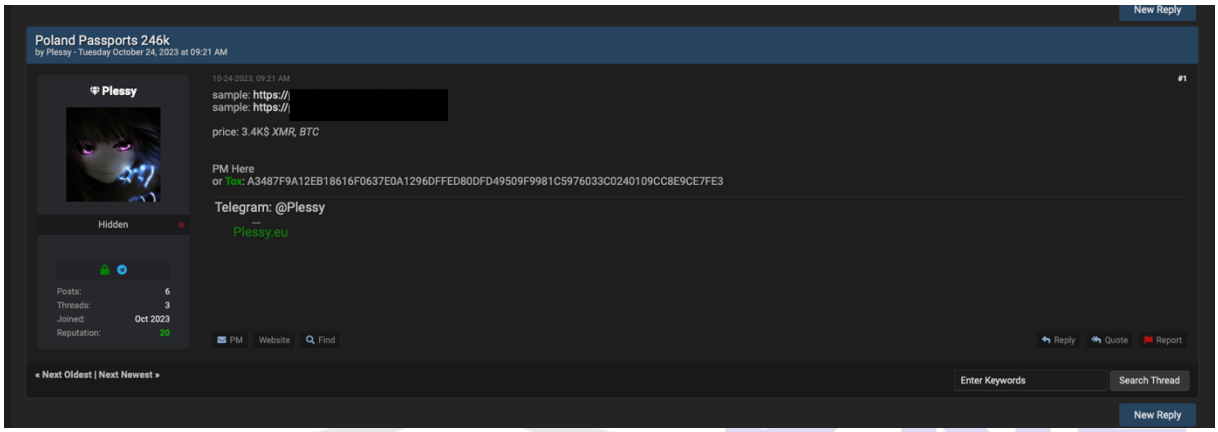
MADCAT RANSOMWARE – wielowymiarowe przestępstwo

Opis analizy:

W dniu 31.10.2023 roku na forum breachforums[.]is użytkownik o nazwie: Plessy opublikował post, w którym ogłasza sprzedaż 246.000 skanów paszportów, pochodzących z Polski.

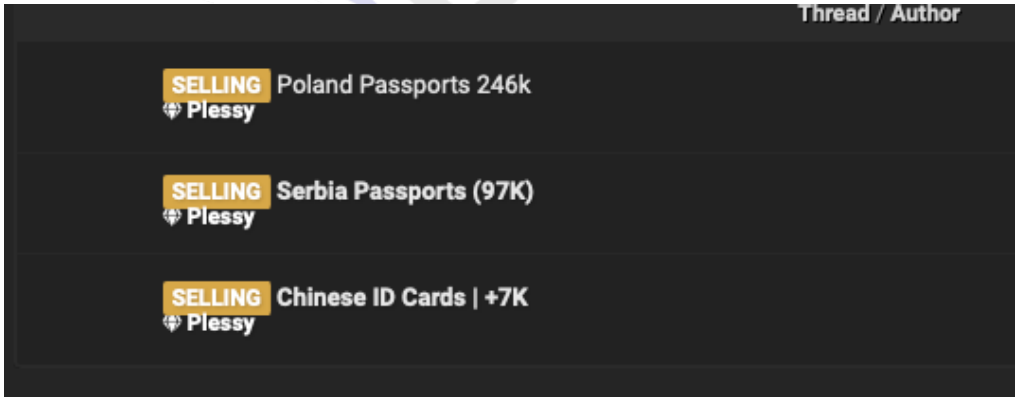


Rysunek 1 – Wątek o sprzedaży dokumentów z Polski.

Za całość tej nielegalnej kolekcji, Plessy żąda sumy 3.400 USD, preferując płatności w kryptowalutach takich jak Monero (XMR) lub Bitcoin (BTC).

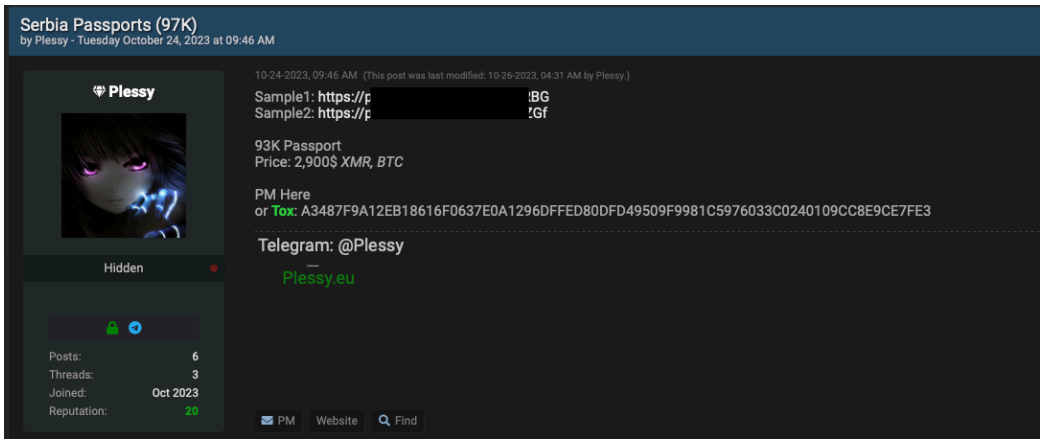
Jako dowód autentyczności swojej oferty, Plessy opublikował linki do próbek paszportów, które twierdzi, że ma w swoim posiadaniu.

