Searchlight Cyber Report Finds a 67% Increase in Ransomware Victims in H1 2025 vs H1 2024

Higher victim count correlates with a greater number of ransomware groups, in spite of the deterioration of Lockbit

PORTSMOUTH, UNITED KINGDOM, September 25, 2025 /EINPresswire.com/ --
Searchlight Cyber - the Continuous Threat Exposure Management company, has published its latest ransomware report based on threat intelligence gathered from the dark web, which shows a marked increase in ransomware victims in the first half of the year. The report - An Escalation in Attacks: The Ransomware Landscape in H1 2025 - records 3,734 victims listed on ransomware leak sites between January and June 2025, which is a 67 percent increase on the same time period last year (H1 2024) and a 20 percent increase on H2 2024.

Other key findings of the report include:
- A 16% increase in the number of active ransomware groups in H1 2025 vs H2 2024.
- The emergence of 35 new ransomware groups that had never been recorded before.
- A concentration of victims in NATO member states, which accounted for 65% of attacks.
- The use of software vulnerabilities by groups like Cl0p to gain access to victim networks.
- The development of new extortion methods, such as ransomware groups hiring “legal teams” that will alert authorities of regulatory breaches if victims don’t pay the ransom.

Luke Donovan, Head of Threat Intelligence at Searchlight Cyber, commented: “Unfortunately, this report shows an aggressive expansion in the global ransomware ecosystem during the first half of 2025, reaching new heights in terms of the number of listed victims. The increase in the number of active groups, driven by technological advancements and the commoditization of ransomware, has led to more organizations being targeted and a tougher landscape for security professionals to monitor. In this environment, it is critical that security teams are continuously gathering threat intelligence on ransomware groups to inform their defenses based on the most up to date information on the threats they are facing.”

The report ranks the top five most active ransomware groups, with detailed profiles of each: Cl0p, Akira, Qilin, RansomHub, and Play. Cl0p ranks first, largely thanks to the number of victims that it amassed at the beginning of the year through the exploitation of the file transfer system, Cleo. This report also includes an analysis of the victim data stolen by Cl0p, which showed the benefits of downloading and analyzing breached content associated with the direct victims of ransomware attacks. This approach allows us to understand the broader impact of ransomware attacks beyond the initial victim. For instance, Searchlight Cyber's analysis of 171 Cl0p victims revealed an average of 36.6GB of leaked data and an average of 102,938 email addresses identified per victim, highlighting the need for robust cybersecurity measures across an organization's entire network, including partners and third-party vendors.

Another major finding of the report is the rapid decline of the ransomware group LockBit, which has fallen from the #2 spot in 2024 to #25 in the first half of this year. This fall from grace is attributed to the ongoing impact of the 2024 law enforcement action against the group, Operation Cronos, which sought to discredit the group among its cybercriminal peers. The impact appears to have been exacerbated by an attack against the group by an unknown actor in May 2025, which included a data leak of victim negotiations between its affiliates and their victims.

Luke Donovan commented: "While our latest report does contain alarming results in terms of victim numbers, the near-total demise of LockBit does provide the security community with a silver lining and path forward. Before Operation Cronos, it would have been almost inconceivable that LockBit - who was amassing more than a thousand victims a year - would be reduced to its current levels. It's a story that demonstrates the power of threat intelligence, cybercriminal investigation, and government-private sector collaboration in combating ransomware threats."

About Searchlight Cyber:

Searchlight Cyber was founded in 2017 with a mission to stop threat actors from acting with impunity. Its External Cyber Risk Management Platform helps organizations to identify and protect themselves from emerging cybercriminal threats with Attack Surface Management and Threat Intelligence tools designed to separate the signal from the noise. It is used by some of the world's largest enterprises, government and law enforcement agencies, and the Managed Security Service Providers at the forefront of protecting customers from external threats. Find out more at www.slcyber.io.

Sonia Awan
Outbloom Public Relations

soniaawan@outbloompr.net
Visit us on social media:
LinkedIn
