MANDIANT
NOW PART OF Google Cloud

CalPERS Cyber Threat Brief 2023

Insights into today's top cyber security trends and attacks

Jamie Parker
Mandiant; Strategic Intelligence & Government

Proprietary + Confidential

Agenda

01 Introduction

02 Supply Chain Compromise Trends

03 Cyber Crime Threats to the Financial Sector

04 Strategic Perspective: 2023 Trends, 2024 Forecast

MANDIANT
NOW PART OF Google Cloud

Supply Chain Compromise Trends

©2023 Mandiant

Supply Chain Compromise

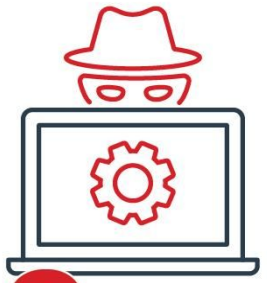
- Mandiant observed a significant rise in supply chain compromises in general, and in malicious software dependencies and developer tools in particular, though use of this tactic remains uncommon.
- We identified several state-sponsored incidents likely intended to support strategic intelligence collection missions. We attribute most observed incidents to China.
- Financially motivated incidents still outpaced state-sponsored cases.

MANDIANT IDENTIFIED EVIDENCE OF MORE SUPPLY CHAIN COMPROMISE INCIDENTS IN 2022 THAN ANY YEAR PREVIOUSLY EXAMINED, THOUGH USE OF THIS TACTIC REMAINS UNCOMMON.

INCREASE FROM 2021 TO 2022

IN 2022, SUPPLY CHAIN COMPROMISES INVOLVING DEVELOPER TOOLS OR SOFTWARE DEPENDENCIES ROSE DRAMATICALLY.

Mandiant identified state sponsored incidents likely intended to support strategic intelligence collection missions. **Most observed incidents we attribute to CHINA**



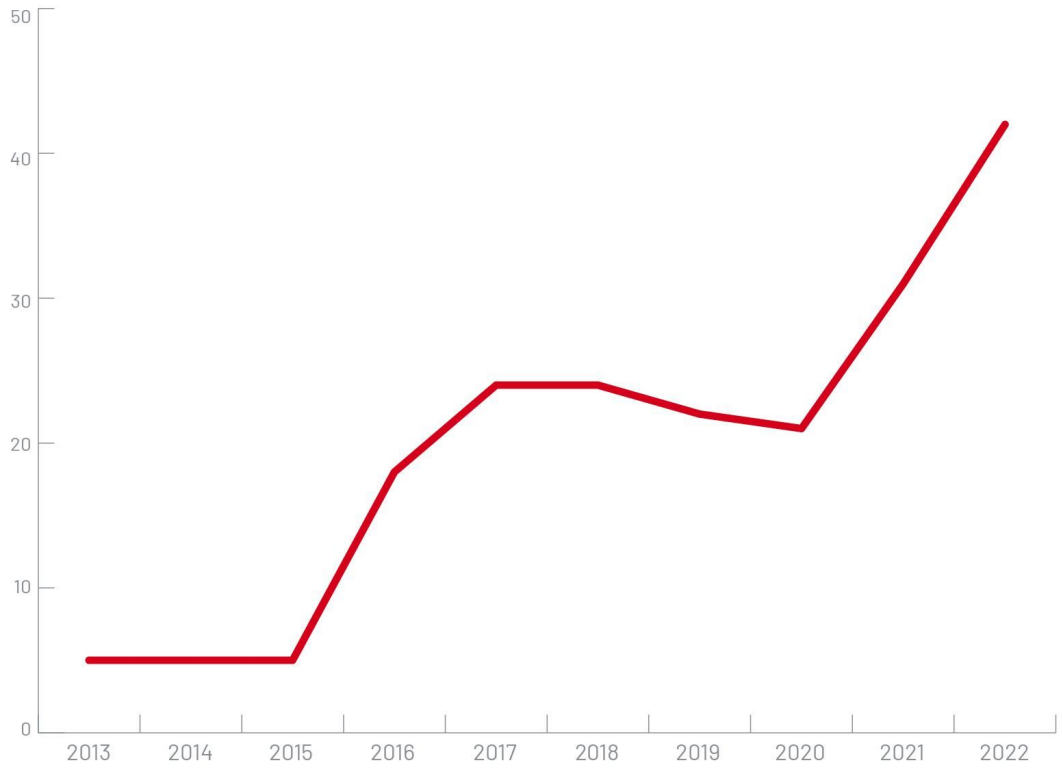
8 ESPIONAGE INCIDENTS

10 FINANCIAL INCIDENTS

Supply Chain Compromise Trends / Motivation

SUPPLY CHAIN COMPROMISES

2013-2022



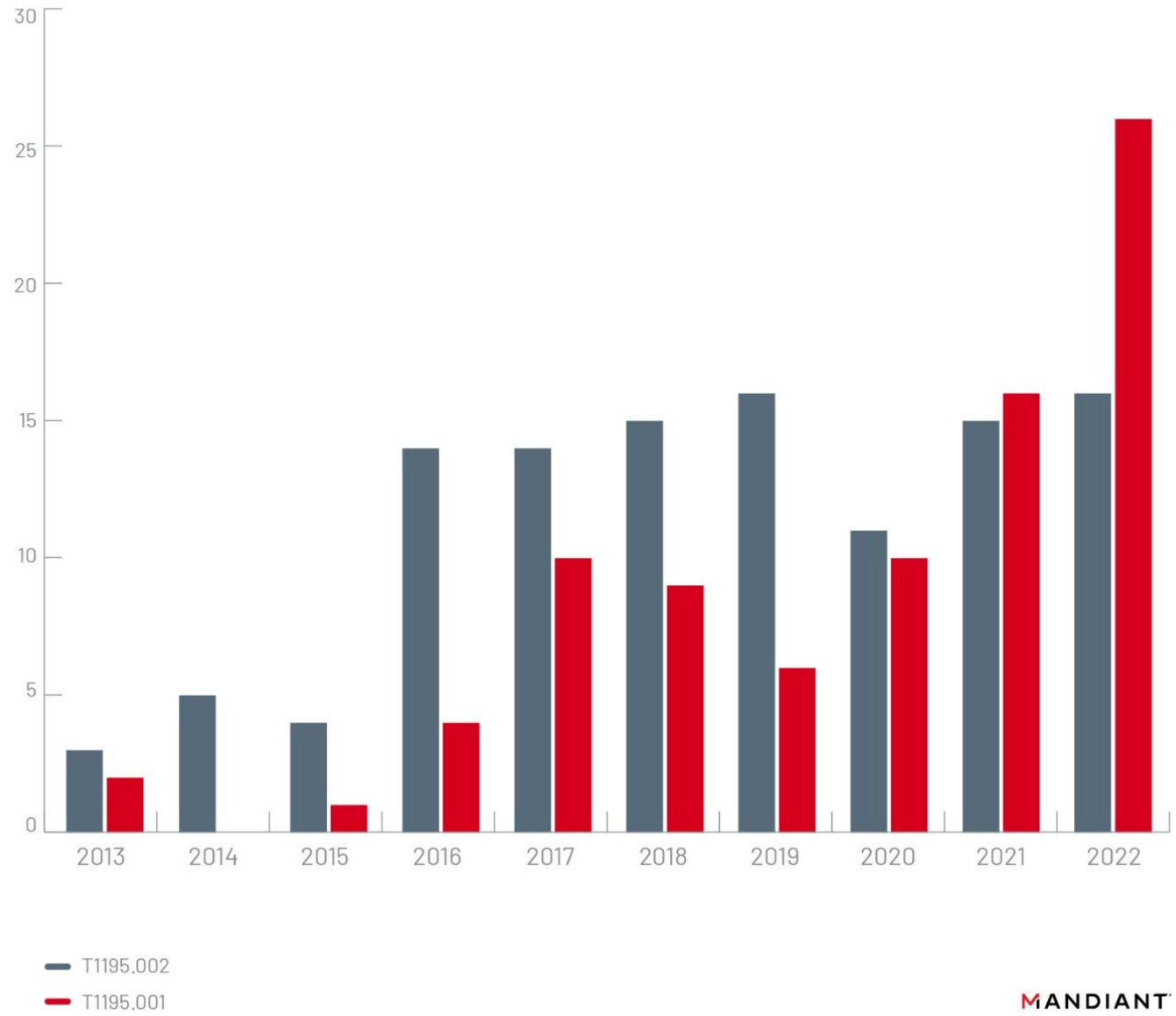
MANDIANT

SUPPLY CHAIN COMPROMISES WITH SUSPECTED ESPIONAGE AND FINANCIAL MOTIVATIONS

MANDIANT

Third-Party Resources and Developer Tools

- Open-source software and code packages as a cost-effective and efficient way to build and maintain their systems.
- Reliance on open-source code also introduces an expansive attack vector.



Supply chain compromises linked to state actors through September 2023

Motive	Suspected Sponsor	Actor	Trojanized Software	Malware
Espionage/Cyber Crime	North Korea	UNC4899	malicious npm packages	malicious payloads
Cyber Crime	North Korea	UNC4899	JumpCloud	malicious payloads
Cyber Crime	North Korea	UNC4736	3CX Desktop App, X_TRADER	malicious payloads
Espionage/Cyber Crime	North Korea	Lazarus Group	PyPI packages	malicious payloads
Espionage	China	Possible UNC3569	Cobra DocGuard	malicious payloads
Espionage	China	TEMP.TICK (UNC135)	legitimate tool installers	"ShadowPy," "Netboty," "Ghostdown"

©2023 Mandiant

MANDIANT
NOW PART OF Google Cloud

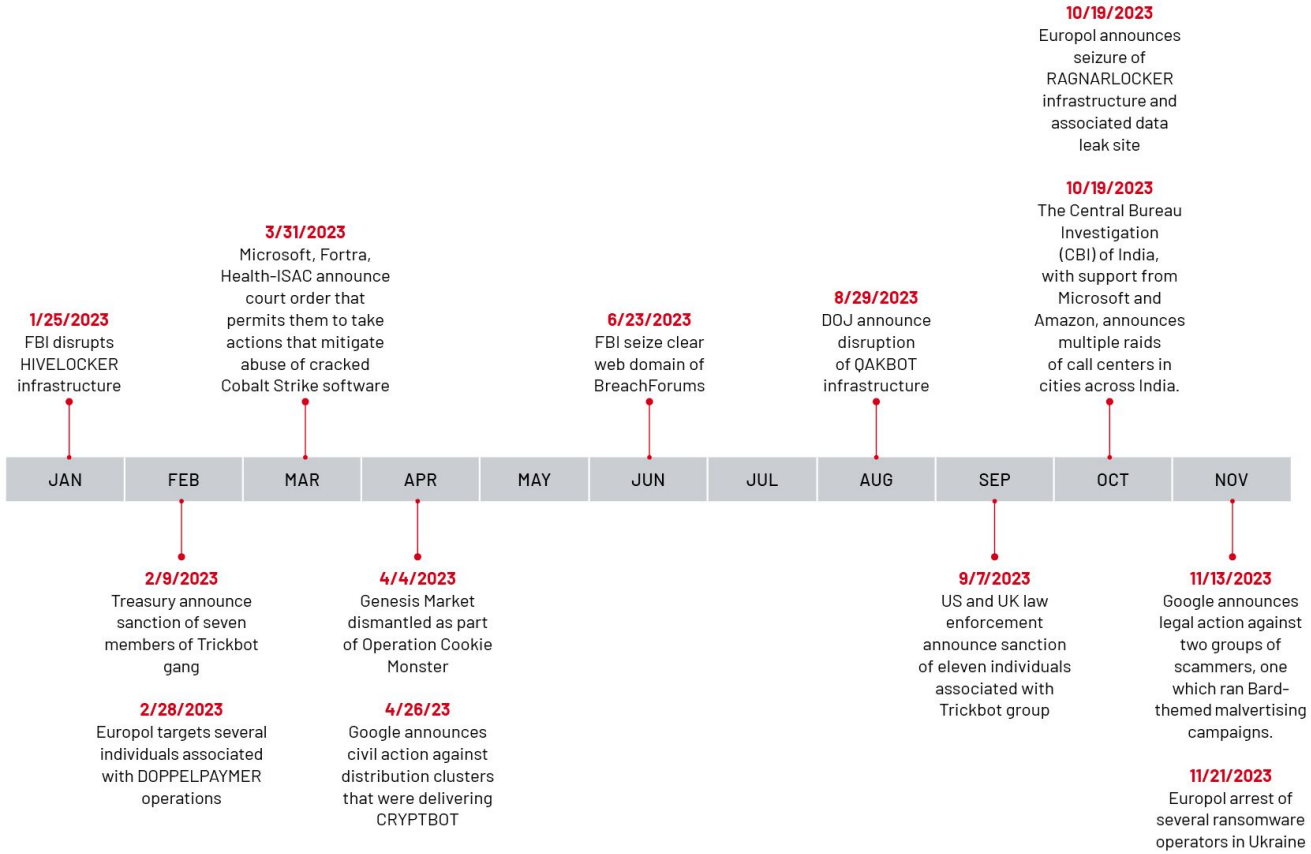
Cyber Crime Threats to the Financial Sector

©2023 Mandiant

Significant Events 2023

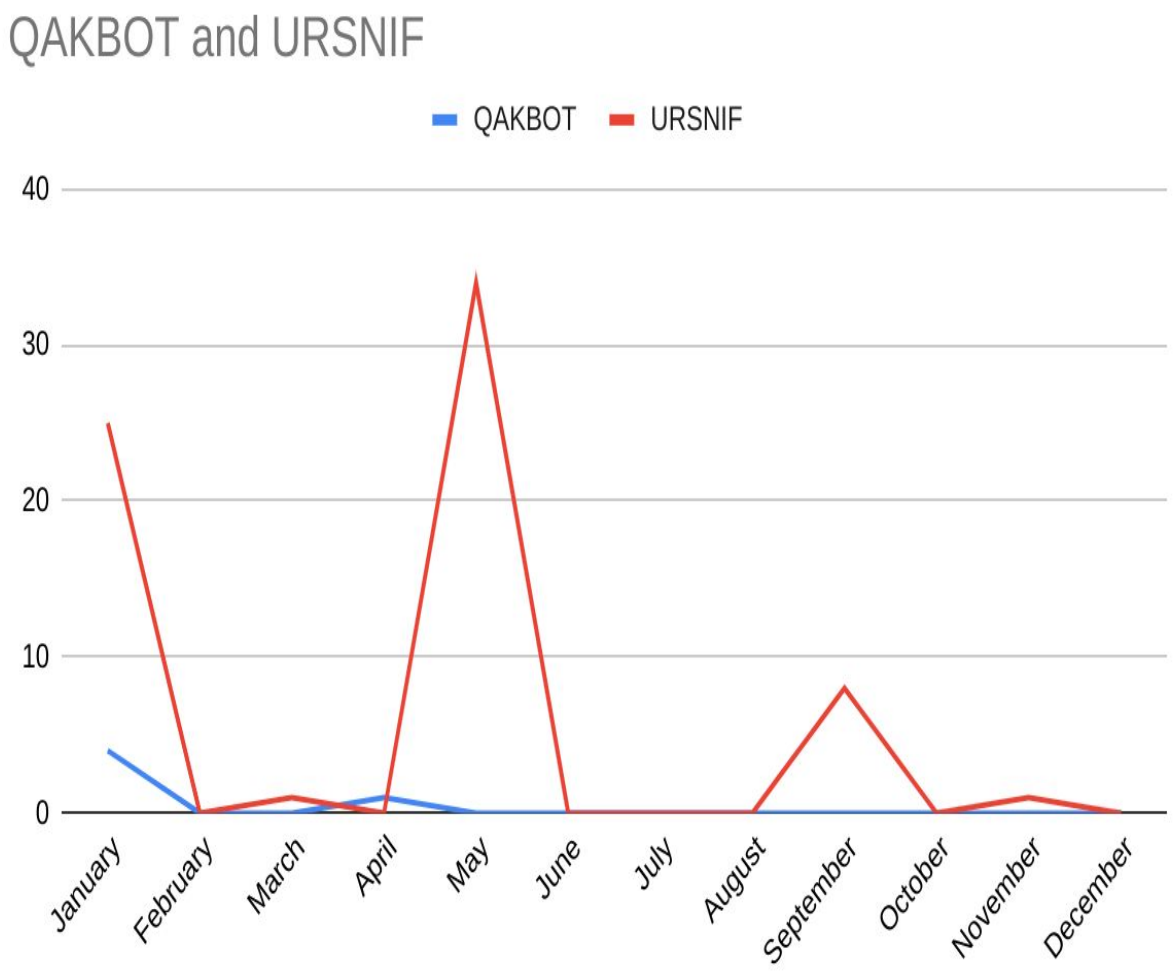
- During the past year, international law enforcement operations have sought to shut down or disrupt cyber criminal activity, including the takedowns of Genesis Market, QAKBOT malware infrastructure, RAGNARLOCKER operations, BreachForums marketplace, and the HIVELOCKER ransomware service.

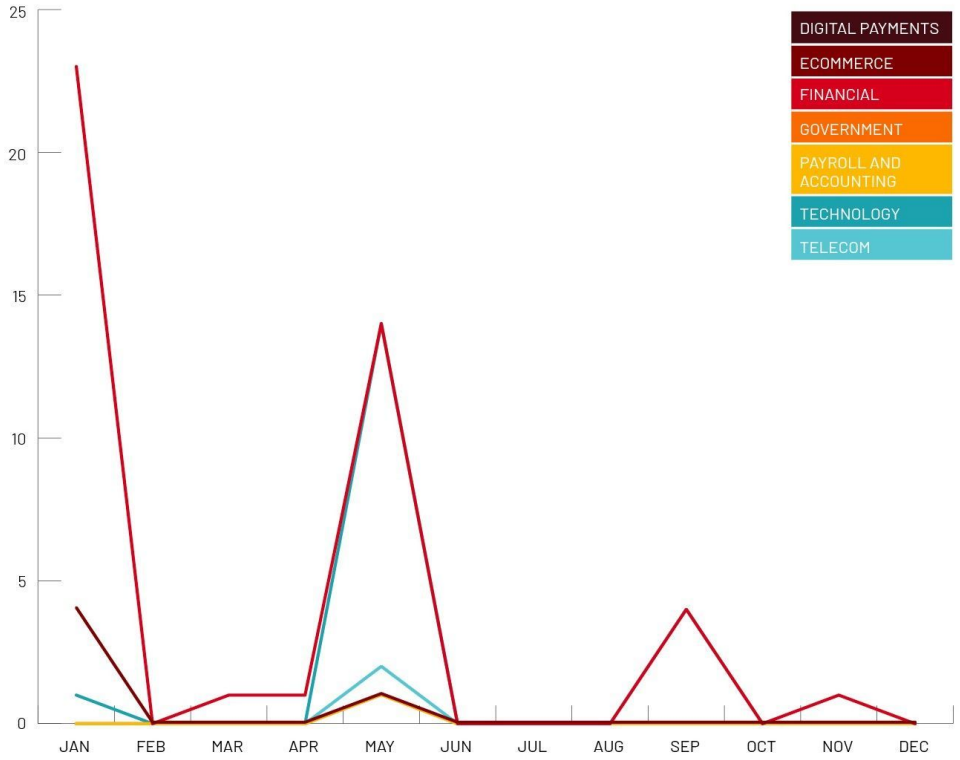
- In addition to takedowns, there were multiple arrests or arrest warrants issued as well as sanctions that impacted members of prominent operations including individuals associated with DOPPELPAYMER ransomware, broader TRICKBOT operations, and several ransomware operators in Ukraine.



Webinjects Configuration Files

Malware families that added new trigger URLs, screenshots, and keywords in 2023

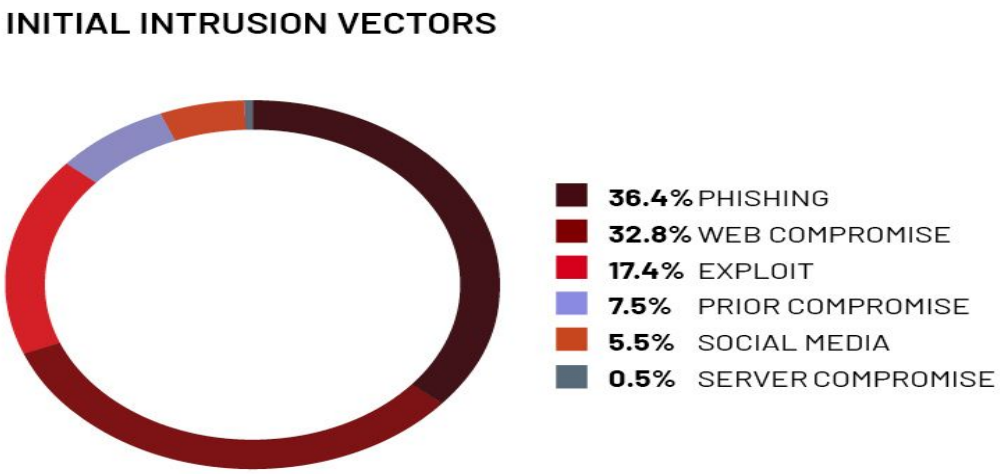


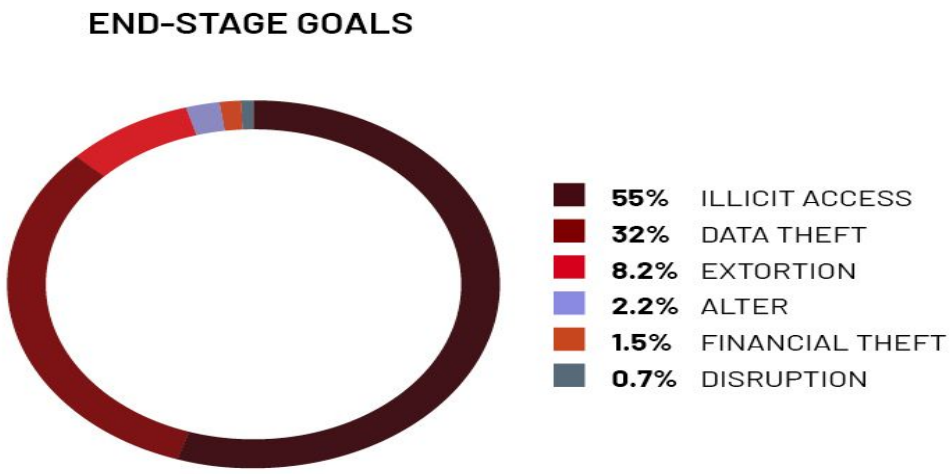


NON-DISTRIBUTION CLUSTERS

MANDIANT

Goal	Summary
Exploit	The threat actor gains access by exploitation of a vulnerability.
Phishing	The threat actor gains access to the victim's environment by distributing malicious emails or SMS messages.
Web Compromise	The threat actor gains access after the victim interacted with a compromised website.
Prior Compromise	The threat actor uses access that we believe was obtained from a distinct entity and sold for a set price or as a percentage of the monetization amount.
Social Media	The threat actor gains access to a victim via interaction through a social media platform such as Facebook or LinkedIn.
Server Compromise	The threat actor gains initial access via compromise of an internet-facing server.





MANDIANT

Ransomware Dwell Times

Change in Global Investigations Involving Ransomware

23% → **18%**

in 2021 in 2022

Change in Global Median Dwell Time – Ransomware

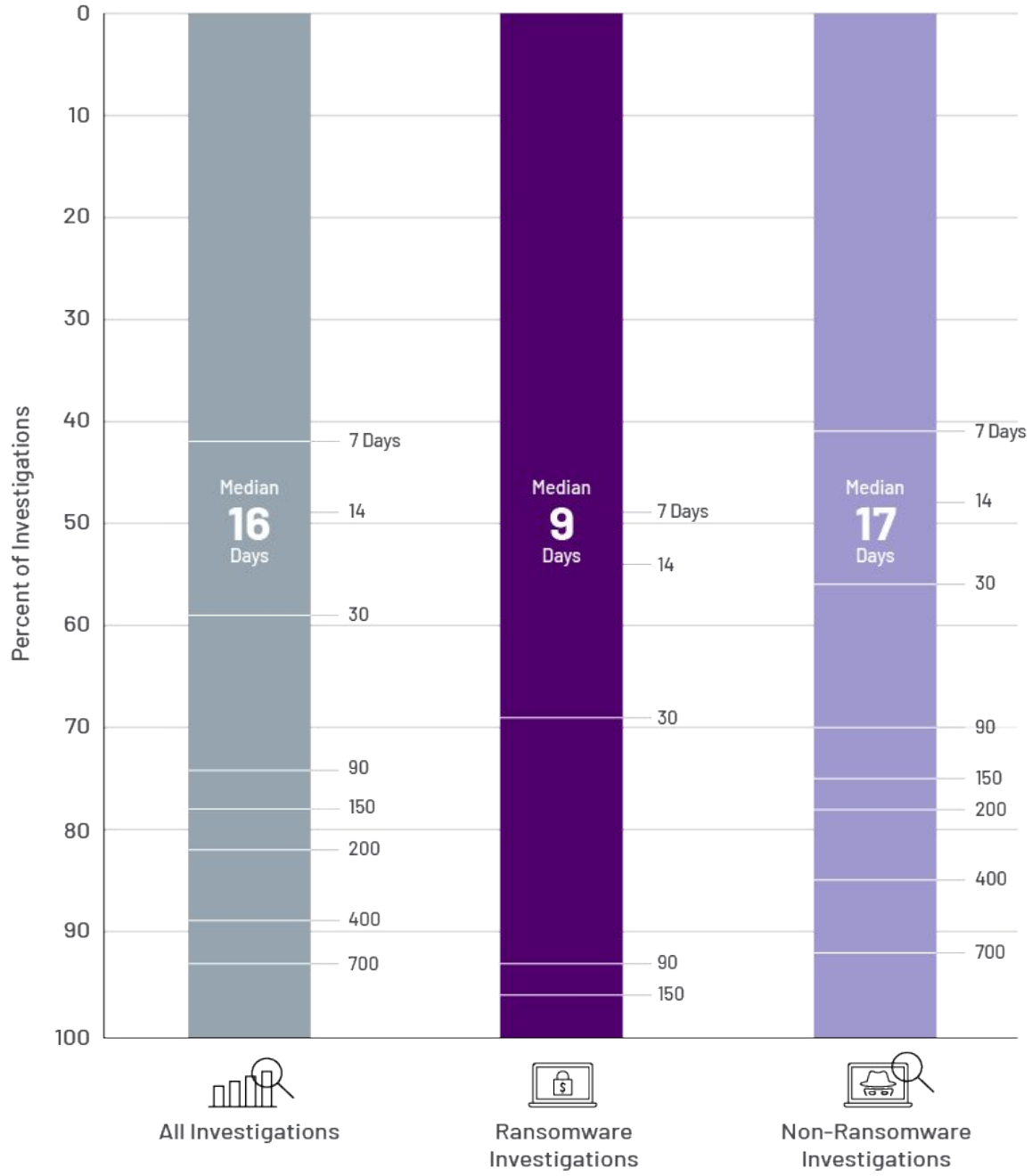
5 → **9**

Days in 2021 Days in 2022

Change in Global Median Dwell Time—Non-Ransomware

36 → **17**

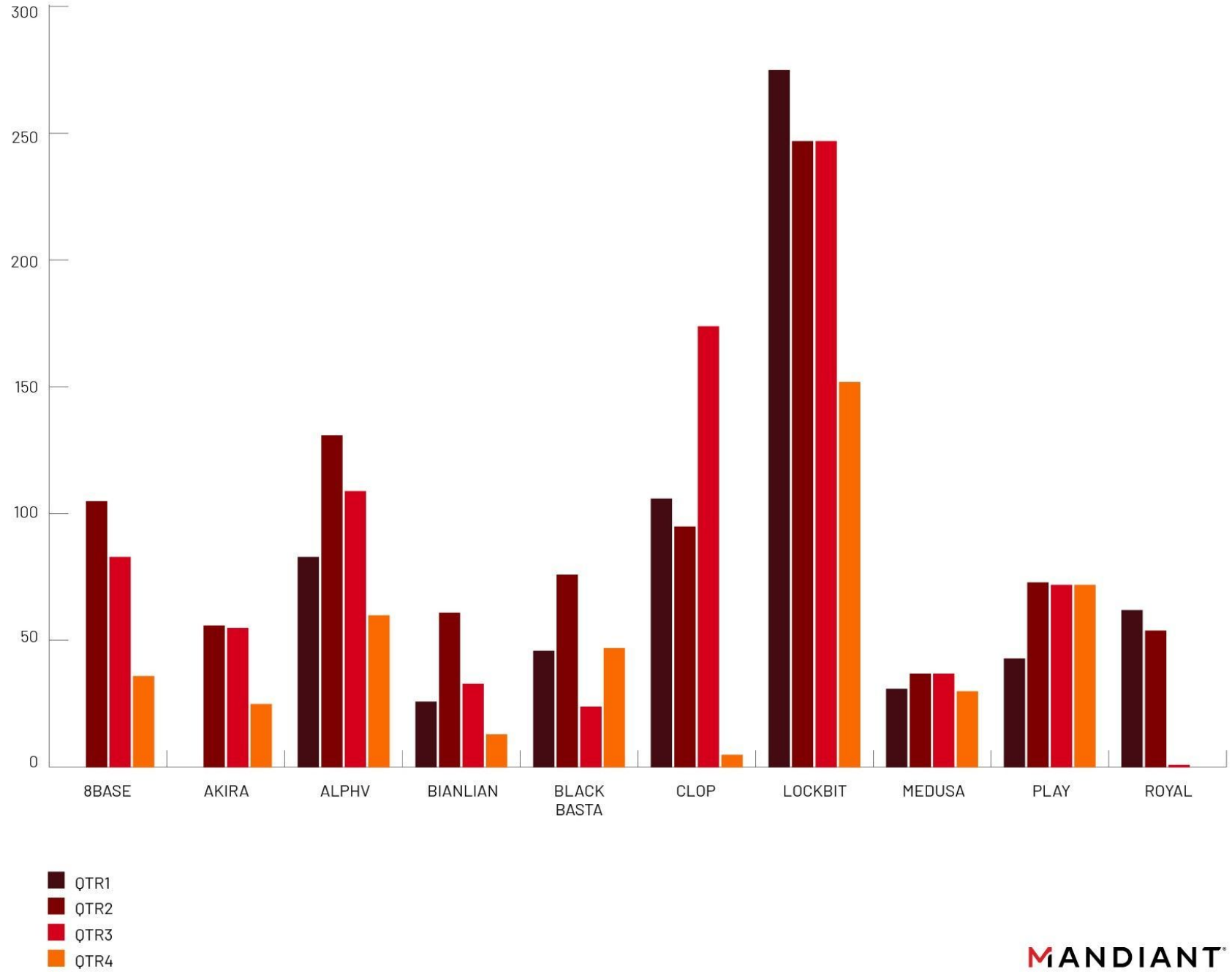
Days in 2021 Days in 2022



©2023 Mandiant

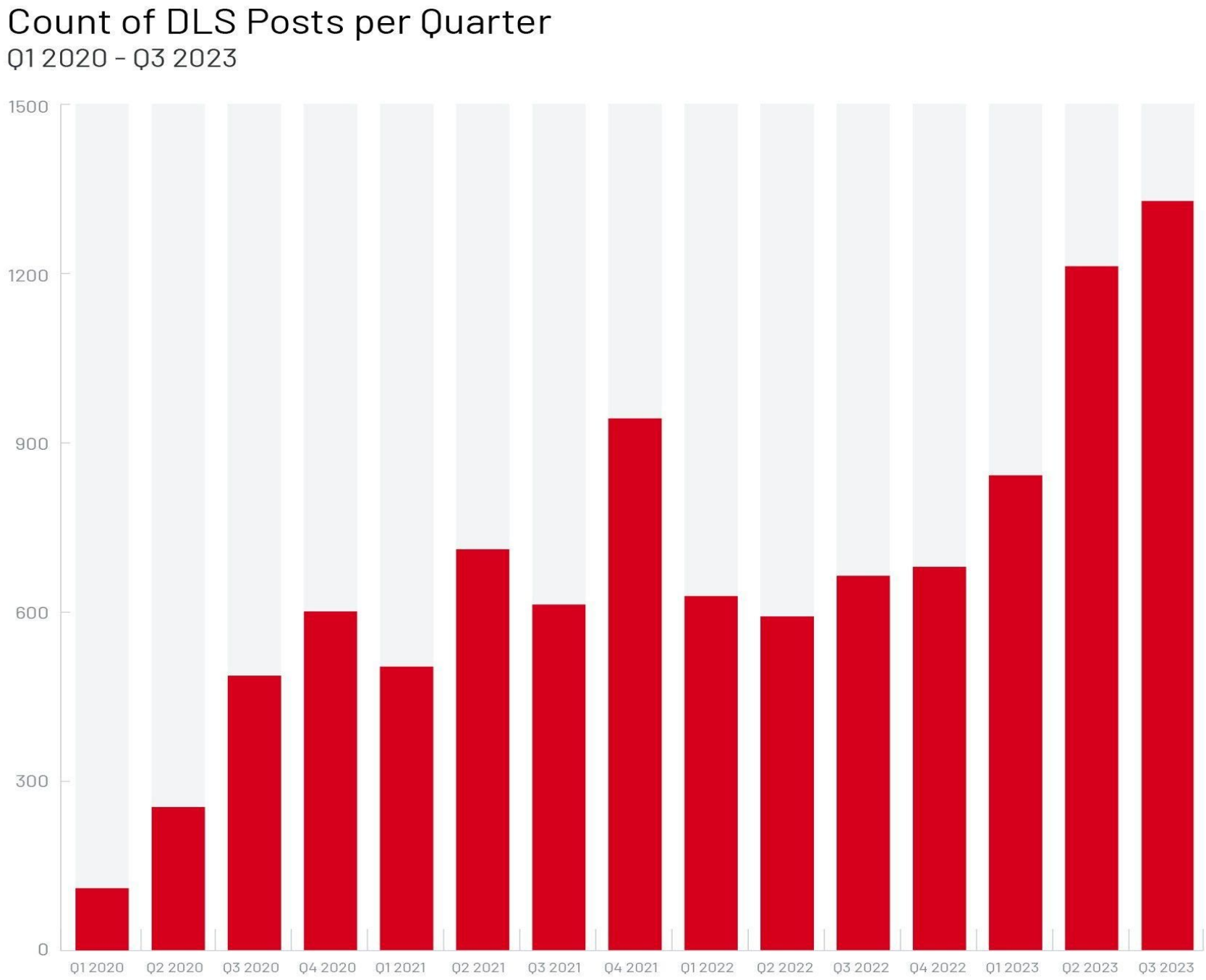
Ransomware Campaigns

- Continue to predominately rely on commercially available and legitimate tools to facilitate their operations.
- Median number of days between initial compromise and ransomware deployment was five days.
- 30% of ransomware incidents occurring within one day of initial attacker access.



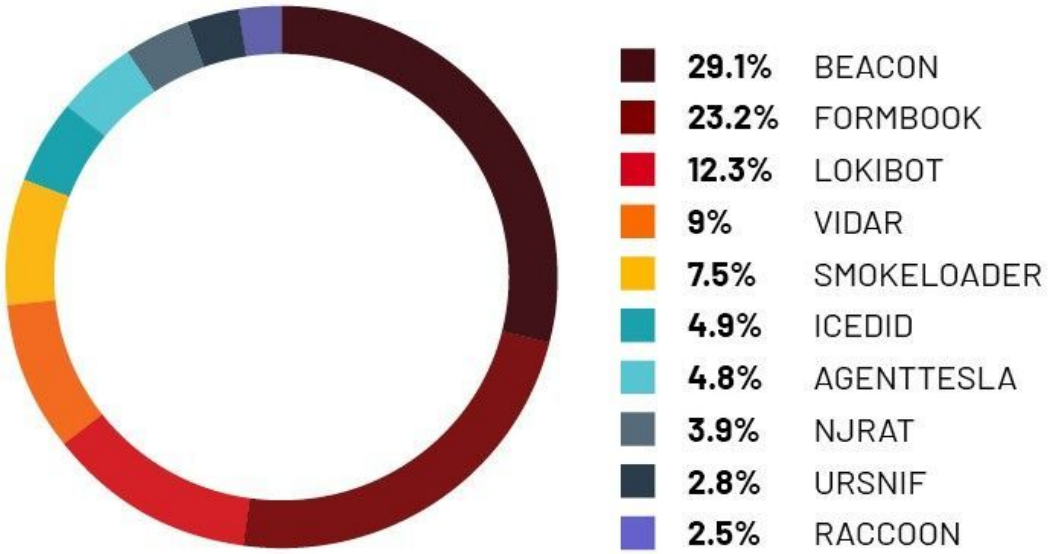
Ransomware and Data Theft Extortion 2023

- Extortion revenue estimates indicate that this threat is growing in 2023
- 2023 ransomware incidents disrupted physical mail delivery, derivatives trading, print and online news production, flights, hospitals, the food supply, and schools.

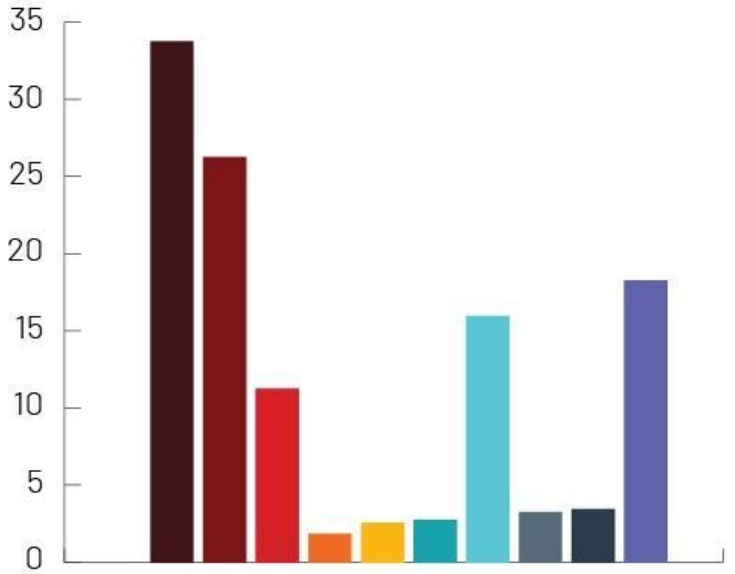


Notable Detection Data Relating to the Financial Sector in 2023

TOP MALWARE DETECTIONS

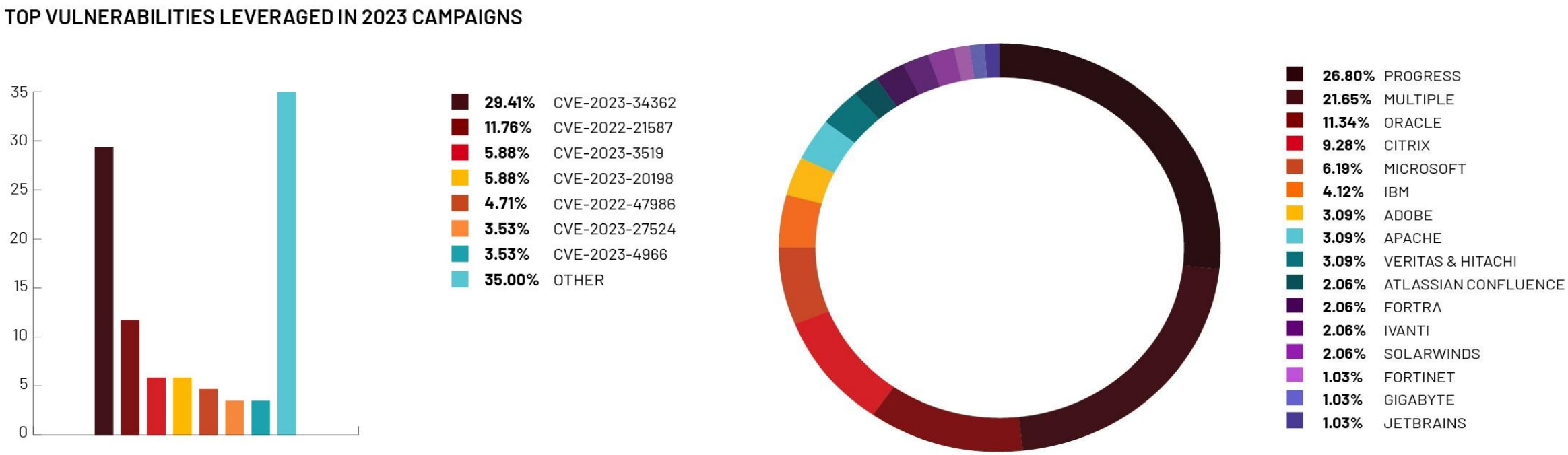


% OF INDUSTRY CLIENTS AFFECTED



MANDIANT

Top Vulnerabilities Leveraged in 2023 Campaigns



©2023 Mandiant

Global Median Dwell Time

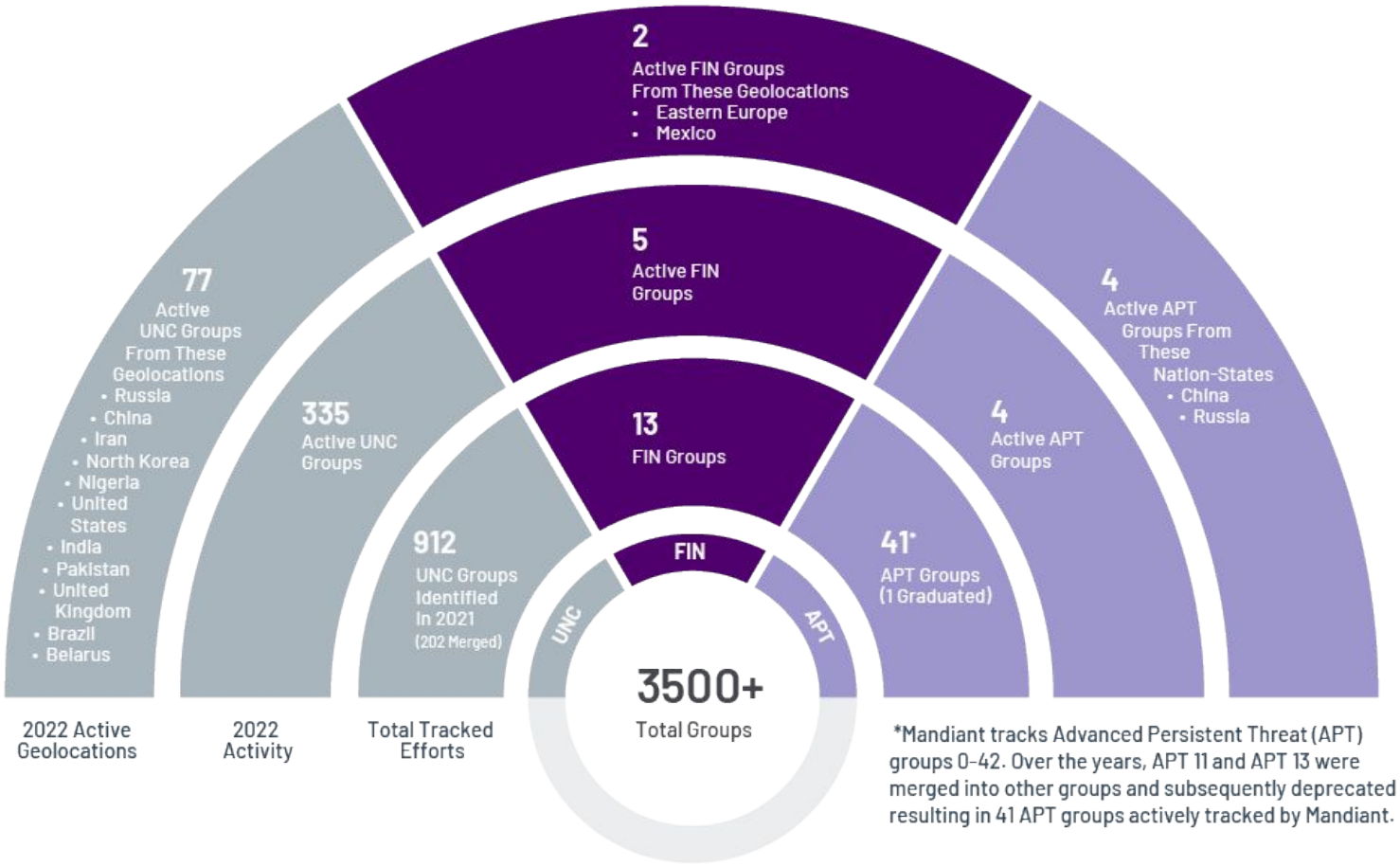
©2023 Mandiant

MANDIANT
NOW PART OF Google Cloud

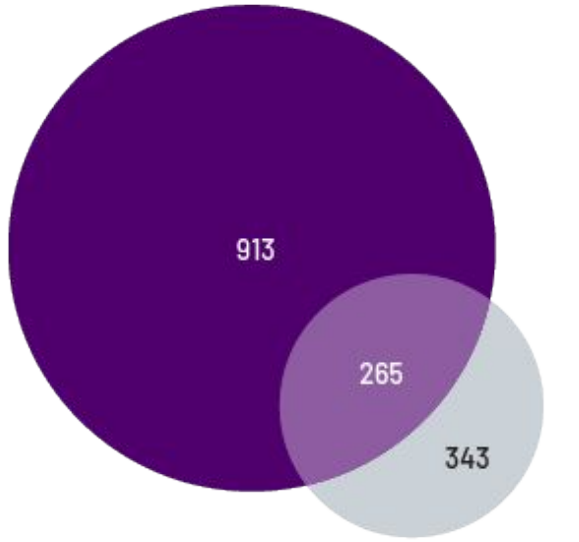
Strategic Perspective: 2023 Trends, 2024 Forecast

©2023 Mandiant

Today's Threat Groups



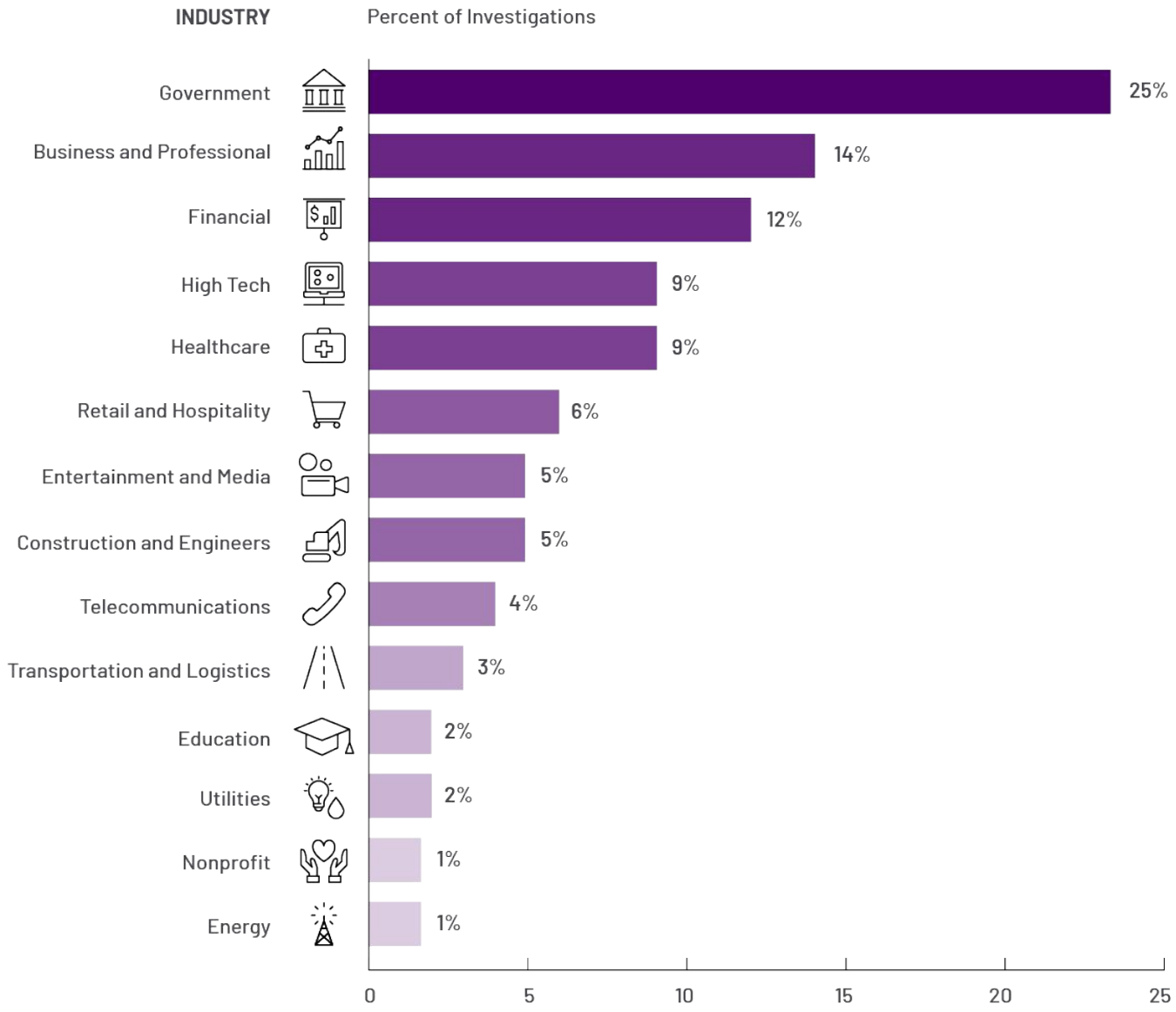
*Mandiant tracks Advanced Persistent Threat (APT) groups 0-42. Over the years, APT 11 and APT 13 were merged into other groups and subsequently deprecated resulting in 41 APT groups actively tracked by Mandiant.



©2023 Mandiant

Top Industries Targeted

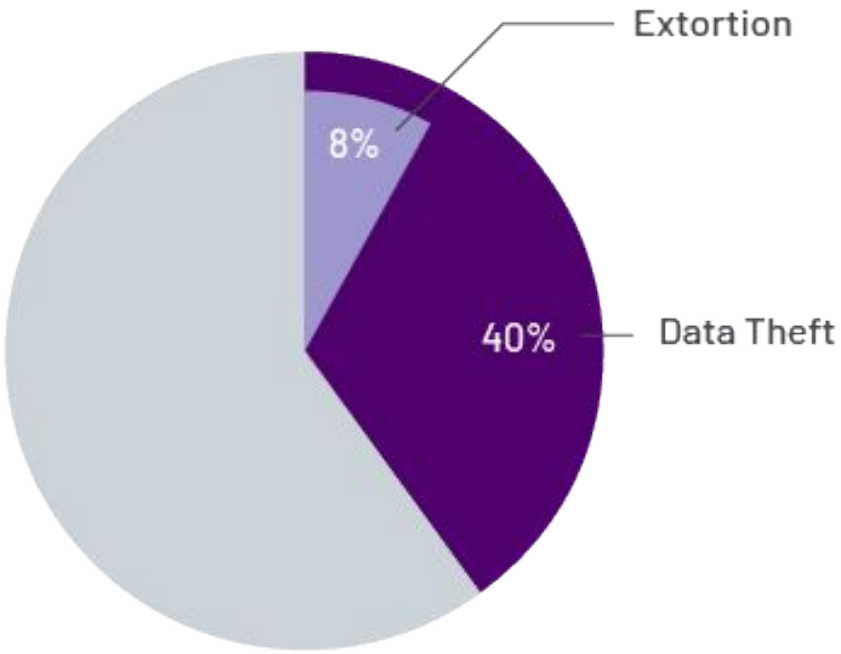
- Response efforts for government-related organizations captured a quarter of all investigations
- This primarily reflects Mandiant's work in support of Ukraine
- The next four most targeted industries are consistent with Mandiant's observations over the last two reporting periods



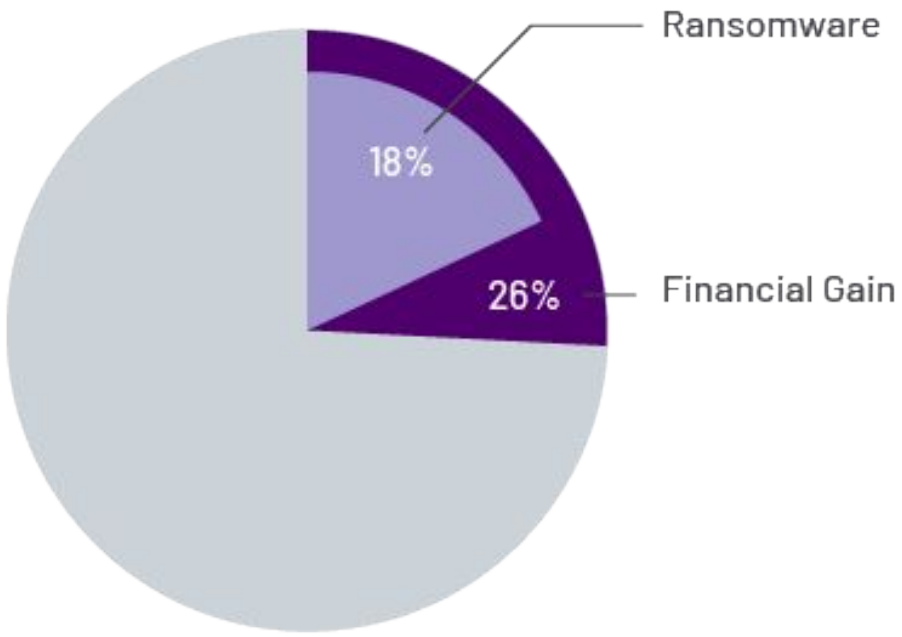
©2023 Mandiant

Adversary Mission Objectives

Data Theft



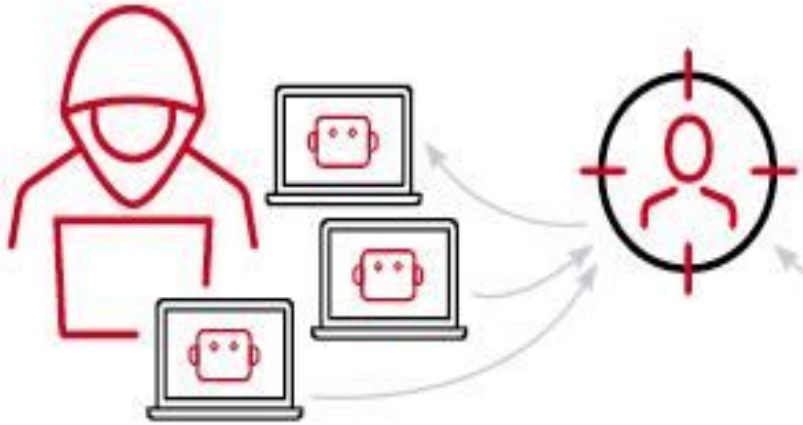
Financial Gain



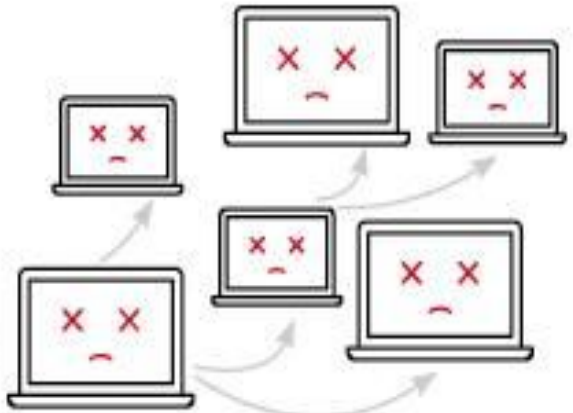
©2023 Mandiant

CHINESE CYBER ESPIONAGE DETECTION EVASION TACTICS INCLUDE

EXPLOIT SECURITY AND NETWORKING DEVICES, VIRTUALIZATION SOFTWARE



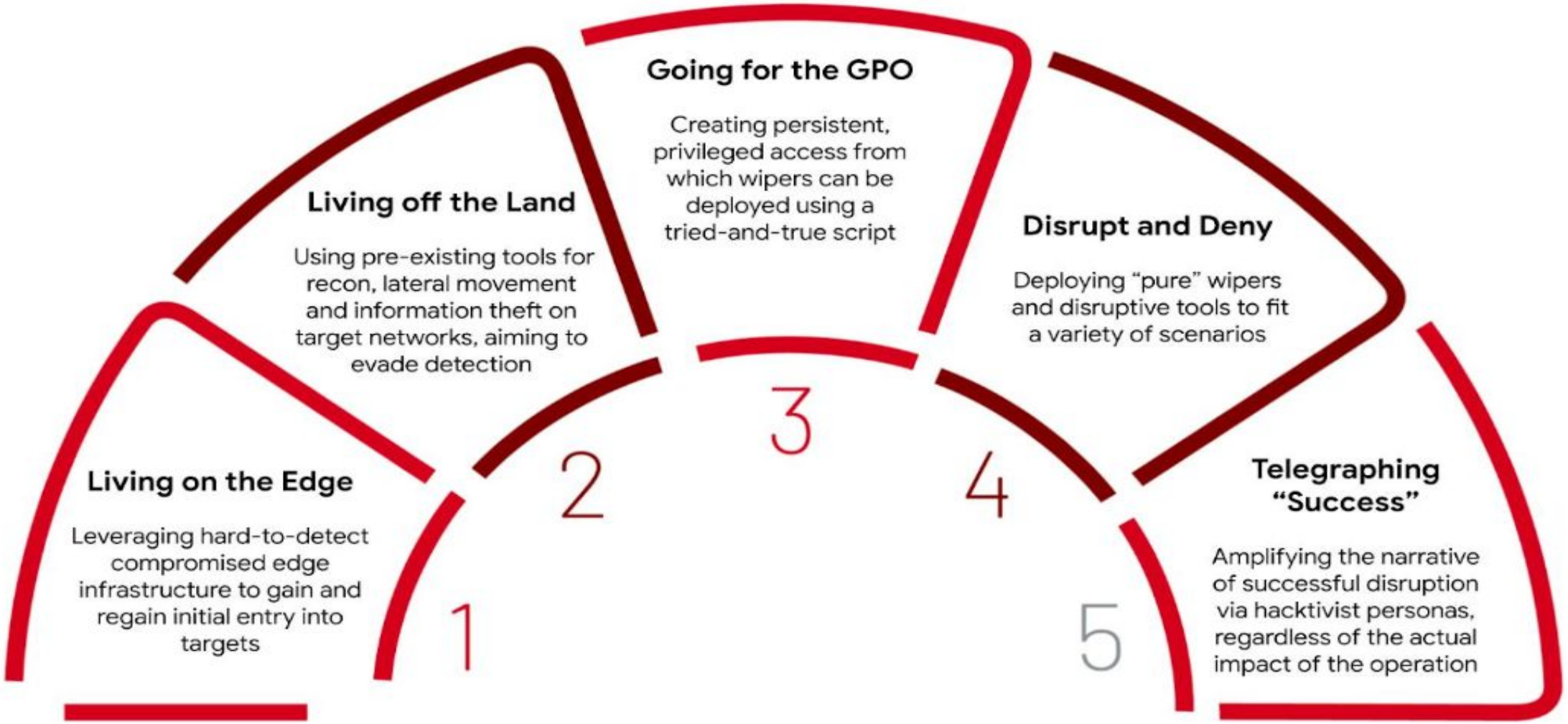
USE BOTNETS TO OBFUSCATE TRAFFIC BETWEEN ATTACKER AND VICTIM



TUNNEL MALICIOUS TRAFFIC INSIDE OF VICTIM NETWORKS THROUGH COMPROMISED SYSTEMS

MANDIANT

The GRU's Disruptive Playbook

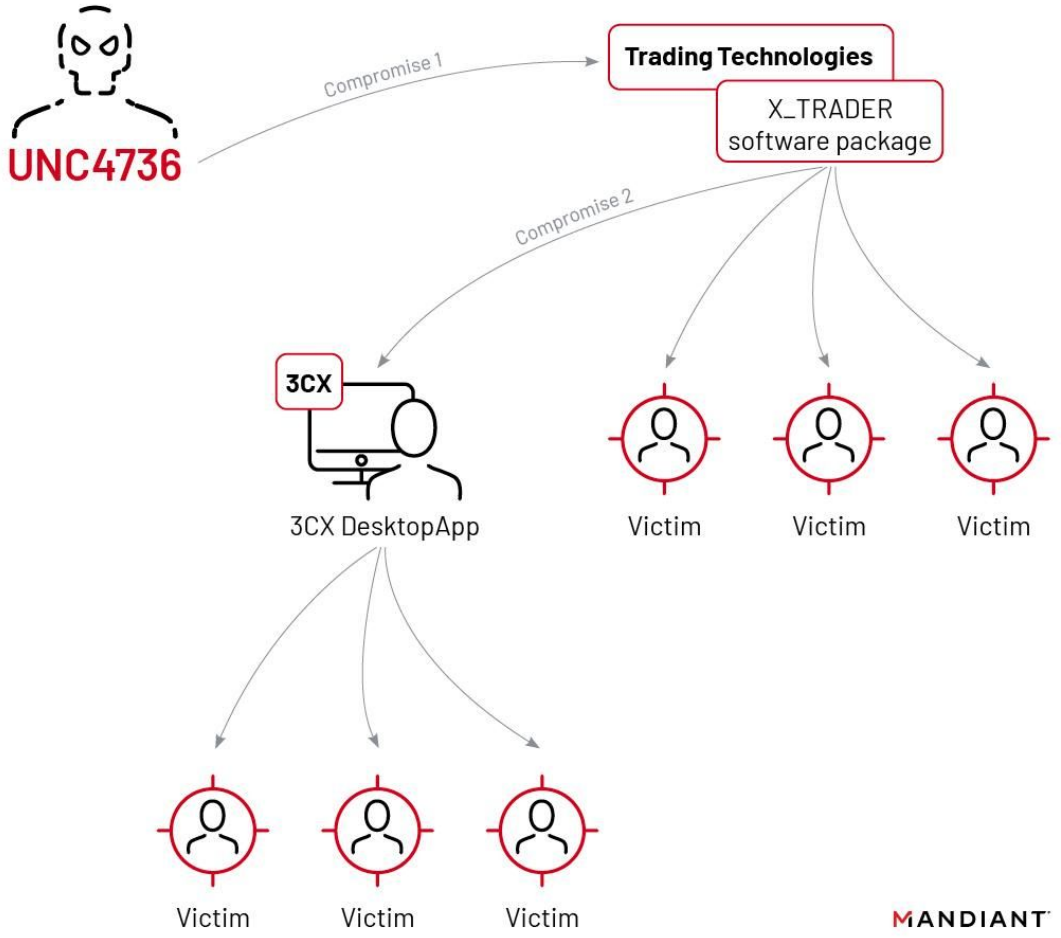


3CX software supply-chain compromise linked to Trading Technologies software supply-chain compromise

In 2023, Mandiant investigated two North Korean supply-chain compromises.

- In March 2023, Mandiant responded to a supply-chain compromise that affected 3CX Desktop App software and involved exploitation of a zero-day vulnerability, CVE-2023-29059. During this response, Mandiant identified that the initial compromise vector of 3CX's network was via malicious software downloaded from the Trading Technologies website.

- In June, UNC4899 targeted a JumpCloud developer with a spear phish, which allowed the threat actor to conduct a supply-chain compromise affecting multiple JumpCloud customers.



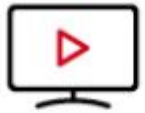
©2023 Mandiant

Will AI Make the Cyber Threat Actor's Job Easier, Better, and Faster?

IMAGES

GAN-Generated Images

Text-to-Image Models



VIDEO

AI-Generated Avatars

AI-Manipulated Video

TEXT

LLMs

AUDIO

Text-to-Voice Models

Voice Cloning

MANDIANT

©2023 Mandiant

MANDIANT
NOW PART OF Google Cloud

Thank You