M-TRENDS 2023

By The Numbers

INFOGRAPHIC

Today's cyber security developments and impactful adversary attacks are revealed through Mandiant incident response investigations and threat intelligence findings from January 1, 2022 to December 31, 2022.

Who Attackers Are

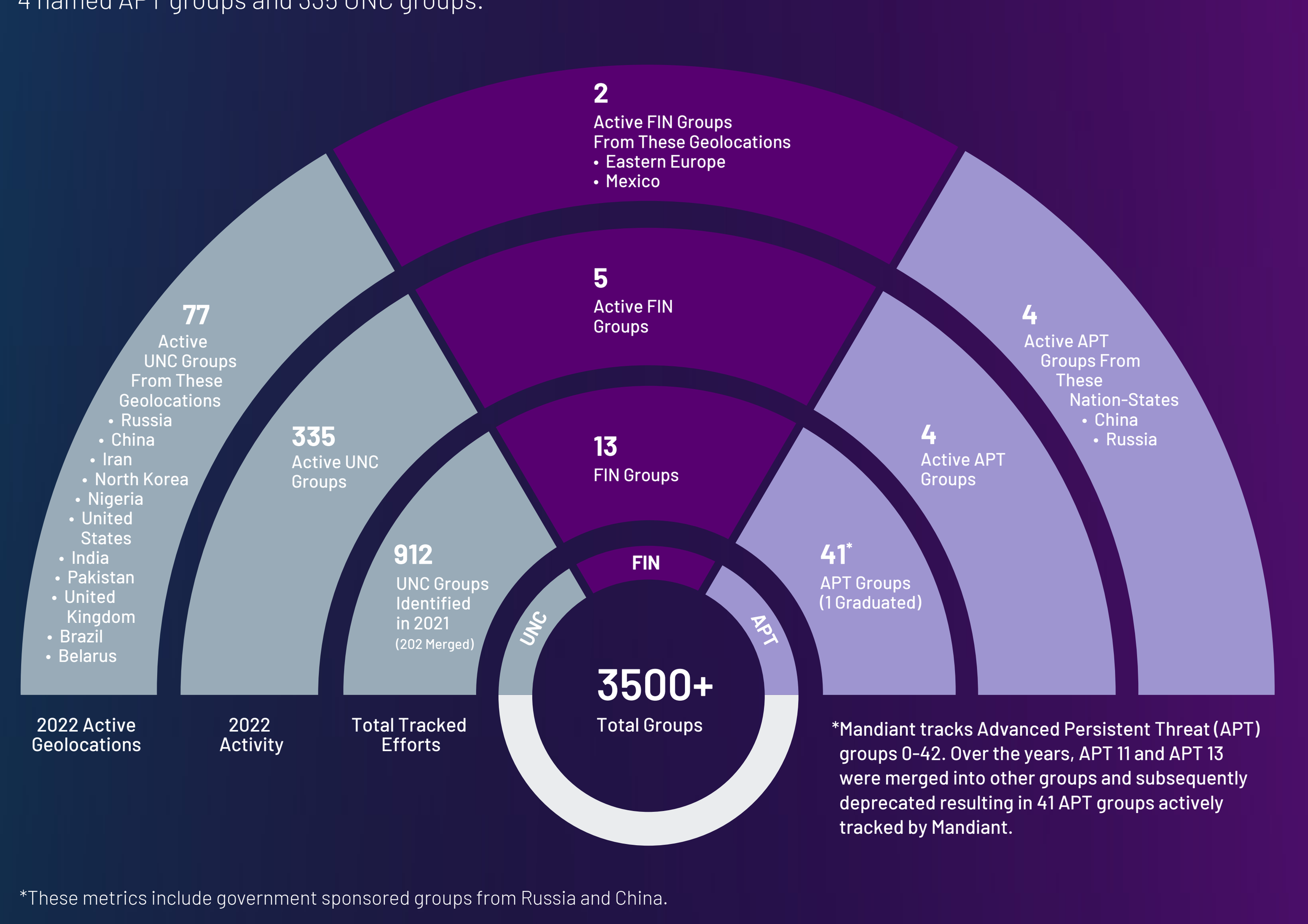
Mandiant experts currently track over 3,500 threat groups, which include 900+ newly tracked groups for this M-Trends reporting period.

Threat Group Spotlight

APT42 is an Iran-nexus threat group that conducts espionage using sophisticated phishing and social engineering attacks. APT42 activity poses a threat to foreign policy officials, commentators, and journalists working on Iran-related projects. Graduated from UNC788.

UNC: uncategorized threat actor
FIN: financially motivated threat actor
APT: advanced persitent threat group

In 2022, Mandiant identified a total of 343 unique threat groups across all intrusions including 5 named FIN groups, 4 named APT groups and 335 UNC 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.

*These metrics include government sponsored groups from Russia and China.

What Do They Target

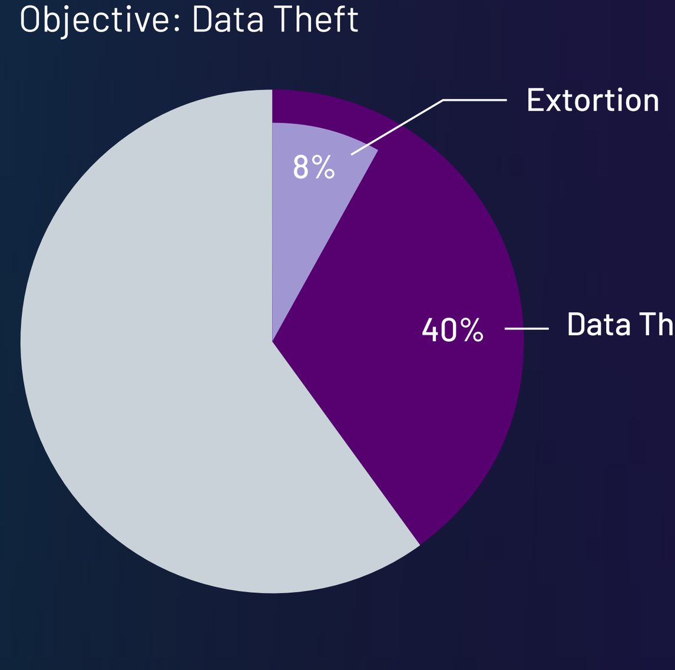
Top Industries Under Attack

1. Government	25%
2. Business and Professional	14%
3. Financial	12%
4. High Tech	9%
5. Healthcare	9%

Attackers continue to target industries where they have been most successful in the past and industries that most interest or benefit them.

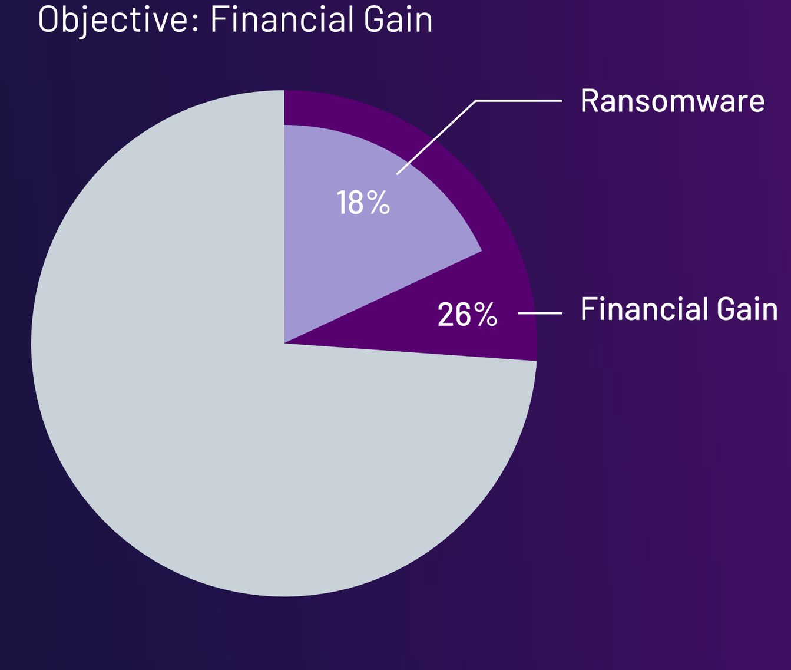
What Do They Want

Objective: Data Theft



Data theft took the top slot in 2022 with 40% of intrusions — in comparison to 29% in 2021. This is the highest percentage for data theft compared to previous years.

Objective: Financial Gain

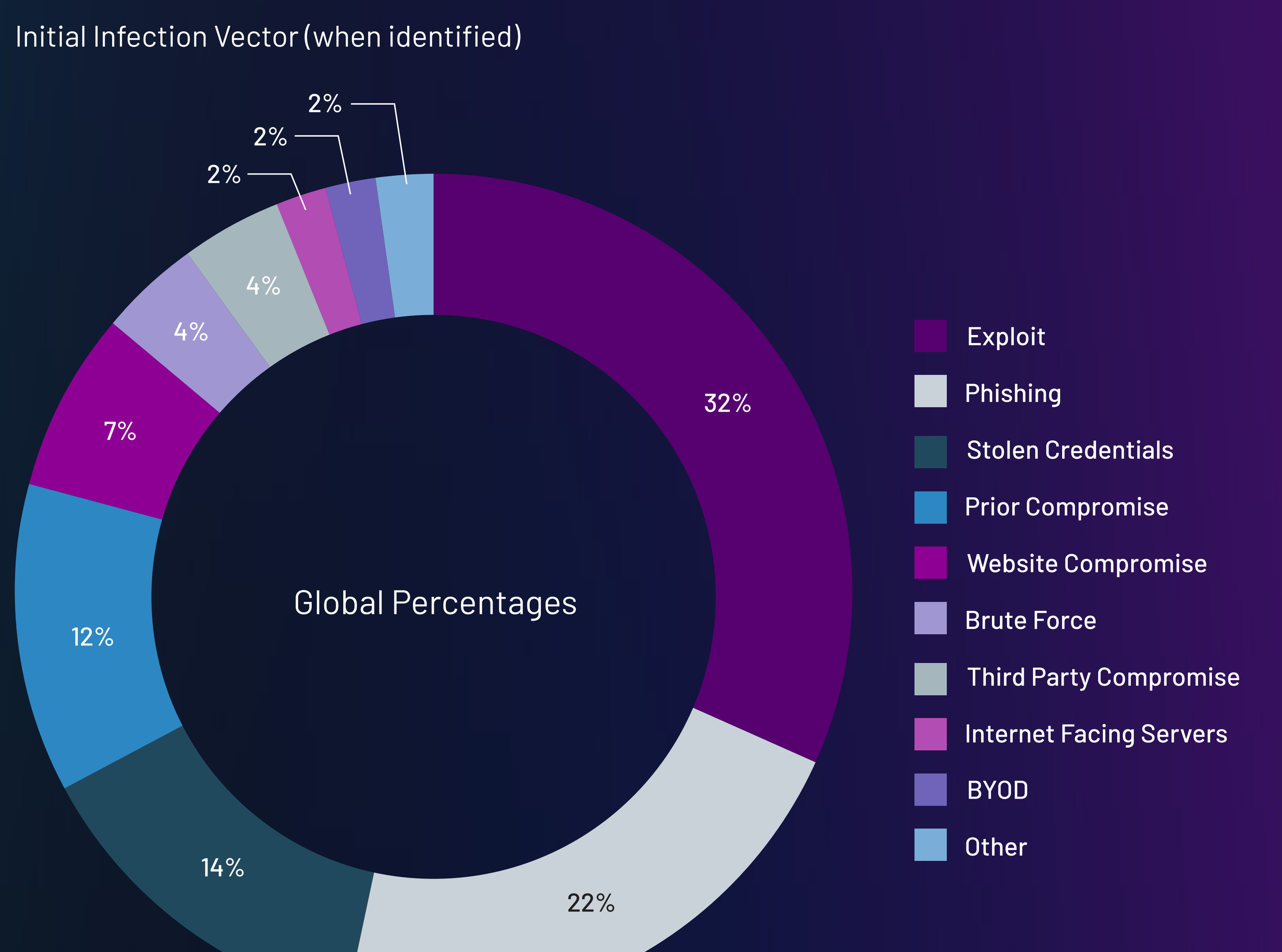


Financial gain continues to be a mainstay for adversaries, with 26% of these intrusions using methods such as extortion, ransom, sold access, illicit transfers or payment card theft.

Where Do They Attack

Targeted Attacks

Initial Infection Vector (when identified)



Most Prevalent Vector by Region

Americas Exploits **38%**	**APAC** Prior Compromise **33%**	**EMEA** Phishing **40%**

Frequently Targeted Technologies

1.	T1059: Command and Scripting Interpreter	50.9%
2.	T1027: Obfuscated Files or Information	43.5%
3.	T1071: Application Layer Protocol	33.1%
4.	T1082: System Information Discovery	31.6%
5.	T1070: Indicator Removal	31.5%
6.	T1083: File and Directory Discovery	29.5%
7.	T1140: Deobfuscate/Decode Files or Information	27.3%
8.	T1021: Remote Services	26.4%
9.	T1105: Ingress Tool Transfer	24.9%
10.	T1105: Create or Modify System Process	24.7%

When Are Attackers Found

Global Median Dwell Time

21 → **16**

Days in 2021 → Days in 2022

Dwell time is calculated as the number of days an attacker is present in a victim environment before they are detected. The median represents a value at the midpoint of a data set sorted by magnitude.

2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
416	243	229	205	146	99	101	78	56	24	21	16

Regional Median Dwell Time

Americas

Median dwell time decreased by a full week — to **10 days in 2022** compared to 17 days in 2021.

APAC

Median dwell time increased to **33 days in 2022** compared to 21 days in 2021.

EMEA

Median dwell time was **20 days in 2022** — a 58% improvement rate compared to 48 days in 2021.

