LOGPOINT

8base is among the top 5 ransomware groups this summer

Aug 24, 2023 10:00 CEST

8base ransomware group significantly boosts activity level

- **8base is among the top 5 ransomware groups this summer, and Logpoint has uncovered the Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise IoCs to look out for.**
- **The ransomware group targets small and medium-sized organizations, which are less likely to have strong security measures.**

COPENHAGEN, Denmark, August 24, 2023 – The 8Base ransomware group has emerged as a persistent and formidable adversary in the ever-changing landscape of cyber threats, targeting multiple sectors, especially small and

medium-sized industries. The group appeared in March 2022, and since June, the activity level has increased significantly, putting the group in the top 5 most active.

“In general, small and medium-sized organizations are more likely to struggle with small security budgets and cybersecurity shortages, which is a dangerous cocktail when a ransomware group like 8base is coming for them,” says Anish Bogati, Logpoint Security Research Engineer. “Small and medium-sized organizations, in particular, should familiarize themselves with 8base, and more importantly, ramp up on security measures to safeguard against it. Understanding the adversary is the key to devising better defensive strategies.”

Logpoint’s research has uncovered the 8base infection chain through malware analysis. 8base use multiple malware families to achieve their goals, including SmokeLoader and SystemBC, in addition to the Phobos ransomware payload. The ransomware group primarily gains initial access through phishing emails and utilizes Windows Command Shell and Power Shell to execute the payload. The adversaries use multiple techniques to ensure persistence within the system, evade defenses, and reach their goals.

Logpoint’s analysis reveals what security teams should look for to detect 8base activity in the system, including suspicious child processes spawned by Microsoft Office products, file executing using WScript or CScript, or scheduled task creation. Knowing the indicators of compromise and TTPs helps organizations proactively identify and mitigate suspicious activities associated with 8base.

“Small and medium-sized organizations must ensure capabilities that enable them to detect and respond to 8base activity at any stage of the infection,” says Anish Bogati. “Proper logging, visibility of assets, and monitoring are essential to a robust cybersecurity strategy because they provide an overview of the network and help to detect anomalies like file dropped in publicly writable folders, modification of registry values and suspicious scheduled task that may indicate a security threat like 8base is at large.”

Read Logpoint’s full report about 8base here and get an in-depth malware analysis, technical analysis, and all means of detecting, investigating, and responding to the threat.

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