Vice Society: a discreet but steady double extortion ransomware group

blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group

[Threat & Detection Research Team](#) July 8 2022

2120 0

Read it later Remove

5 minutes reading

Table of contents

This blog post on Vice Society ransomware group was originally published as a FLINT report ([SEKOIA.IO](#) Flash Intelligence) sent to our clients on June 29, 2022.

Vice Society

With Love!

V-society.official@onionmail.org, ViceSociety@onionmail.org

What is Vice Society?

Vice Society is a little-known double extortion group that joined the cybercrime ecosystem a year ago. Since then, it showed a steady activity, encrypting and exfiltrating its victim's data and threatening their victims to leak their information to pressure them into paying a ransom. Unlike other RaaS (Ransomware-as-a-Service) double extortion groups, **Vice Society focuses on getting into the victim system to deploy ransomware binaries sold on Dark web forums.** This is likely a way for this group to save resources in developing its own ransomware.

SEKOIA.IO investigations show they are currently leveraging the Zeppelin ransomware targeting Windows systems, while HelloKitty samples were retrieved from their campaigns targeting Linux systems at the end of 2021. We also believe the group representatives are English native speakers.

Analysis

The Vice Society group mainly targets small or middle-sized companies in human-operated double-extortion campaigns.

Since its launch and until mid-June 2022, the group claimed campaigns targeting at least 88 victims, all of whom are still listed on their dedicated data leak site (DLS).

While some ransomware gangs refrain from targeting healthcare, government and education organisations, Vice Society was not observed applying such restrictions. This group notably targets public school districts and other academic institutions, as 26.1% of the victims listed on their data leak site are educational-related entities. The group also shows a strong focus on the health sector.
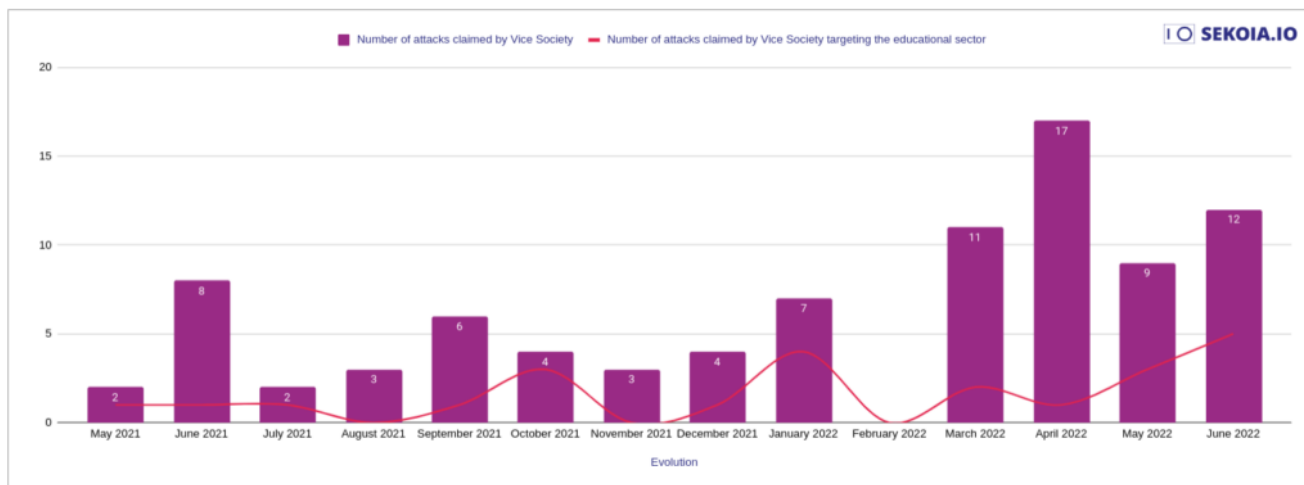
Figure 1. Evolution of publicly disclosed ViceSociety ransomware attacks

When asked by BleepingComputer why it targets healthcare organisations, the group responded with the following message: "Why not? They always keep our private data open. […] they don't even try to protect our data. They have billions of government money. […] USA president gave a big amount to protect government networks and where is their protection? Where is our protection? If the IT department doesn't want to do their job we will do ours and we don't care if it is a hospital or university."
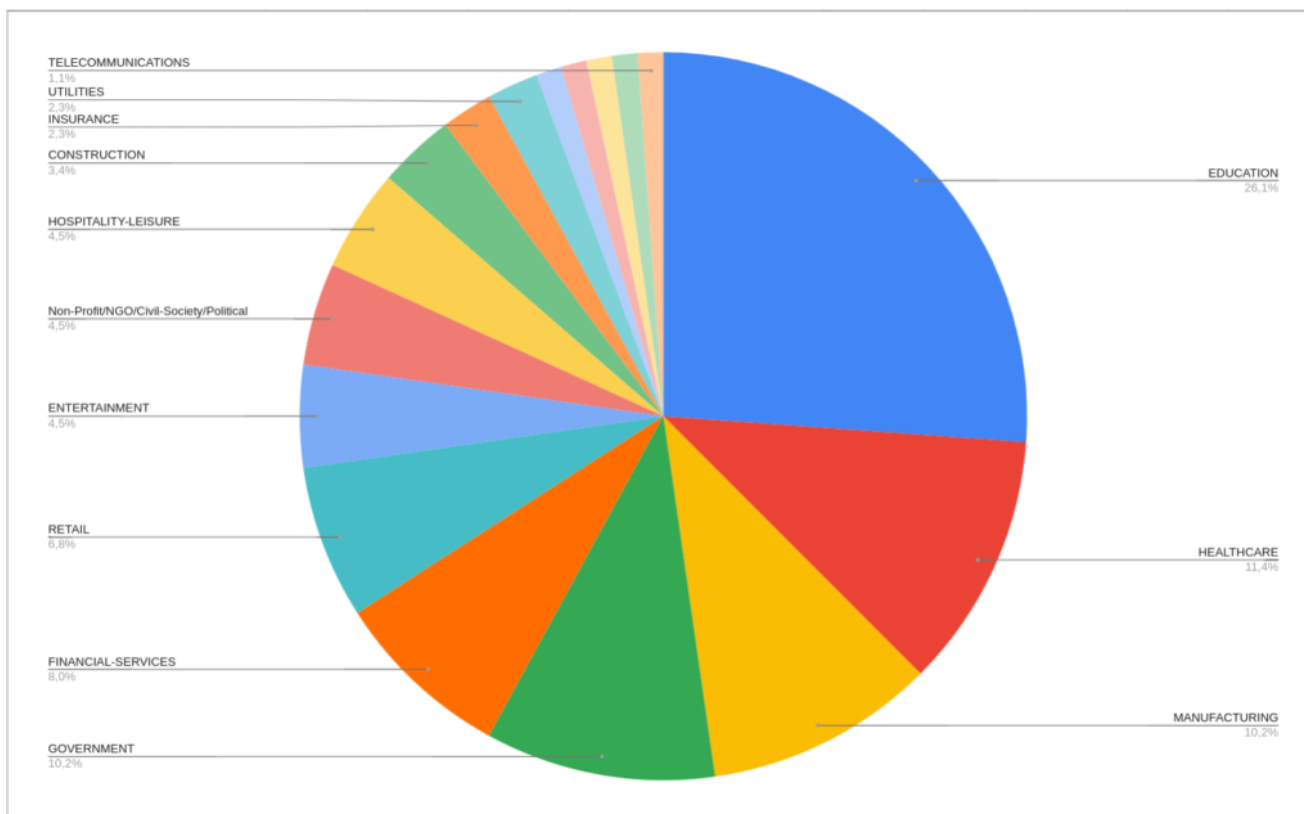

