

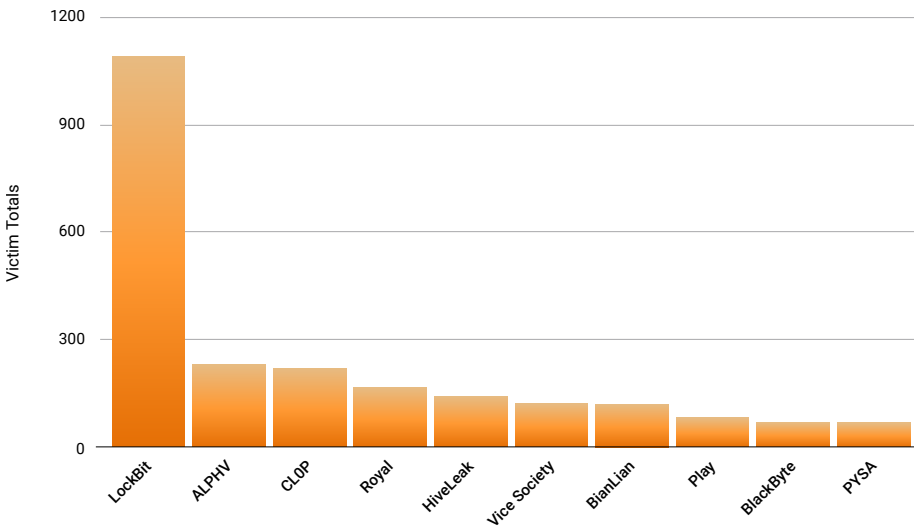
Ransomware on the Move

Evolving exploitation techniques and the active pursuit of zero-days

Ransomware groups are on the move, using aggressive methods of victimization such as zero-day and one-day vulnerability abuse, and multiple extortion schemes to maximize damage to organizations.

LockBit dominates the ransomware scene, accounting for 39% of victim organizations

Ransomware Group Victim Count
Oct 1, 2021 – May 31, 2023



LockBit's success can be attributed to its constant enhancements in its software. However, CLOP is gaining dominance and making a name for itself with its rampant abuse of zero-day vulnerabilities in file transfer software.

143% ↑

Increase in ransomware victims due to the active abuse of zero-day and one-day vulnerabilities by groups like CLOP



Victims attacked by multiple ransomware groups are nearly 6x more likely to experience a subsequent attack within the first 3 months



77%

Increase in ransomware victims in Europe, the Middle East, and Africa (EMEA)

204%

Increase in ransomware victims in Asia-Pacific, and Japan (APJ)

How do attackers maximize their extortion tactics?

Initial foothold
(Spear) Phishing, 0-day and 1-day vulnerabilities, credential abuse



Lateral movement
Spread across the network for maximum damage or impact



Exfiltration
Find and steal valuable data: This is becoming one of the primary methods of extortion



Encryption
Efficient and secure encryption to prevent recovery and disrupt operations



Ransom demand
Victims pay the ransom, or attackers publish their confidential data on leak sites



DDoS attacks
DDoS attacks to disrupt operations; serves as additional extortion tactic



Intimidation and harassment
Attackers call or email victim's customers or partners to mount pressure



Ransomware groups may exploit vulnerabilities that can lead directly to data theft

In recent months, some ransomware attackers have used only exfiltrated data for ransom

Additional pressure to coerce victims to pay ransom



For more information and insights about ransomware trends, the shift in attack techniques, and mitigation strategies, read our full report.

[Download the full report](#)