

W4 Jan | EN | Story of the week: Ransomware on the Darkweb

 medium.com/s2wlab/w4-jan-en-story-of-the-week-ransomware-on-the-darkweb-7595544363b1

Hyunmin Suh

March 15, 2021



[Hyunmin Suh](#)

Jan 26, 2021

.

4 min read

It ain't over yet till the DDoS Sings



S2W LAB publishes weekly reports of the Ransomware activities that took place at Dark Web. Report includes summary of victimized firms, Top 5 targeted countries and industrial sectors, status of dark web forum posts by ransomware operator, etc.

Executive Summary

The number of victimized firms uploaded on the darkweb ransomware site decreased (-22) compared to the past week, and the number of ransomware groups remained same. Industrials sector still positioned at the highest proportion of the industries, but Services sector seemed to increase rapidly which needs to receive careful attention.

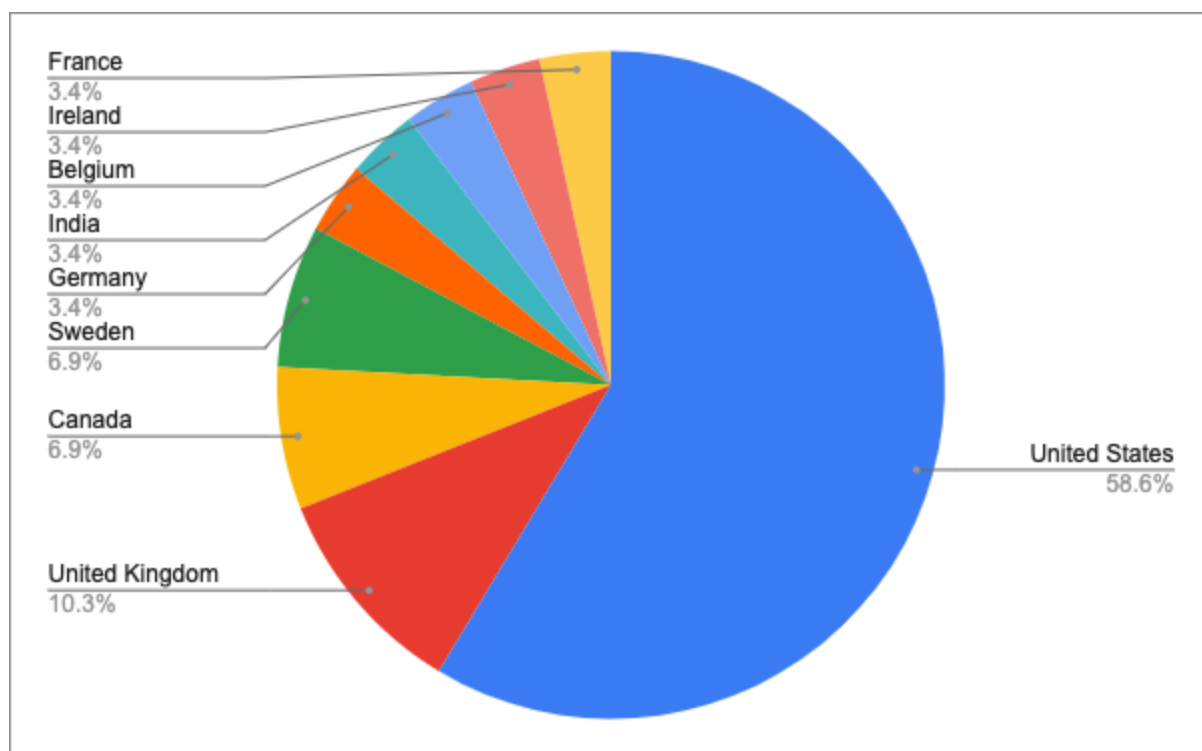
Looking back to our previous story, Avaddon mentioned ‘arsenal to “persuade”’ which turned out to be a DDoS attack against victimized firms. As Avaddon seems to be attempting a variety of arsenals to negotiate, victimized firms need to be aware of the secondary attack.

1. Weekly Status

A. Status of the victimized firms (01/18 ~ 01/24)

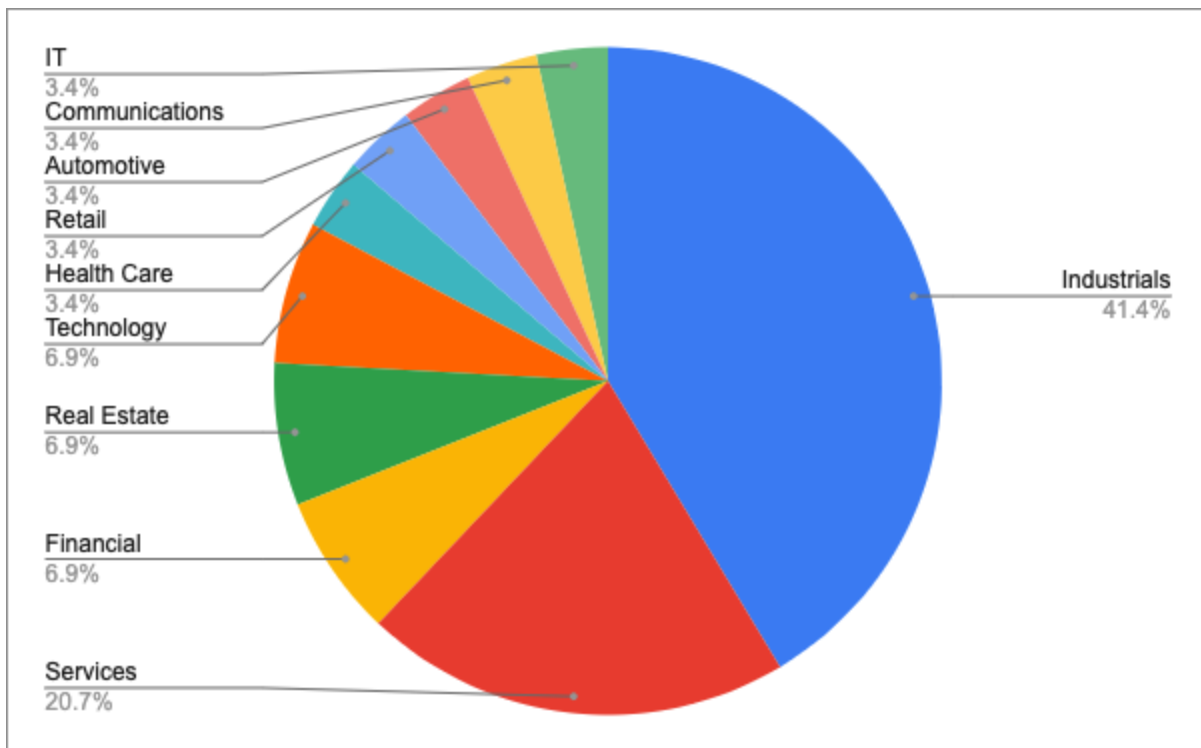
- For a week, were mentioned and a change in the state of the data leaked from the victim company in the ransomware site was detected.
- Activity from detected

B. TOP 5 targeted countries



1. United States — 58.6%
2. United Kingdom — 10.3%
3. Canada — 6.9%
4. Sweden — 6.9%
5. Germany — 3.4%

C. TOP 5 targeted industrial sectors



1. Industrials — 41.4%
2. Services — 20.7%
3. Financial — 6.9%
4. Real Estate — 6.9%
5. Technology — 6.9%

2. Status of active Ransomware forum posts @ Dark Web

A. Avaddon

- Exploit[.]IN, XSS[.]IS
- Avaddon
- 06/03/2020
-

| Weekly Summary of Activity

Avaddon
kilobyte
●●

Posted 14 hours ago (edited) Report post ↗

We are working, ready to accept adverts on networks and rdp

Networkers start 25/75
RDP start 30/70

From news:

- Rolled out support for XP and 2003 win
- Updated the locker, added new functionality
- Ran through the panel and made a couple of new features
- Tried new ways to pressure corpses

Articles: <https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/>

Edited 14 hours ago by Avaddon

+ Quote 🗨

BLOG AVADDON: avaddongun7rngel.onion ✕

- 01/26/2021
- Rolled out Windows OS support for XP and 2003
- Updated the locker with new functions
- Ran through the panel adding couple of new features
- Tried new ways to pressure victims
- Related article:

Referring to previous SoW...

Avaddon
kilobyte
●●

Posted Sunday at 09:49 AM Report post ↗

We are working, ready to accept networkers with a start rate of 25/75. RDP start 35/65.

We can also accept English-speaking ads if you have a reputation or a deposit.

From the news:

- The development of the HP locker and much more is underway.
- Several new ways have been added to our arsenal to "persuade" the office to cooperate.
- We also actively cooperate with the recovery offices.

+ Quote 🗨

BLOG AVADDON: avaddongun7rngel.onion ✕

- The phrase 'arsenal to "persuade"' mentioned by Avaddon in the previous post turns out to be a DDoS attack against victimized firms.
- The size of DDoS is clearly mentioned but the harassment of the victims will intensify in order to give a huge pressure.

Articles & Analysis report on Avaddon

Avaddon Ransomware Analysis Article

- Trend Micro (07/08/2020) 'Ransomware Report: Avaddon and New Techniques Emerge, Industrial Sector Targeted'

- Related article:

B. Babuk

- Raidforums
- biba99
- 08/26/2020
-

| Weekly Summary of Activity



- 01/21/2021
- Babuk Locker version supports linux based (*nix) Virtual Servers (esxi) and NAS

| Articles & Analysis report on Babuk

Babuk Locker Analysis Article

- Bleeping Computer (01/05/2021) 'Babuk Locker is the first new enterprise ransomware of 2021'
- Related article:

C. Lockbit

- Exploit[.]IN, XSS[.]IS
- LockBit
- 01/17/2020
-

| Weekly Summary of Activity

LockBit
kilobyte

Posted Thursday at 03:36 PM

No way. Wait for LockBit 2.0. No set.

+ Quote


Seller
3
40 posts
Joined
01/16/20 (ID: 99278)
Activity
other / other
Deposit
10B

- 01/21/2021
- Reply post implying that new Lockbit 2.0 is undergoing

For Reminder, Lockbit's first post

LockBit
kilobyte

Posted January 17, 2020 (edited)



Seller
3
40 posts
Joined
01/16/20 (ID: 99278)
Activity
other / other
Deposit
10B

The development of the lockbit has been going on since September 2019, they could not decipher it, there were attempts. There are no school emails, multithreading, which, in fact, loads the system more than encrypts, there is no.

The software is written in C and assembler, **encryption through the IO completion port**, a port scanner on local subnets, **finds all DFS, SMB, WebDav balls**, admin panel in the torus, automatic test decryption, issuing a decryptor, chat with PUSH notifications, **Jabber bot sending correspondence**, shutting down services / processes on the list and preventing the file from being opened at the moment. Setting file permissions and removing blocking attributes, deleting shadow copies, clearing logs, mounting hidden partitions, drag'n'drop files and folders, console / hidden mode of operation. Encrypts files in chunks in different places, the larger the file size, the more chunks. Algorithm AES + RSA.

The ransom amount is determined by you after communicating with the terpila, you receive payment to your wallets, in a convenient currency. Jabber bot completely replaces the admin panel, ban, decrypt, chat - all this without leaving the jabber.

Work speed clearly

Disk	1216 MB/sec Disk I/O
Network	775 Mbps Network I/O

M.2 SSD

Монитор ресурсов

Файл Монитор Справка

Обзор ЦП Память Диск Сеть
ЦП 80% - использование ЦП
Диск 2799 МБ/с - дисковый ево...

We do not work in the CIS. We negotiate the terms of renting software individually. We are not chasing the number of advertisers, we are interested in quality. The first decrypt is free as a test. English-speaking software can be provided only with a Russian-speaking guarantor. For those who have experience of working with another PP, that is, they know what to do, do not ask unnecessary questions, regularly pay%, are ready to provide software on more favorable terms.

For contact in PM.

Edited May 28, 2020 by LockBIT

LockBit Ransomware Analysis Article

- Sophos News (04/24/2020) 'LockBit ransomware borrows tricks to keep up with REvil and Maze'
- Related article: