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

medium.com/s2wlab/w4-july-en-story-of-the-week-ransomware-on-the-darkweb-c61965d0386a

S2W July 23, 2021

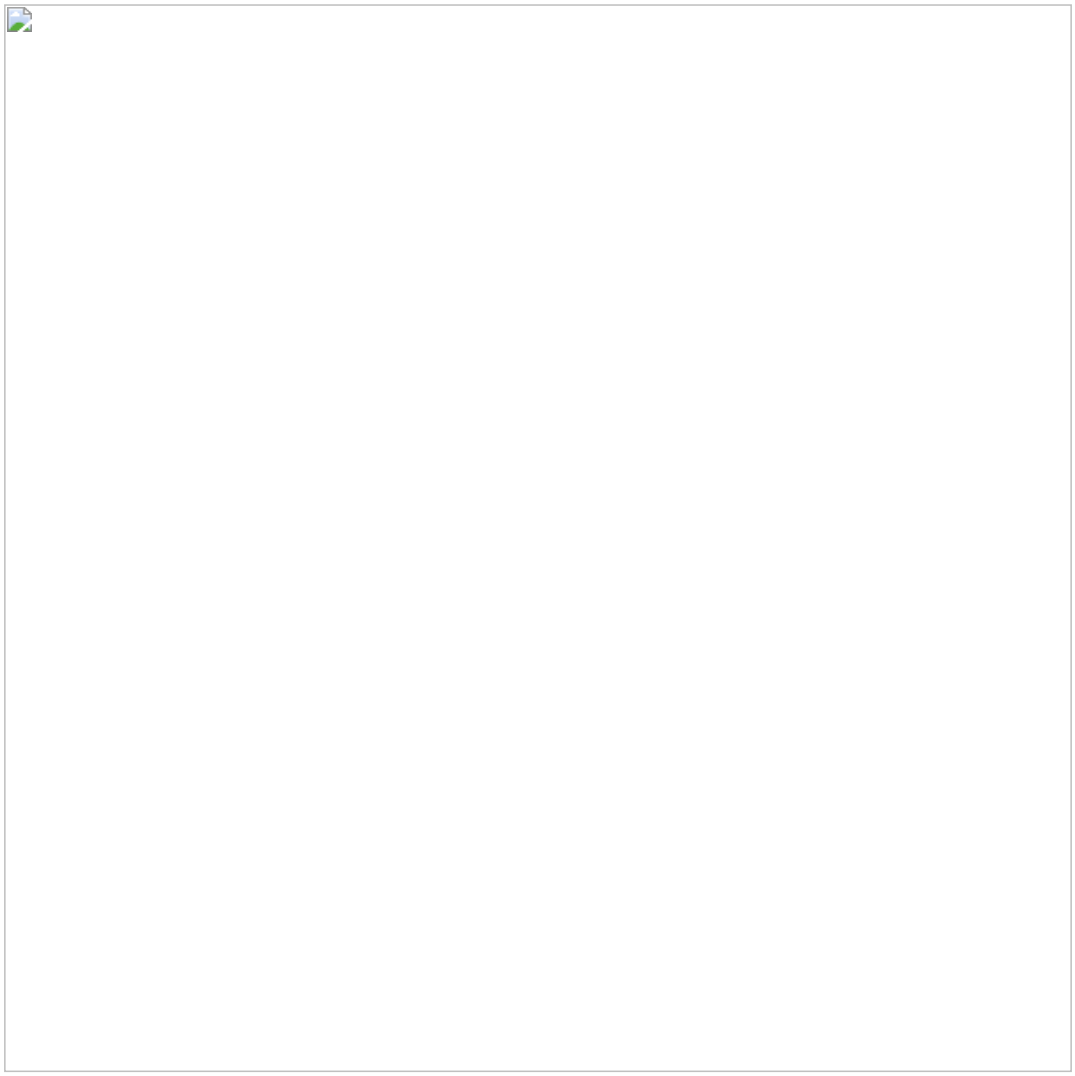
S2W

Jul 22, 2021

.

9 min read

Kind but Bad Guy



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.

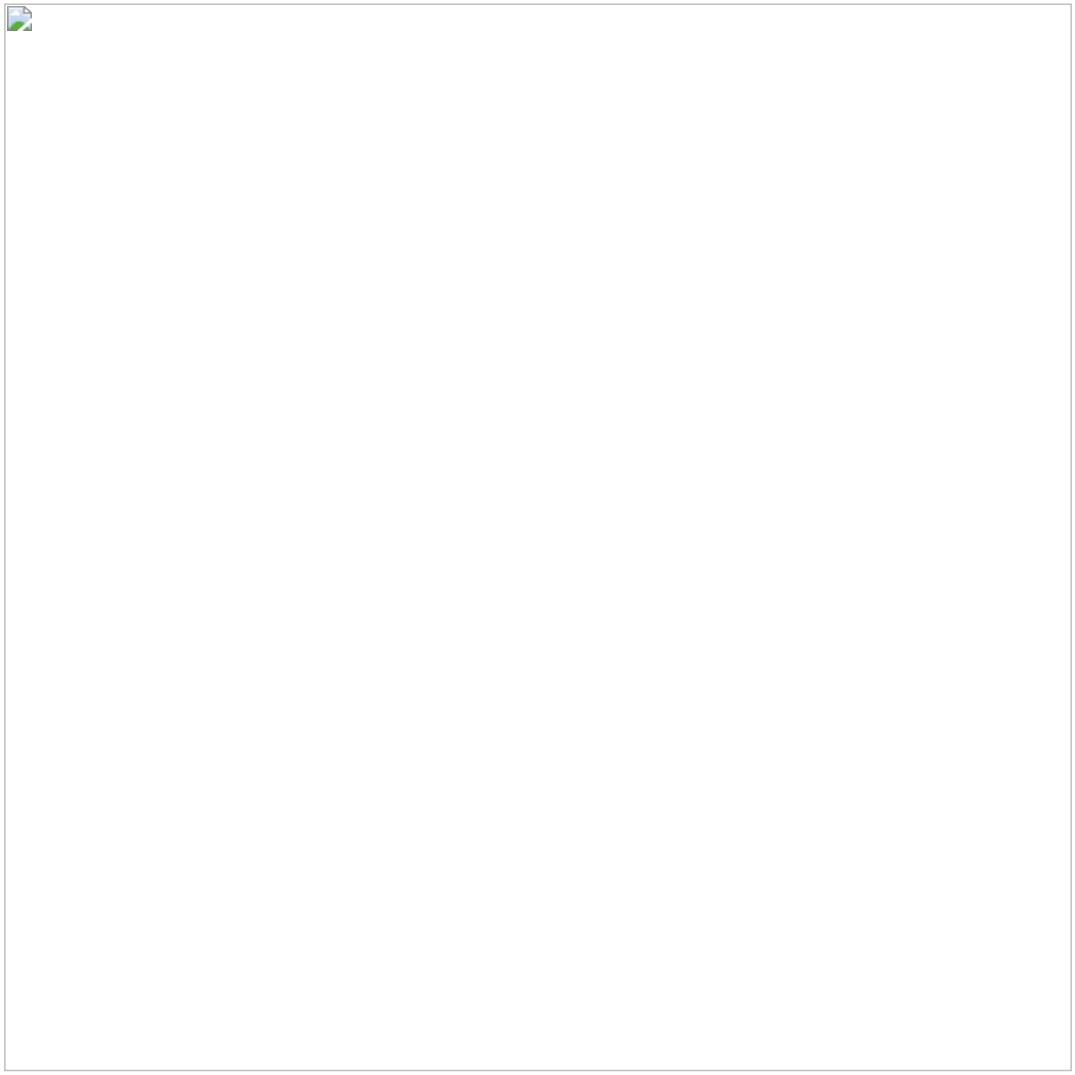
Executive Summary

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

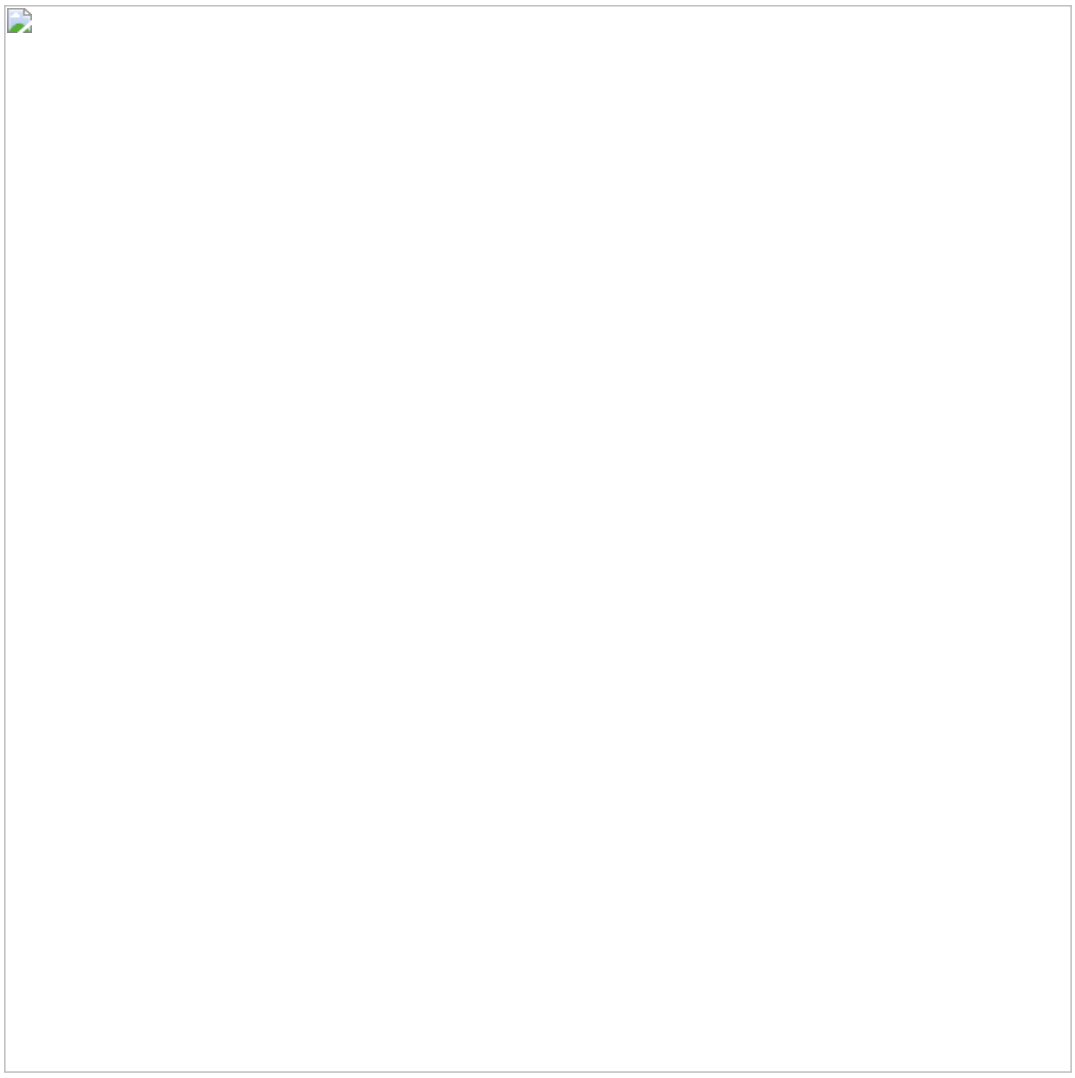
1. Weekly Status

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

- For a week, a total of were mentioned
- activities were detected

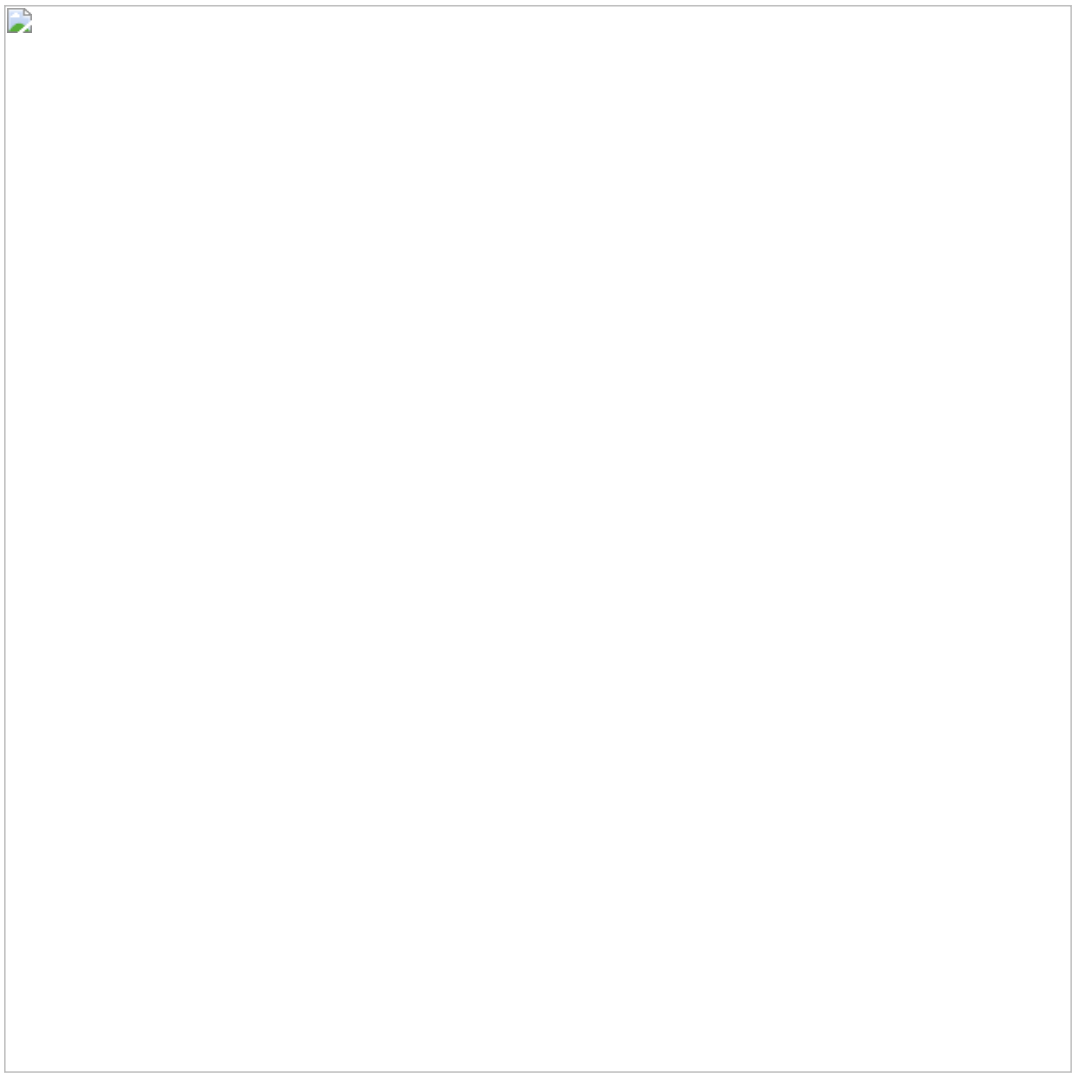


B. TOP 5 targeted countries



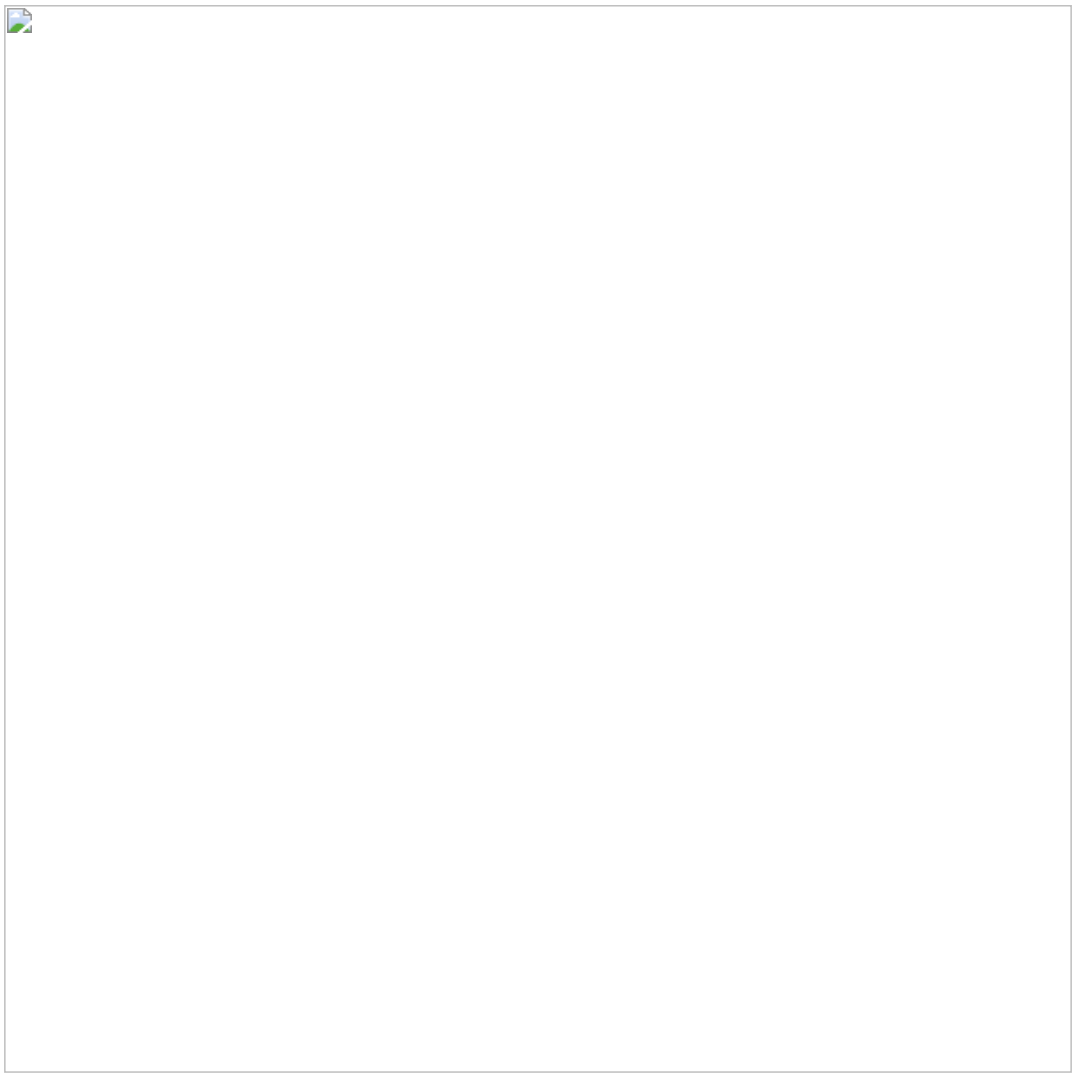
1. United States — 23.5%
2. United Kingdom — 11.8%
3. Germany & Spain & France & Peru — 5.9%
4. Others — 2.9%

C. TOP 5 targeted industrial sectors



1. Financial & Law — 11.8%
2. Logistics & Transportation & Government- 8.8%
3. Others — 2.9%

D. Top 5 Ransomware

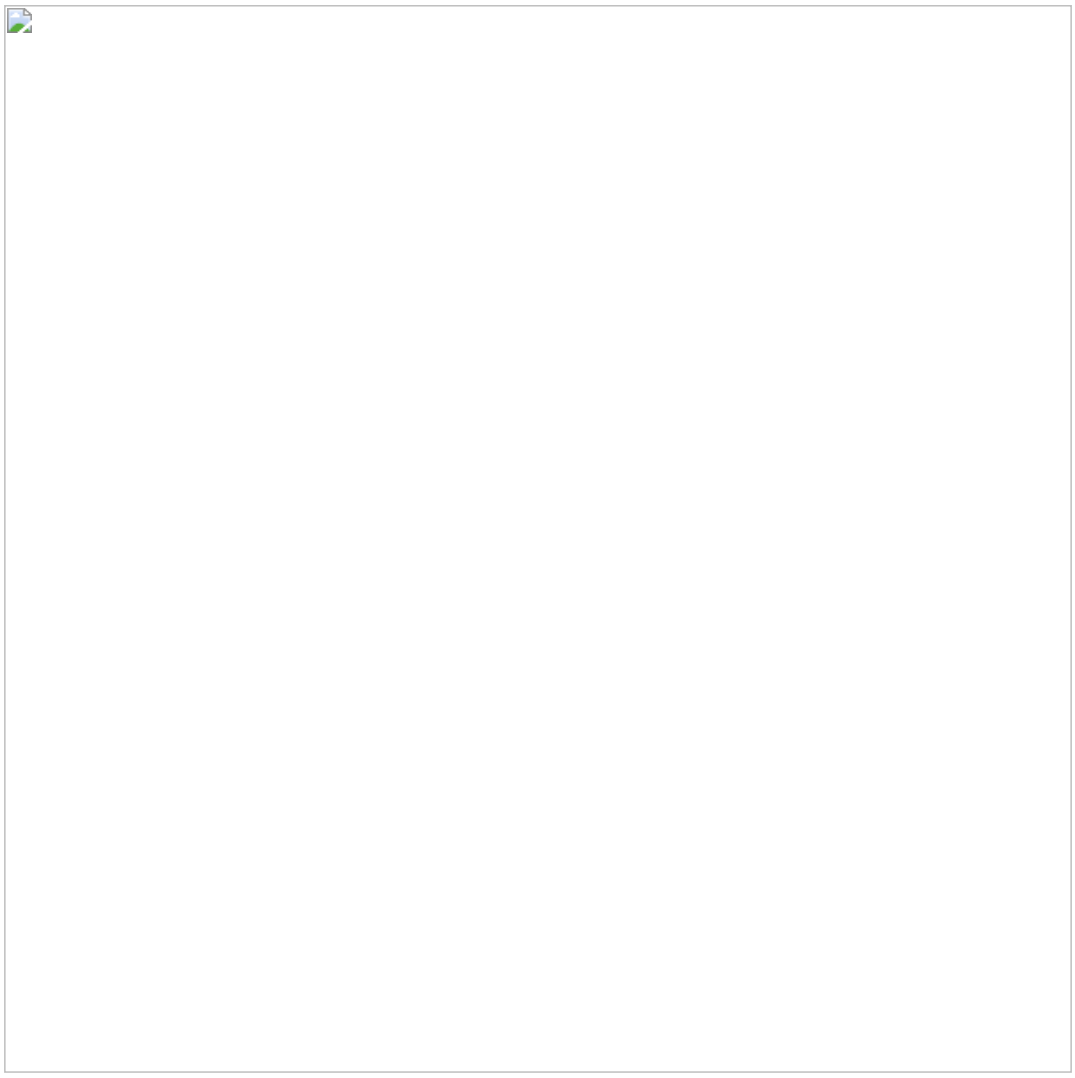


1. Lockbit — 32.4%
2. Avos — 17.6%
3. hive — 11.8%
4. prometheus — 8.8%
5. grief — 5.9

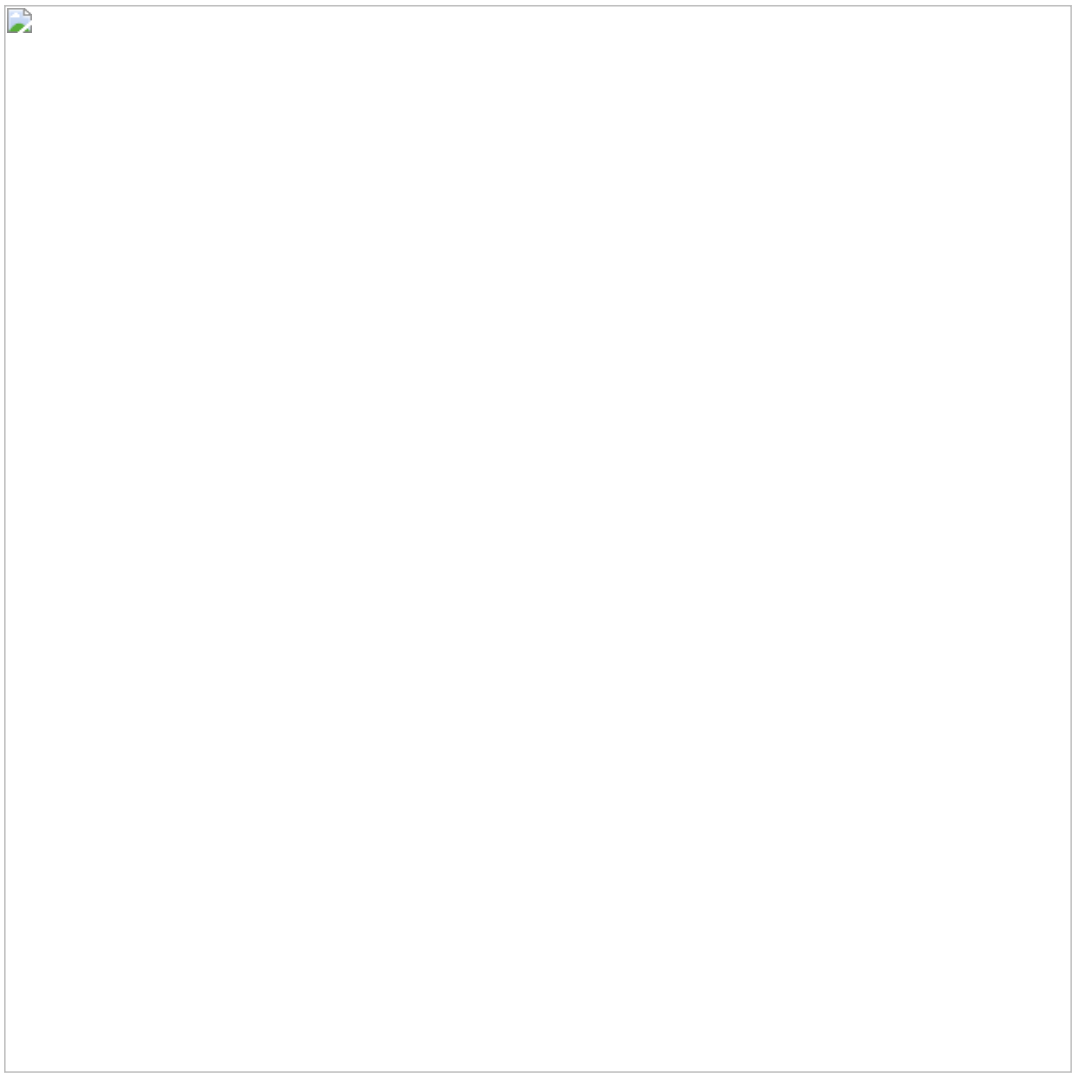
E. Current status of data leak site operated by ransomware groups

