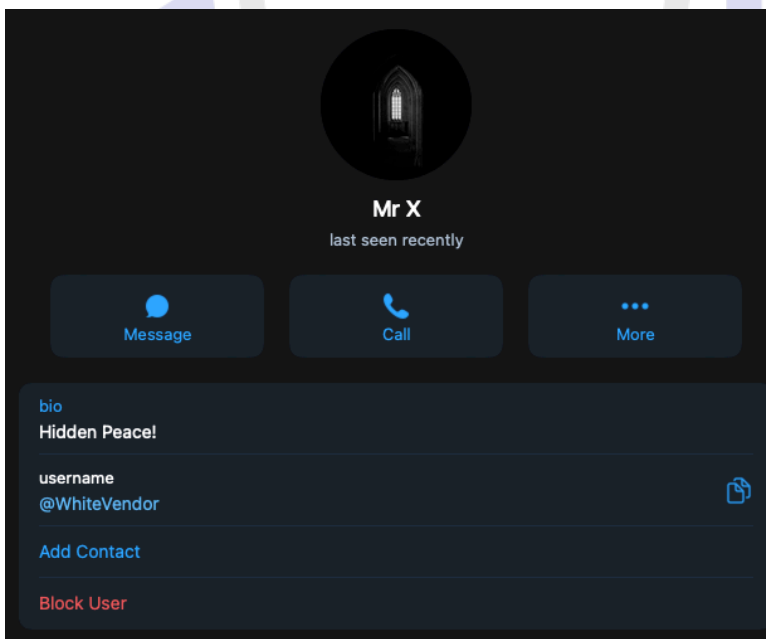


Figure 12 @WhiteVendor

User @WhiteVendor also has an account on breachforums[.]is, where he has taken a username as - **Rooted**:

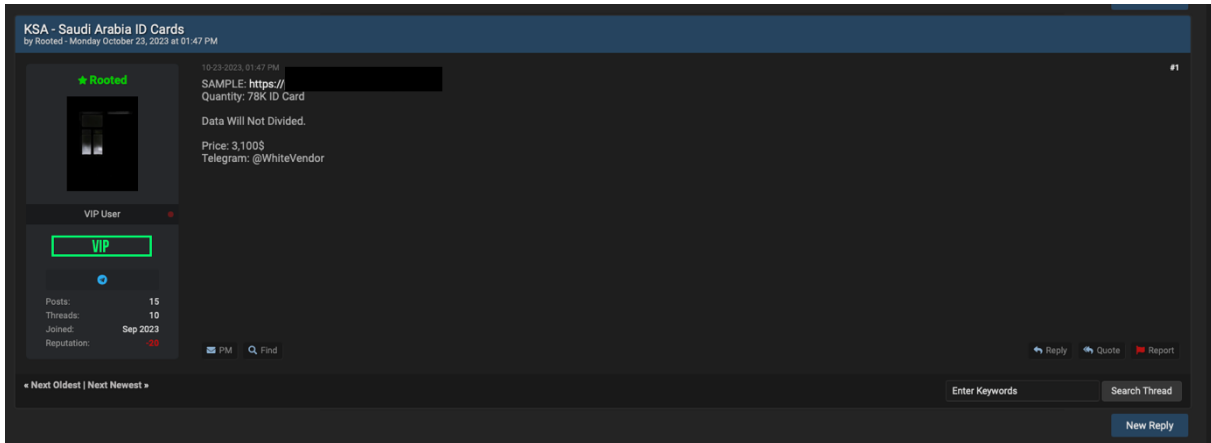


Figure 13

You can see that the way of presenting information regarding files for sale is very similar to that of user @Plessy.

The threads on breachforums[.]is forum created by user @Rooted mainly refer to document files (passports, IDs):