Ponadto, wspomniany użytkownik deklaruje posiadanie do sprzedaży innych baz z dokumentami:



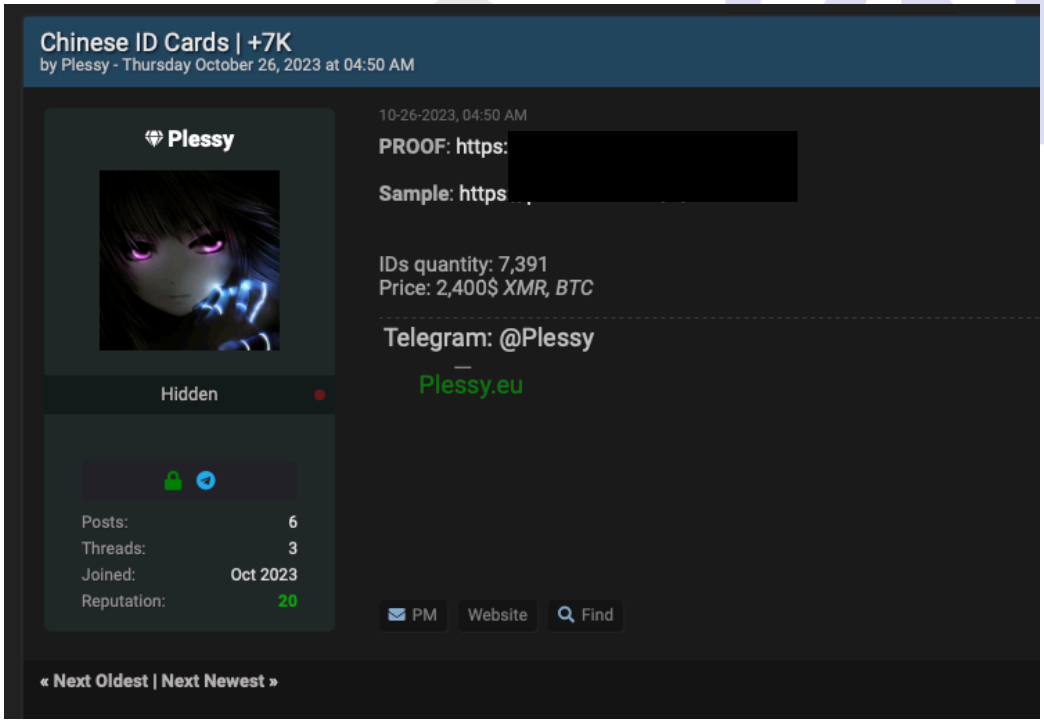
Rysunek 2 Wszystkie wątki utworzone przez użytkownika @Plessy.

Paszporty – Serbia:



Rysunek 3 Wątek o sprzedaży dokumentów z Serbii

ID Cards – Chiny:



Rysunek 4 Wątek o sprzedaży dokumentów z Chin

Analiza Profilu Użytkownika 'Plessy' na Breachforums

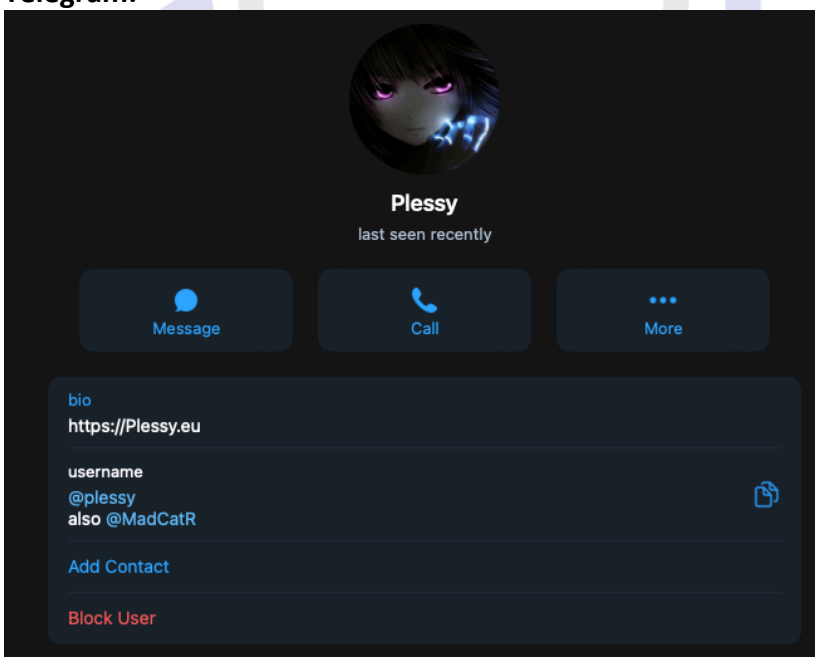
Data Założenia Konta: 23 października 2023 r.

