# Hunting LockBit Variations using Logpoint

logpoint.com/en/blog/hunting-lockbit-variations-using-logpoint/

Rasmus Plambech October 18, 2022

*– Anish Bogati & Nilaa Maharjan; Logpoint Global Services & Security Research*

## Executive Summary:

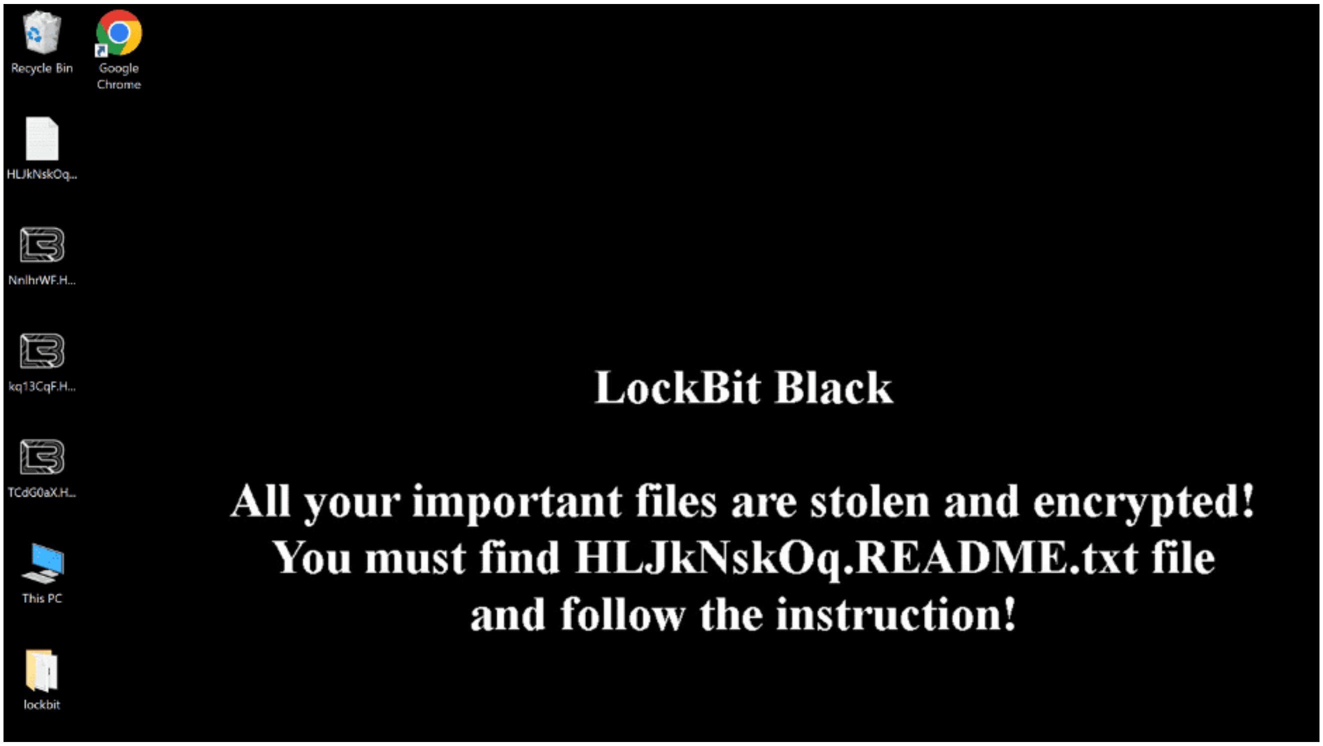
- LockBit has been implicated as the most active ransomware and has been involved in the most attacks compared to others of its kind.
- LockBit emerged in September 2019 functioning as ransomware-as-a-service (RaaS).
- Since then it evolved into LockBit2.0 as a variant of the original LockBit ransomware gang.

  During this time, the gang started a double extortion model.
- Currently running as LockBit3.0, or LockBit Black, the ransomware gang is actively targeting multiple sectors, most commonly banking, financial services, and insurance (BFSI).
- LockBit shares behaviors with MegaCortex and LockerGoga. It is self-spreading, targeted, and uses similar tools.
- The largest case of LockBit includes Accenture in August 2021 which stole 6 terabytes of data and demanded $50 million in ransom.
- LockBit 3.0 announced its own bug bounty program to let security researchers and hackers alike find flaws in their projects and infrastructure hosted on the dark web.

## What is LockBit?

LockBit, formerly known as “ABCD” ransomware due to the conversion of encrypted files to the “.abcd” extension is a ransomware-as-a-service (RaaS) malware. The threat actors have been updating this ransomware features and capabilities since it was first detected in September 2019. It also advertised itself as the fastest ransomware to encrypt files. It shares some similarities with Darkside/black matter ransomware, uses passwords to run like blackcat/aplhv, and is believed to be part of the LockerGoga & MegaCortex family.

LockBit’s family of ransomware is known to be self-spreading, yet has been found targeting specific companies that are able to pay a large ransom.



LockBit Black

All your important files are stolen and encrypted!
You must find HLJkNskOq.README.txt file
and follow the instruction!

Image Showing Desktop Wallpaper after Encryption Process is Completed

The LockBit creators offer access to the ransomware program and its infrastructure to third-party hackers known as affiliates, who break into networks and install it on systems in exchange for a cut of up to 75% of the ransom paid by victims. LockBit, like most similar RaaS gangs, employ double extortion tactics in which its associates exfiltrate data from victim organizations and threaten to disclose it online.

According to research by ransomware incident response provider Coveware, LockBit was responsible for 15% of ransomware assaults seen in the first quarter of 2022, trailing only Conti with 16%. According to a more recent assessment, LockBit was responsible for 40% of the ransomware assaults seen by NCC Group in May, followed by Conti.

While the overall number of ransomware incidents has decreased in recent months, the percentage that LockBit accounts for is likely to rise, partly because the Conti operation is believed to have shut down or splintered into smaller groups, and partly because LockBit is attempting to attract more affiliates by claiming to offer better terms than competitors.

## Origin and Evolution

LockBit has evolved from the early days of ABCD. The RaaS affiliate program was released in early 2020, followed by the data leak site and the addition of data leak extortion later that year.

During its first year of operation, LockBit remained a minor participant, with other high-profile gangs—Ryuk, REvil, Maze, and others—being more successful and in the spotlight. With the release of LockBit 2.0 and after some of the other gangs shut down their activities due to too much pressure, the LockBit ransomware gained traction in the second half of 2021.

According to researchers from Palo Alto Networks' Unit 42, LockBit 2.0 was "the most impactful and widely deployed ransomware variant we have observed in all ransomware breaches during the first quarter of 2022, considering both leak site data and data from cases handled by Unit 42 incident responders." The group's LockBit 2.0 site, which it uses to publish data from corporations whose networks it has infiltrated, names 850 victims, but the gang claims to have ransomed over 12,125 firms so far.

The group also claims that the LockBit 2.0 ransomware has the quickest encryption procedure, which according to Splunk researchers is only partially true. LockBit 1.0 and the ransomware program PwndLocker appear to be faster than LockBit 2.0, but the encryption process is still quite fast, thanks in part to the fact that these threats use partial encryption. LockBit 2.0, for example, encrypts only the first 4KB of each file, rendering it unreadable and unusable while also allowing the attack to finish quickly before incident responders have time to shut down systems and isolate them from the network.

Researchers have found connections between the current LockBit ransomware variant and BlackMatter, a rebranded form of the DarkSide ransomware strain that shut down in November 2021.

LockBit 3.0, also known as LockBit Black, was released in June 2022, including a new leak site and the world's first ransomware bug bounty program, with Zcash cryptocurrency as a payment option.

It encrypts each file by appending the extension "HLJkNskOq" or "19MqZqZ0s" and changes the icons of the locked files to the ".ico" file dropped by the LockBit sample to initiate the infection.

## Who is LockBit targeting?

According to BlackFog's most recent "Ransomware Trend Report," there is a renewed emphasis on weaker targets, such as education (33% increase), government (25% increase), and manufacturing (24% increase).

Attacks in June on the University of Pisa (which paid a $4.5 million ransom), Brooks County in Texas (which paid a $37,000 ransom with taxpayer money), and the Cape Cod Regional Transit Authority all demonstrate this.

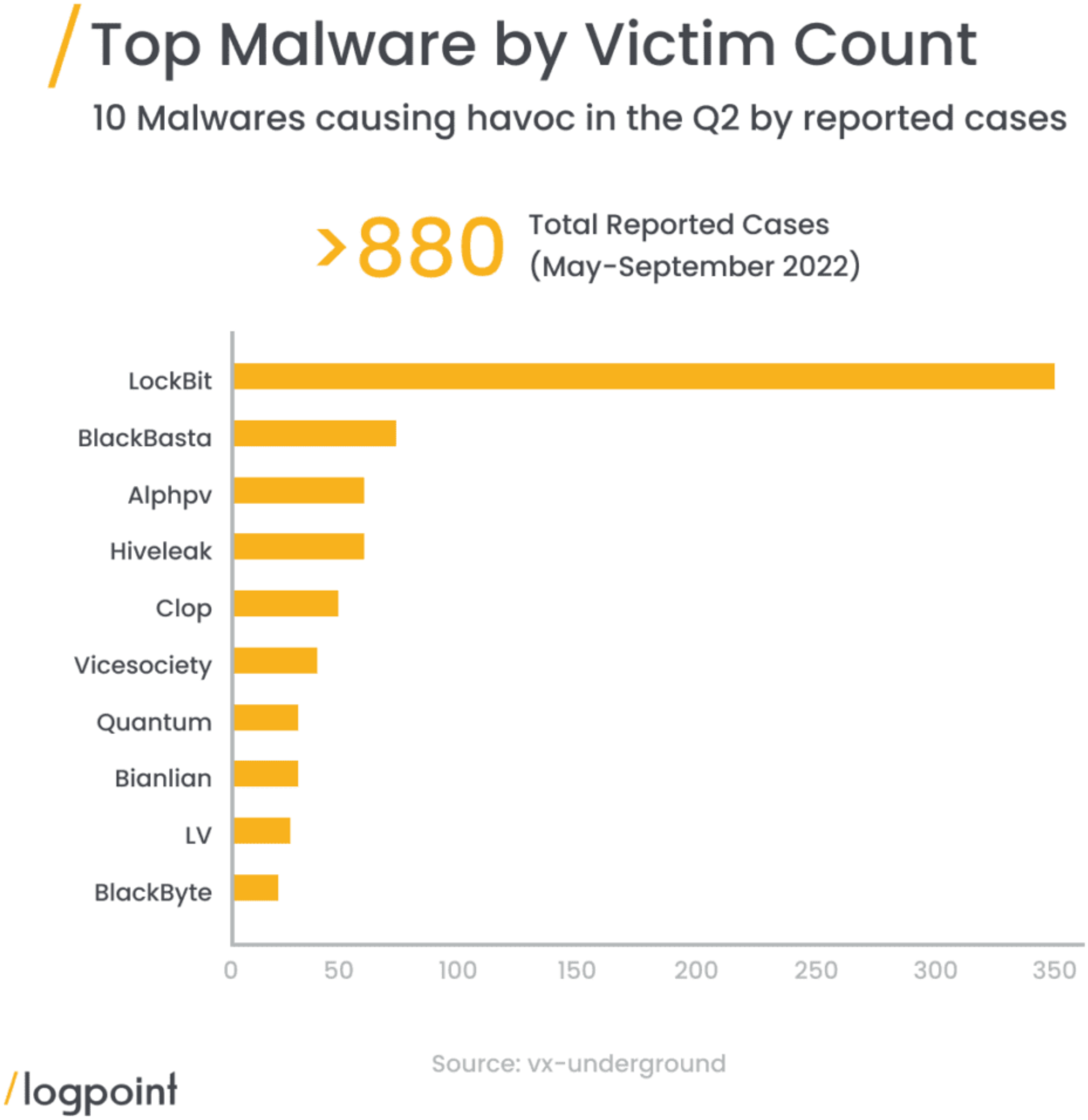
In total, 31 publicly publicized ransomware incidents were recorded by BlackFog in June.

Matt Hull, NCC Group's worldwide lead for strategic threat intelligence, finally pointed to "major changes" in the ransomware threat landscape, adding that "it is evident we are in a transitory phase."

“This is an ever-changing landscape that must be constantly evaluated,” he said.

According to data from LockBit’s data leak site, nearly half of the victim organizations were from the United States, followed by Italy, Germany, Canada, France, and the United Kingdom. According to the LockBit gang member in the previous interview, the concentration on North American and European firms is owing to a larger prevalence of cyber insurance as well as higher profits in these regions. Professional and legal services, construction, the federal government, real estate, retail, high tech, and manufacturing have been the most impacted industry verticals. The malware also includes code that stops it from being executed on PCs configured with Eastern European language settings.

Based on tweets by @VX-underground Twitter bot @RansomwareNews from May 17 to September 221, LockBit accounted for twice as much as its closest competitor, BlackBastaa, Aplhv/BlackCat, Hiveleak, and clop.

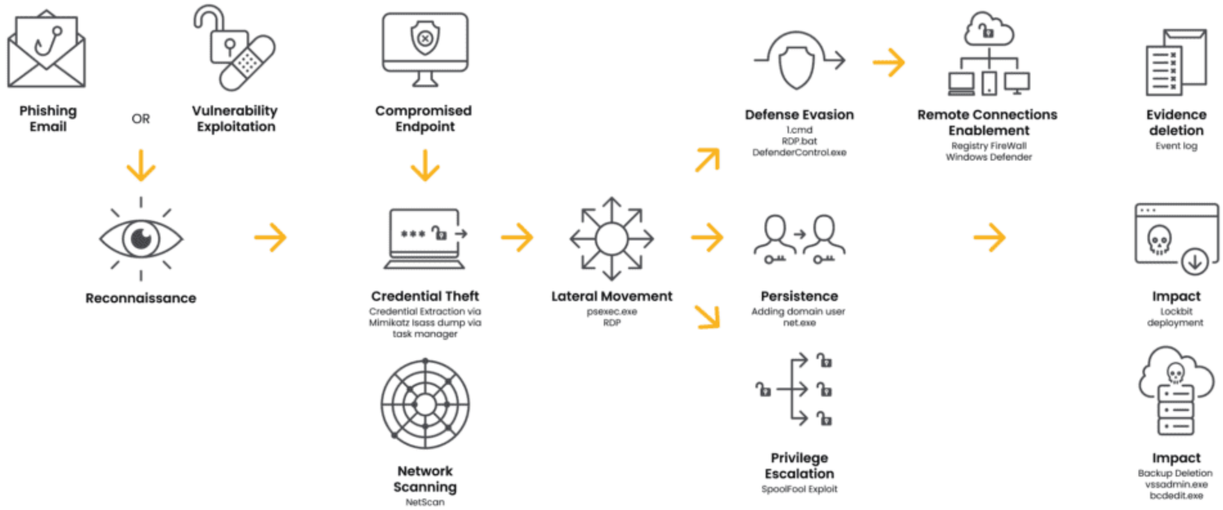


It should also be noted that the LockBit gang has created a separate malware application called StealBit that can be used to automate data exfiltration. This tool uploads the data directly to LockBit's servers rather than using public file hosting sites, which may erase the data in response to victim complaints. The group has also created the LockBit Linux-ESXi Locker, which can encrypt Linux servers and VMware ESXi virtual machines.

LockBit attackers spent roughly 70 days within a network before releasing the ransomware in Q4 2021, 35 days in Q1 2022, and fewer than 20 days in Q2 2022. This means that enterprises have less time to detect network attacks in their early stages and prevent ransomware deployment. According to Palo Alto Networks, the attackers' willingness to bargain and lessen the ransom sum has also decreased. Last year, the attackers were willing to reduce the ransom sum by more than 80%, but currently, victims may only expect a 30% price drop on average.

## LockBit Operations

After obtaining initial access to networks, LockBit affiliates deploy various tools to expand their access to other systems. These tools involve credential dumpers like Mimikatz; privilege escalation tools like ProxyShell, tools used to disable security products and various processes such as GMER, PC Hunter, and Process Hacker; network and port scanners to identify active directory domain controllers, remote execution tools like PsExec or Cobalt Strike for lateral movement. The activity also involves the use of obfuscated PowerShell and batch scripts and rogue scheduled tasks for persistence.



Once deployed, the LockBit ransomware can also spread to other systems via SMB connections using collected credentials as well as by using Active Directory group policies. When executed, the ransomware will disable Windows volume shadow copies and delete various system and security logs.

The malware then collects system information such as hostname, domain information, local drive configuration, remote shares, and mounted storage devices then will start encrypting all data on the local and remote devices it can access. After encrypting all the files LockBit also changes the file's icon with their icon.

After the registry entry is created then the icon from the "C:\ProgramData" is loaded in the registry value. When the encryption process of a file is completed then the icons of files are changed to the icon present in the above mention registry key.

However, it skips files that would prevent the system from functioning. In the end, it drops a ransom note by changing the user's desktop wallpaper with information on how to contact the attackers.

We go into a lot of detail on how the threat actors have been operating, and the Tactic, Techniques, and Procedures(TTPs) they have been using through static and dynamic analysis in the report attached below. We uncovered multiple files, domains, and botnet networks that are still active in the wild. All artifacts are provided as lists and the associated alerts are available to download as part of Logpoint's latest release, as well as through Logpoint's download center.

Logpoint Emerging Threats Protection Service provides the service subscribers with customized investigation and response playbooks, tailored to your environment. Contact the global services team here.

The report containing the analysis, infection chain, detection, and mitigation using logpoint SIEM and SOAR can be downloaded from the link below.

Download report

Download report

## Contact Logpoint

Contact us and learn why industry-leading companies choose Logpoint:

Contact Logpoint