Quick analysis of Haron Ransomware (feat. Avaddon and Thanos)

medium.com/s2wlab/quick-analysis-of-haron-ransomware-feat-avaddon-and-thanos-1ebb70f64dc4

S2W July 23, 2021

S2W

Jul 22, 2021

.

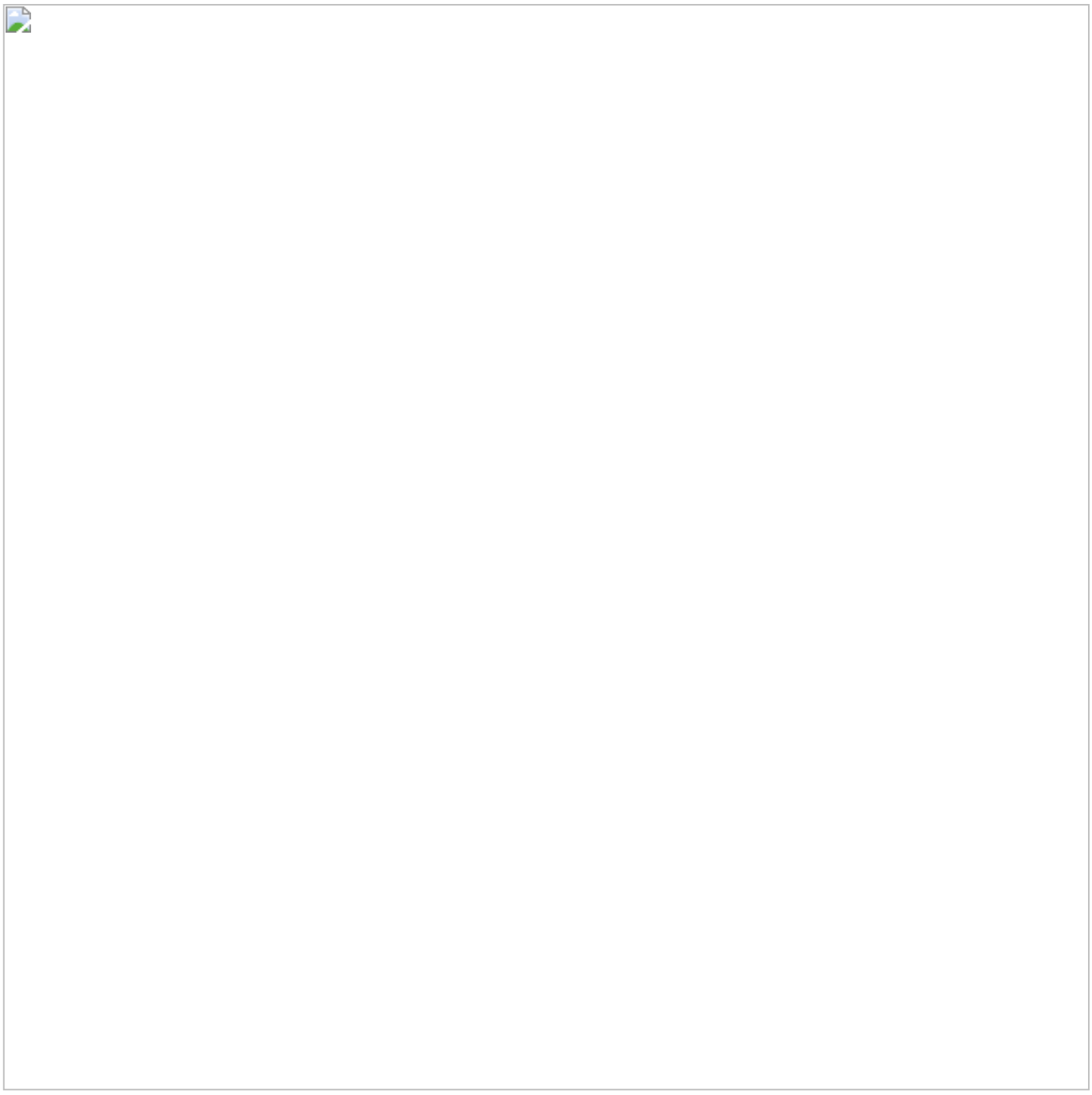
4 min read

Author: Talon @ S2WLAB

Haron ransomware was first discovered in July 2021. When infected with this ransomware, the extension of the encrypted file is changed to the victim's name. They are using a ransom note and operating their own leak site similar to Avaddon ransomware. They have disclosed only one victim on the leak site so far.

Detailed analysis

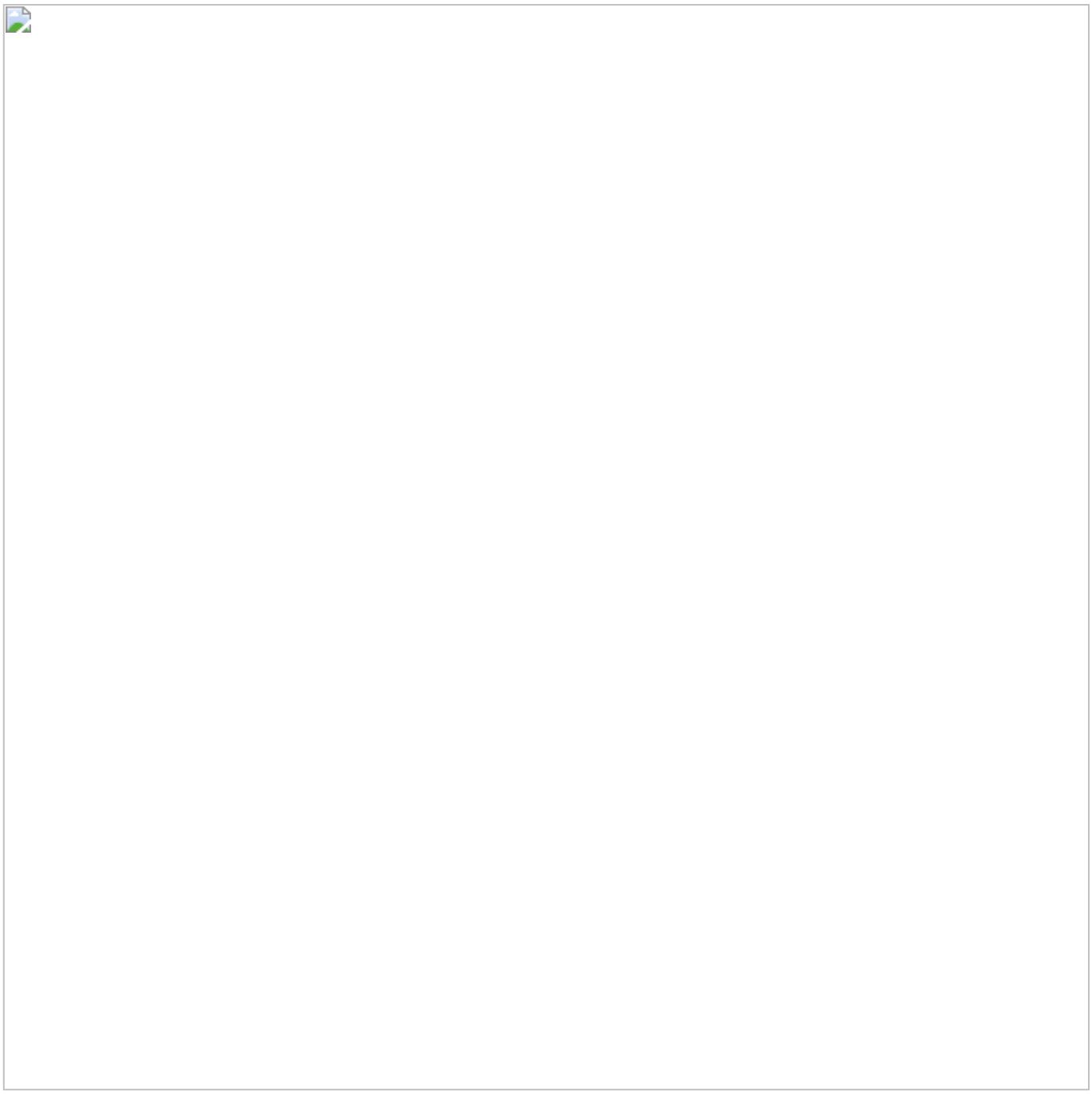
A. Similarity of ransom notes



- The highlighted part in the picture above is the same part between Haron and Avaddon.
- The main difference is that Haron suggests a specific ID and Password for victim to log in to the negotiation site.

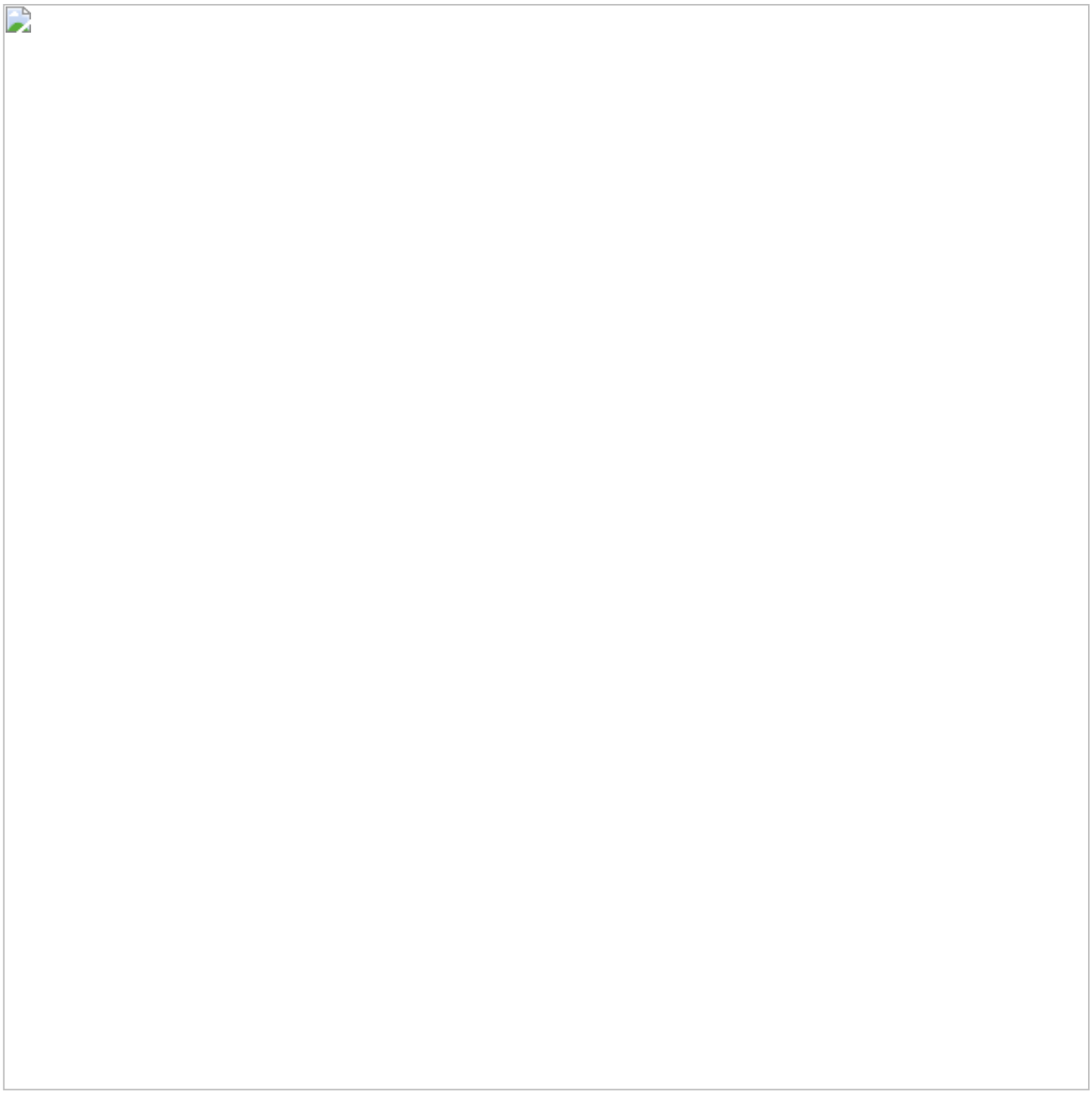
B. Similarity of negotiation sites

B-1. Haron operates the negotiation site and leak site on the same domain



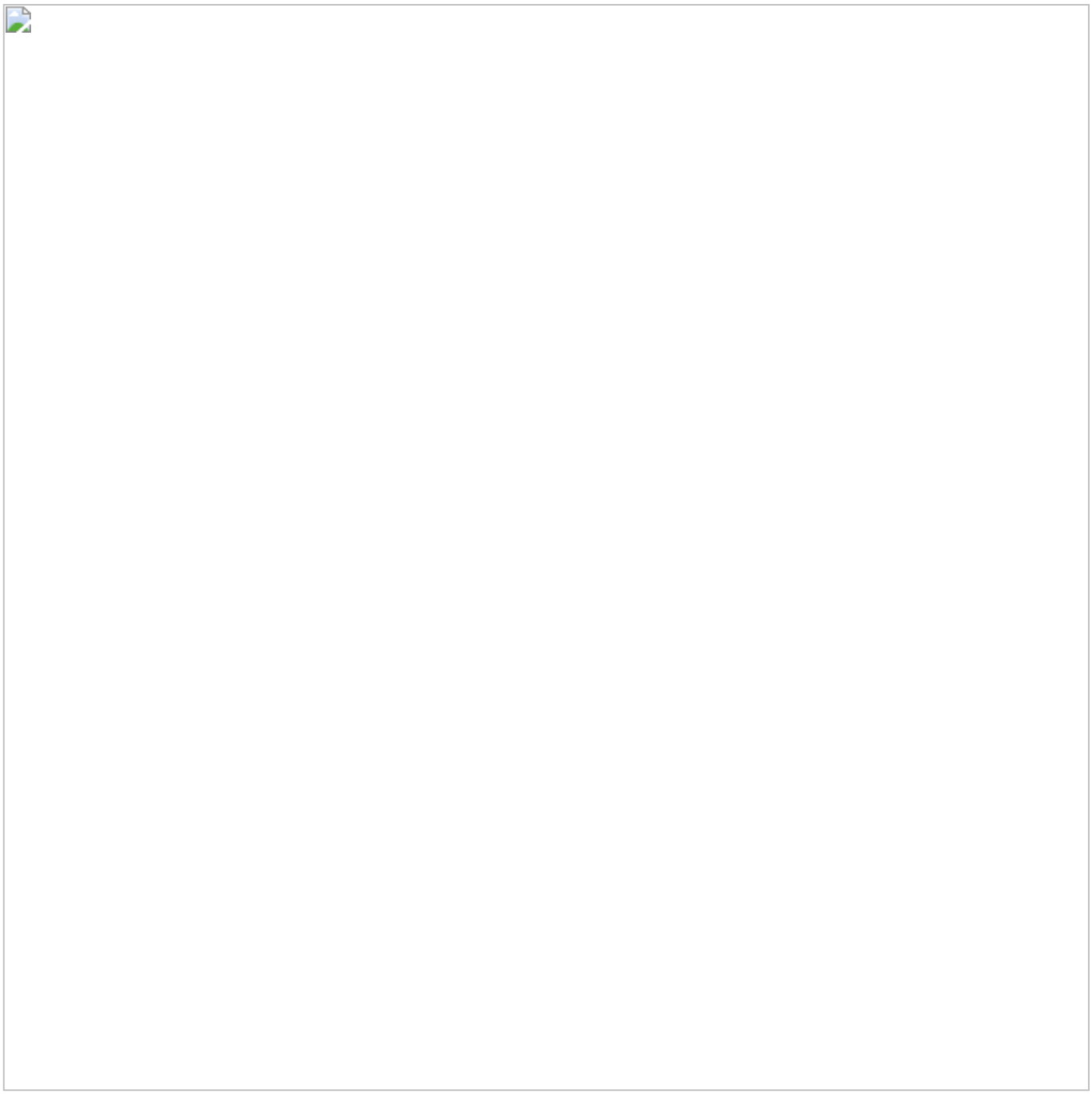
- Avaddon operated negotiation and leak sites on different domain addresses.
- In the case of Haron, ID and password are required to have access to the negotiation page.

B-2. Comparing the contents of the negotiation sites



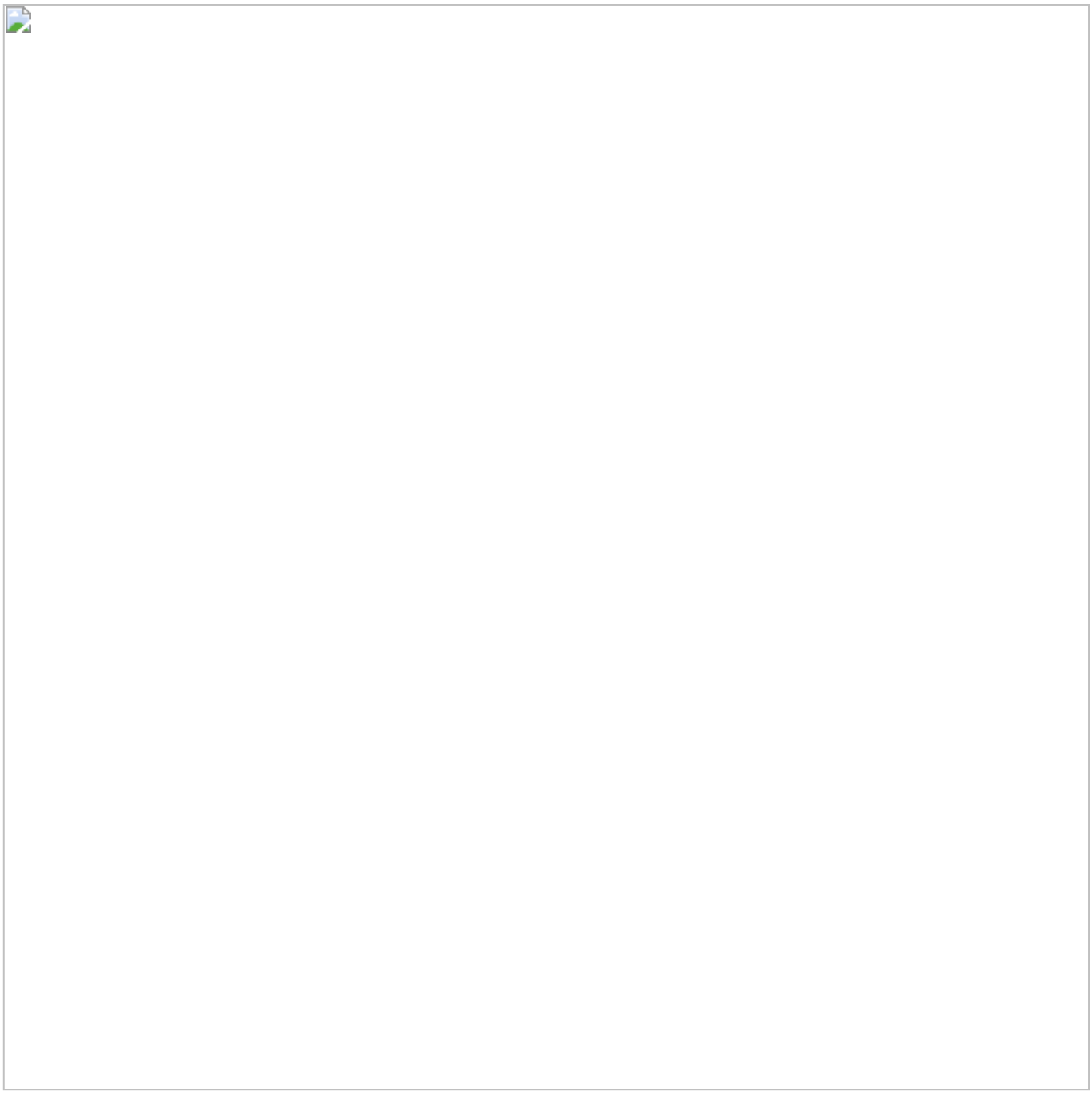
- The appearance of negotiation site is almost identical except for the name of ransomware “Haron” or “Avaddon”
- The overall interface and string of the negotiation page are similar, but the date notation hh:mm dd:MM:yyyy has converted to hh:mm and icon in the chat window has disappeared

B-3. Haron’s chat feature is built based on open source

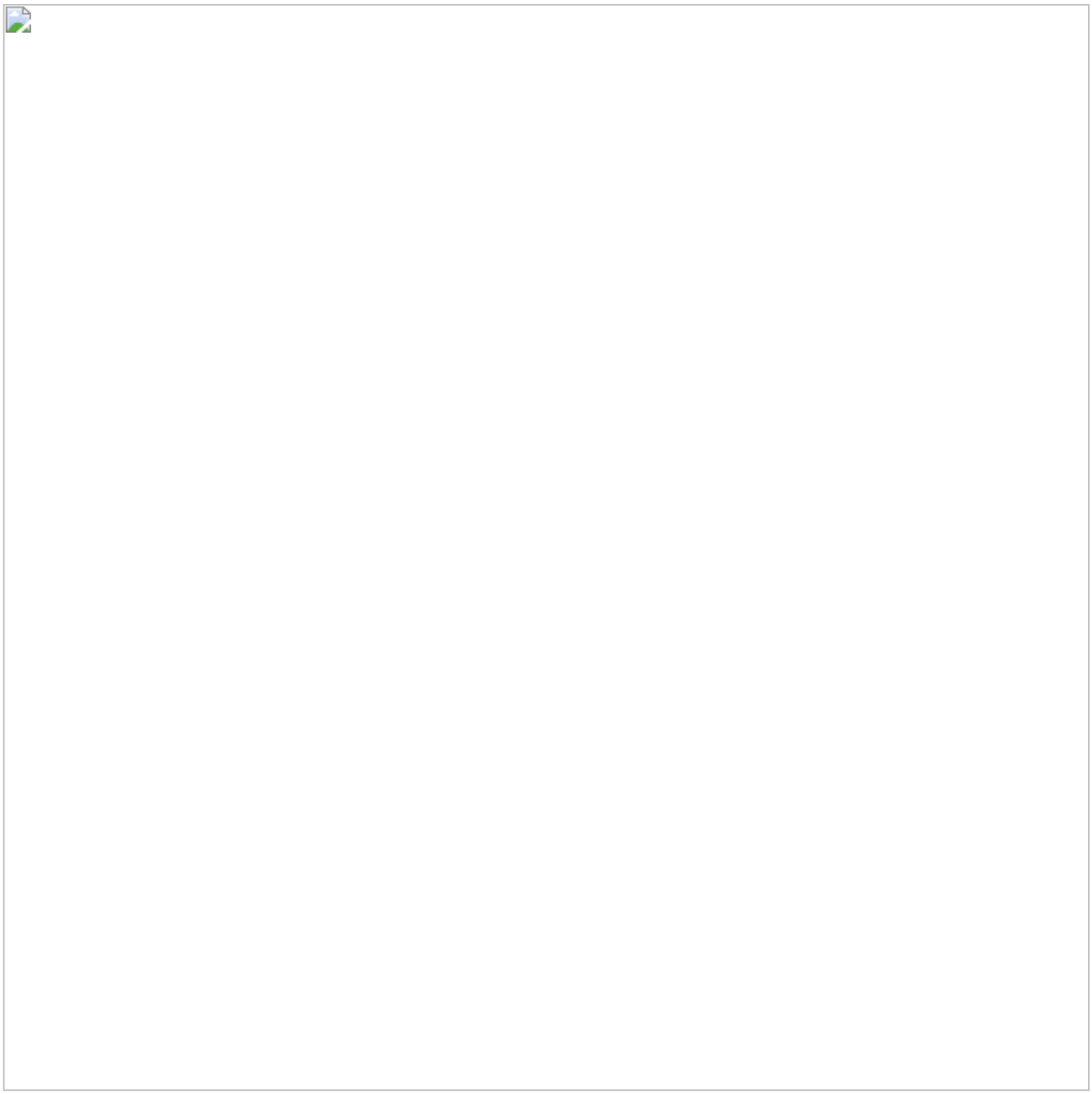


The JavaScript used for chat is the open-source code published on the Russian Developer Forum in the past.

C. Similarity of the leak sites



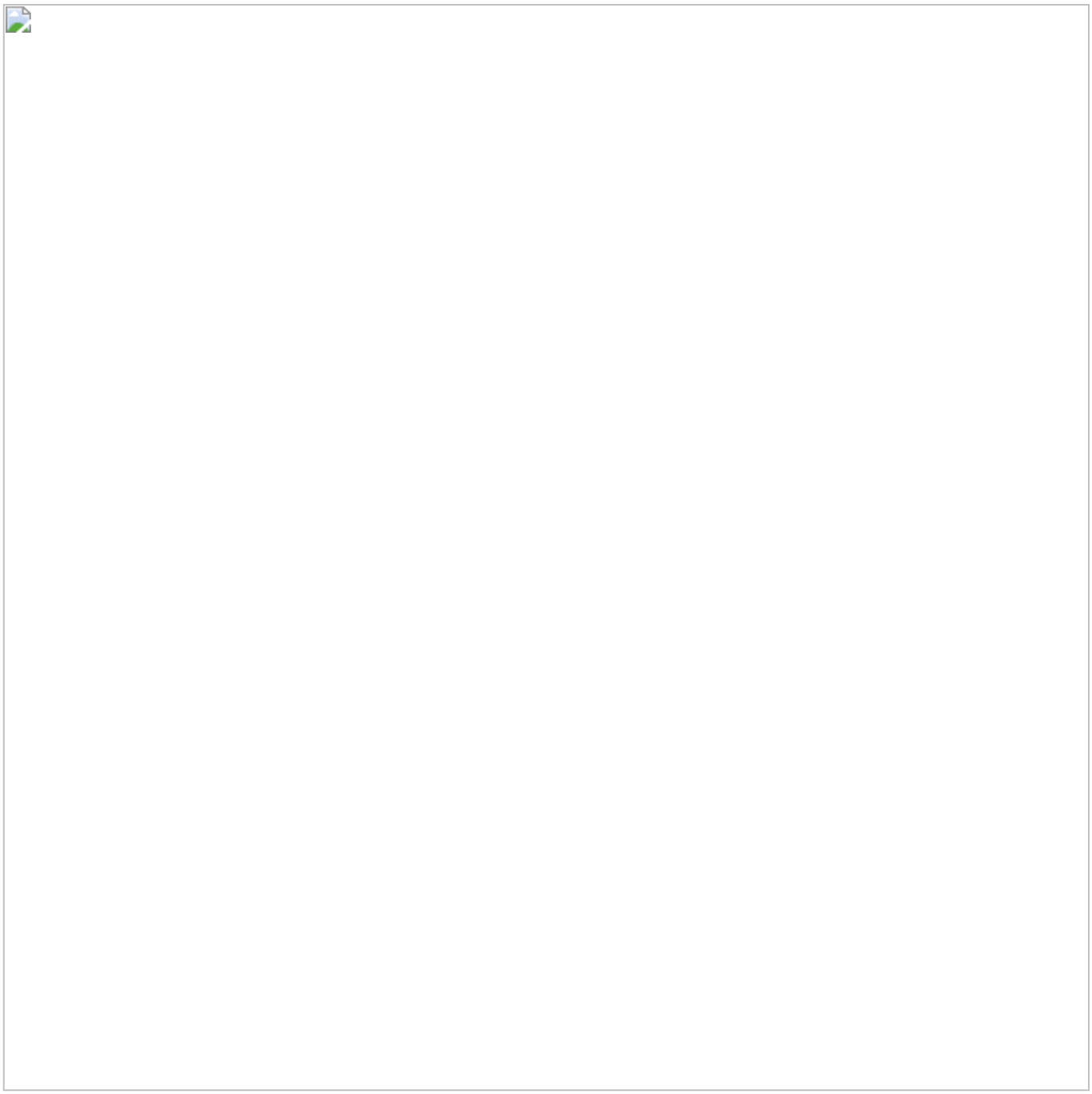
- As shown in the picture above, the leak site of Haron has the same structure as that of Avaddon.
- Haron also uses a strategy to induce negotiations within that period by setting the time for the next data update, but there is no DDoS attack notice yet. It has not been confirmed whether they would carry out a DDoS attack like Avaddon.
- Also, Avaddon gave 10 days for negotiation, but Haron gave about 6 days.