Aktywność na Forum:
Plessy wykazuje ograniczoną aktywność poza własnymi wątkami. Zauważono jego udział w dwóch dyskusjach: jedna dotyczyła wycieku danych QiCard w Iraku, a druga – incydentu bezpieczeństwa w serwisie eKosova.

Szczegóły jego aktywności można śledzić pod linkiem:
hxxps://breachforums[.]is/search.php?action=results&sid=8b986392ea7dd81c124be0561efcdc0b.

Metody Kontaktu Podane przez Plessy'ego:
Telegram: @Plessy
Strona internetowa: Plessy[.]eu
Tox (Secure Messaging):
A3487F9A12EB18616F0637E0A1296DFFED80DFD49509F9981C5976033C0240109CC8E9CE7FE3

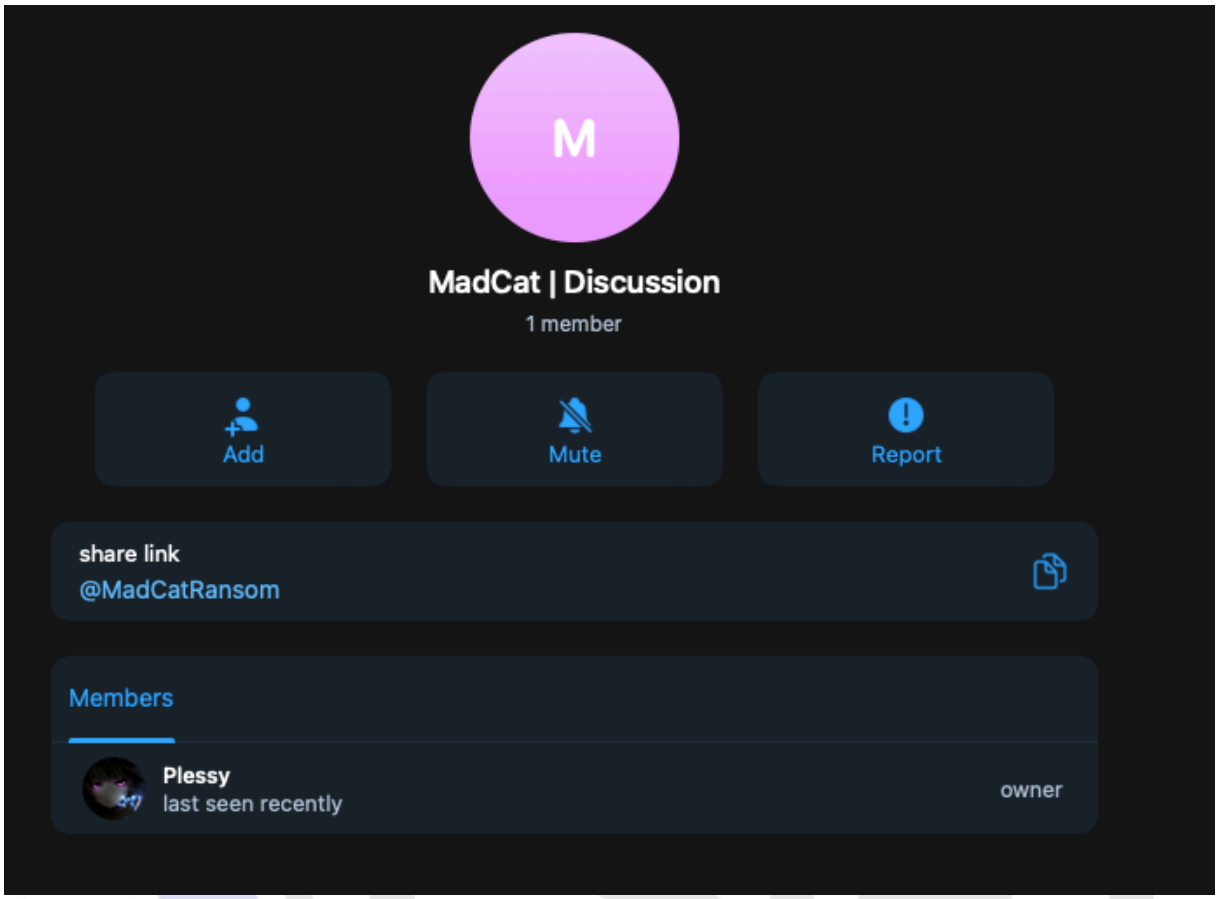
Telegram:



Rysunek 4 Telegram @plessy

W biografii w komunikatorze Telegram zostały wypisane:
- adres www strony internetowej: plessy[.]eu
- nazwy użytkowników: @plessy oraz @MadCatR

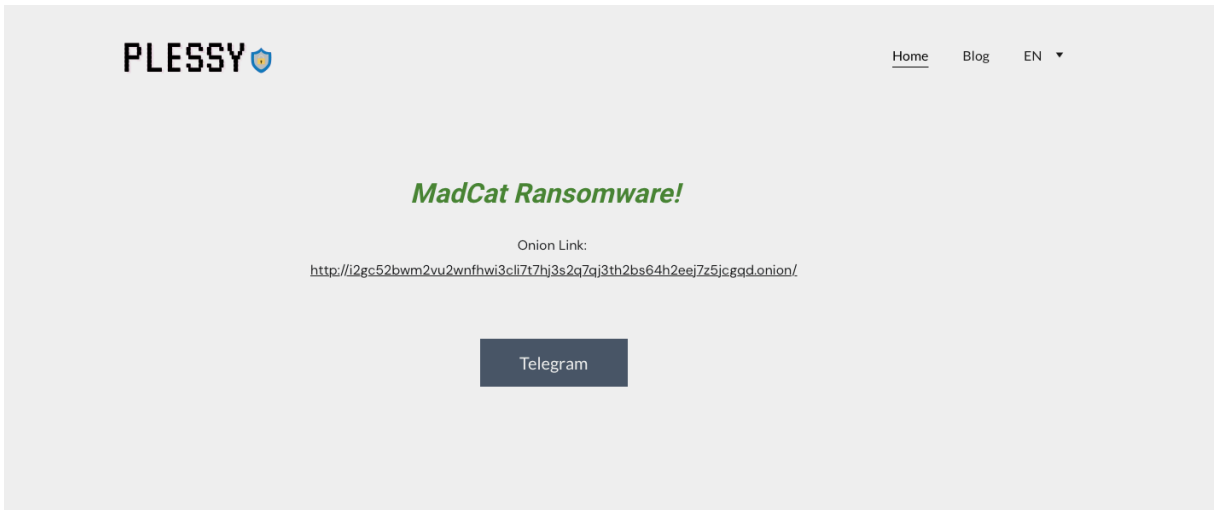
Podczas wyszukiwania konta **@MadCatR** możemy znaleźć powiązany kanał:



Rysunek 5 Kanał MadCatRansom

Kanał to @MadCatRansom, gdzie jedynym użytkownikiem jest użytkownik **@Plessy**. Sama nazwa kanału sugeruję, że może być to grupa **Ransomware**.

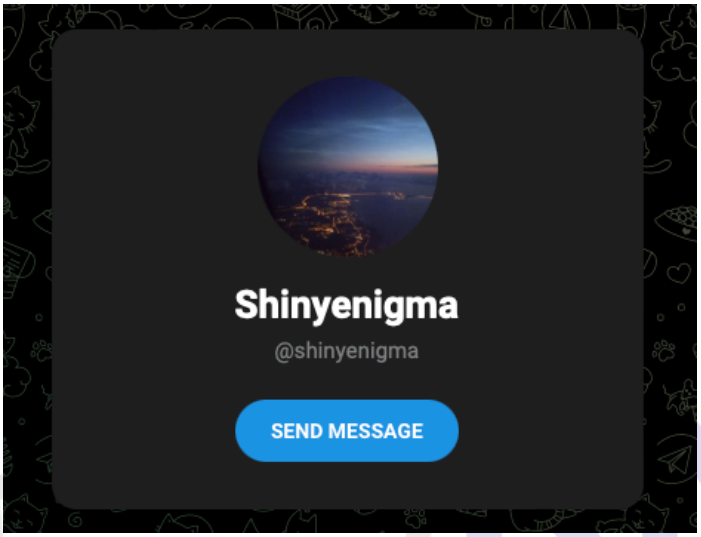
Strona internetowa:



Rysunek 6 Strona internetowa plessy[.]eu

Na stronie głównej plessy[.]eu znajduje się link URL, który przekierowuje do strony w sieci TOR pod adresem:
hxxp://i2gc52bwm2vu2wnohwi3cli7t7hj3y2q7qj3th2bs64h2eej7z5jcgqd[.]onion.

