



Cyber Threats



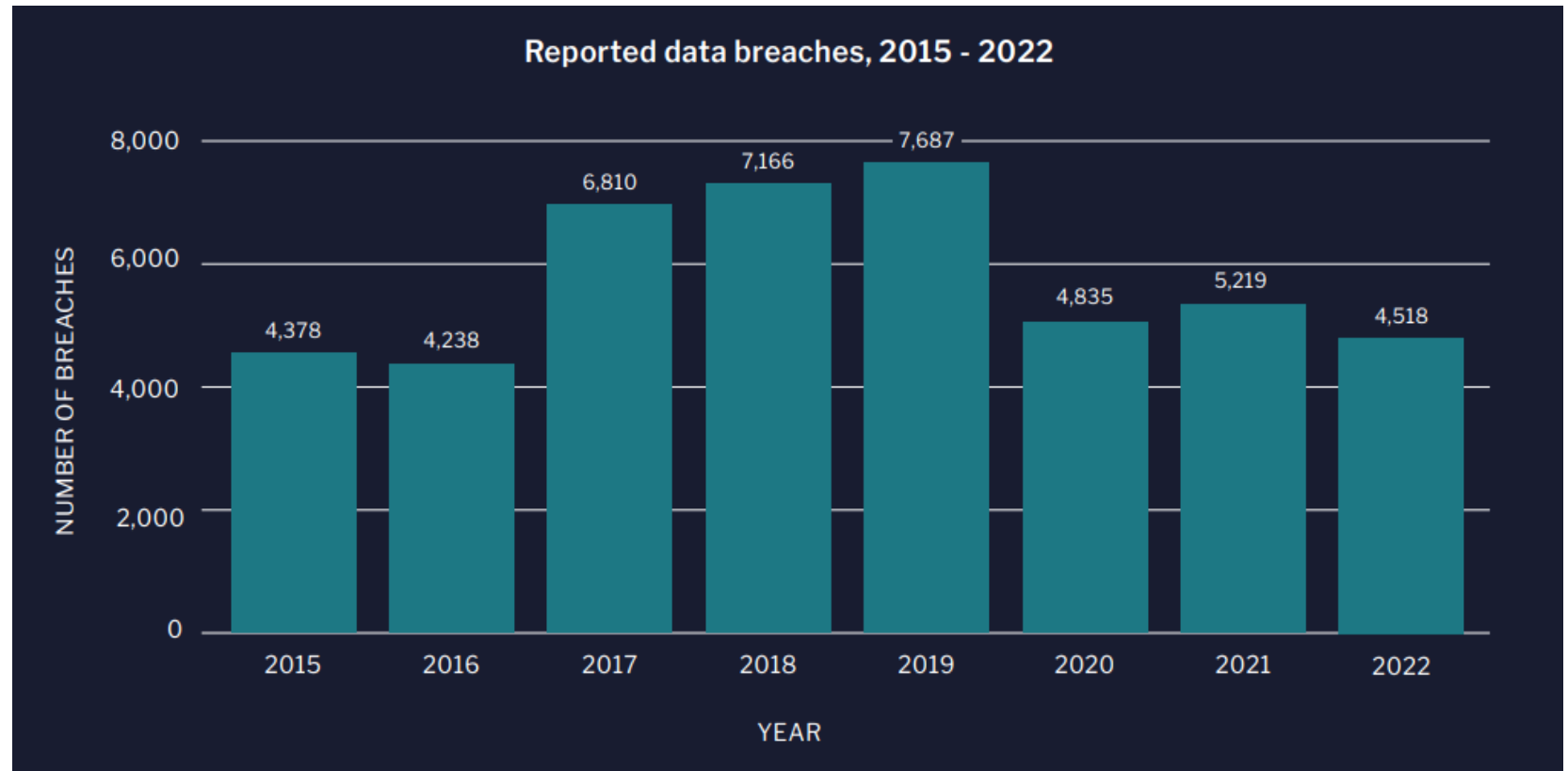
FBI CYBER

FBI Priorities

1. Counterterrorism
(International/Domestic)
2. Foreign Counterintelligence
- 3. Cyber Crime**
4. Public Corruption
5. Civil Rights
6. Transnational Criminal
Enterprise
7. White Collar Crime
8. Violent Crime

Cyber Actor's Goal

- The main goal of a cyber attack is to acquire information – names, passwords, financial records
- Information feeds the cyber criminal ecosystem

