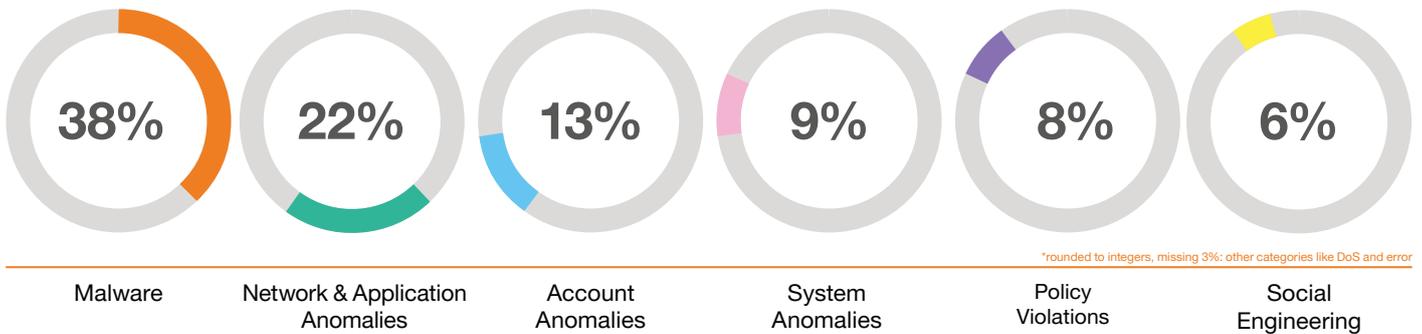# Orange Cyberdefense

orange™

Security Navigator 2022

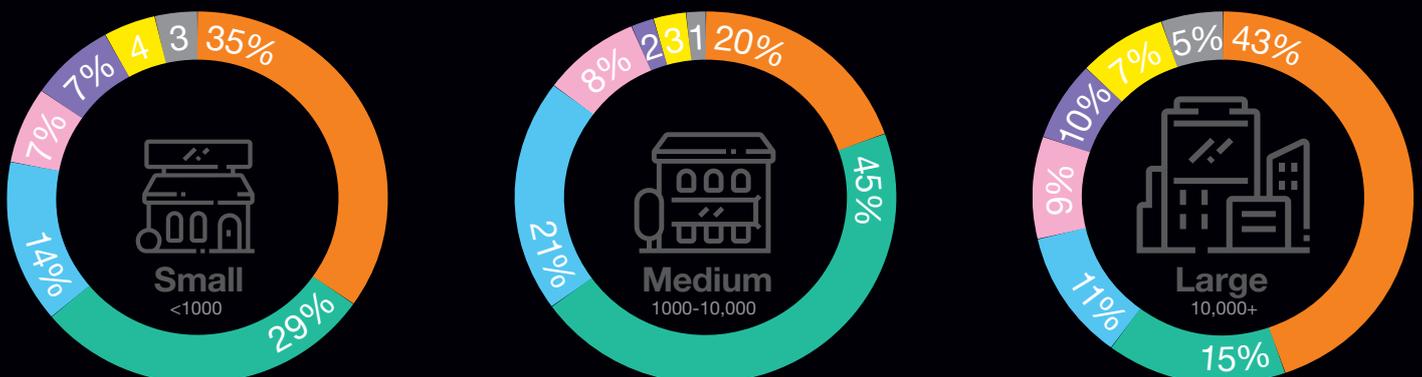## Research-driven insights to build a safer digital society

- Get the 'big picture' of cybersecurity

- 100% first-hand information from the 18 global SOCs & 14 CyberSOCs of Orange Cyberdefense, the CERT, Epidemiology Labs & World Watch

- Gain invaluable insights into the threat landscape

- Expert reports and technology reviews on topics like Ransomware, Cyber Extortion and the analysis of leak sites

- Check attack patterns and statistics for your business size and vertical

- Learn what the most disrupting events in 2021 were and how that projects into the future

- Here are some interesting findings. Get the full 90-page report for free here!

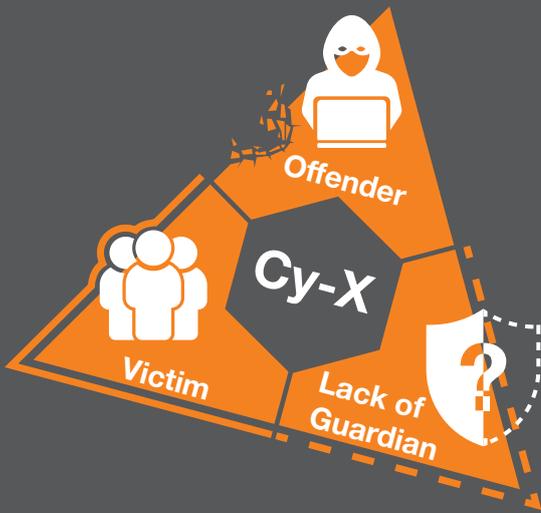## Funnel: 94,806 incidents ▶ 34,158 confirmed security incidents

38%	22%	13%	9%	8%	6%
Malware	Network & Application Anomalies	Account Anomalies	System Anomalies	Policy Violations	Social Engineering

*rounded to integers, missing 3%: other categories like DoS and error

A matter of scale: Incidents by business size

Legend: ■ Malware ■ Network & Application ■ Account ■ System ■ Policy Violations ■ Social Engineering ■ Others

Small <1000
- 35% Malware
- 29%
- 14%
- 7%
- 7%
- 4
- 3

Medium 1000-10,000
- 20% Malware
- 45%
- 21%
- 8%
- 2
- 3
- 1

Large 10,000+
- 43% Malware
- 15%
- 11%
- 9%
- 10%
- 7%
- 5%

CSI Cyber Extortion (Cy-X):
The criminology of Ransomware

We leave the position of the defender or attacker and instead explore the perspective of Cy-X as a crime. In criminology the term of "routine activity theory" (RAT) is a standard way of analyzing crime. According to RAT three factors need to be present for a crime to occur: A a motivated offender, a suitable victim and the lack of a capable guardian. Mapping these tree factors to Cy-X helps us understand how we can address the root causes of this crime on a strategic level.

These techniques could prove highly effective and are largely independent of the actual technical implementation that threat actors use and defenders try to cancel in their digital arms race.

Offender

Cy-X

Victim

Lack of Guardian

Ransomware off-road:
Beyond encryption

Our experts have observed 67 leak sites frequently used for Double-Extortion and Cy-X. Our research team has monitored these sites for several months and collected data on more than 3000 extortions. What we found made a complete chapter.

From this data set we try to give an overview of the criminal scene behind Cy-X, we analyze who the actors are and which countries, industries and business sizes are their victims. We get a glimpse of the shifts in regard to actors and technologies we frequently see going on "behind the scenes".

Cy-X leak threats

Threatened exposure cases observed on leak sites over time (e.g. for double extortion)

■ leak threats

| | Jan | Feb | Mrz | Apr | Mai | Jun | Jul | Aug | Sep | Okt | Nov | Dez | Jan | Feb | Mrz | Apr | Mai | Jun | Jul | Aug | Sep |

For more information check www.orangecyberdefense.com!