Prometheus x Spook: Prometheus ransomware rebranded Spook ransomware.

By S2W

Published: 2021-10-05 · Archived: 2026-04-05 23:46:39 UTC

3 min read

Oct 5, 2021

S2W TALON

Press enter or click to view image in full size

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.

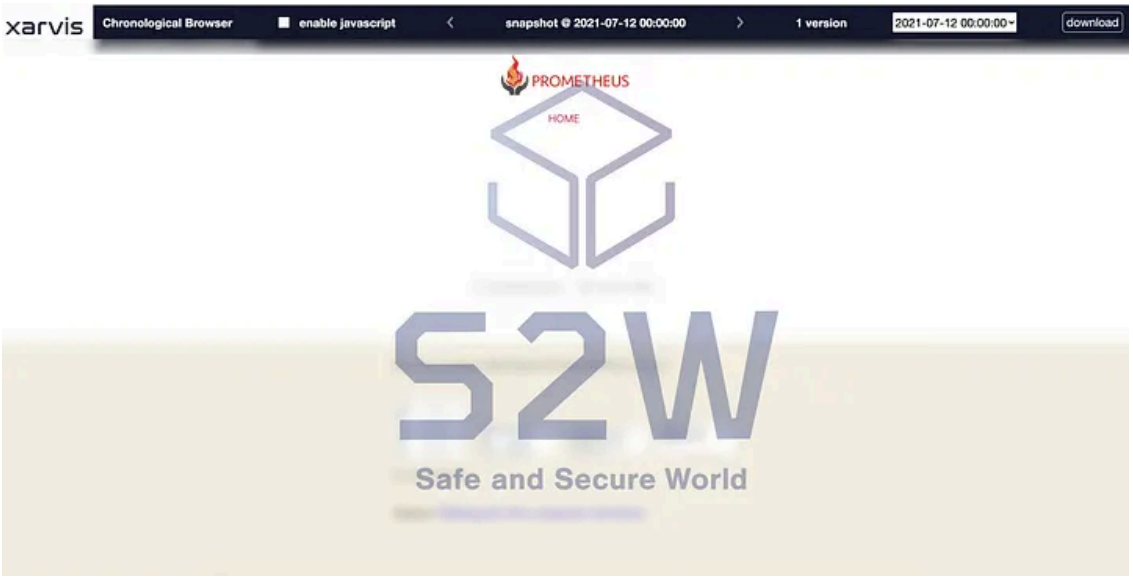
Detailed analysis

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 is not working now. Hence Prometheus ransomware stopped the activities on now.**

Press enter or click to view image in full size



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.

Press enter or click to view image in full size

The double extortion site operated by Spook ransomware

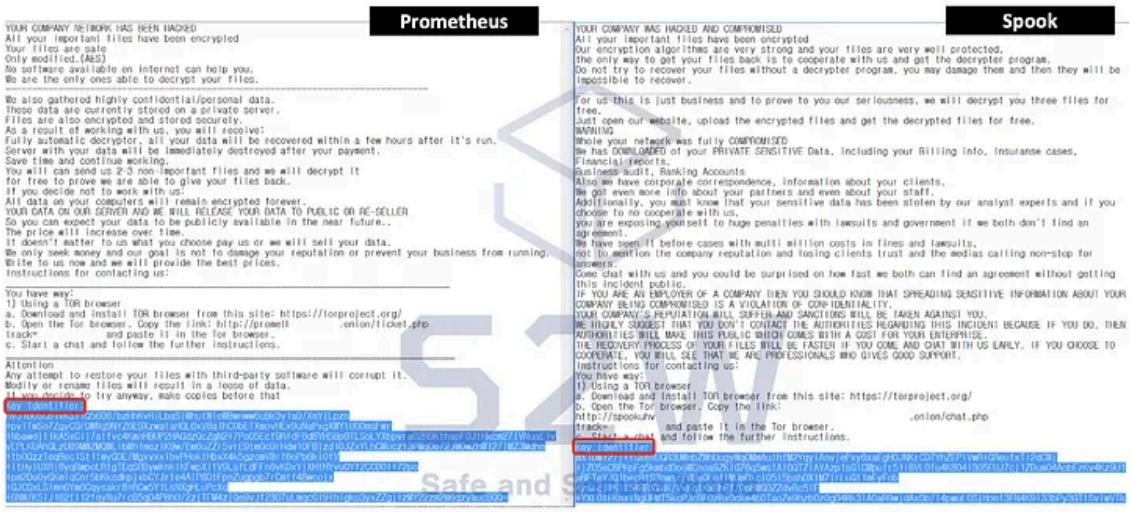
2. Prometheus x Spook: Spook ransomware same as Prometheus ransomware.

- 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 **Thanos builder**, 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.

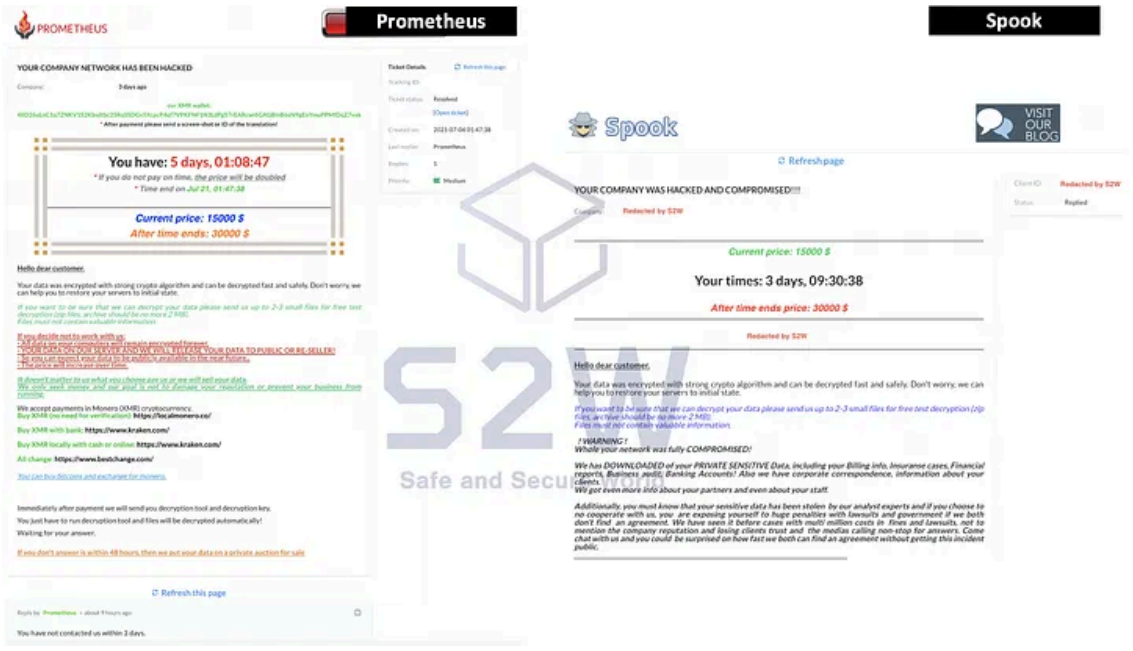
  Press enter or click to view image in full size



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.

Press enter or click to view image in full size



Compared the negotiation page between Prometheus x Spook

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

Files

Get S2W's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

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

Press enter or click to view image in full size

Compared the victim page between Prometheus x Spook

1. All posts published the same string "**For sale company data: {the name of victim}**".
2. Show the status of negotiation with victims through the field of "**Status".**
3. Move the posts using the tabs **PREVIOUS, NEXT**

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.

- Homepage:https://www.s2w.inc
- Facebook: https://www.facebook.com/S2W
- Twitter: https://twitter.com/S2W_Official