Thread Title	Category	Replies	Views	Last Post
RagnarLocker Ransomware seized! (1 2)	World News	12	1,213	10-26-2023, 02:59 PM Last Post: Katz
SELLING China/Japan Passports HQ First Hand	Leaks Market	2	782	10-26-2023, 07:26 AM Last Post: johnhanna
SELLING KSA - Saudi Arabia ID Cards	Leaks Market	0	268	10-23-2023, 01:47 PM Last Post: Rooted
KSA - Saudi Arabia DB	Sellers Place	1	672	10-23-2023, 08:06 AM Last Post: adstfdasgsdggag
SELLING Morocco Passports Database [5G]	Leaks Market	1	599	10-22-2023, 09:17 PM Last Post: kamakox
SELLING Korea Passports Database	Leaks Market	0	503	10-22-2023, 01:00 AM Last Post: Rooted
Kuwait Documents Database [Priv8 Leak] (1 2)	Other Leaks	10	3,934	10-12-2023, 12:52 AM Last Post: hoube97
Egypt Citizen Database	Sellers Place	0	421	10-10-2023, 02:18 AM Last Post: Rooted
Telene Group Cell_Phone Database	Databases	5	1,692	10-05-2023, 08:37 AM Last Post: VIPLeads
Kuwait Passports PDF - NEW	Other Leaks	2	734	09-30-2023, 02:30 AM Last Post: Rooted

Figure 14

It is interesting to note that user @Rooted, to sell passports from China and Japan, cheated his customer out of 19.5 XMR:

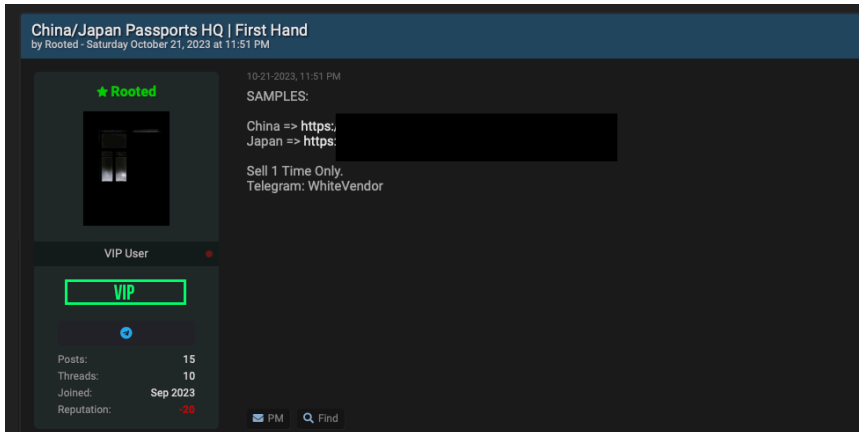


Figure 15

As evidenced by the review of a dissatisfied customer:

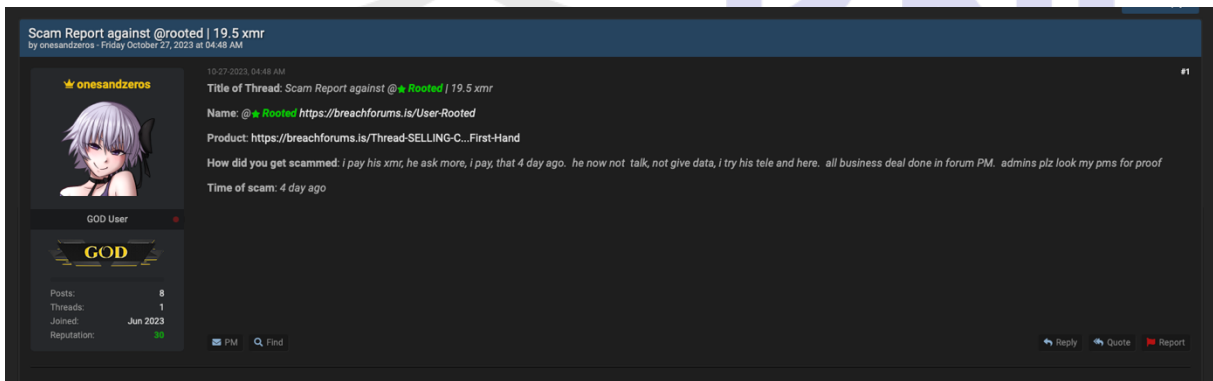


Figure 16

Conclusion:

The analysis conducted showed significant indications suggesting that Plessy and WhiteVendor users may be the same person. Such conclusions are based on observation of the writing style, methods of creating threads and the sales profile, which focuses on identity documents, including passports and IDs. It was noted that in the face of negative feedback regarding the attempt to sell documents from China and Japan, user WhiteVendor abandoned the use of his account and started a new online business under the pseudonym @Plessy - also as a scammer.

Further evidence irrefutably points to a link between the two users and the MADCAT ransomware group. In particular, the victims are contacted through the @WhiteVendor Telegram account, highlighting the link between these identities and the group's criminal activity.

A simplified diagram of relationships, based on the above analysis:

