MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Oregon State Legislature

Joint Committee On Information Management and Technology

Randy Rose
Senior Director of Intelligence
September 22, 2021

Who We Serve

MS-ISAC Membership

117
New Members Since August 2

11,574
Total Members

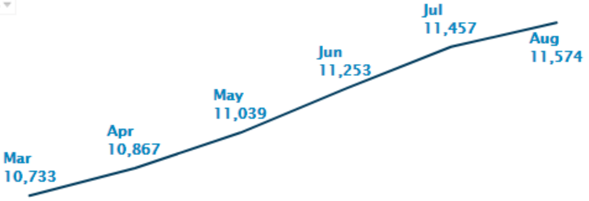
50 States

80 Fusion Centers

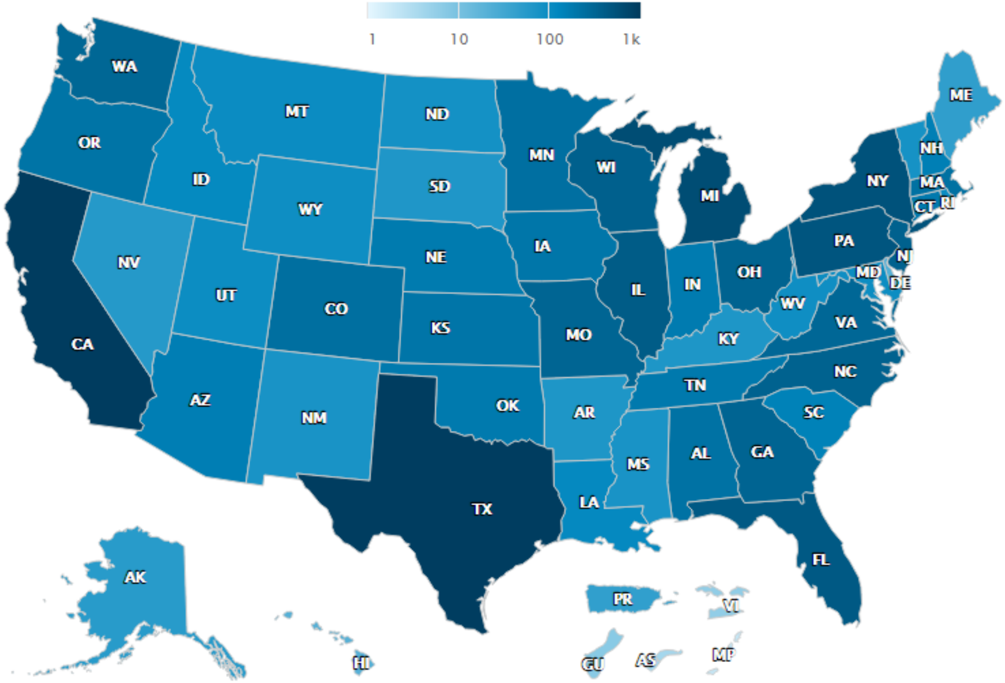
163 Tribal

68 Territory

11,213 Other



Membership Growth



Confidential & Proprietary

TLP:WHITE

MS-ISAC®

Security Operations Center

24 x 7 x 365

Support

Network Monitoring Services
+
Research and Analysis

Analysis & Monitoring

Threats, Vulnerabilities
+
Attacks

Reporting

Cyber Alerts & Advisories

Web Defacements

Account Compromises

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Confidential & Proprietary

