# Lockbit 3.0: Another Upgrade to World's Most Active Ransomware

socradar.io/lockbit-3-another-upgrade-to-worlds-most-active-ransomware/

April 6, 2022


Lockbit Ransomware gang, also known as Bitwise Spider, are the cybercriminal masterminds behind the popular Lockbit Ransomware-as-a-service. They are one of the most active ransomware gangs with generally multiple victims per day, sometimes higher. On March 16, 2022, they began continuously announcing new victims on their **Dark Web site** much faster than any ransomware group. SOCRadar has detected more than 22 victims in 48 hours.

## Origins of the Lockbit Ransomware

They have begun their operations in September 2019 as ABCD ransomware and then changed its name to Lockbit. They have rebranded and came back with even better ransomware on June 2021, as **Lockbit 2.0**. We have seen that the Lockbit 2.0 ransomware introduced new features such as shadow copy and **log file deletion** to make recovery harder for the victims. In addition, Lockbit has the fastest encryption speed among the most popular ransomware gangs, with around 25 thousand files encrypted in under one minute.

The gang is believed to be originated in Russia. According to a detailed analysis of Lockbit 2.0, the ransomware checks the default system language and avoids encryption, and stops the attack if the **victim system's** language is Russian or the language of one of the nearby

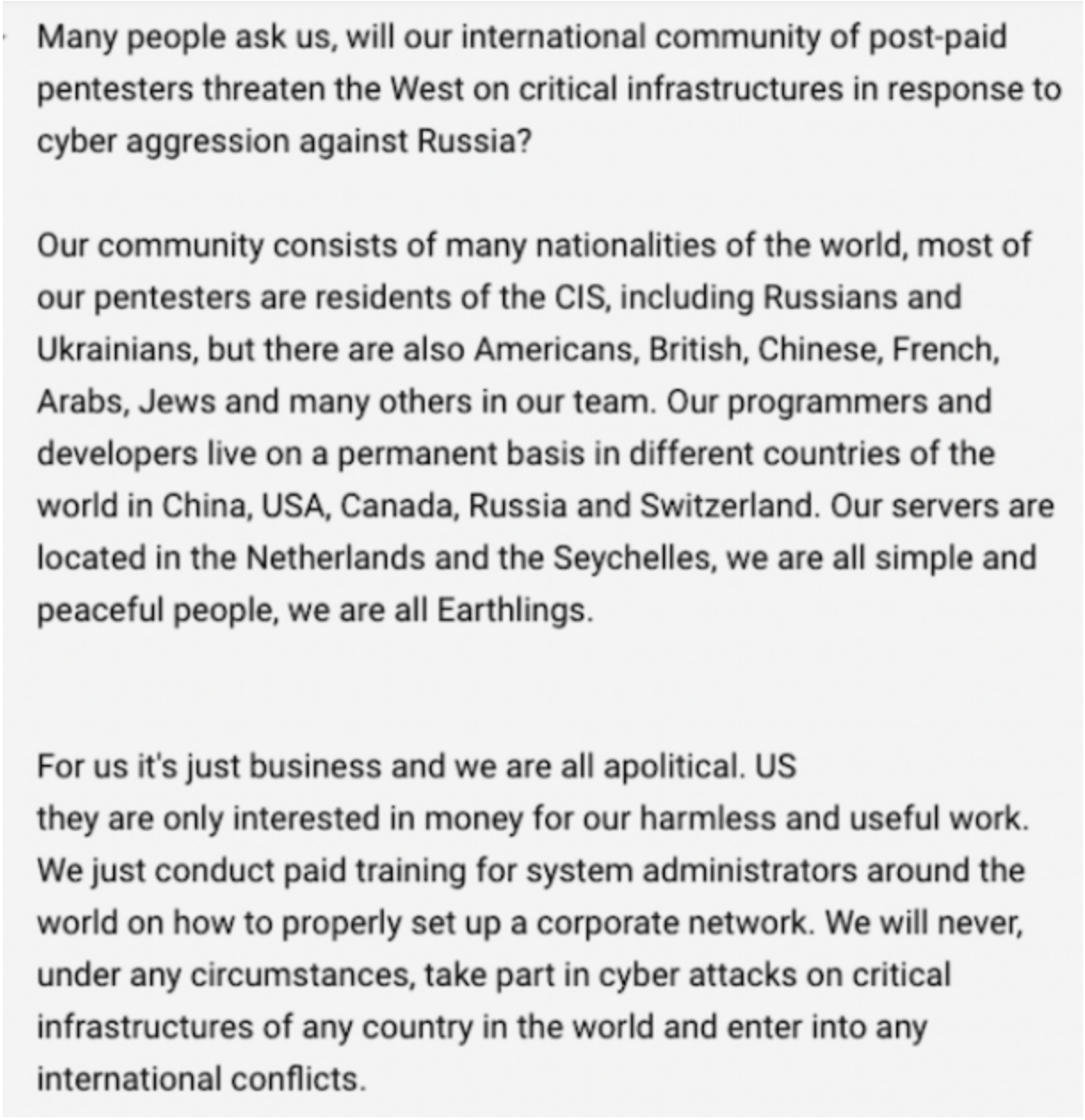
countries.

```
  GetSystemDefaultUILanguage = (v0 + *(v97[7] + 4 * *(v97[9] + 2 * v105 + v0) + v0));
LABEL_28:
  GetSystemDefaultUILanguage_1 = GetSystemDefaultUILanguage;
LABEL_29:
  sys_def_UI_lang = GetSystemDefaultUILanguage();
  if ( sys_def_UI_lang != 0x82C                 // Azerbaijani (Cyrillic, Azerbaijan)
    && sys_def_UI_lang != 0x42C                 // Azerbaijani (Latin, Azerbaijan)
    && sys_def_UI_lang != 0x42B                 // Armenian (Armenia)
    && sys_def_UI_lang != 0x423                 // Belarusian (Belarus)
    && sys_def_UI_lang != 0x437                 // Georgian (Georgia)
    && sys_def_UI_lang != 0x43F                 // Kazakh (Kazakhstan)
    && sys_def_UI_lang != 0x440                 // Kyrgyz (Kyrgyzstan)
    && sys_def_UI_lang != 0x819                 // Russian (Moldova)
    && sys_def_UI_lang != 0x419                 // Russian (Russia)
    && sys_def_UI_lang != 0x428                 // Tajik (Cyrillic, Tajikistan)
    && sys_def_UI_lang != 0x442                 // Turkmen (Turkmenistan)
    && sys_def_UI_lang != 0x843                 // Uzbek (Cyrillic, Uzbekistan)
    && sys_def_UI_lang != 0x443                 // Uzbek (Latin, Uzbekistan)
    && sys_def_UI_lang != 0x422 )               // Ukrainian (Ukraine)
  {
    goto LABEL_72;
  }
```

Lockbit 2.0 checks the language of the victim machine

## Lockbit on Russia – Ukraine Cyberwar

In the cyber crisis between Russia and Ukraine, which began on February 23rd, 2022, Lockbit announced that it would not participate in the **cyberattacks**. They announced that they would not take part in cyberattacks on international conflicts. They are only in it for the business and do not care about politics. Another very active ransomware gang also believed to be from Russia, Conti, had stated that they would be siding with Russia, which some members of Conti were not pleased with. Following the events, some insider members of **Conti** began leaking internal chat logs and source code for the Conti locker and decryptor. You can read more about the Conti Leaks in our blog post.


Many people ask us, will our international community of post-paid pentesters threaten the West on critical infrastructures in response to cyber aggression against Russia?

Our community consists of many nationalities of the world, most of our pentesters are residents of the CIS, including Russians and Ukrainians, but there are also Americans, British, Chinese, French, Arabs, Jews and many others in our team. Our programmers and developers live on a permanent basis in different countries of the world in China, USA, Canada, Russia and Switzerland. Our servers are located in the Netherlands and the Seychelles, we are all simple and peaceful people, we are all Earthlings.

For us it's just business and we are all apolitical. US
they are only interested in money for our harmless and useful work. We just conduct paid training for system administrators around the world on how to properly set up a corporate network. We will never, under any circumstances, take part in cyber attacks on critical infrastructures of any country in the world and enter into any international conflicts.

Lockbit's announcement on the Russia-Ukraine Cyberwar

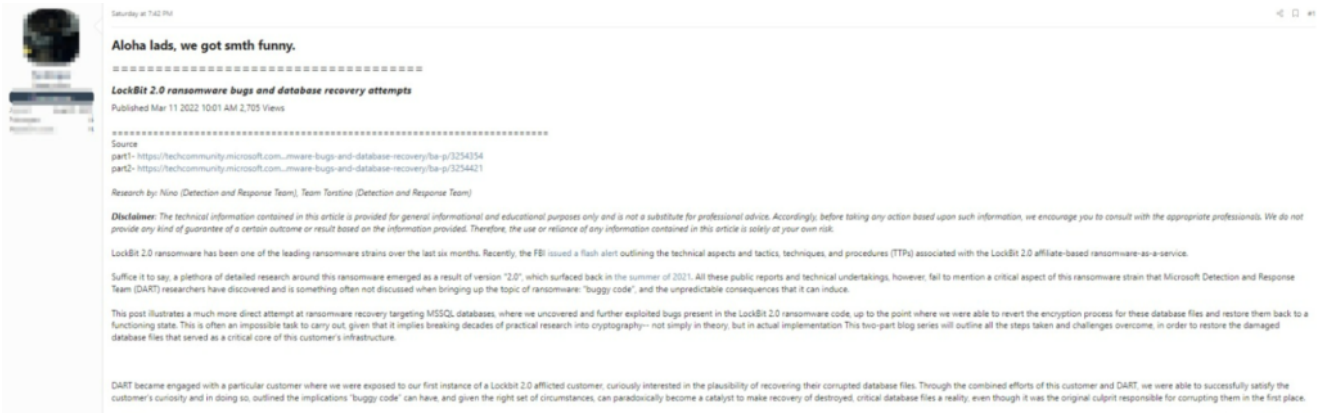
A funny detail about the gang is that they are confident in their skills and arrogant. On March 25, 2022, a member of Lockbit has announced on a hacker forum that they'll be giving a million dollars to an FBI agent who can doxx them, placing a million-dollar bounty on its own head.

A member of Lockbit placing bounty on its own head

## Dark Web Gossips: Lockbit 3.0 Emerging

FBI's cyber division published an FBI Flash security advisory on Lockbit 2.0's **Indicators of Compromise (IOCs)** on March 4th, 2022. After the FBI's advisory, a user in a Dark Web forum has posted a forum entry with the title "Kockbit fuckup thread." In the post, the user addresses the bugs found in Lockbit 2.0 ransomware and a recovery method for the victims, addressing the FBI's advisory along with Microsoft's Detection and Response Team's (DART's) research on Lockbit. Below, you can find the links for Microsoft DART's research. Microsoft DART researchers have discovered a method by uncovering and exploiting bugs found in the Lockbit 2.0 ransomware, enabling them to successfully revert the encryption process on an MSSQL database of one of Lockbit's victims.

- https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-1-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254354
- https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-2-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254421



Dark web forum post on Lockbit bugs and a recovery method

A member of the Lockbit ransomware group has commented on the post explaining the reason for the MSSQL bug. The Lockbit member says the bug will not exist in Lockbit 3.0, signaling the newest version's release.


Lockbit member's comment on the post

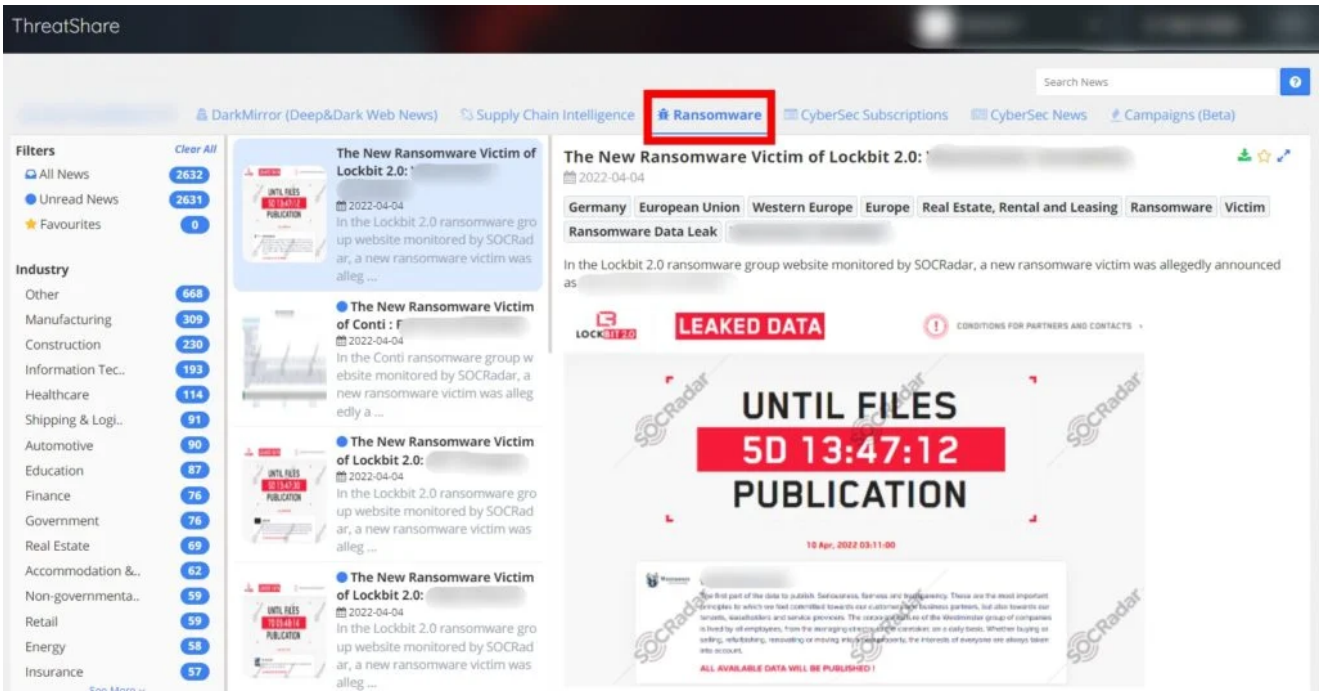
After a couple of days, on March 17, the cyber research team **vx-underground** has posted a screenshot of their talks with one of Lockbit's associates. On the screenshot, the vx-underground researcher asks when Lockbit 3.0 is being released, and the Lockbit affiliate says the newest version will be released in one or two weeks.


Source: vx-underground

The Lockbit group is still using the Lockbit 2.0 name, but we can expect an update in the following month. It has been two weeks since vx-underground tweeted their conversation with the Lockbit affiliate, but the Lockbit team has no deadline to uphold. They can release the new version whenever they want.

The new features and upgrades in Lockbit 3.0 is still a mystery. **SOCRadar CTIA** team will follow the updates regarding Lockbit 3.0 and bring you the latest updates.,

## Stay Up-to-date About Lockbit and Other Ransomware Groups




SOCRadar's ThreatShare keeps you updated about ransomware gangs

SOCRadar's Extended Threat Intelligence module, **ThreatShare**, allows you to keep up to date with the developments regarding ransomware groups by following communication channels such as deep and darknet forums, social media, Telegram, ICQ, etc. Shares along with screenshots and texts.

SOCRadar's analyst team translates the collected raw data into contextual intelligence and presents it in a searchable interface. It helps your SOC team develop security strategies based on country, sector, or region.

Discover SOCRadar® Free Edition

With SOCRadar® Free Edition, you'll be able to:

- Discover your unknown hacker-exposed assets
- Check if your IP addresses tagged as malicious
- Monitor your domain name on hacked websites and phishing databases
- Get notified when a critical zero-day vulnerability is disclosed

Free for 12 months for 1 corporate domain and 100 auto-discovered digital assets. Get free access.