GUIDEPOINT SECURITY

The State of...

RANSOMWARE

6.8 new victims every day in 2022

AND WAYS TO USE THREAT INTELLIGENCE TO LEVEL THE PLAYING FIELD

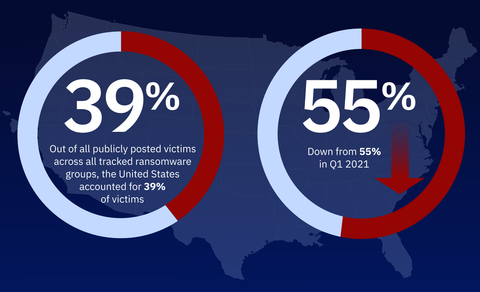
Throughout Q1 '22, there were over 600 victims across a wide variety of industry verticals, which were publicly posted to ransomware leak sites across 40 different ransomware groups.

600 victims

40 different ransomware groups

Top 5 Ransomware Groups with Publicly Posted Victims accounted for nearly ⅔ of all publicly posted ransomware victims that we track:

1. Lockbit
2. Conti
3. Hive
4. Alphvm
5. Karakurt



Top 10 Industries with Publicly Posted Victims

1. Retail
2. Technology
3. Manufacturing
4. Banking and Finance
5. Industrial Services
6. Construction
7. Healthcare
8. Government
9. Education
10. Hospitality

The **40** ransomware groups we tracked publicly posted an average of

6.8 new victims every day in Q1 2022.

As of March 27, there were only **five days in Q1 2022** when there were no new additions to publicly posted ransomware victims across the tracked ransomware groups.

Operationalizing Threat Intelligence

Take all this data, from what seems like an endless supply of sources, and focus on the consolidation, contextualization, and integration into our operational cybersecurity groups including SOC, vulnerability management, and IT. Then...

- Have a Platform That You Can Control
- Automate and Orchestrate Where Possible
- View Your Attack Surface from the Attacker's Perspective
- Have Eyes and Ears on the Dark Web

Read our latest Threat Research Report to gain a better understanding of how to improve your threat intelligence capability.

Download Threat Research Report

GUIDEPOINT SECURITY

www.guidepointsecurity.com

Research conducted by: Drew Schmitt, Principal Threat Intelligence Analyst
GuidePoint Research and Intelligence Team (GRIT)