M-TRENDS 2022

INFOGRAPHIC

Today's cyber security trends revealed through Mandiant incident response investigations and threat intelligence findings from October 1, 2020 to December 31, 2021.

WHO ATTACKERS ARE

Mandiant experts currently track 2,800+ threat groups, which include 1,141 UNC groups, 13 FIN groups and 40 APT groups from this reporting period.

Threat Group Spotlights

FIN12

FIN12 is a financially motivated group behind prolific RYUK ransomware attacks. Relies heavily on partners to obtain initial access into victim environments. Graduated from UNC1878.

FIN13

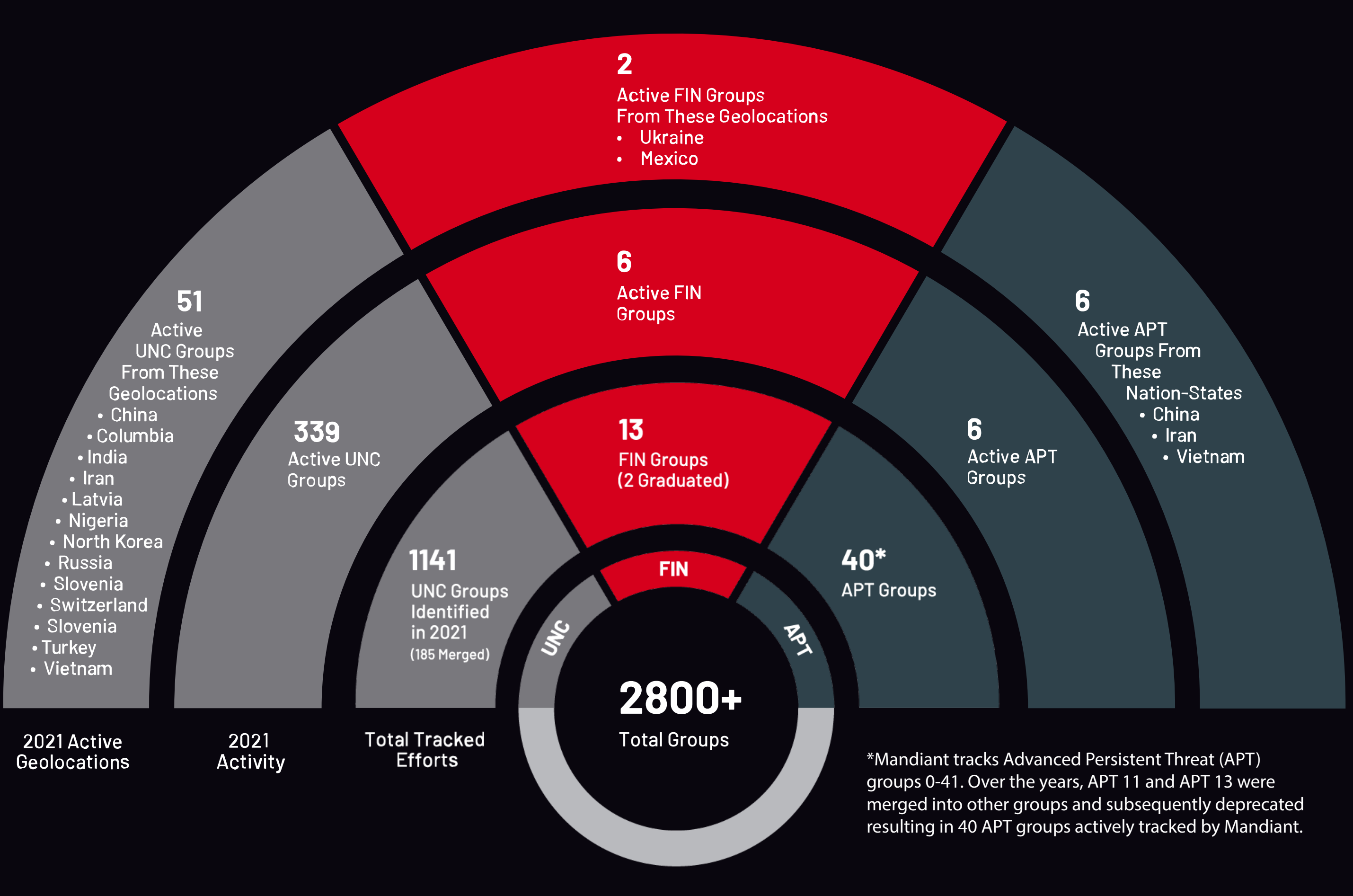
FIN13 is a financially motivated group that conducts fraudulent transfers from POS systems and ATMs—currently targeting Mexico. Graduated from UNC886.

UNC

UNC2891 targets Linux and Unix environments, with a strong focus on Oracle Solaris-based systems.

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

In 2021, Mandiant saw intrusions that involved 351 distinct threat groups, of which 80% were newly tracked. This speaks to the evolving threat landscape that security teams are up against.



*Mandiant tracks Advanced Persistent Threat (APT) groups 0-41. Over the years, APT 11 and APT 13 were merged into other groups and subsequently deprecated resulting in 40 APT groups actively tracked by Mandiant.

WHAT DO THEY TARGET

Top Industries Under Attack

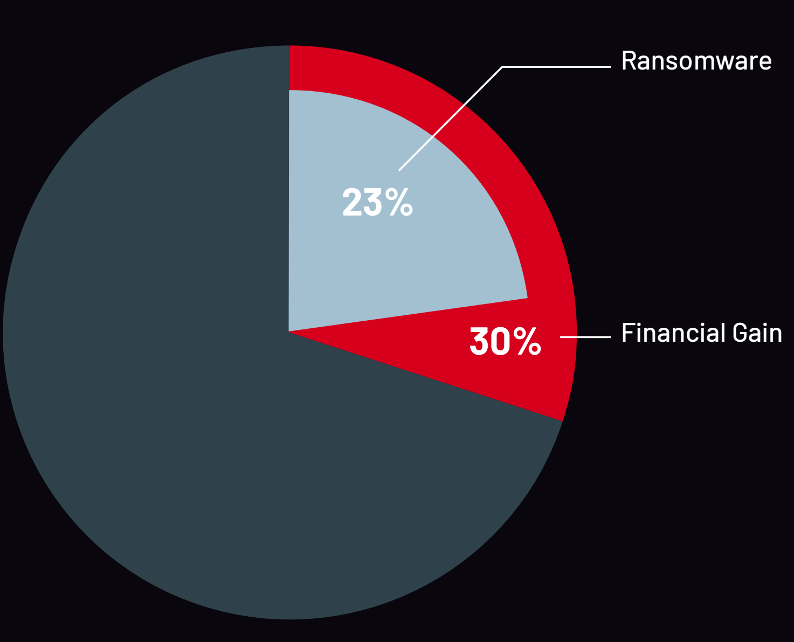
1 Business and Professional Services
4 Healthcare
2 Financial
5 High Tech
3 Retail and Hospitality

The most targeted industries remain generally consistent each year, but their relative rankings do change.

In this reporting period, Mandiant observed a high volume of compromises attributed to vulnerabilities and misconfigurations in on-premises Active Directory and cloud-based infrastructures.

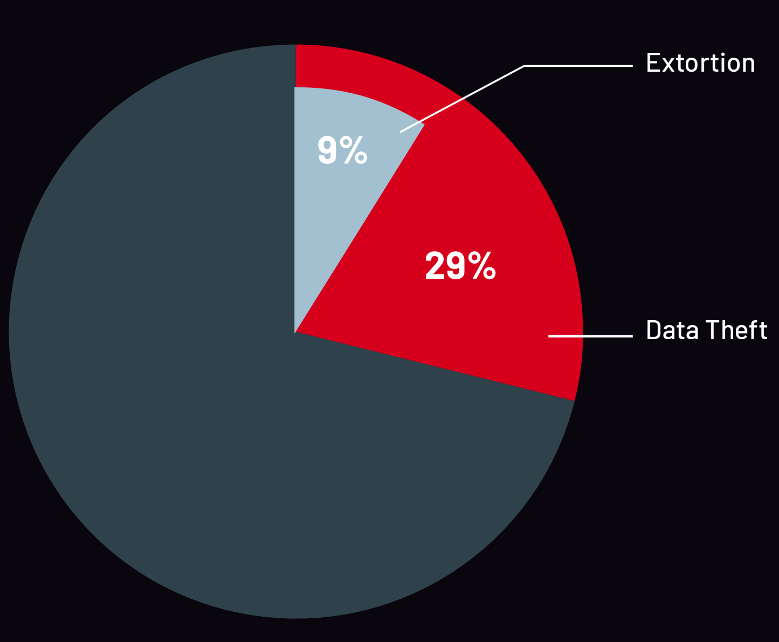
What Do They Want

Objective: Financial Gain



3 out of 10 intrusions stemmed from attackers seeking monetary gain through methods such as extortion, ransom, payment card theft and illicit transfers.

Objective: Data Theft

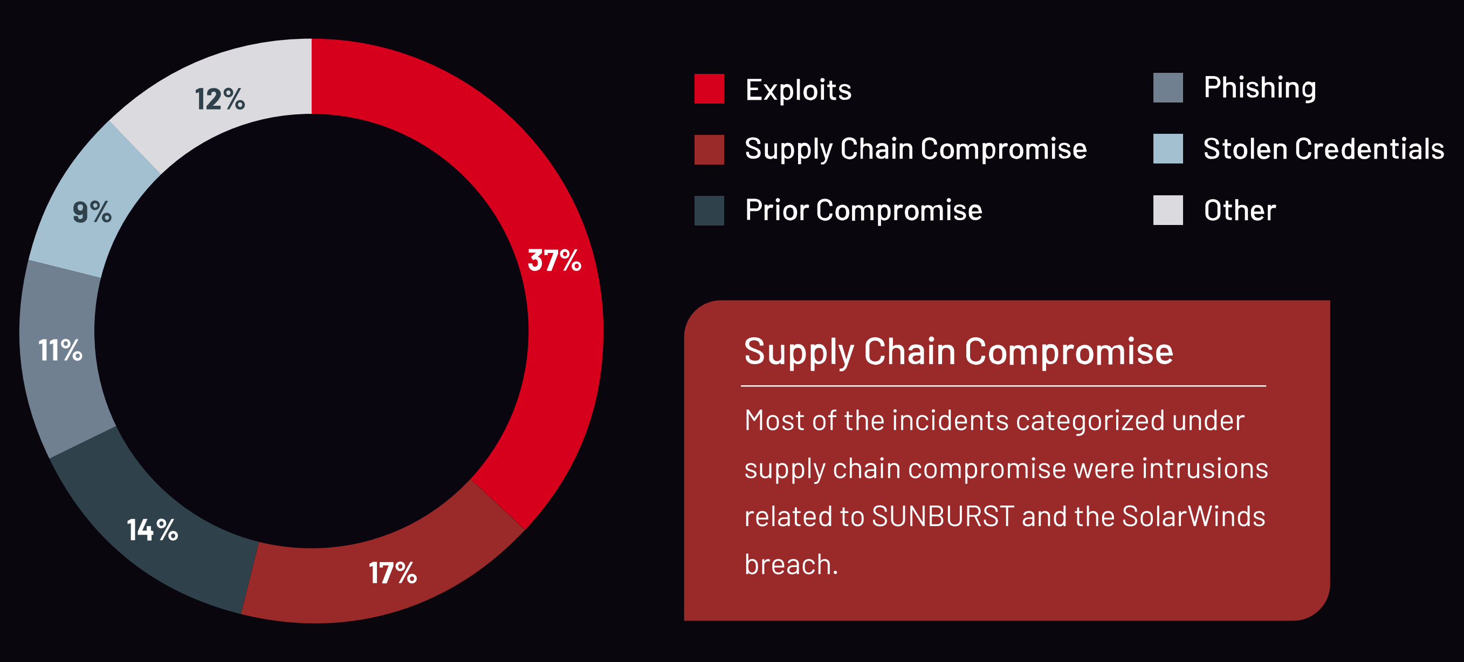


Adversaries are using data theft as leverage during negotiations for payment.

WHERE DO THEY ATTACK

Targeted Attacks

Initial Infection Vector, 2021 (When Identified)

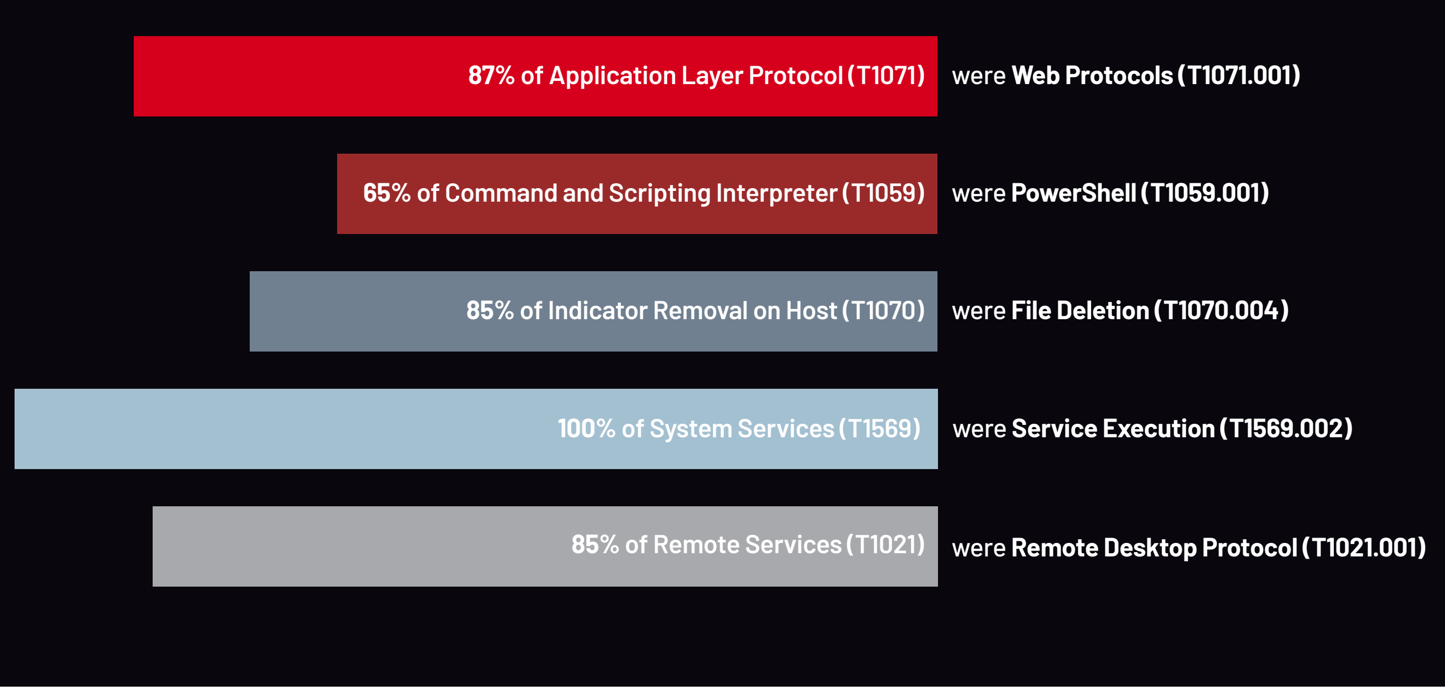


Supply Chain Compromise

Most of the incidents categorized under supply chain compromise were intrusions related to SUNBURST and the SolarWinds breach.

51% of intrusions saw adversaries use obfuscation (encryption or encoding) to make detection and subsequent analysis more difficult for security teams.

Frequently Targeted Technologies



87% of Application Layer Protocol (T1071) were **Web Protocols (T1071.001)**
65% of Command and Scripting Interpreter (T1059) were **PowerShell (T1059.001)**
85% of Indicator Removal on Host (T1070) were **File Deletion (T1070.004)**
100% of System Services (T1569) were **Service Execution (T1569.002)**
85% of Remote Services (T1021) were **Remote Desktop Protocol (T1021.001)**

WHEN ARE ATTACKERS FOUND

Global Median Dwell Time

24 DAYS IN 2020 → **21** DAYS IN 2021

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.

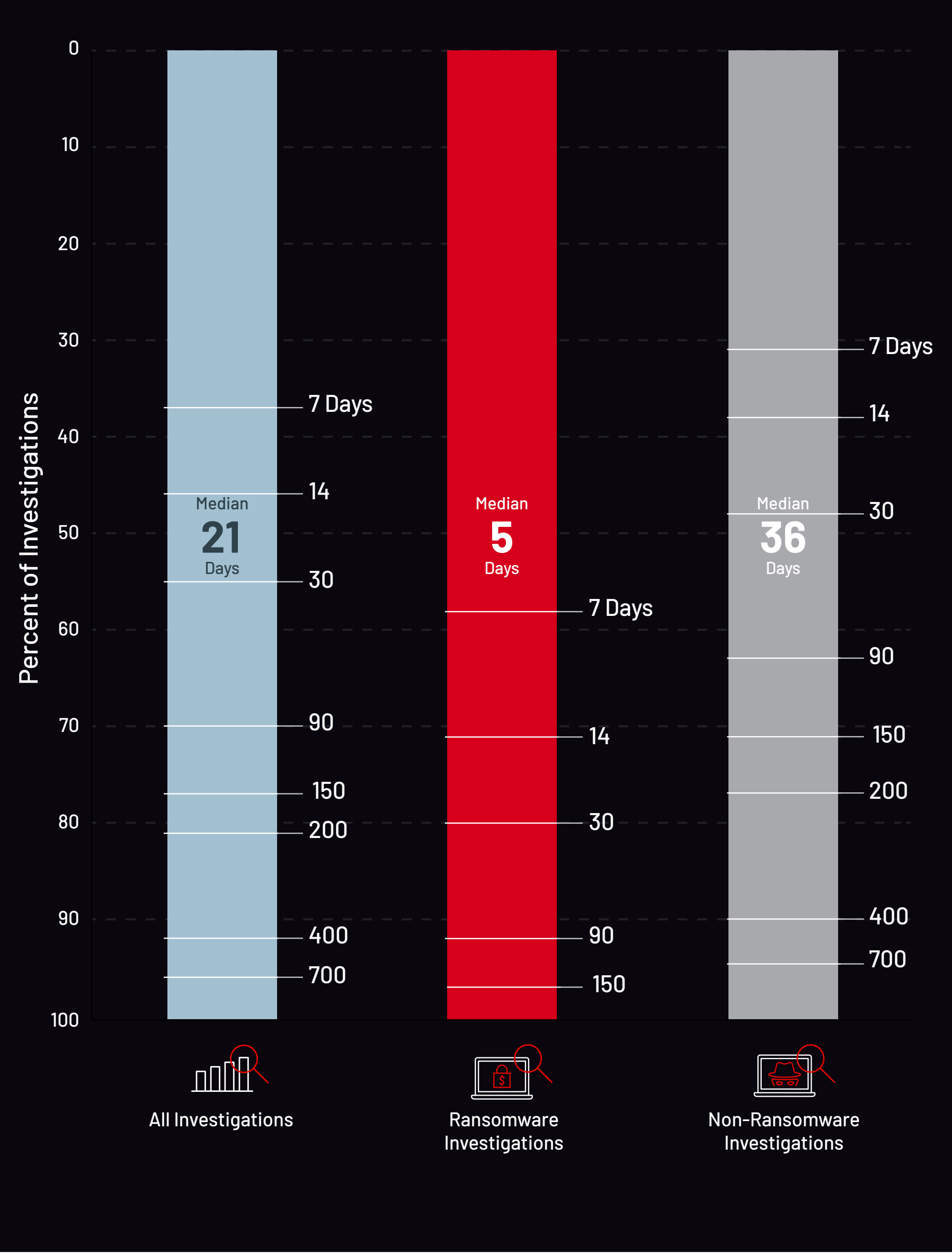
Year	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Days	416	243	229	205	146	99	101	78	56	24	21

Global Ransomware Median Dwell Time

Change in Investigations Involving Ransomware
25% IN 2020 → **23%** IN 2021

No Change in Global Median Dwell Time: Ransomware
5 DAYS IN 2020 → **5** DAYS IN 2021

Change in Global Median Dwell Time: Non-ransomware
45 DAYS IN 2020 → **36** DAYS IN 2021



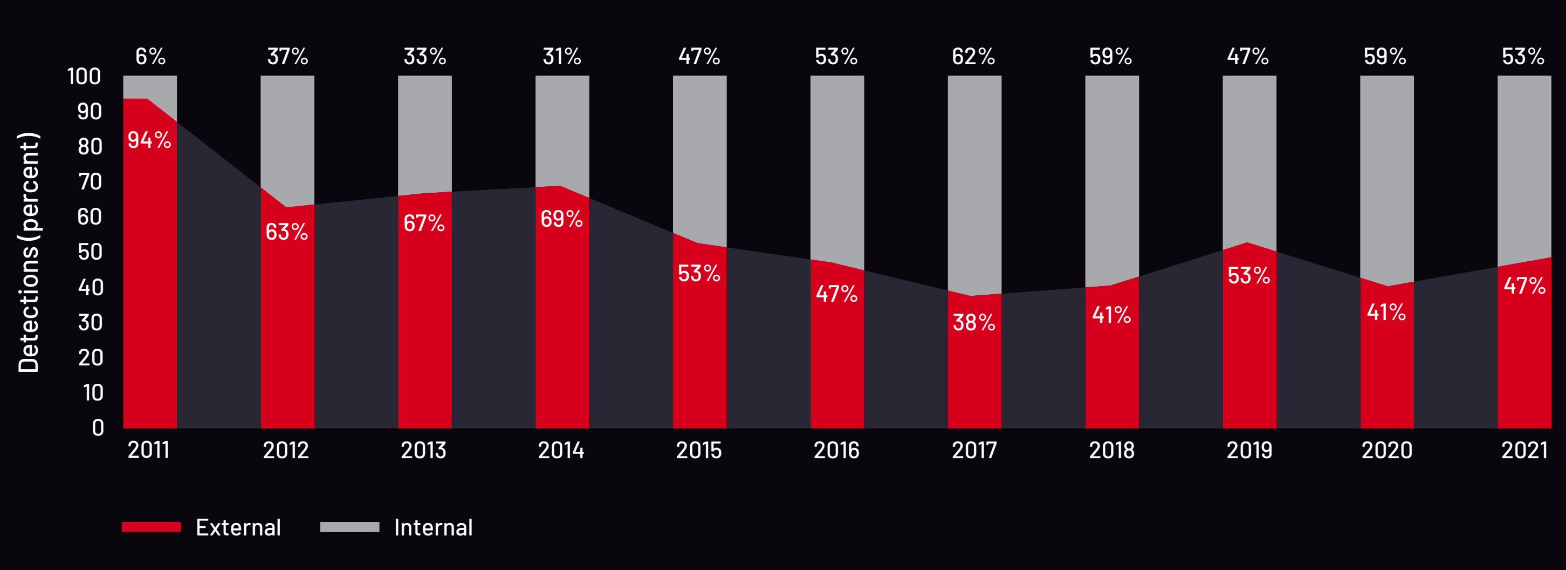
HOW ARE ATTACKERS FOUND

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

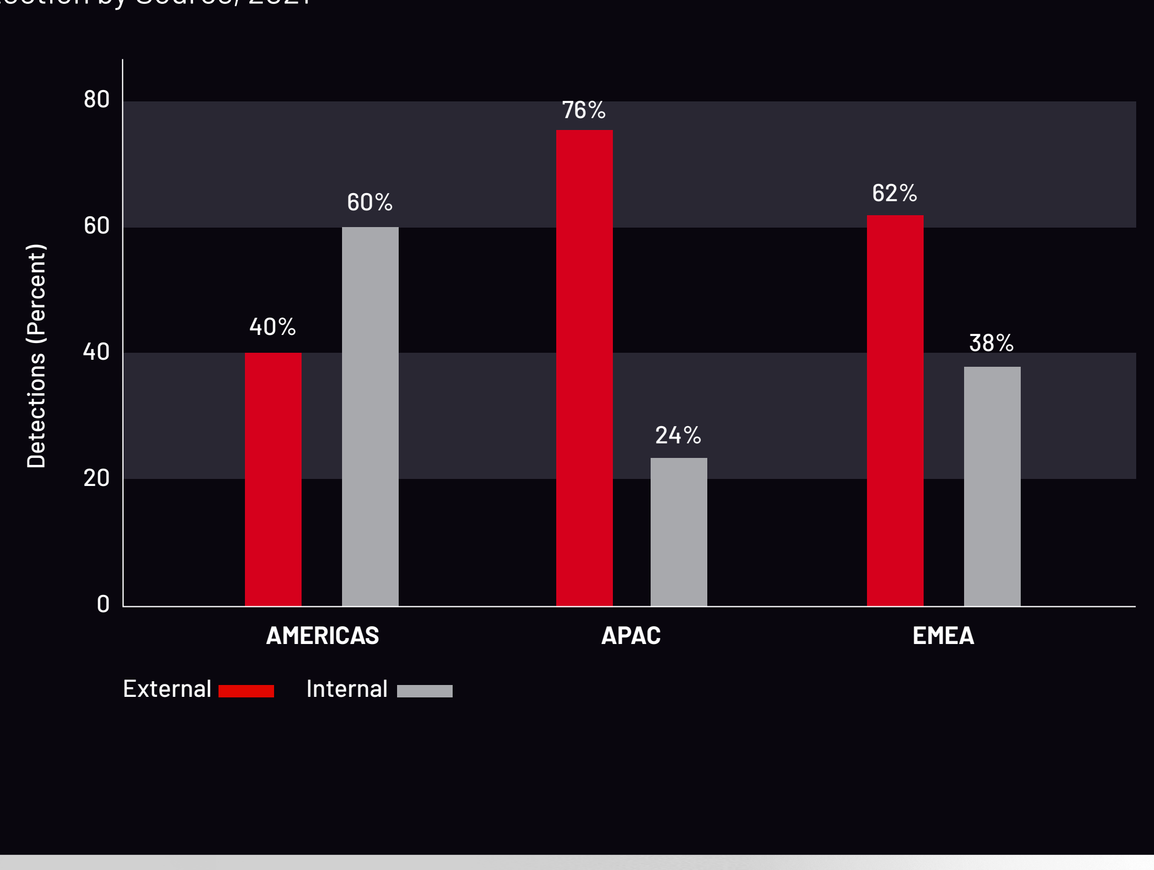
External notification is when an outside entity informs an organization it has been compromised.

Detection by Source

Global Detection by Source, 2011-2021



Regional Detection by Source, 2021



DISCOVER MORE DETAILS, LEARNINGS AND MITIGATION STRATEGIES AT **mandiant.com/m-trends.**

MANDIANT