- 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



Current status of monitoring data leak site operated by ransomware



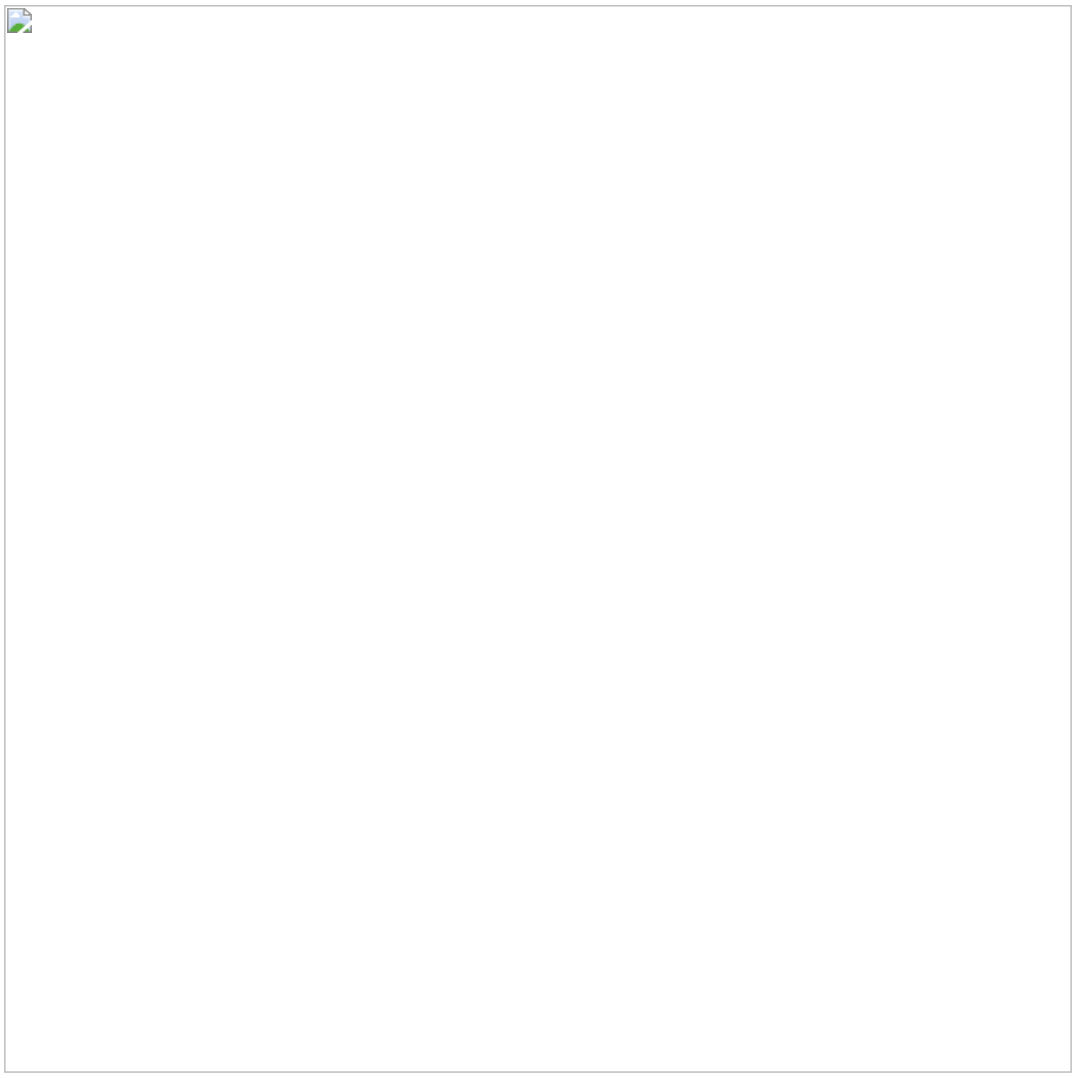
A. Suncrypt ransomware

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

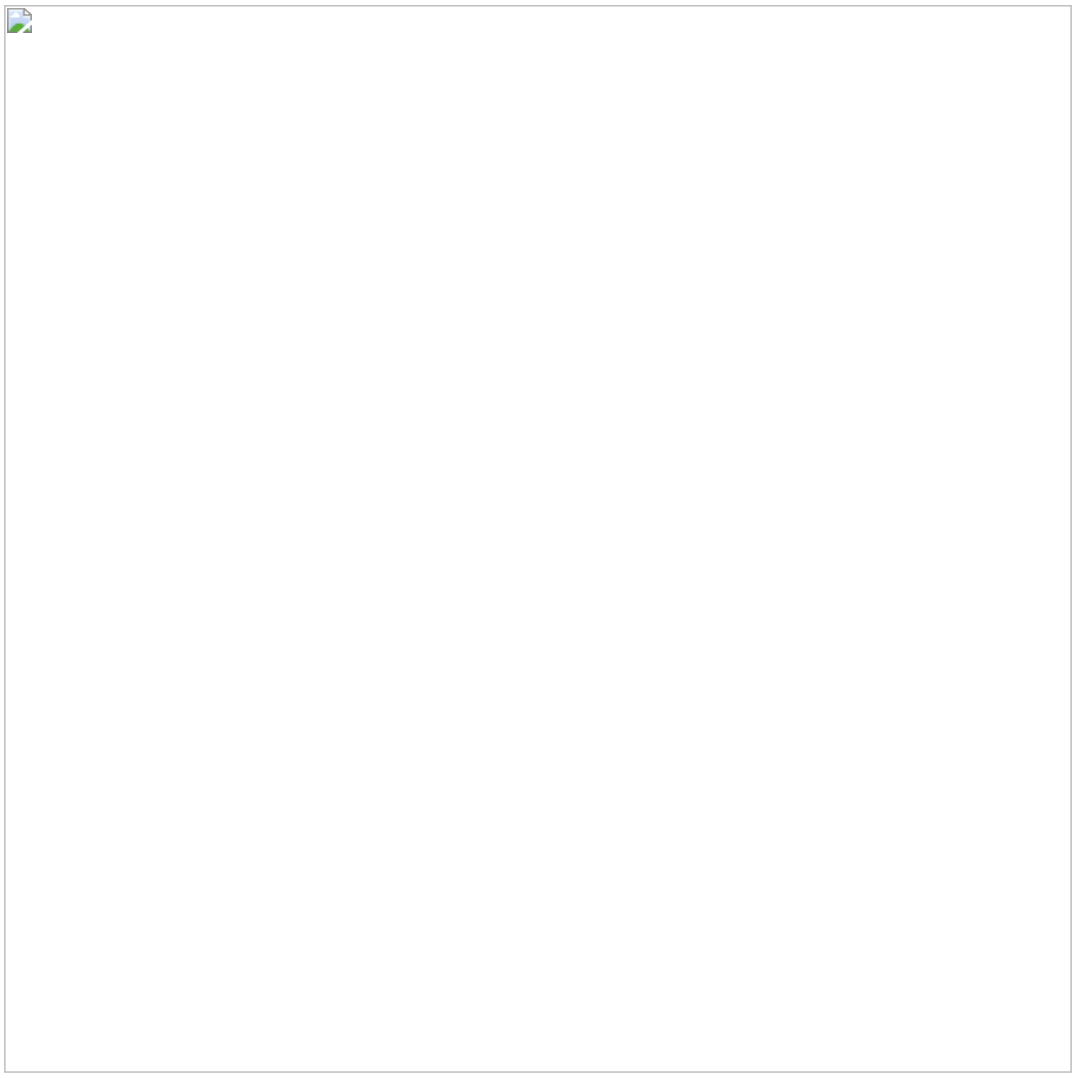
The industries affected by Suncrypt were mainly Services, Technology, and Retail, and HQ was mainly attacked by United States, Belgium, and Germany.

Suncrypt infected companies

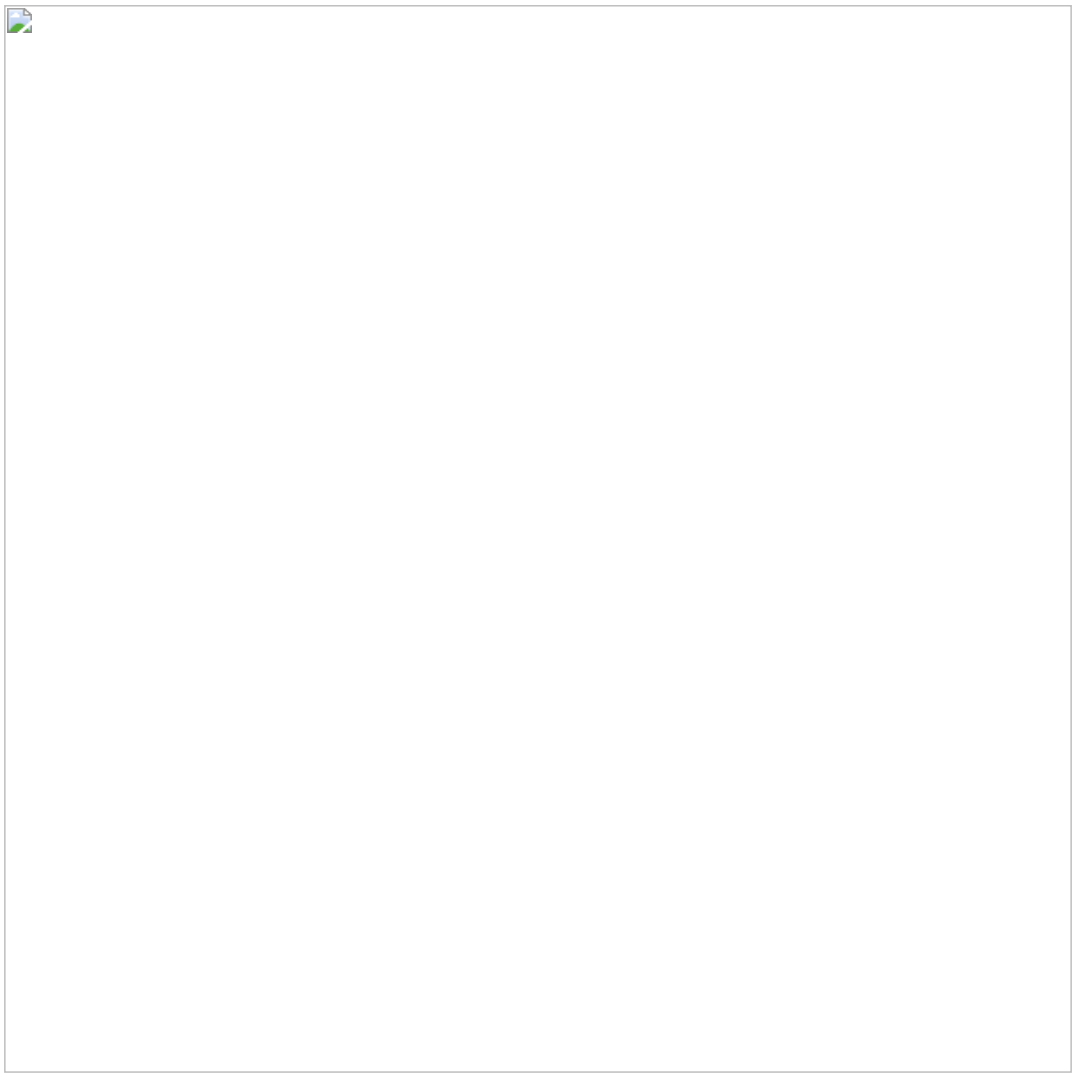


A-1. Suncrypt infected companies

- 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 :
- Via Ransom note, Suncrypt guides you through 1:1 chat page and details for negotiation



