Hive Shutdown Incident

February 2023

Cyberint

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Ransomware is one of the most painful threats to organizations worldwide. As this industry keeps on growing both in number of groups and improved technology, every now and then global authorities are able to get their hands on individuals and important data that can mitigate and prevent this threat.

This week, the FBI was able to take down the notorious Hive Ransomware group's Onion Site.

After a long investigation and extensive hours and efforts, the FBI compromised the group's servers and took down their entire operation.

Although these are great news, and Hive has suffered major damages, both financial and possibly legal, the cyber security community's opinions are split between who is the next to fall in the ransomware industry and does it matter? or is it just a slap on the wrist?

THE INCIDENT

The U.S. Department of Justice declared a significant triumph in the battle against ransomware last week by taking down and confiscating the infrastructure of Hive (Figure 1).

Figure 1: The Shutdown message on Hive group's Onion site

Hive is one of the most consistent groups in the ransomware industry, and was located in the top 10 ransomware groups on 2022. It was introduced to our lives in mid-2021 and is claimed to compromise and ransomed around 1500 victims so far.

In a press conference conducted by FBI Director Christopher Wray, it was disclosed that the FBI took control of servers in Los Angeles last Wednesday, holding the crucial data of the Hive gang. The operation was the result of months of investigation, starting with the FBI's infiltration of Hive's network in July 2022. With access to the network, the FBI acquired the keys to decrypt ransomware and distributed them to 1,300 past and current Hive targets.

OPERATION METHODS

From what we currently know, it seems that the FBI had an undercover presence in the group's operation for months as this individual tried to exfiltrate any relevant data regarding the group's techniques, infrastructure, decryption keys and maybe information about individuals.

In addition to that effort, in the end of this operation, the FBI probably had direct access to the group's infrastructure which they used to obtain any possible data and to perform the shutdown.

When considering the state in which the FBI was, there was no major benefit of shutting the website down, it would be much more profitable for them to keep their undercover presence as much as possible which is leading to speculations that Hive already knew something wrong and predicted the shutdown.

COMMUNITY DISCUSSION

The cyber security community talked a lot about this event given the fact it is rear to see major groups taken down in recent years.

WHO IS NEXT?

Many members of the cyber community already speculate and wishing Hive is the first of many to come in the next months.

Some speculations already put LockBit as the next ransomware to fall and Everest which their Onion site was having some connectivity issues in recent days (Figure 2).

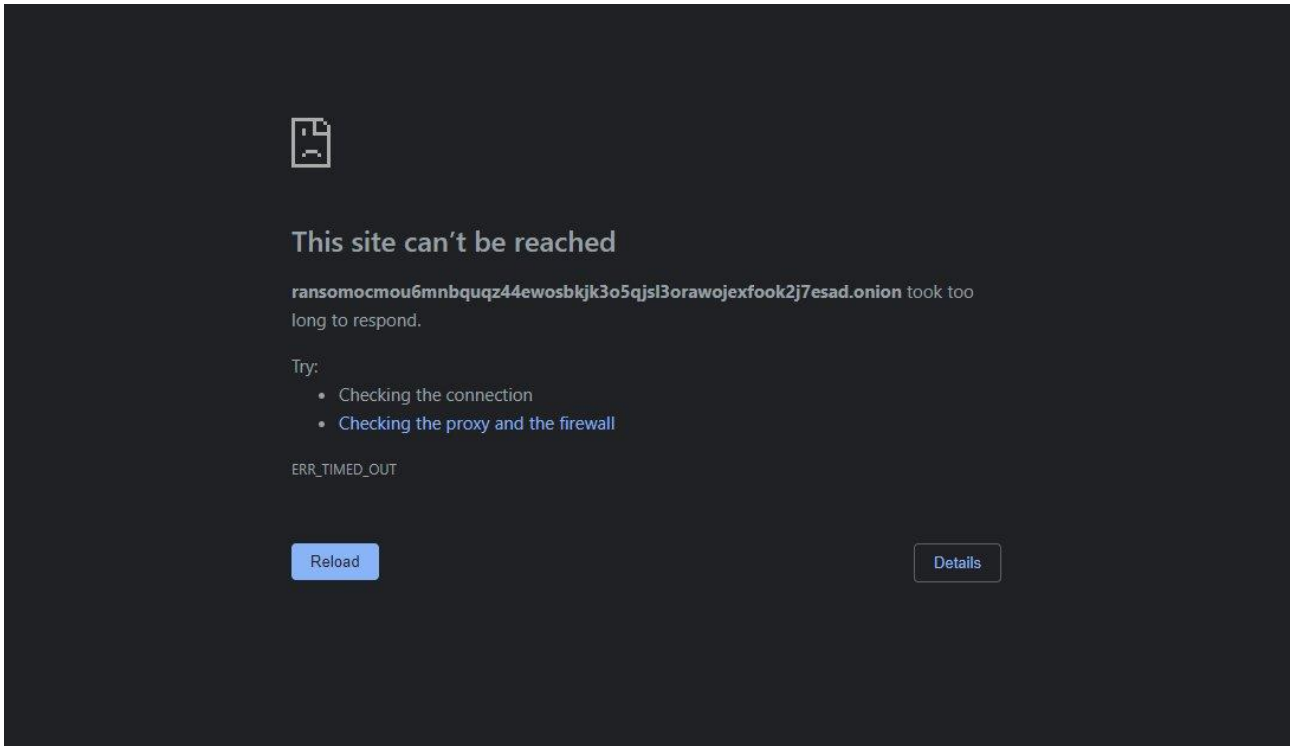

Figure 2: Everest Ransomware Onion connectivity issues

Overall, it seems that many are optimistic and think that the FBI and other law authorities finally found effective ways to infiltrate the groups and might cause and actual threat to them.

DOES IT MATTER? PESSIMISM OR REALISM?

As mentioned, many celebrate the takedown of Hive site, but many others raises the simple question - "Does it matter?".

There is no argument. This operation is important and will and already has its benefits. Still, if we try to look at the effect it will have on the ransomware industry in general, one can not wonder if anything significant is going to change.

While the seizure of a lot of valuable data is an amazing accomplishment, servers, and infrastructures are much easier to replace than people. Nothing can guarantee that Hive's operators and high-profile members will ever be arrested.

Of course that we don't know what information was obtained by the FBI, and we do believe that any arrest that the law authorizes can make will happen. Still, the challenge gets much bigger if the operators are located outside of the jurisdiction of the FBI such as Russia and other countries that are known for being a shelter to ransomware groups.

CONCLUSIONS

The shutdown of Hive's website is a great news for all of us, it seems that the development of the Ransomware-as-a-Service (RaaS) business model opened the door to many low-mid sophistication threat actors, but also to undercover agents and lowered the suspicious around new members of a group.

The Cyberint Research Team believes that the FBI will take down other groups in the future using the same methodology they used with Hive to halt and damage the operation of these threat groups.

It seems that shutdown is not necessarily a solution of the ransomware industry, but it is surely a great way to buy some time and the assessments shows that this shutdown saved around $130 million in damages for potential victims.

Overall, it seems that Hive have suffered major financial damage and might even lead to the arrest of mid-low-ranked members or affiliates. it will take weeks and even months to rebrand itself and get back to the industry.

Hive was the sixth most popular group in the ransomware industry on 2022, responsible for 7% of all published ransomware cases and was one of approximately 50 active ransomware groups.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

USA - NY

Tel: +1-646-568-7813
368 9th Ave, Suite 11-108, New York, NY 10001

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 2210

UNITED KINGDOM

Tel: +44-203-514-1515
6 The Broadway, Mill Hill NW7 3LL, London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536