CYBLE®

REPORT

Ransomware Threat Pulse

SEPTEMBER 2024

Table of **Contents**

Executive Summary

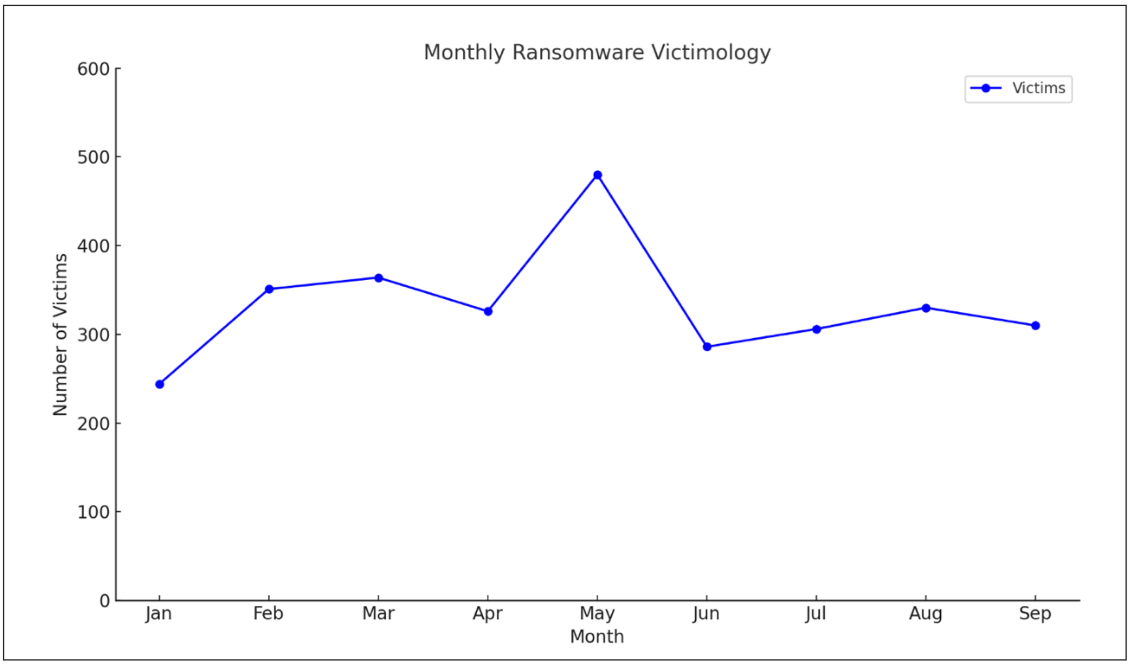
The **Ransomware Threat Pulse for September 2024** by Cyble Research & Intelligence Labs (CRIL) provides an in-depth analysis of global ransomware trends and emerging threats. With 310 publicly disclosed victims this month, the report shows the ongoing impact on various sectors and highlights the tactics employed by major ransomware groups. Cyble also observed a noticeable decline in ransomware activities this month, likely due to enforcement actions.

- **310 ransomware victims** were disclosed in September 2024, with the U.S. being the most affected.
- **RansomHub** remains the most active ransomware group, targeting U.S. corporations for the third consecutive month.
- **Play has replaced LockBit** in the top five, followed by Medusa, Qilin, and BlackSuit.
- The **construction, healthcare, IT, ITES, and manufacturing** sectors were the most impacted.
- New ransomware groups identified include **Orca, InvaderX** (Ransomware-as-a-Service), **Valencia, The Brotherhood,** and **RedRose**.

This report is a crucial resource for understanding current ransomware risks and equipping organizations to strengthen their cybersecurity posture.

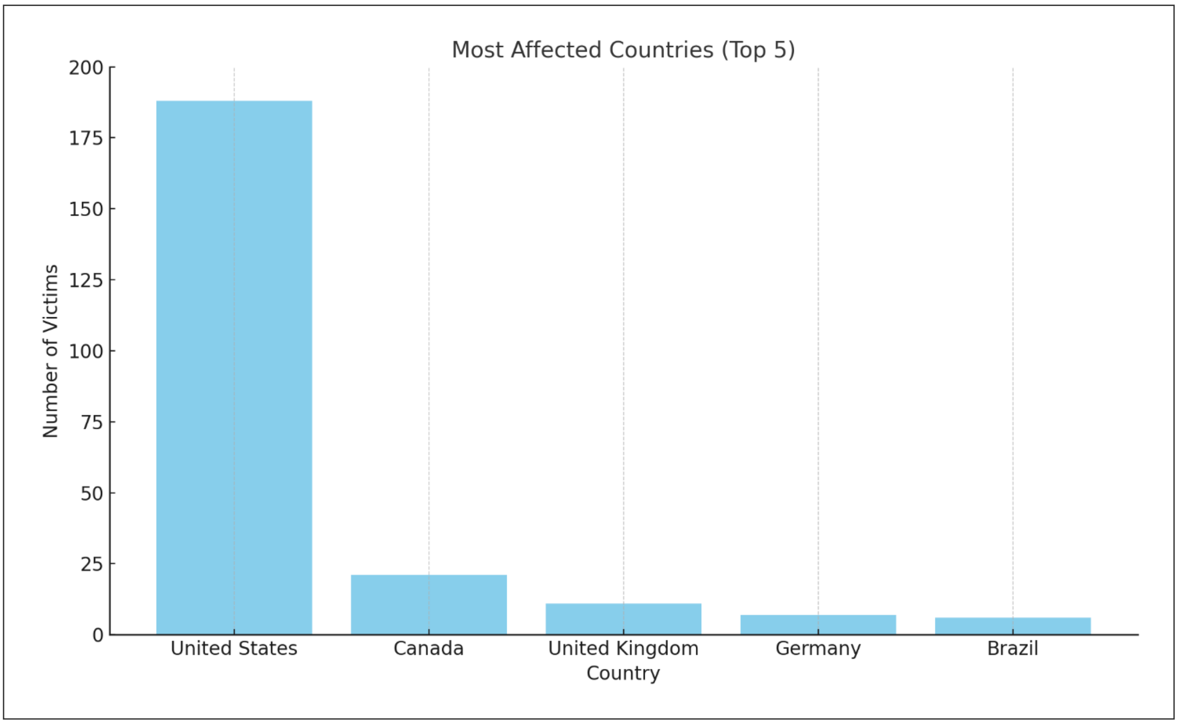
Key Statistics

310 ransomware victims were detected in September



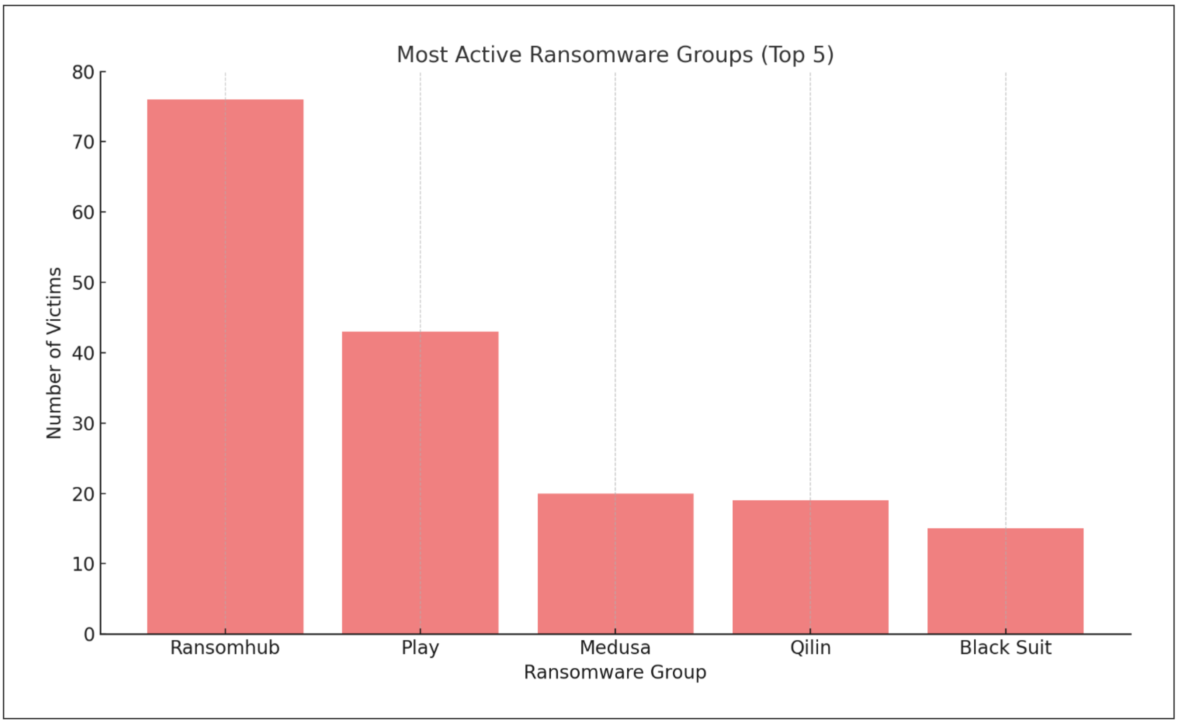
- September saw 310 publicly disclosed ransomware incidents, down from 330 in August.

U.S. was the most targeted country



- The U.S. experienced the highest number of attacks (188), with other affected countries including Canada (21), the U.K. (11), Germany (7), and Brazil (6).
- The majority of incidents targeted mid-sized companies, reflecting a continuing trend of adversaries favoring victims with sufficient resources to pay a ransom while often lacking robust cybersecurity defenses.

RansomHub was the most active ransomware group



- RansomHub was the most active ransomware group for the third month in a row, primarily targeting U.S. businesses.
- The Play group rose in activity, pushing LockBit out of the top five. The group's main target sectors were healthcare and professional services.
- Medusa, Qilin, and BlackSuit rounded out the top five, leveraging novel approaches to initial access and data encryption.

Sectoral Deep Dive into Ransomware Attacks

Ransomware activity in August 2024 significantly impacted various sectors across different regions. A detailed breakdown reveals the following patterns:

- **Americas:** The United States and Canada were primary targets, with the construction sector bearing the brunt of attacks. Healthcare and professional services also saw increased incidents, driven by the exploitation of vulnerabilities in outdated systems.
- **Europe & CIS:** The United Kingdom, France, Germany, and Italy faced frequent attacks, particularly targeting the construction and IT industries. RansomHub and LockBit were among the most active groups in the region.
- **Asia & Oceania:** Japan and Australia saw notable ransomware activities, with a growing focus on finance and IT. The META (Middle East, Turkey, Africa) region experienced fewer incidents, though sectors such as construction and IT continued to face threats.
- **Middle East, Turkey, and Africa (META):** The META (Middle East, Turkey, Africa) region experienced fewer incidents, though sectors such as construction and IT continued to face threats.

Top Weaponized Vulnerabilities in September

CVE-2024-40766 – Akira

The Akira ransomware exploited this vulnerability to gain unauthorized access to corporate networks. This flaw enabled attackers to escalate privileges and execute malicious code, compromising targeted environments.

CVE-2023-48788 – Medusa

Medusa ransomware leveraged this remote code execution vulnerability to infiltrate vulnerable systems. It allowed attackers to deploy ransomware payloads quickly, leading to data encryption and extortion.

CVE-2022-47966 – Multiple Threat Actors

This older vulnerability continued to be a popular target. Threat actors exploited it to bypass authentication measures and gain control over critical infrastructure, often used as a steppingstone to launch further attacks.

CVE-2023-4966 – Embargo Ransomware

The Embargo ransomware group exploited this flaw to breach hybrid cloud environments. Attackers targeted unpatched systems, gaining a foothold to deploy ransomware and establish persistence.

CVE-2023-29300 – Targeted Attacks

Several ransomware operators used this vulnerability for initial access, particularly in industries like IT services and healthcare. It allowed them to bypass security protocols and install malicious tools for encryption.

CVE-2023-38203 – Cloud-Based Infiltration

This vulnerability was commonly used in attacks on cloud infrastructure. Exploitation enabled threat actors to gain unauthorized access and compromise cloud storage, facilitating large-scale data theft and ransomware deployment.

Activities on Underground Forums

InvaderX: New Ransomware-as-a-Service unveiled on RAMP Forum

- On September 4, InvaderX, a new Ransomware-as-a-Service (RaaS) program, was announced on the RAMP forum.
- The program, developed in Rust, advertises advanced capabilities such as Twofish encryption, utilizes ECIES for XChaCha12 hybrid encryption, and a proprietary one-time number generator designed to prevent key stream theft and produce unique keys for each encryption session.
- The RaaS also provides DDoS services and custom features with the capability to target globally, except within CIS and BRICS regions.

New Ransomware Group "The Brotherhood" Established

- On September 09, 2024, a ransomware group titled "The Brotherhood" was established in collaboration with BlackForums, which is a malware/leaks forum and BloodForge a Ransomware as a service (RaaS).
- The RaaS currently has features such as AES-256 and ChaCha20 encryption, information grabber, privilege escalation, network working, anti-AV measures, real-time monitoring, delayed encryption, and single execution lock. The service is being offered at a price of $750 per slot.

About Cyble

Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.

See Cyble in Action

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067