Ponadto, na tej samej stronie, pod ikoną Telegrama, umieszczono odnośnik do profilu użytkownika @shinyenigma na platformie Telegram:



Rysunek 7 @shinyenigma

Strona Plessy[.]eu została zbudowana za pomocą kreatora stron internetowych: Hostinger Website Builder:

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

Rysunek 8 Kod źródłowy strony plessy[.]eu

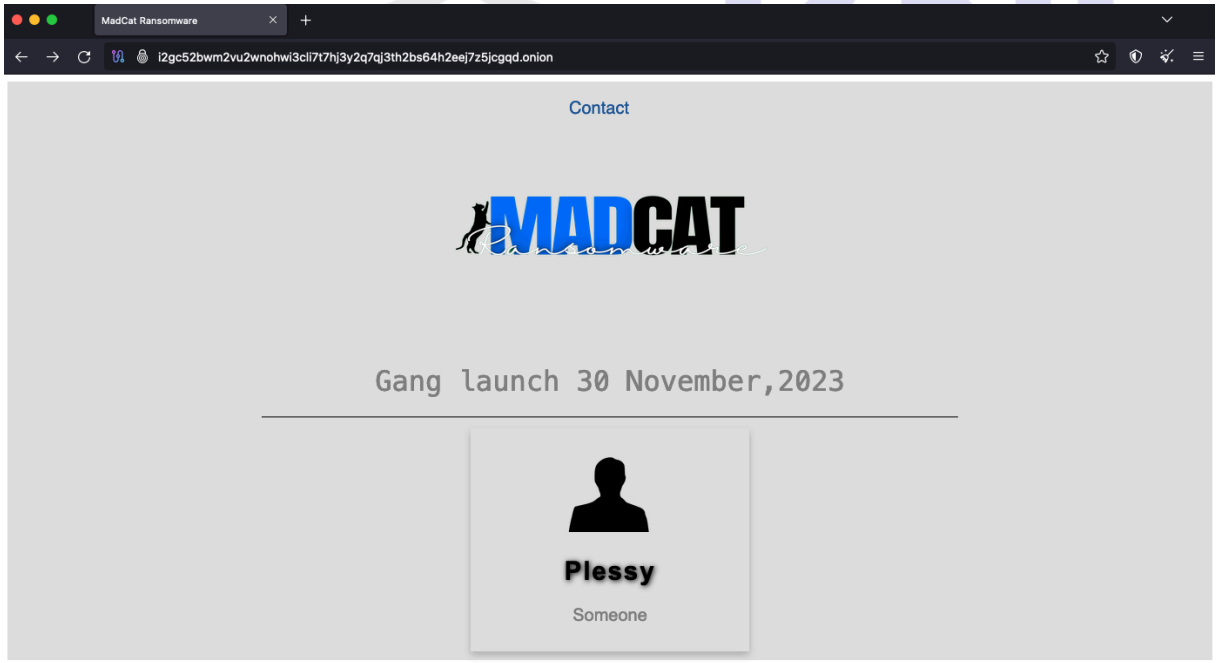
Meta-name pochodzący ze strony Plessy:

```
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
```

Na podstronie Blog – data wpisu 26.10.2023 (hxxps://plessy[.]eu/hackers-resources-and-tools0) widnieje logo z treścią: MADCAT Ransomware.

Rysunek 9 logo MADCAT Ransomware

TOR - MADCAT Ransomware
URL: hxxp://i2gc52bwm2vu2wnohwi3cli7t7hj3y2q7qj3th2bs64h2eej7z5jcgqd[.]onion/

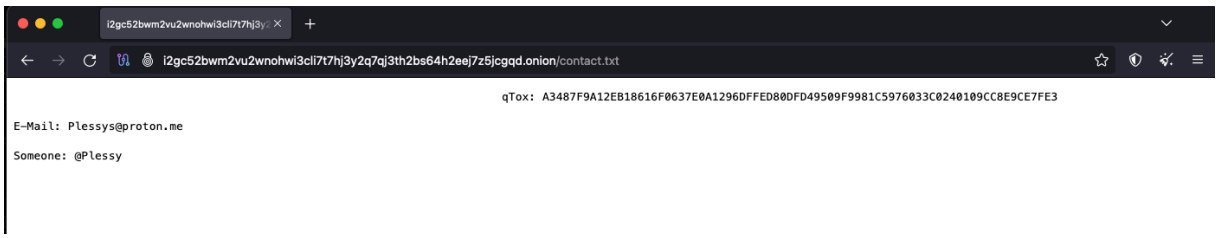


Rysunek 10 Strona główna strony MADCAT Ransomware

Na głównej stronie w sieci TOR pojawia się logo MADCAT Ransomware, identyczne z tym, które było widoczne na stronie plessy[.]eu w dziale Blog. Obecny jest również napis: „Gang startuje 30 listopada 2023”, co może wskazywać, że grupa ta nie rozpoczęła jeszcze oficjalnie działalności.

Osoba wymieniona na tej stronie jest użytkownikiem o pseudonimie **Plessy**, co najprawdopodobniej wskazuje na tę samą osobę, która zamieściła post na forum breachforums.

