RAPID7

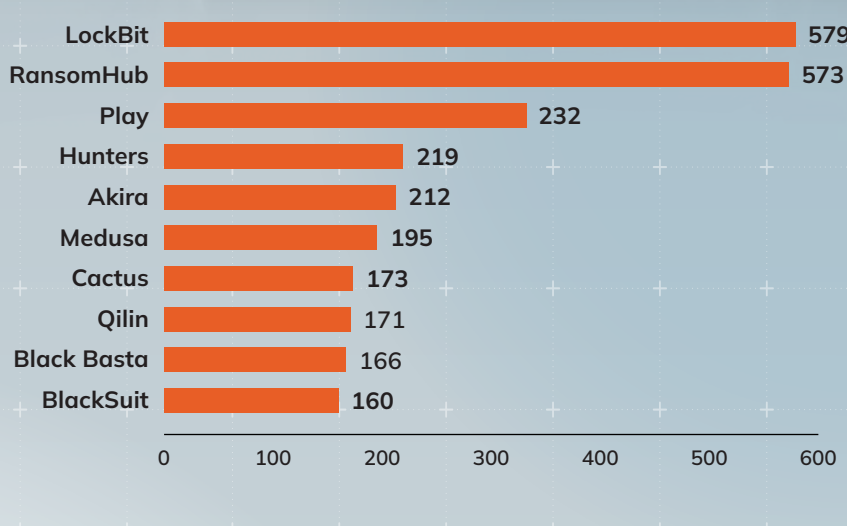
RAPID7.COM

# 2024 THREAT LANDSCAPE STATISTICS FROM RAPID7 LABS

## RANSOMWARE EXTORTION

### TOP 10 RANSOMWARE GROUPS BY NO. OF LEAK SITE POSTS

JAN 1 - NOV 30, 2024




## MOST OBSERVED MALWARE IN 2024

More than one-quarter (28%) of the customer incidents Rapid7 responded to in 2024 involved one of these three malware families.

**SocGholish**
**14%**
of incidents.

**GootLoader**
**10%**
of incidents.

**AsyncRAT**
**4%**
of incidents.

## NOTABLE 2024 VULNERABILITIES

| VENDOR AND PRODUCT | CVE(S) | TARGET CLASSIFICATION | EXPLOITED AS 0DAY? |
|---|---|---|---|
| Broadcom VMware vCenter Server | CVE-2023-34048 | Common software | Yes |
| Broadcom VMware ESXi | CVE-2024-37085 | Common software / hardware | Yes |
| Ivanti Connect Secure | CVE-2023-46805, CVE-2024-21887 | Network pivot | Yes |
| Ivanti Connect Secure | CVE-2024-21888, CVE-2024-21893 | Network pivot | Yes |
| Palo Alto Networks PAN-OS | CVE-2024-3400 | Network pivot | Yes |
| CrushFTP | CVE-2024-4040 | File transfer | Yes |
| Check Point Security Gateway | CVE-2024-24919 | Network pivot | Yes |
| Fortinet FortiManager | CVE-2024-47575 | Network pivot | Yes |
| Palo Alto Networks PAN-OS | CVE-2024-0012, CVE-2024-9474 | Network pivot | Yes |
| Fortinet FortiOS | CVE-2024-21762 | Network pivot | Unclear |
| Jenkins | CVE-2024-23897 | Supply chain attack vector | -- |
| ConnectWise ScreenConnect | CVE-2024-1708, CVE-2024-1709 | Common software | -- |
| JetBrains TeamCity | CVE-2024-27198, CVE-2024-27199 | Supply chain attack vector | -- |
| Fortra GoAnywhere MFT | CVE-2024-0204 | File transfer | -- |
| SolarWinds Serv-U | CVE-2024-28995 | File transfer | -- |
| Progress Software MOVEit Transfer | CVE-2024-5806, CVE-2024-5805 | File transfer | -- |
| Atlassian Confluence Server | CVE-2023-22527 | Common software | -- |
| Veeam Backup & Replication | CVE-2024-40711 | Common software | -- |
| SonicWall SonicOS | CVE-2024-40766 | Network pivot | -- |
| Broadcom VMware vCenter Server | CVE-2024-38812, CVE-2024-38813 | Common software | -- |
| Ivanti Endpoint Manager (EPM) | CVE-2024-29847 | Common software | -- |
| Adobe Commerce and Magento | CVE-2024-34102 | Common software | -- |
| Apache OFBiz | CVE-2024-45195 | Common software | -- |
| PHP | CVE-2024-4577 | Common software | -- |
| ServiceNow | CVE-2024-5217, CVE-2024-4879 | Common software | -- |

# RAPID7 LABS 2024 THREAT LANDSCAPE STATISTICS

## MDR: MOST OBSERVED MALWARE

**SocGholish**
**14%**
of incidents.

**GootLoader**
**10%**
of incidents.

**AsyncRAT**
**4%**
of incidents.

## RANSOMWARE ACTIVITY

**33** new or rebranded threat actors appeared between January 1 and December 10.

**75** groups actively posted to their leak sites during that time.

**573** leak site posts by popular Ransomware-as-a-Service (RaaS) group RansomHub from January through November, second only to LockBit at 579.

## MFA: MORE IMPORTANT THAN EVER

**56% OF INCIDENTS**

between January 1 and November 30 involved remote access to systems where multi-factor authentication (MFA) was missing or unenforced — **making inadequate MFA the largest driver of incidents for the year.**

Source: **2024 Threat Landscape Statistics: Ransomware Activity, Vulnerability Exploits, and Attack Trends**

RAPID7