LOGPOINT

LockBit: A deep-dive into the rapidly evolving RaaS gang and its unique business model

Oct 18, 2022 14:37 CEST

LockBit: A deep-dive into the rapidly evolving RaaS gang and its unique business model

- **New Logpoint study unfolds the ransomware threat landscape in the wake of the LockBit 3.0 launch in June 2022**
- **LockBit 3.0 introduces new unique services such as automatic data exfiltration and the world's first ransomware bug-bounty program**

COPENHAGEN, Denmark & BOSTON, October 18, 2022 – Logpoint's Global Services has identified 800 reported LockBit cases from May to September, which is twice as many as the closest competitors, BlackBasta, Alphpv/BlackCat, Hiveleak, and Clop, combined. LockBit is the most active RaaS strain, and Logpoint Global Services has investigated the threat in its latest Emerging Threats report.

“Ransomware groups have come and gone, techniques and tactics have evolved significantly, and activity levels have risen and fallen,” says Doron Davidson, VP Logpoint Global Services. “The latest variation, LockBit 3.0, also known as LockBit Black, represents yet another shift in the ransomware threat landscape. Organizations now face shorter time to detect attacks in the early stages and prevent ransomware deployment, and reduced opportunity to negotiate the ransom terms.”

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. In addition, the attackers’ willingness to reduce the ransom has decreased significantly from an average of 80% last year to only 30% this year.

The LockBit threat development

LockBit is self-spreading and targeted and uses the double extortion model, in which its associates exfiltrate data from victim organizations and threaten to disclose it online. In June 2022, LockBit 3.0 launched a new bug bounty program to let security researchers and hackers find flaws in the gang’s projects and infrastructure hosted on the dark web. The LockBit creators have also developed an automatic data exfiltration tool called StealBit to improve the process.

While the overall number of ransomware incidents has decreased in recent months, the percentage that LockBit accounts for is likely to rise. This is partly because the Conti operation has allegedly shut down or splintered into smaller groups and partly because LockBit is attempting to attract more affiliates by offering better terms than their competitors, which appears to be successful.

The creators behind promote LockBit 3.0 as the world’s fastest and most stable ransomware. LockBit encrypts rapidly due to partial encryption. It only encrypts 4 KB of each file, enough to render it unreadable and unusable, allowing the attack to finish quickly before incident responders have time to shut down systems and isolate them from the network.

LockBit ransomware business model

The LockBit creators offer ransomware to affiliates for a cut of up to 75% of the ransom paid by victims. LockBit primarily targets organizations in North America and Europe due to the widespread prevalence of cyber insurance and higher profits. The malware also includes code that stops it from being executed on PCs configured with Eastern European language settings.

“Our report illustrates how ransomware gangs like LockBit operate as businesses. How they strive for a competitive advantage, develop their offerings, and innovate new products to stay relevant to their users. In reality, ransomware groups mirror software companies and are included in an entire ecosystem,” says Doron Davidson.

According to research by Coveware, LockBit was responsible for 15% of ransomware assaults in the first quarter of 2022, only behind 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. The most impacted industry verticals count professional and legal services, construction, the federal government, real estate, retail, high tech, and manufacturing.

Read Logpoint’s blog post about the findings here, and access the full Emerging Threats report, Hunting LockBit Variations Using Logpoint. The report offers an in-depth vulnerability analysis, means to detect and respond to the threat, including a collection of rules applicable to the procedures carried out by LockBit, and insights about incident investigation and response.

About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint’s SIEMand NDRtechnologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in

Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit http://logpoint.com.

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98