1:1 chat page with Suncrypt operator

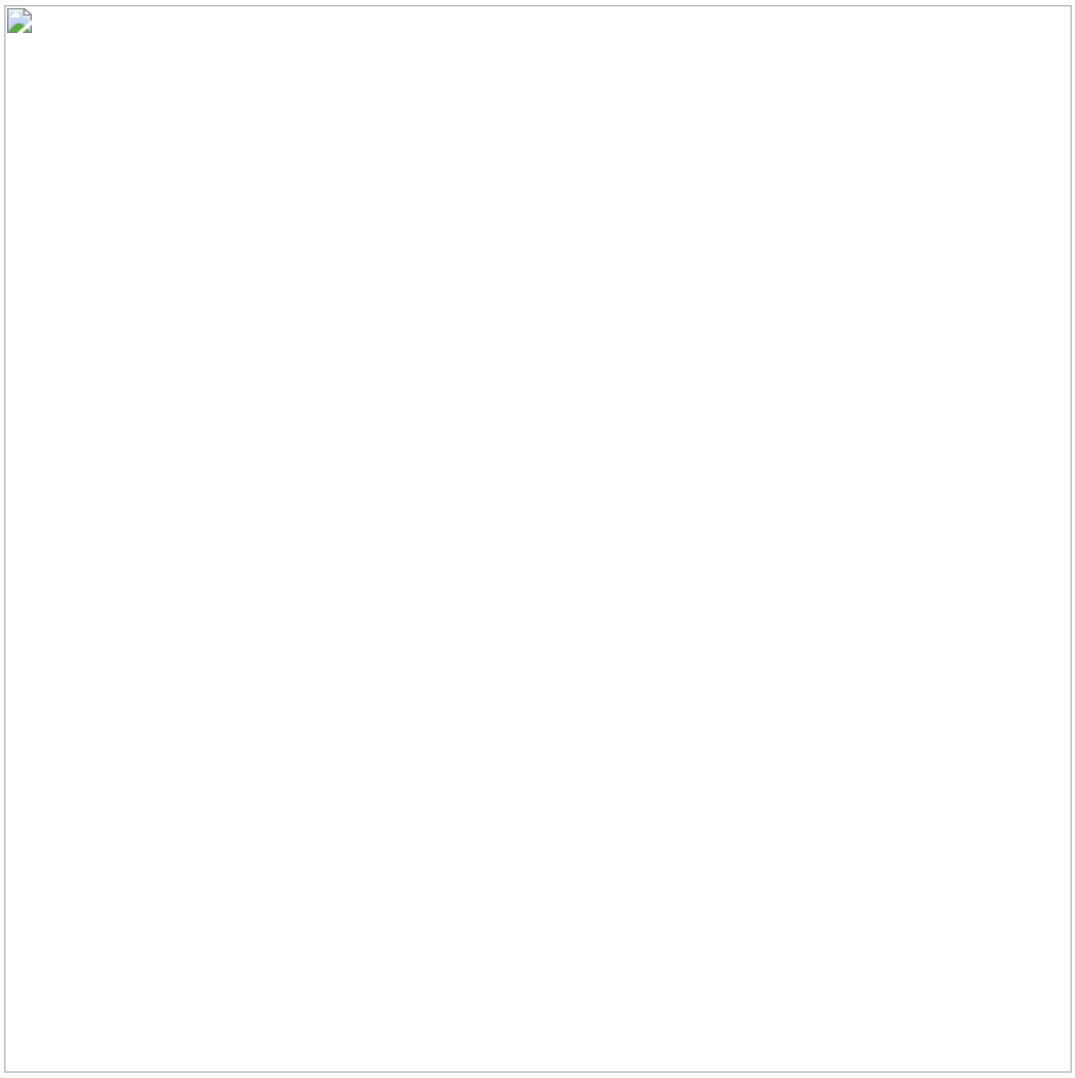


A-2. Negotiation the price of the victim company

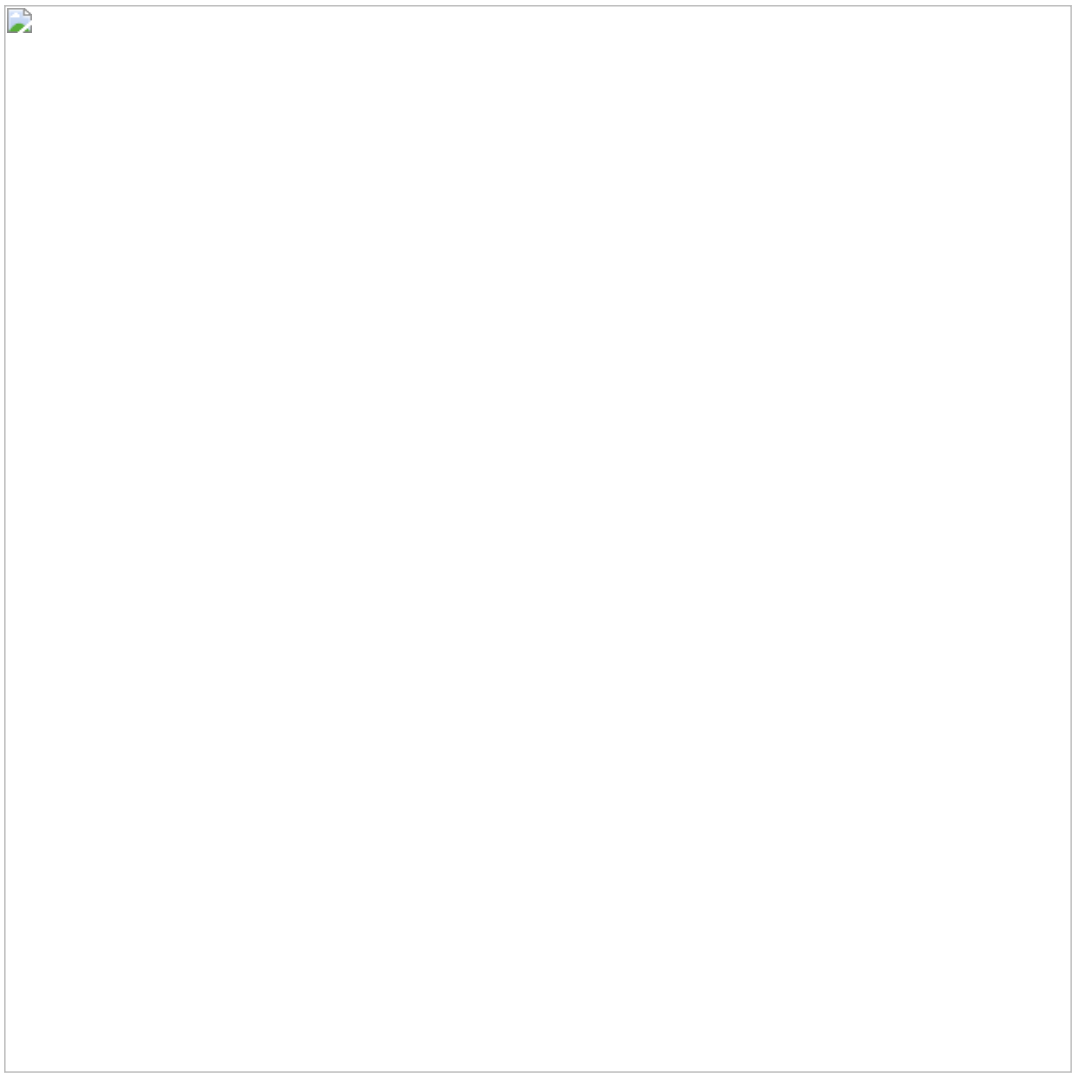
- A negotiator is involved to mediate the price between Suncrypt and the victim company.
- The negotiator offers an amount of 750,000 (USD) from Suncrypt for the following three items that the victim company can provide if paid

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

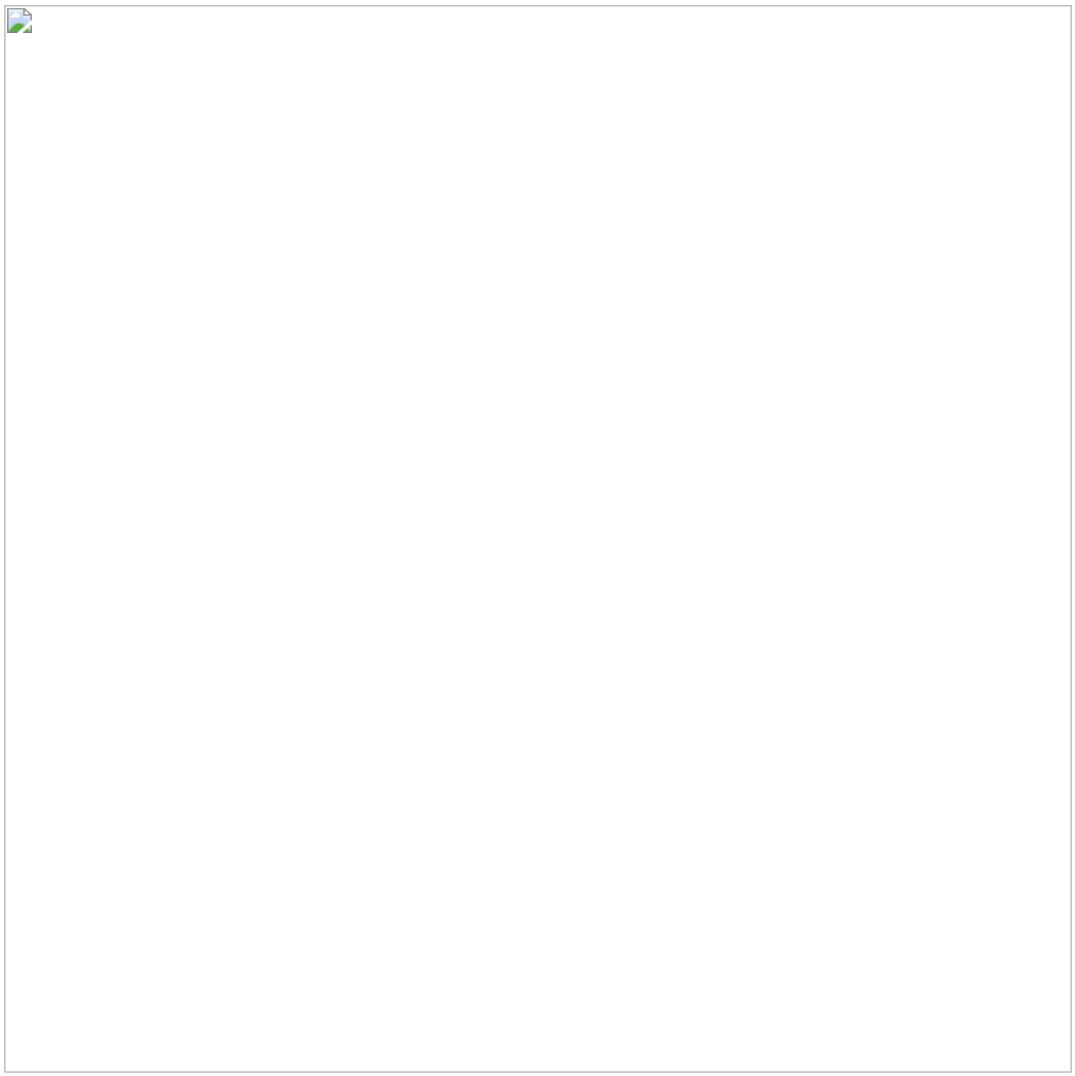
   He also mentioned that paying the amount will stop DDoS attacks on the company's website, and that the price can be lowered through fast delivery and negotiation



- 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.



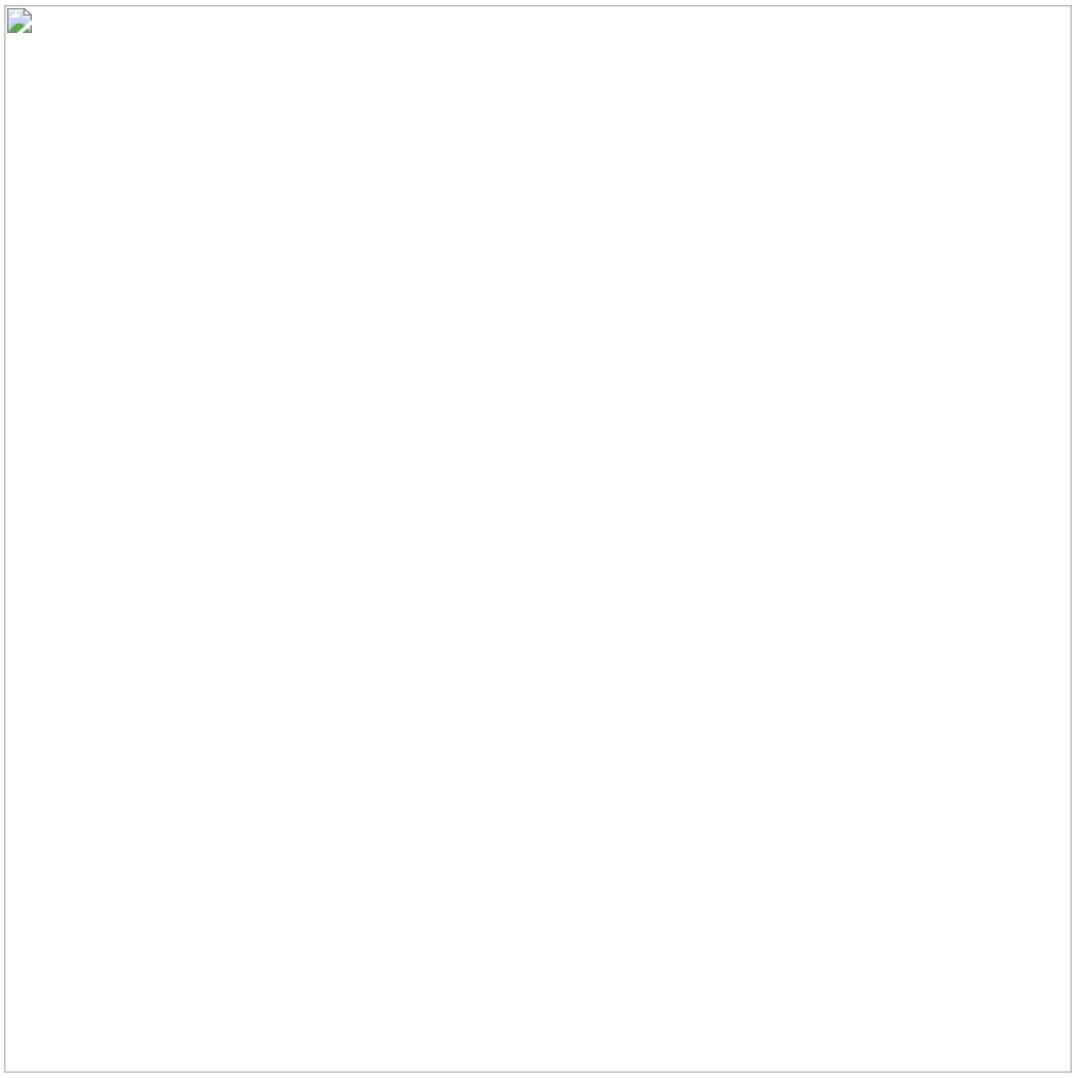
- Accordingly, Suncrypt delivered the bitcoin address and the victim company transferred about 7.04 BTC to the address.
- Payment date : 2021–06–15 05:46
- Bitcoin Address : bc1qqqj3tjv0yztrvda95paau4rwve2gkqpwqfld7v



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.

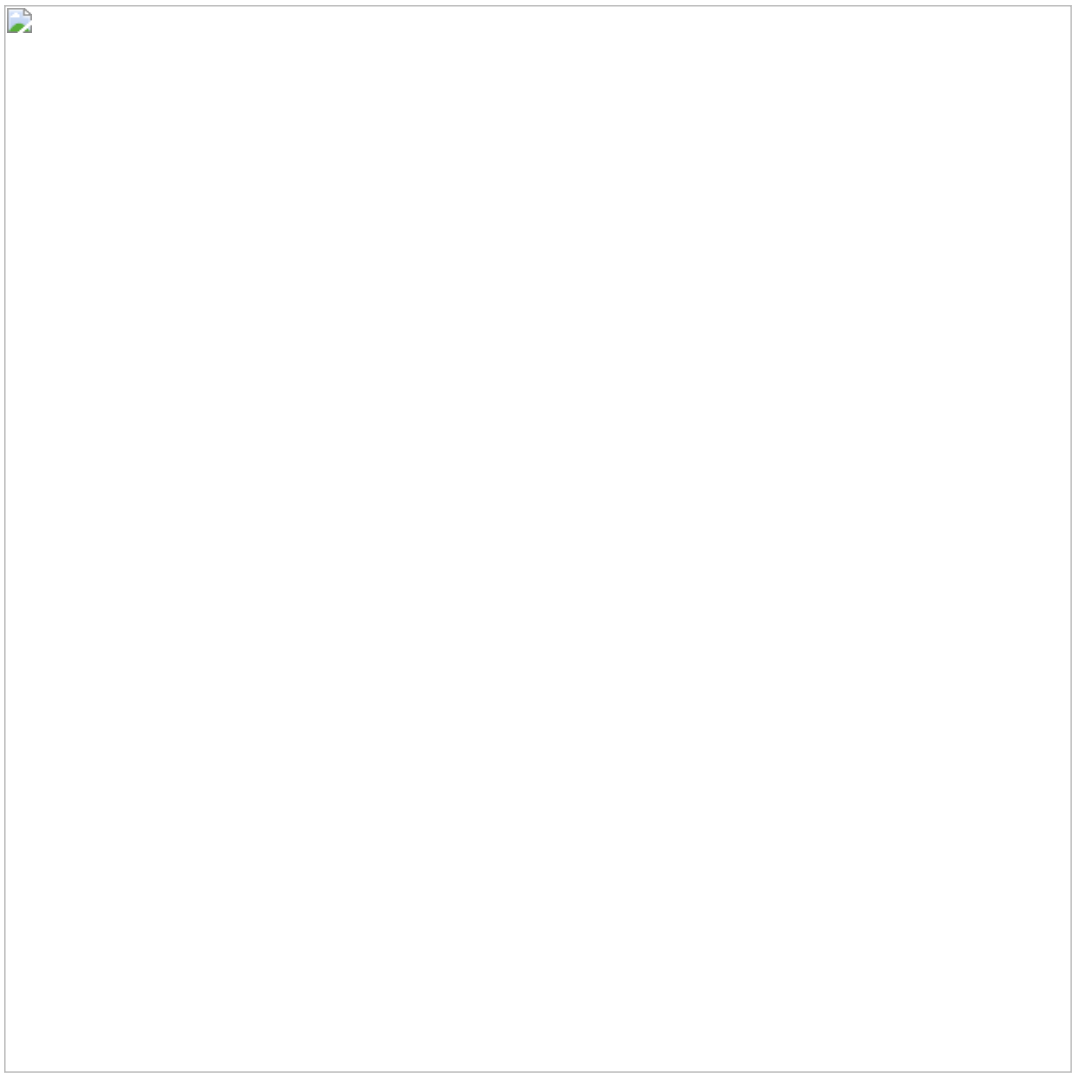
1) Decryptor

decrypt files encrypted by ransomware and detailed instructions



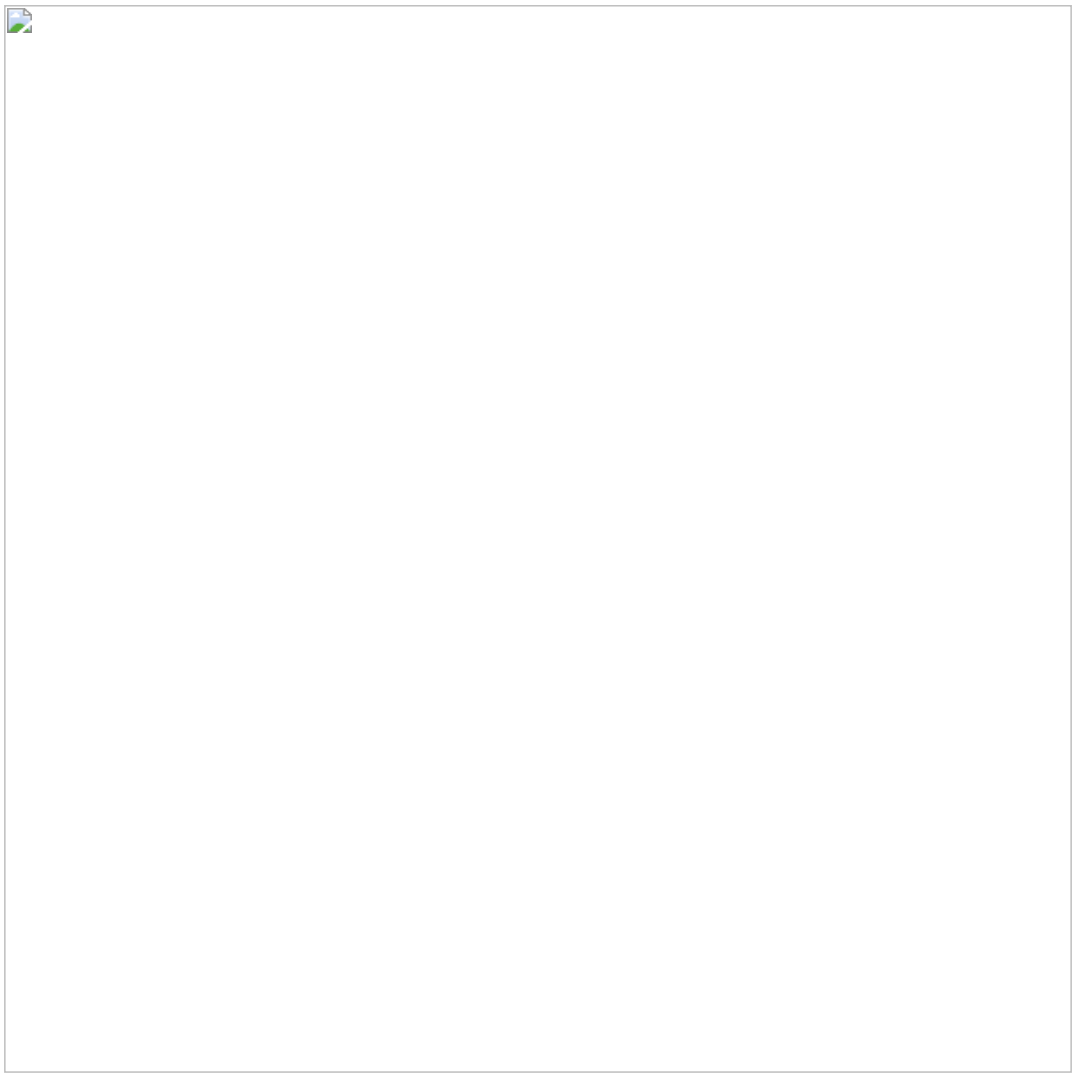
2) The erasure Log

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



3) The security report

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



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, , 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

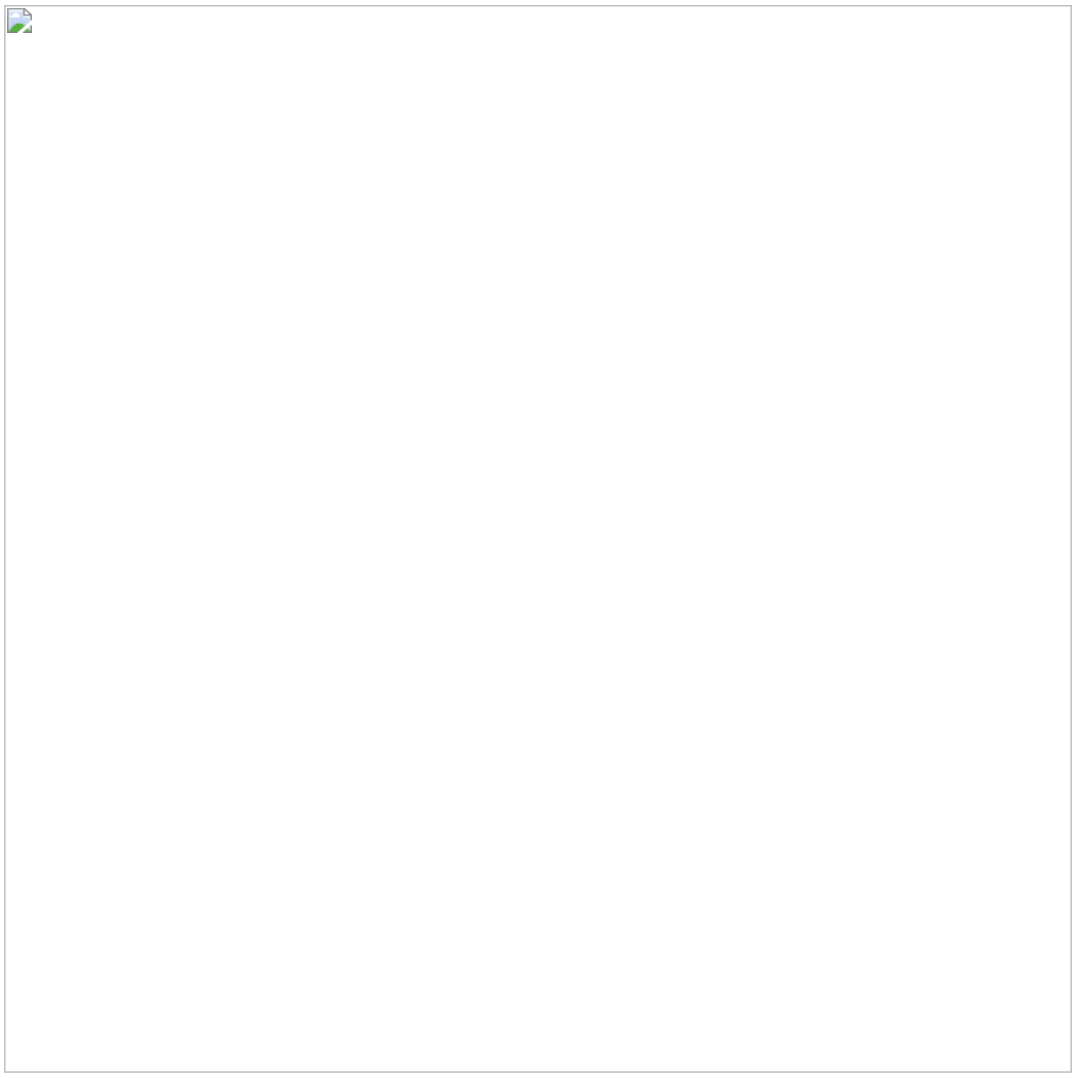
8. Also try configure 2FA (at all network pc) when you connect to remote desktop

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

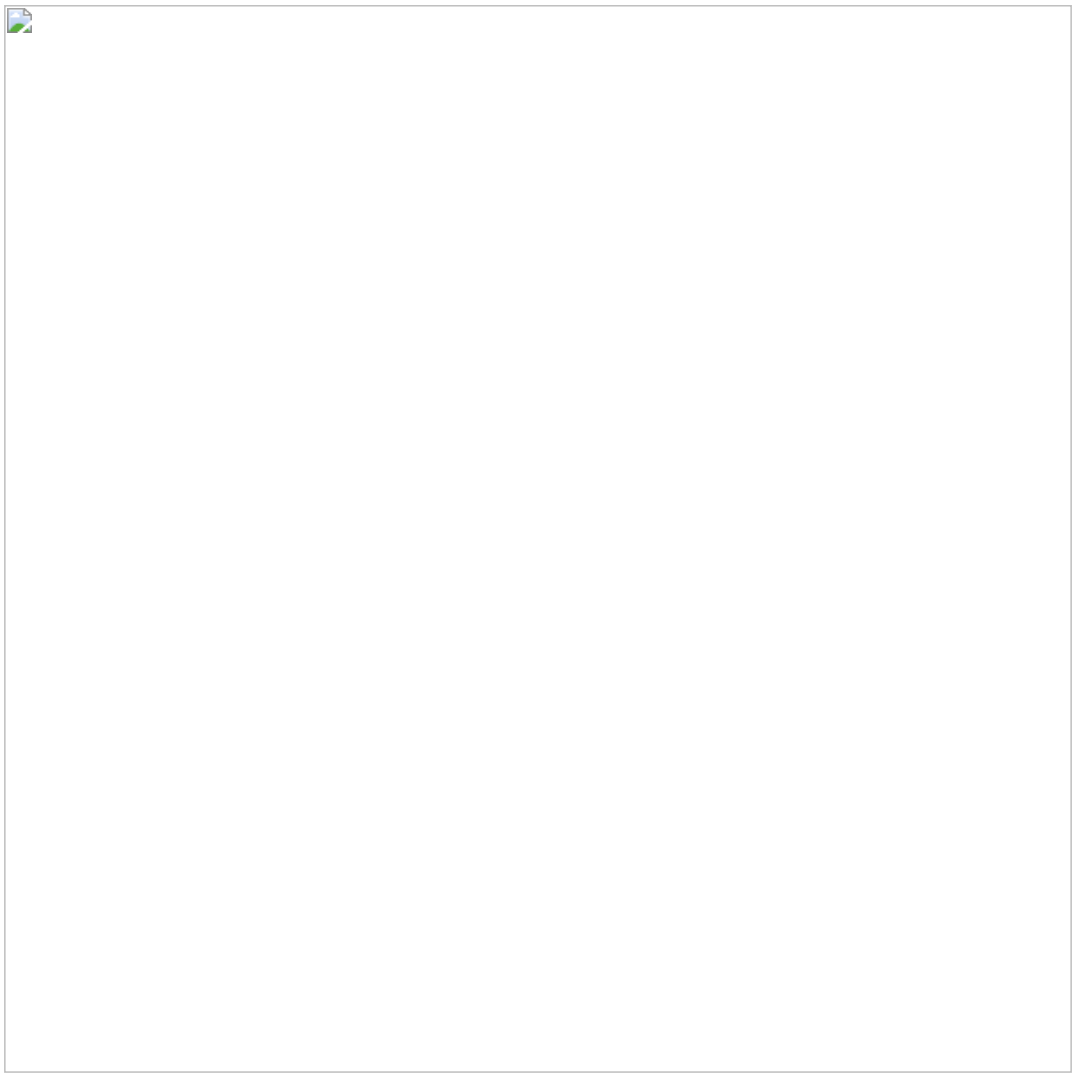
A-3. Transaction analysis

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

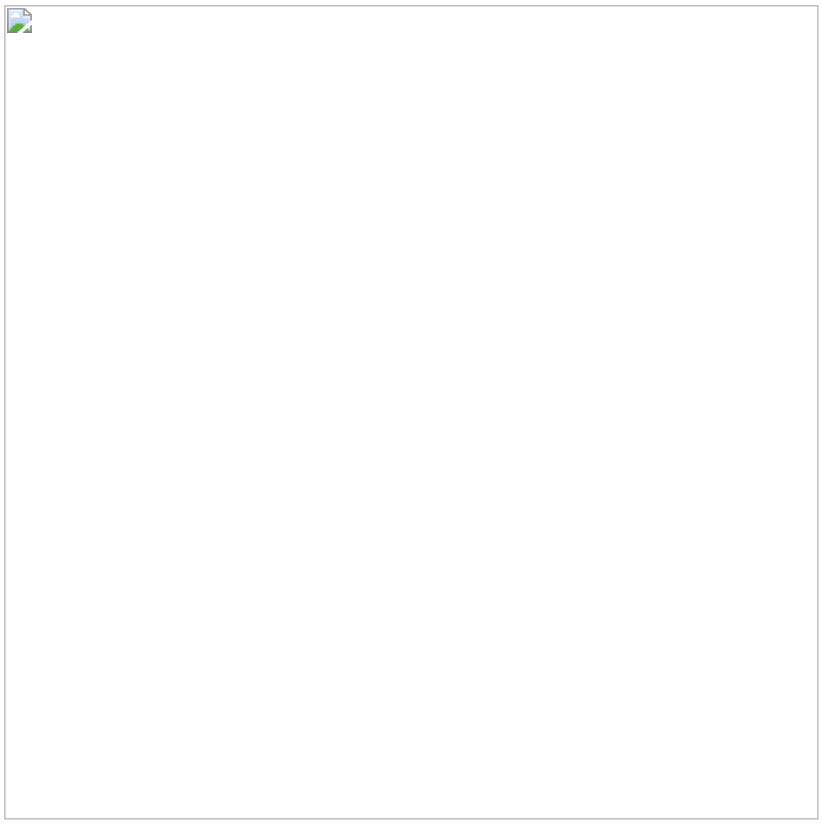


Bitcoin transaction analysis via Xarvis

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

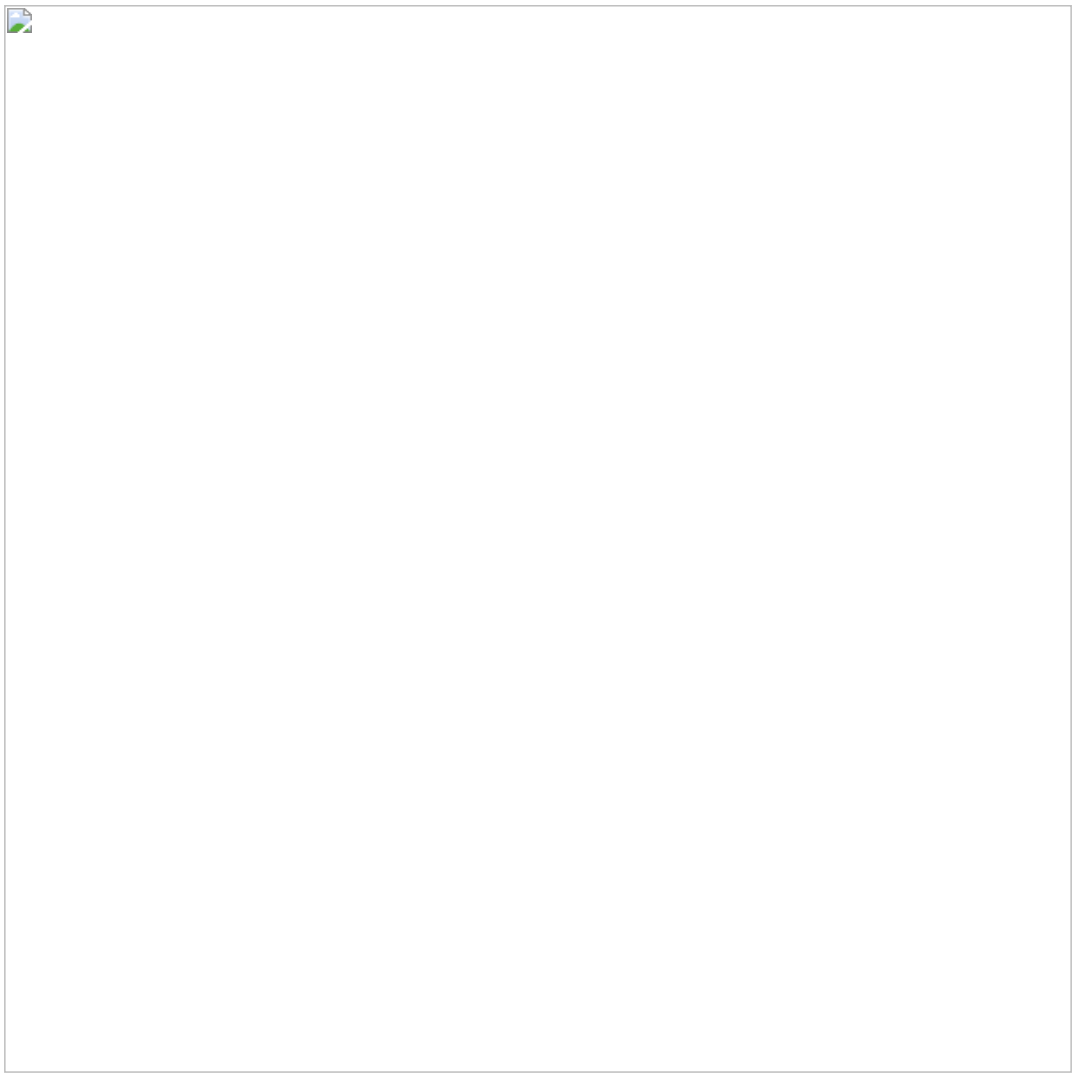


- If you look at the amount divided by performing Coin mixing, it is distributed in exactly the same amount.
- In particular, the pattern in which the same amount is divided by a combination of 0.001 BTC, 0.002 BTC, and 0.004 BTC is a typical feature of mixing performed by ChipMixer, and it is suspected 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

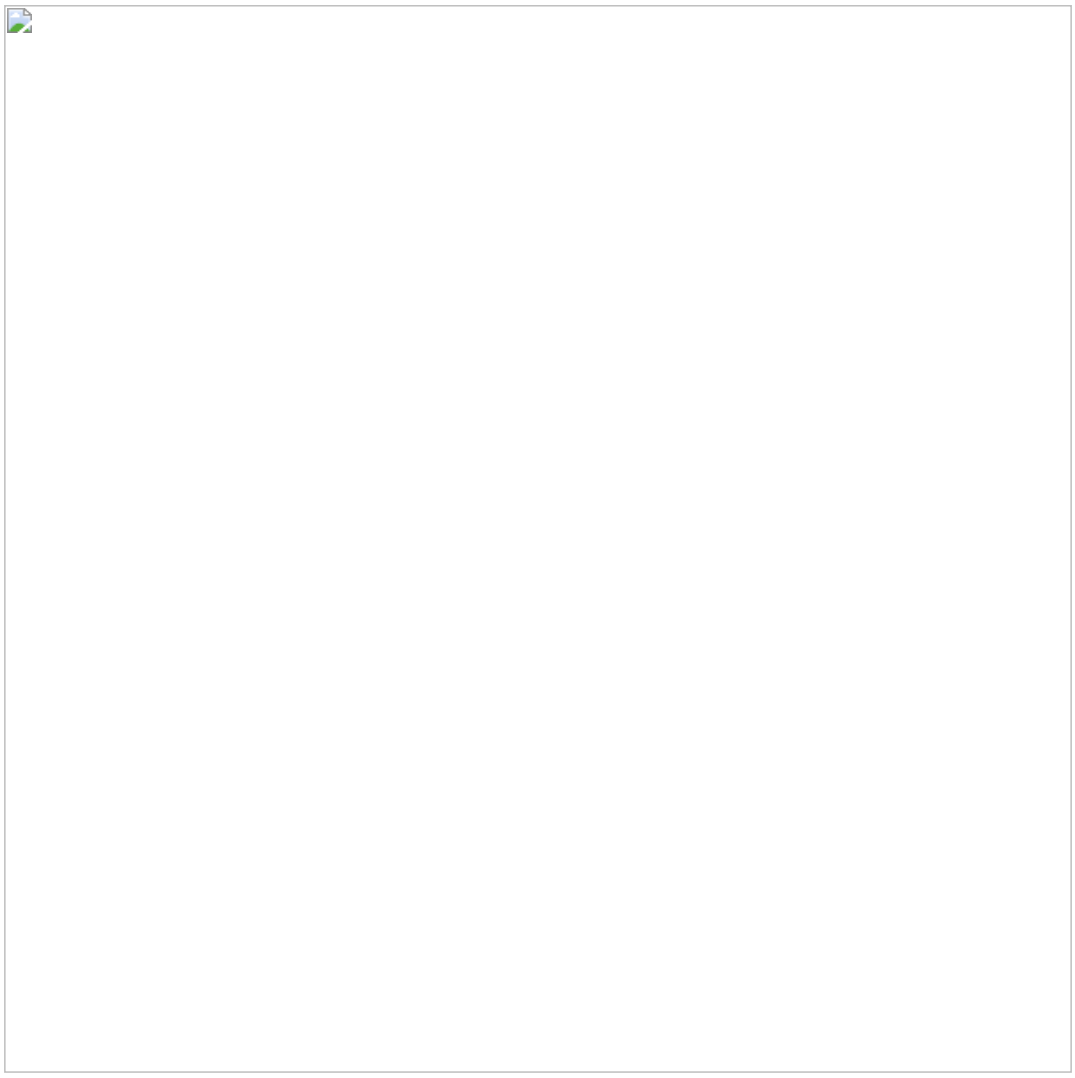


C. RAMP(Babuk/Payload.bin)

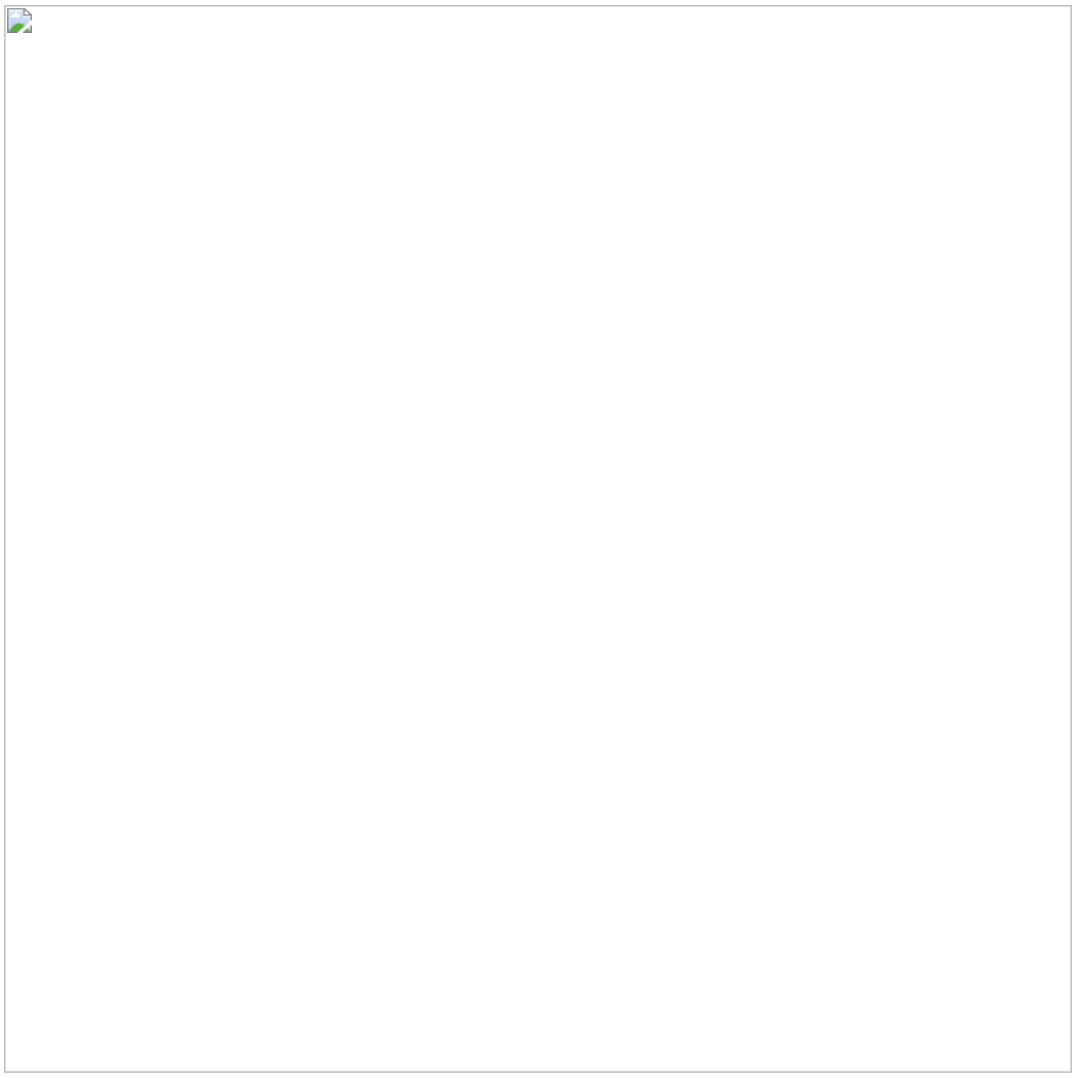
It has been changed to a membership forum, and the number of community active users and posts is gradually increasing



User status as of 2021.07.20



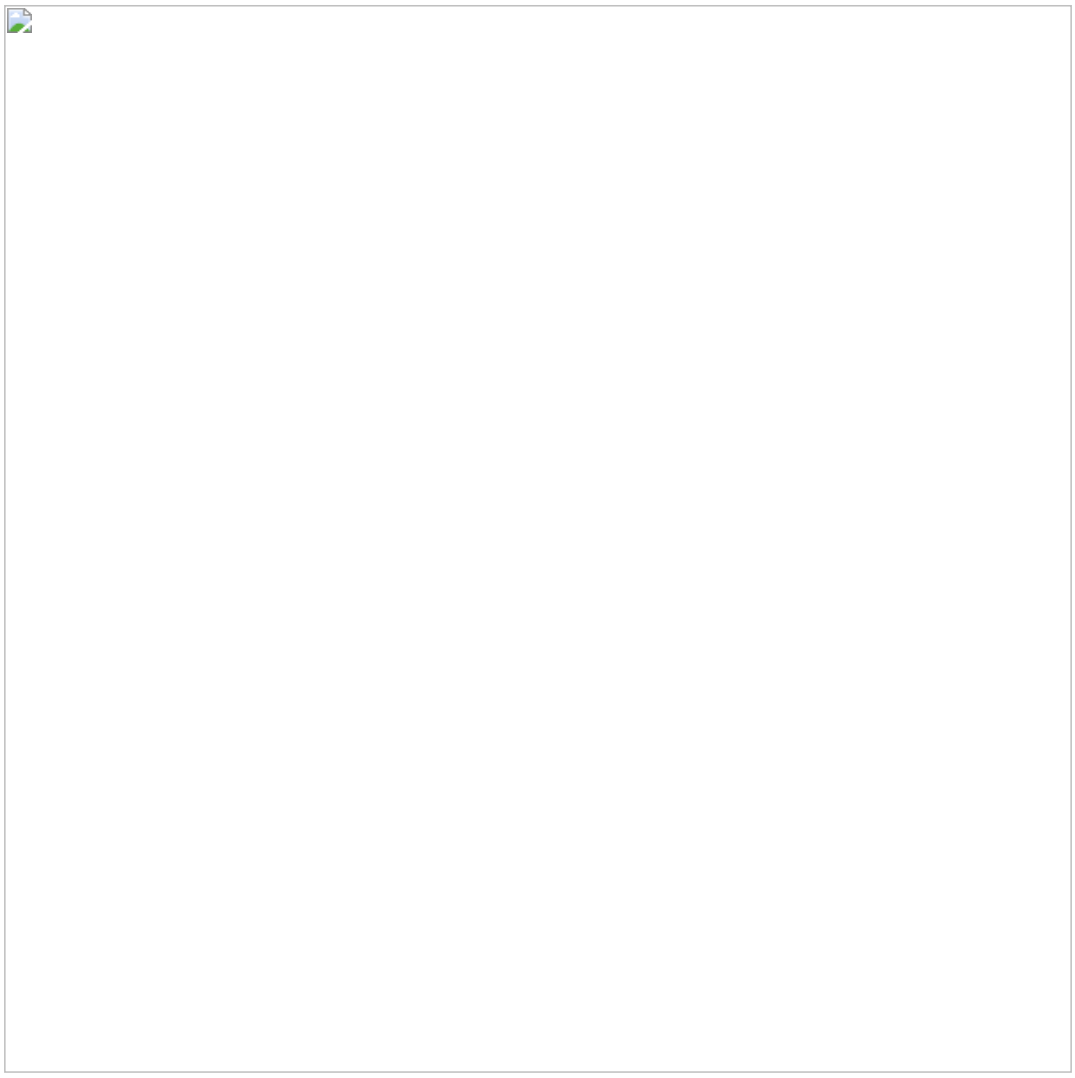
Admin Orange, Moderator 777 Users are the most active



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

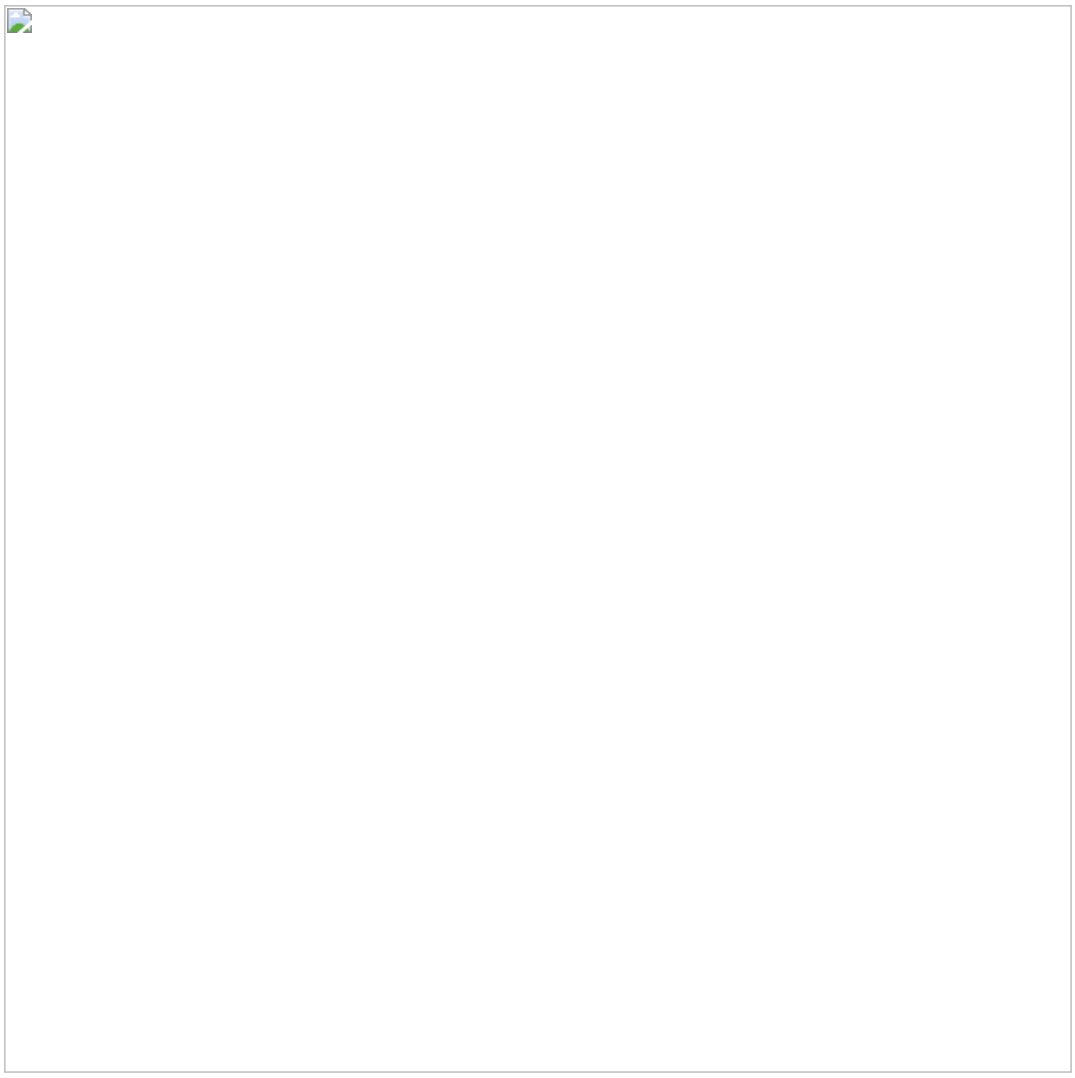
- Currently, the RAMP forum is operated for the purpose of promoting affiliate programs and sales services related to ransomware RaaS, so the credential information posted on the forum is highly likely to be misused by ransomware groups
- According to a post posted on July 15, 2021, a user has announced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



