Trellix ADVANCED RESEARCH CENTER

Threat Intelligence Group

Advanced Research Center

Threat Analysis Report: US Financial Sector

Period: December 31, 2024 - March 31, 2025 (90 days)
Sector Focus: Financial
Region: United States
Report Date: March 31, 2025

The information presented in this report was compiled from Trellix's Insights platform as well as Trellix's Advanced Threat Landscape Analysis System (ATLAS).

Insights data is collected and vetted, from internal research as well as open-source data incidents and events by the Trellix Threat Intelligence Group (TIG).

ATLAS is a data analysis tool that seamlessly integrates Trellix's data sources (Repper, REST, RealProtect, JCM, etc.) and provides enrichment data for global emerging threats such as sector and geolocation.

The data from both platforms is correlated to provide a dedicated view for campaigns consisting of events, threat actors, IOCs, and more. The Trellix Insights and ATLAS platforms give customers unprecedented access to malicious file, domain, and IP detections from Trellix's sensors strategically placed around the globe.

Executive Summary

This comprehensive threat analysis report combines intelligence from multiple sources including ransomware activity, campaign data, underground forums, and threat actor analysis to provide a holistic view of threats targeting the US financial sector over the past 90 days.

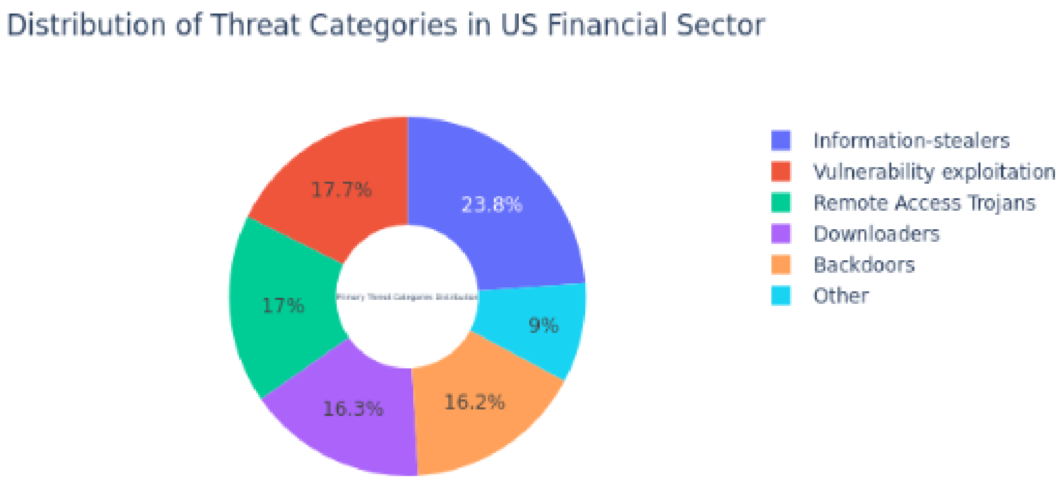
Key Findings

1. Threat Activity Volume

- Over 66 million security detections recorded
- 599 unique malicious campaigns identified
- Peak activity observed in late March 2025
- Limited public ransomware disclosures, likely due to strong security measures and non-public incident handling

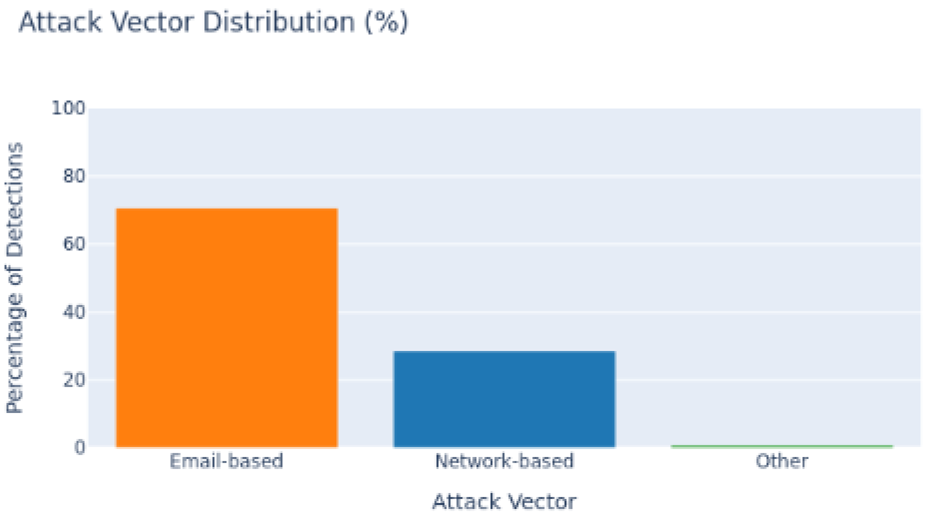
2. Primary Threat Categories

- Information-stealers (23.8%)
- Vulnerability exploitation (17.7%)
- Remote Access Trojans (17.0%)
- Downloaders (16.3%)
- Backdoors (16.2%)