Global Ransomware Median Dwell Time

Change in Global Investigations Involving Ransomware

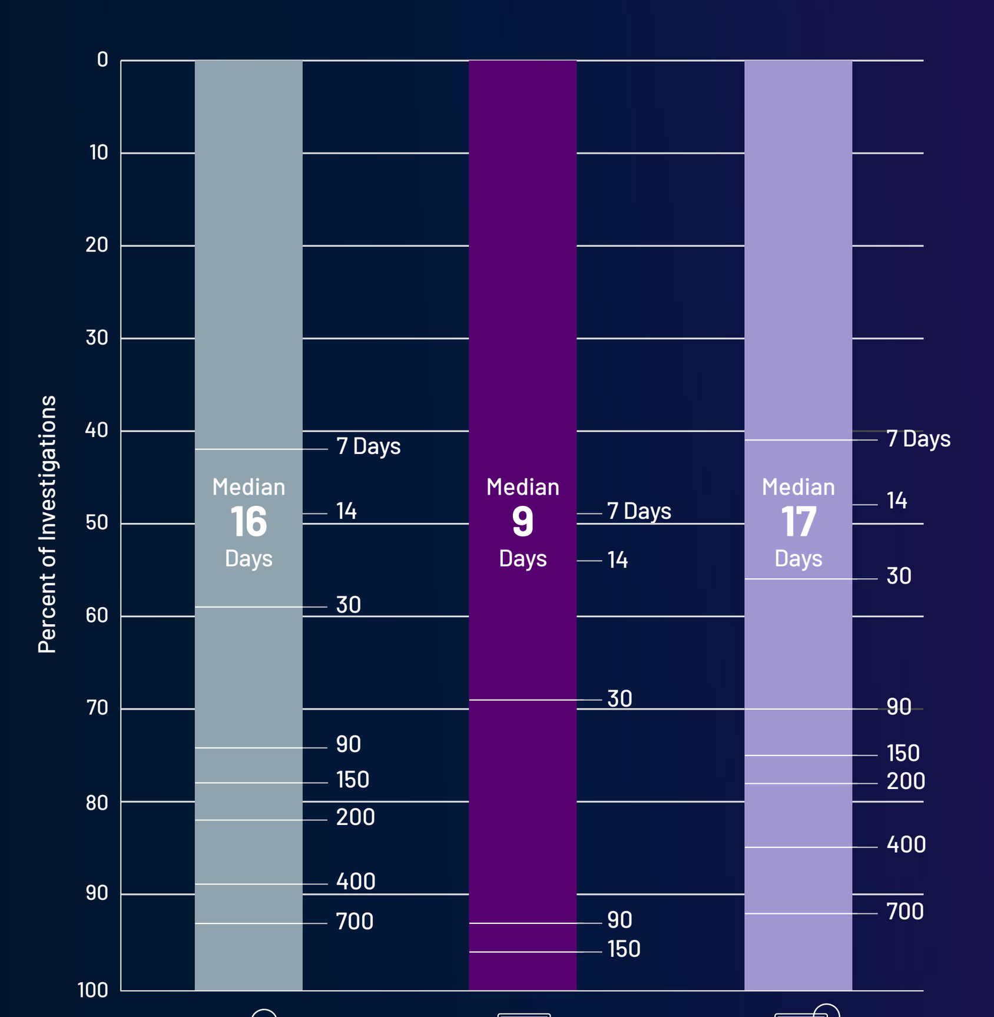
23% in 2021 → **18%** in 2022

Change in Global Median Dwell Time — Ransomware

5 Days in 2021 → **9** Days in 2022

Change in Global Median Dwell Time — Non-Ransomware

36 Days in 2021 → **17** Days in 2022



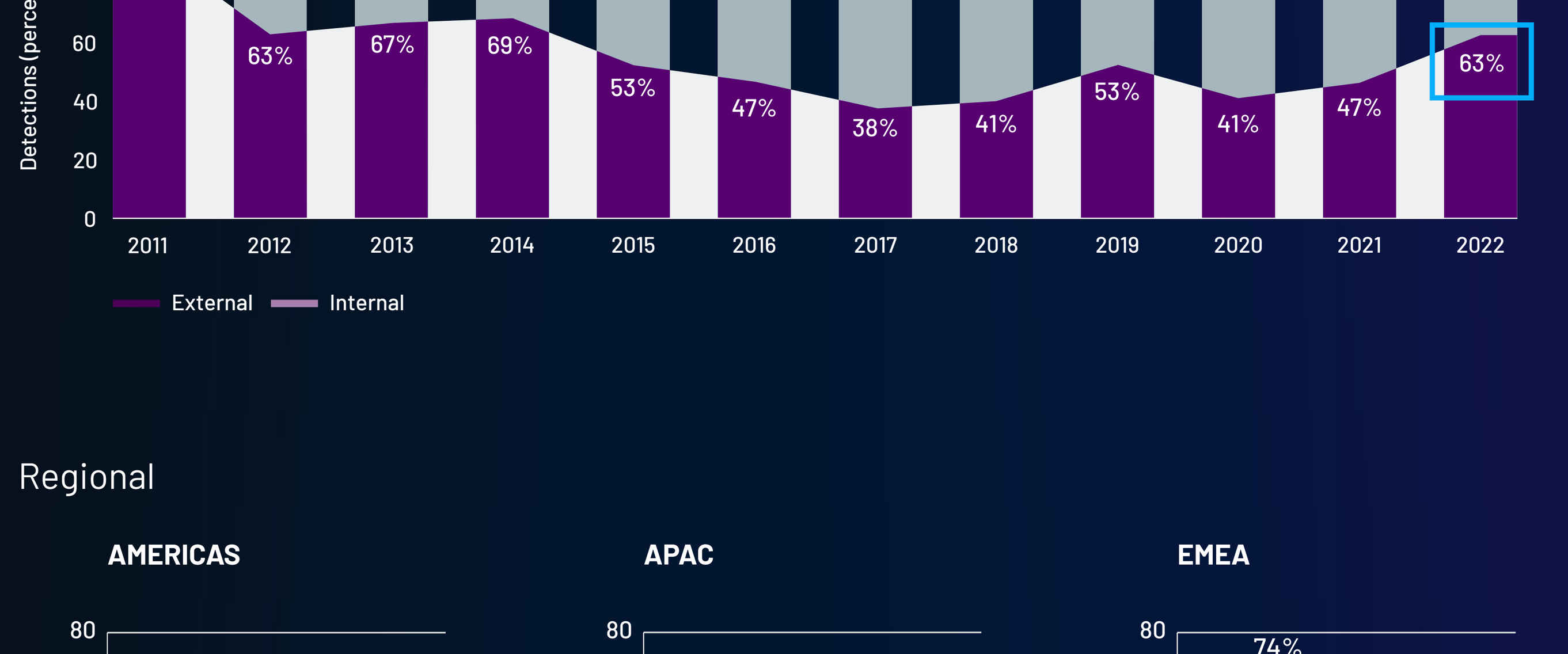
How Are Attackers Found

Internal detection is when an organization independently discovers it has been compromised.

