

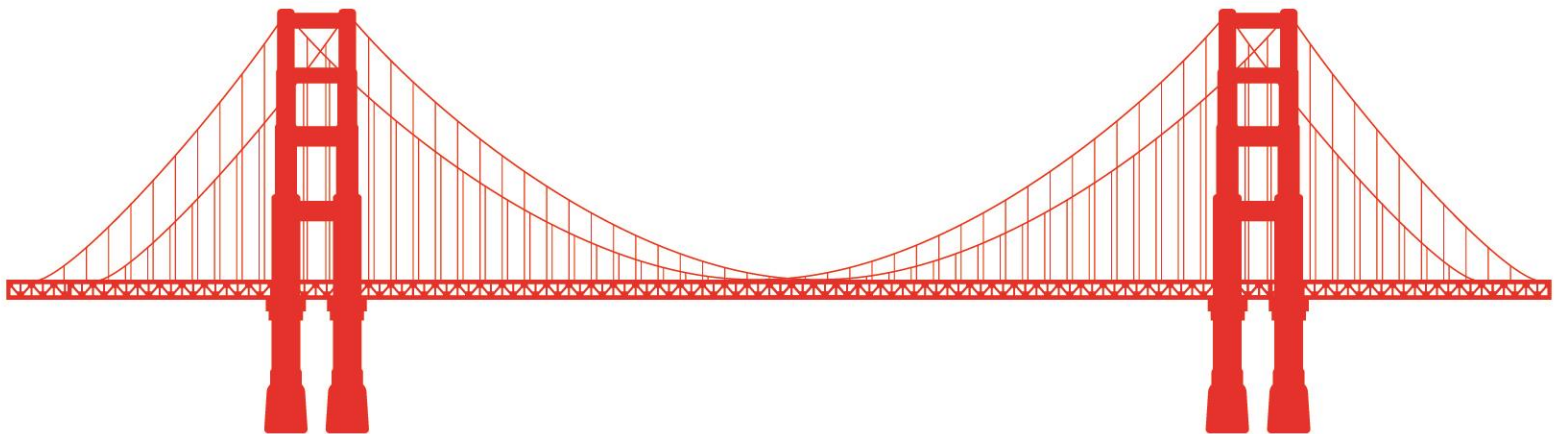


FEDERAL BUREAU OF INVESTIGATION  
**San Francisco Division**



# **Cyber Threat Forecast 2025**

**Ryan M. Pardee, Special Agent, Cyber Task Force**



# About the FBI



- 38,000 Employees
- Criminal and national security
  - Investigation Driven
- Share Cyber with USSS for criminal matters
- International and Domestic Focus



FEDERAL BUREAU OF INVESTIGATION  
**San Francisco Division**

UNCLASSIFIED



## FBI, HHS issue advisory on cyberthreat actors targeting health care to divert payments

🕒 Jun 25, 2024 - 04:12 PM

# Royal Ransomware FBI and CISA Releas

CYBERSECURITY ADVISORY

**Release Date:** August 07, 2024

## #StopRansomware: ALPHV Blackcat

ttacks have spread ac

**Last Revised:** February 27, 2024

**Alert Code:** AA23-353A

healthcare and public

improvised communication methods by creating victim-specific emails to notify of the initial compromise. Since mid-December 2023, of the nearly 70 leaked victims, the healthcare sector has been the most commonly victimized. This is likely in response to the ALPHV Blackcat administrator's post encouraging its affiliates to target hospitals after operational action against the group and its infrastructure in early December 2023.



FEDERAL BUREAU OF INVESTIGATION  
San Francisco Division

# HHS OCR Reported Breaches 2024



586 Total Breaches

Average Breach = 307,309 affected individuals

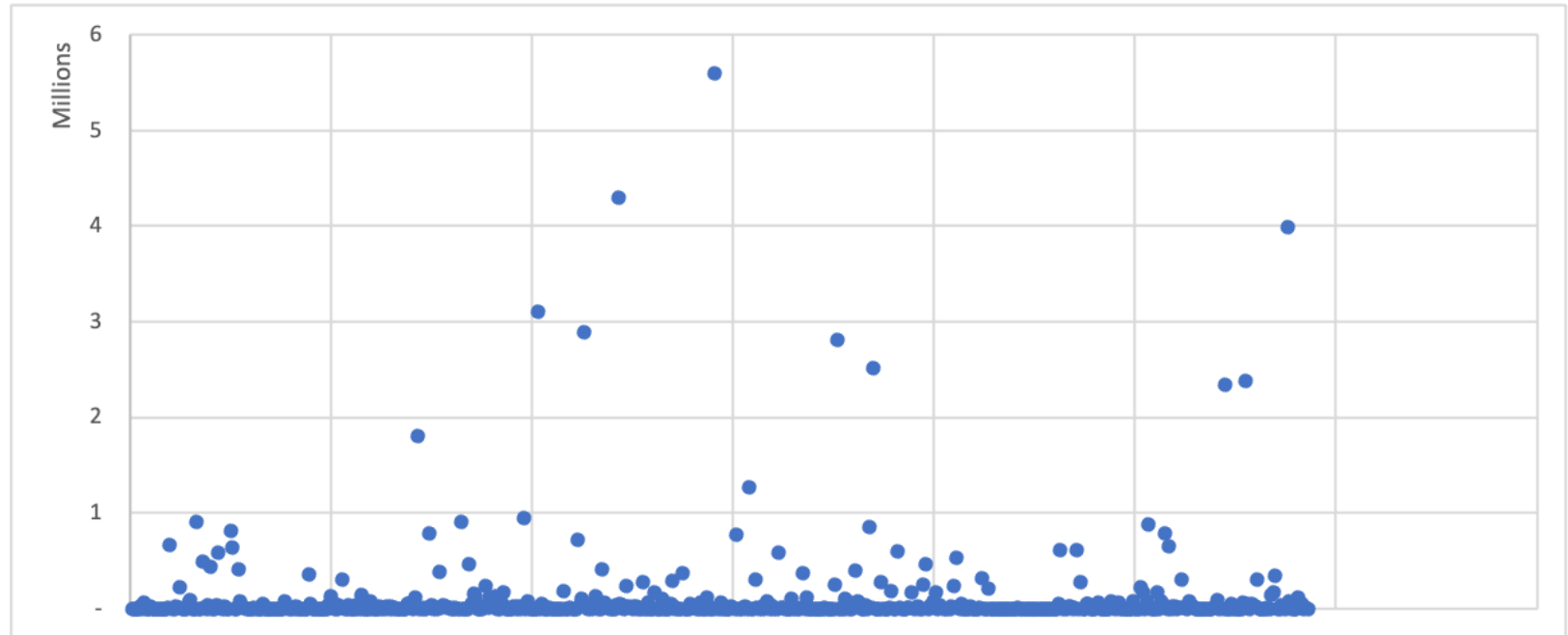


Chart missing two major breaches







– 100 Million and 13.4 Million



FEDERAL BUREAU OF INVESTIGATION  
San Francisco Division

# Cyber Threat Actors



	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
ACTIONS	Hacktivists might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.	Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.	Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.



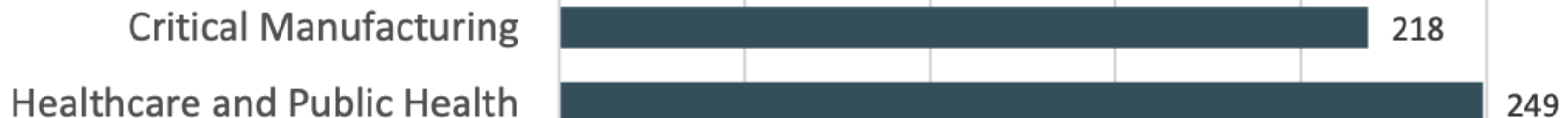
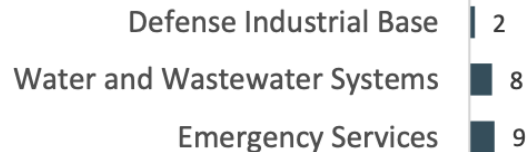
# Driving factors



- Direct payments - Ransomware
- Intrinsic value - Healthcare information
- Opportunistic - SOHO



## Infrastructure Sectors Affected by Ransomware



# Artificial Intelligence



Deepfakes



Malware



Big Data



Military  
Tech



Disinformation

- Deepfakes: False images, voice cloning
- Malware: Enhanced sophistication, faster and more efficient attacks, autonomous
- Big Data: Targeting and Collection
- Military Tech: Autonomous vehicles, hypersonic missiles
- Disinformation: Politically divisive issues to sow discord



# Defenses



- Social Engineering
- MFA
- Updates/Patches
- Back-up/Resilience
- Information sharing
  - FBI/CISA
  - Industry Groups
  - Infragard.org
- IC3.gov
  - FFKC



## 2023 CRIME TYPES

### By Complaint Count

<i>Crime Type</i>	<i>Complaints</i>
Phishing/Spoofing	298,878
Personal Data Breach	55,851
Non-payment/Non-Delivery	50,523
Extortion	48,223
Investment	39,570







# Thank You



FEDERAL BUREAU OF INVESTIGATION  
**San Francisco Division**