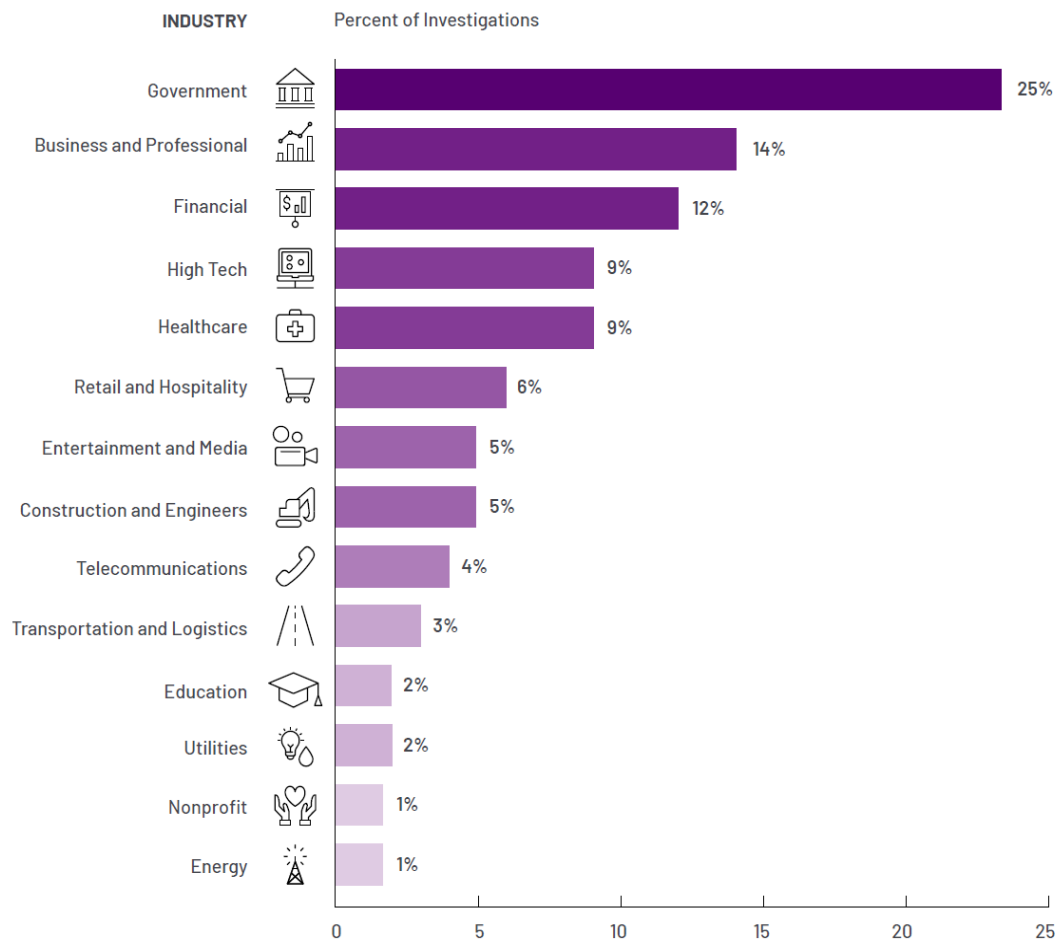


Source: "State of Cyber Threat Intelligence: 2023", Flashpoint



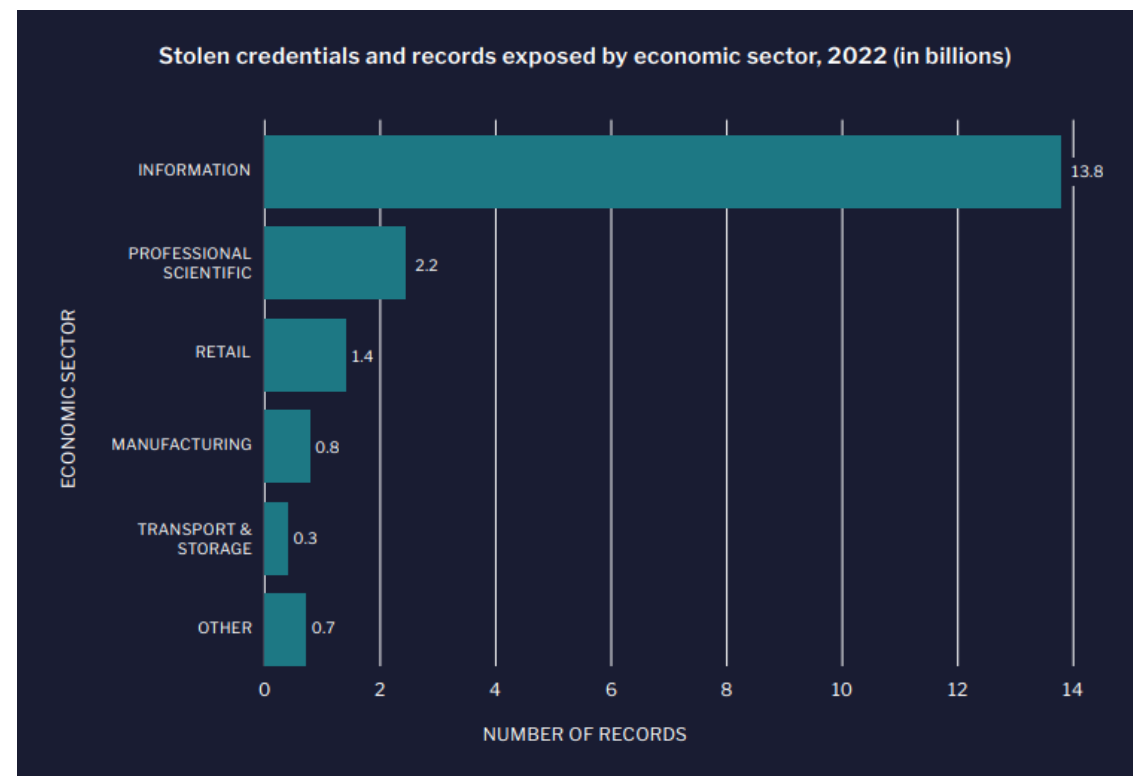
FBI CYBER

You Are the Targets?



Global Industries Targeted 2022







Source: Mandiant



Source: "State of Cyber Threat Intelligence: 2023", Flashpoint



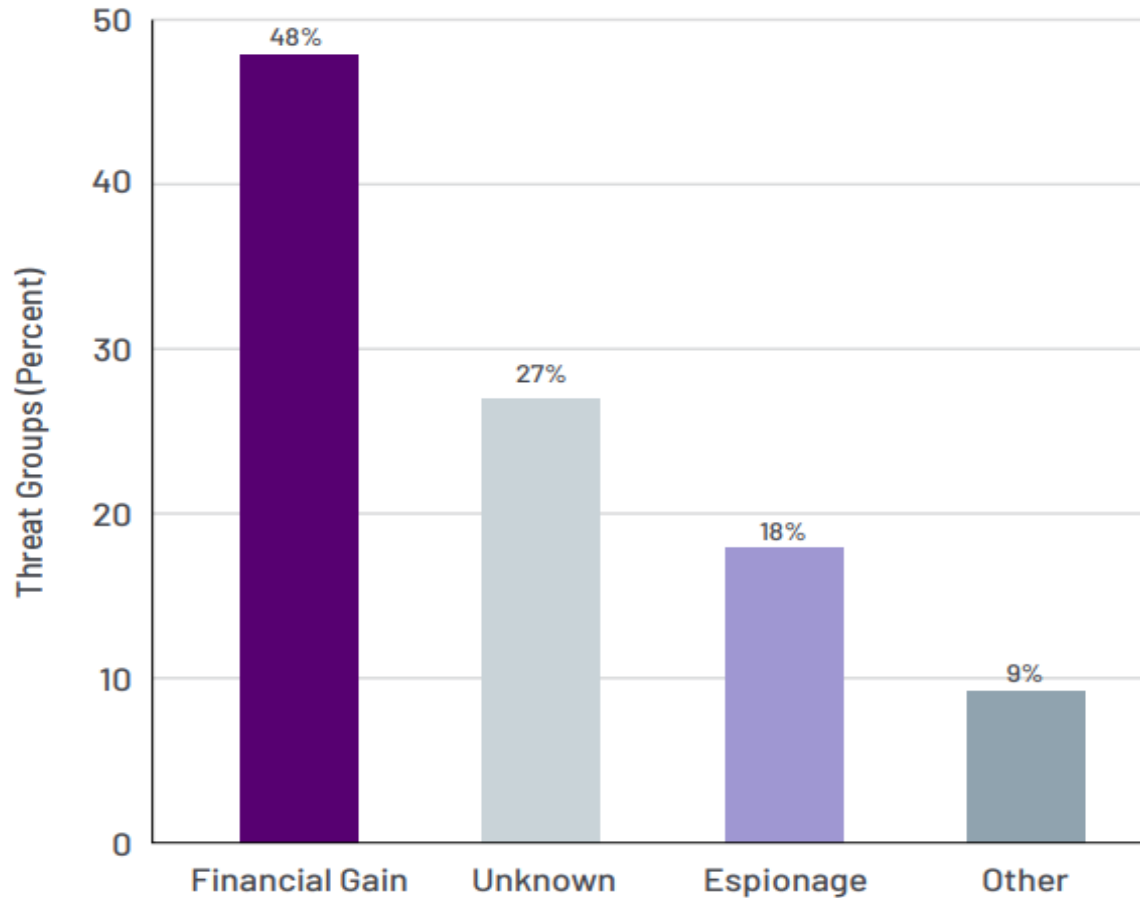
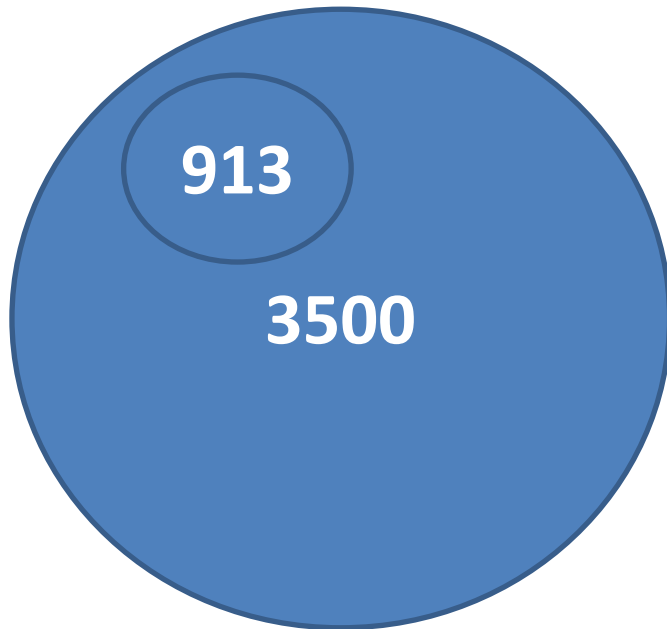
FBI CYBER

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hacktivists 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.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Cyber Actor Threat Groups

Cyber Actor Threat Groups

Mandiant is tracking more than 3500 threat groups



"M-Trends 2023 Report" Mandiant

FBI CYBER

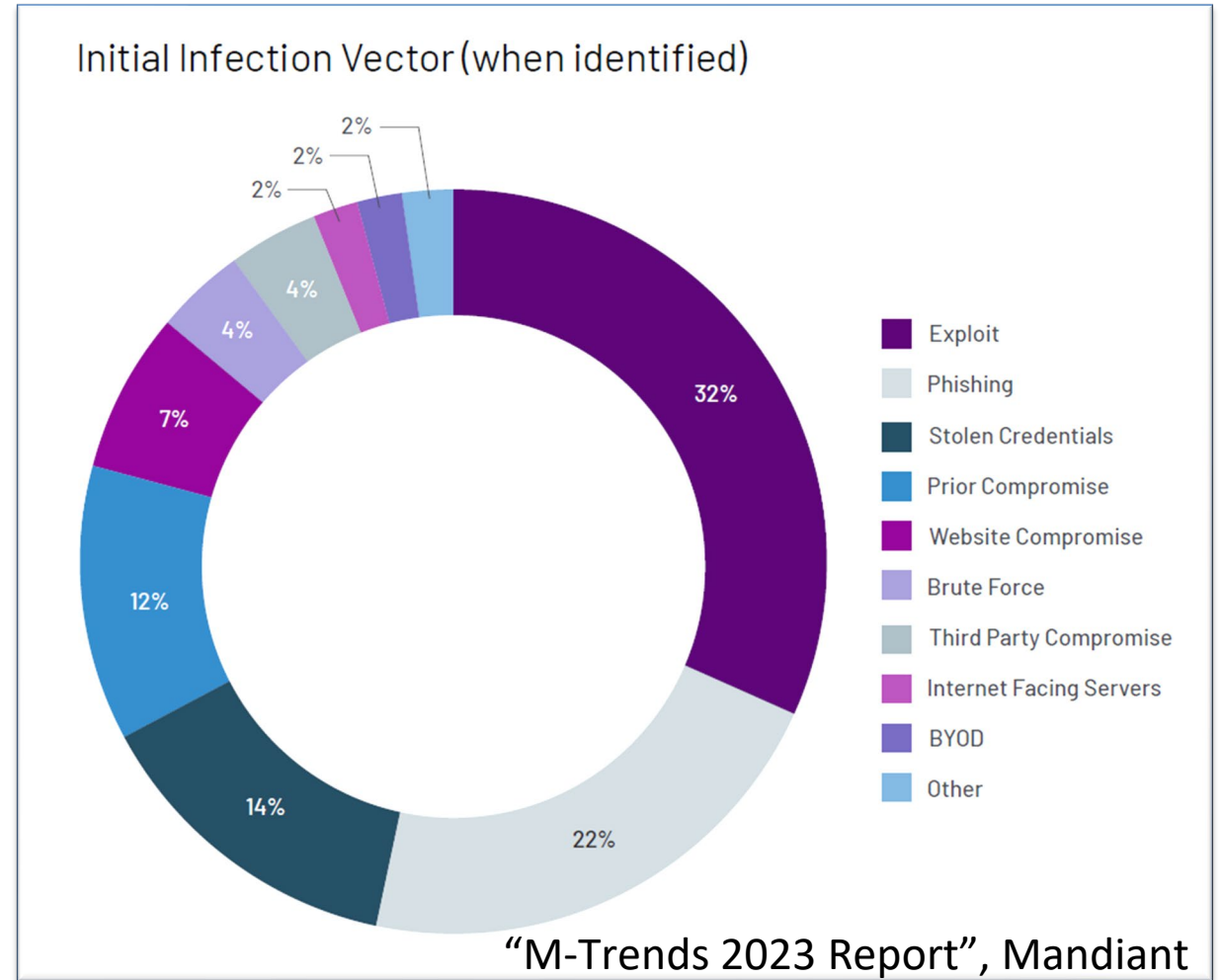


Initial Infection Vector

Top Vulnerabilities

Unpatched and
outdated systems

Lack of Education and
Training



FBI CYBER

Common Vulnerabilities and Exposures (CVE)

- Publicly disclosed security flaw
- Flashpoint collected 26,900 disclosed vulnerabilities this year — too many for one organization to patch in a timely manner
- Focus on CVEs being publicly discussed

According to Flashpoint's collections, there are over 306,000 known vulnerabilities—97,000 of which cannot be found in CVE and NVD.



F B I C Y B E R

Adversary Tactics

According to
CrowdStrike, cyber
actors continued to
move beyond
malware to gain
initial access and
persistence

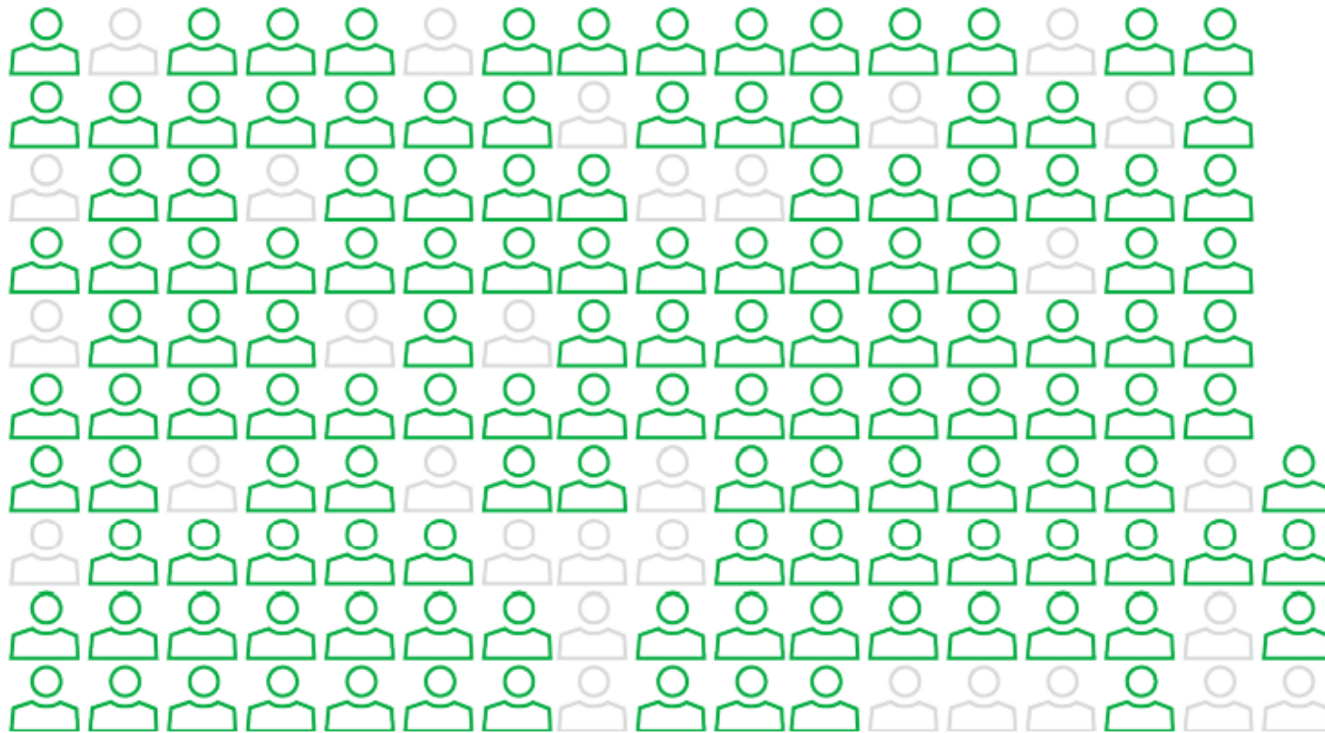
ADVERSARY TACTICS		Malware-Free
71%	2022	
62%	2021	
51%	2020	
40%	2019	
39%	2018	

Source: "2023 Global Threat Report", CrowdStrike



F B I C Y B E R

Users: The Biggest Vulnerability



The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike.

Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

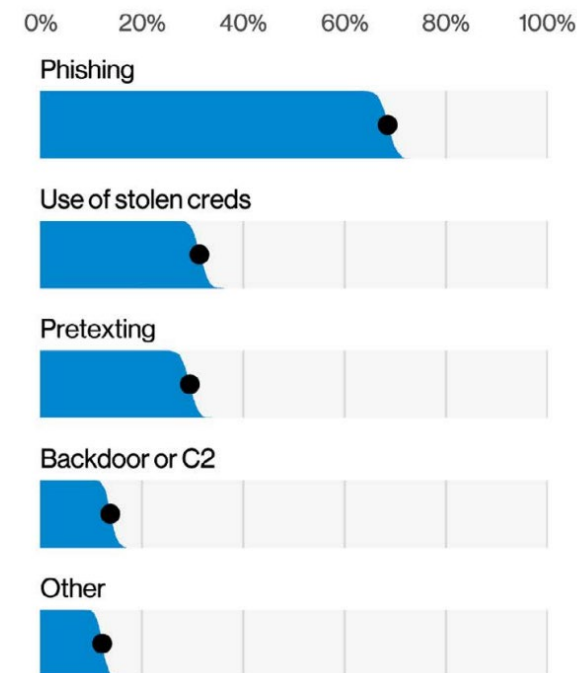


F B I C Y B E R

Source: "2022 Data Breach Investigations Report", Verizon Corporation

Social Engineering

- The psychological manipulation of people into performing specified actions or divulging personal or confidential information



Source: “2022 Data Breach Investigations Report”,
Verizon Corporation



F B I C Y B E R

Phishing Effectiveness

- Campaign of just 10 emails yields greater than 90% success rate
- Average time from start of campaign to first compromise: 1 minute 22 seconds

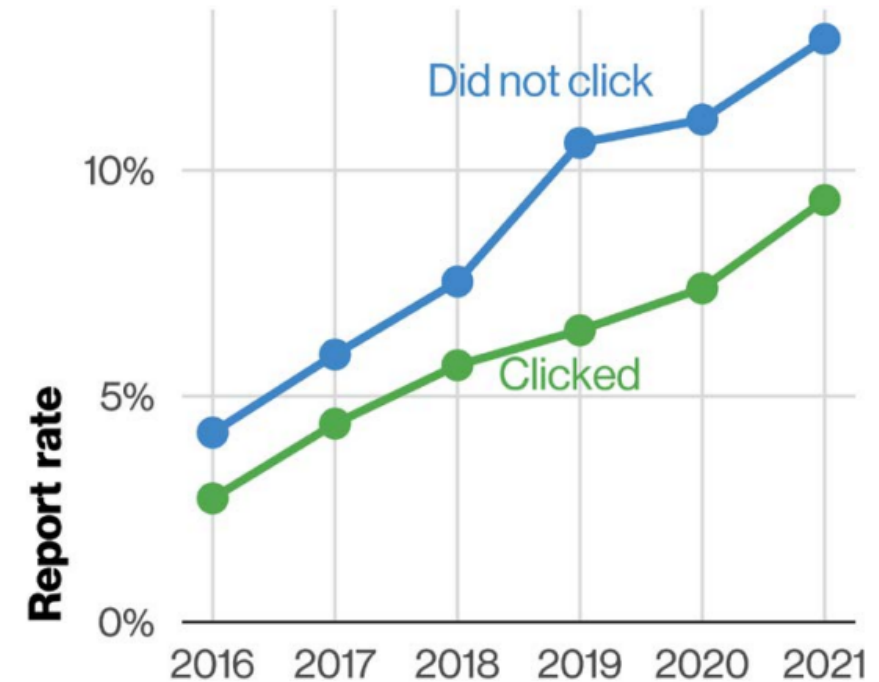


Figure 48. Phishing email report rate by click status (n=295,825,679)

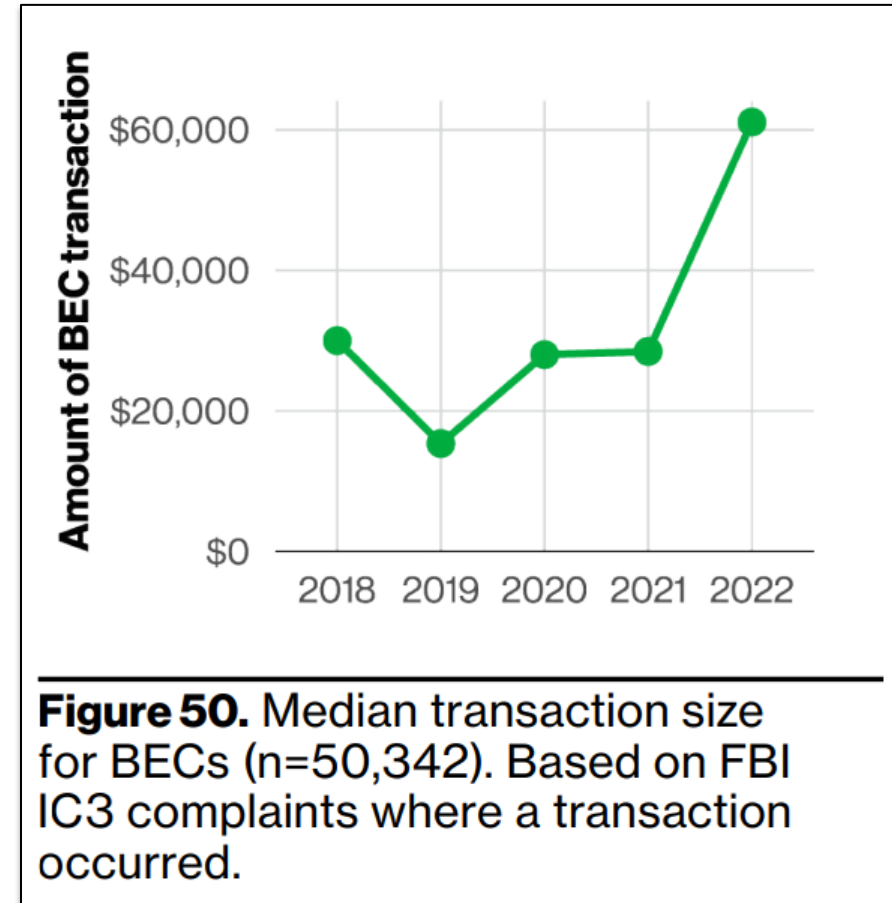


F B I C Y B E R

Source: “2022 Data Breach Investigations Report”, Verizon Corporation

Business Email Compromises

- Sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.
- Actors compromise or impersonate legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.



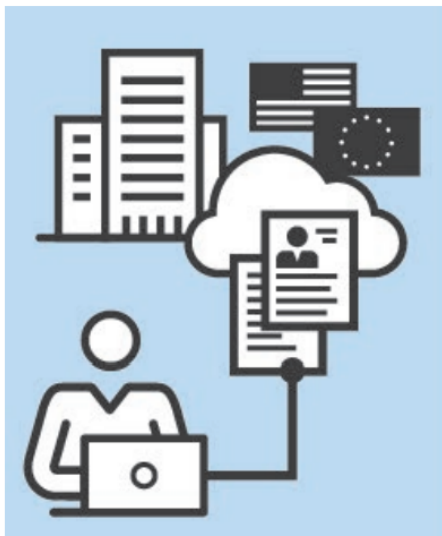
“2022 Data Breach Investigations Report” Verizon Corporation



F B I C Y B E R

Business Email Compromises

HOW IT OCCURS



Step 1

Identify Target

BEC actors target businesses and organizations, exploiting online information to develop a profile on the victim company and its executives.



Step 2

Grooming

Typically, someone in the finance department is targeted by spearphishing emails and/or phone calls. Criminal actors manipulate and exploit human nature through persuasion and pressure.



Step 3

Exchange of Information

With the victim convinced they are conducting a legitimate business transaction, they are provided with fraudulent wiring instructions.



Step 4

Wire Transfer

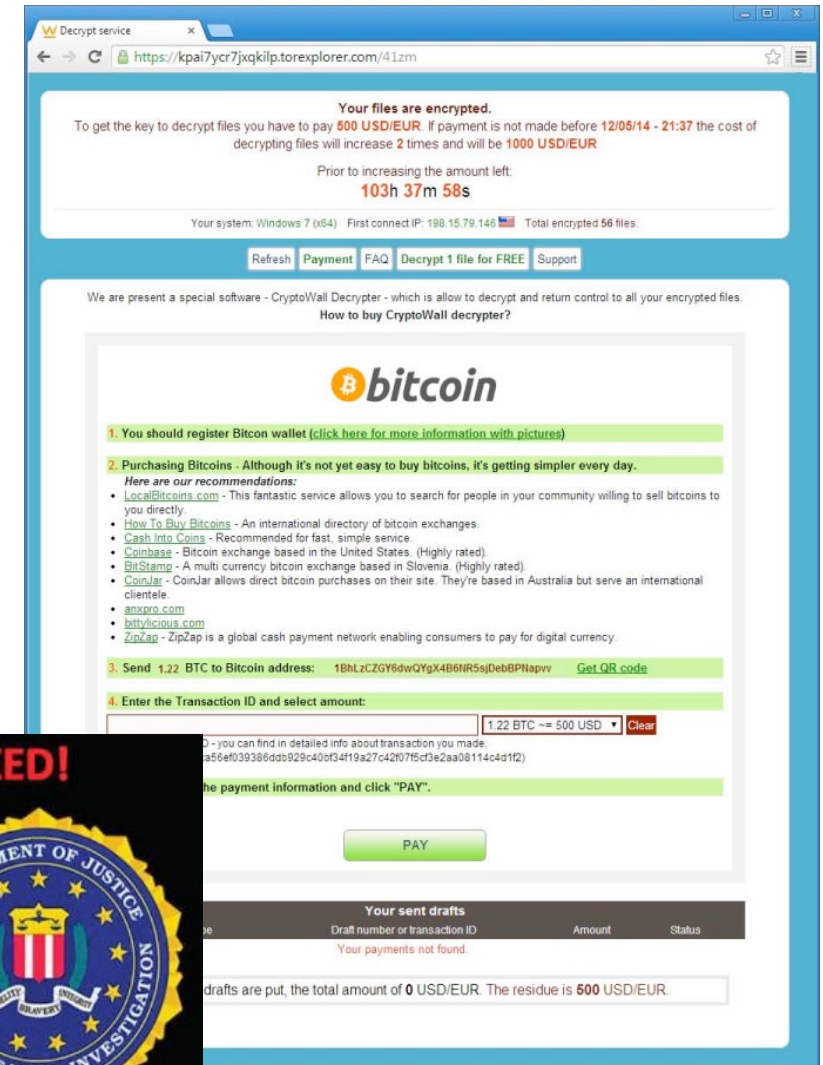
Upon transfer, the funds are steered to a bank account controlled by the BEC actors.



FBI CYBER

Ransomware

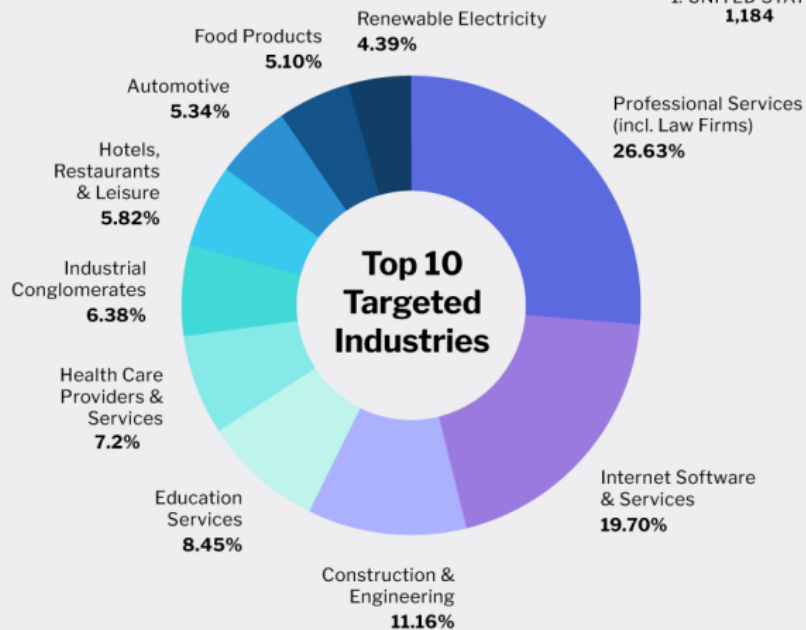
- Malware that encrypts data on a computer making it unusable.
- Actors hold data hostage until a ransom is paid.
- Actors apply additional pressure by threatening to delete or publicly release the victim's data.
- **The FBI does not encourage paying the ransom** because:
 - It encourages actors to attack again
 - It does not guarantee file recovery
 - Proceeds often fund illicit activities



