IT NATION

SECURE™

hosted by ⋀ CONNECTWISE

MSP Threat Report

Presented by Drew Sanford & Bryson Medlock

IT NATION™ SECURE

Agenda

Key findings from the 2023 MSP Threat Report

- 2022 security incidents in review
- Ransomware
- Vulnerabilities

How to protect yourself and clients with enterprise-class cybersecurity solutions

MSP Threat Briefing Series

*Threat briefing series focused on the **MSP** cybersecurity landscape*

In this series we cover:

- A review of major **MSP-focused** threats

- Emerging and continuing cyberattack trends

- Actions MSPs can take in 2023 to thwart the threats

IT NATION

One of the most important steps an MSP can take to improve their cybersecurity posture is to leverage threat intelligence.

-

2023 MSP Threat Report Findings

These findings are based on an analysis of over half a million discrete incidents by the **ConnectWise Cyber Research Unit (CRU)**—a dedicated team of seasoned cybersecurity professionals with deep engineering, IT administration, security operations, and incident analysis and response expertise who identify and research new vulnerabilities and publicly share what they find across the community.

The CRU monitors ransom leak sites and malicious botnets for new threats, uses OSINT resources, and utilizes data from ConnectWise SIEM™ to help create content and complete research.

IT NATION

2023 MSP Threat Report Findings: 2022 Security Incidents

The CRU reviewed data from over 440,000 cybersecurity incidents that impacted our MSP partners and their clients in 2022. Below is a breakdown of the number of incidents reviewed per business sector.

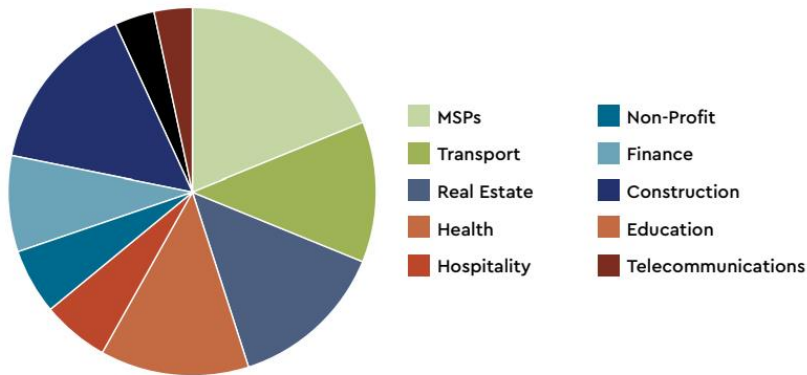## Top 10 MITRE ATT&CK® Techniques in Security Incidents

Security Incidents by Sector

Legend:
- MSPs
- Transport
- Real Estate
- Health
- Hospitality
- Non-Profit
- Finance
- Construction
- Education
- Telecommunications

Figure 1.0: Top 10 Business Sectors affected by the 440,000 security incidents reviewed by the CRU in 2022

Legend:
- T1203 - Exploitation for Client Execution
- T1547 - Boot or Logon Autostart Execution
- T1218 - System Binary Proxy Execution
- T1202 - Indirect Command Execution
- T1055 - Process Injection
- T1485 - Data Destruction
- T1486 - Data Encrypted for Impart
- T1078 - Valid Accounts
- T1490 - Execution Guardrails
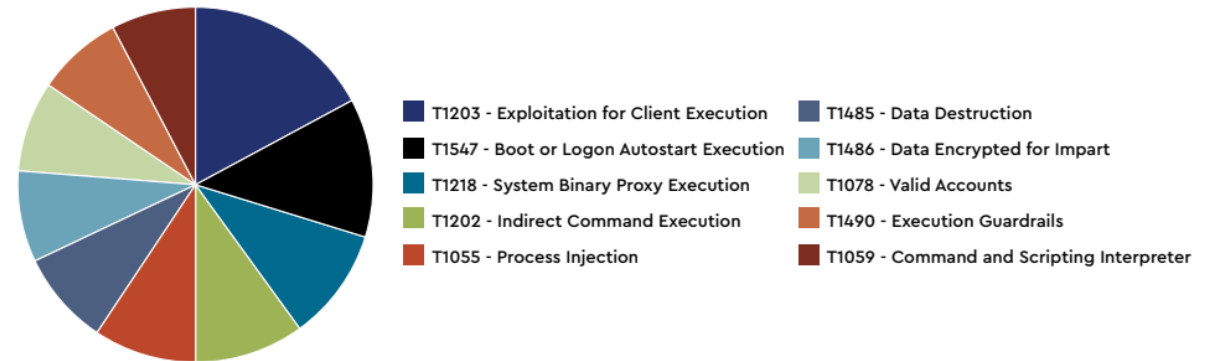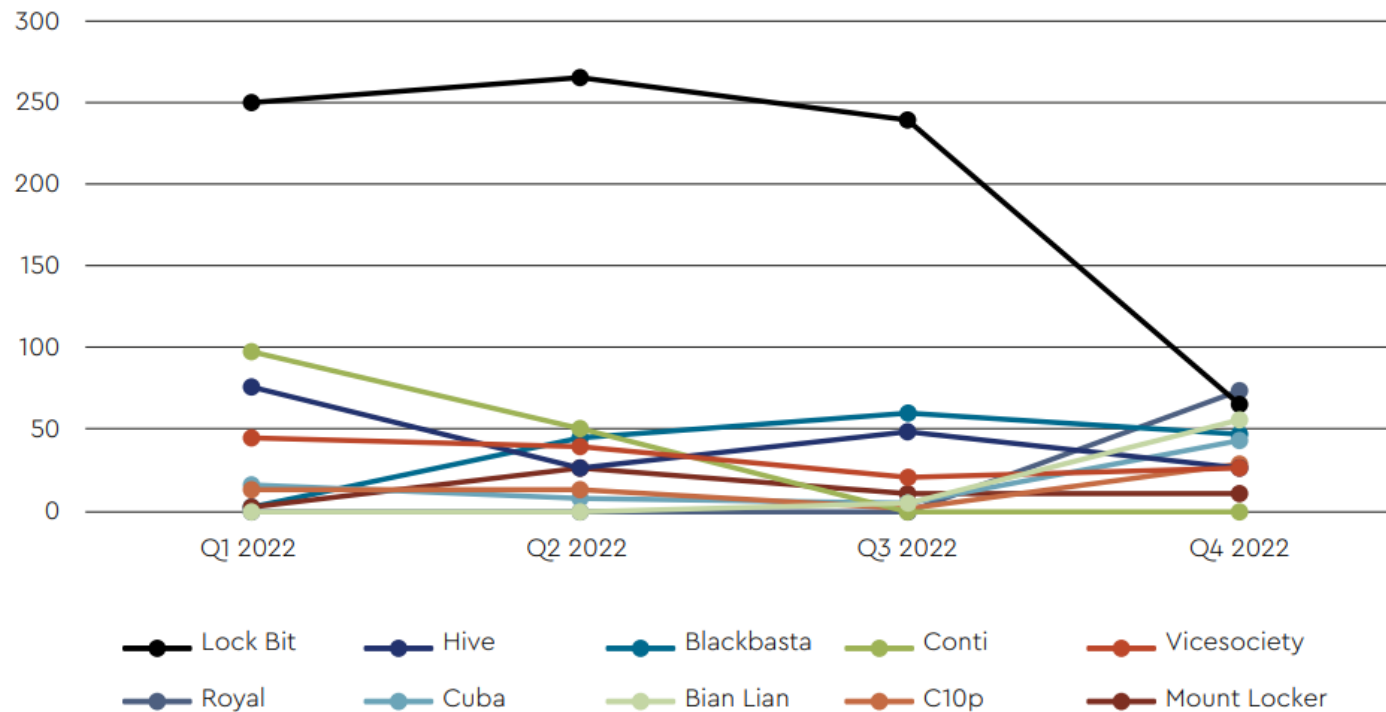- T1059 - Command and Scripting Interpreter

Figure 1.1: Top 10 MITRE ATT&CK(C) Techniques observed in the 440,000 security incidents reviewed by the CRU in 2022

IT NATION

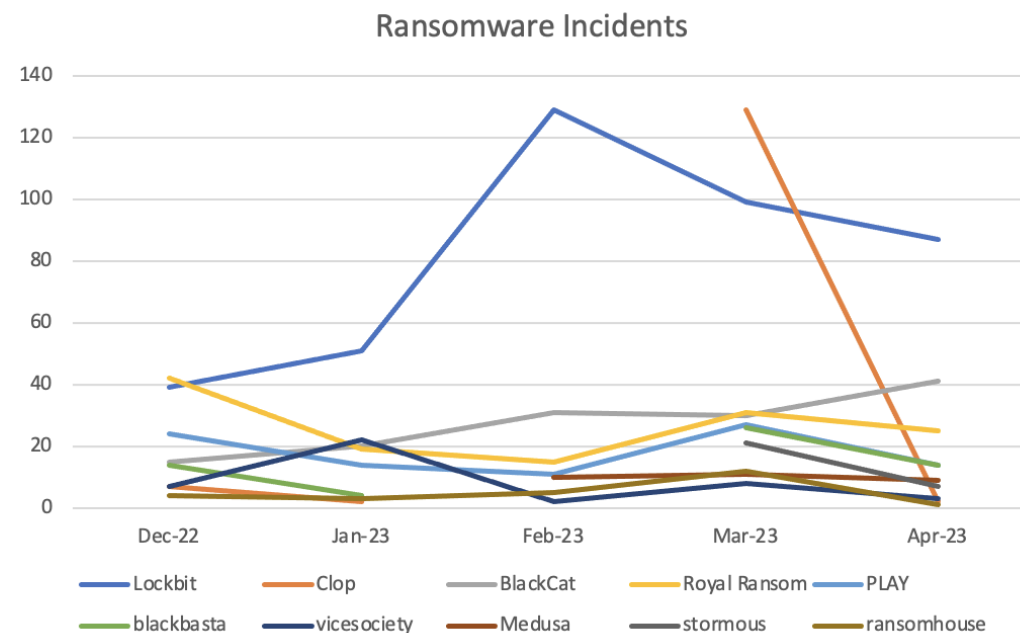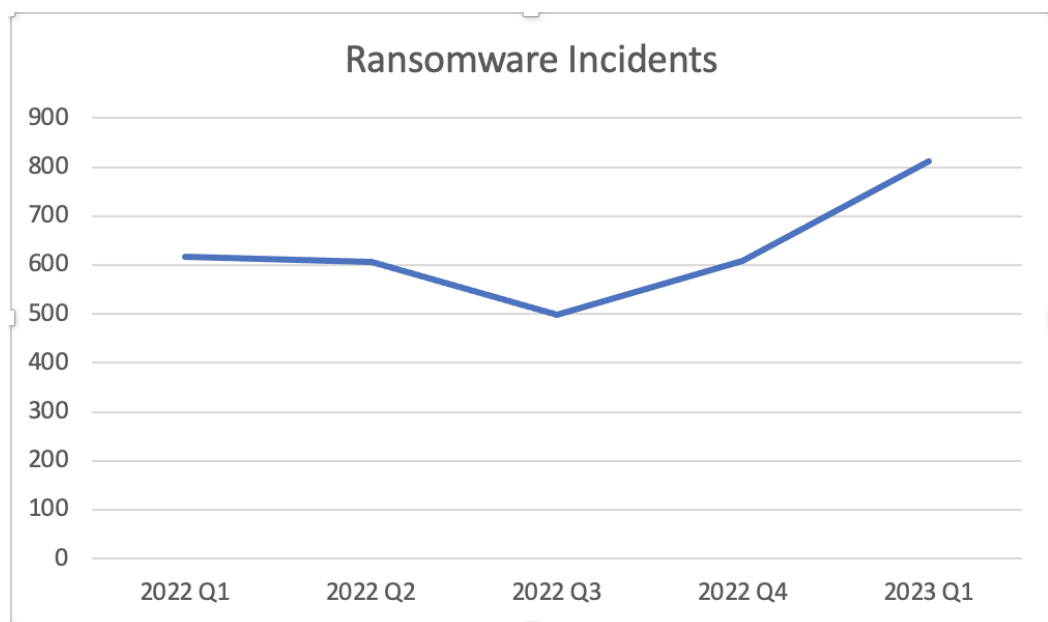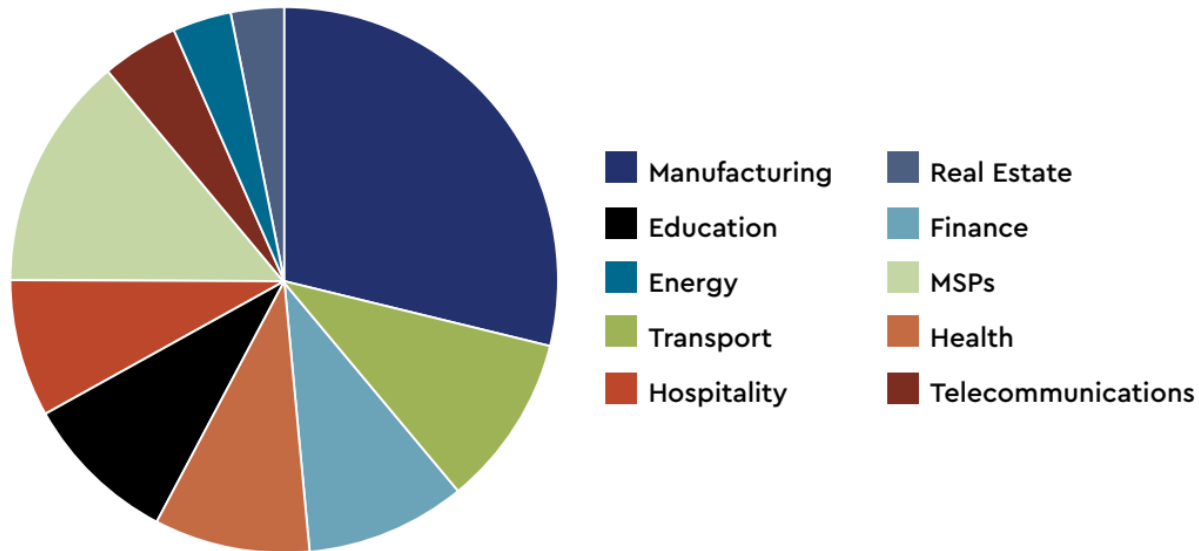# 2023 MSP Threat Report Findings: Ransomware

Top 10 Ransomware in 2022

IT NATION

2023 MSP Threat Report Findings: Ransomware

Business Sectors targeted by Ransomware 2022

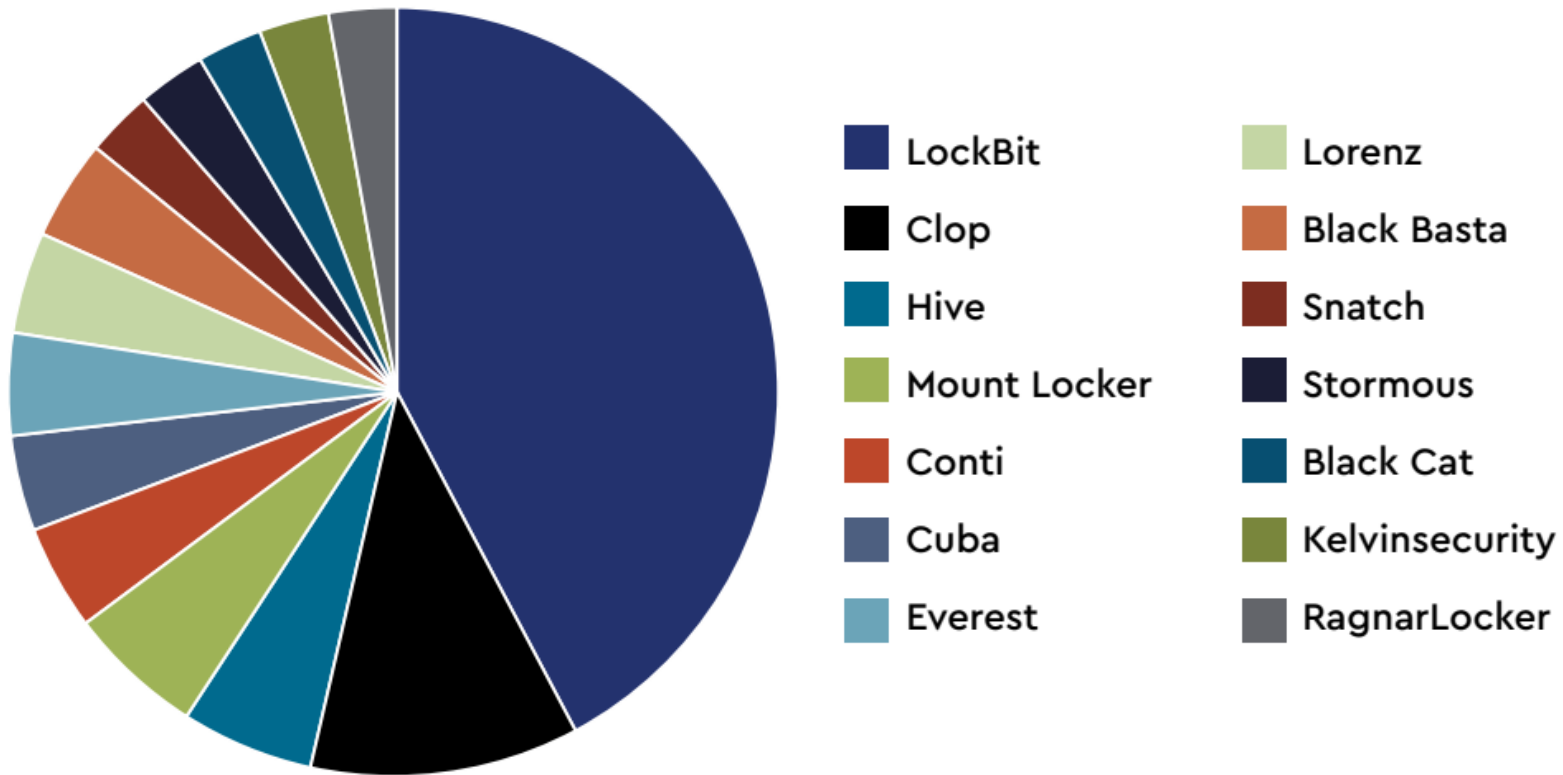- Manufacturing
- Education
- Energy
- Transport
- Hospitality
- Real Estate
- Finance
- MSPs
- Health
- Telecommunications

Top 10 Countries targeted by Ransomware 2022

- USA
- Germany
- Italy
- United Kingdom
- France
- Canada
- Spain
- Brazil
- Switzerland
- India

IT NATION
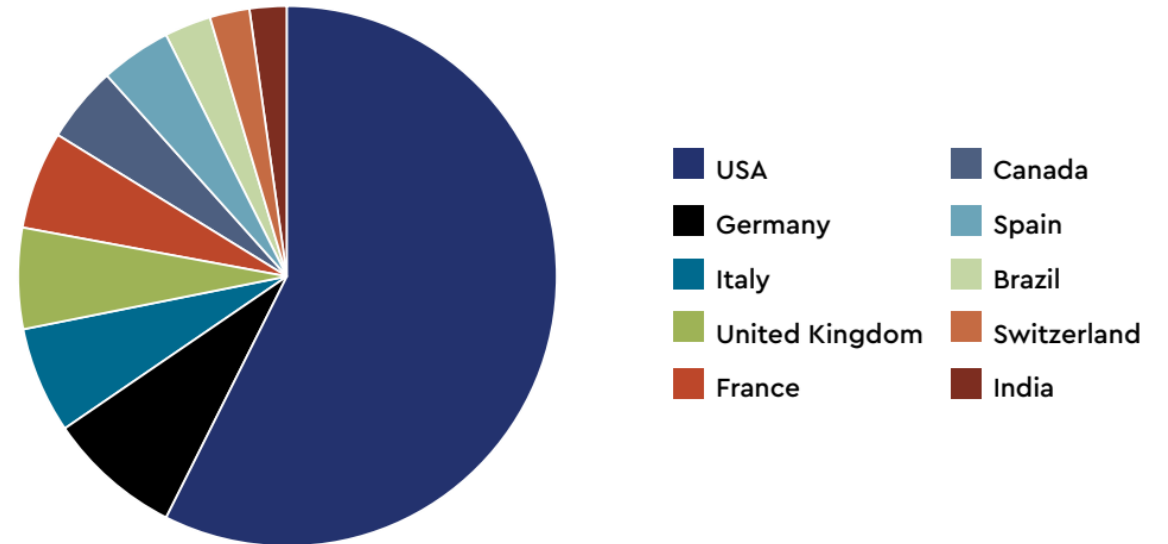
2023 MSP Threat Report Findings: Ransomware

Ransomware Targeting MSPs

Legend:
- LockBit
- Clop
- Hive
- Mount Locker
- Conti
- Cuba
- Everest
- Lorenz
- Black Basta
- Snatch
- Stormous
- Black Cat
- Kelvinsecurity
- RagnarLocker

IT NATION

Don't forget to fill out your

SESSION SURVEY