2023 Mid-Year Threat Review: Trends from the First Half of the Year

The first half of 2023 saw significant threat activity coming from some well-established sources and attack vectors. Our Mid-Year Threat Review looks at these trends and provides guidance for organizations. Below are a few highlights from the report.

Snapshot of the H1 2023 Threat Landscape

12+
new widely exploited vulnerabilities in H1 2023

38%
of new widely exploited vulns were zero-day attacks

39%
of incidents observed by our managed services team stem from missing or lax multi-factor authentication

79
Rapid7 tracked 79 known state-sponsored attacks

24%
of state-sponsored attacks exploited public-facing applications

Tried and true attack vectors are still working for threat actors. These are the initial access vectors our incident response team observed during the first half of the year.

H1 2023 Initial Access Vectors

39%
Remote Access

27%
Vulnerability Exploitation

13%
Phishing Payloads

6%
Supply Chain Compromise

4%
Insider Threat

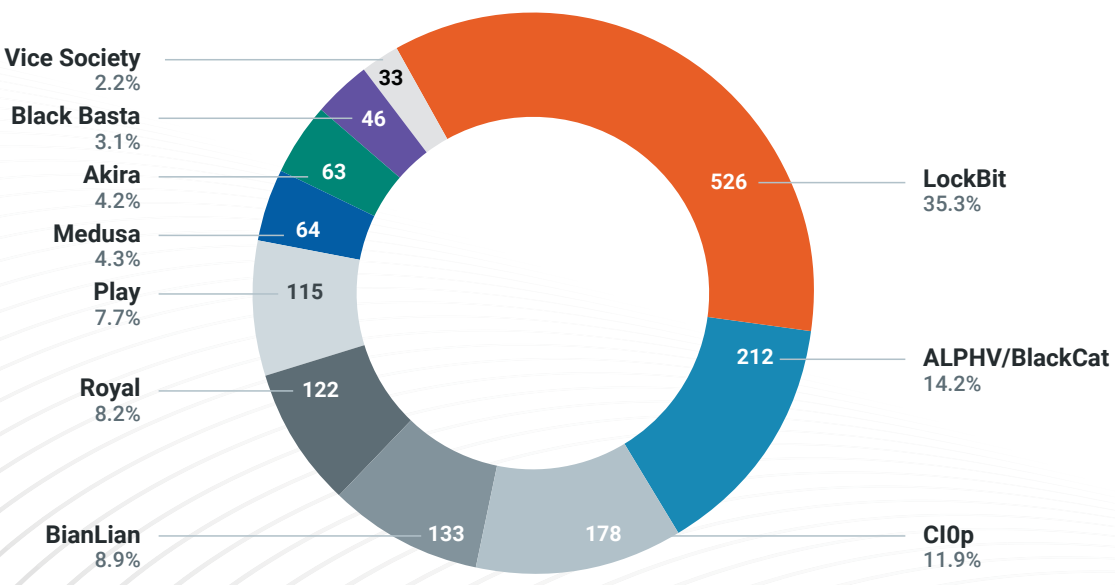
11%
Other

Source: Rapid7 MDR Incident Response

Ransomware Attacks and the Actors Who Perpetrate Them

At least **1,500 organizations were known victims of ransomware** over the first half of the year. The top ransomware groups have remained relatively stable with a handful of newcomers, such as Akira, emerging.

Below are ransomware incidents attributed to major groups:



A Persistently Elevated Threat Landscape

The threat landscape for 2023 continues to present significant challenges for security teams and business leaders. Our new report offers practical real-world guidance to protect your organization from these attacks.

Get the full **2023 Mid-Year Threat Review** Report

DOWNLOAD REPORT

RAPID7