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

By Hyunmin Suh

Published: 2021-03-15 · Archived: 2026-04-05 14:25:38 UTC

It ain’t over yet till the DDoS Sings

Press enter or click to view image in full size

> 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.

Get Hyunmin Suh’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

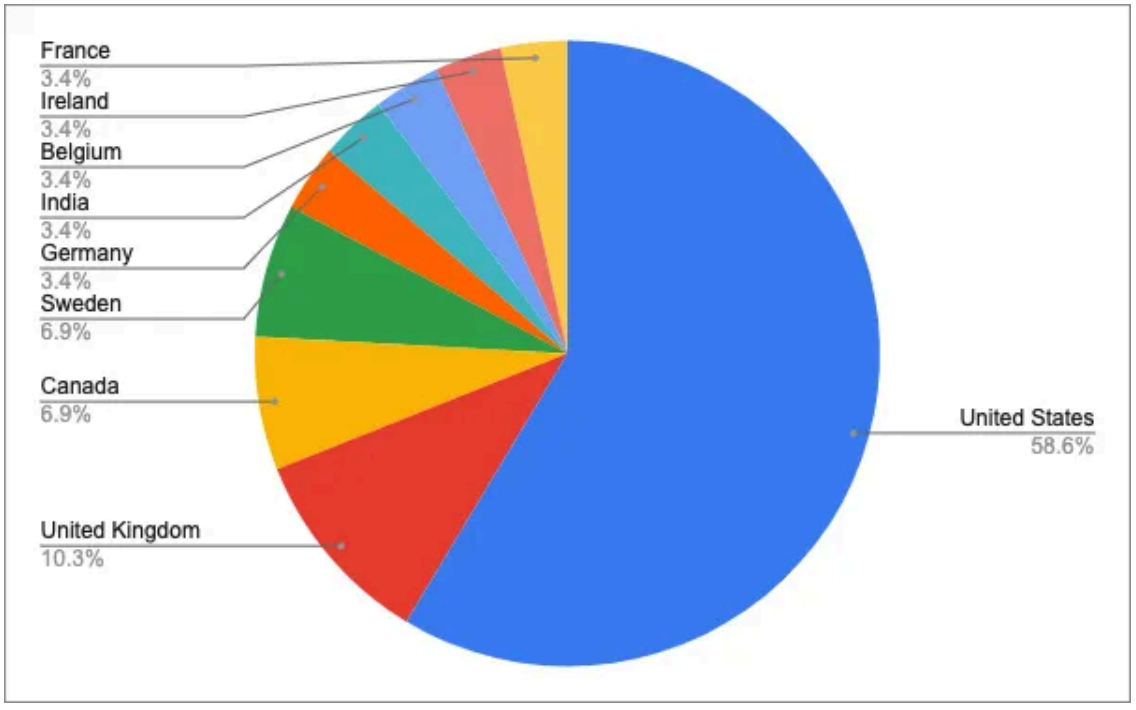
Looking back to our previous story, Avaddon mentioned ‘arsenal to “persuade”’ which turned out to be a DDoS attack against victimized firms. As Avaddon seems to be attempting a variety of arsenals to negotiate, victimized firms need to be aware of the secondary attack.

1. Weekly Status

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

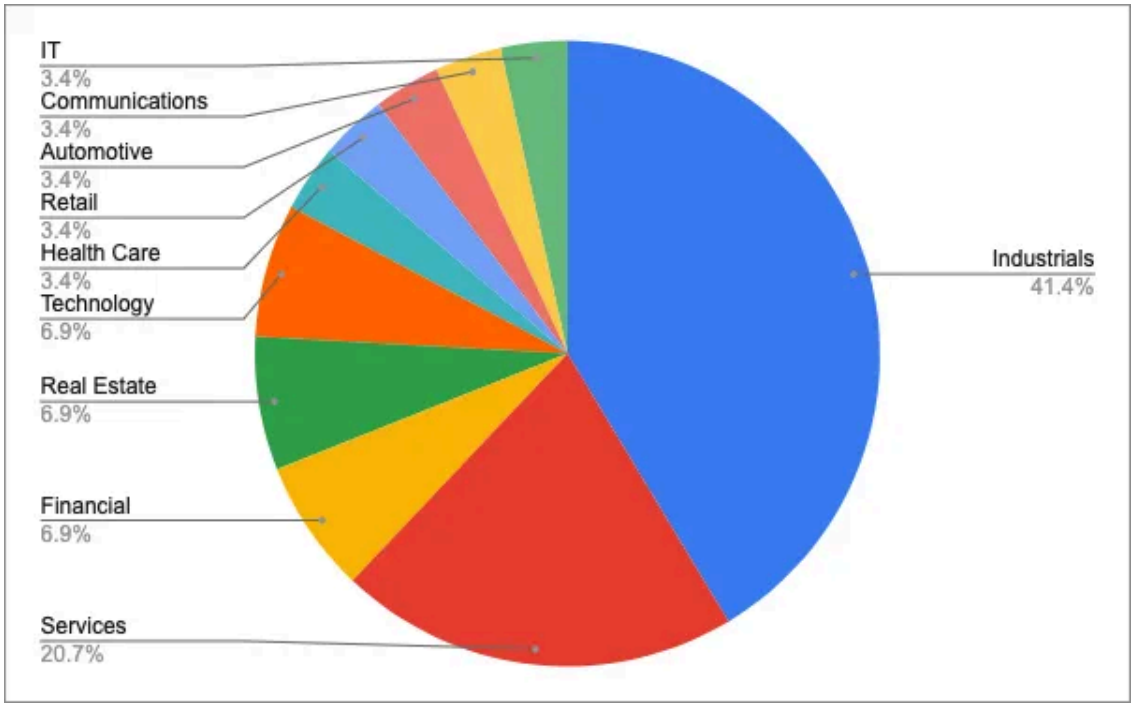
- For a week, **a total of 29 companies** were mentioned and a change in the state of the data leaked from the victim company in the ransomware site was detected.
- Activity from **7 threat groups** detected

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

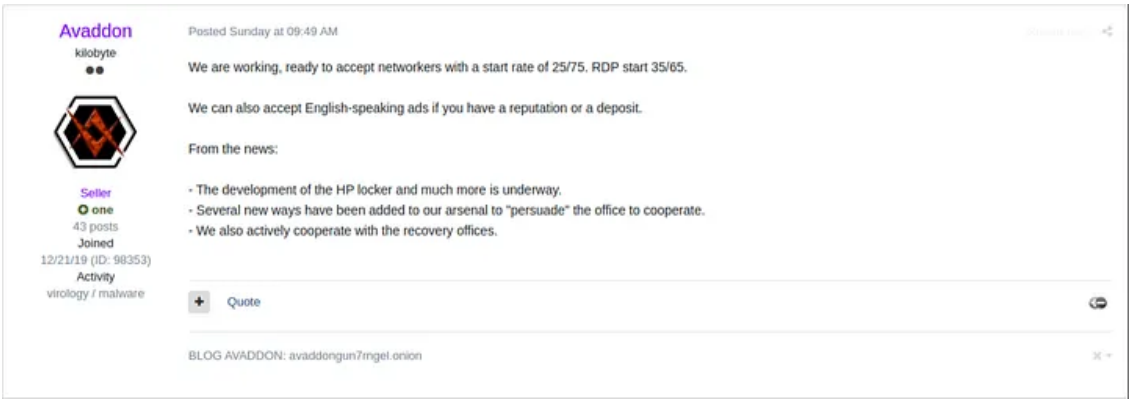
- **Forums:** Exploit[.]IN, XSS[.]IS
- **User ID:** Avaddon
- **Initial Date of Activity:** 06/03/2020
- **Leaked Site in Operation (Y/N): Y**

> **Weekly Summary of Activity**
>
> Press enter or click to view image in full size

- **Posted Date:** 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: https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/

> **Referring to previous SoW…**

Press enter or click to view image in full size



- 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: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted

B. Babuk

- **Forums:** Raidforums
- **User ID:** biba99
- **Initial Date of Activity:** 08/26/2020
- **Leaked Site in Operation (Y/N): Y**

> **Weekly Summary of Activity**

Press enter or click to view image in full size

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

> **Articles & Analysis report on Babuk**

Babuk Locker Analysis Article

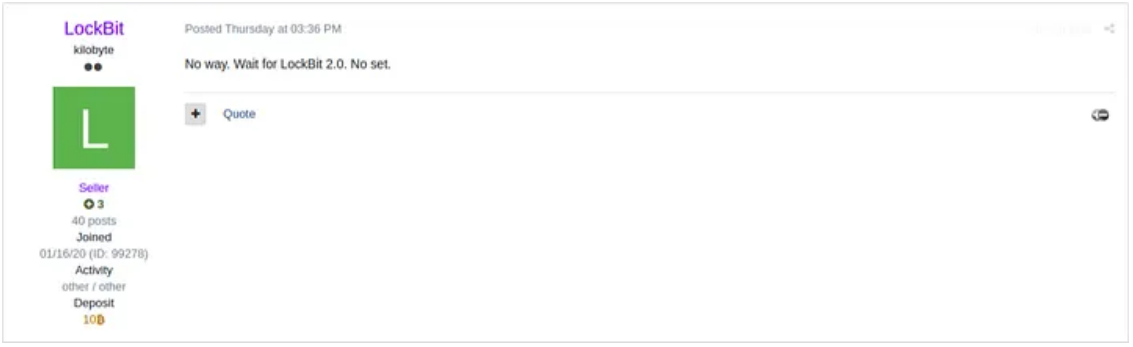
- Bleeping Computer (01/05/2021) ‘Babuk Locker is the first new enterprise ransomware of 2021’
- Related article: https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/

C. Lockbit

- **Forums:** Exploit[.]IN, XSS[.]IS
- **User ID:** LockBit
- **Initial Date of Activity:** 01/17/2020
- **Leaked Site in Operation (Y/N): Y**

> **Weekly Summary of Activity**

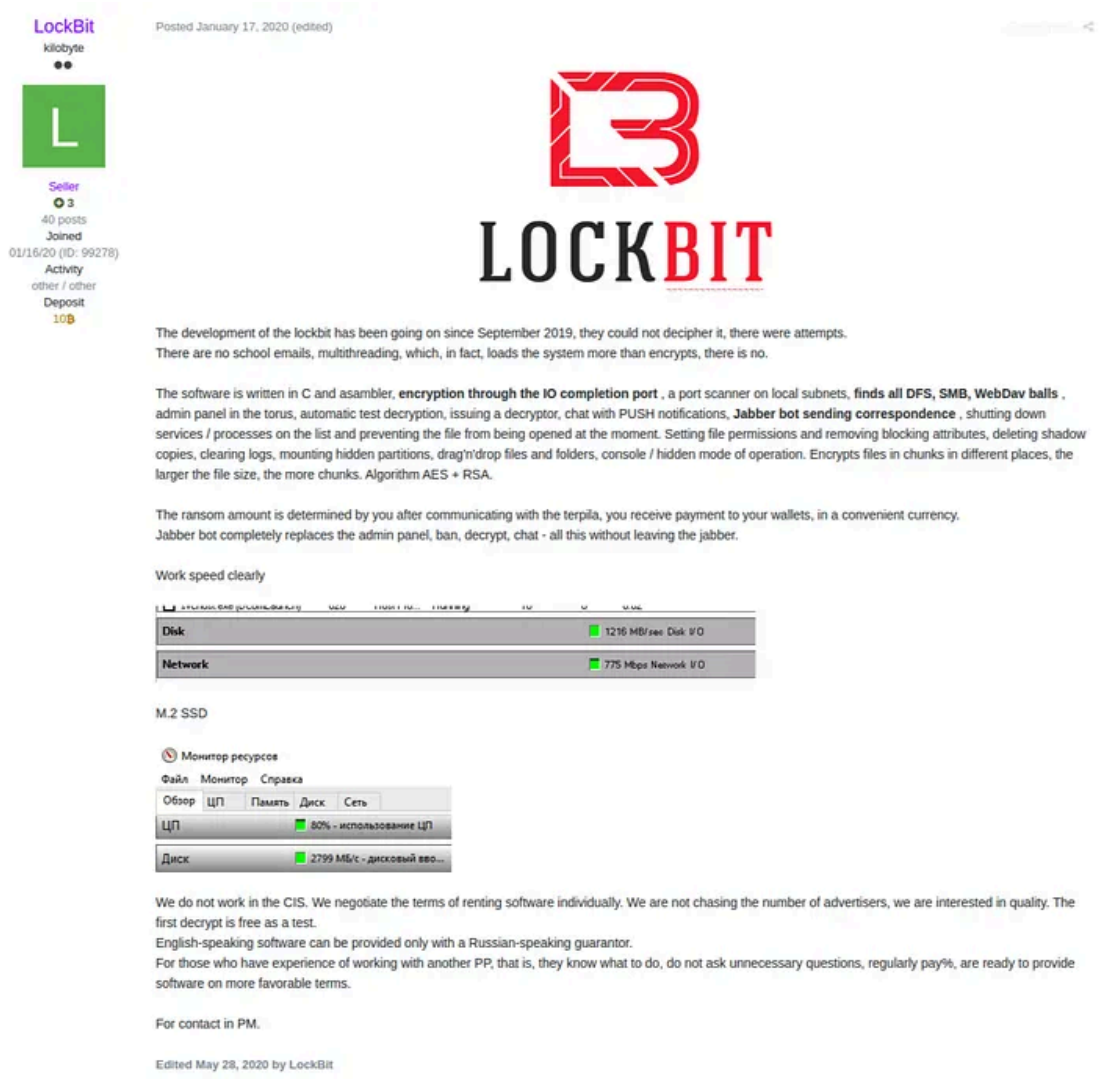
Press enter or click to view image in full size



- **Posted Date:** 01/21/2021
- Reply post implying that new Lockbit 2.0 is undergoing

For Reminder, Lockbit's first post

Press enter or click to view image in full size



> ### Articles & Analysis report on Avaddon

LockBit Ransomware Analysis Article

- Sophos News (04/24/2020) ‘LockBit ransomware borrows tricks to keep up with REvil and Maze’
- Related article: https://news.sophos.com/en-us/2020/04/24/lockbit-ransomware-borrows-tricks-to-keep-up-with-revil-and-maze/

- https://www.s2wlab.com
- Facebook https://www.facebook.com/S2WLAB/
- Twitter https://twitter.com/s2wlab
