

Case Analysis of Suncrypt Ransomware Negotiation and Bitcoin Transaction

 medium.com/s2wlab/case-analysis-of-suncrypt-ransomware-negotiation-and-bitcoin-transaction-43a2194ac0bc

S2W

September 9, 2021



S2W

Sep 9, 2021

.

5 min read

Hotsauce | S2W TALON

Executive Summary

- In May 2021. The United state's company was infected by the Suncrypt ransomware, and after a long negotiation of about 3 weeks, the victim paid the ransom with Bitcoin, and Suncrypt finally deleted the leaked data and informed security report, and the negotiations were finished.
- As a result of tracking the Bitcoin paid by the victim, it was sent to the Binance, OKEX, Huobi exchange and confirmed the circumstances of ChipMixer Mixing.

Detailed analysis

1. About Suncrypt ransomware

- Suncrypt is a Ransomware as a Service (RaaS) that uses a closed affiliate program on the dark web and first appeared in October 2019.
- Suncrypt says "The Suncrypt group is a huge fan of a Win-Win style of negotiations and the minimal damage policy" and they provide a security report when the negotiation is complete, emphasizing that they are a reliable "business" rather than a ransomware "hack".

2. Analysis of Suncrypt Ransomware Negotiation

- Suncrypt ransomware left a HTML type ransom note on the infected PC with information on key points and how to access the 1:1 negotiation page.

- You can start negotiating with Suncrypt by accessing the 1:1 negotiation page guided by the ransom note.

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 what we promised.

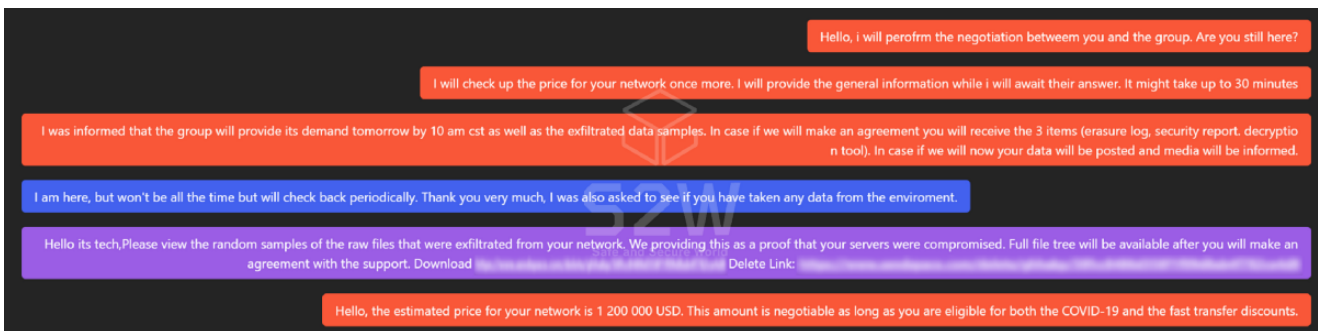
Turning this issue to a bug bounty will save your private information, reputation and will allow you to use the security report and avoid this kind of situations in future.

Victim company

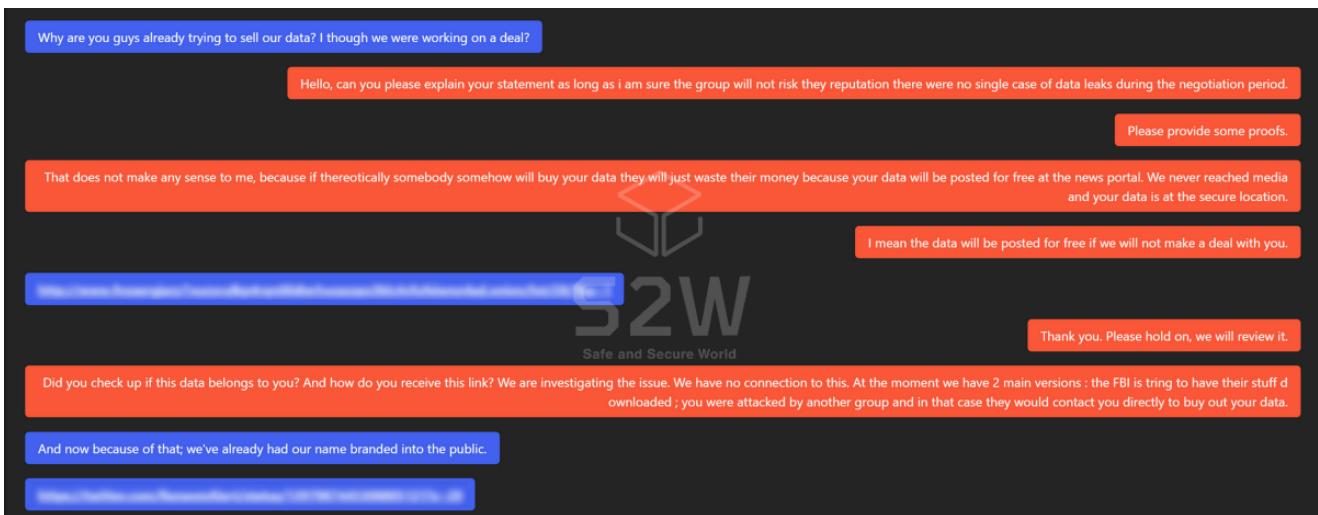
- In May 2021, an American company D was infected with the Suncrypt ransomware.
- On the 1:1 negotiation page, Suncrypt said that after 72 hours the exfiltrated data will be posted at our news website and DDoS attack will be stopped only after progress is made in the negotiation.
- Suncrypt requested 1,200,000 USD as a payment amount, presenting sample files and listings as proof and guaranteeing to provide the following three items upon completion of the negotiation.

- 1.
- 2.
- 3.

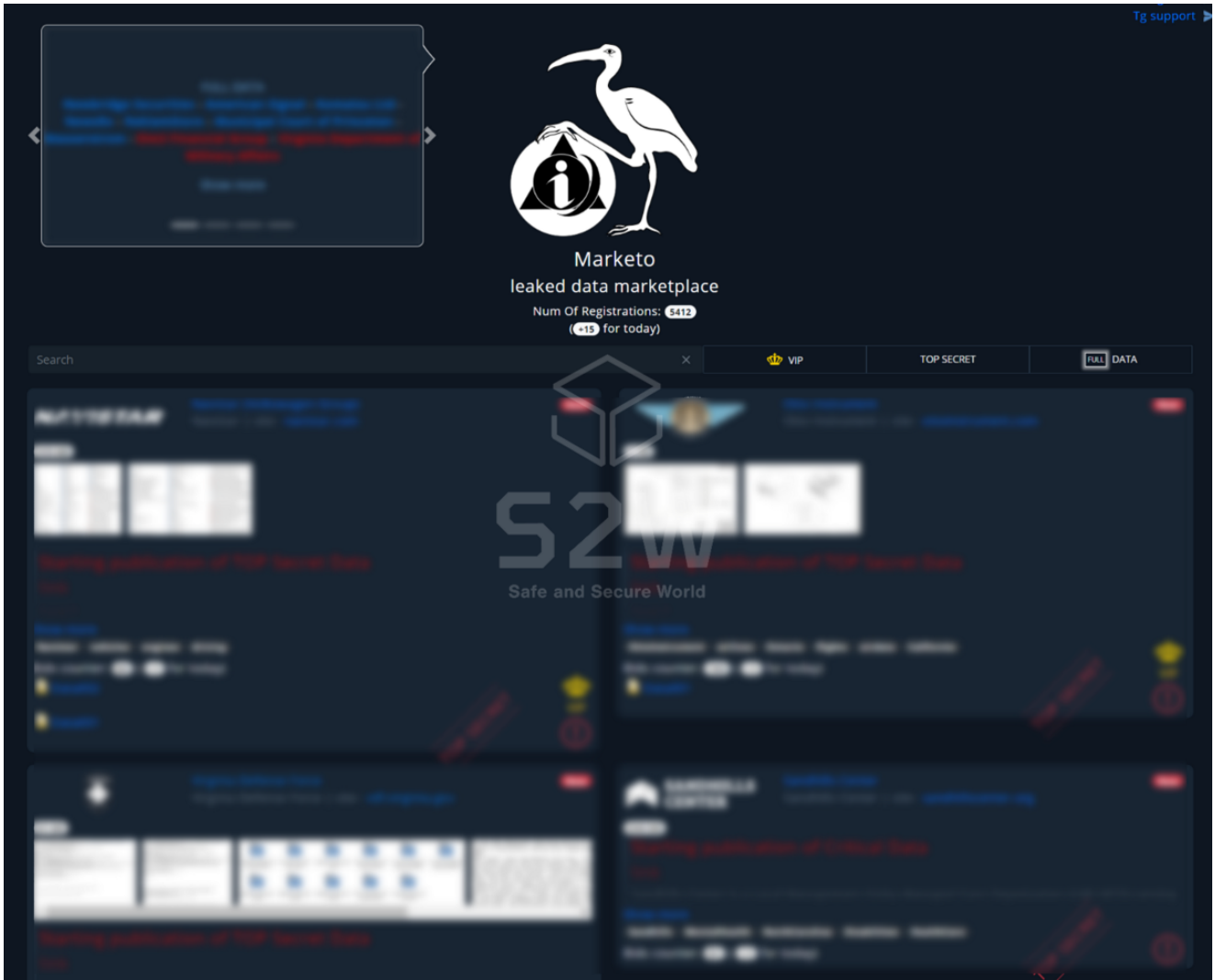
Suncrypt seems to have separate roles of negotiator and technician, as a person who appears to be a technician/developer who calls himself Tech (purple chat) participates in the negotiation.



- During the negotiations, the victim company gave a link to a posted on Marketo / Twitter and protested why they were already selling our data.
- Suncrypt said and denied it had nothing to do with us.



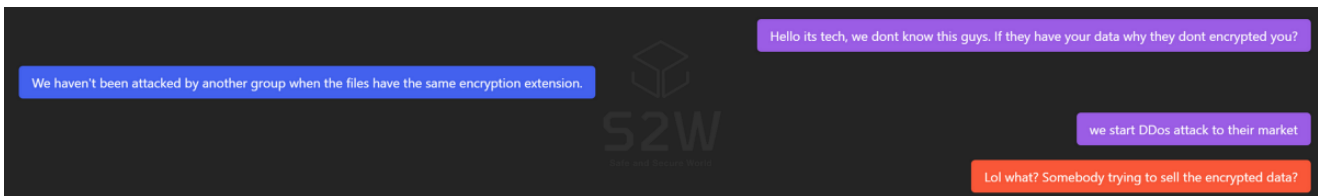
- Marketo is a marketplace of stolen data, first appeared in April 2021.
- Leaked data is selling publicly by bidding auctions.



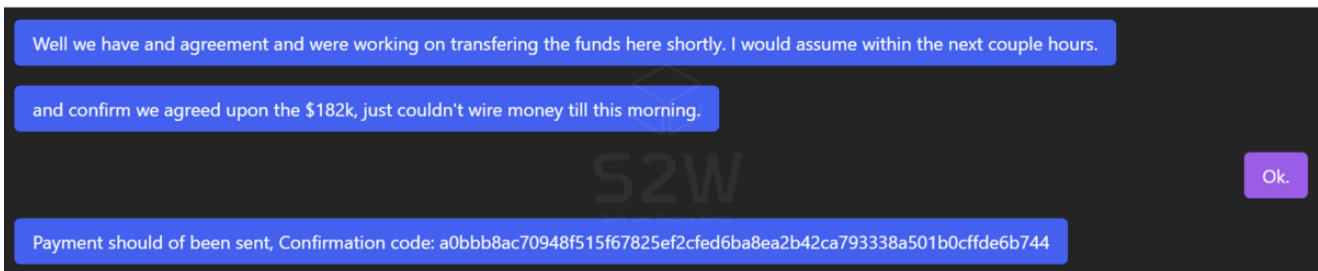
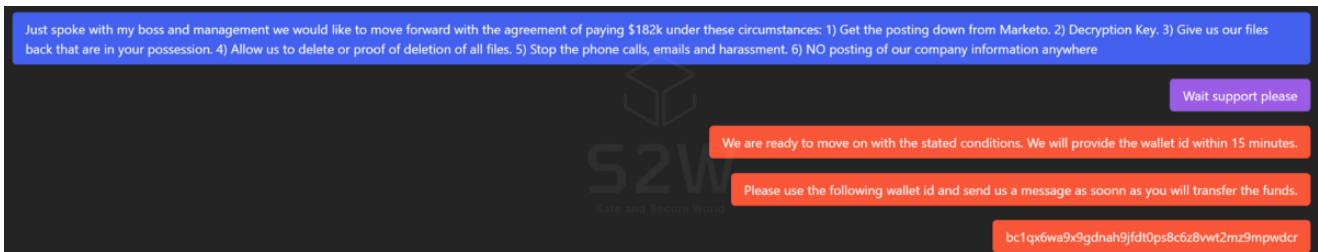
Selling leak data of victim companies uploaded to Marketo.



- Since the victim company does not have files encrypted with extensions other than Suncrypt, it seems that Marketo only stole data without separate encryption, and it is possible that leaked by Suncrypt and Marketo both.
- Suncrypt's Tech said that they start DDoS attack to Marketo.

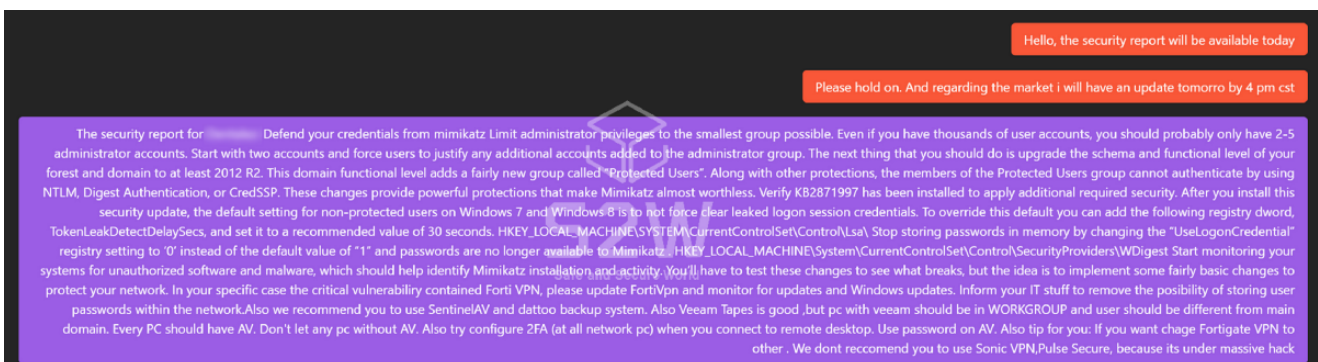


After several price negotiations, the victim company paid 182,000 USD, demanding even to delete the post on Marketo.



Suncrypt closes the negotiation by providing erasure log and security report after confirming Bitcoin deposit.

Security Report — same contents are provided in case of other victim company that were infected at around the same time




— erasure logs to prove that Suncrypt has deleted all files stolen from the victim company.


```
1 Using /dev/urandom for random input.
2 Wipe mode is secure (38 special passes)
3 Wiping
4 Wiping
5 Wiping
6 Wiping
7 Wiping
8 Wiping
9 Wiping
10 Wiping
11 Wiping
12 Wiping
13 Wiping
14 Wiping
15 Wiping
16 Wiping
17 Wiping
18 Wiping
19 Wiping
20 Wiping
21 Wiping
22 Wiping
23 Wiping
24 Wiping
25 Wiping
26 Wiping
27 Wiping
28 Wiping
29 Wiping
30 Wiping
```

Suncrypt said that we are trying to bring down the fake post or getting a proof that data is fake, but leak data posted on Marketo have not yet been deleted and are still on selling.

Hello, the actual data not yet discovered to be deleted. At the moment we are seeing different ways of marketo support to explain the origins of unexistent data. Please wait for the progress. At the moment we see that your data is secured and we are trying to bring down the fake post or getting a proof that data is fake. We could not buy out your data its just not there.

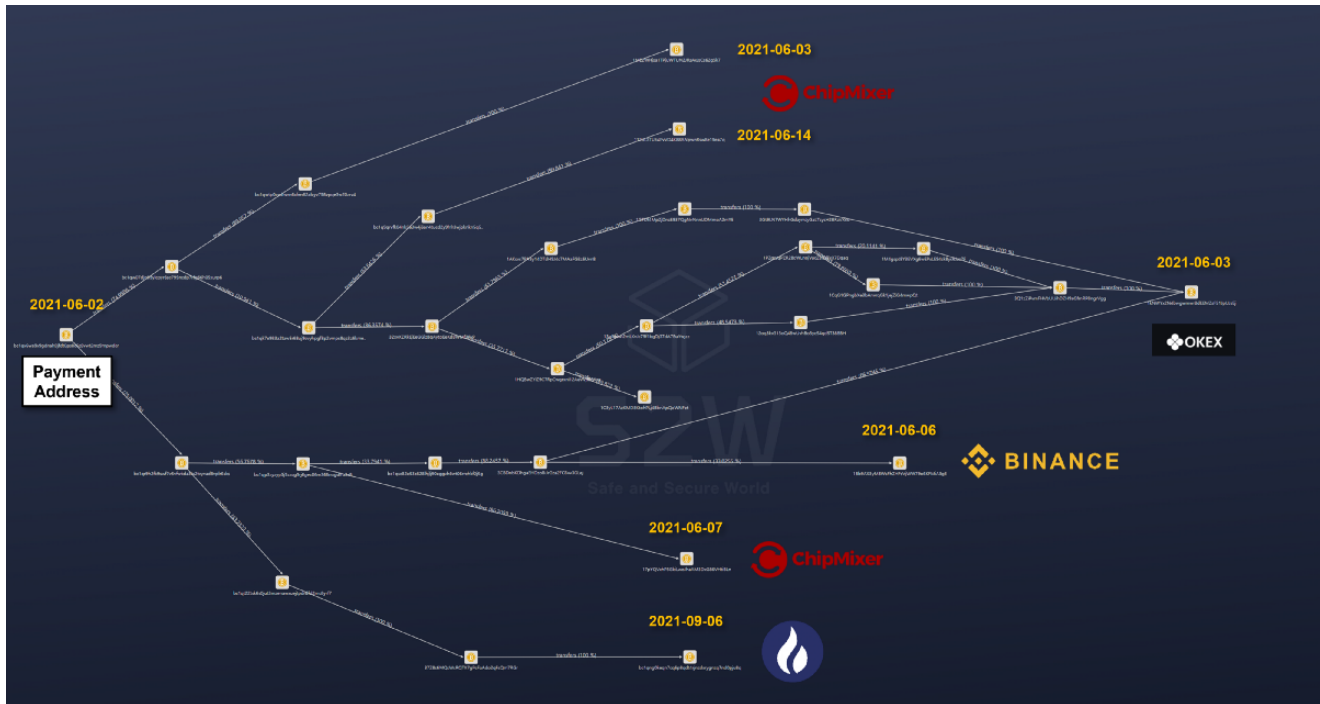
Anything new?

 Hello, thank you for your message. No available specialists at the moment. Please check back during the business hours: 10 AM to 6 PM CST.

Still looking to get the Marketo listing taken down.

3. Analysis of payment address

- Tracking the bitcoins paid by the victim company
- Payment address : bc1qx6wa9x9gdnah9jfdt0ps8c6z8vwt2mz9mpwdcr
- Amounts : 5.03350949 BTC
- Transaction date : 2021-06-02
- The 5.03350949 BTC paid by the victim company was divided into several branches and each performed ChipMixer Mixing, transferred to Binance, OKEX, Huobi wallet



3.1 Money Laundering with ChipMixer Mixing

After several addresses, approximately 4 BTC was laundered through ChipMixer Mixing

Bitcoin Address

- 1ME2WHjsa1TPjuWTUN2JRsaXJsCs62gSk7
- 112oLSTUE4PvVD4K88ANpwnRsw8e19ea7q
- 17pYQVxhPSGkiLwoJhaAM3DxG86VHtiBLn

3.2 Transactions to Exchange wallet

After several addresses, approximately 1 BTC was withdrawn to Binance, OKEX, Huobi exchange

Bitcoin Address

- 1Bb9AX3yM8WsFhZHFsvjWW79o6KFMiA3gE
- 3CBDnbKdhgaEHDzoBiJrGza2FC6vv3GLEj
- 37Z8s6MQsWsRQTX7gPcFaAdo2qFsQm7RGr

Conclusion

- , the Suncrypt ransomware mainly uses ChipMixer for bitcoin laundering
- Judging from the negotiation chat content, suncrypt seems to be divided into Ransomware operator, Negotiation manager, Tech manager, etc.