Figure 2. Sectors most impacted by the Vice Society ransomware group

73.9% of known victims of this cybercriminal group are located in France, the United States of America, the United Kingdom, Spain, Italy, Germany and Brazil.
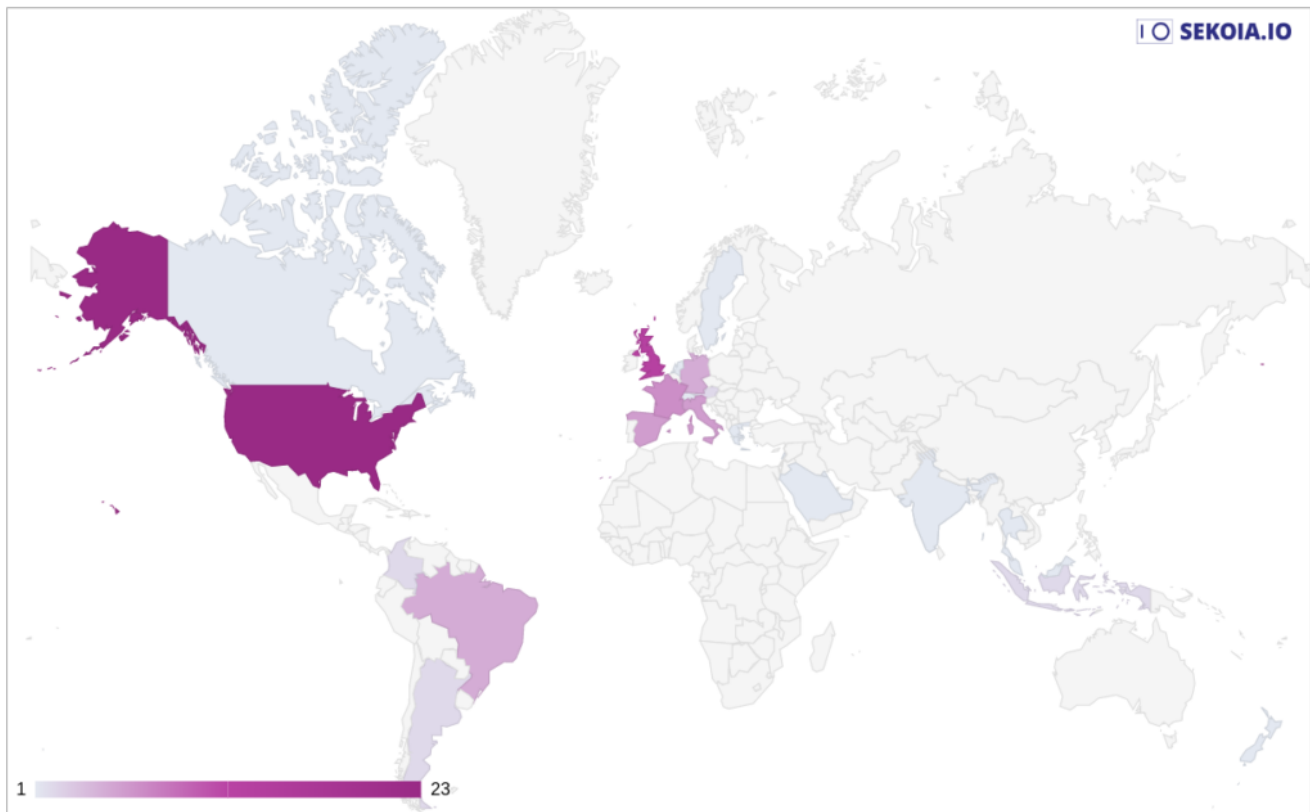
Figure 3. Countries most impacted by the Vice Society ransomware group, by increasing number of attacks

Vice Society Data Leak Site onion displays an old style design and old HTML coding style, it is written in UK English language oftentimes showing a cynical sense of humour. We assess this threat group possibly impersonates a British persona as part of their TTPs.
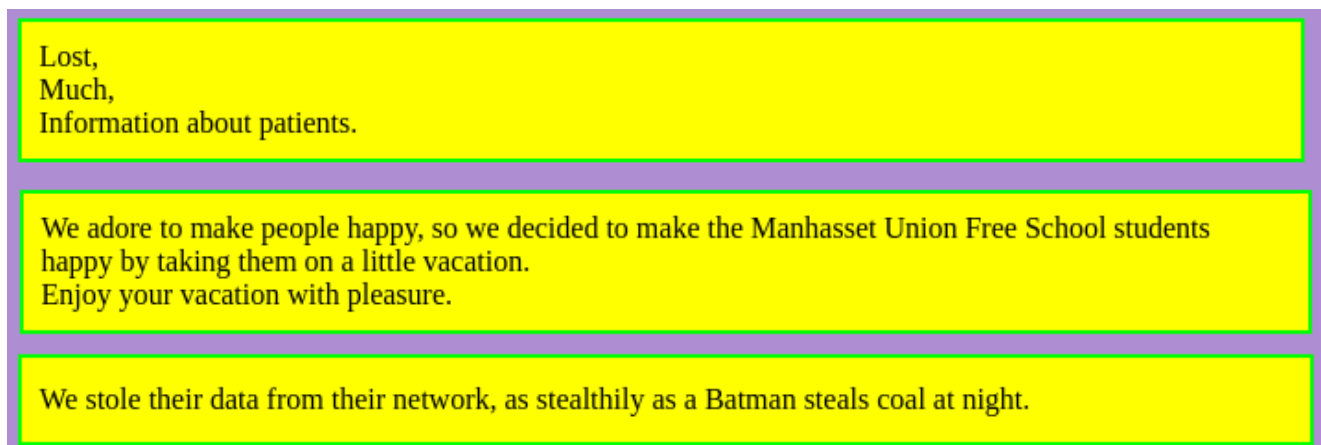

Figure 4. Samples of cynical messages published alongside victims' leak

Vice Society group operators leverage very common pentesters skills, as described by Talos in one of their report. Exploiting publicly available vulnerabilities (such as PrintNightmare) to perform remote code execution seems to be the most advanced technique the group has been observed using. Additionally, Vice Society does not resort to self developed capabilities.

Figure 5. Vice Society ransom note left by a ransomware sample

Based on their ransom note, SEKOIA.IO found several samples embedding this note. While the ransom notes evolved over time, their principal point of contact (v-society[.]official@onionmail[.]org) and DLS remain the same.

Oldest samples from 2021 are HelloKitty ransomware for Linux (ELF binaries), and most recent ones (June 2022) are Zeppelin ransomware. The Zeppelin samples masquerade as legitimate Windows processes and seem to be linked to the PrintNightmare vulnerability exploitation. They are customised for Vice Society (besides the ransom note) with the file encrypted extension using the format ".v-society.XXX-XXX-XXX", which is consistent with other ransomware operators using the Zeppelin ransomware.

The Zeppelin ransomware is offered as a Ransomware-as-a-Service (RaaS) on several Russian-speaking cybercrime forums (such as XSS, BHF, DarkMarket, IFUD). The ransomware developers behind Zeppelin goes under the name "buransupport" and its presence on several underground forums dates back to at least May 2019.

On 5 November 2019, the actors behind the "buransupport" moniker began to advertise a ransomware variant called Zeppelin. At first, the goal was to share the builder in order to obtain some reviews of the new Zeppelin encrypter (based on the VegaLocker and Buran malware).

In June 2021, "buransupport" was advertising an affiliate program for its "Offline ransomware Zeppelin".

ALL YOUR FILES HAVE BEEN ENCRYPTED BY "VICE SOCIETY"
All your important documents, photos, databases were stolen and encrypted.

If you don't contact us in 7 days we will upload your files to darknet.

The only method of recovering files is to purchase an unique private key.
We are the only who can give you tool to recover your files.

To proove that we have the key and it works you can send us 2 files and we decrypt it for free (not more than 2 MB each).

This file should be not valuable!

Write to email: brendaevans4454@onionmail.org

Alternative email: warreinolds77@onionmail.org

Public emai:l v-society.official@onionmail.org

Our tor website: vsociethok6sbprvevl4dlwbqrzyhxcxaqpvcqt5belwvsuxaxsutyad.onion

Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price (they add their fee to ours) or you can become a victim of a scam.

Figure 6. Zeppelin offline crypto-locker advertisement on a cybercrime forum on 13 June 2021

The author of the publication describes the ransomware functionalities, including "a robust crypto algorithm using global and session key + random file keys, scanning of all local drives and all available network paths, high speed, termination of some processes to release open files, possibility to encrypt files without extensions change".

"Buransupport" is still present and active on cybercrime forums, but no activity related to the Zeppelin ransomware was reported in 2022.

SEKOIA.IO assess that the Vice Society group is currently staying under the radar, likely as a way to not attract Law Enforcement Agencies (LEA)'s attention and continue their activities in the long term.

As for the low number of ViceSociety related samples found in public repositories SEKOIA.IO assess it is possibly linked to the lack of cybersecurity resources of their main targeted verticals – healthcare and education. An other possible explanation, as described by Talos, is that their Defensive evasion techniques (*e.g.* deleting security logs), limit the possibility of investigating during post-incident.

Vice Society ransomware IOCs

HelloKitty samples from end of 2021 (for Linux) with Vice Society ransom note:

```
78efe6f5a34ba7579cfd8fc551274029920a9086cb713e859f60f97f591a7b04
```

```
754f2022b72da704eb8636610c6d2ffcbdae9e8740555030a07c8c147387a537
```

Recent samples (may 2022), using Zeppelin ransomware with the Vice Society ransom note. Some of these samples use Windows binary names.

24efa10a2b51c5fd6e45da6babd4e797d9cae399be98941f950abf7b5e9a4cd7

307877881957a297e41d75c84e9a965f1cd07ac9d026314dcaff55c4da23d03e

Ab440c4391ea3a01bebbb651c80c27847b58ac928b32d73ed3b19a0b17dd7e75

Aa7e2d63fc991990958dfb795a0aed254149f185f403231eaebe35147f4b5ebe

bafd3434f3ba5bb9685e239762281d4c7504de7e0cfd9d6394e4a85b4882ff5d

YARA

https://github.com/reversinglabs/reversinglabs-yara-rules/blob/develop/yara/ransomware/Win32.Ransomware.Zeppelin.yara

References

If you liked this article, you can also read our blog post: XDR vs Ransomware.

Chat with our team!

Would you like to know more about our solutions? Do you want to discover our XDR and CTI products? Do you have a cybersecurity project in your organization? Make an appointment and meet us!

Contact us