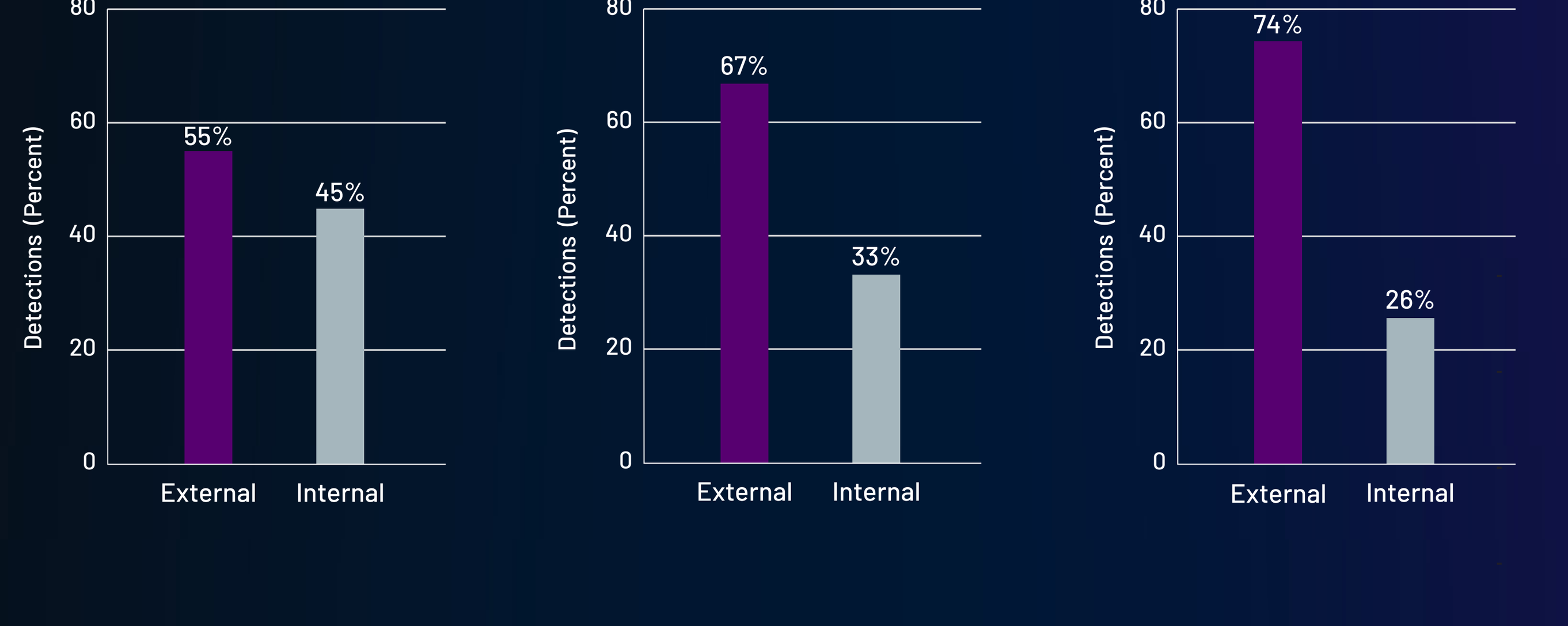
External notification is when an outside entity informs an organization it has been compromised.

Detection By Source

Global



Regional



Visit **mandiant.com/m-trends** to learn more, download the full report and access additional resources.

Learn more at www.mandiant.com

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190 (703) 935-1700833.
3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud