W4 July | EN | Story of the week: Ransomware on the Darkweb

By S2W

Published: 2021-07-23 · Archived: 2026-04-05 21:15:47 UTC

9 min read

Jul 22, 2021

Kind but Bad Guy

Press enter or click to view image in full size

With contribution from

, , , | S2W LAB Talon

> SoW (Story of the Week) publishes a report summarizing ransomware's activity on the Darkweb. The report includes summary of victimized firms, Top 5 targeted countries and industrial sectors, status of dark web forum posts by ransomware operators, etc.

Executive Summary

1. [Statistics] There are a total of 34 ransomware victims in one week, and the US still accounts for the largest share at 23.5%, but the overall distribution is even in Southeast Asia and South America
2. [Darkweb] The operator of the Suncrypt ransomware guarantees a reliable transaction with the victim, and finally writes a security report on what to do to avoid such a breach
3. [Cryptocurrency] Suncrypt uses ChipMixer to launder Bitcoin received from victims
4. [Darkweb] LockBit2.0 Affiliate Program Promotion Activities Spotted on RAMP Forum
5. [Termination] KelvinsecTeam banned from the deep web hacking forum after its long journey of posting thousands of hacking related contents

1. Weekly Status

A. Status of the infected companies (07/12~07/18)

- For a week, a total of **34 infected companies** were mentioned
- **11 threat groups'** activities were detected

Press enter or click to view image in full size

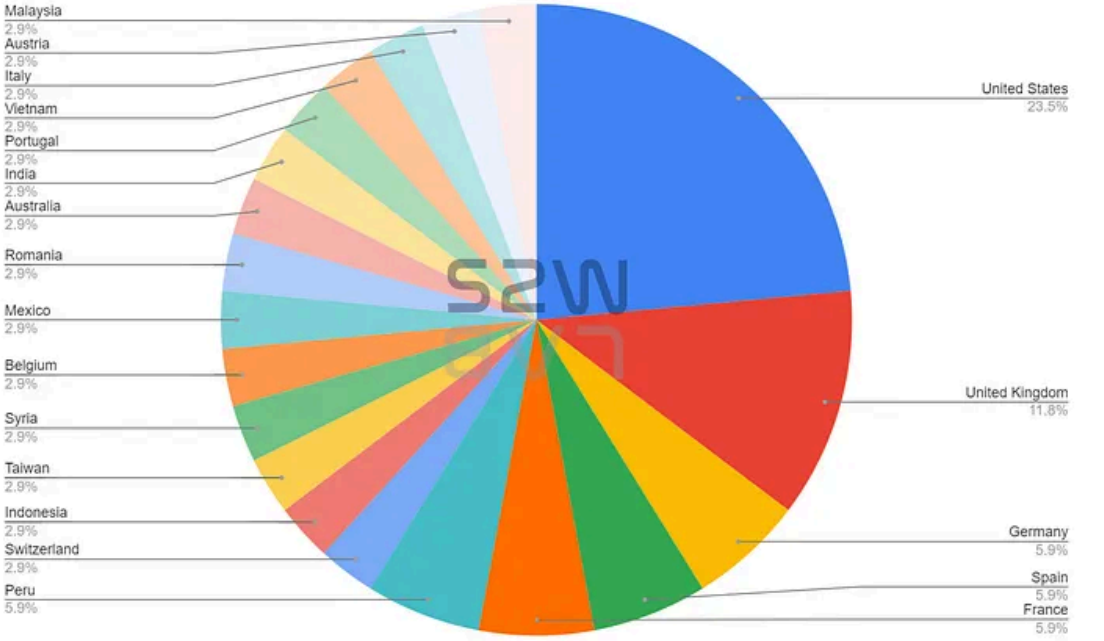
A. Status of the infected companies (07/12~07/18)

Name	Date updat...	HQ	Industry	Adversary
	07/12/2021	Germany	Government	Grief
	07/12/2021	Switzerland	Financial	Grief
	07/12/2021	Spain	Engineering	conti
	07/12/2021	france	energy	conti
	07/12/2021	United States	Military	marketo
	07/12/2021	france	IT	everest
	07/12/2021	Peru	Food production	Prometheus
	07/12/2021	Indonesia	Entertainment	Prometheus
	07/12/2021	Taiwan	Telecommunication	ransomexx
	07/13/2021	Syria	Logistics	Avos
	07/13/2021	United States	Law	Avos
	07/13/2021	Spain	Logistics	Avos
	07/13/2021	Belgium	Real estate	Avos
	07/13/2021	Peru	Financial	Prometheus
	07/14/2021	United Kingdom	Transportation	lockbit
	07/14/2021	Mexico	Transportation	lockbit
	07/14/2021	United Kingdom	Law	Avos
	07/15/2021	Romania	Agricultural	lockbit
	07/15/2021	United Kingdom	security	xing
	07/16/2021	United Kingdom	Education	Vsociety
	07/17/2021	Australia	Law	lockbit
	07/17/2021	United States	Law	lockbit
	07/17/2021	India	Media	Hive
	07/17/2021	United States	Others	Hive
	07/17/2021	Portugal	Airline	Hive
	07/17/2021	United States	Retail	Hive
	07/18/2021	Vietnam	Financial	lockbit
	07/18/2021	Italy	Fashion	lockbit
	07/18/2021	Austria	Transportation	lockbit
	07/18/2021	United States	Materials	lockbit
	07/18/2021	Germany	Financial	lockbit
	07/18/2021	Malaysia	Logistics	lockbit
	07/18/2021	United States	Government	Avos
	07/18/2021	United States	Services	Vsociety

Santinized by S2W LAB

B. TOP 5 targeted countries

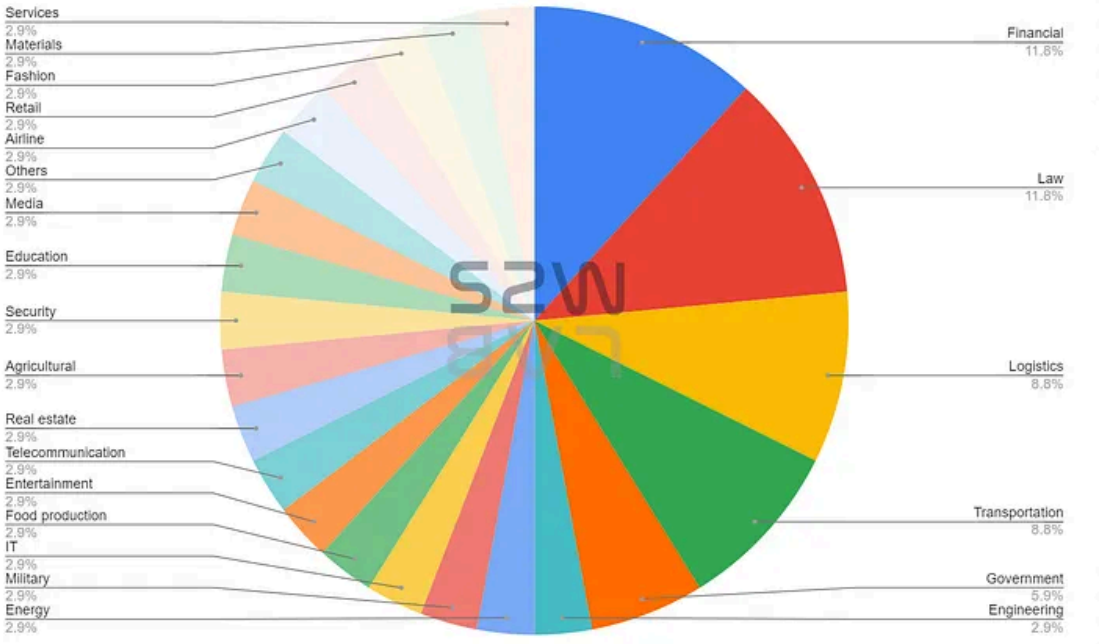
Press enter or click to view image in full size



1. United States — 23.5%
2. United Kingdom — 11.8%
3. Germany & Spain & France & Peru — 5.9%
4. Others — 2.9%

C. TOP 5 targeted industrial sectors

Press enter or click to view image in full size

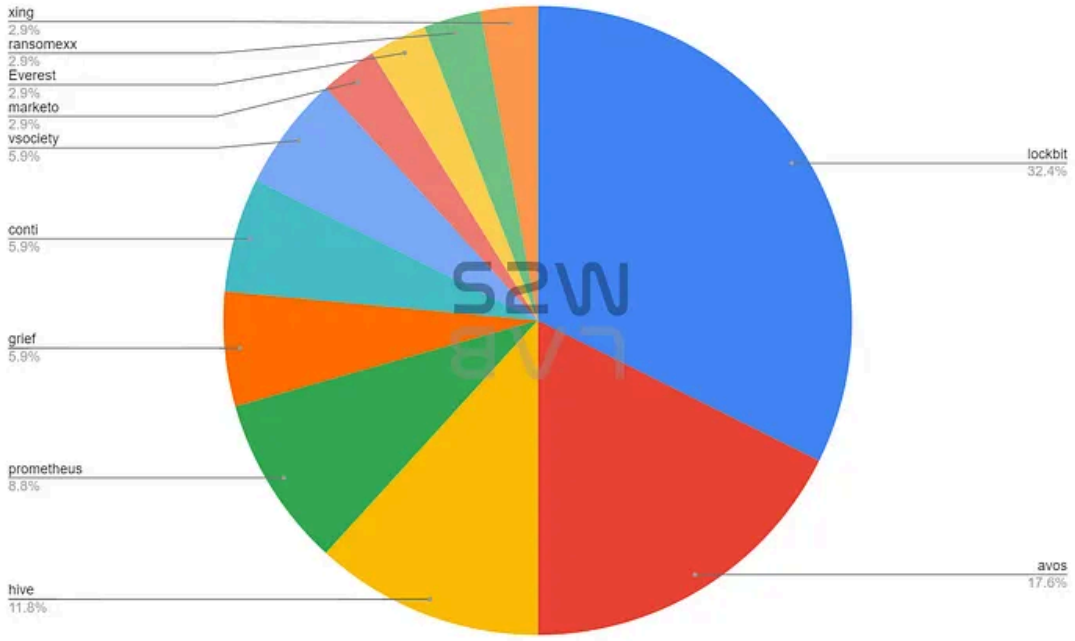


1. Financial & Law — 11.8%

2. Logistics & Transportation & Government- 8.8%
3. Others — 2.9%

D. Top 5 Ransomware

Press enter or click to view image in full size



1. Lockbit — 32.4%
2. Avos — 17.6%
3. hive — 11.8%
4. prometheus — 8.8%
5. grief — 5.9

E. Current status of data leak site operated by ransomware groups

- We are keep monitoring the status of data leak sites operated by ransomware groups and approximately 22 sites operate stably while 6 sites are unstable.
- “Latest Updated” is based on the date the victim company information was updated.

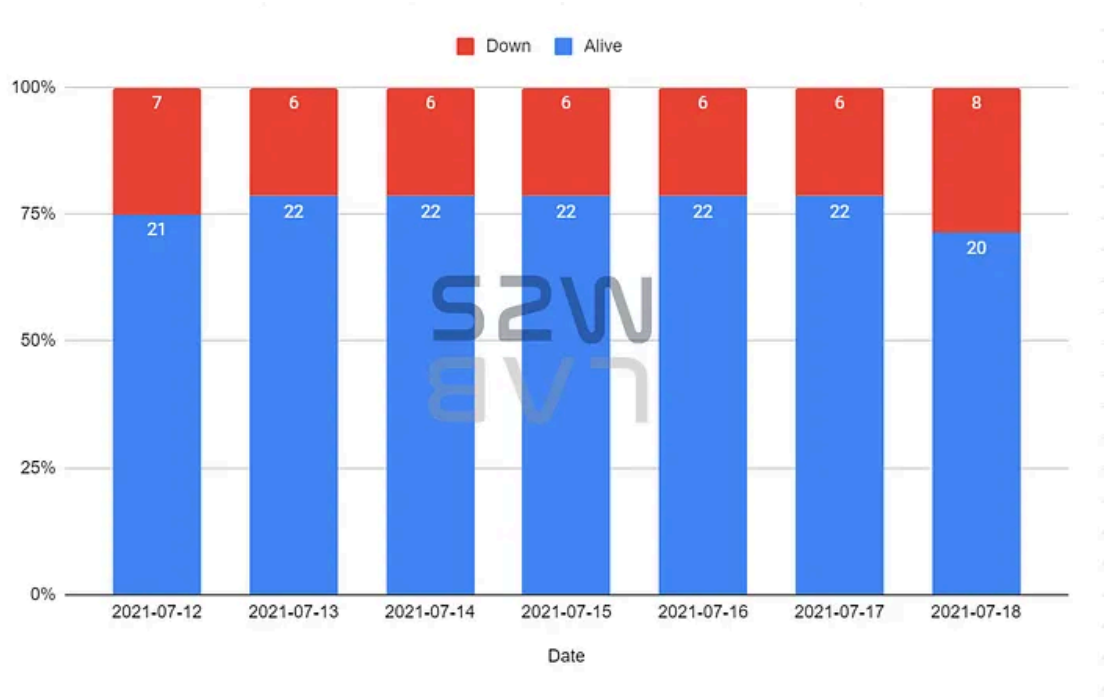
Monitoring data leak site operated by ransomware

Press enter or click to view image in full size

Ransomware	Status	Latest Updated
Grief	Live	07/12/2021
Prometheus	Live	07/13/2021
Mount Locker	Live	03/17/2021
Conti	Live	07/12/2021
Pysa	Live	06/15/2021
LV Ransomware	Live	06/22/2021
Vice society	Live	07/18/2021
Hive	Live	07/17/2021
LockBit	Live	07/18/2021
Cuba	Live	06/25/2021
Pay2Key	Live	05/02/2021
Nefilim	Live	05/31/2021
RansomExx	Live	06/03/2021
Marketo	Live	07/12/2021
Astro Team	Live	05/24/2021
REvil	Live	06/30/2021
Suncrypt	Live	06/20/2021
Payload bin	Live	06/08/2021
CL0P	Live	06/30/2021
DoppelPaymer	Live	06/25/2021
XING LOCKER	Live	07/15/2021
Lorenz	Live	06/24/2021
? "Leaks from darknet..."	Live	06/28/2021
Arvin Club	Live	06/28/2021
Ragnar Locker	Live	06/25/2021
Avaddon	Down	06/10/2021
? NONAME	Down	06/21/2021
SynAck	Down	06/16/2021

- Current status of monitoring data leak site operated by ransomware

  Press enter or click to view image in full size



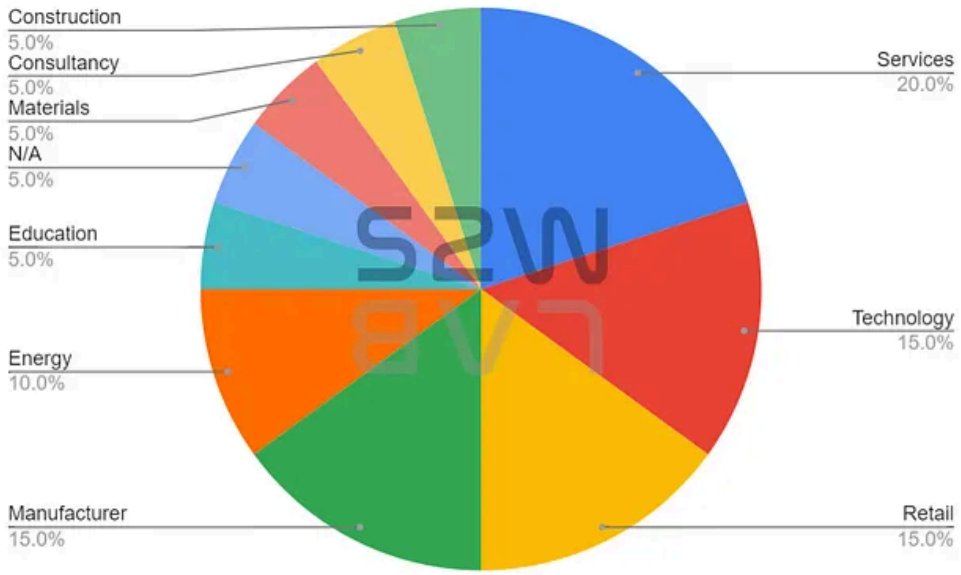
A. Suncrypt ransomware

- Suncrypt, which had not been updated by the victim company for half a year, was recently confirmed to have resumed activity after the victim’s negotiation page was discovered

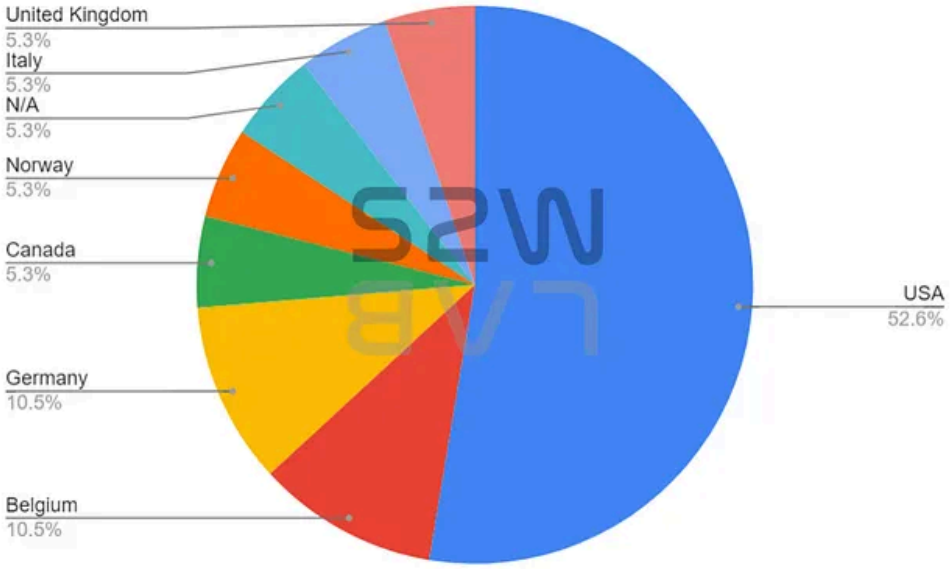
TOP 5 targeted industrial sectors & countries

- The industries affected by Suncrypt were mainly Services, Technology, and Retail, and HQ was mainly attacked by United States, Belgium, and Germany.

  Press enter or click to view image in full size



Press enter or click to view image in full size



Suncrypt infected companies

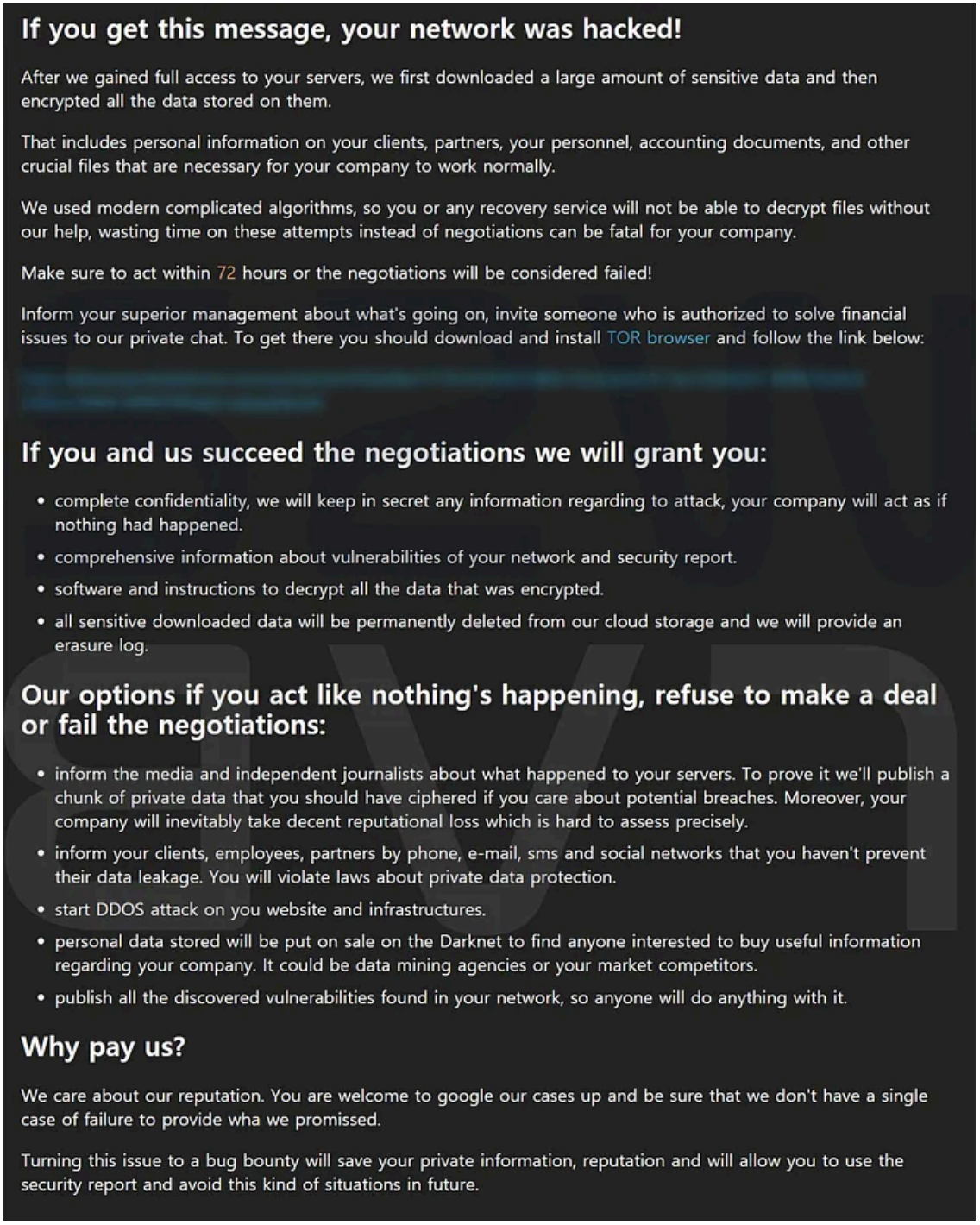
Press enter or click to view image in full size

Victim	Date	Industry	HQ
	08/01/2020	Consultancy	United States
	08/08/2020	Manufacturer	Canada
	08/14/2020	Retail	Norway
	08/14/2020	Services	United States
	08/21/2020	Services	United States
	08/24/2020	Education	United States
	08/25/2020	Technology	Belgium
	09/26/2020	Energy	United States
	08/28/2020	N/A	N/A
Santinized by S2W LAB	09/09/2020	Construction	United States
	09/10/2020	Services	United States
	09/10/2020	Technology	Italy
	09/15/2020	Energy	Belgium
	09/15/2020	Materials	United States
	09/15/2020	Technology	United States
	09/18/2020	Manufacturer	Germany
	09/22/2020	Retail	United Kingdom
	09/27/2020	Services	Germany
	09/29/2020	Retail	United States

A-1. Suncrypt infected companies

- In June 2021, Company C in the United States is infected with Suncrypt ransomware, internal files are leaked and encrypted, and the main website is subjected to DDoS attacks until pay BTC to Attacker
- Malware SHA256 : [509e16db291fb5b1ecf79154590f038d76e6579425daaee035db6480b4f2c33c]
- Via Ransom note, Suncrypt guides you through 1:1 chat page and details for negotiation

Press enter or click to view image in full size



If you get this message, your network was hacked!

After we gained full access to your servers, we first downloaded a large amount of sensitive data and then encrypted all the data stored on them.

That includes personal information on your clients, partners, your personnel, accounting documents, and other crucial files that are necessary for your company to work normally.

We used modern complicated algorithms, so you or any recovery service will not be able to decrypt files without our help, wasting time on these attempts instead of negotiations can be fatal for your company.

Make sure to act within 72 hours or the negotiations will be considered failed!

Inform your superior management about what's going on, invite someone who is authorized to solve financial issues to our private chat. To get there you should download and install TOR browser and follow the link below:

If you and us succeed the negotiations we will grant you:

- complete confidentiality, we will keep in secret any information regarding to attack, your company will act as if nothing had happened.
- comprehensive information about vulnerabilities of your network and security report.
- software and instructions to decrypt all the data that was encrypted.
- all sensitive downloaded data will be permanently deleted from our cloud storage and we will provide an erasure log.

Our options if you act like nothing's happening, refuse to make a deal or fail the negotiations:

- inform the media and independent journalists about what happened to your servers. To prove it we'll publish a chunk of private data that you should have ciphered if you care about potential breaches. Moreover, your company will inevitably take decent reputational loss which is hard to assess precisely.
- inform your clients, employees, partners by phone, e-mail, sms and social networks that you haven't prevent their data leakage. You will violate laws about private data protection.
- start DDOS attack on you website and infrastructures.
- personal data stored will be put on sale on the Darknet to find anyone interested to buy useful information regarding your company. It could be data mining agencies or your market competitors.
- publish all the discovered vulnerabilities found in your network, so anyone will do anything with it.

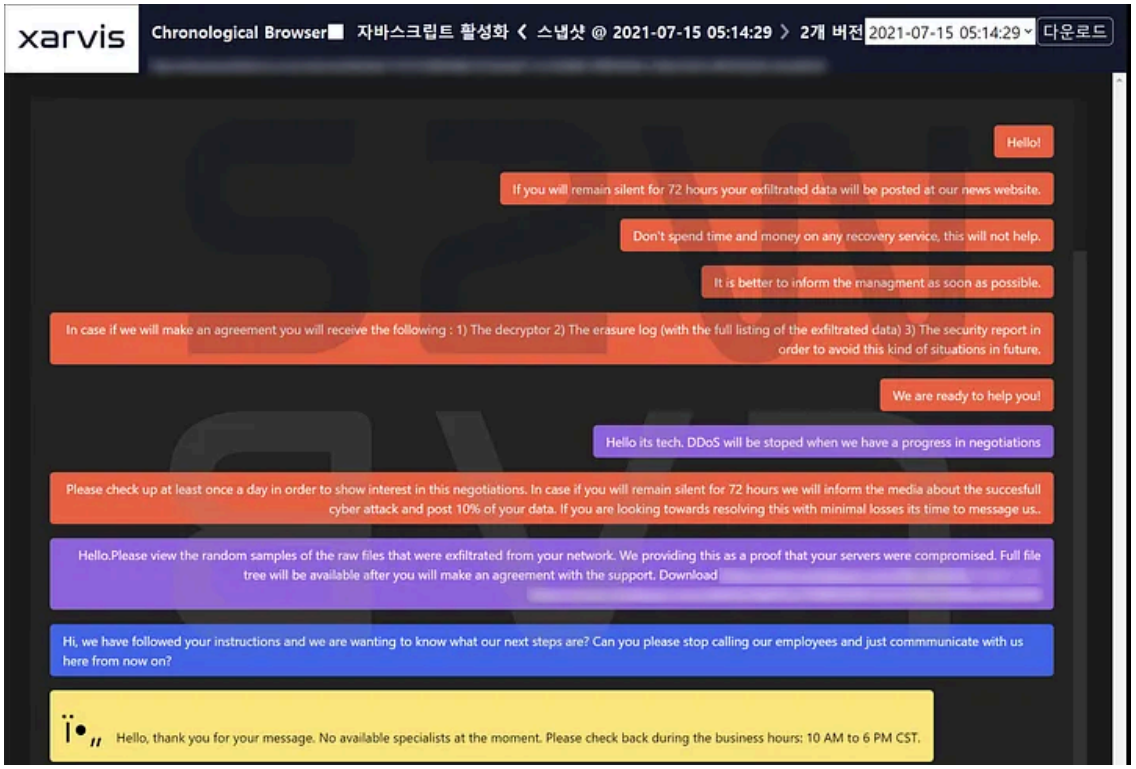
Why pay us?

We care about our reputation. You are welcome to google our cases up and be sure that we don't have a single case of failure to provide wha we promissed.

Turning this issue to a bug bounty will save your private information, reputation and will allow you to use the security report and avoid this kind of situations in future.

- 1:1 chat page with Suncrypt operator

Press enter or click to view image in full size



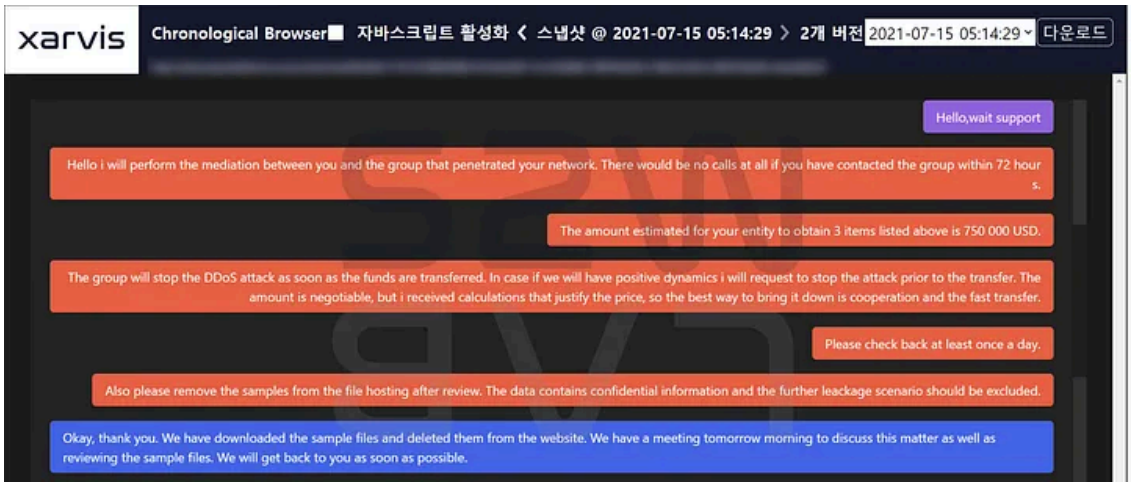
A-2. Negotiation the price of the victim company

- A negotiator is involved to mediate the price between Suncrypt and the victim company.
- The negotiator offers an amount of 750,000 (USD) from Suncrypt for the following three items that the victim company can provide if paid

1. **Decryptor** : decrypt files encrypted by ransomware
2. **The erasure Log** : A deletion log to confirm that Suncrypt has deleted all the leaked files
3. **The security report** : to avoid this kind of situations in the future

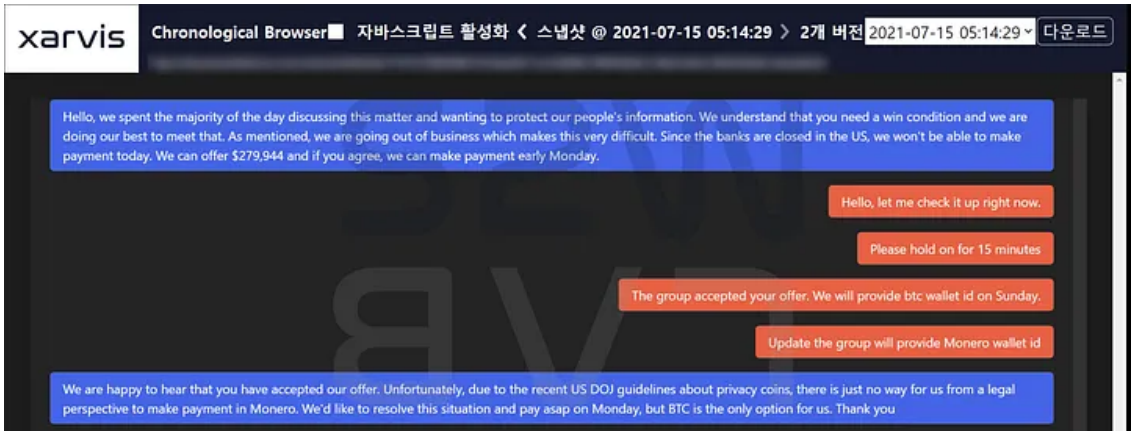
- He also mentioned that paying the amount will stop DDoS attacks on the company's website, and that the price can be lowered through fast delivery and negotiation

Press enter or click to view image in full size



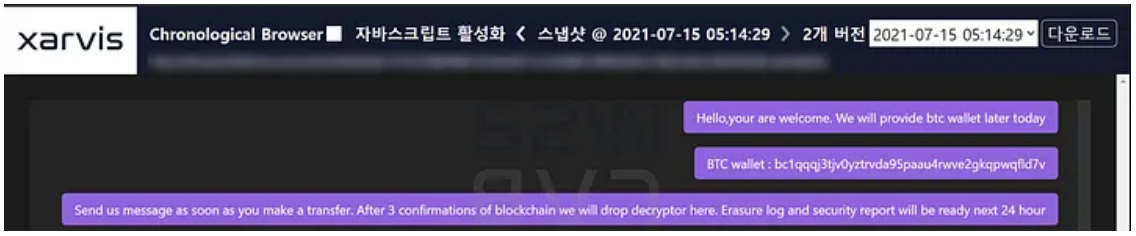
- After several rounds of negotiations, the victim company finally offered a $279,944 amount, and Suncrypt accepted it.
- Victims responded that they could not pay with Monero from a legal point of view, only Bitcoin, according to the U.S. Department of Justice's (DOJ) Guidline on Privacy Coins.

Press enter or click to view image in full size



- Accordingly, Suncrypt delivered the bitcoin address and the victim company transferred about 7.04 BTC to the address.
- Payment date : 2021–06–15 05:46
- Bitcoin Address : bc1qqqj3tjv0yztrvda95paau4rwve2gkqpwqfld7v

Press enter or click to view image in full size

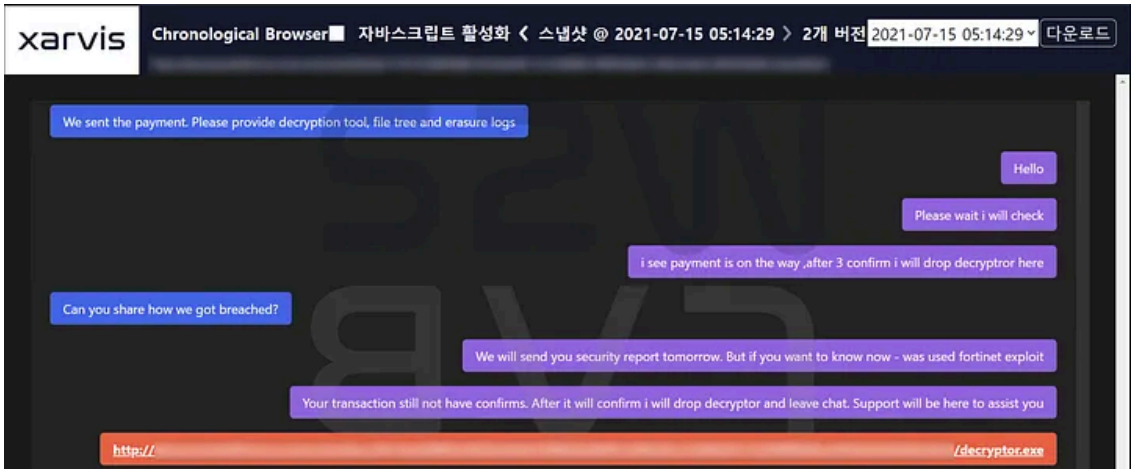


- After confirming the amount paid, Suncrypt provides the first three items (Decryptor, The erasure Log, The security report) that he said will be provided when the transaction is complete.

1) Decryptor

- decrypt files encrypted by ransomware and detailed instructions

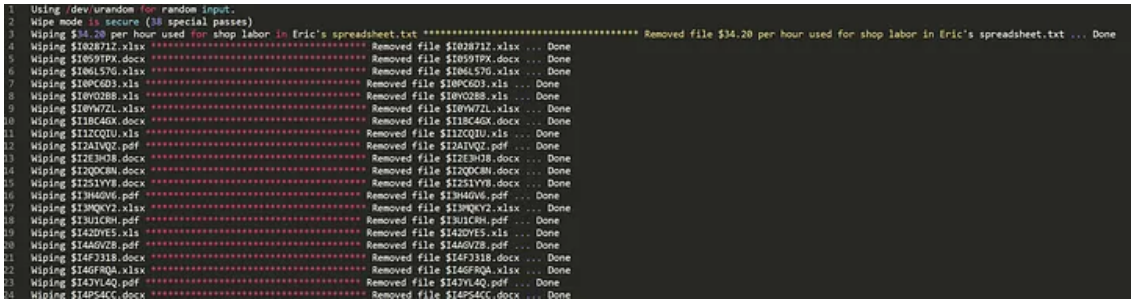
Press enter or click to view image in full size



2) The erasure Log

- An erasure logs to prove that Suncrypt has deleted all files stealed from the victim company

  Press enter or click to view image in full size



3) The security report

- Suncrypt also provides complete after-sales service in details report that to avoid this kind of situations in the future

  Press enter or click to view image in full size

A-3. Security consulting offered by Suncrypt

1. Defend your credentials from mimikatz

- Limit administrator privileges to the smallest group possible
- Even if you have thousands of user accounts, you should probably only have 2–5 administrator accounts
- Start with two accounts and force users to justify any additional accounts added to the administrator group
- upgrade the schema and functional level of your forest and domain to at least 2012 R2

**This domain functional level adds a fairly new group called “Protected Users”. Along with other protections, the members of the Protected Users group cannot authenticate by using NTLM, Digest Authentication, or CredSSP. These changes provide powerful protections that make Mimikatz almost worthless.

2. Verify KB2871997 has been installed to apply additional required security.

- After you install this security update, the default setting for non-protected users on Windows 7 and Windows 8 is to not force clear leaked logon session credentials
- To override this default you can add the following registry dword, **TokenLeakDetectDelaySecs**, and set it to a recommended value of 30 seconds

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\TokenLeakDetectDelaySecs

- Stop storing passwords in memory by changing the “UseLogonCredential” registry setting to ‘0’ instead of the default value of “1” and passwords are no longer available to Mimikatz

**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest

UseLogonCredential 0 : not store credentials in memory

UseLogonCredential 1 : store credentials in memory

3. Start monitoring your systems for unauthorized software and malware, which should help identify Mimikatz installation and activity

4. In your specific case the critical vulnerabiliry contained Forti VPN, please update FortiVpn and monitor for updates and Windows updates

5. Inform your IT stuff to remove the posibility of storing user passwords within the network

6. Also we recommend you to use SentinelAV and dattoo backup system. Also Veeam Tapes is good ,but pc with veeam should be in WORKGROUP and user should be different from main domain

7. Every PC should have AV. Don’t let any pc without AV

8. Also try configure 2FA (at all network pc) when you connect to remote desktop

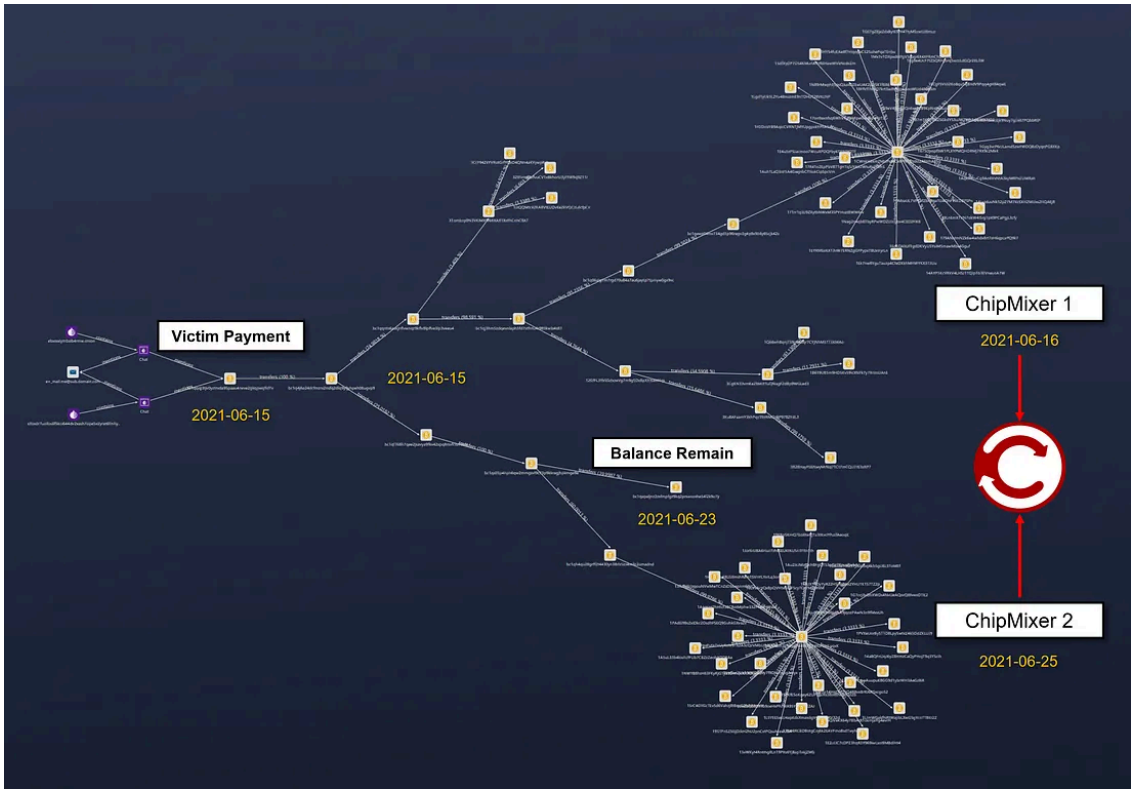
9. Use password on AV

10. Also tip for you: If you want chage Fortigate VPN to other . We dont reccomend you to use Sonic VPN,Pulse Secure, because its under massive hack

A-3. Transaction analysis

- Bitcoin transaction analysis paid by victim
- Payment date : 2021–06–15 05:46
- Amounts : 7.044 BTC

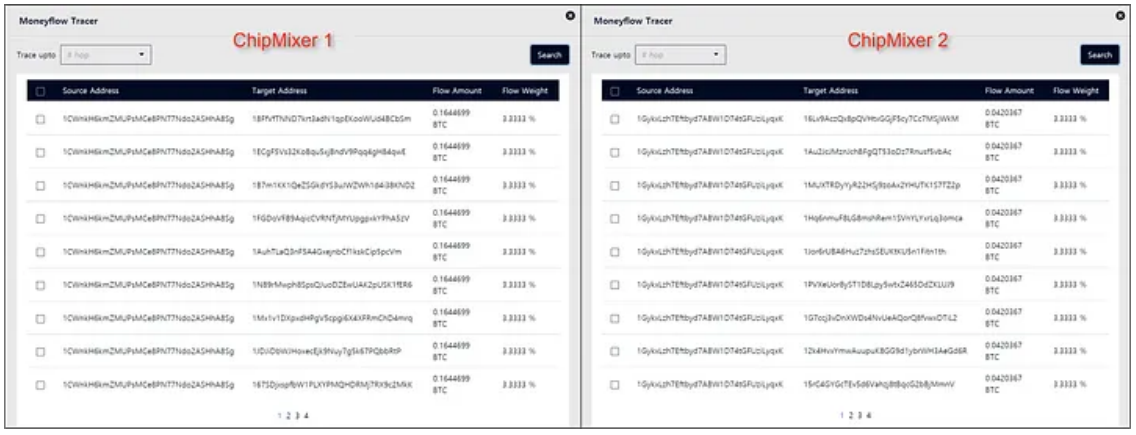
  Press enter or click to view image in full size



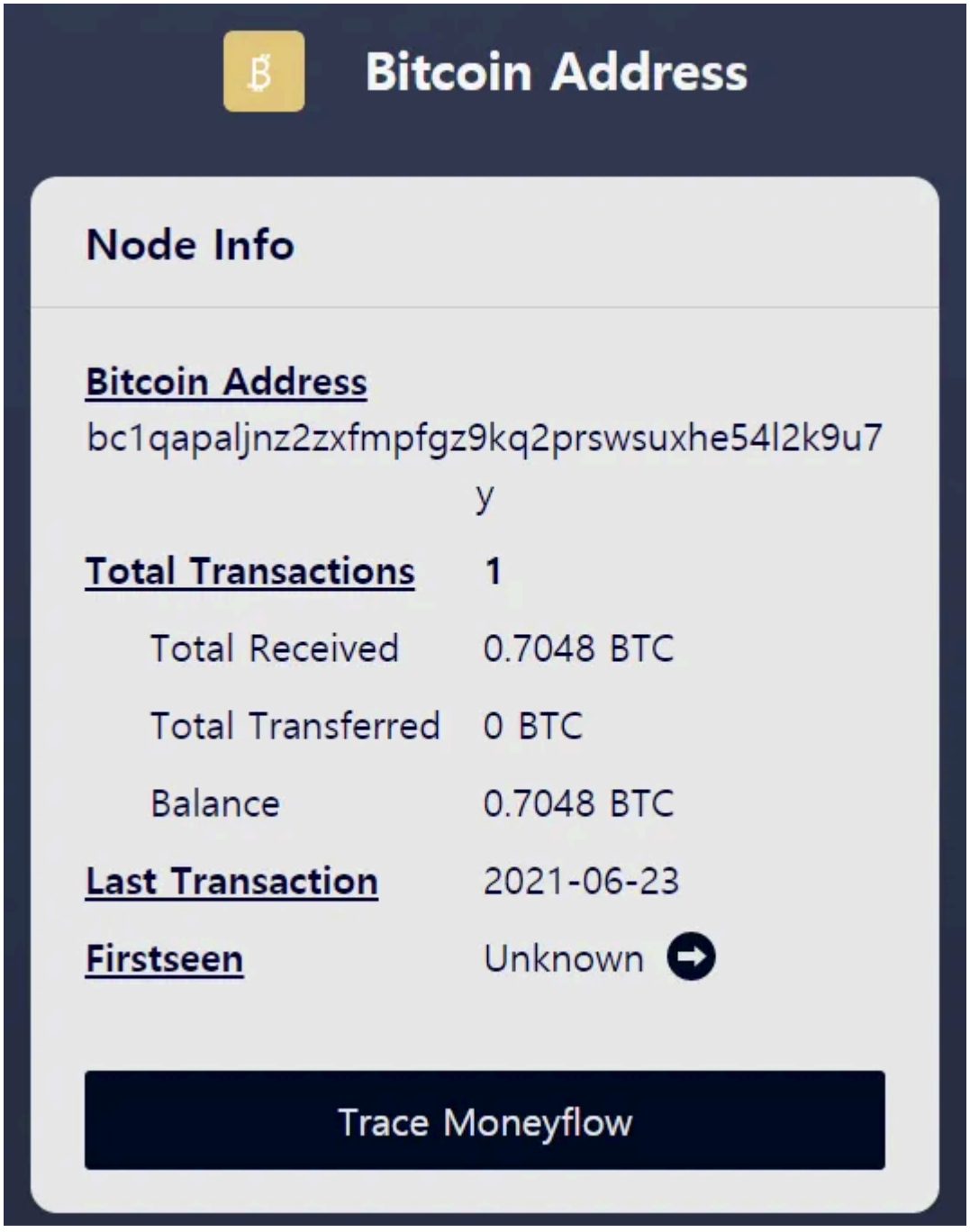
Bitcoin transaction analysis via Xarvis

- 6.1951973 BTC amount, which is about 88%, finally flows to the following two addresses, and money laundering is performed through coin mixing
- **ChipMixer(coin mixing) 1**
- Address : 1CWnkH6kmZMUPsMCe8PN77Ndo2ASHhA8Sg
- Amounts : 4.9340973 BTC
- Transactions time : 2021–06–16 07:40
- **ChipMixer(coin mixing) 2**
- Address : 1GykxLzh7Eftbyd7ABW1D74tGFUziLyqxK
- Amounts : 1.2611 BTC
- Transactions time : 2021–06–25 09:41

Press enter or click to view image in full size



- If you look at the amount divided by performing Coin mixing, it is distributed in exactly the same amount.
- In particular, the pattern in which the same amount is divided by a combination of 0.001 BTC, 0.002 BTC, and 0.004 BTC is a typical feature of mixing performed by ChipMixer, and it is suspected that coin laundering was attempted using ChipMixer.
- Currently, there are addresses that have some remaining amount excluding them, and it seems that monitoring is needed for transactions in this addresses.
- Address : bc1qapaljnz2zxfmpfgz9kq2prswsuxhe54l2k9u7y
- Amounts : 0.7048 BTC



C. RAMP(Babuk/Payload.bin)

- It has been changed to a membership forum, and the number of community active users and posts is gradually increasing

  Press enter or click to view image in full size

- User status as of 2021.07.20

  Press enter or click to view image in full size

- Admin Orange, Moderator 777 Users are the most active

  Press enter or click to view image in full size

User list

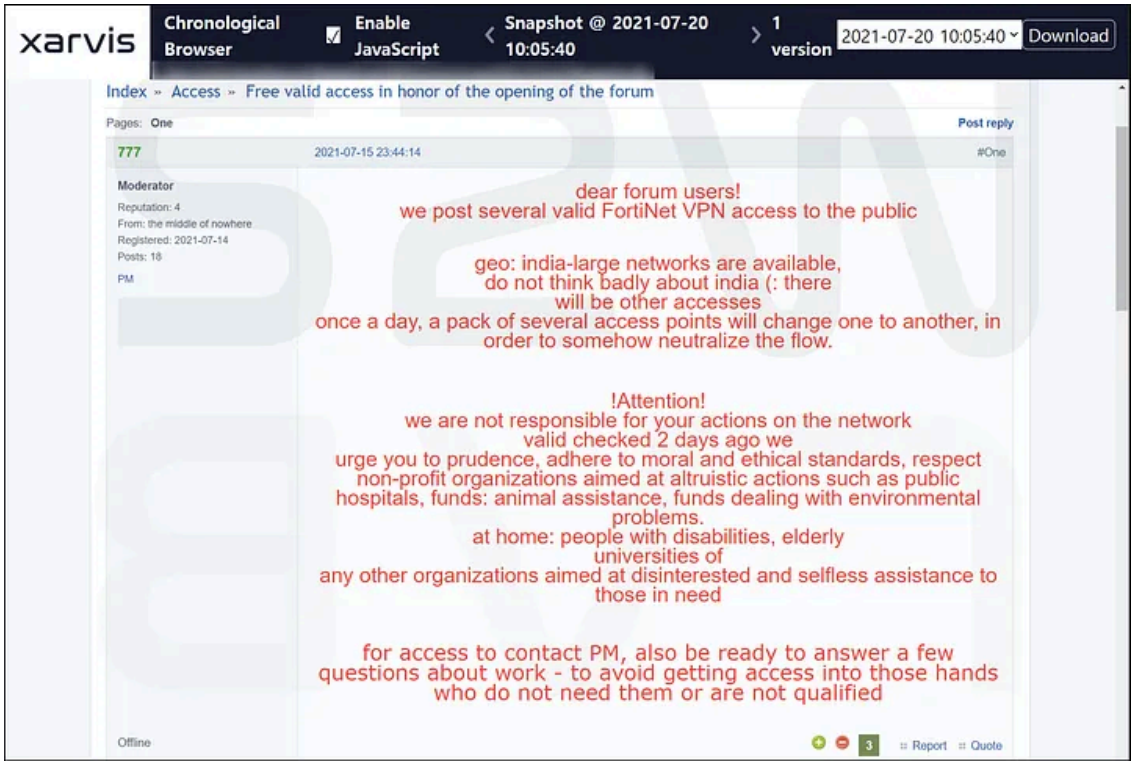
Username	Title	Posts	Registered
Orange	Admin	46	2021-07-11
777	Moderator	22	2021-07-14
KAJIT	Member	16	2021-07-16
pomidor	Member	7	2021-07-17
pacho2	Member	5	2021-07-18
Дед-в-бункере	Member	4	2021-07-16
Novichok	Member	4	2021-07-19

C-1. The post of selling FortiNet VPN

REvil ransomware has posted a purchase article on an underground forum to purchase VPN-related access information, and there is a possibility that ransomware groups may use VPN-related access information purchased through DDW in a ransomware attack

- Currently, the RAMP forum is operated for the purpose of promoting affiliate programs and sales services related to ransomware RaaS, so the credential information posted on the forum is highly likely to be misused by ransomware groups
- According to a post posted on July 15, 2021, a user has announced that Fortinet VPN access information will be posted

  Press enter or click to view image in full size

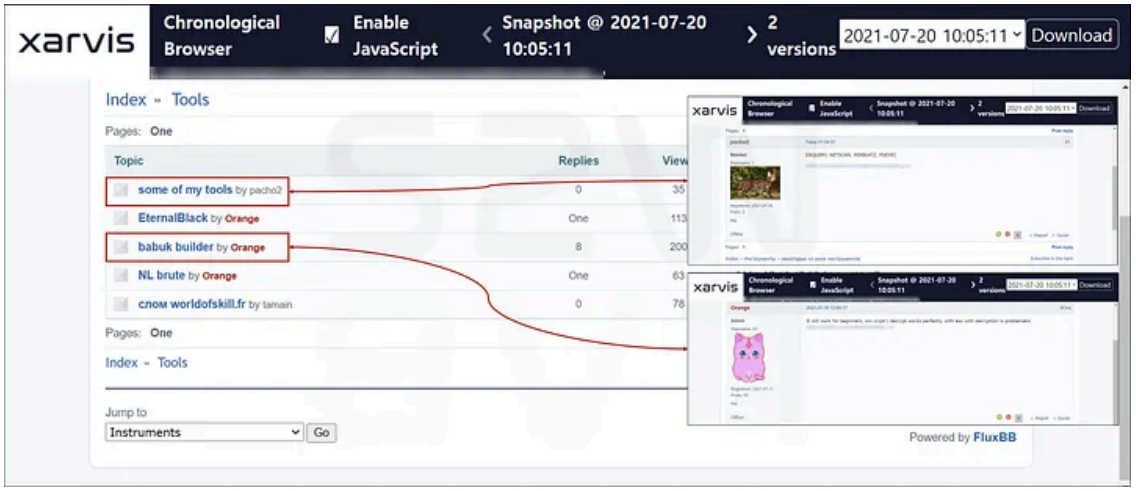


- The user who posted the first thread has not yet found any additional posts about VPN access information
- Forum admin posted credentials to access vsphere data center

C-2. Sharing hacking tools

- Tools used for hacking are shared among forum members

  Press enter or click to view image in full size



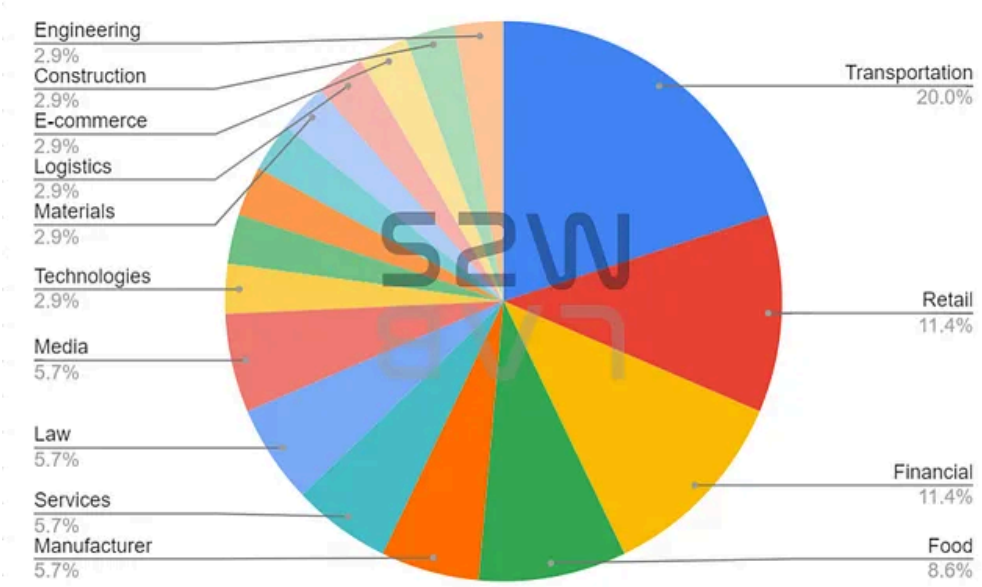
- Mimikatz: A tool that can steal Windows account passwords
- Netscan : port scanning tool
- Dsquery: Active Directory query tool (collect user accounts, domain trusts, permission information)
- Psexec : Used to download or upload files via network share.
- Babuk Builder: A tool to create Babuk ransomware

C-3. LockBit promoting LockBit affiliate program

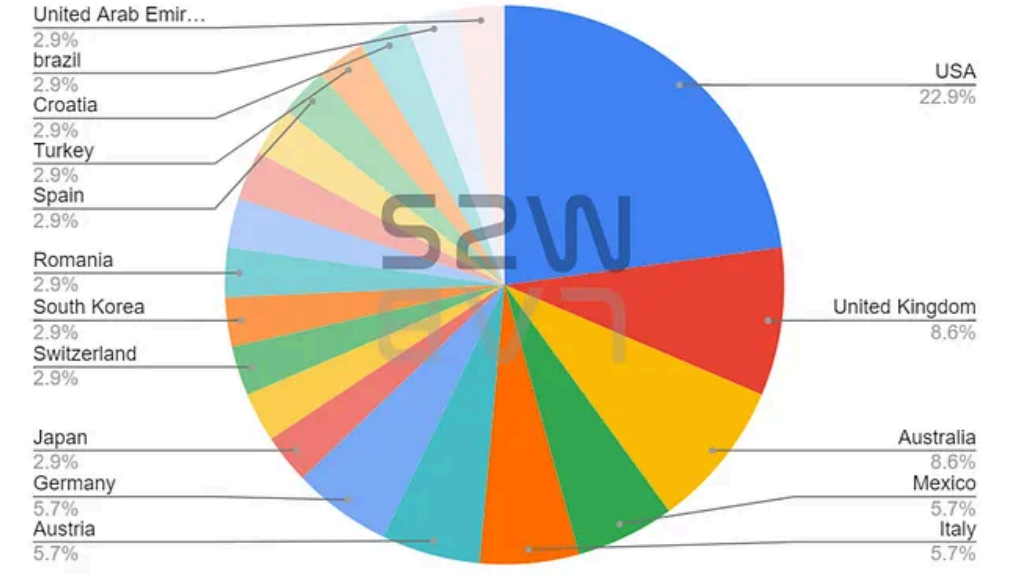
- On July 15, 2021, it was confirmed that the operator of LockBit, which has been showing the most activity for the past week, is actively promoting the LockBit affiliate program.
- Compared to other ransomware, the activity level was low, and information about 11 new victims was posted on the Rick site this week.
- The industries affected by LockBit were mainly Transportation, Retail and Financial, and the HQ was mainly attacked by United States, United Kingdom and Australia.

TOP 5 targeted industrial sectors & countries

Press enter or click to view image in full size

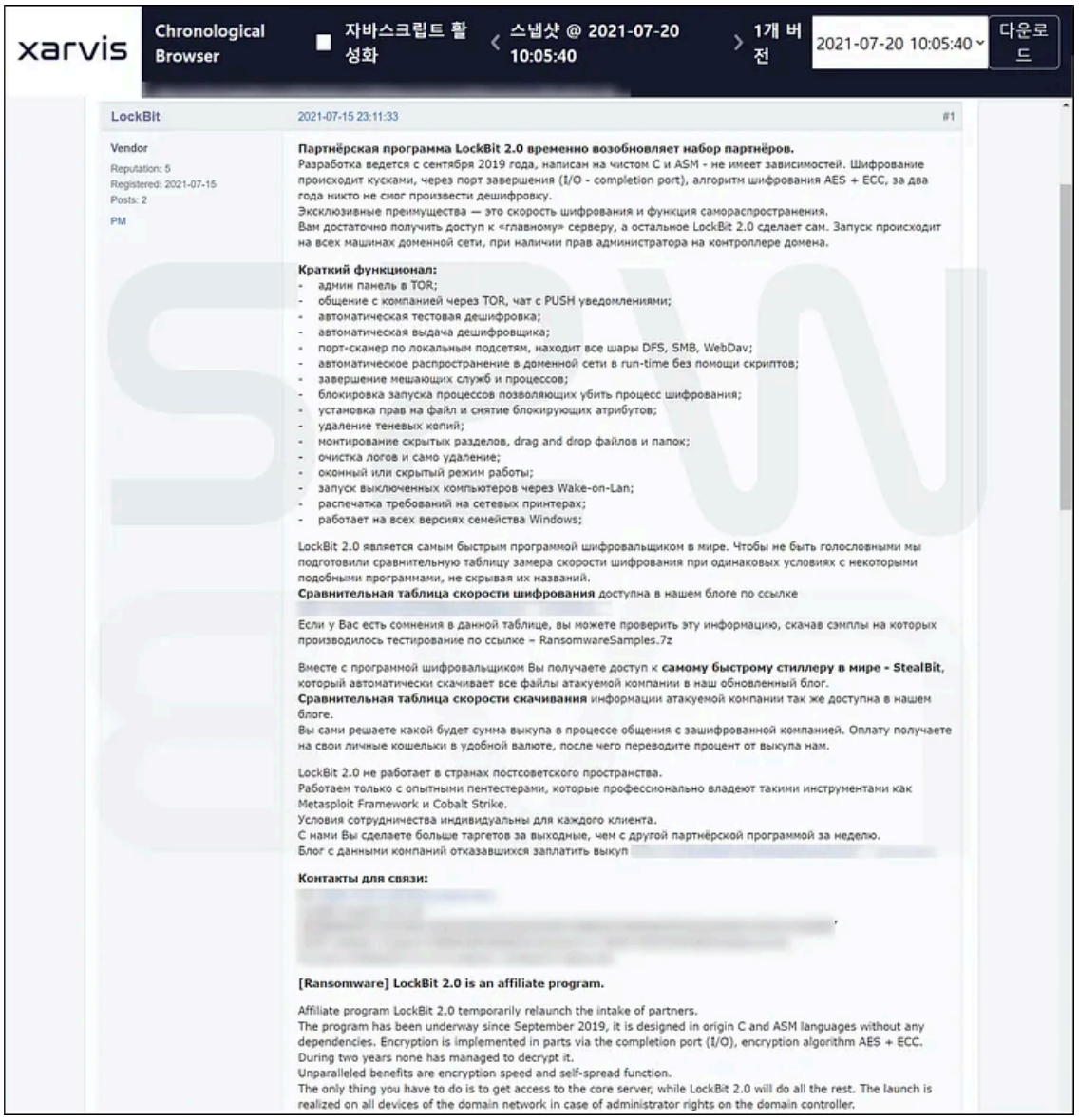


Press enter or click to view image in full size



The post of LockBit promoting LockBit affiliate program

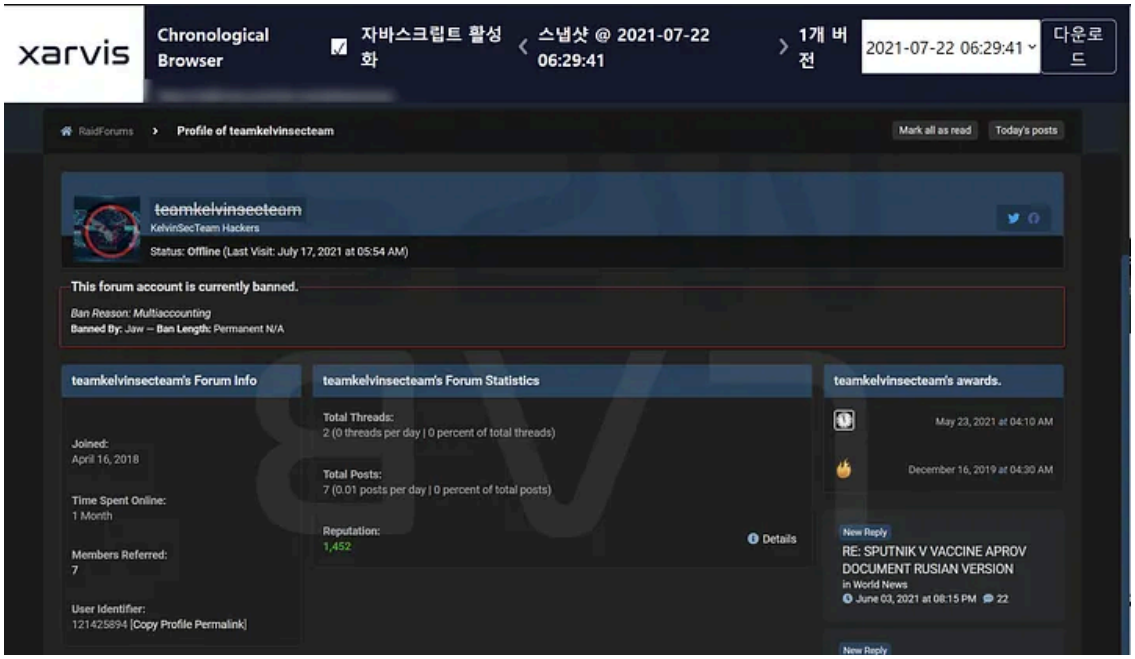
Press enter or click to view image in full size



3. Posts related to Underground Forum @Dark Web

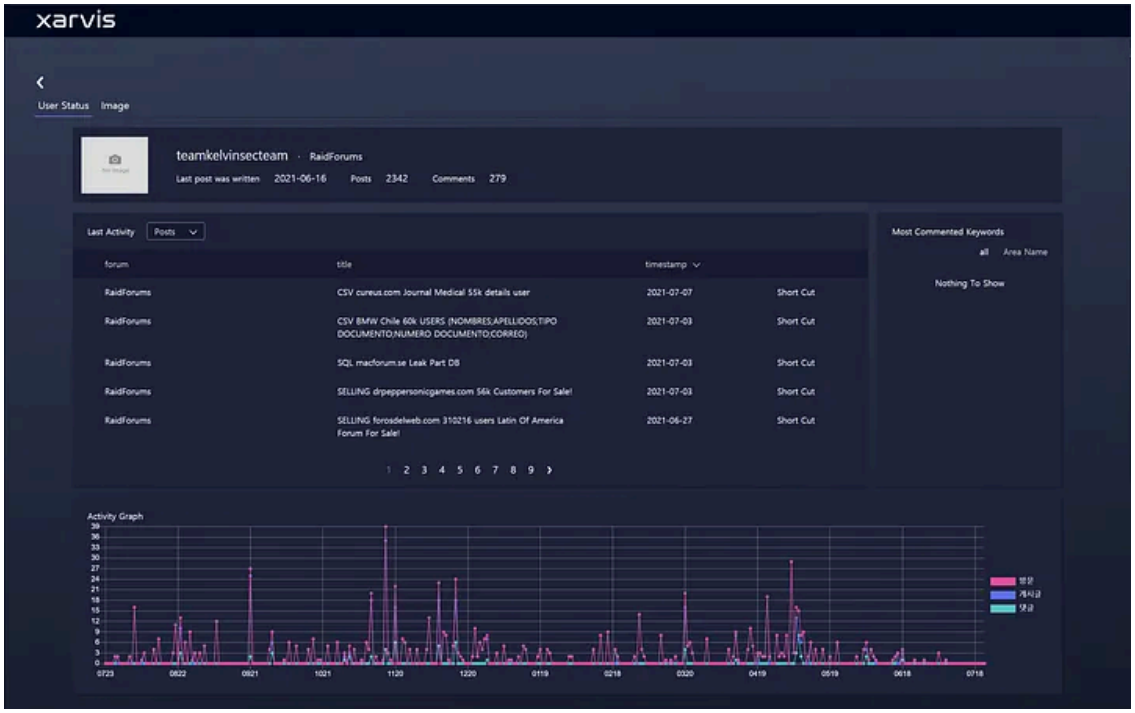
A. Banned @teamkelvinsecteam

Press enter or click to view image in full size



- Teamkelvinsecteam is an active user on Radiforums, and has posted more than 1,000 hacking related posts during the active period
- It is known as a famous hacking group within the forum and has a high reputation
- All posts written in the past are now deleted

Press enter or click to view image in full size



Conclusion

- As the Suncrypt ransomware victim paid a high cost, it is necessary to review and apply the security consulting content that could be obtained as a post-service service to other companies.

- As the number of active users in the RAMP forum increases, continuous monitoring of users and posts is necessary.

- Homepage: https://www.s2wlab.com
- Facebook: https://www.facebook.com/S2WLAB/
- Twitter: https://twitter.com/s2wlab
