FIREEYE | MANDIANT

M-TRENDS 2021

FIREEYE MANDIANT SERVICES | SPECIAL REPORT

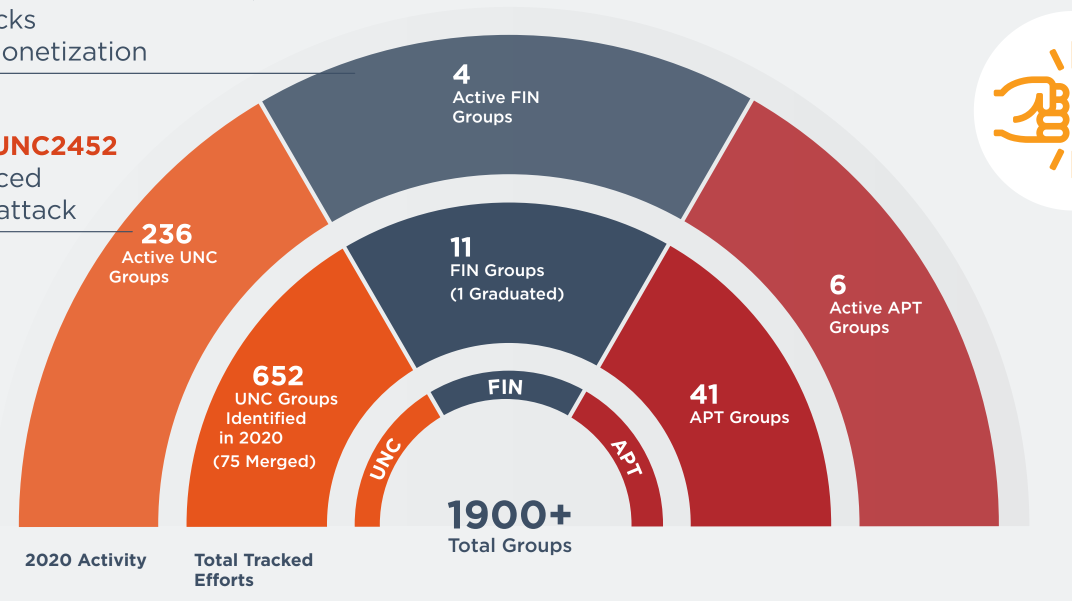
Cyber security trends revealed through Mandiant incident response investigations and engagements from October 1, 2019 to September 30, 2020.

WHO ATTACKERS ARE

Today's Threat Groups

FIN11 (graduated from UNC902)
Phishing attacks focused on monetization

SUNBURST/UNC2452
Highly advanced supply chain attack



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

Today, adversaries more frequently work together to complete their missions.

Multiple Threat Groups Identified per Environment

2020 **29%**

2019 **15%**

WHAT THEY TARGET

Top Industries Under Attack

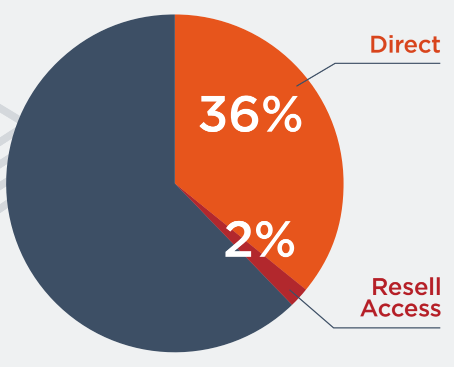
- Business/ Professional Services
- Retail/ Hospitality
- Healthcare
- High Tech
- Financial

Attackers targeting pandemic-related industries
APT32, APT41, UNC788, UNC2062

WHAT THEY WANT

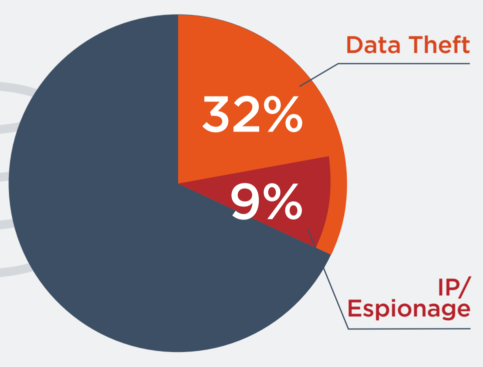
Targeted Attacks

Objective: Financial Gain



***Direct** financial gain includes extortion, ransom, payment card theft and illicit transfers.*

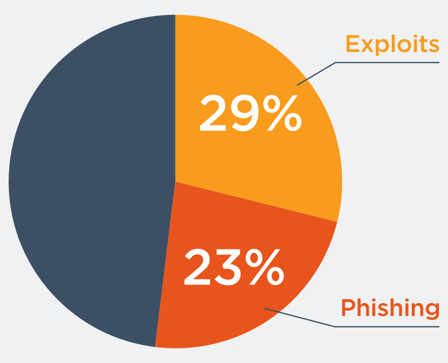
Objective: Data Theft



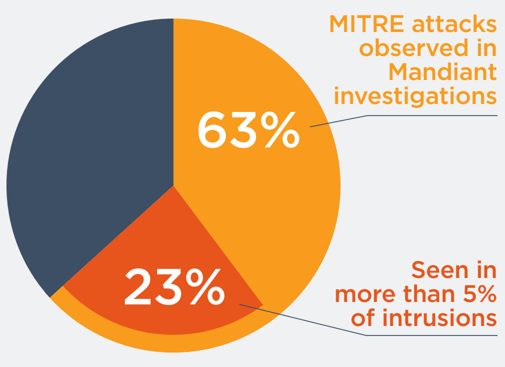
HOW THEY ATTACK

Most Frequently Used Techniques

Initial Infection Vector
(when identified)



MITRE ATT&CK



***MITRE ATT&CK®** is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.*

Frequently Targeted Techologies

88% Remote Desktop Protocol (T1021.001) for intrusions using **remote services (T1021)**
Used in 25% of all intrusions

100% Windows services (T1569.002) for intrusions using **system services (T1569)**
Used in 31% of all intrusions

80% PowerShell (T1059.001) for intrusions using **command or scripting interpreter (T1059)**
Used in 41% of all intrusions

A Surge in Ransomware

One in four Mandiant incident response engagements involved ransomware.

2020 **25%**

2019 **14%**

Global Median Dwell Time

Ransomware Investigations
2020
5 Days

Non-Ransomware Investigations
2020
45 Days

WHEN WE FIND THEM

Global Median Dwell Time

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

All Investigations

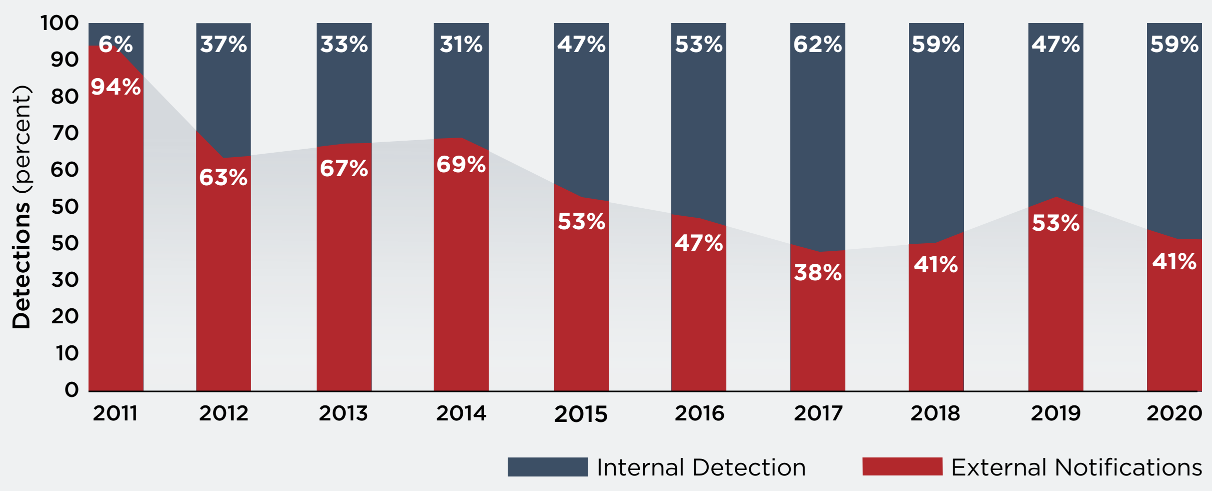
***Dwell time** is calculated as the number of days an attacker is present in a victim environment before they are detected. The median represents a value at the midpoint of a data set sorted by magnitude.*

HOW WE FIND THEM

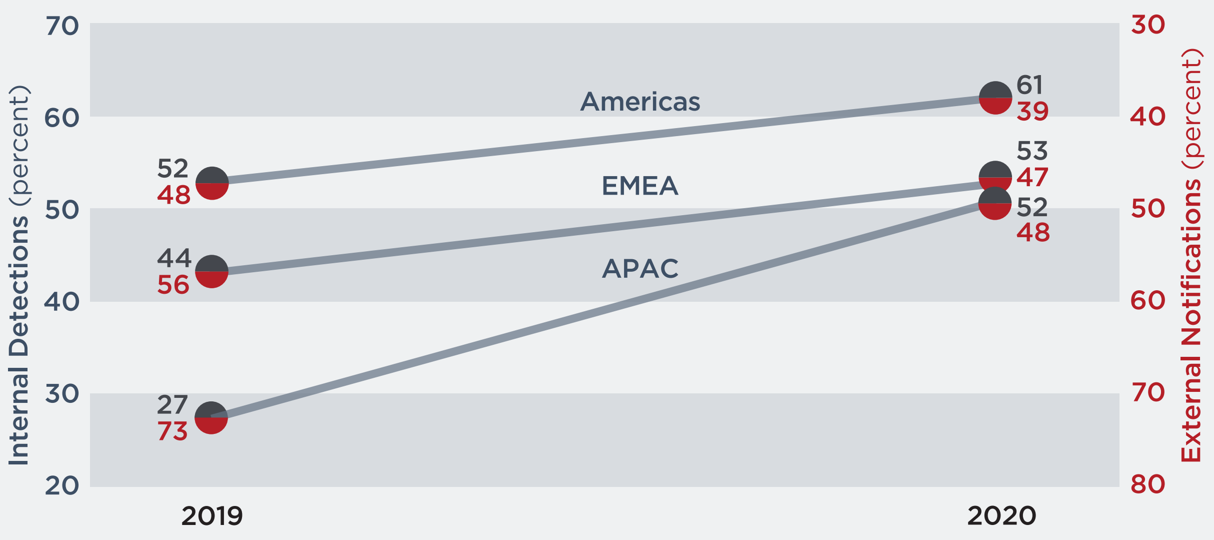
Global Detection by Source: 2011–2020

***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.*



Regional Detection by Source: 2019 and 2020



To discover more details, learnings and mitigation strategies, read the full report at **www.fireeye.com/m-trends**

Disclosure Case studies and examples are drawn from our experiences and activities working for a variety of customers, and do not represent our work for any one customer or set of customers. In many cases, facts have been changed to obscure the identity of our customers and individuals associated with our customers.

©2021 FireEye, Inc. All rights reserved. FireEye and Mandiant are registered trademarks of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. M-EXT-IG-US-EN-000377-01

FIREEYE™ | MANDIANT®