Prometheus x Spook: Prometheus ransomware rebranded Spook ransomware.

medium.com/s2wlab/prometheus-x-spook-prometheus-ransomware-rebranded-spook-ransomware-6f93bd8ab5dd

S2W October 5, 2021

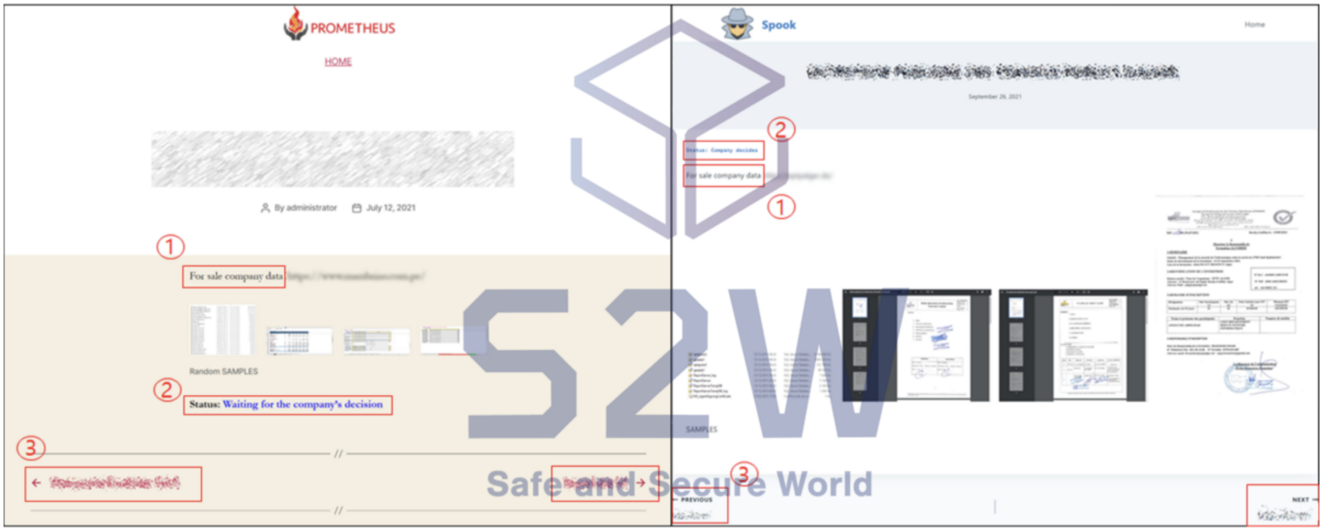
S2W

Oct 5, 2021

·

3 min read

S2W TALON



For sale company data

Status: Waiting for the company's decision

Status: Company decides

For sale company data

Compared the victim page between Prometheus x Spook

Executive Summary

- Spook ransomware started on September 26th, 2021.
- The double extortion site of Spook ransomware is similar to the double extortion site of Prometheus ransomware.
- Spook ransomware is very similar to Prometheus ransomware with ransom notes and websites. Hence Prometheus ransomware was rebranded to Spook ransomware and still using Thanos Builder.

Detailed analysis

1. Prometheus ransomware was rebranded to Spook ransomware.

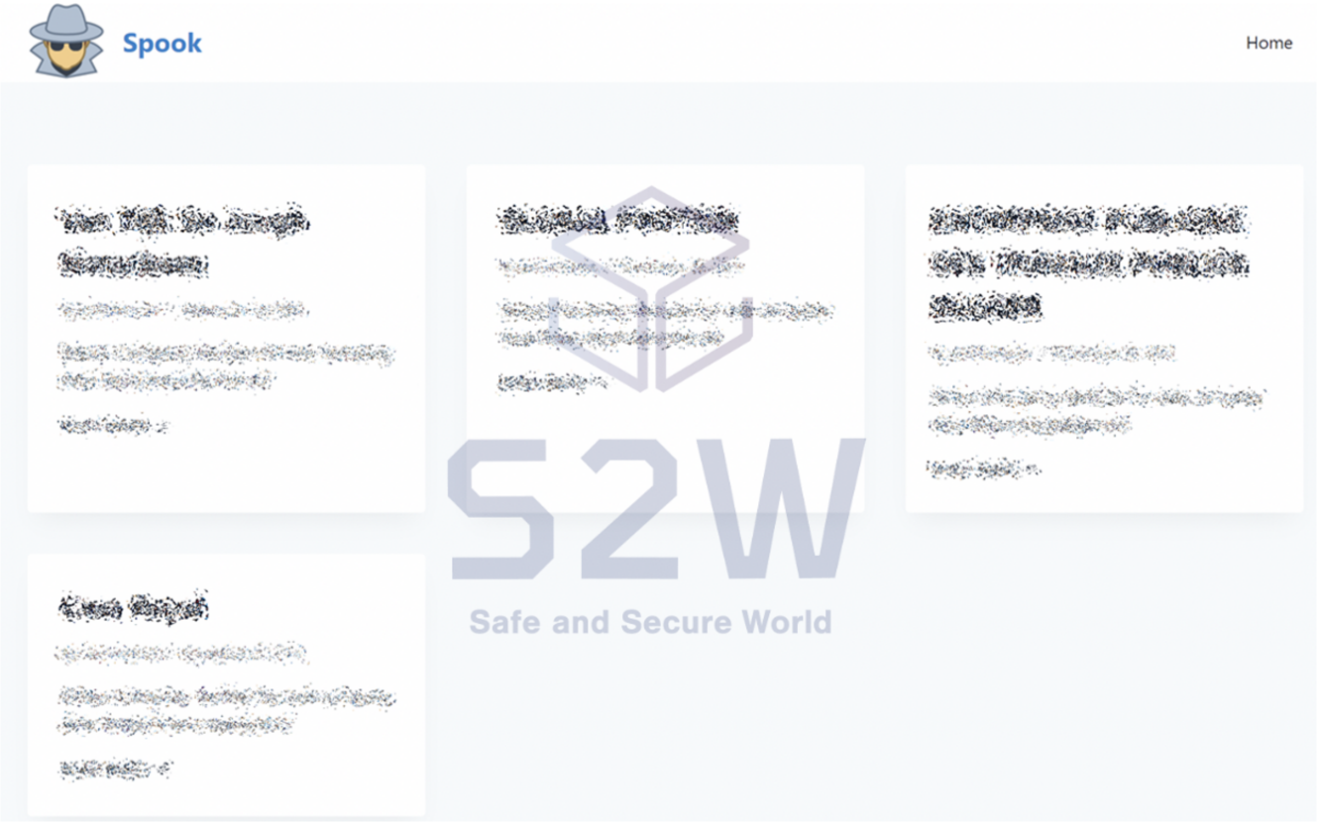
1–1. Prometheus ransomware was last updated on July 13th, 2021.

- The double extortion site operated by Prometheus last updated the information of infected victim companies on July 13th, 2021.
-

The double extortion site operated by Prometheus ransomware

1–2. Spook ransomware started on September 26th, 2021.

Spook ransomware published the information of infected victim companies starts on September 26th, 2021.



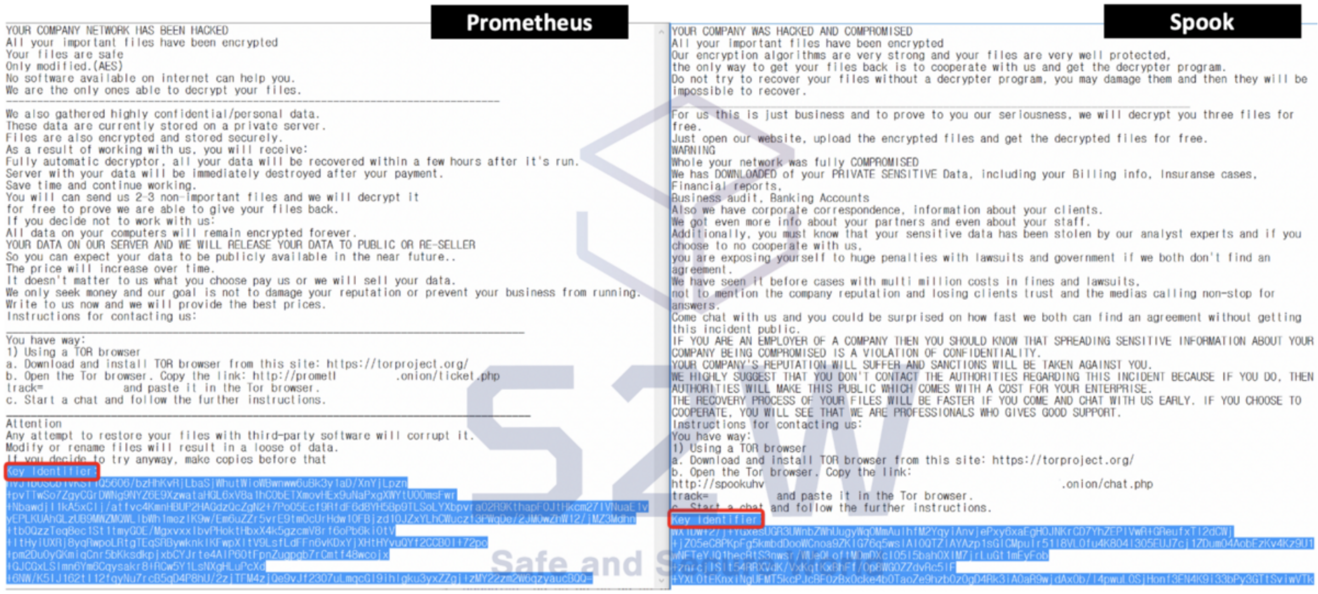
The double extortion site operated by Spook ransomware

2. Prometheus x Spook: Spook ransomware same as Prometheus ransomware.

The ransom note, the negotiation page, the files, and the resources on the double extortion site of Spook ransomware are similar to Prometheus ransomware.

2–1. The ransom note of Spook ransomware is similar to the ransom note of Prometheus ransomware.

Key Identifier is the signature method of Thanos builder. When the user created the ransomware using , we can check the signature of “Key Identifier” on the ransom note. Based on this signature, we have confirmed the fact that Prometheus ransomware and Spook ransomware were generated by Thanos builder.

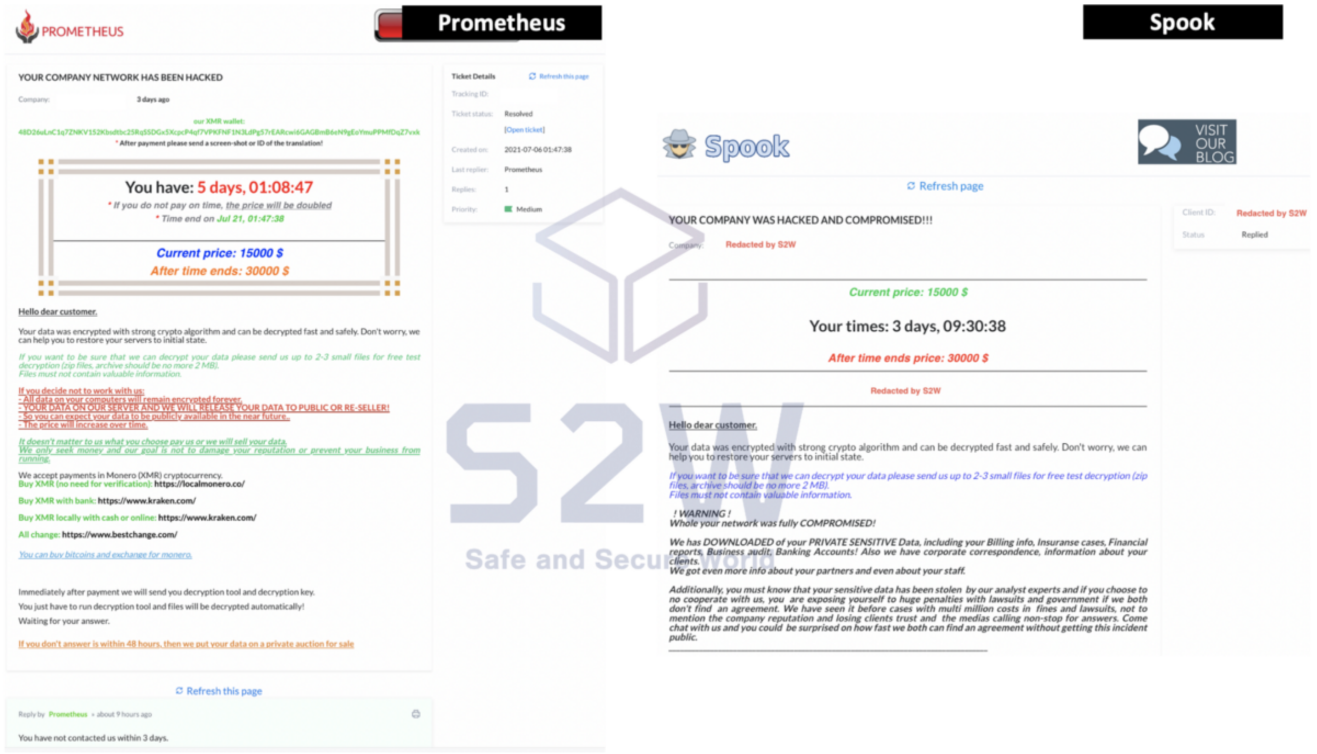


```
YOUR COMPANY NETWORK HAS BEEN HACKED
All your important files have been encrypted
Your files are safe
Only modified.(AES)
No software available on internet can help you.
We are the only ones able to decrypt your files.
--------------------------------------------------------------------------------
We also gathered highly confidential/personal data.
These data are currently stored on a private server.
Files are also encrypted and stored securely.
As a result of working with us, you will receive:
Fully automatic decryptor, all your data will be recovered within a few hours after it's run.
Server with your data will be immediately destroyed after your payment.
Save time and continue working.
You will can send us 2-3 non-important files and we will decrypt it
for free to prove we are able to give your files back.
If you decide not to work with us:
All data on your computers will remain encrypted forever.
YOUR DATA ON OUR SERVER AND WE WILL RELEASE YOUR DATA TO PUBLIC OR RE-SELLER
So you can expect your data to be publicly available in the near future..
The price will increase over time.
It doesn't matter to us what you choose pay us or we will sell your data.
We only seek money and our goal is not to damage your reputation or prevent your business from running.
Write to us now and we will provide the best prices.
Instructions for contacting us:
________________________________________________________________________________
You have way:
1) Using a TOR browser
a. Download and install TOR browser from this site: https://torproject.org/
b. Open the Tor browser. Copy the link: http://prometl          .onion/ticket.php
track=             and paste it in the Tor browser.
c. Start a chat and follow the further instructions.
________________________________________________________________________________
Attention
Any attempt to restore your files with third-party software will corrupt it.
Modify or rename files will result in a loose of data.
If you decide to try anyway, make copies before that
Key Identifier:
[illegible]Q5606/bzHhKvRjLbaSjWhutWioWBwnww6uBk3y1aD/XnYjLpzn
+pvTTwSo7ZgyCGrDWNg9NYZ6E9XzwataHGL6xV8a1hC0bETXmovHEx9uNaPxgXWYtU00msFwr
+NbawdjI1kA5xClj/atfvc4KmnHBUP2HAGdzQcZgN2+7Po05Ecf9RfdF6d8YH5Bp9TLSoLYXbpvra02R9KthapF0JtHkcm27IVNuaE1v
yEPLKUAhGLzUB9MWZMQWLIbWh1mezIK9w/Em6uZZr5vrE9tm0cUrHdw10FBjzd10JZxYLhCWucz13PWgDe/2JM0wZhW12/jMZ3Mdhn
+tb0QzzTeq8ec1St1tmyG0E/MgxvxxIbvPHoktHbxX4k5gzcmV8rf6oPb6kI0tV
+ItHyIUXRj8yqRwpoLRtgTEqSRBywknkIKFwpXItV9LsfLdFFn6vKDxYjXHtHYvuQYf2CCB0I+72pc
+pm2Du0yGKmiqCnr5bKksdkpjxbCYJrte4AIP60tFpnZugpgb7rCmtf48wcojx
+GJCGxLSImn6Ym6Cqysakr8+RCw5Y1LsNXgHLuPcXd
+6NW/K5IJ162tI12fqyNu7rcB5qD4P8hU/2zjTFM4zjQe9vJf2307uLmqcGI9ihIgku3yxZZgj+zMY22zm2W6qzyaucBQQ=
```

```
YOUR COMPANY WAS HACKED AND COMPROMISED
All your important files have been encrypted
Our encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter program.
Do not try to recover your files without a decrypter program, you may damage them and then they will be
impossible to recover.
________________________________________________________________________________
For us this is just business and to prove to you our seriousness, we will decrypt you three files for
free.
Just open our website, upload the encrypted files and get the decrypted files for free.
WARNING
Whole your network was fully COMPROMISED
We has DOWNLOADED of your PRIVATE SENSITIVE Data, including your Billing info, Insuranse cases,
Financial reports,
Business audit, Banking Accounts
Also we have corporate correspondence, information about your clients.
We got even more info about your partners and even about your staff.
Additionally, you must know that your sensitive data has been stolen by our analyst experts and if you
choose to no cooperate with us,
you are exposing yourself to huge penalties with lawsuits and government if we both don't find an
agreement.
We have seen it before cases with multi million costs in fines and lawsuits,
not to mention the company reputation and losing clients trust and the medias calling non-stop for
answers.
Come chat with us and you could be surprised on how fast we both can find an agreement without getting
this incident public.
IF YOU ARE AN EMPLOYER OF A COMPANY THEN YOU SHOULD KNOW THAT SPREADING SENSITIVE INFORMATION ABOUT YOUR
COMPANY BEING COMPROMISED IS A VIOLATION OF CONFIDENTIALITY.
YOUR COMPANY'S REPUTATION WILL SUFFER AND SANCTIONS WILL BE TAKEN AGAINST YOU.
WE HIGHLY SUGGEST THAT YOU DON'T CONTACT THE AUTHORITIES REGARDING THIS INCIDENT BECAUSE IF YOU DO, THEN
AUTHORITIES WILL MAKE THIS PUBLIC WHICH COMES WITH A COST FOR YOUR ENTERPRISE.
THE RECOVERY PROCESS OF YOUR FILES WILL BE FASTER IF YOU COME AND CHAT WITH US EARLY. IF YOU CHOOSE TO
COOPERATE, YOU WILL SEE THAT WE ARE PROFESSIONALS WHO GIVES GOOD SUPPORT.
Instructions for contacting us:
You have way:
1) Using a TOR browser
a. Download and install TOR browser from this site: https://torproject.org/
b. Open the Tor browser. Copy the link:
http://spookuhv                              .onion/chat.php
track=          and paste it in the Tor browser.
c. Start a chat and follow the further instructions.
Key Identifier
[illegible]UGR3UWnbZWhUugyWq0MmAuIhfM2YqyIAnvjePxy6xaEgH0JNKrCD7YhZEPIVwR+GReufxTI2dCWj
+jZ05eC8PKpFg5kmbdDooWCnoa9ZKIG76q5wsIAI0QTZIAYAzp1sGICMpuIr51I8VL0fu4K804I305EUJ7cj1ZDum04AobEzKv4Kz9U1
wNFTeYJQ1hecRtS3nwsr/WUe0LoftMDmDXcI05I5bah0XIM7jrLuGt1mEyFob
+znrcjISIt54RRXVdK/VxKqtKxBhFf/Op8WG0ZZdvRc5IF
+YXL0tEKnxiNgUFMT5kcPJcBF0zBx0cke4b0TaoZe9hzb0z0g04Rk3iA0aR9wjdAx0b/I4pwuL0SjHonf3EN4K9i33bPy3GTtSviwVTk
```

Compared the ransom note between Prometheus x Spook

2–2. The negotiation page of Spook ransomware is similar to the ransom note of Prometheus ransomware.



YOUR COMPANY NETWORK HAS BEEN HACKED

Company: 3 days ago

our XMR wallet:
48D26uLnC1q7ZNKV152Kbsdtbc25Rq5SDGx5XcpcP4qf7VPKFNF1N3LdPg57rEARcwi6GAGBmB6eN9gEoYmuPPMfDqZ7vxk

* After payment please send a screen-shot or ID of the translation!

You have: 5 days, 01:08:47

* If you do not pay on time, the price will be doubled

* Time end on Jul 21, 01:47:38

Current price: 15000 $

After time ends: 30000 $

Hello dear customer.

Your data was encrypted with strong crypto algorithm and can be decrypted fast and safely. Don't worry, we can help you to restore your servers to initial state.

If you want to be sure that we can decrypt your data please send us up to 2-3 small files for free test decryption (zip files, archive should be no more 2 MB).
Files must not contain valuable information.

If you decide not to work with us:
- All data on your computers will remain encrypted forever.
- YOUR DATA ON OUR SERVER AND WE WILL RELEASE YOUR DATA TO PUBLIC OR RE-SELLER!
- So you can expect your data to be publicly available in the near future..
- The price will increase over time.

It doesn't matter to us what you choose pay us or we will sell your data.
We only seek money and our goal is not to damage your reputation or prevent your business from running.

We accept payments in Monero (XMR) cryptocurrency.
Buy XMR (no need for verification): https://localmonero.co/

Buy XMR with bank: https://www.kraken.com/

Buy XMR locally with cash or online: https://www.kraken.com/

All change: https://www.bestchange.com/

You can buy bitcoins and exchange for monero.

Immediately after payment we will send you decryption tool and decryption key.

You just have to run decryption tool and files will be decrypted automatically!

Waiting for your answer.

If you don't answer is within 48 hours, then we put your data on a private auction for sale

Ticket Details	Refresh this page
Tracking ID:	
Ticket status:	Resolved [Open ticket]
Created on:	2021-07-06 01:47:38
Last replier:	Prometheus
Replies:	1
Priority:	🟩 Medium

Refresh this page

Reply by Prometheus » about 9 hours ago

You have not contacted us within 3 days.

YOUR COMPANY WAS HACKED AND COMPROMISED!!!

Company: Redacted by S2W

Client ID:	Redacted by S2W
Status	Replied

Current price: 15000 $

Your times: 3 days, 09:30:38

After time ends price: 30000 $

Redacted by S2W

Hello dear customer.

Your data was encrypted with strong crypto algorithm and can be decrypted fast and safely. Don't worry, we can help you to restore your servers to initial state.

If you want to be sure that we can decrypt your data please send us up to 2-3 small files for free test decryption (zip files, archive should be no more 2 MB).
Files must not contain valuable information.

! WARNING !
Whole your network was fully COMPROMISED!

We has DOWNLOADED of your PRIVATE SENSITIVE Data, including your Billing info, Insuranse cases, Financial reports, Business audit, Banking Accounts! Also we have corporate correspondence, information about your clients.
We got even more info about your partners and even about your staff.

Additionally, you must know that your sensitive data has been stolen by our analyst experts and if you choose to no cooperate with us, you are exposing yourself to huge penalties with lawsuits and government if we both don't find an agreement. We have seen it before cases with multi million costs in fines and lawsuits, not to mention the company reputation and losing clients trust and the medias calling non-stop for answers. Come chat with us and you could be surprised on how fast we both can find an agreement without getting this incident public.

Compared the negotiation page between Prometheus x Spook

2–3. The files and resources related to victims are located on the same path.

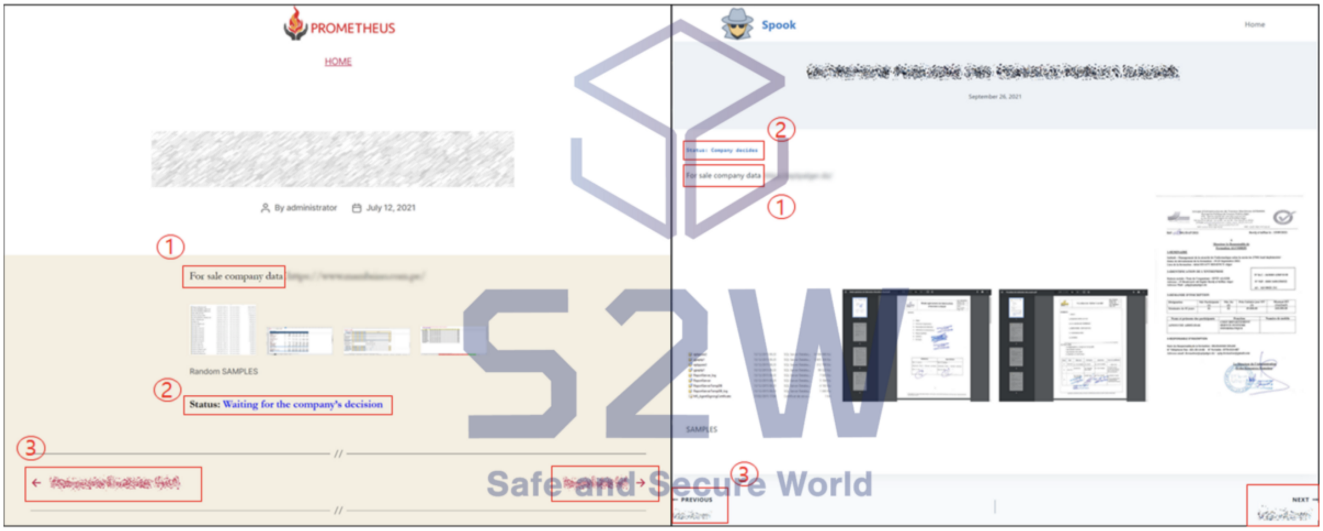
Files

Spook ransomware: http://spookuhv****.onion/blog/wp-content/uploads/2021/05/1-15.png

Prometheus ransomware: http://promethw****.onion/blog/wp-content/uploads/2021/05/1-15.png

> In this path, the webserver has the files of victims infected by Prometheus ransomware. Hence they are operating the same web server for the double extortion site.

Resources



Compared the victim page between Prometheus x Spook

1. All posts published the same string “”.
2. Show the status of negotiation with victims through the field of “
3. Move the posts using the tabs

Conclusion

- Spook ransomware was rebranded Prometheus ransomware. They derived from Thanos and using similar UI & resources to Prometheus ransomware.
- Prometheus ransomware and Spook ransomware are the same ransomware attack group through the same string and the resources on the double extortion site.

CYBER THREAT INTELLIGENCE DIVISION
TALON