- 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



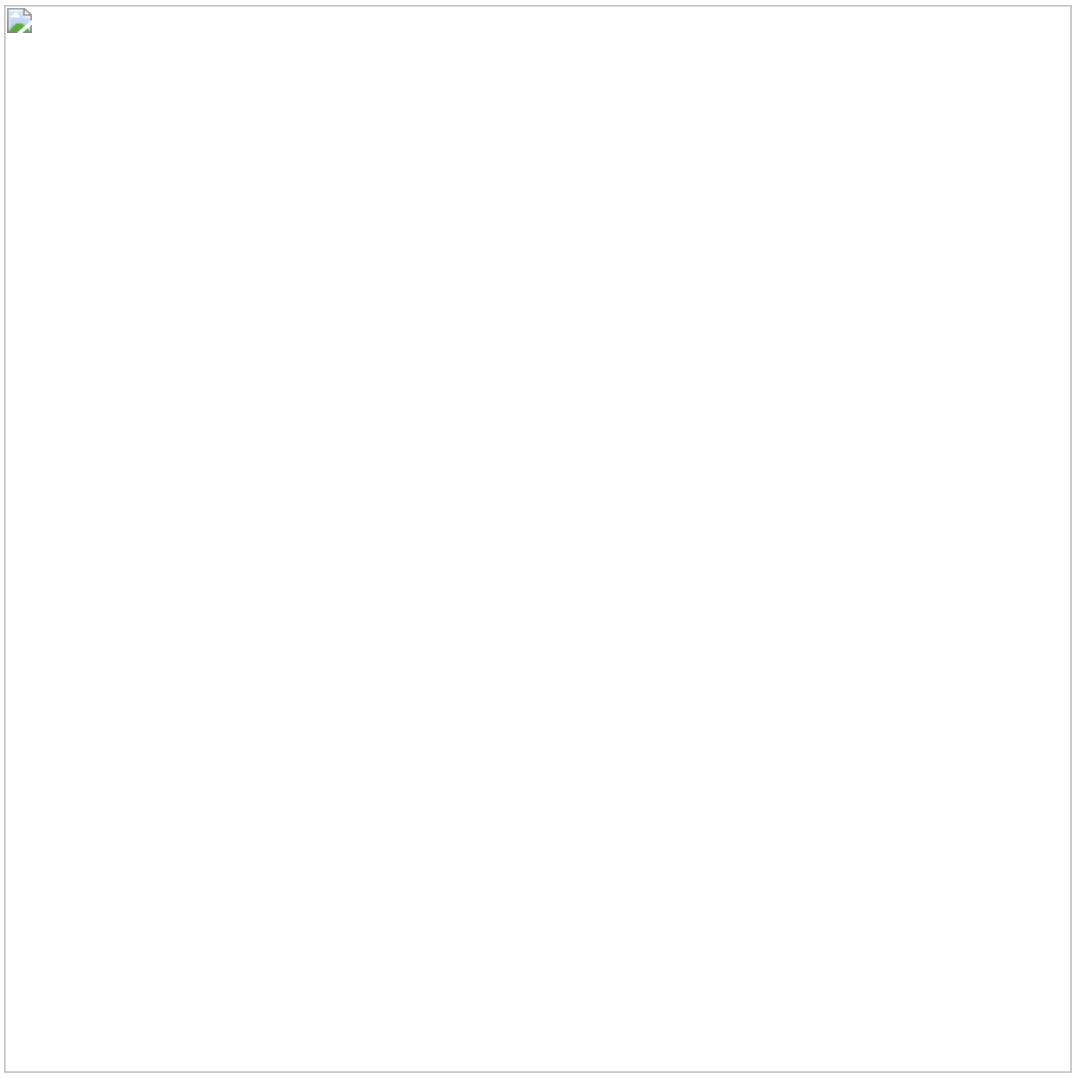
- Mimikatz: A tool that can steal Windows account passwords
- Netscan : port scanning tool
- Dsquery: Active Directory query tool (collect user accounts, domain trusts, permission information)
- Psexec : Used to download or upload files via network share.
- Babuk Builder: A tool to create Babuk ransomware

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.

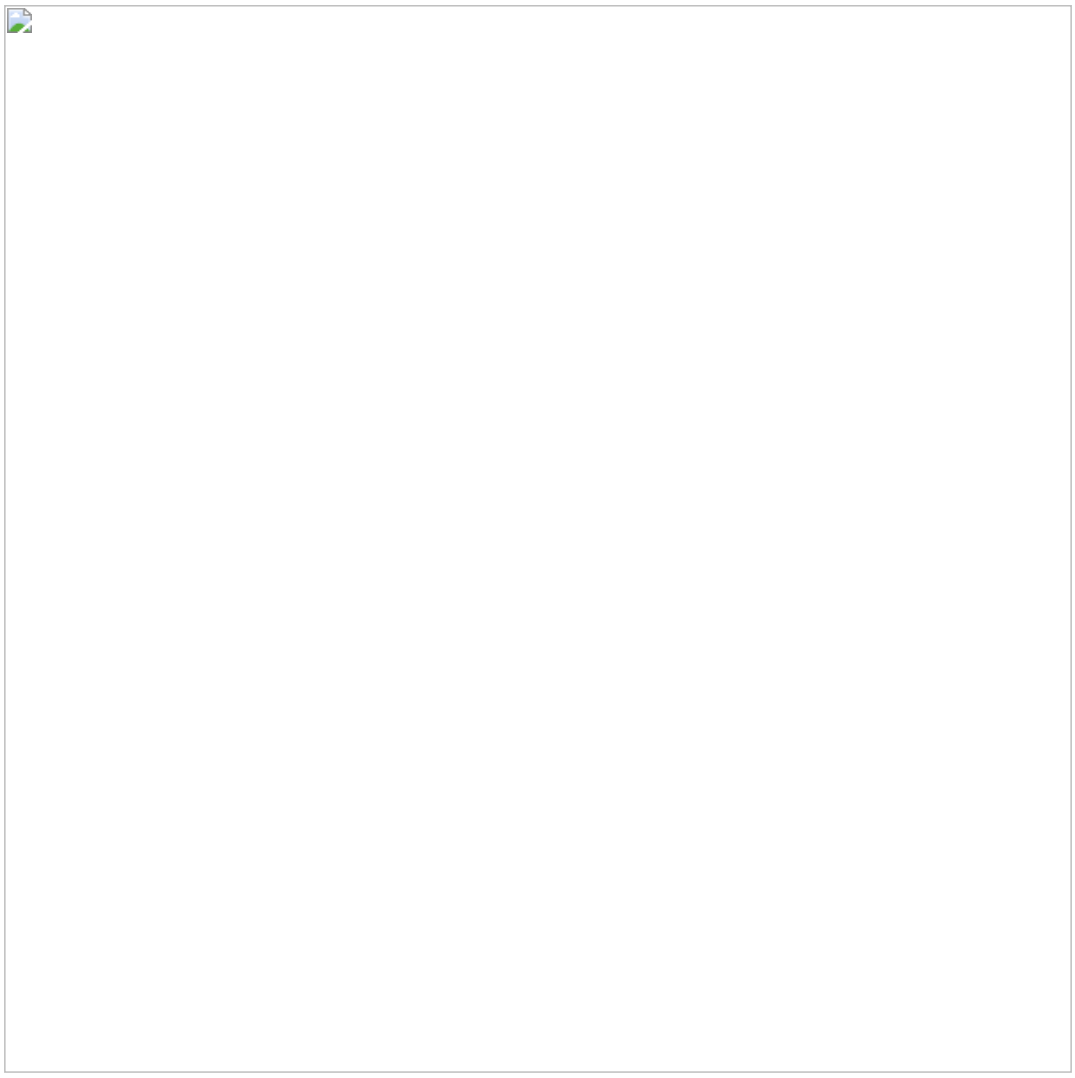
TOP 5 targeted industrial sectors & countries

The post of LockBit promoting LockBit affiliate program

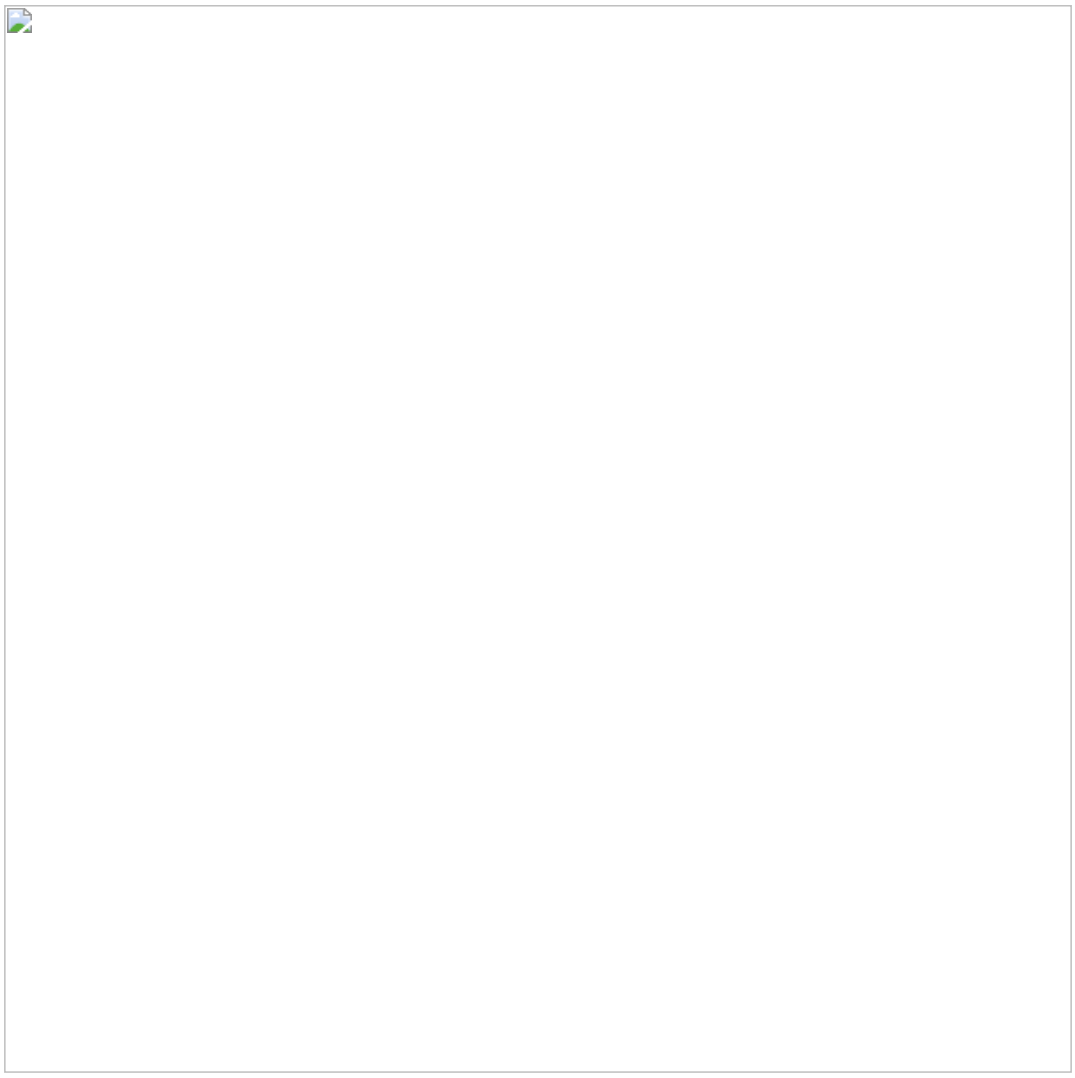


3. Posts related to Underground Forum @Dark Web

A. Banned @teamkelvinsecteam



- 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



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.