FBI CYBER

Ransomware

State of Ransomware 2022



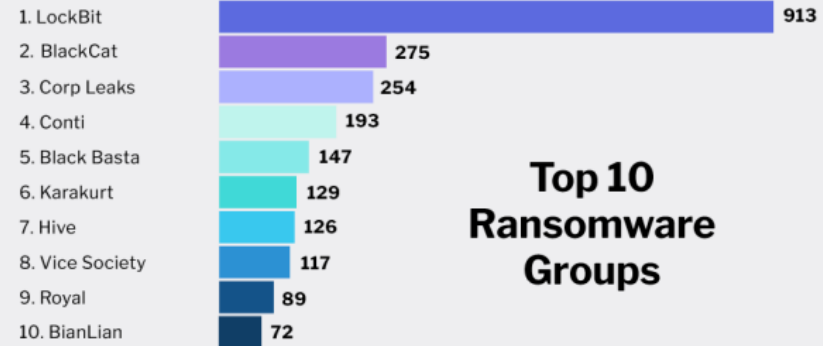
Top 12 Targeted Countries

LISTED IN ORDER WITH
NUMBER OF ATTACKS



RANSOMER NAME

VICTIM POSTS



Top 10 Ransomware Groups

© Copyright 2023 Flashpoint. Based on data from the Flashpoint Intelligence Platform | <https://flashpoint.io/platform/ransomware/>

FLASHPOINT



FBI CYBER

Minimizing Risks (Corporate)

- Anti-virus/malware/spyware, firewall
- Deploy patches quickly – 5 day window before exploited
- Use current software; minimum one generation behind (vendors stop distributing patches to older versions)
- User training
- Multi-factor authentication
- Encryption
- Know your assets



F B I C Y B E R

Minimizing Risks (Individual)

- Keep anti-virus/malware/spyware up to date
- Bank on a separate computer
- Use complex passwords
- Use caution on “open” networks
- Always review monthly statements carefully
- Check your credit reports annually
- Enable encryption on wireless routers
- Be suspicious of unsolicited e-mail with links
- Check web URLs and links very carefully



BEC: Minimizing Risk and Impact

- **Implement awareness and training programs:** All employees should go through regular training detailing the threat of BEC and how it is delivered, as well as best practices to prevent BEC by learning how to identify phishing emails and how to respond to suspected compromises.
- **Confirm payments via telephone prior to disbursing funds:** Require that the finance department contact vendors via the original phone numbers on file prior to transferring funds. Any phone numbers listed in a fund transfer request could be associated with the malicious actor.
- **Flag suspicious emails:** Create an email rule to flag email communications where the “reply” email address is different from the “from” email address shown.
- **Clearly distinguish between internal and external email senders:** Establish a warning notification that clearly distinguishes emails that originated from an external sender.



Ransomware: Minimizing Risk and Impact

- Backup your data, system images, and configurations
- Test your backups and keep them offline
- Utilize multifactor authentication
- Update and patch your systems
- Make sure your security solutions are fully up to date
- Review and exercise your incident response plan



F B I C Y B E R

When to Report?

- Electronic evidence dissipates over time, so **speed is essential** in a cyber intrusion investigation.
- Enlisting the FBI's help **as soon as an incident is discovered** enables quick investigative action and allows the preservation of evidence which increases the odds of a successful prosecution or other action to disrupt the perpetrators.
- **Develop a relationship with their local FBI field office prior to an incident.** Proactively building a relationship with the FBI provides companies with a dedicated FBI point-of-contact in the event of an incident and provides access to FBI cyber mitigation resources.



How Do I Report a Cyber Incident to the FBI?

FBI Field Offices

(local or international)
www.fbi.gov/contact-us

**FBI Internet Crime
Complaint Center (IC3)**
www.ic3.gov

Online Tips and Leads Form
tips.fbi.gov

FBI Tip Line

1-800-CALL-FBI
(1-800-225-5324)

CyWatch 24/7 Cyber Center
1-855-292-3937 or
cywatch@fbi.gov



FBI CYBER

What Should be Reported?

- Logs for the affected machines
- A timeline of events
- The identity of whoever reported the incident
- The identity of the victim of the incident
- The nature of the incident
- When the incident was initially detected
- How the incident was initially detected
- The actions that have already been taken
- Who has been notified of the incident



F B I C Y B E R

Why Should I Report?

In response to a reported cyber incident, the FBI may be able to:

- Identify and stop the activity. Potentially recover any transferred funds.
- Seize or disrupt the actor's technical infrastructure.
- Share valuable insights from other investigations that may help mitigate damage and prevent future incidents.
- Support your organization's data breach response.



FBI CYBER

How Will the FBI Protect Your Data and Interests?

- The FBI's efforts are directed towards the attacker and their actions on the system/network and not on the victim's defenses.
- The FBI works closely with the victim's legal counsel to address concerns.
- The FBI is mindful of the reputational harm that a cyber incident can cause.
- Often, the FBI requires only technical details to advance investigations not privileged communications or unrelated documents.
- FBI investigations are carefully coordinated with victim companies to minimize disruption to normal business operations.



F B I C Y B E R

Partnership is Critical

- Establish a relationship with your local FBI office prior to an incident
- Discuss your priorities and needs with the FBI
- Seek to understand the FBI's process



FBI CYBER



Questions?