D. Comparative analysis of Haron and Avaddon

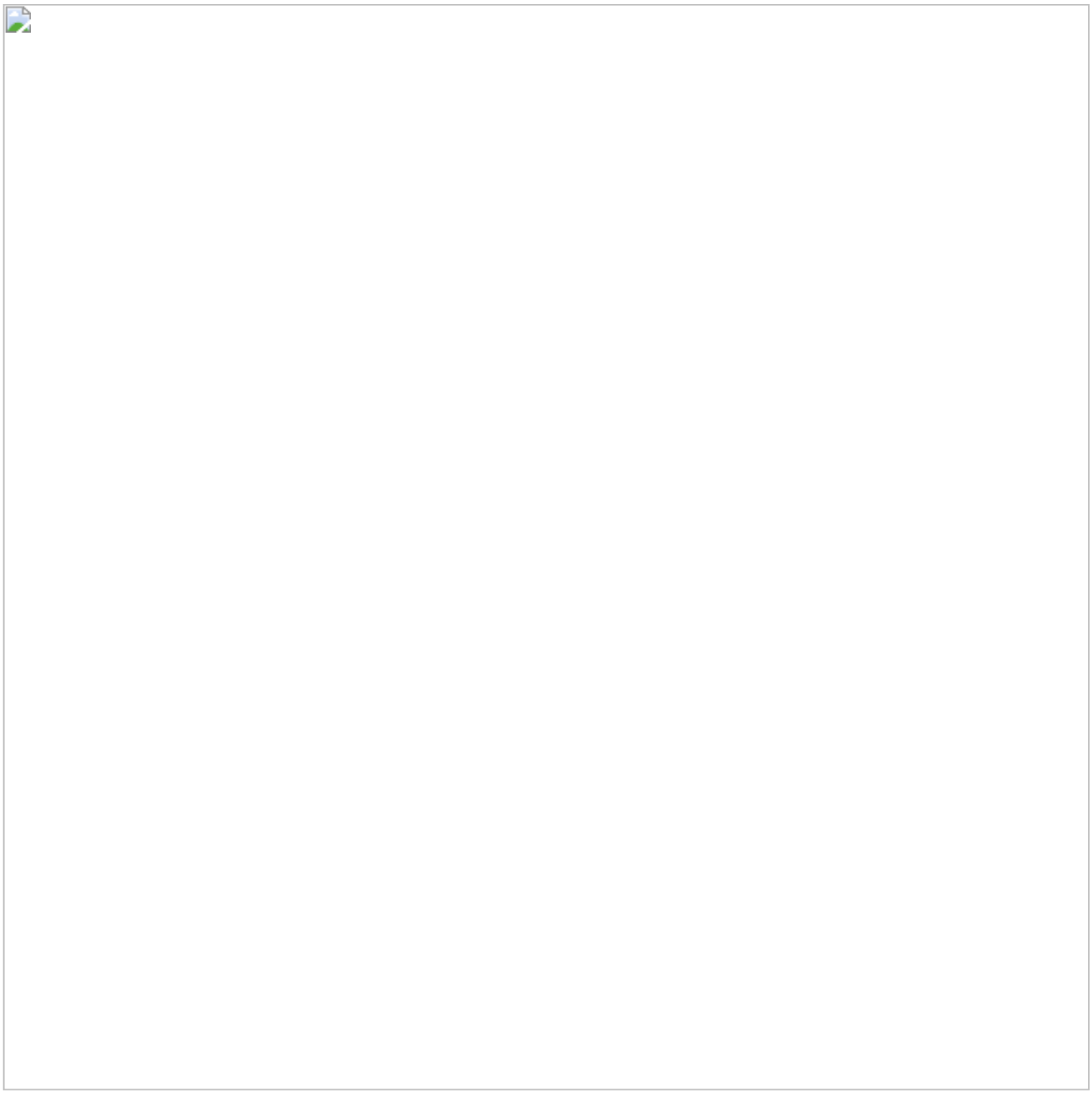
D-1. The files related to Avaddon

- There are logos, icons as well as sample data of victims used by Avaddon on the Haron's server. However, all of the files can be collected at the client level.
- The last modified date of the files is the same as the date (2021–06–11) when Avaddon disappeared after sending the decryption key to BleepingComputer



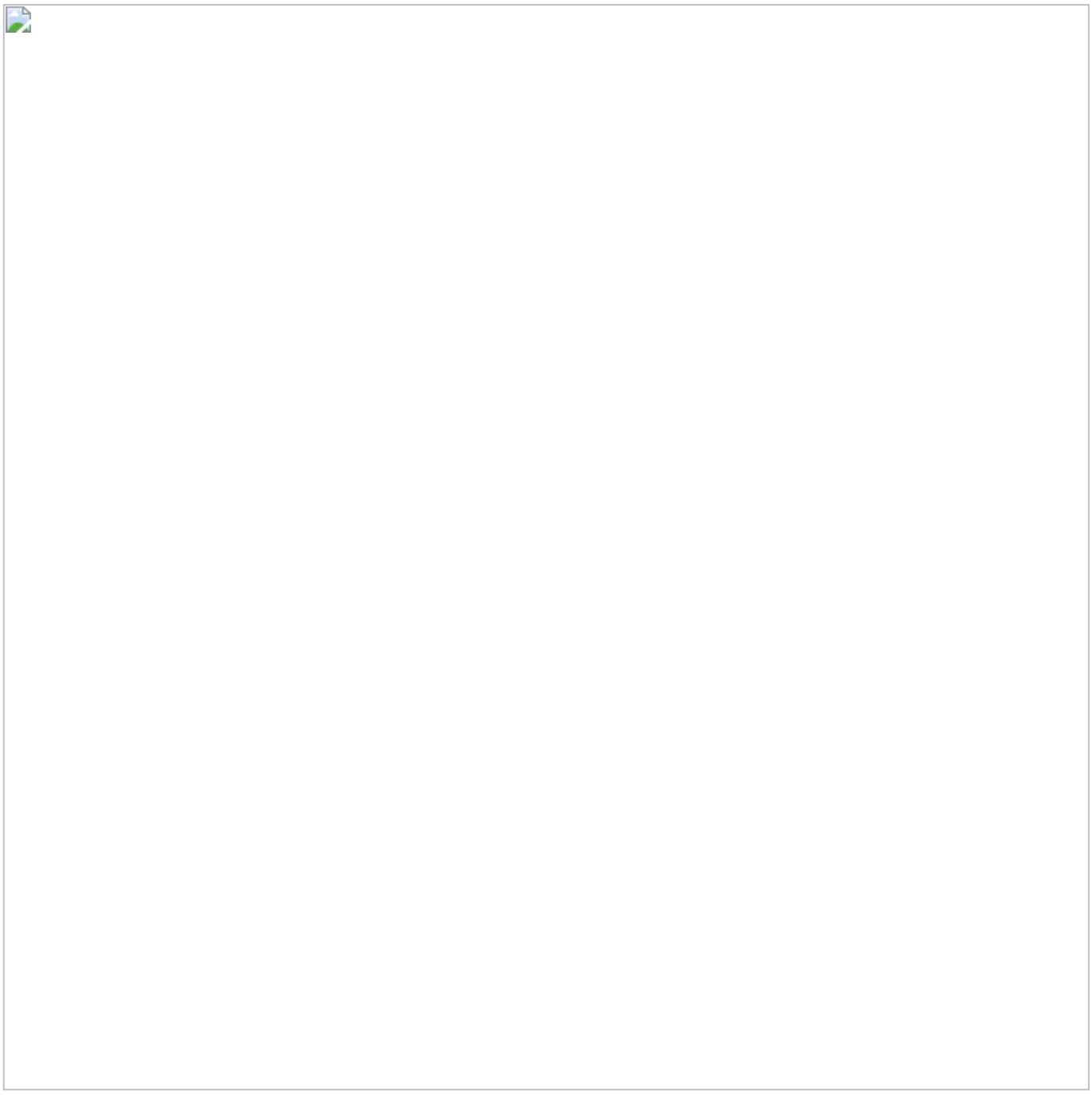
D-2. Haron is based on Thanos Ransomware

Haron is using Thanos Ransomware to infect victims. Even the functions are almost the same as before.



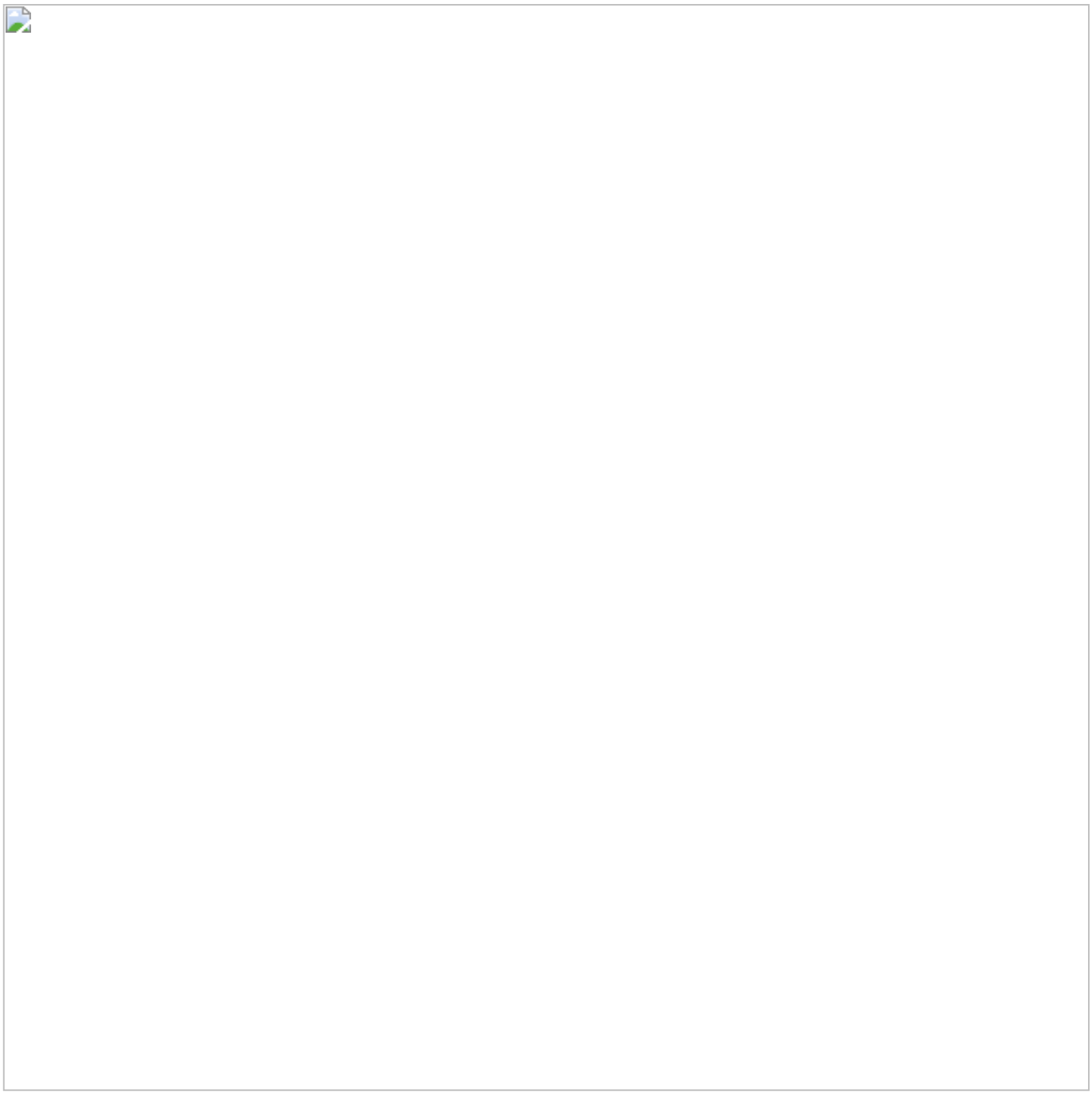
Thanos ransomware is a RaaS that has been sold on DDW since 2019

> https://medium.com/s2wlab/story-of-the-week-ransomware-on-the-darkweb-2-ace644c6db3f



Recently, Thanos builder has been published on github.

> https://github.com/Hacker-Data/Thanos-Ransomware-Builder



Conclusion

1. It is difficult to conclude that Haron is a re-emergence of Avaddon based on our analysis.

- Avaddon developed and used their own C++ based ransomware.
- But Haron is using C# based Thanos ransomware which is publicly available.
- The Web Interface of Haron's Leak site is almost identical to that of Avaddon ransomware assuming that Haron mimicked Avaddon's UI.- When ransomware gangs rebrand, they usually change many things such as the design of the leak site.- Example : Gandcrab → Sodinokibi/REvil, Babuk → Payload.bin

2. Haron ransomware gang doesn’t have their own dedicated skills compared to other well known ransomware gangs such as Avaddon.

- Using Thanos ransomware leaked to the public.
- Using open-source chat feature on their negotiation site.
- Copycat UI from Avaddon on their leak site.
- Insufficient authentication process when accessing the negotiation site.- Anyone can enter the negotiation and leak site using test/test account. * However, after this publication, the test account has removed.

Malware Hash

1. Haron : 6e6b78a1df17d6718daa857827a2a364b7627d9bfd6672406ad72b276014209c
2. Thanos : c460fc0d4fdaf5c68623e18de106f1c3601d7bd6ba80ddad86c10fd6ea123850