

NOWHERE TO HIDE + EMEA

2022 Falcon OverWatch Threat Hunting Report



Every year, CrowdStrike's proactive 24/7 threat hunting team, Falcon OverWatch™, publishes its findings and technical analysis detailing the novel and prominent adversary tradecraft and emerging intrusion trends the team unearthed during the preceding 12-month period from July 1, 2021 through June 30, 2022. The following contains OverWatch's findings, analysis and case studies relevant to the Europe, Middle East and Africa (EMEA) region.

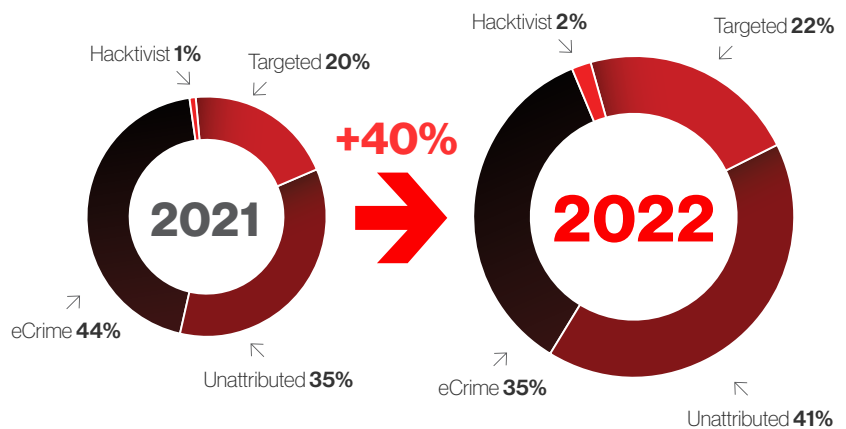
EMEA Hit by a Balance of eCrime and Targeted Intrusions

- +** OverWatch tracked a near **40% increase in interactive intrusions** year-over-year (YoY) against victim organizations operating in EMEA.
- +** **eCrime accounted for 35% of the interactive intrusion activity in EMEA**, while **targeted intrusions increased to 22%** and **hacker activity made up 2%**; the remaining 41% of intrusions were unattributed.

EMEA intrusions are relatively balanced in terms of eCrime and targeted intrusion types, which is in contrast to the two other regions, where intrusion types vary more widely. **22% EMEA, 35% APAC, 7% Americas.**

EMEA: Intrusion Campaigns by Threat Type

July 2020 to June 2021 vs. July 2021 to June 2022



eCrime

Financially motivated criminal intrusion activity

Targeted

State-nexus intrusion activity that includes cyber espionage, destructive or disruptive attacks, and currency generation to support a regime

Hacker

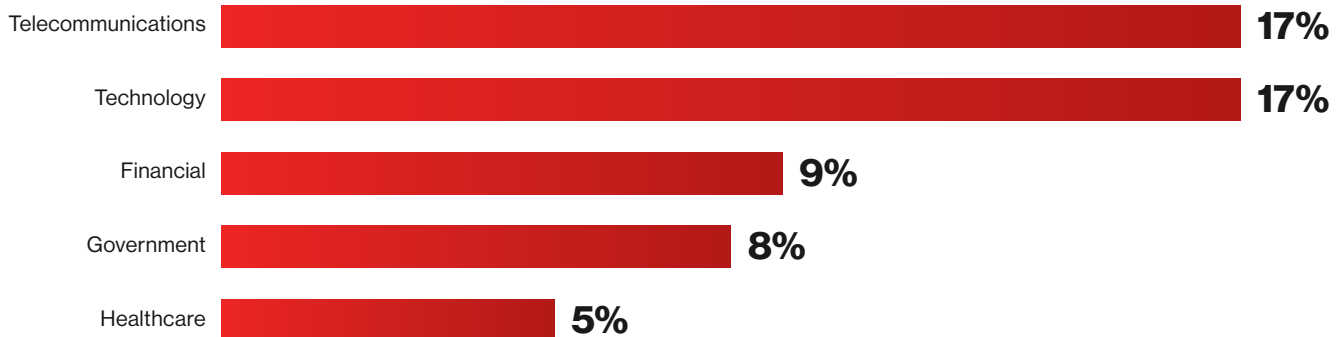
Intrusion activity undertaken to gain momentum, visibility or publicity for a cause or ideology

Unattributed








Insufficient data available for high-confidence attribution

Telecommunications and Technology

Frequent Industry Targets in EMEA



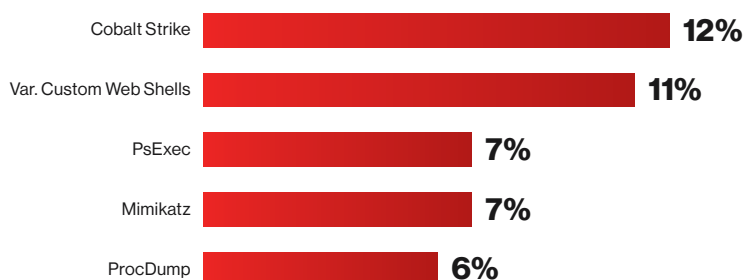
Adversaries Operating in EMEA

-  PROPHET SPIDER
-  VICE SPIDER
-  STATIC KITTEN
-  NEMESIS KITTEN
-  COSMIC WOLF
-  CARBON SPIDER
-  LABYRINTH CHOLLIMA

- +** The most commonly tracked threat groups in the EMEA region included two eCrime actors: **PROPHET SPIDER** and **VICE SPIDER**, and three targeted intrusion actors: **STATIC KITTEN (Iran)**, **NEMESIS KITTEN (Iran)** and **COSMIC WOLF (Turkey)**.¹
- +** Five threat actors were seen consistently across all three regions (listed in order of attack frequency): **PROPHET SPIDER**, **CARBON SPIDER (eCrime)**, **NEMESIS KITTEN**, **LABYRINTH CHOLLIMA (North Korea)** and **COSMIC WOLF**.
- +** For organizations operating in EMEA, the top five industry verticals by intrusion frequency were **telecommunications (17%)**, **technology (17%)**, **financial (9%)**, **government (8%)** and **healthcare (5%)**.

Custom Web Shells Leveraged Heavily in EMEA Intrusions

EMEA: Top 5 Tools



The top five tools observed in use in intrusions in the EMEA region were **Cobalt Strike (12%)**, **various custom web shells (11%)**, **PsExec (7%)**, **Mimikatz (7%)** and **ProcDump (6%)**. Both Mimikatz and Cobalt Strike appeared in the top five across all three regions.

¹ CrowdStrike Falcon Intelligence is responsible for the classification and attribution of all covered adversary names mentioned in this report; for more information on specific threat actor groups, please visit <https://adversary.crowdstrike.com>.



Cobalt Strike



Objectives

Command and Control (C2),
Defense Evasion, Persistence



Targets

Windows-run Hosts



Characteristics

- Robust penetration-testing tool with lightweight post-exploitation agent, beacon
- Beacon payload enables interaction with an infected machine
- Majority of big game hunting incidents feature Cobalt Strike

PsExec



Objectives

Command and Control (C2), Lateral
Movement, Privilege Escalation



Targets

Windows-run Hosts



Characteristics

- Compromised use of legitimate system admin utility
- Versatile capabilities to remotely execute host commands
- Used to escalate Administrator privileges to System through service creation



Know the Tradecraft.
Know the Adversary.
Hunt Relentlessly.



Download the Full Report

crowdstrike.com