W dziale Kontakt na stronie MADCAT Ransomware znajduje się krótka informacja odnosząca się do preferowanych kanałów komunikacji:

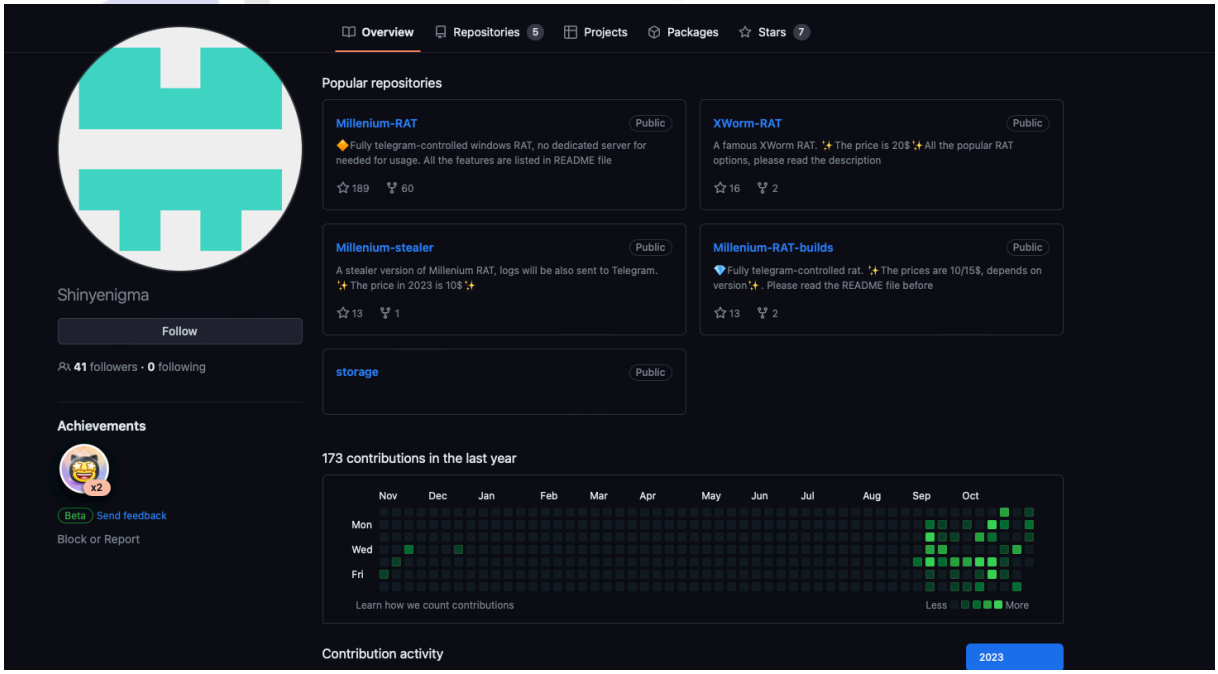


Prócz tych, które można było zobaczyć na forum Breachforums, znajdziemy również adres mailowy: plessys@proton[.]me.

Pozostała analiza:
Telegram: @shinyenigma

Szukając informacji o użytkowniku, który był podlinkowany na stronie plessy[.]eu, można znaleźć profil na Github.com o tożsamej nazwie (https://github.com/Shinyenigma).

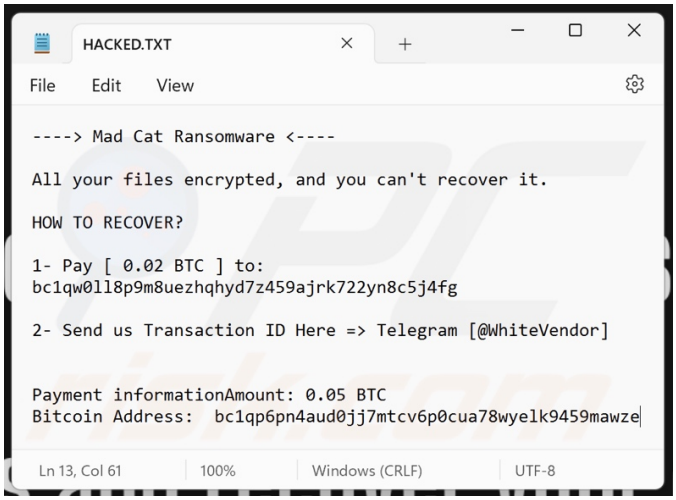
Ww. użytkownik na profilu publikuje kody źródłowe malware (stealer, RAT):



