securonix

2023 Threat Landscape Retrospective: Key Threats and Trends Analyzed by Securonix ATS

Quarterly Threat Highlights

Q1

Found by Microsoft, **Threat actor MERCURY collaborates with DEV-1084** in resource disruption and destruction across on-premises and cloud networks. Of note, DEV-1084 waits weeks to months in reconnaissance and lateral movement.

Securonix Threat Labs identifies TACTICAL#OCTOPUS, in a complex and targeted phishing scheme using tax-themed emails to distribute malware to U.S. entities.

First observed in late 2022, **Royal Ransomware targets critical infrastructure** like manufacturing and healthcare, bypassing signature-based detection methods.

Q2

Since patched, **MOVEit Transfer web application found to have several SQL injection flaws.**

Cl0p ransomware group identified as responsible for MOVEit vulnerability attackers.

Q3

Rhysida Ransomware targets large range of sectors with phishing attacks and Cobalt Strike to infiltrate networks and deploy their ransomware.

Okta reports security breaches where threat actors accessed Okta's support case management system using credentials stolen from social engineering.

Q4

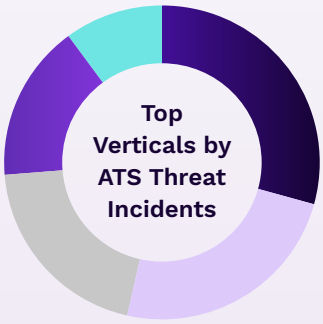
Israel and Hamas conflict extends beyond physical battlefields into cyberspace with DDoS attacks targeting Israeli public warning websites, starting in parallel with Hamas missile attacks on Israeli cities.

Citrix releases security bulletin around Bleed vulnerability for Citrix NetScaler ADC and Gateway appliances. Attackers bypassed password requirements and multi-factor authentication, leading to session hijacking and enabling lateral movement, credential harvesting, and data access.

Targeted Sectors

The aviation industry saw a significant rise in cybersecurity threats, placing it among the top five sectors for escalated ATS threat incidents. The MOVEit software compromise and high-profile data breaches at major carriers like Southwest Airlines underscore a growing trend of cyberattacks aimed not only at data theft but also at undermining the overall security and operations of the aviation sector.

- **29.7%** - Technology
- **16%** - Healthcare
- **13.1%** - Financial
- **10.9%** - Real Estate
- **10.3%** - Aviation
- **6.9%** - Food and Beverage
- **6.9%** - Entertainment
- **6.3%** - Manufacturing



- **29.7%** - Technology
- **24%** - Financial
- **20%** - Other
- **16%** - Healthcare
- **10.3%** - Aviation

2023 Cyber Threats Retrospective

Autonomous Threat Sweeper

300+
Elevated Threat Incidents

2.2K
Cumulative Hours Saved

1.5K
Emerging Threats Analyzed & Swept

45K
TTPs/IoCs Codified & Swept

2.1K
Investigated Potential Threats

250
Unique Threat Sources Reviewed

Top 5 ATS Data Sources

1. IDS/IPS/Threat Detection
2. Data Loss Prevention (Endpoint/Network)
3. Endpoint Management
4. Email/Email Security
5. Antivirus/Malware/EDR

Top 5 Threats Identified

1. Malicious extensions in Chrome Web Store
2. Mallox Ransomware
3. Trigona Ransomware
4. ProxyNotShell
5. Royal Ransomware

Top 5 IoC Types Codified

1. Hash Values
2. Domain
3. IP Address
4. URL
5. Process Name

Learn More About Securonix ATS

Securonix Autonomous Threat Sweeper (ATS) complements security operations teams by automatically hunting for new and emerging threats in current and long-term historical data based on the latest threat intelligence from external feeds and our internal Securonix Threat Labs.

ATS detects TTPs through a combination of machine learning and human curation to analyze patterns and anomalies in historical SIEM data. This approach proactively combines the latest threat data and research to identify ongoing attacks and uncover latent threats that may have been overlooked, were previously undetectable, or are biding time within a network. ATS then automates the initiation of incident response.

This infographic summary captures major cybersecurity challenges and responses in 2023. For a deeper dive into specific threats and detailed analyses, visit us at securonix.com or email scia@securonix.com.