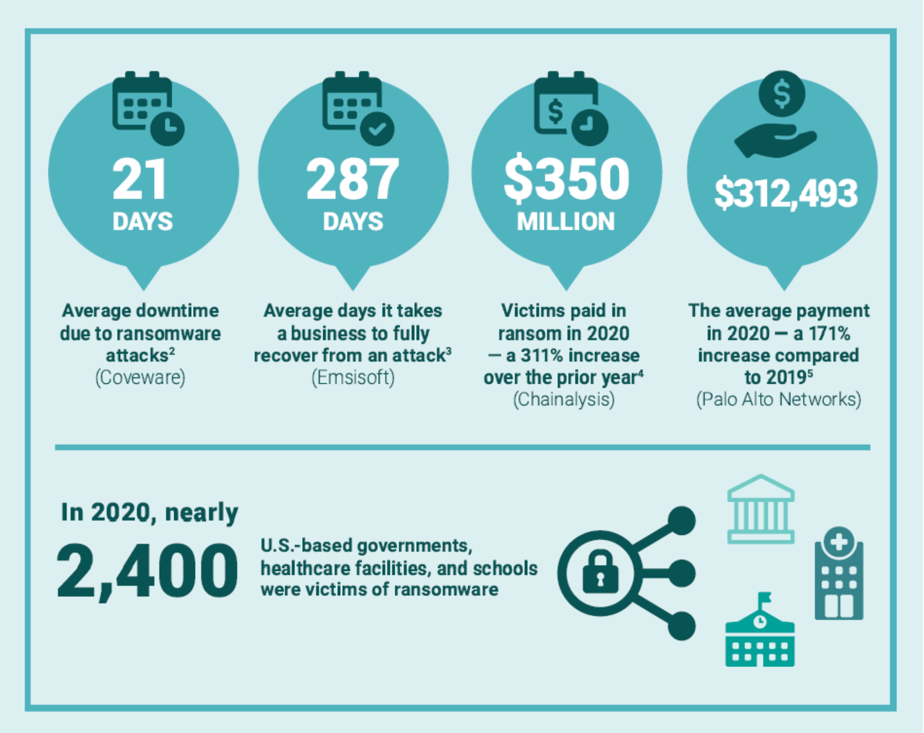
MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

The Scope of the Threat to SLTTs

Ransomware

Highest Impact Threat for SLTTs

- Malware typically encrypts data and attacker holds the key for ransom
- Evolution from commodity ransomware to big game hunting or post-compromise ransomware
- Increased use of double extortion
- Nearly half of all victims experienced data corruption
- Ransoms for SLTTs have increased into the 6 figure range
- Largest ransom ever paid ($40M) in 2021



21 DAYS
Average downtime due to ransomware attacks[2]
(Coveware)

287 DAYS
Average days it takes a business to fully recover from an attack[3]
(Emsisoft)

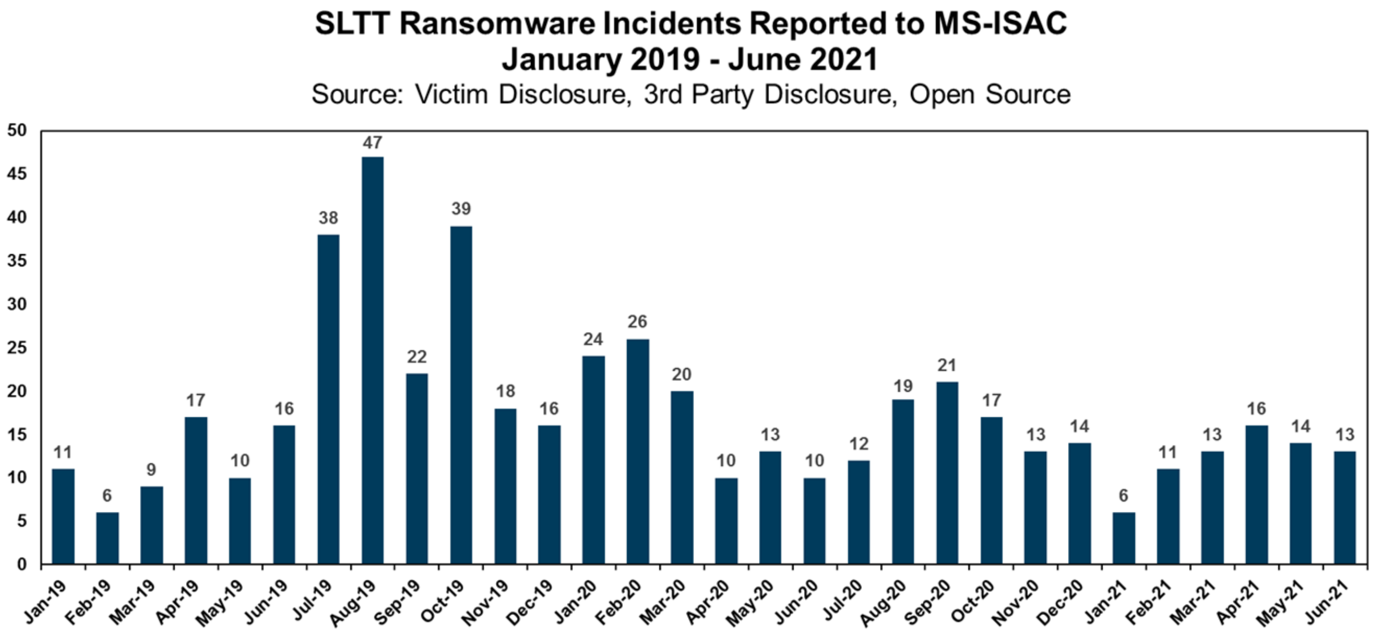
$350 MILLION
Victims paid in ransom in 2020 — a 311% increase over the prior year[4]
(Chainalysis)

$312,493
The average payment in 2020 — a 171% increase compared to 2019[5]
(Palo Alto Networks)

In 2020, nearly **2,400** U.S.-based governments, healthcare facilities, and schools were victims of ransomware

Ransomware Reporting Trends 2019 to Present

Across all MS-ISAC Membership


SLTT Ransomware Incidents Reported to MS-ISAC
January 2019 - June 2021
Source: Victim Disclosure, 3rd Party Disclosure, Open Source

- **153% increase of reported SLTT ransomware attacks from 2018 to 2019**
- **Increase attributed to:**
  - Relationship with dropper malware
  - Attacks on MSPs
  - Sophisticated Ransomware-as-a-Service (RaaS) model
- **Threat remained elevated in 2020, although 20% decrease in reporting**
- **Not depicted in the graph:**
  - Ransom demand increase
  - Double extortion increase
  - Intrusion vectors

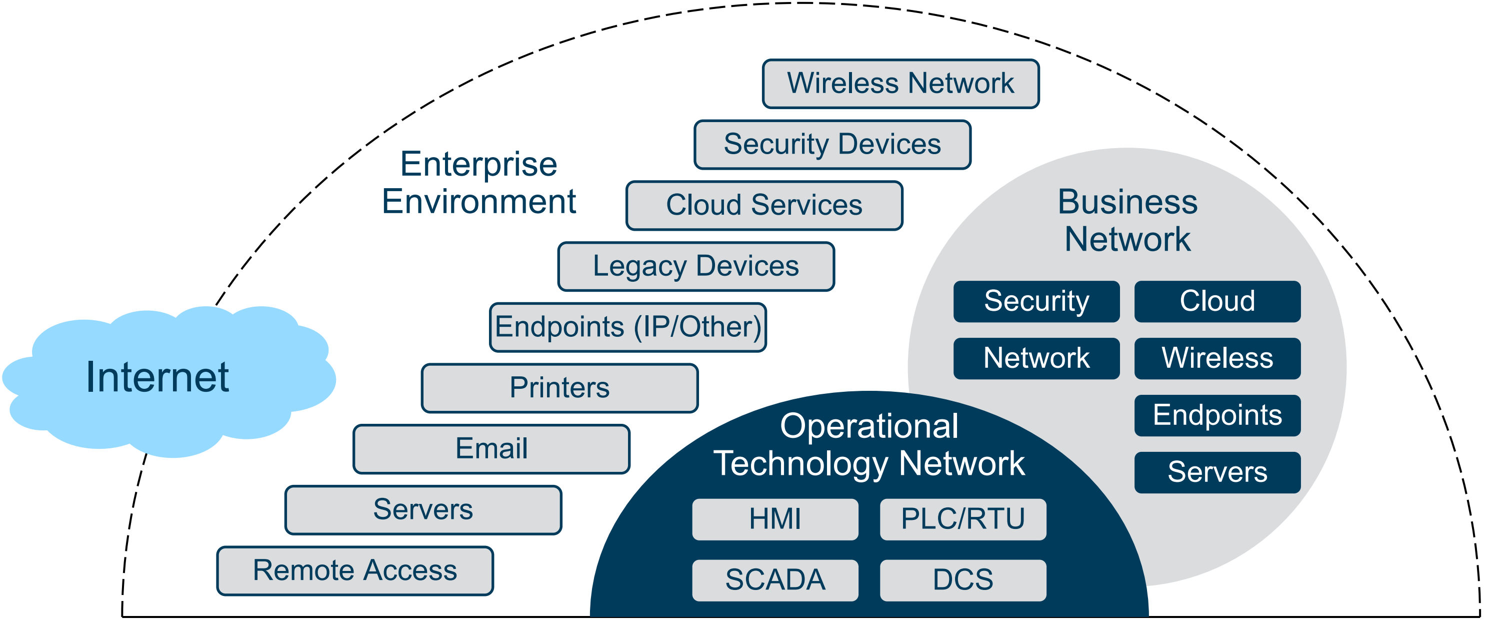
Confidential & Proprietary

TLP:AMBER

Public Safety Landscape

Increased Technology Integration Means Increased Attack Vectors

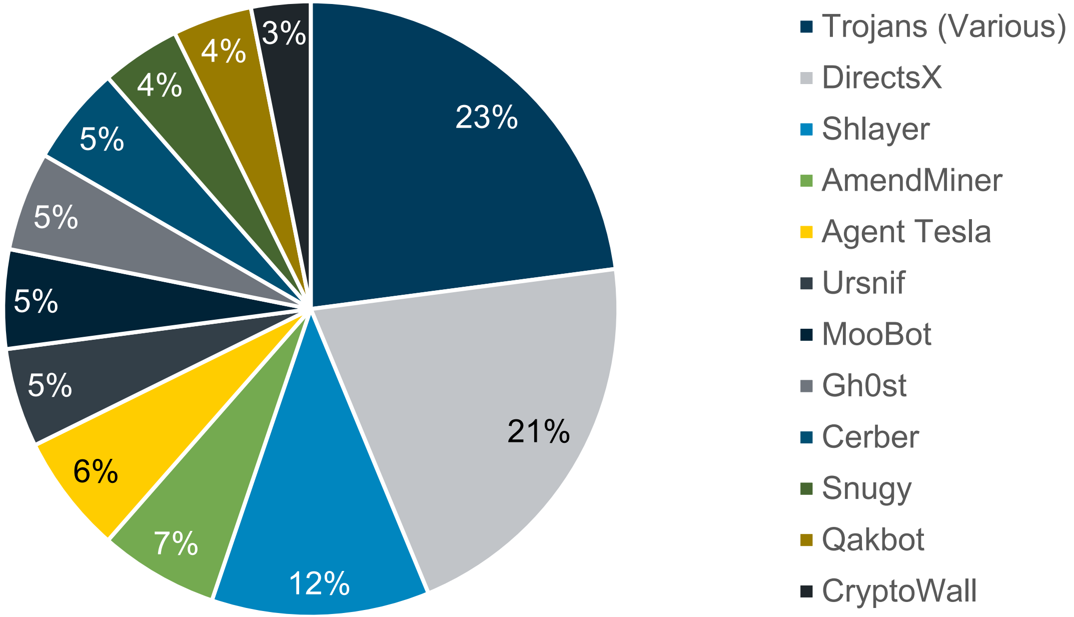
- Modern technology integration into OT networks increasing exponentially
- Air-gapping no longer an effective solution to modern threats



MS-ISAC®

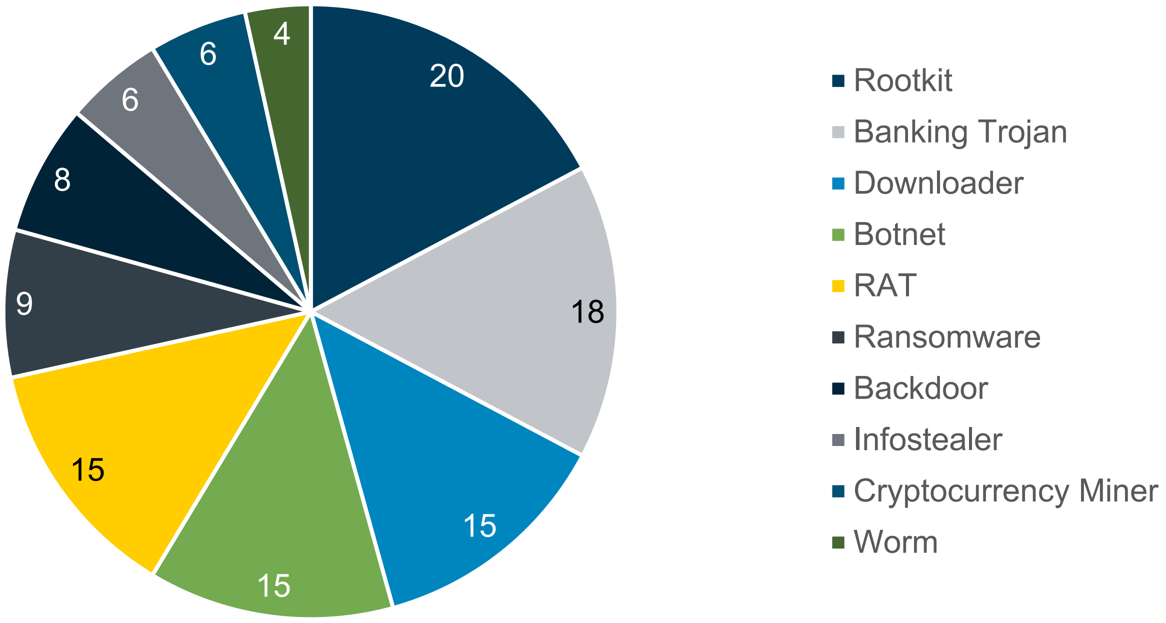
Oregon

Top 12 Malware Incidents Last Year



Oregon

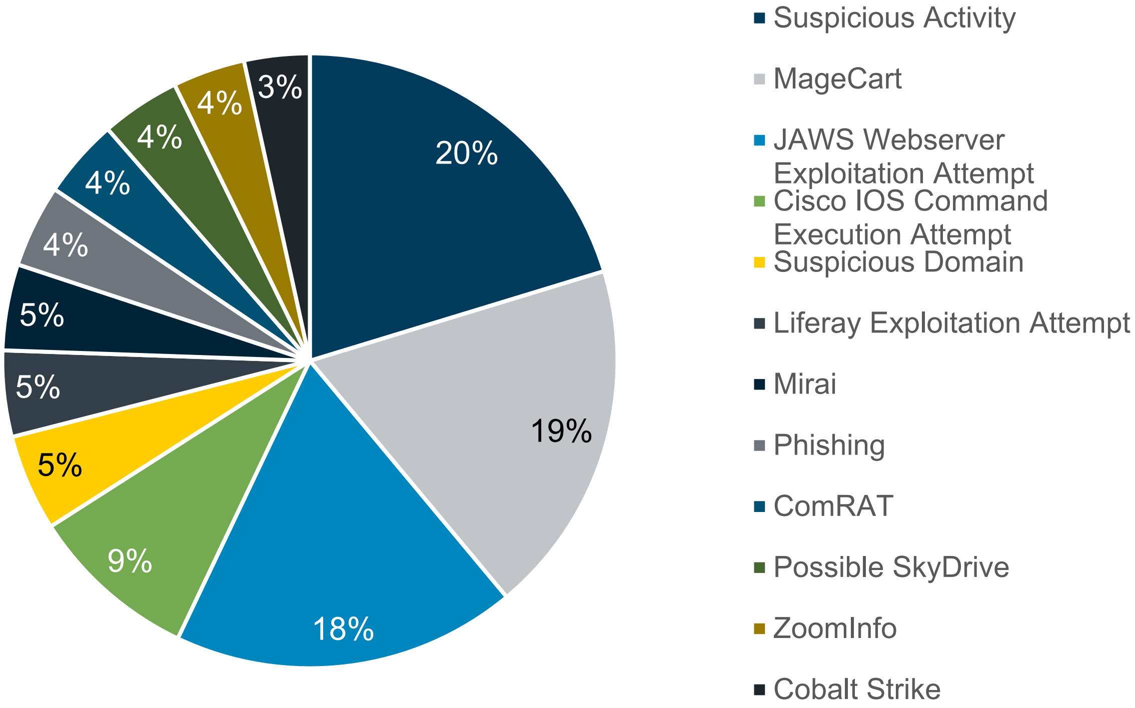
Top 10 Malware Incident Categories Last Year



MS-ISAC®

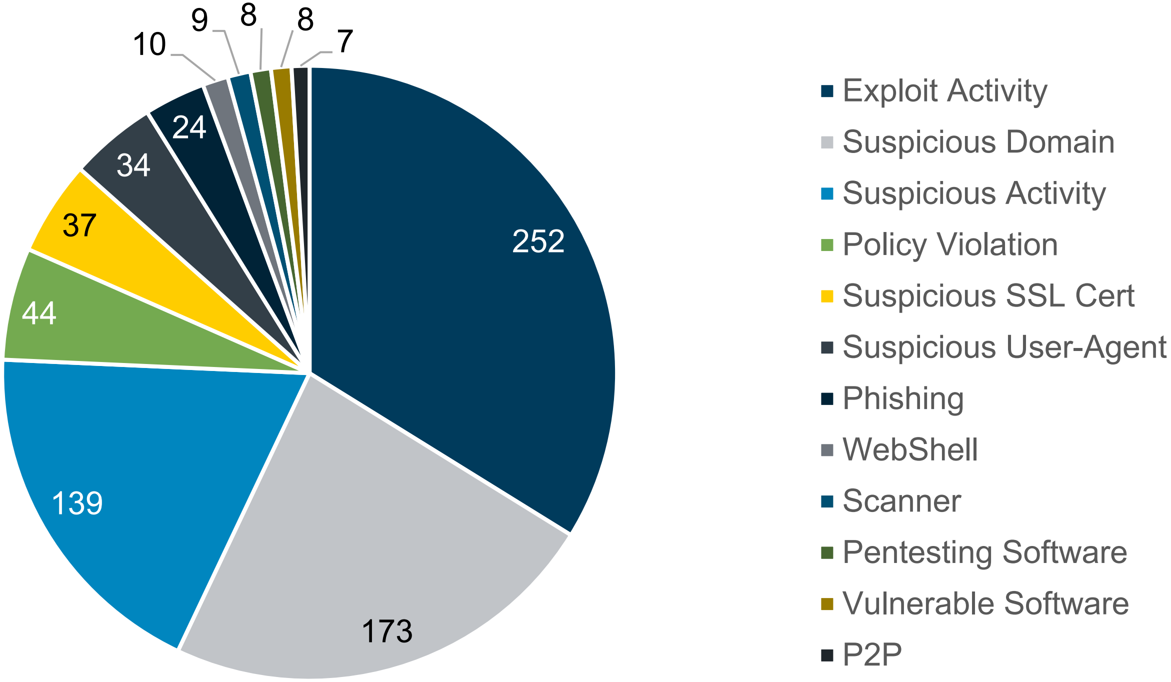
Oregon

Top 12 Non-Malware Incidents Last Year



Oregon

Top 10 Non-Malware Incident Categories Last Year



MS-ISAC®

Multi-State Information Sharing & Analysis Center®

Recommendations

Recommendations

Building a Cybersecurity Culture

- **Encourage Oregon SLTTs to join the MS-ISAC!**
  - Take advantage of our free cybersecurity services for SLTTs
  - Seek our help in applying for the grants under the new infrastructure bill
- **Implement the 18 CIS Controls starting with Implementation Group 1**
- **Use Hardened Images and CIS Benchmarks**
- **Regularly audit critical systems, especially those with direct access to the Internet, such as those found in hospitals, power plants, and water sanitation systems**

MS-ISAC®

Multi-State Information Sharing & Analysis Center®

Thank You