Rysunek 11 https://github.com/Shinyenigma

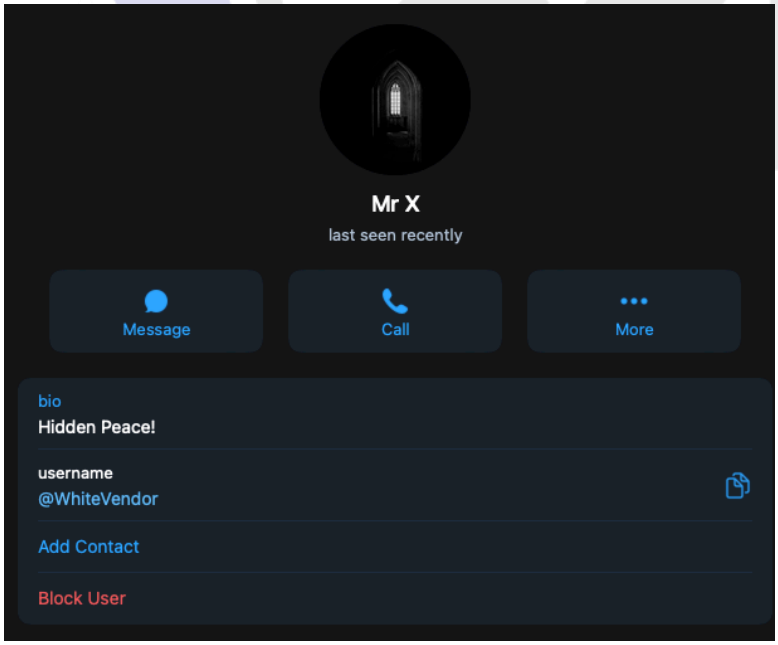
Ransomware i oszustwa

W Internecie można odnaleźć notatki jakie zostawia swoim ofiarom grupa Ransomware Madcat:



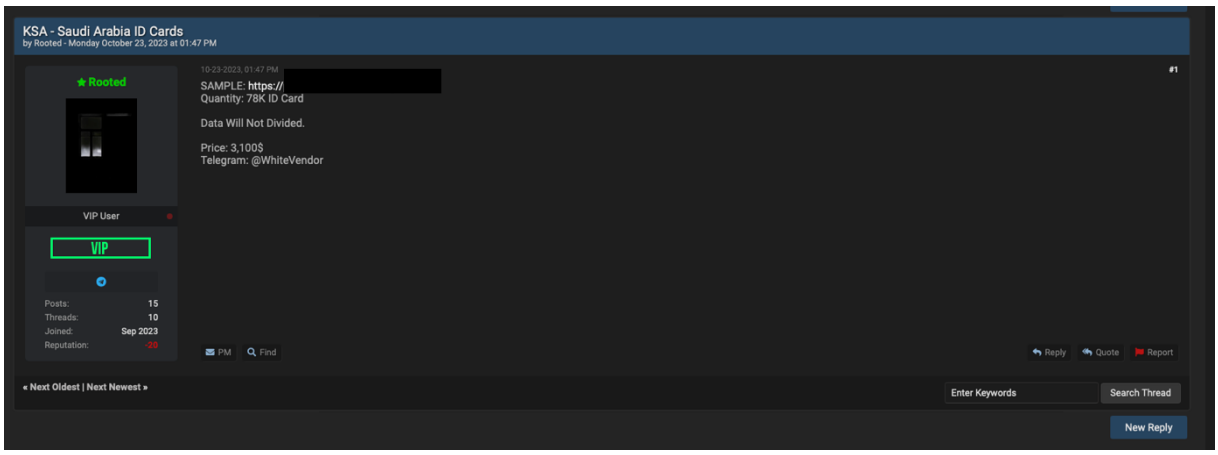
Rysunek 12 https://www.pcrisk.pl/narzedzia-usuwania/12395-mad-cat-ransomware

Należy zwrócić uwagę na konto Telegram: @WhiteVendor, którego profil prezentuje się w ten sposób:



Rysunek 13 @WhiteVendor

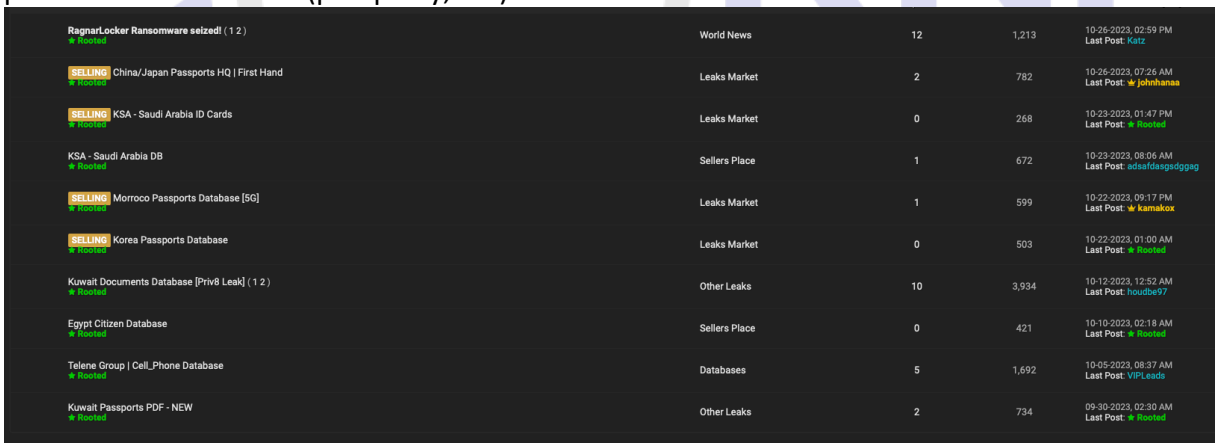
Użytkownik @WhiteVendor posiada również konto na breachforums[.]is, gdzie przybrał nazwę użytkownika jako – **Rooted:**



Rysunek 14 Sprzedaż dokumentów z Arabii Saudyjskiej.

