LockBit 3.0: “Making the ransomware great again”

cluster25.io/2022/07/06/lockbit-3-0-making-the-ransomware-great-again/

July 6, 2022

LockBit is a major player in the ransomware scene and has contributed heavily for this cyber-crime model to become one of the most popular and imitated in the threats landscape. The version 2.0 of its project entered the scene in July 2021 showing immediately the potential to become one of the leading syndicate in this “business”. The collective distinguished itself for having pointed out some distintive technical characteristics of its product and for several public statements where the speed

and efficiency of its ransomware have been defined, by gang representatives, “unmatched” if compared to what the community had been able to observe up to that moment. Always according to LockBit members the 2.0 project could count on:

1. The fastest encryption speed on the market
2. A tool specifically aimed at data exfiltration
3. Automated mechanisms for payload distribution and data encryption

Recently, on 27 of June, 2022, LockBit released the third version of its project and many new features seem to have been included in it. For example one main thing to note that differs from the 2.0 is the fact that the group has come up with another way to pressure and extort its victims. Like other threat groups, LockBit works mainly through its own DLS (Data Leak Site) through which it manages and deals with the victims of its operations. Until now, these victims were given a well-defined period of time to pay the requested ransom. In project 3.0 the collective seems to have included new possibilities for negotiations; Indeed, by paying a specific fee is now possible to extend the timer by 24 hours, destroy all data from the website, or download all data right away. This could be a way also to cover the extortion technique, not making public the actual ransom price. Basically, they are maximizing the money they can get from each victim. Another interesting aspect of this third version is the **Bug Bounty Program**; this appears to be an initiative never taken from any other group before. The group not only offers rewards for
finding vulnerabilities or for doxxing the managers but is rewarding for “brilliant ideas” to be added in the R-a-a-S as well. Currently, however, it’s to be pointed out that the group is continuing to update also the LockBit 2.0 DLS, where new victims have recently been added.

LockBit 3.0

Cluster25 obtained a sample of **LockBit 3.0** and analyzed it in order to understand its functionalities and its behavior. During the analysis also emerged interesting similarities between this version and samples related to other ransomware families (**BlackMatter**/**DarkSide**) that may suggest a possible correlation between threat groups behind the development of this piece of malware. The new version of LockBit (**Lockbit 3.0** or **LockBitBlack**) uses a code protection mechanism consisting in the presence of encrypted code sections in the binary, so to hinder the malware detection, especially when performed through automated analysis. To activate the proper execution of the malware, a **decryption key** must be provided as a **parameter** (**-pass**) when the malicious file is launched, and without this key its behavior just results in a software crash at the beginning of its execution. The decryption key used for the analyzed sample is reported below:

db66023ab2abcb9957fb01ed50cdfa6a

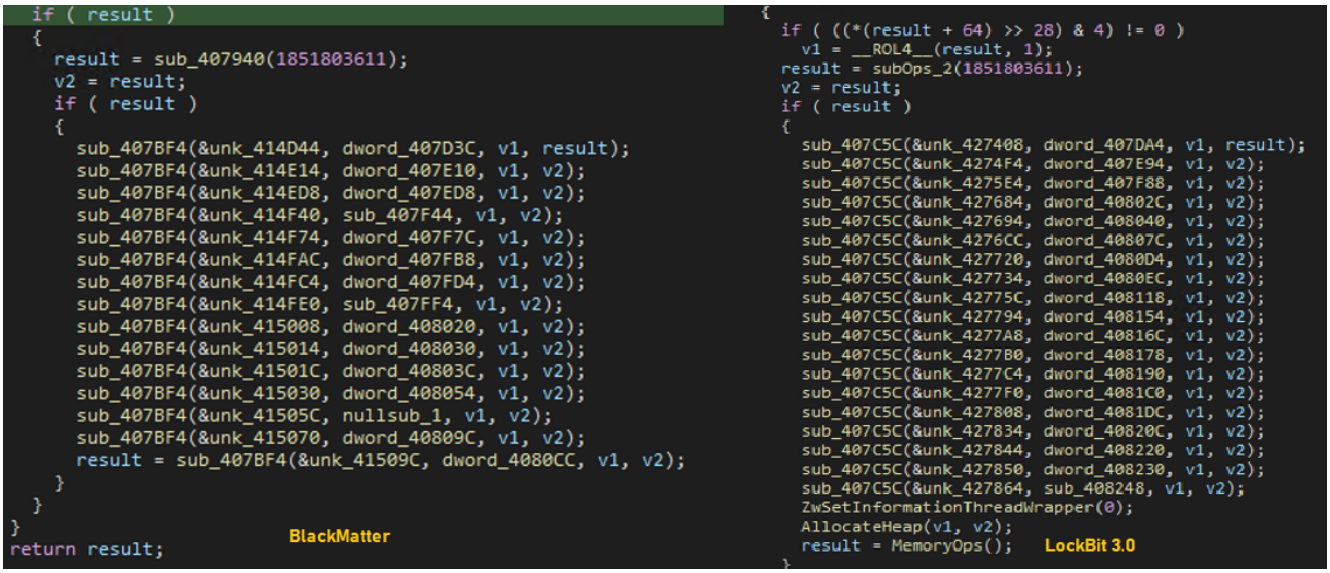
When the program starts, the fist subroutine to be called (**sub_41B000**) is responsible to perform the decryption of the sections of the binary, by retrieving the decryption key from the execution parameters and by passing it through a **RC4 Key Scheduling Algorithm (KSA)** algorithm. Later, the sections to decrypt are accessed by reading the **Process Environment Block** (PEB) and the decryption takes place, according to evidence below:

```
launch_command = GetLaunchCommand();
v2 = sub_41B248(launch_command, v8);
if ( v2 )
{
  sub_41B2F4(v11, v8);
  v10 = RC4_KSA(v11, v12, v9);
  ImageBaseAddress = GetPeb()->Mutant;
  section = ImageBaseAddress + ImageBaseAddress[15];
  to_decrypt_length = *(section + 3);
  section_to_decrypt = section + 248;
  do
  {
    v2 = sub_41B0EC(section_to_decrypt, 0);
    if ( v2 == 0x76918075 || v2 == 0x4A41B || v2 == 0xB84B49B )
      LOBYTE(v2) = DoCodeDecription(ImageBaseAddress + *(section_to_decrypt + 3), *(section_to_decrypt + 4), v9, v10);
    section_to_decrypt += 40;
    --to_decrypt_length;
  }
  while ( to_decrypt_length );
}
return v2;
}
```

An anti-Analysis mechanism implemented by the malware regards the **dynamic loading of the Win32 APIs** needed to perform its malicious behavior. The subroutine responsible to load and map the needed APIs into memory is analyzable only on the decrypted/unpacked version of the malware. The way the APIs are resolved consists in a call to a subroutine (**sub_407C5C**) that receives as input an obfuscated string that is **XORed** with the key **0x4506DFCA**, so to decrypt the **Win32 API** name to be resolved.

```
v4 = a2 + 1;
result = sub_407AE0(*a2 ^ 0x4506DFCA);
if ( result )
{
  v6 = (a1 + 4);
  while ( 1 )
  {
    result = *v4++;
    if ( result == -858993460 )
      break;
    v7 = subOps_2(result ^ 0x4506DFCA);
    v8 = a4(a3, 0, 16);
    if ( *(v8 + 16) != -1414812757 )
      *v6++ = v8;
    *v8 = -72;
    v9 = Selector(0, 4u);
    if ( v9 )
    {
      switch ( v9 )
      {
        case 1u:
          v13 = Selector(1u, 9u);
          *(v14 + 1) = __ROR4__(v7, v13);
          *(v14 + 5) = -16191;
          *(v14 + 7) = v13;
          *(v14 + 8) = -7937;
          break;
        case 2u:
          *(v10 + 1) = v7 ^ 0x4506DFCA;
```

Furthermore, the analysis showed an interesting similarity between this subroutine and the one used in the **BlackMatter** ransomware. In fact, the above-mentioned decryption steps are present in both the malware, as also visible in the screenshot below, taken from a **BlackMatter** sample:

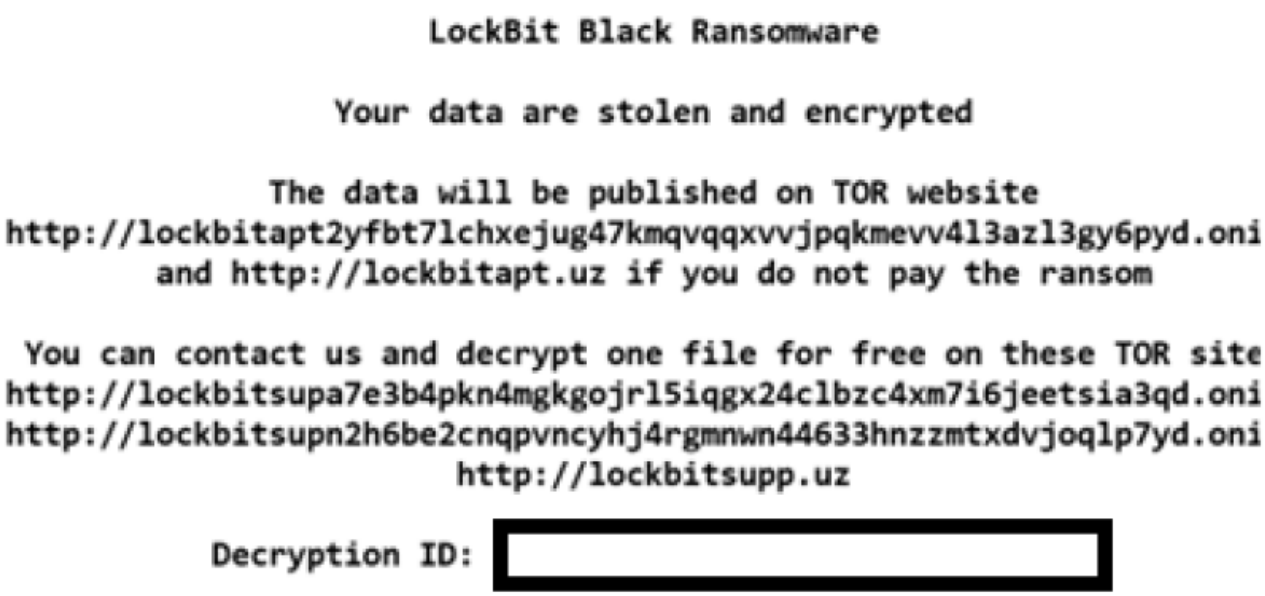


The analysis also showed other sections of the code that are similar between the samples of Lockbit 3.0 and BlackMatter, suggesting a possible correlation between the threat groups behind the implementation of the two ransomware. To hinder the analysis, LockBit 3.0 also uses **string obfuscation**, which is done though a simple decryption algorithm (**XOR**) to decrypt the strings. Regarding the **file encryption**, the ransomware uses a multi-thread approach. Files are encrypted with AES, in case of large files, not all content is encrypted, but only a part of sections in it. Moreover, files are renamed replacing filenames and their extension with random dynamic and static string: with the analyzed sample, the extension used was **.HLJkNskOq** and filenames were replaced by random 7 characters strings (e.g. **Tle9pEW.HLJkNskOq**). Also, a new icon is associated with the encrypted files, which is written on the disk in an .ico image file in the directory **C:\ProgramData**, under the name **HLJkNskOq.ico**. The ransom note is written in every directory containing encrypted files. It states that data is stolen and encrypted and that if the ransom is not paid it will be published on the darknet. The ransom note also contains the .onion URLs to the TOR website, and instruct the victim to contact the attackers using the provided websites and personal ID. As usual, the ransom note warns that deleting or modifying the encrypted files will prevent their decryption.

```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once you

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmgvggxvvjpgkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecgggadevyiwgxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njqngpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcriqzqdjprwuqkkut63nbvy2d5r4w2aqyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kqtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmgvggxvvjpgkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecgggadevyiwgxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njqngpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcriqzqdjprwuqkkut63nbvy2d5r4w2aqyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kqtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation.

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID
```

Finally, when the encryption process ends, also the victim's wallpaper is changed with the image below, which instructs the victim to read the ransom note:

Moreover, LockBit 3.0 also has the capability to print a version of its ransom note using connected printers using WinSpool APIs, as can be seen by the process **splwow64.exe** launched after the malware execution. The printed file is shown below:



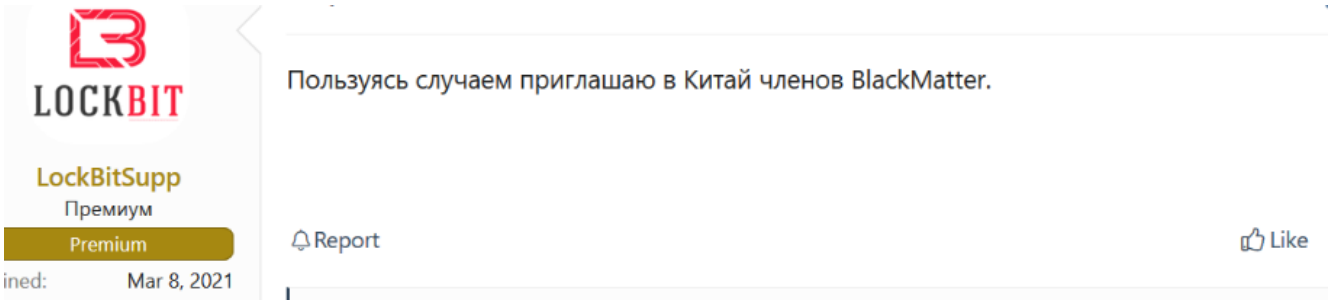
Finally, one of the last operations performed by the malware consists in setting a considerable amount of modification in the keys of the Windows Registry related to the Windows Event Log, in order to disable the monitoring of event such as the one associated with Windows Defender. These modifications can be traced in the subkeys of the registry starting from

> **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\<Log Name>**

Where the **Enabled** subkey associated with each log is set to **0**.

CONCLUSIONS

The LockBit 3.0 project is proof of the extreme dynamism of the ransomware business. Potentially, the group appears to have acquired skills from other groups that have actively operated in the sector in the past. Interesting the code overlaps with BlackMatter as the relations between the two groups may be not casual; on September 2021 **Cluster25** observed a coordinated attack handled simultaneously by members of the **LockBit** and **BlackMatter** crews. Despite the observation of simultaneous attacks can be considered a quite common event in the ransomware world, this one is going to confirm once again the high degree of complexity of the **Russian-speaking** ransomware ecosystem which very often is based on personal relationships between the different teams members. Furthermore, on November 2021, **BlackMatter** shuts down its activities and declares the quit of its business. As the **BlackMatter** gang quitted the operations several team members were transferred to other **R-a-a-S** partnerships, specifically **LockBit**. **Cluster25** also noted the direct involvement of **LockBit** representatives in trying to acquire the members of the BlackMatter group, at that time in the process of winding up, as reported by the image below.



Finally, the strong similarity of the 3.0 payload to **BlackMatter** could suggest either a purchase of the latter's code or a current collaboration of the **LockBit** collective with some former **BlackMatter** developers.

ATT&CK MATRIX

TACTIC	TECHNIQUE	DESCRIPTION
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1106	Native API
Execution	T1204.002	User Execution: Malicious File
Privilege Escalation	T1134	Access Token Manipulation
Defense Evasion	T1622	Debugger Evasion
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
Defense Evasion	T1112	Modify Registry

INDICATORS OF COMPROMISE

CATEGORY	TYPE	VALUE
PAYLOAD	SHA256	80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce
PAYLOAD	SHA1	f2a72bee623659d3ba16b365024020868246d901
PAYLOAD	MD5	38745539b71cf201bb502437f891d799

Written by: Cluster25

Tagged as: ransomware, LockBit, BlackMatter, DarkSide, Crimeware, LockBit 3.0, LockBitBlack.

Previous post

energy Cluster25 / May 27, 2022

Cyberwarfare targeting the energy sector. Is Europe under threat?

The energy sector is a pivotal one for the whole contemporary economy. A disrupt of its functions could cause huge problems for the economy of a certain country. In this report C25 listed some of the most famous cases of [...]

Post comments (0)

Leave a reply

Your email address will not be published. Required fields are marked *