3. Attack Vectors

- Email remains dominant (70.6% of detections)
- Network-based attacks (28.6% of detections)
- Multiple layers of attack observed through endpoint security
- Heavy focus on cloud-based infrastructure, particularly data warehouses



4. Notable Threat Actors

Ransomware Groups

- Clop
- Ransomhub
- Akira
- Babuk-Bjorka
- Lynx

UNC5537 (Emerged 2024)

- Financially motivated threat actor
- US-based with international connections
- Specializes in database and data exfiltration
- Uses sophisticated tools targeting cloud infrastructure

Equation Group

- State-sponsored actor with extremely high sophistication
- Global presence across 42+ countries

Copyright © 2024 Musarubra US LLC

- Advanced custom malware capabilities
- Targets multiple sectors including financial institutions

5. Underground Criminal Activity

Banking Fraud Operations

- Multiple threat actors targeting major US banks
- Advertised transaction limits:
  - Chase/BOA: $10,000-15,000
  - USAA: $7,000-20,000
  - PNC: $7,000-15,000
  - Wells Fargo: $5,000-10,000

Data Trading

- Credit card data (CVV) selling for $30-45 per record
- Large-scale breach data available (100,000+ records)
- Business banking accounts specifically targeted
- Organized operations with profit-sharing arrangements

Notable Database Breach

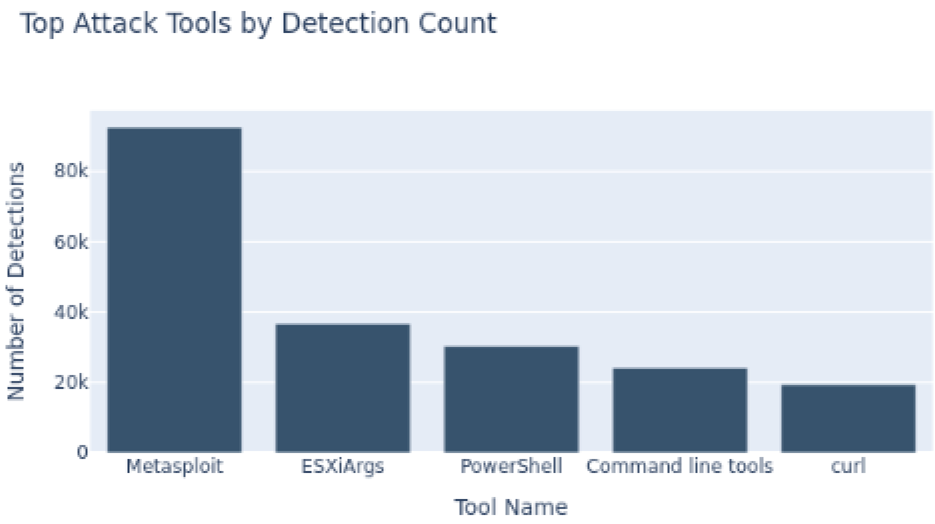
- Significant Gemini cryptocurrency exchange breach
- Approximately 100,000 US customer records exposed
- Targeting high-income individuals and financial sector customers

Attack Tools and Techniques

Most Common Attack Tools

1. Metasploit (92,457 detections)
2. ESXiArgs Ransomware (36,632 detections)
3. PowerShell (30,249 detections)
4. Command line tools (24,158 detections)
5. curl (19,406 detections)

Copyright © 2024 Musarubra US LLC



Sophisticated Custom Tools

- SnowSight: Advanced SQL/Python-based data analysis
- FrostBite: Custom reconnaissance tool
- Bvp47: Sophisticated Linux backdoor
- DoublePulsar: Memory-based kernel payload

Conclusion

The US financial sector faces a complex threat landscape combining sophisticated state-sponsored actors, organized cybercrime groups, and emerging threats targeting cloud infrastructure. While the sector demonstrates strong security maturity, continued vigilance and security enhancement are essential to address evolving threats.

The combination of limited public ransomware disclosures and high detection volumes suggests effective security measures are in place, but also highlights the need for continued investment in security infrastructure and monitoring capabilities.

Report generated: March 31, 2025 Trellix Threat Intelligence Group (TIG)
Classification: TLP:AMBER

Copyright © 2024 Musarubra US LLC