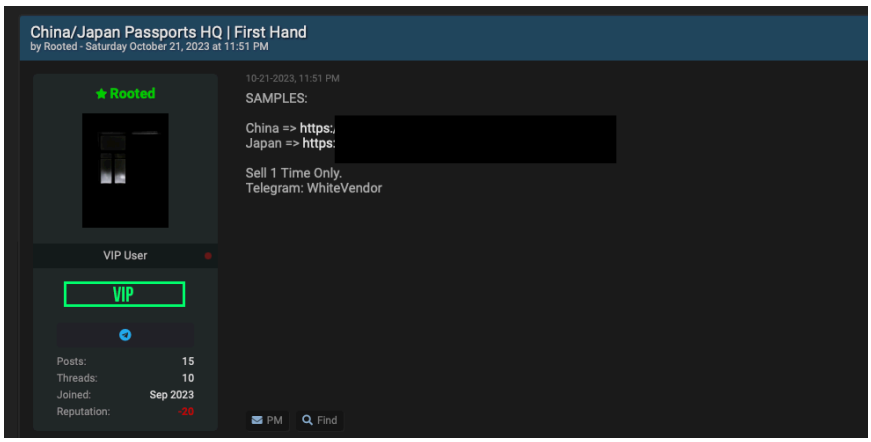
Można zauważyć, że sposób przedstawiania informacji dotyczącej plików na sprzedaż jest bardzo podobny jak w przypadku użytkownika @**Plessy**.

Wątki na forum breachforums[.]is, które tworzył użytkownik @**Rooted** nawiązują głównie do plików z dokumentami (paszporty, IDs):



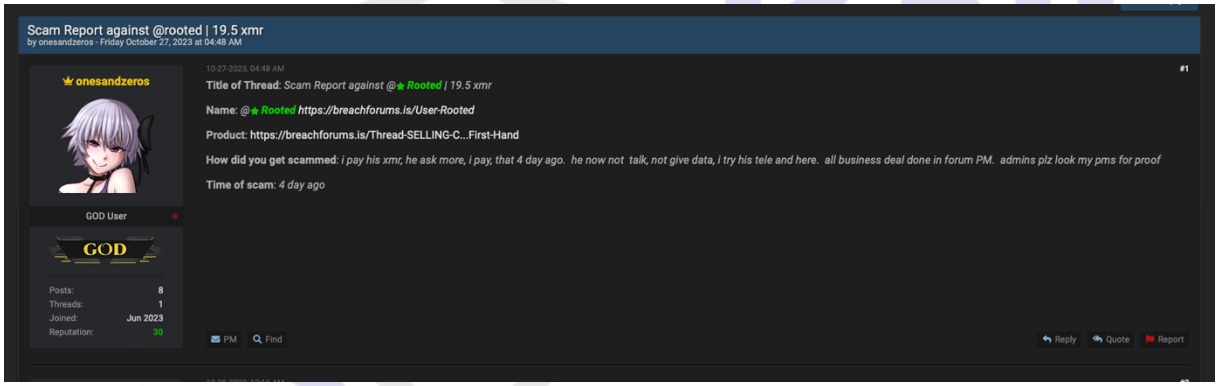
Rysunek 15 Wszystkie wątki utworzone przez użytkownika @Rooted.

Ciekawostką jest to, że użytkownik @Rooted przy próbie sprzedaży paszportów z Chin oraz Japonii, oszukał swojego klienta na 19.5 XMR:



Rysunek 16 Sprzedaż dokumentów z Chin oraz Japonii.

Czego dowodem jest recenzja niezadowolonego klienta:



Rysunek 17 Recenzja użytkownika, który zakupił dokumenty.

Podsumowanie:

Przeprowadzona analiza wykazała istotne przesłanki sugerujące, że użytkownicy Plessy i WhiteVendor mogą być tą samą osobą. Takie wnioski nasuwają się na podstawie obserwacji stylu pisania, metod tworzenia wątków oraz profilu sprzedaży, który skupia się na dokumentach tożsamości, w tym paszportach i ID. Zwrócono uwagę, że w obliczu negatywnych opinii dotyczących próby sprzedaży dokumentów z Chin i Japonii, użytkownik WhiteVendor zaniechał korzystania ze swojego konta i pod pseudonimem @Plessy rozpoczął nową działalność online – również jako oszust.

Dalsze dowody wskazują nieodwołalnie na powiązanie obu użytkowników z grupą ransomware MADCAT. W szczególności, kontakt z ofiarami odbywa się poprzez konto na Telegramie @WhiteVendor, co podkreśla związek między tymi tożsamościami, a przestępczą aktywnością grupy.

Uproszczony schemat powiązań, na podstawie powyższej analizy: