LockBit explained: How it has become the most popular ransomware

By Lucian Constantin

Published: 2022-07-05 · Archived: 2026-04-06 00:40:55 UTC

LockBit is one of the most prominent ransomware-as-a-service (RaaS) operations that has targeted organizations over the past several years. Since its launch in 2019, LockBit has constantly evolved, seeing unprecedented growth recently driven by other ransomware gangs disbanding.

The LockBit creators sell access to the ransomware program and its infrastructure to third-party cybercriminals known as affiliates who break into networks and deploy it on systems for a cut of up to 75% of the money paid by victims in ransoms. Like most similar RaaS gangs, LockBit engages in double extortion tactics where its affiliates also exfiltrate data out of victim organizations and threaten to publish it online.

According to a report by ransomware incident response firm Coveware, LockBit accounted for 15% of ransomware attacks the company saw during the first quarter of 2022, second only to Conti with 16%. In a more recent report, cybersecurity firm NCC Group reported that LockBit was responsible for 40% of the ransomware attacks the company saw in May, followed by Conti.

While the number of ransomware incidents has been decreasing overall in recent months, the percent that LockBit accounts for is likely to increase, partly because the Conti operation is believed to have shut down or splintered into smaller groups and because LockBit is trying to attract more affiliates claiming to offer better conditions than competitors.

How LockBit has evolved

This ransomware threat was originally known as ABCD after the file extension .abcd that it left on encrypted files. The RaaS affiliate program was launched in early 2020 and the data leak site and addition of data leak extortion was announced later that year.

LockBit remained a relatively small player during its first year of operation with other high-profile gangs being more successful and in the spotlight—Ryuk, REvil, Maze and others. The LockBit ransomware started to gain more traction in the second half of 2021 with the launch of LockBit 2.0 and after some of the other gangs shut down their operations after attracting too much heat.

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,” researchers from Palo Alto Networks’ Unit 42 said in a report. The LockBit 2.0 site that the gang uses to publish data from organizations whose networks they breached lists 850 victims, but the gang claims it has ransomed over 12,125 organizations so far.

The group also claims that the LockBit 2.0 ransomware has the fastest encryption routine, which is only partially true according to tests by researchers from Splunk. LockBit 1.0 and a ransomware program known as PwndLocker seem to be faster than LockBit 2.0, but the encryption routine is still very fast partly because these threats perform partial encryption. LockBit 2.0, for example, encrypts only the first 4KB of each file, which is enough to render them unreadable and unusable while also allowing the attack to complete very fast before incident responders have time to shut down systems and isolate them from the network.

How does LockBit select and target victims?

Since many affiliates distribute LockBit, the access vectors they use are varied: from spear-phishing emails with malicious attachments to exploiting vulnerabilities in publicly facing applications and using stolen VPN and RDP credentials. The LockBit affiliates are known to also buy access from other parties.

According to a 2021 public interview with an alleged LockBit gang member, the group has a policy against targeting organizations operating in the healthcare, education, charity and social services sectors. However, LockBit affiliates haven't followed these guidelines in some cases and attacked organizations from healthcare and education, the Palo Alto researchers warned.

Based on data from LockBit's data leak site, almost half of the victim organizations were from the U.S., followed by Italy, Germany, Canada, France and the UK. The focus on North American and European organizations is due to higher prevalence of cyber insurance in these regions as well as higher revenues, the LockBit gang member said in the old interview. The most impacted industry verticals have been professional and legal services, construction, federal government, real estate, retail, high tech, and manufacturing. The malware also contains code that prevents its execution on systems with Eastern European language settings.

It's also worth noting that the LockBit gang has developed a separate malware program called StealBit that can be used to automate the exfiltration of data. This tool uploads the data directly to LockBit's servers instead of using public file hosting services that could delete the data following complaints from victims. The gang has also developed a tool called the LockBit Linux-ESXi Locker to encrypt Linux servers and VMware ESXi virtual machines.

The amount of time that LockBit attackers spend inside a network before deploying the ransomware has decreased over time from around 70 days in Q4 2021 to 35 days in Q1 2022 and less than 20 days in Q2 2022. This means organizations have less time to detect the network intrusions in their early stages and stop the ransomware from being deployed. The willingness of the attackers to negotiate and lower the ransom amount has also decreased according to Palo Alto Networks. Last year, the attackers were willing to drop the ransom amount by over 80 percent, while now victims can only expect a 30 percent price drop on average.

How does LockBit perform lateral movement and payload execution?

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

The file encryption routine uses AES and with a locally generated key that's further encrypted using an RSA public key. The malware only encrypts the first 4KB of each file and appends the ".lockbit" extension to them.

The FBI issued a public alert about LockBit in February that contains indicators of compromise taken from incidents investigated in the field, as well as recommendations for organizations.

LockBit 3.0 and its bug bounty program

In June, the LockBit creators announced version 3.0 of their affiliate program and malware after reportedly having it in beta testing for two months. The gang also launched a bug bounty program that offers between $1,000 and $1 million for vulnerabilities in both the ransomware program and the gang's infrastructure, such as its Tor-hosted website, secure messenger and more.

The gang even went as far as to launch a $1 million challenge to anyone who manages to find out the identity of the person running its affiliate program, essentially asking for its highest-ranking member to be doxxed. This is not the first time LockBit has engaged in unusual practices. Its ransom notes include financial offers to insiders who can provide access to networks and organizations and its bug bounty program also offers rewards for ideas on how to improve the ransomware operation, software and infrastructure that the gang hasn't yet considered.

While the technical changes to the LockBit 3,0 itself, the screenshots shared by LockBit suggest that the Zcash cryptocurrency will be accepted for ransom payments along with Bitcoin and Monero in the new version. The addition of Zcash could be an attempt to make payments harder to trace.

According to the Palo Alto researchers, the addition of the bug bounty program might have been driven by researchers finding a bug in LockBit 2.0 that allowed reversion of the encryption process on MSSQL databases.

In early June, cybersecurity firm Mandiant released a report connecting some LockBit intrusions to a threat actor tracked as UNC2165 that used the Hades ransomware in the past and has significant activity overlaps with Evil Corp, a notorious cybercriminal group that's on the Treasury Department's list of sanctioned entities. Evil Corp is responsible for the creation of the Dridex botnet, the WastedLocker ransomware and other threats in the past and sending ransom payments to cybercriminals associated with it is in violation of the sanctions.

"The adoption of an existing ransomware is a natural evolution for UNC2165 to attempt to obscure their affiliation with Evil Corp," the Mandiant researchers said. "Both the prominence of LockBit in recent years and its

successful use by several different threat clusters likely made the ransomware an attractive choice. Using this RaaS would allow UNC2165 to blend in with other affiliates, requiring visibility into earlier stages of the attack lifecycle to properly attribute the activity, compared to prior operations that may have been attributable based on the use of an exclusive ransomware."

The LockBit gang later dismissed these connections as false and released a statement saying it has nothing to do with Evil Corp and its alleged leader Maxim Yakubets, who is on the FBI's Cyber's Most Wanted list.
