On the Horizon: Ransomed.vc Ransomware Group Spotted in the Wild

socradar.io/on-the-horizon-ransomed-vc-ransomware-group-spotted-in-the-wild/

August 21, 2023

[Update] November 9, 2023: "End of an Era, the Sinking of Ransomed.VC"

[Update] October 5, 2023: See the subheading: "RansomedVC De-anonymized Itself After Moving to WordPress."

[Update] October 2, 2023: See the subheadings: "RansomedVC Partners with STORMOUS Hackers," and "The Outcome of the Sony Leak."

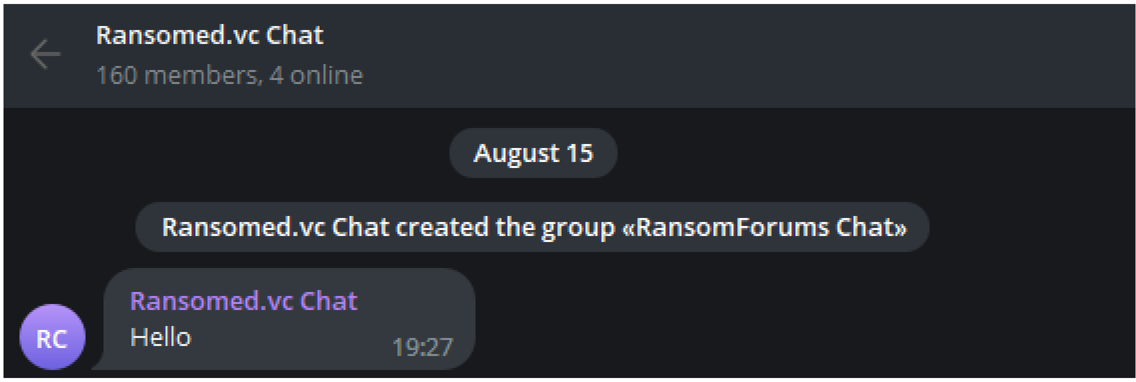
[Update] September 15, 2023: See the subheading: "Ransomed.vc Interview."

[Update] September 4, 2023: The Ransomed team is collaborating with Everest Ransomware, read more under: "Old Ties, New Threats: Everest Echoes."

[Update] August 24, 2023: Added subheadings: "Ransomed.vc Lists Three New Victims and Receives Payment for a Previous Attack," "An Extortion Approach That Utilizes GDPR Fines."

We have been monitoring Telegram for a long time as many of the threat actors and dark web activities are also actively running on Telegram. A Telegram group that we previously monitored as **RansomForums** had recently announced that they would be doing a project called **Ransomed.vc**.

The group's owner has renamed his private chat room to Ransomed.vc Chat:



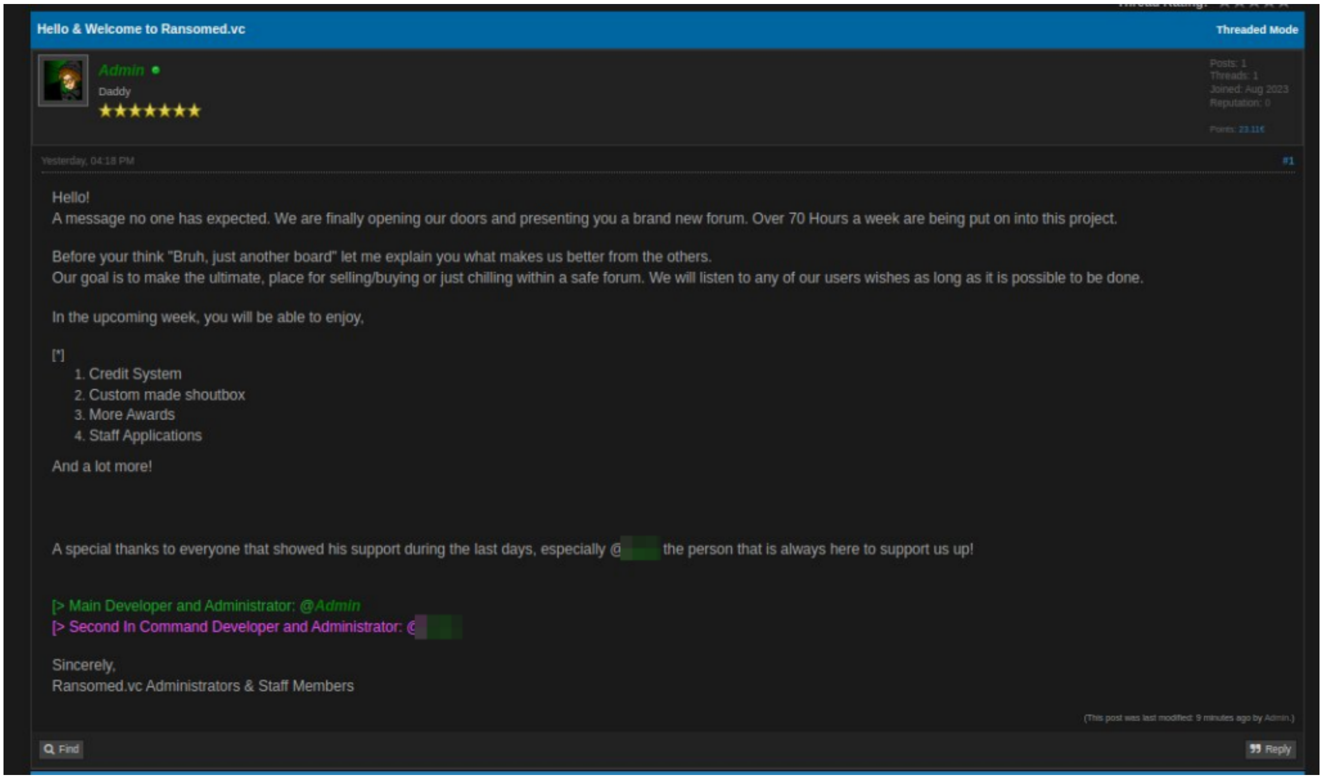
Ransomed.vc Chat
160 members, 4 online

August 15

Ransomed.vc Chat created the group «RansomForums Chat»

Ransomed.vc Chat
Hello 19:27

Figure. 1. First Message of Ransomed.vc Chat room



Hello & Welcome to Ransomed.vc

Admin

Daddy

Posts: 1
Threads: 1
Joined: Aug 2023
Reputation: 0

Points: 23.11€

Yesterday, 04:18 PM #1

Hello!
A message no one has expected. We are finally opening our doors and presenting you a brand new forum. Over 70 Hours a week are being put on into this project.

Before your think "Bruh, just another board" let me explain you what makes us better from the others.
Our goal is to make the ultimate, place for selling/buying or just chilling within a safe forum. We will listen to any of our users wishes as long as it is possible to be done.

In the upcoming week, you will be able to enjoy,

[*]

1. Credit System
2. Custom made shoutbox
3. More Awards
4. Staff Applications

And a lot more!

A special thanks to everyone that showed his support during the last days, especially @[redacted] the person that is always here to support us up!

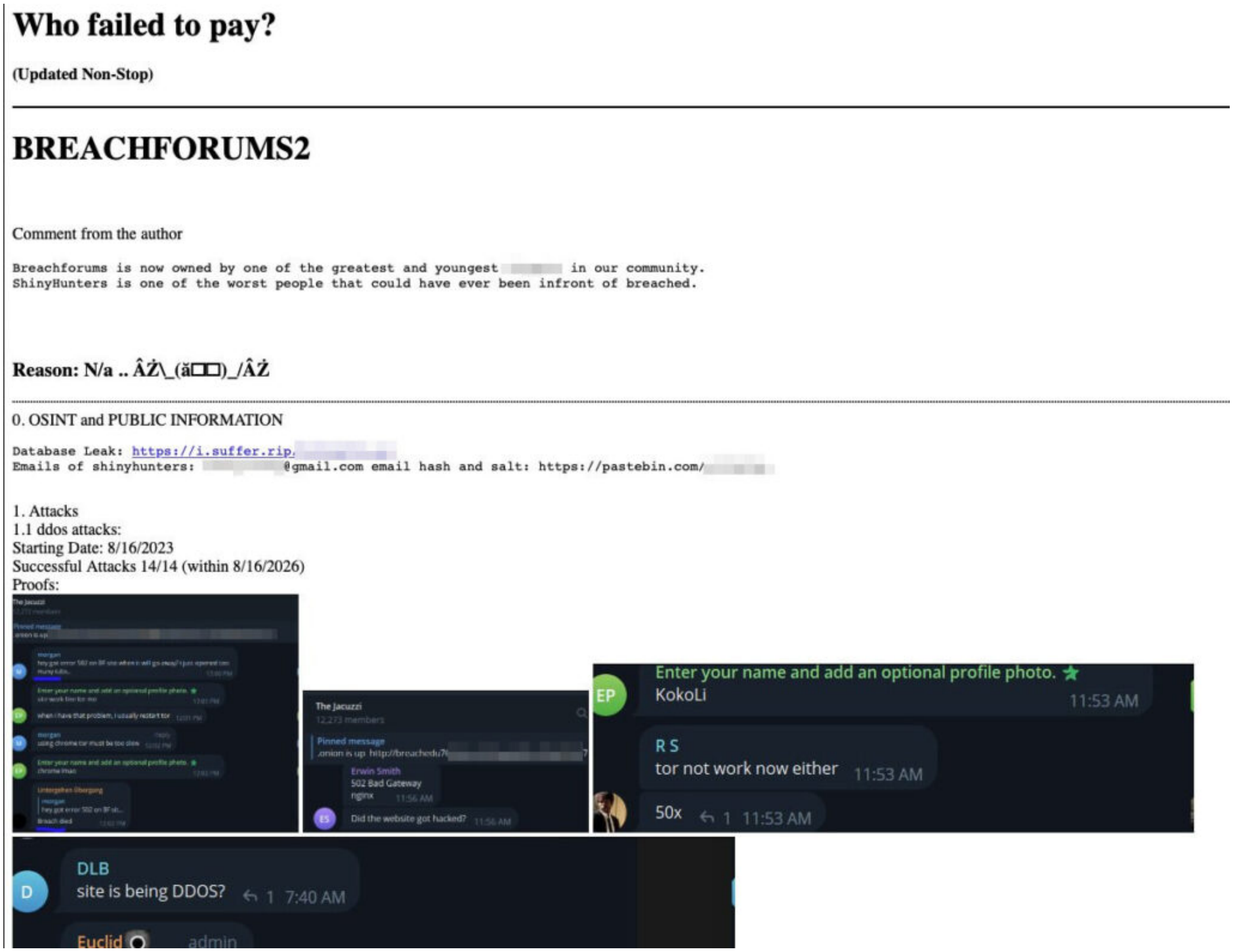
[> Main Developer and Administrator: @*Admin*
[> Second In Command Developer and Administrator: @[redacted]

Sincerely,
Ransomed.vc Administrators & Staff Members

(This post was last modified: 9 minutes ago by Admin.)

Figure 2. Welcome post of Ransomed.vc (Source: FalconFeedsio)

However, the site suffered a DDoS attack shortly after its launch and was dubbed BreachForums2 by the attackers:



Who failed to pay?

(Updated Non-Stop)

BREACHFORUMS2

Comment from the author

```
Breachforums is now owned by one of the greatest and youngest [redacted] in our community.
ShinyHunters is one of the worst people that could have ever been infront of breached.
```

Reason: N/a .. ÂŻ_(ă□□)_/ÂŻ

0. OSINT and PUBLIC INFORMATION

```
Database Leak: https://i.suffer.rip/[redacted]
Emails of shinyhunters: [redacted]@gmail.com email hash and salt: https://pastebin.com/[redacted]
```

1. Attacks
1.1 ddos attacks:
Starting Date: 8/16/2023
Successful Attacks 14/14 (within 8/16/2026)
Proofs:

The Jacuzzi
12,273 members
Pinned message
.onion is up [redacted]

morgan
hey got error 502 on BF site when it will go away? i just opened too many tabs..

Enter your name and add an optional profile photo. ★
site work fine for me

when i have that problem, i usually restart tor

morgan
using chrome tor must be too slow

Enter your name and add an optional profile photo. ★
chrome lman

[illegible]
morgan
hey got error 502 on BF sit...
Breach died

The Jacuzzi
12,273 members
Pinned message
.onion is up http://breachedu7[redacted]

Erwin Smith
502 Bad Gateway
nginx 11:56 AM

Did the website got hacked? 11:56 AM

Enter your name and add an optional profile photo. ★
KokoLi 11:53 AM

R S
tor not work now either 11:53 AM

50x ↩ 1 11:53 AM

DLB
site is being DDOS? ↩ 1 7:40 AM

Euclid admin

Figure 3. Ransomed.vc's screenshot after being attacked (Source: Karol Paciorek)

Another Twitter user also discovered that RansomForums' favicon icon looks the same as BreachForums' favicon.

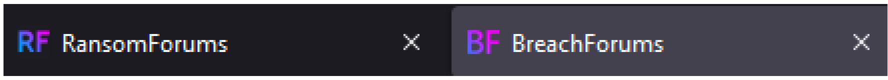
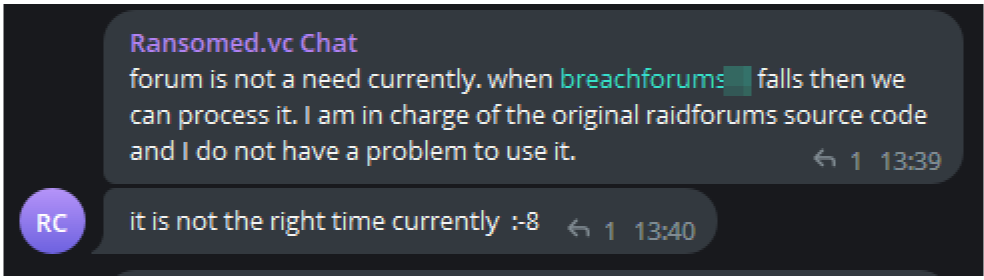


Figure 4. Favicons of RansomForums and BreachForums (Source: Crocodyli)

According to the group owner's chat messages, the admin will not use the forum for a while until Breachforums is closed and he has the source code of RaidForums:

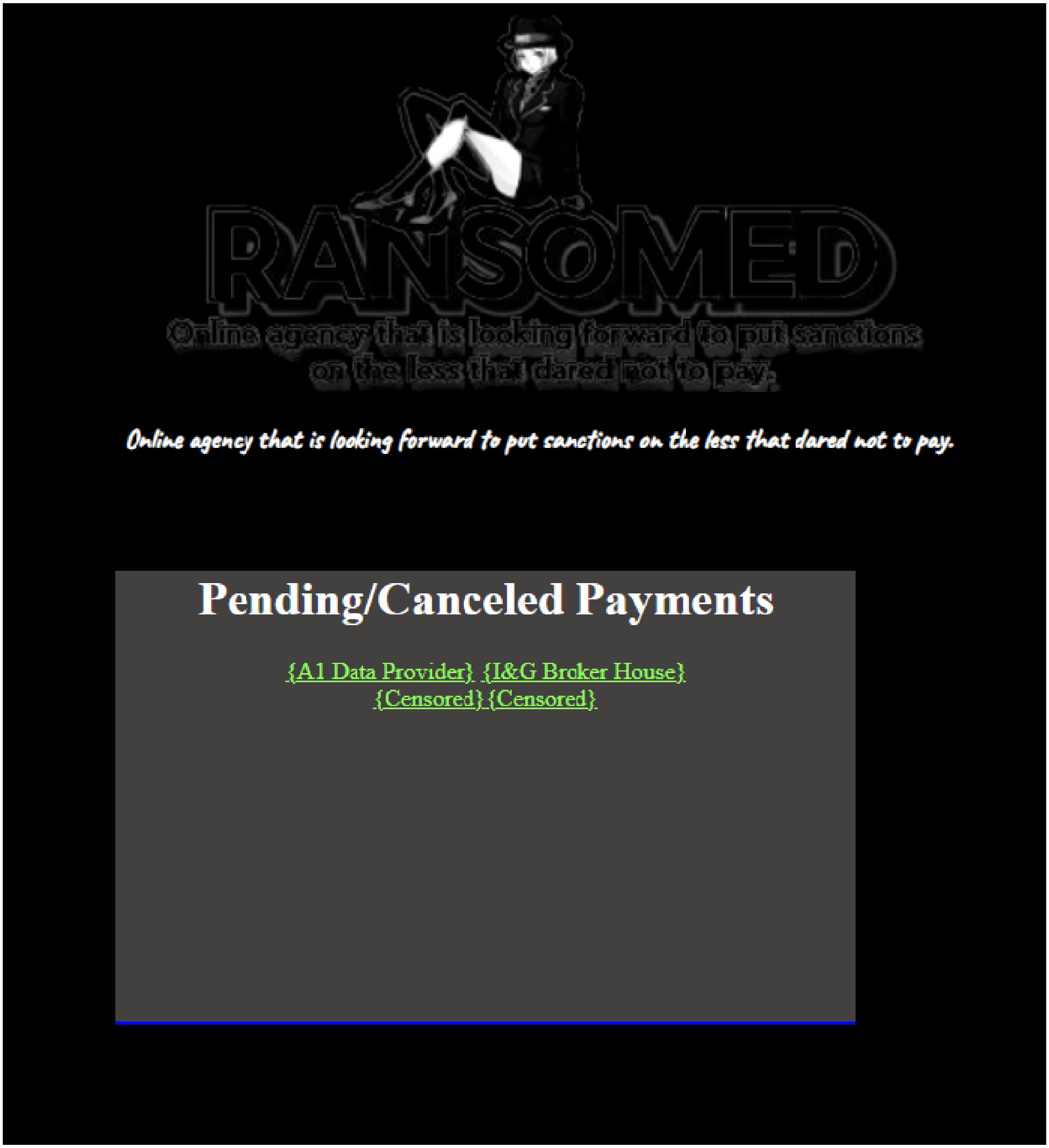


Ransomed.vc Chat
forum is not a need currently. when breachforums[redacted] falls then we can process it. I am in charge of the original raidforums source code and I do not have a problem to use it. ↩ 1 13:39

RC
it is not the right time currently :-8 ↩ 1 13:40

Figure 5. Telegram group owner's statement

After this process, Ransomed.vc was transformed into a site sharing ransom victims:


RANSOMED
Online agency that is looking forward to put sanctions on the less that dared not to pay.

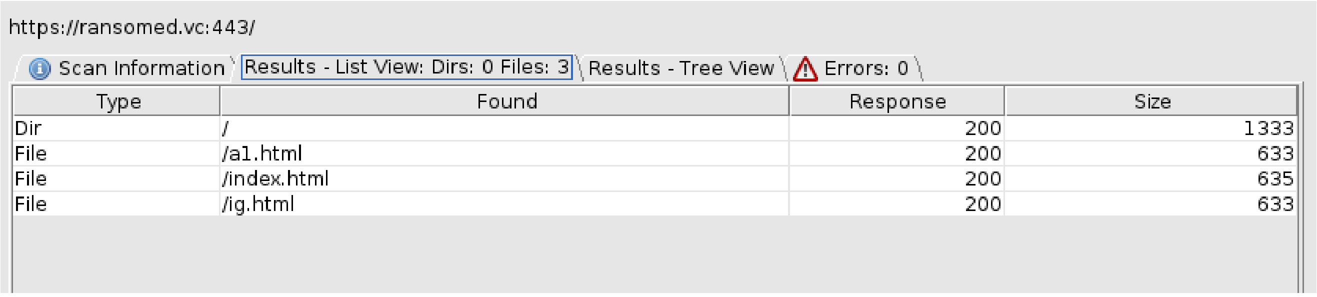
Online agency that is looking forward to put sanctions on the less that dared not to pay.

Pending/Canceled Payments

{A1 Data Provider} {I&G Broker House}
{Censored} {Censored}

Figure 6. Main page of Ransomed.vc

When we search the directories of the page domain, we see that they do not have any other **subpages** other than the ones they have shared at the moment:

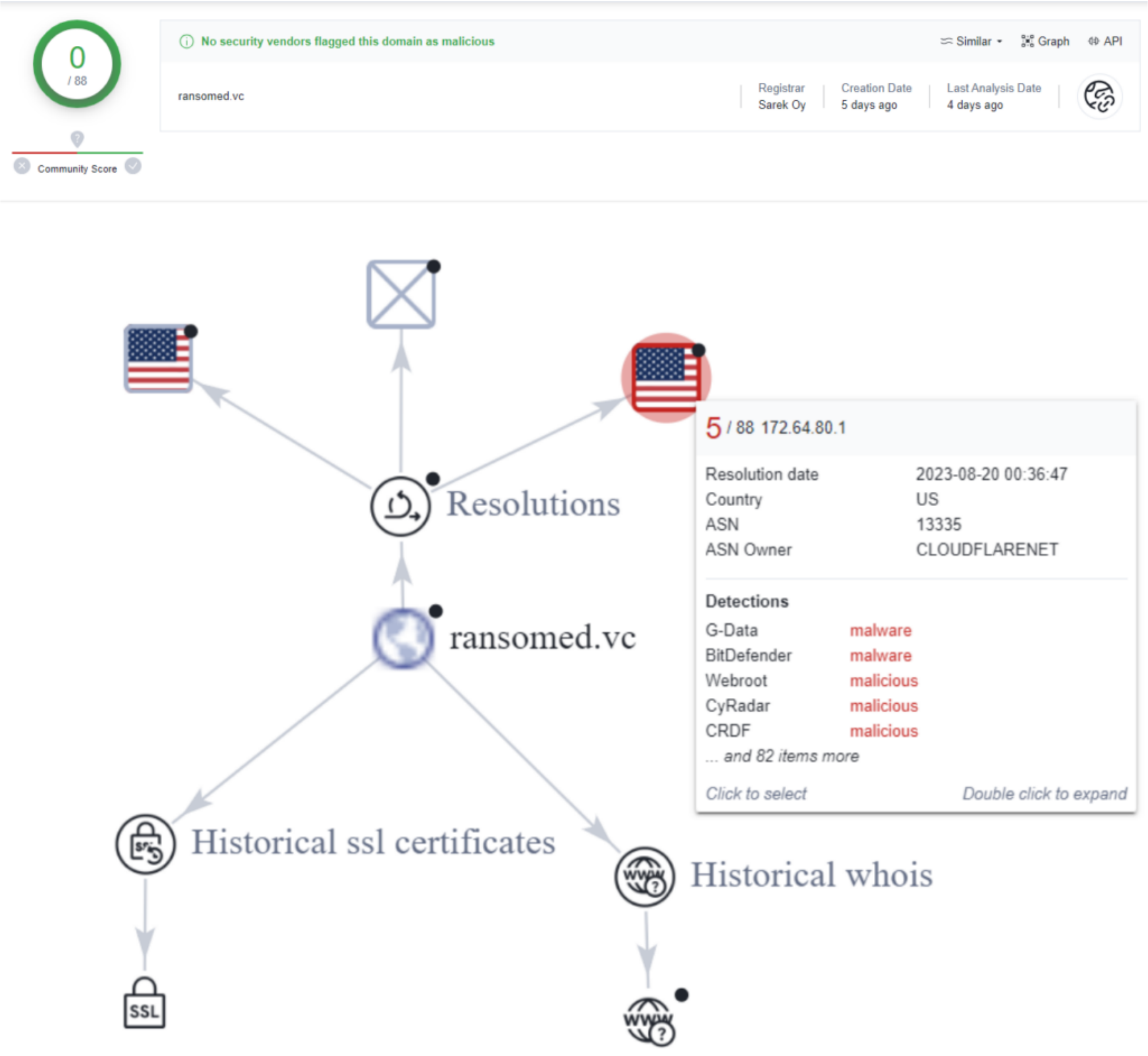


https://ransomed.vc:443/

Type	Found	Response	Size
Dir	/	200	1333
File	/a1.html	200	633
File	/index.html	200	635
File	/ig.html	200	633

Figure 7. Dirbuster output of Ransomed.vc domain

When we check the domain in VirusTotal, it appears clean, but in the relation graph, it is linked to an IP address tagged as malicious:



0 / 88

No security vendors flagged this domain as malicious

ransomed.vc

Registrar: Sarek Oy
Creation Date: 5 days ago
Last Analysis Date: 4 days ago

5 / 88 172.64.80.1

Resolution date	2023-08-20 00:36:47
Country	US
ASN	13335
ASN Owner	CLOUDFLARENET

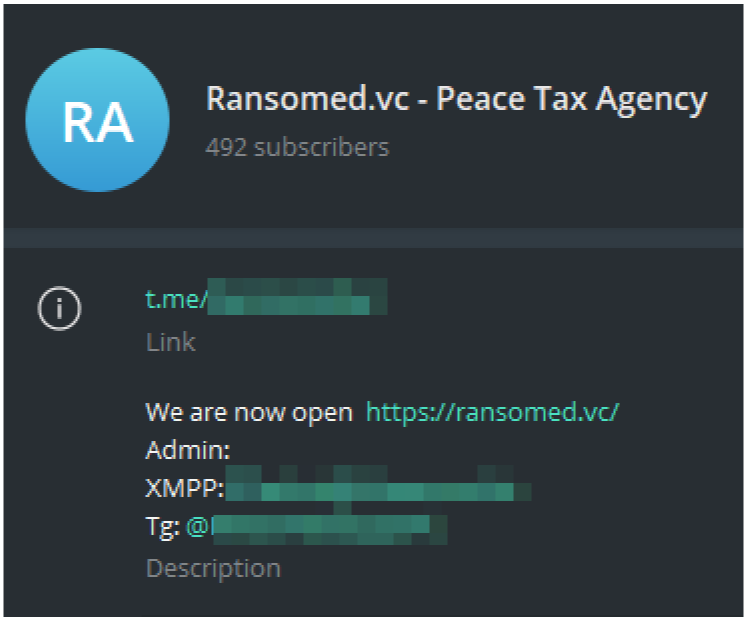
Detections

G-Data	malware
BitDefender	malware
Webroot	malicious
CyRadar	malicious
CRDF	malicious

... and 82 items more

Figure 8. VirusTotal output and Relation graph of Ransomed.vc domain (Source:VirusTotal)

In addition, the group shares victim posts on its Telegram channel, which they actively use:



Ransomed.vc - Peace Tax Agency

492 subscribers

t.me/[redacted]

Link

We are now open https://ransomed.vc/

Admin:

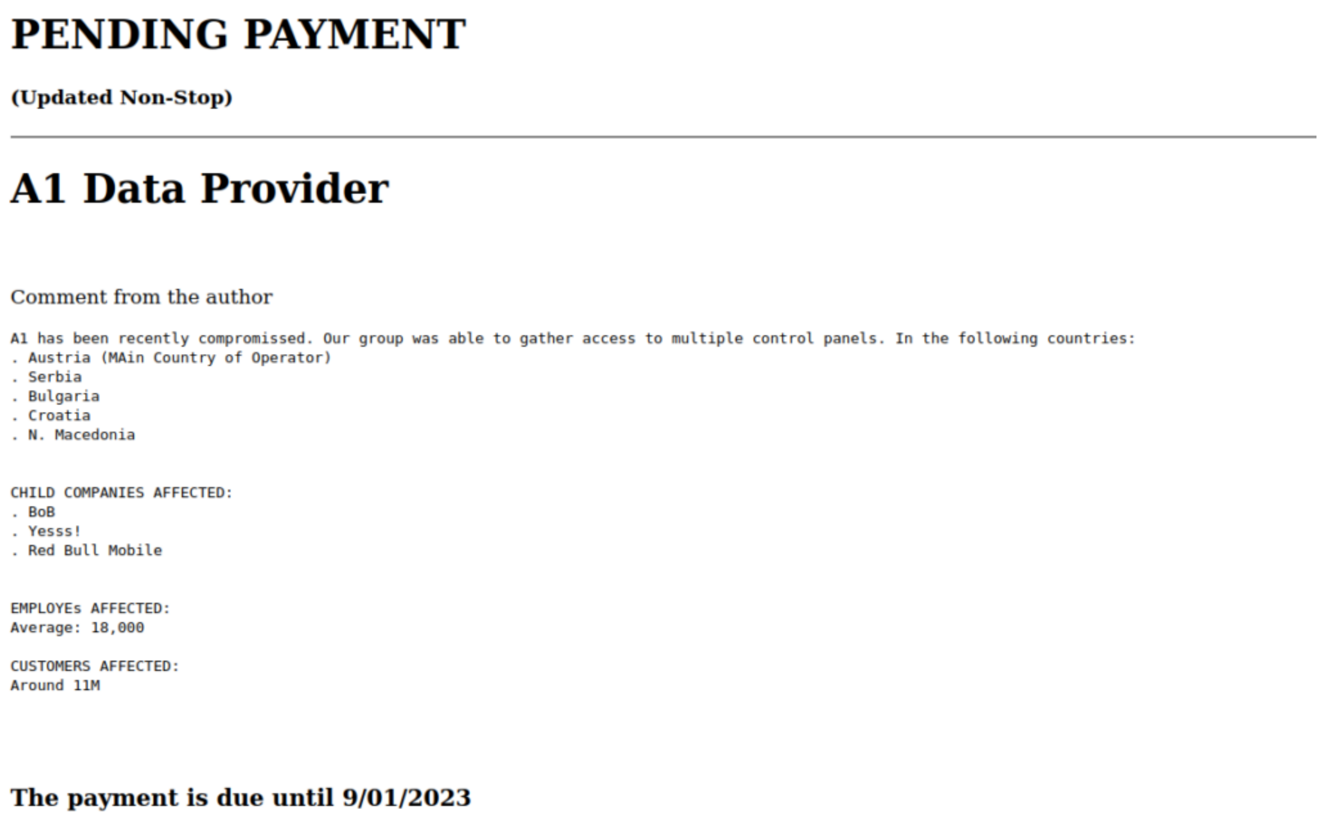
XMPP: [redacted]

Tg: @[redacted]

Description

Figure 9. Telegram channel information

First Victims of Ransomed.vc



PENDING PAYMENT

(Updated Non-Stop)

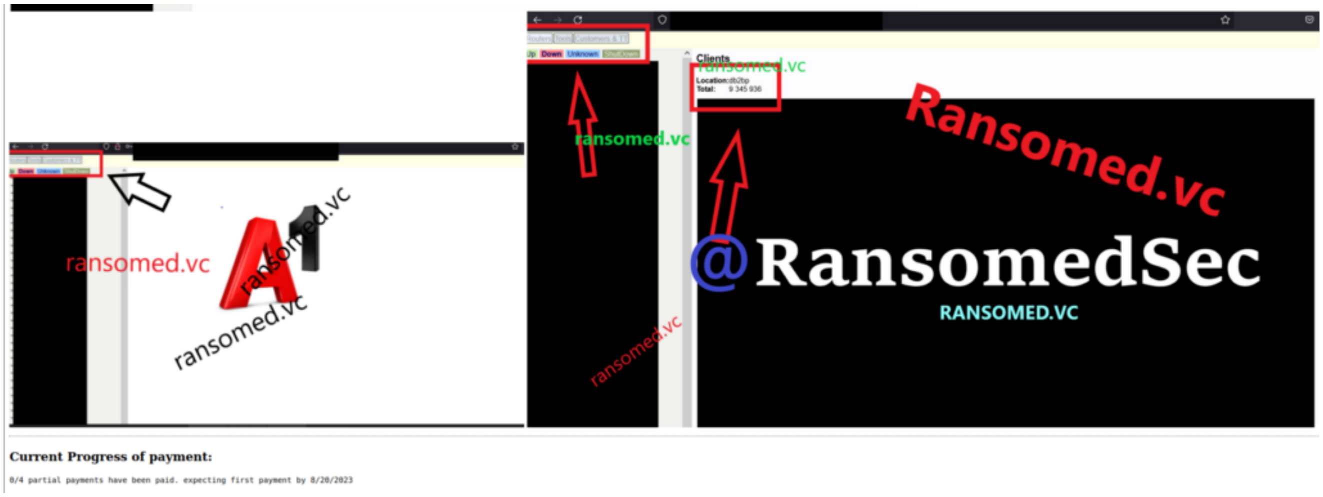
A1 Data Provider

Comment from the author

```
A1 has been recently compromissed. Our group was able to gather access to multiple control panels. In the following countries:
. Austria (MAin Country of Operator)
. Serbia
. Bulgaria
. Croatia
. N. Macedonia


CHILD COMPANIES AFFECTED:
. BoB
. Yesss!
. Red Bull Mobile


EMPLOYEs AFFECTED:
Average: 18,000

CUSTOMERS AFFECTED:
Around 11M
```

The payment is due until 9/01/2023

Figure 10. A1 Data Provider has been compromised by Ransomed.vc

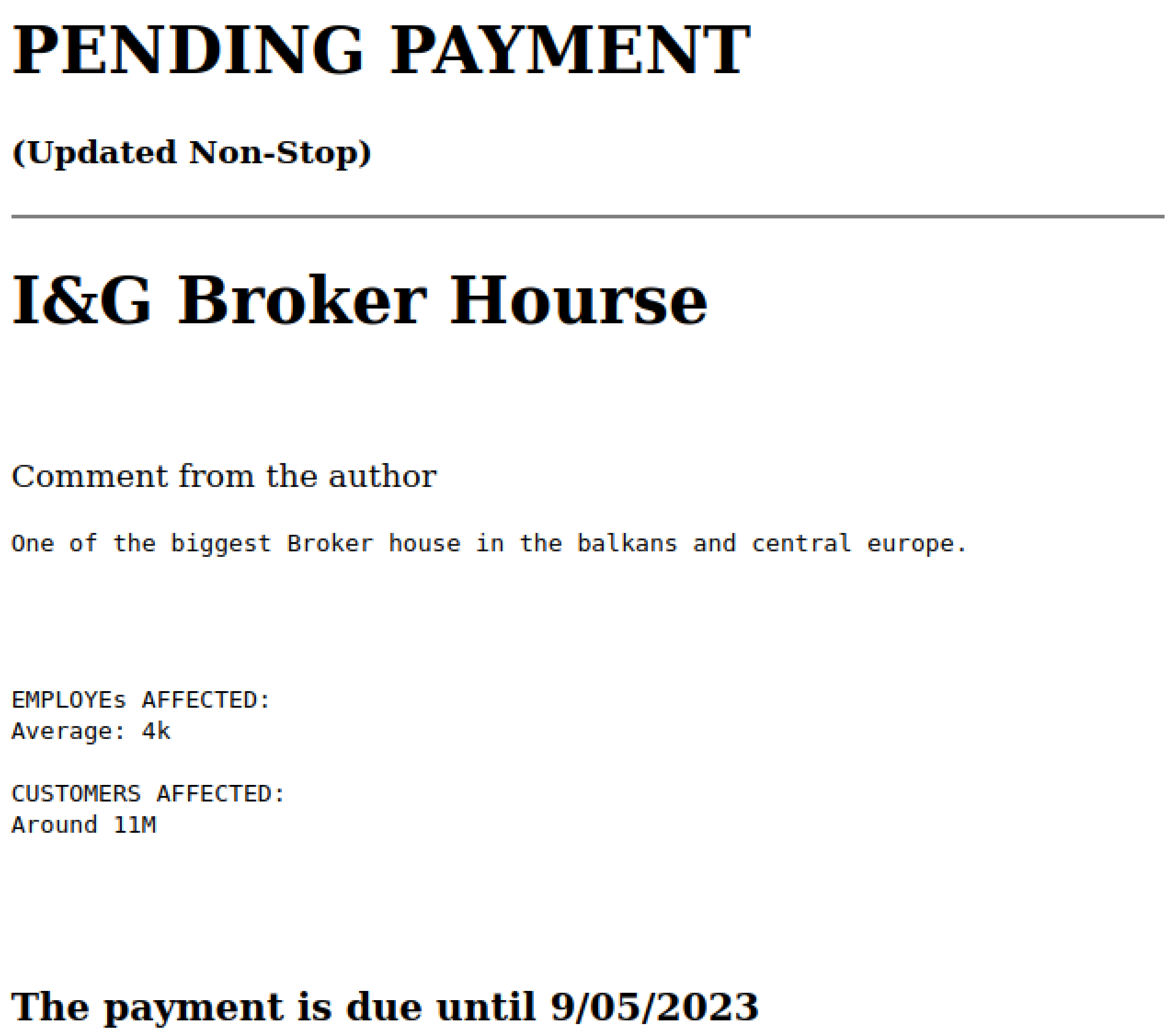


Current Progress of payment:

0/4 partial payments have been paid. expecting first payment by 8/20/2023

Figure 11. A1 Data Provider's screenshots of Ransomed.vc

I&G Broker House:



PENDING PAYMENT

(Updated Non-Stop)

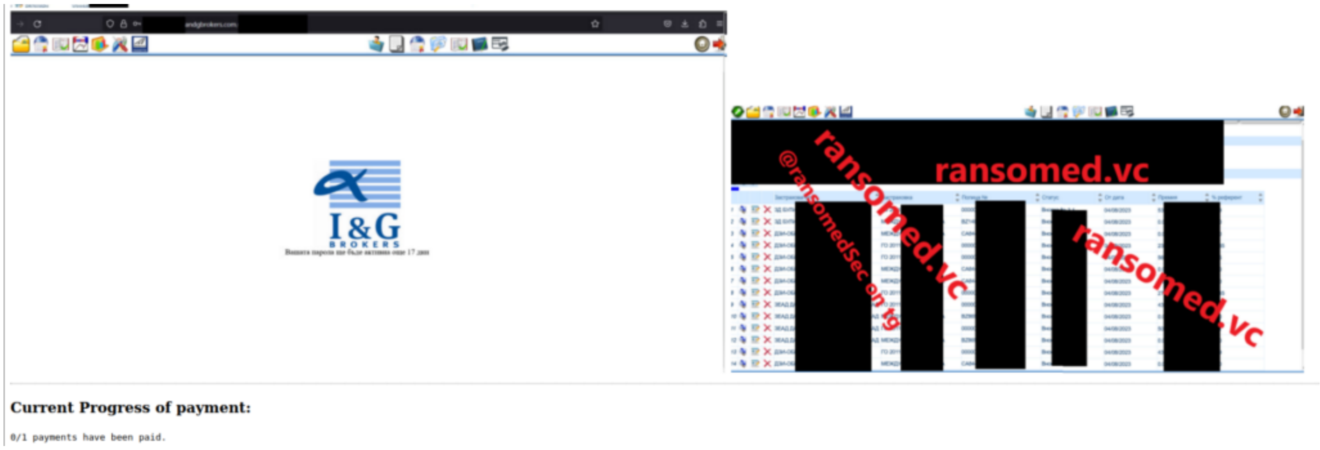
I&G Broker Hourse

Comment from the author

```
One of the biggest Broker house in the balkans and central europe.



EMPLOYEs AFFECTED:
Average: 4k

CUSTOMERS AFFECTED:
Around 11M
```

The payment is due until 9/05/2023

Figure 12. I&G Broker House



Вашата парола ще бъде активна още 17 дни

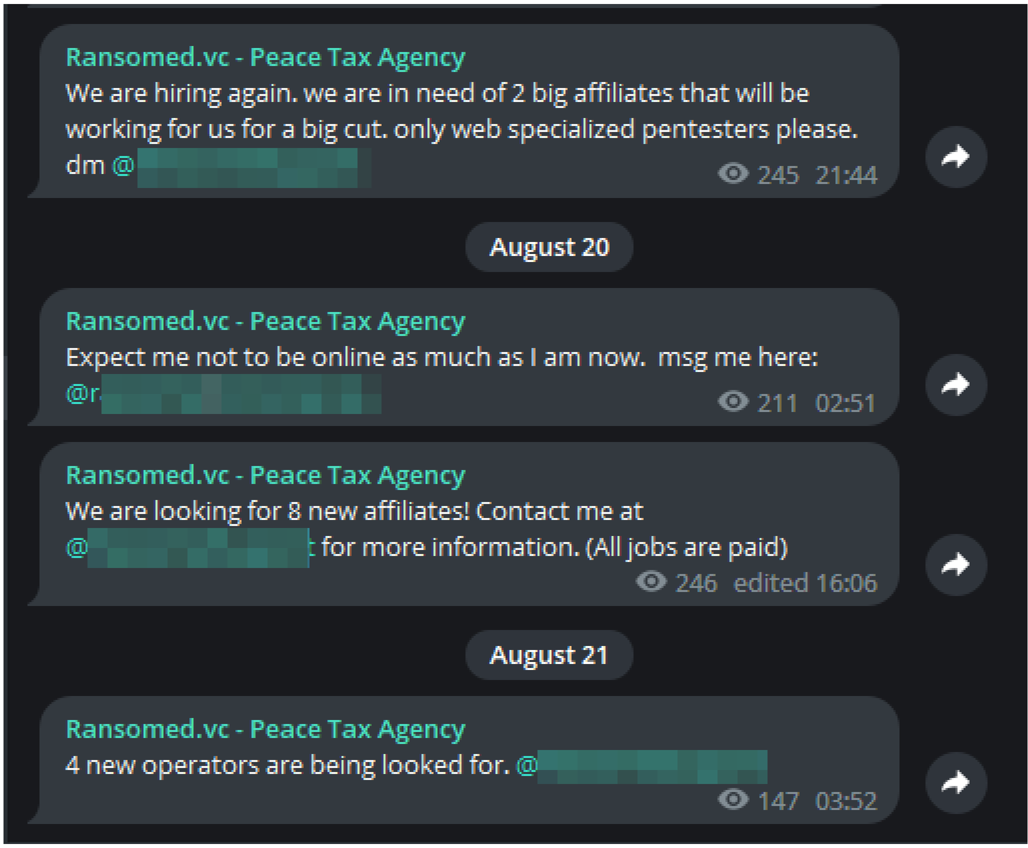
[redacted]

Current Progress of payment:

0/1 payments have been paid.

Figure 13. I&G Broker House's screenshots of Ransomed.vc

We also see that they are looking for new operators on their Telegram channels, which suggests that there may be **more victim announcements** in the near future.



Ransomed.vc - Peace Tax Agency
We are hiring again. we are in need of 2 big affiliates that will be working for us for a big cut. only web specialized pentesters please. dm @[redacted]
245 21:44

August 20

Ransomed.vc - Peace Tax Agency
Expect me not to be online as much as I am now. msg me here: @r[redacted]
211 02:51

Ransomed.vc - Peace Tax Agency
We are looking for 8 new affiliates! Contact me at @[redacted] for more information. (All jobs are paid)
246 edited 16:06

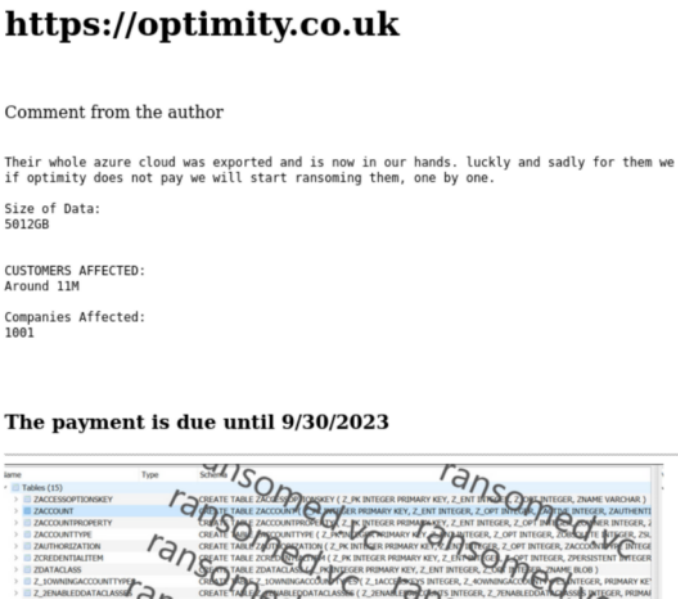
August 21

Ransomed.vc - Peace Tax Agency
4 new operators are being looked for. @[redacted]
147 03:52

Figure 14. Ransomed.vc Telegram posts about they are looking for new operators

Ransomed.vc Lists Three New Victims and Receives Payment for a Previous Attack

Based on the latest information, the Ransomed.vc group has targeted three new victims. One of these victims is **Optimity**, a provider of managed IT services. The threat actors assert that they have exported Optimity's entire **Azure Cloud**, which granted them access to over a thousand companies.



https://optimity.co.uk

Comment from the author

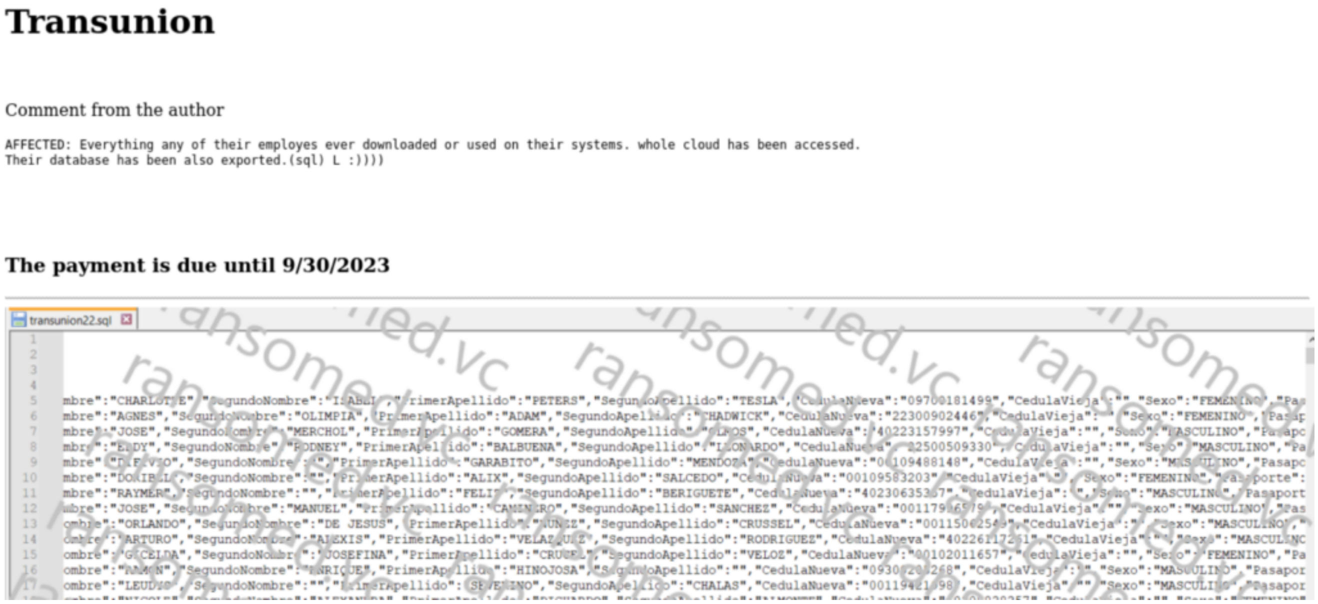
```
Their whole azure cloud was exported and is now in our hands. luckly and sadly for them we have taken access to more than 1000 companies.
if optimity does not pay we will start ransoming them, one by one.

Size of Data:
5012GB


CUSTOMERS AFFECTED:
Around 11M

Companies Affected:
1001
```

The payment is due until 9/30/2023

lame	Type	Schema
Tables (15)		
ZACCESSOPTIONSKEY		CREATE TABLE ZACCESSOPTIONSKEY (Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZNAME VARCHAR)
ZACCOUNT		CREATE TABLE ZACCOUNT (Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZACTIVE INTEGER, ZAUTHENTI
ZACCOUNTPROPERTY		CREATE TABLE ZACCOUNTPROPERTY (Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZOWNER INTEGER, Z
ZACCOUNTTYPE		CREATE TABLE ZACCOUNTTYPE (Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZOBSOLETE INTEGER, ZSL
ZAUTHORIZATION		CREATE TABLE ZAUTHORIZATION (Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZACCOUNTTYPE INTEGE
ZCREDENTIALITEM		CREATE TABLE ZCREDENTIALITEM (Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZPERSISTENT INTEGER
ZDATACLASS		CREATE TABLE ZDATACLASS (Z_PK INTEGER PRIMARY KEY, Z_ENT INTEGER, Z_OPT INTEGER, ZNAME BLOB)
Z_1OWNINGACCOUNTTYPES		CREATE TABLE Z_1OWNINGACCOUNTTYPES (Z_1ACCESSKEYS INTEGER, Z_4OWNINGACCOUNTTYPES INTEGER, PRIMARY KE
Z_2ENABLEDDATACLASSES		CREATE TABLE Z_2ENABLEDDATACLASSES (Z_2ENABLEDACCOUNTS INTEGER, Z_7ENABLEDDATACLASSES INTEGER, PRIMAR

Figure 15. Optimity

Another exported database belongs to **Transunion**. The ransom threat actors claimed that they successfully infiltrated the entire cloud, gaining possession of all materials used and downloaded by Transunion employees. One such dataset has also been obtained for a company named **Jhooker.**



Transunion

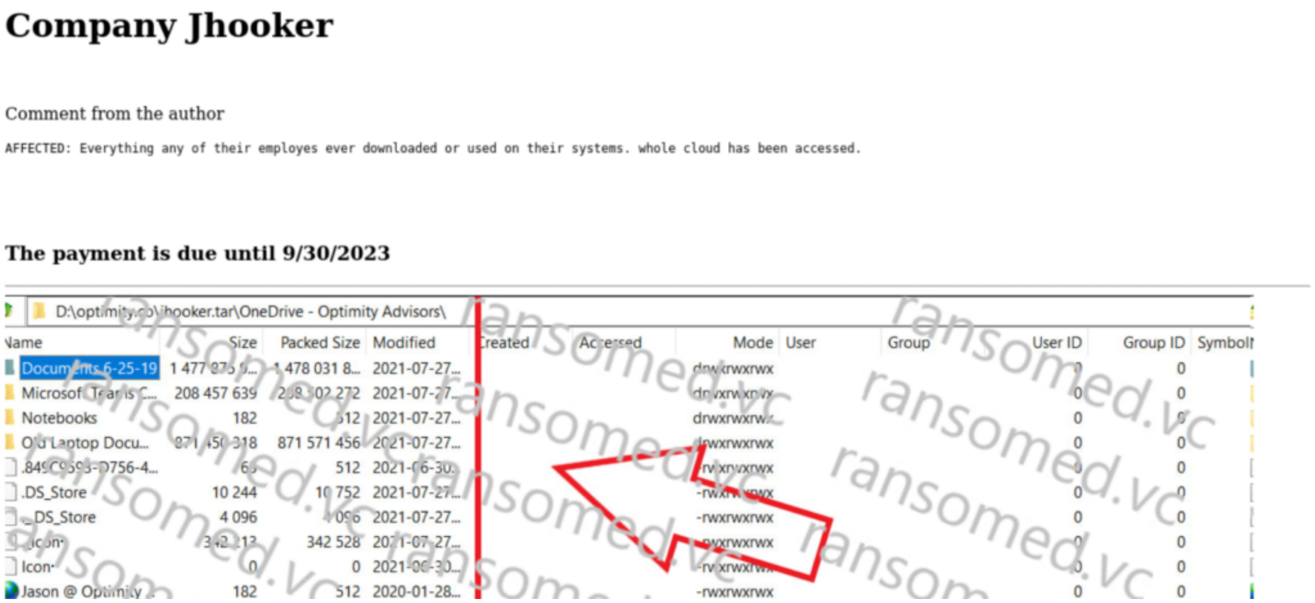
Comment from the author

```
AFFECTED: Everything any of their employes ever downloaded or used on their systems. whole cloud has been accessed.
Their database has been also exported.(sql) L :))))
```

The payment is due until 9/30/2023

```
mbre":"CHARLOTTE","SegundoNombre":"ISABEL","PrimerApellido":"PETERS","SegundoApellido":"TESLA","CedulaNueva":"09700181499","CedulaVieja":"","Sexo":"FEMENINO","Pas
mbre":"AGNES","SegundoNombre":"OLIMPIA","PrimerApellido":"ADAM","SegundoApellido":"CHADWICK","CedulaNueva":"22300902446","CedulaVieja":"","Sexo":"FEMENINO","Pasap
mbre":"JOSE","SegundoNombre":"MERCHOL","PrimerApellido":"GOMERA","SegundoApellido":"OLMOS","CedulaNueva":"40223157997","CedulaVieja":"","Sexo":"MASCULINO","Pasapo
mbre":"EDDY","SegundoNombre":"RODNEY","PrimerApellido":"BALBUENA","SegundoApellido":"LEONARDO","CedulaNueva":"22500509330","CedulaVieja":"","Sexo":"MASCULINO","Pa
mbre":"DIEVIO","SegundoNombre":"","PrimerApellido":"GARABITO","SegundoApellido":"MENDOZA","CedulaNueva":"00109488148","CedulaVieja":"","Sexo":"MASCULINO","Pasapo
mbre":"DORIBEL","SegundoNombre":"","PrimerApellido":"ALIX","SegundoApellido":"SALCEDO","CedulaNueva":"00109583203","CedulaVieja":"","Sexo":"FEMENINO","Pasaporte":
mbre":"RAYMER","SegundoNombre":"","PrimerApellido":"FELIZ","SegundoApellido":"BERIGUETE","CedulaNueva":"40230635367","CedulaVieja":"","Sexo":"MASCULINO","Pasaport
mbre":"JOSE","SegundoNombre":"MANUEL","PrimerApellido":"CAMINERO","SegundoApellido":"SANCHEZ","CedulaNueva":"00117976579","CedulaVieja":"","Sexo":"MASCULINO","Pas
ombre":"ORLANDO","SegundoNombre":"DE JESUS","PrimerApellido":"NUNEZ","SegundoApellido":"CRUSSEL","CedulaNueva":"00115002549","CedulaVieja":"","Sexo":"MASCULINO","
ombre":"ARTURO","SegundoNombre":"ALEXIS","PrimerApellido":"VELAZQUEZ","SegundoApellido":"RODRIGUEZ","CedulaNueva":"40226117261","CedulaVieja":"","Sexo":"MASCULINO
ombre":"GICELDA","SegundoNombre":"JOSEFINA","PrimerApellido":"CRUCEL","SegundoApellido":"VELOZ","CedulaNueva":"00102011657","CedulaVieja":"","Sexo":"FEMENINO","Pa
ombre":"RAMON","SegundoNombre":"ENRIQUE","PrimerApellido":"HINOJOSA","SegundoApellido":"","CedulaNueva":"09300200268","CedulaVieja":"","Sexo":"MASCULINO","Pasapor
ombre":"LEUDYS","SegundoNombre":"","PrimerApellido":"SEVERINO","SegundoApellido":"CHALAS","CedulaNueva":"00119421098","CedulaVieja":"","Sexo":"MASCULINO","Pasapor
```

Figure 16. Transunion



Company Jhooker

Comment from the author

AFFECTED: Everything any of their employes ever downloaded or used on their systems. whole cloud has been accessed.

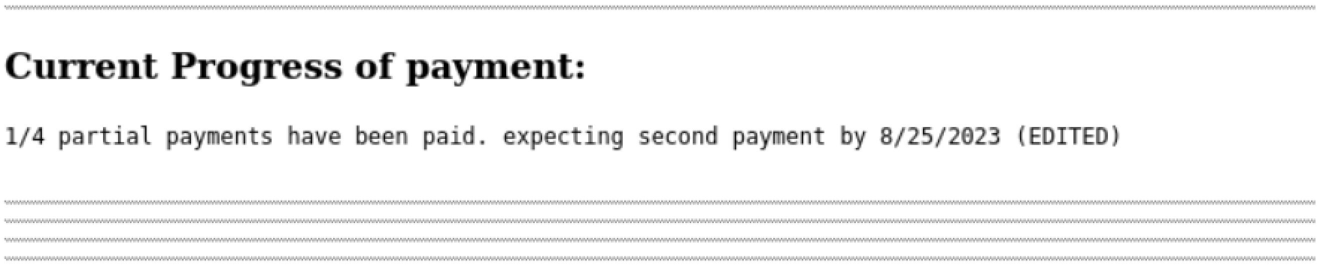
The payment is due until 9/30/2023

D:\optimity.co\jhooker.tar\OneDrive - Optimity Advisors\

Name	Size	Packed Size	Modified	Created	Accessed	Mode	User	Group	User ID	Group ID	Symbol
Documents 6-25-19	1 477 875 9...	1 478 031 8...	2021-07-27...			drwxrwxrwx			0	0	
Microsoft Teams C...	208 457 639	208 502 272	2021-07-27...			drwxrwxrwx			0	0	
Notebooks	182	512	2021-07-27...			drwxrwxrwx			0	0	
Old Laptop Docu...	871 450 318	871 571 456	2021-07-27...			drwxrwxrwx			0	0	
.849C9593-D756-4...	65	512	2021-06-30...			-rwxrwxrwx			0	0	
.DS_Store	10 244	10 752	2021-07-27...			-rwxrwxrwx			0	0	
._DS_Store	4 096	4 096	2021-07-27...			-rwxrwxrwx			0	0	
._Icon	342 213	342 528	2021-07-27...			-rwxrwxrwx			0	0	
Icon	0	0	2021-06-30...			-rwxrwxrwx			0	0	
Jason @ Optimity ...	182	512	2020-01-28...			-rwxrwxrwx			0	0	

Figure 17. Jhooker

Furthermore, the ransomware operation has apparently received a payment following their attack on A1 Data Provider. However, only one out of four payments has been fulfilled. It appears that the ransom group accepts **payments in installments**, a departure from the norm among ransomware groups we have encountered so far.



Current Progress of payment:

1/4 partial payments have been paid. expecting second payment by 8/25/2023 (EDITED)

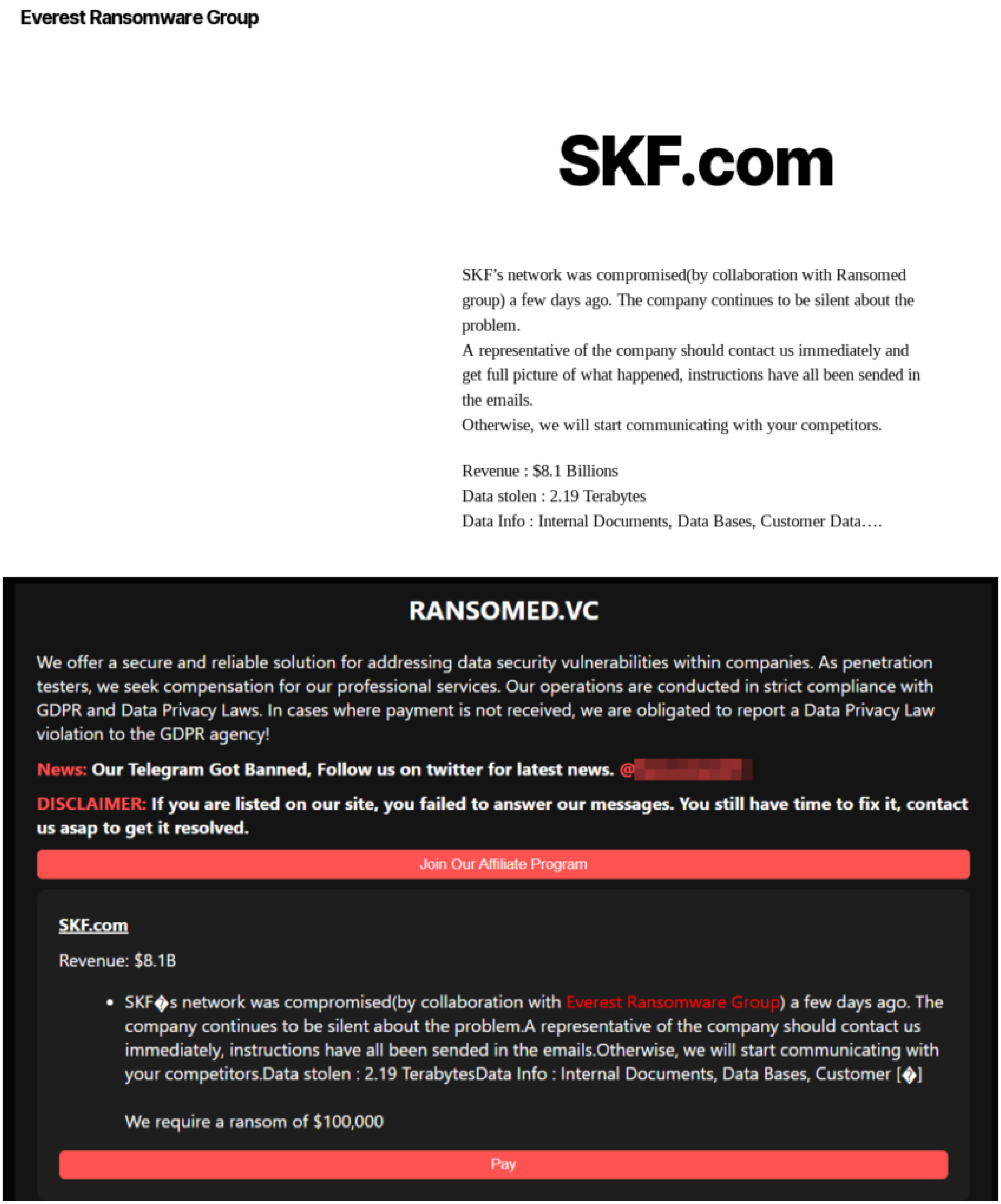
Figure 18. ¼ partial payments have been paid by A1 Data Provider.

An Extortion Approach That Utilizes GDPR Fines

An additional revelation about the group has been shared in a tweet by vx-underground. The Ransomed.vc group seems to use an extortion strategy that leverages **GDPR** (Europe's General Data Protection Laws). Essentially, the group coerces victims into either paying the ransom or facing GDPR fines upon the exposure of their data. This GDPR-based extortion scheme diverges from the typical extortion approaches, as these threat actors **exploit protective laws** to intimidate victims for financial gain.

Old Ties, New Threats: Everest Echoes

In a recent post by the Ransomed team, we noticed that they are collaborating with Everest Ransomware, as evident in the details of **SKF.com**'s victim announcement. Upon reviewing Everest's claim post, we observed Everest also made the same post. Everest is a threat actor that has been active since 2020. Everest has been involved in ransomware attacks, initial access brokering, and data extortion activities. Additionally, they have been active on platforms such as XSS Forum and Breached.



Everest Ransomware Group

SKF.com

SKF’s network was compromised(by collaboration with Ransomed group) a few days ago. The company continues to be silent about the problem.
A representative of the company should contact us immediately and get full picture of what happened, instructions have all been sended in the emails.
Otherwise, we will start communicating with your competitors.

Revenue : $8.1 Billions
Data stolen : 2.19 Terabytes
Data Info : Internal Documents, Data Bases, Customer Data….

RANSOMED.VC

We offer a secure and reliable solution for addressing data security vulnerabilities within companies. As penetration testers, we seek compensation for our professional services. Our operations are conducted in strict compliance with GDPR and Data Privacy Laws. In cases where payment is not received, we are obligated to report a Data Privacy Law violation to the GDPR agency!

News: **Our Telegram Got Banned, Follow us on twitter for latest news.** @[redacted]

DISCLAIMER: **If you are listed on our site, you failed to answer our messages. You still have time to fix it, contact us asap to get it resolved.**

SKF.com

Revenue: $8.1B

- SKF�s network was compromised(by collaboration with Everest Ransomware Group) a few days ago. The company continues to be silent about the problem.A representative of the company should contact us immediately, instructions have all been sended in the emails.Otherwise, we will start communicating with your competitors.Data stolen : 2.19 TerabytesData Info : Internal Documents, Data Bases, Customer [�]

  We require a ransom of $100,000

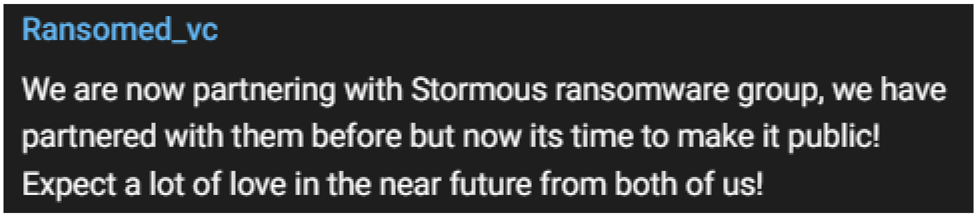
Fig. 19. Everest and Ransomed’s claim posts about SKF.com

Considering that Ransomed was one of the founders of BlackForums after Breached and Everest was active in Breached, we can infer that their fellowship is not for a single operation but a history.

RansomedVC Partners with STORMOUS Hackers

RansomedVC recently announced on Telegram that they have forged an alliance with Stormous ransomware.

The threat group's most recent message on its channel stated that while they had partnered in the past, they are now officially confirming it:

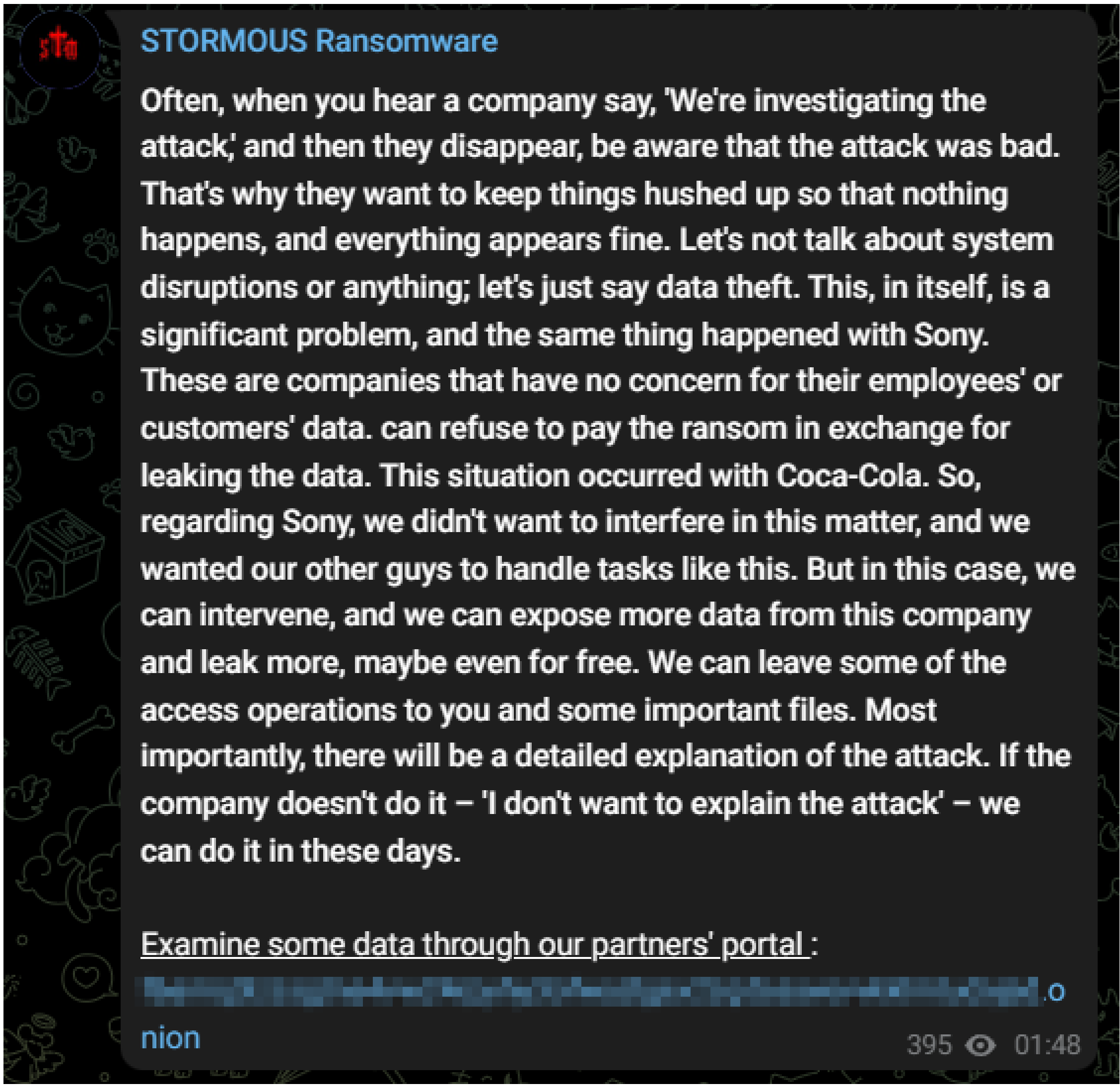


Ransomed_vc

We are now partnering with Stormous ransomware group, we have partnered with them before but now its time to make it public! Expect a lot of love in the near future from both of us!

Fig. 20. RansomedVC's announcement about partnering with Stormous.

The fact that Stormous referred to the RansomedVC group as a partner in its own Telegram channel with one of their recent posts fully confirms their partnership.



STORMOUS Ransomware

Often, when you hear a company say, 'We're investigating the attack,' and then they disappear, be aware that the attack was bad. That's why they want to keep things hushed up so that nothing happens, and everything appears fine. Let's not talk about system disruptions or anything; let's just say data theft. This, in itself, is a significant problem, and the same thing happened with Sony. These are companies that have no concern for their employees' or customers' data. can refuse to pay the ransom in exchange for leaking the data. This situation occurred with Coca-Cola. So, regarding Sony, we didn't want to interfere in this matter, and we wanted our other guys to handle tasks like this. But in this case, we can intervene, and we can expose more data from this company and leak more, maybe even for free. We can leave some of the access operations to you and some important files. Most importantly, there will be a detailed explanation of the attack. If the company doesn't do it – 'I don't want to explain the attack' – we can do it in these days.

Examine some data through our partners' portal :
[redacted].onion

395 01:48

Fig. 21.

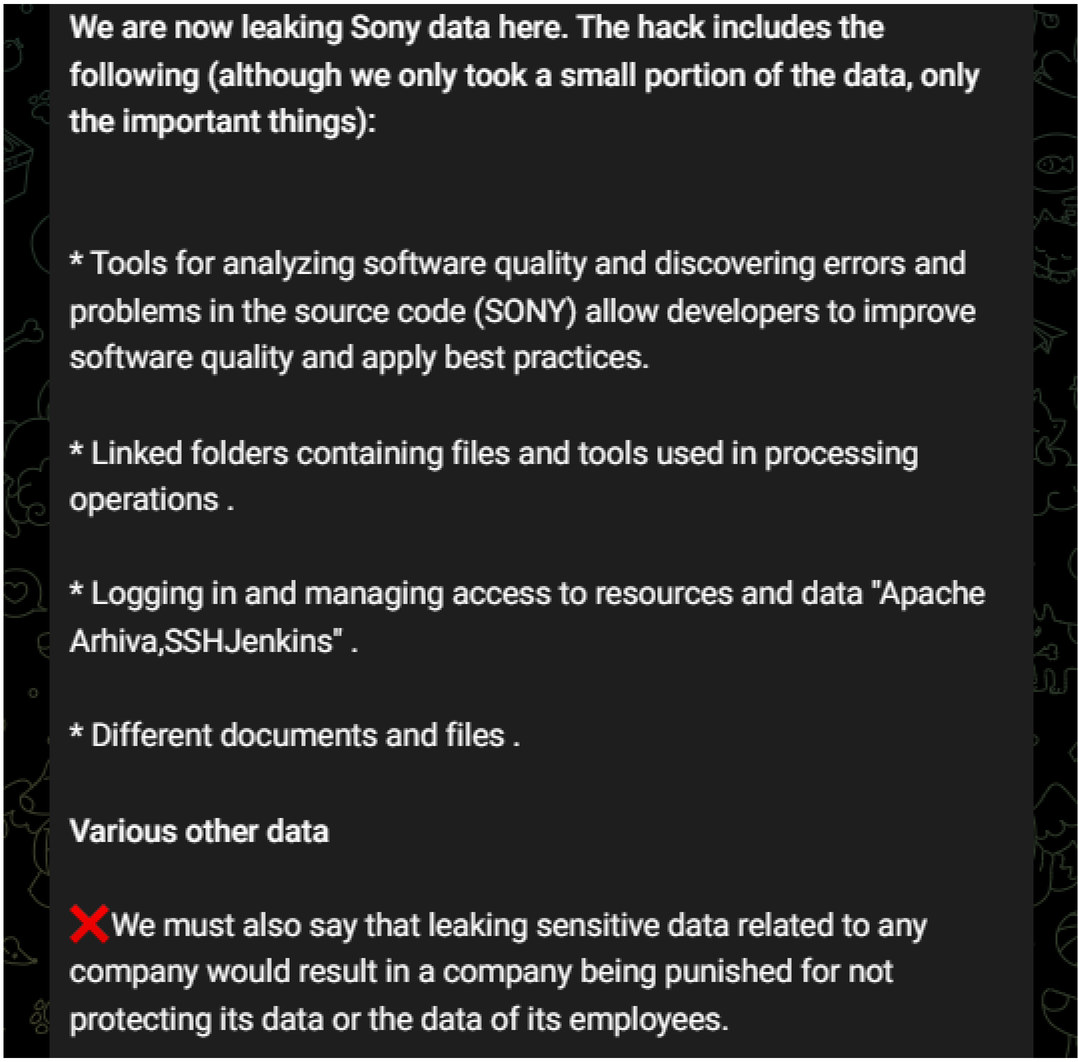
Stormous' message on Telegram.

In the message, the ransomware group also commented on the Sony breach, suggesting that they might intervene and **potentially release more data** for free.

The two ransomware groups appear to be trying to exert pressure on Sony, possibly with the aim of **further extorting** their victim or **damaging their brand reputation**. With the official partnership now established, we may expect to receive more updates regarding the Sony situation.

The Outcome of the Sony Leak

In a subsequent update, the RansomedVC threat actors have leaked the data they claimed to possess from the Sony breach on their Telegram channel. They mentioned that they extracted **only the important data** from Sony. See the message below:



We are now leaking Sony data here. The hack includes the following (although we only took a small portion of the data, only the important things):

* Tools for analyzing software quality and discovering errors and problems in the source code (SONY) allow developers to improve software quality and apply best practices.

* Linked folders containing files and tools used in processing operations .

* Logging in and managing access to resources and data "Apache Arhiva,SSHJenkins" .

* Different documents and files .

Various other data

❌We must also say that leaking sensitive data related to any company would result in a company being punished for not protecting its data or the data of its employees.

Fig. 22.

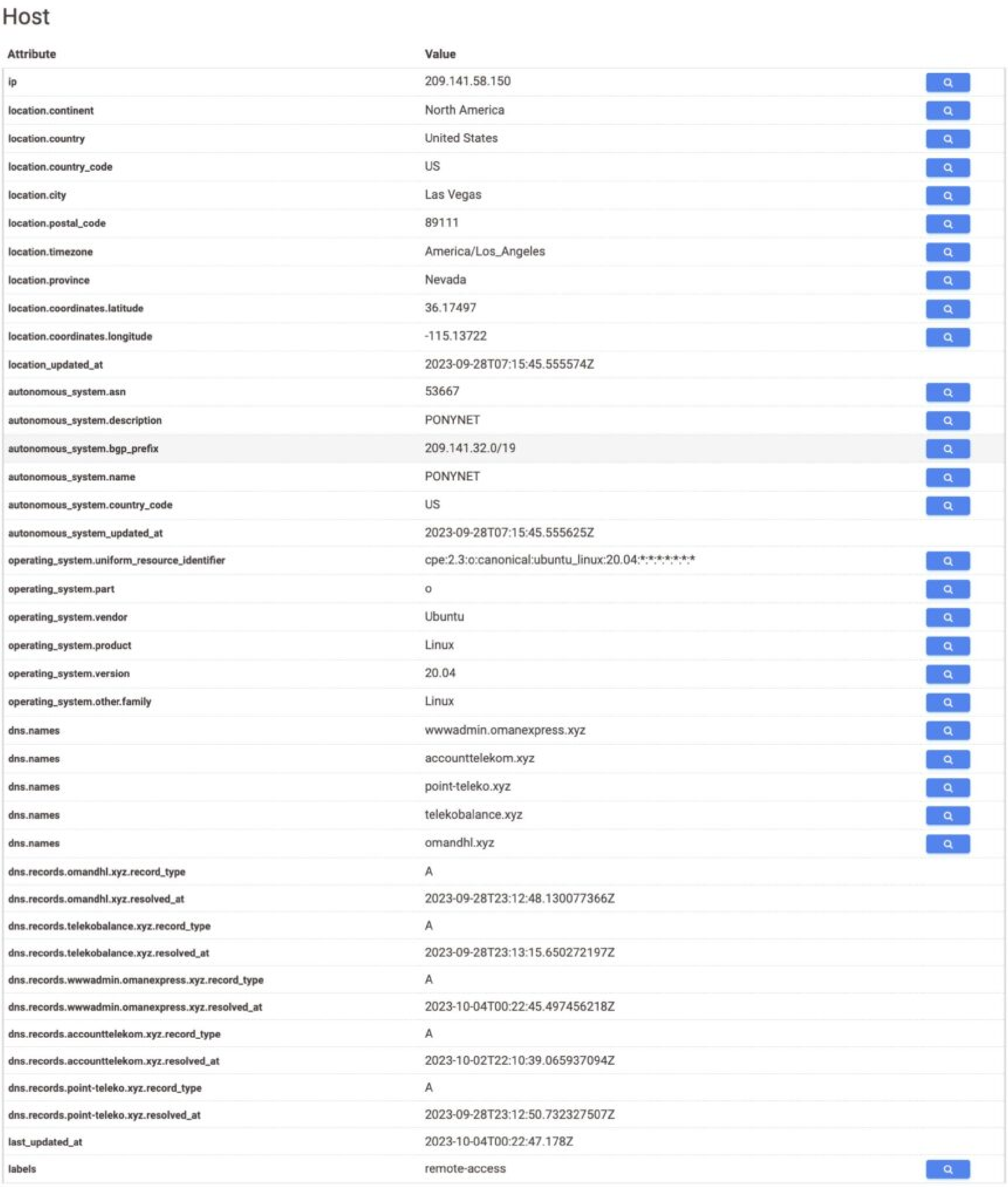
RansomedVC leaks the data from the Sony breach.

To learn more about the Sony breach, visit our other blog post: What You Need to Know About the Alleged Sony Breach

RansomedVC De-anonymized Itself After Moving to WordPress

RansomedVC has recently transitioned its website to WordPress, following the setup of a new virtual private server (VPS), hosted by a bulletproof hosting provider known as PONYNET.

Unfortunately for the RansomedVC threat actors, this migration has inadvertently exposed their **origin IP address** and a variety of associated **DNS entries**.

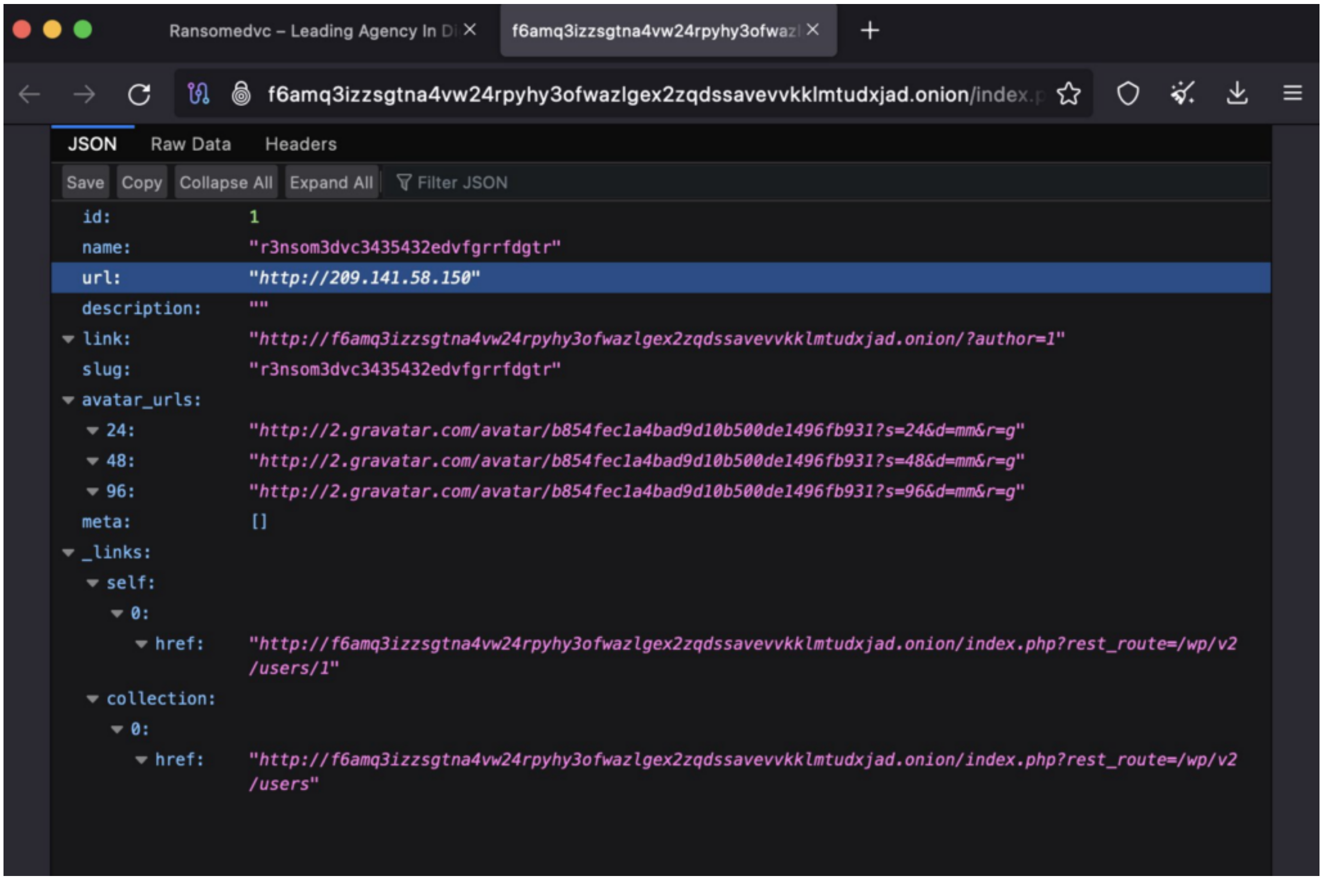


Host

Attribute	Value	
ip	209.141.58.150	🔍
location.continent	North America	🔍
location.country	United States	🔍
location.country_code	US	🔍
location.city	Las Vegas	🔍
location.postal_code	89111	🔍
location.timezone	America/Los_Angeles	🔍
location.province	Nevada	🔍
location.coordinates.latitude	36.17497	🔍
location.coordinates.longitude	-115.13722	🔍
location_updated_at	2023-09-28T07:15:45.555574Z	
autonomous_system.asn	53667	🔍
autonomous_system.description	PONYNET	🔍
autonomous_system.bgp_prefix	209.141.32.0/19	🔍
autonomous_system.name	PONYNET	🔍
autonomous_system.country_code	US	🔍
autonomous_system_updated_at	2023-09-28T07:15:45.555625Z	
operating_system.uniform_resource_identifier	cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:*:*:*:*:*	🔍
operating_system.part	o	🔍
operating_system.vendor	Ubuntu	🔍
operating_system.product	Linux	🔍
operating_system.version	20.04	🔍
operating_system.other.family	Linux	🔍
dns.names	wwwadmin.omanexpress.xyz	🔍
dns.names	accounttelekom.xyz	🔍
dns.names	point-teleko.xyz	🔍
dns.names	telekobalance.xyz	🔍
dns.names	omandhl.xyz	🔍
dns.records.omandhl.xyz.record_type	A	
dns.records.omandhl.xyz.resolved_at	2023-09-28T23:12:48.130077366Z	
dns.records.telekobalance.xyz.record_type	A	
dns.records.telekobalance.xyz.resolved_at	2023-09-28T23:13:15.650272197Z	
dns.records.wwwadmin.omanexpress.xyz.record_type	A	
dns.records.wwwadmin.omanexpress.xyz.resolved_at	2023-10-04T00:22:45.497456218Z	
dns.records.accounttelekom.xyz.record_type	A	
dns.records.accounttelekom.xyz.resolved_at	2023-10-02T22:10:39.065937094Z	
dns.records.point-teleko.xyz.record_type	A	
dns.records.point-teleko.xyz.resolved_at	2023-09-28T23:12:50.732327507Z	
last_updated_at	2023-10-04T00:22:47.178Z	
labels	remote-access	🔍

Exposed host information. (Source: X)

Additionally, their actions have led to oversights, as the site seems to be affected by vulnerability known as CVE-2017-5487 (Unauthorized Information Disclosure vulnerability in WordPress 4.7 before 4.7.1). The vulnerability further reveals RansomedVC's origin IP. The sensitive information is available within the profile of the administrator user:


Ransomedvc – Leading Agency In D
f6amq3izzsgtna4vw24rpyhy3ofwaz
f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion/index.p
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
id:                 1
name:               "r3nsom3dvc3435432edvfgrrfdgtr"
url:                "http://209.141.58.150"
description:        ""
▾ link:             "http://f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion/?author=1"
slug:               "r3nsom3dvc3435432edvfgrrfdgtr"
▾ avatar_urls:
  ▾ 24:             "http://2.gravatar.com/avatar/b854fec1a4bad9d10b500de1496fb931?s=24&d=mm&r=g"
  ▾ 48:             "http://2.gravatar.com/avatar/b854fec1a4bad9d10b500de1496fb931?s=48&d=mm&r=g"
  ▾ 96:             "http://2.gravatar.com/avatar/b854fec1a4bad9d10b500de1496fb931?s=96&d=mm&r=g"
meta:               []
▾ _links:
  ▾ self:
    ▾ 0:
      ▾ href:       "http://f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion/index.php?rest_route=/wp/v2
                    /users/1"
  ▾ collection:
    ▾ 0:
      ▾ href:       "http://f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion/index.php?rest_route=/wp/v2
                    /users"
```

Ransomed.vc's origin IP has been revealed. (Source: X)

The intention behind this disclosure by @htmalgae is to highlight how the threat actors hastily **de-anonymized** their hidden service before its full restoration was completed.

Ransomed.vc Interview

Daily Dark Web published an interview with Ransomed.vc on September 14th. The interview shows how a ransomware operator thinks and sheds light on many claims and points about Ransomed[.]vc. Some highlights from the interview are as follows:

Can you introduce your group and explain why you engage in ransomware attacks?

– Of course I can, we are a big team I have to say of 77 affiliates and a few more groups in partnership. We are financially motivated so this answers the second part of the question

> *More on the topic of their working scheme:*

What are the primary motivations behind your attacks? Is it for financial gain, ideological reasons, or something else?

– Financial gain and sometimes political reason.

How do you choose your targets? Are you targeting large corporations, small businesses, or individual users?

– I require at least 5M in revenue so it is even worth to work on.

Their answers to some of the claims we included in this article were as follows:

In a recent post by the Ransomed team, they are collaborating with Everest Ransomware. Could you specify the nature of your connection with the Everest Group?

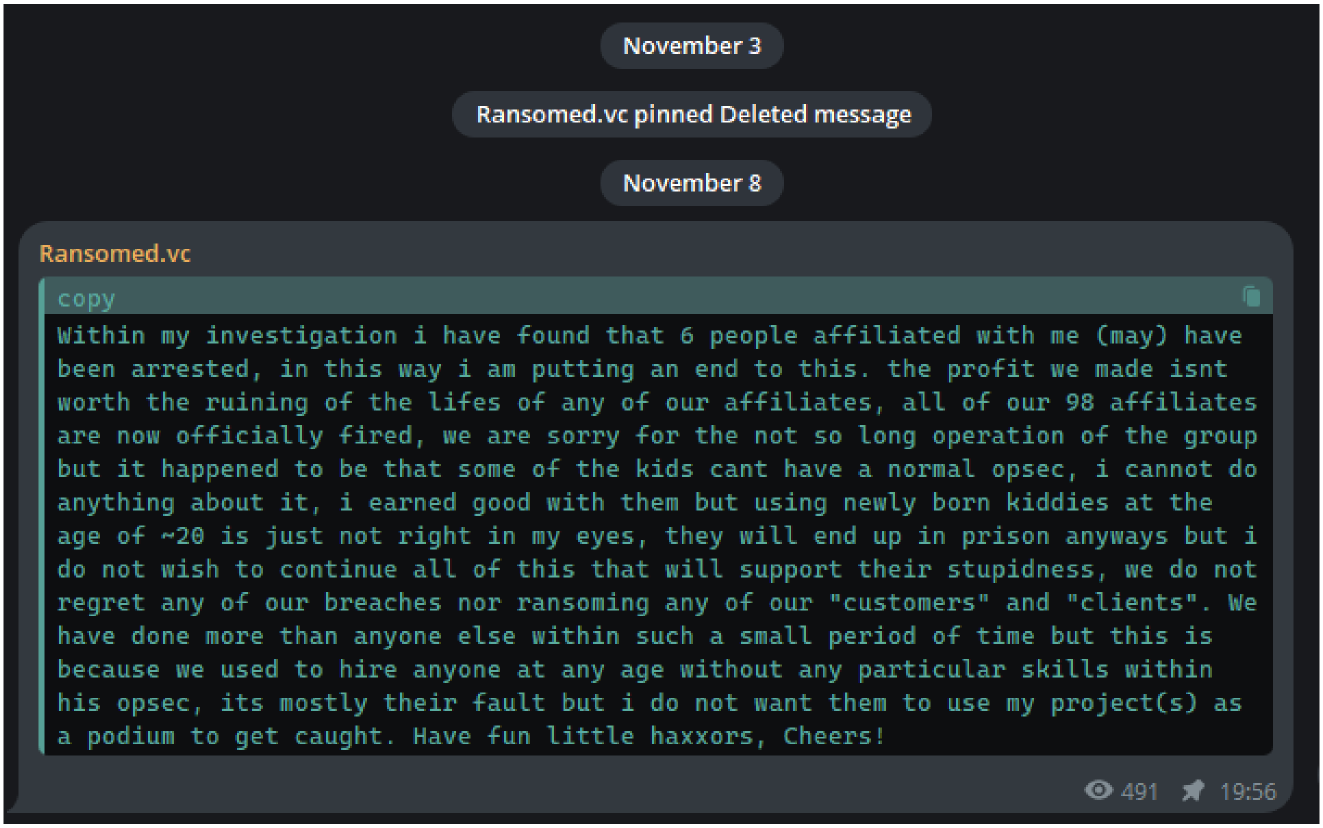
– Old friends dont forget their friends.

Alleged ties between Exposed Forum and Ransomed: Could you specify the nature of your connection with the Exposed Forum?

– I have seen the news yeah, idk what I can say about it, never been in their forum neither will I ever be.

Don't forget to check out Daily Dark Web's post for the full interview.

End of an Era, the Sinking of Ransomed.VC



November 3

Ransomed.vc pinned Deleted message

November 8

Ransomed.vc

```
Within my investigation i have found that 6 people affiliated with me (may) have
been arrested, in this way i am putting an end to this. the profit we made isnt
worth the ruining of the lifes of any of our affiliates, all of our 98 affiliates
are now officially fired, we are sorry for the not so long operation of the group
but it happened to be that some of the kids cant have a normal opsec, i cannot do
anything about it, i earned good with them but using newly born kiddies at the
age of ~20 is just not right in my eyes, they will end up in prison anyways but i
do not wish to continue all of this that will support their stupidness, we do not
regret any of our breaches nor ransoming any of our "customers" and "clients". We
have done more than anyone else within such a small period of time but this is
because we used to hire anyone at any age without any particular skills within
his opsec, its mostly their fault but i do not want them to use my project(s) as
a podium to get caught. Have fun little haxxors, Cheers!
```

Ransomed.vc's last post on Telegram about the end of the operation

Ransomed.vc shared a Telegram post announcing the shutdown of their operations due to the **arrest of six individuals** associated with their group. The announcement acknowledged that the financial gains did not outweigh the harm caused to their affiliates' lives. It highlighted the mistake of hiring young and inexperienced people, which led to security lapses and likely contributed to their arrests. However, the post contained no apology for the ransomware attacks they were involved in. Concluding the post, Ransomed.vc distanced themselves from the actions of their former associates and the ongoing illegal activities, signing off with a casual farewell.

There are some questions in mind:

- What will happen to the Ransomed forum?
- What will happen to the victims?

We'll see in the future…

Bonus:

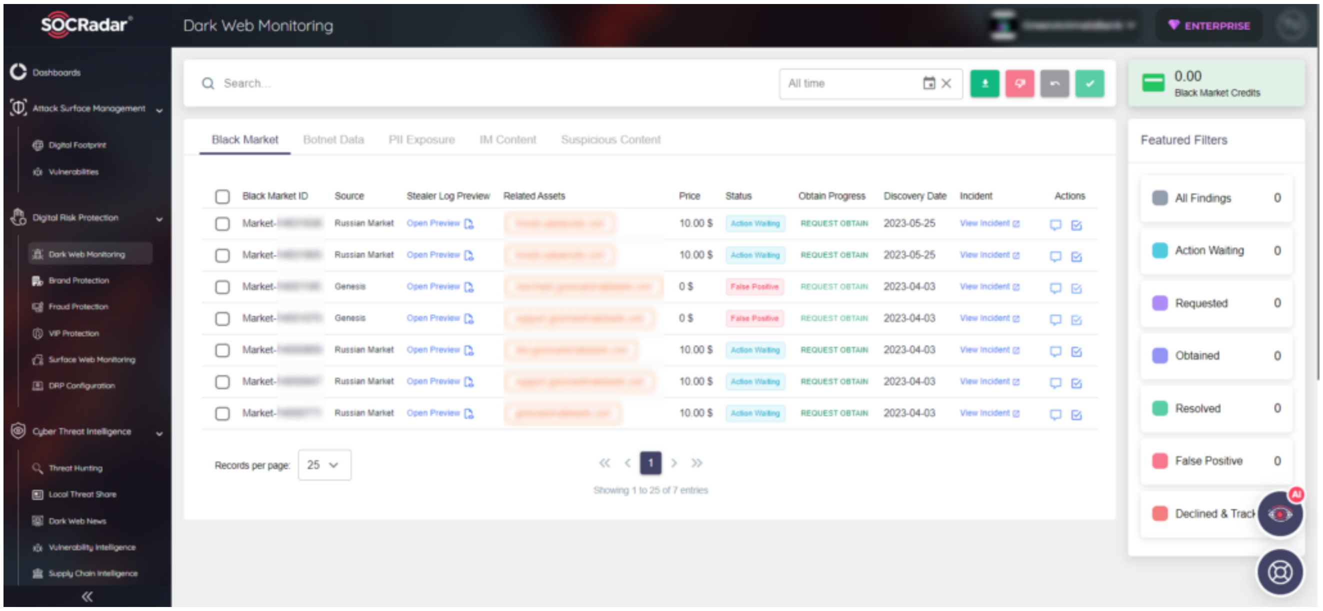
Twitter is buzzing with claims that the Ransomed admins are impotent and self-report their affiliates to the feds. We don't know if these rumors are true, but we discuss such rumors in another blog series, not here.

Follow Dark Peep if you want to know about rumors and interesting incidents happening on the dark web!

Discovering the Dark Web Landscape: SOCRadar XTI Monitoring and Threat Insights

Utilizing advanced monitoring techniques and AI-driven intelligence, SOCRadar XTI consistently surveils the entire web landscape, including the clear, dark, and deep web, alongside other hacker channels on platforms like Telegram. With its robust monitoring capabilities, SOCRadar provides an invaluable service by **alerting** organizations before compromise.

For a deeper understanding of the hidden facets of the internet and insights into threat actors operating from the depths of the dark web, and their malicious toolsets, **explore our platform.**



☐	Black Market ID	Source	Stealer Log Preview	Related Assets	Price	Status	Obtain Progress	Discovery Date	Incident	Actions
☐	Market-[redacted]	Russian Market	Open Preview	[redacted]	10.00 $	Action Waiting	REQUEST OBTAIN	2023-05-25	View Incident	
☐	Market-[redacted]	Russian Market	Open Preview	[redacted]	10.00 $	Action Waiting	REQUEST OBTAIN	2023-05-25	View Incident	
☐	Market-[redacted]	Genesis	Open Preview	[redacted]	0 $	False Positive	REQUEST OBTAIN	2023-04-03	View Incident	
☐	Market-[redacted]	Genesis	Open Preview	[redacted]	0 $	False Positive	REQUEST OBTAIN	2023-04-03	View Incident	
☐	Market-[redacted]	Russian Market	Open Preview	[redacted]	10.00 $	Action Waiting	REQUEST OBTAIN	2023-04-03	View Incident	
☐	Market-[redacted]	Russian Market	Open Preview	[redacted]	10.00 $	Action Waiting	REQUEST OBTAIN	2023-04-03	View Incident	
☐	Market-[redacted]	Russian Market	Open Preview	[redacted]	10.00 $	Action Waiting	REQUEST OBTAIN	2023-04-03	View Incident	

Records per page: 25

Showing 1 to 25 of 7 entries

SOCRadar Dark Web Monitoring

Furthermore, you can request **a free dark web report** here to learn the scope of your exposure to such threats and bolster your overall security posture.