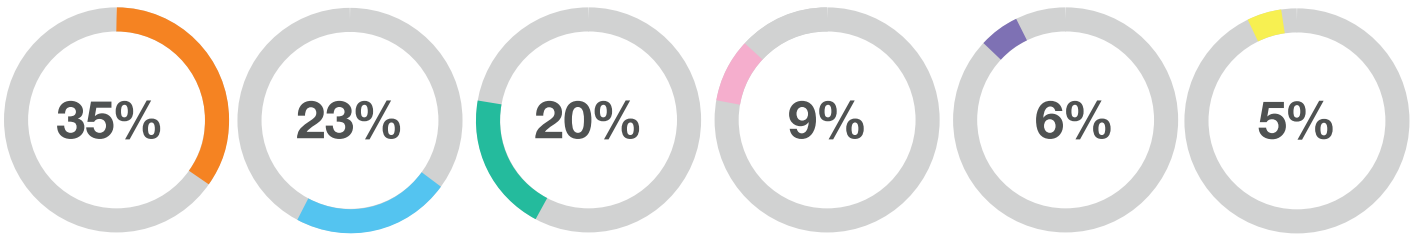
Orange
Cyberdefense

Security Navigator 2021

Research-driven insights to build a safer digital society

- Get the 'big picture' of cybersecurity
- 100% first-hand information from the 17 SOCs & CyberSOCs of Orange Cyberdefense, the Epidemiology Labs & World Watch
- Gain invaluable insights into the threat landscape
- Expert reports and technology reviews on topics like videoconferencing solutions and the cybercrime ecosystem
- Check attack patterns and statistics for your business size and vertical
- Learn what the most disrupting events in 2020 were and how that projects into the future
- Here are some interesting findings. Get the full 90-page report for free!

Funnel: 1,775,505 events ▶ 18,910 verified security incidents



*rounded to integers, missing 2%: other categories like DoS and error

Network & Application Anomalies | Account Anomalies | Malware | System Anomalies | Policy Violations | Social Engineering

A matter of size: Median number of incidents per organization

Some of our Medium sized businesses have dealt with a very low number of Confirmed Incidents this year. This is a positive indicator, and this has led to an overall decrease in Confirmed Incidents per business since last year.

Small	Medium	Large
Organizations (<1,000 employees)	Organizations (<10,000 employees)	Organizations (10,000+ employees)
101	77	278

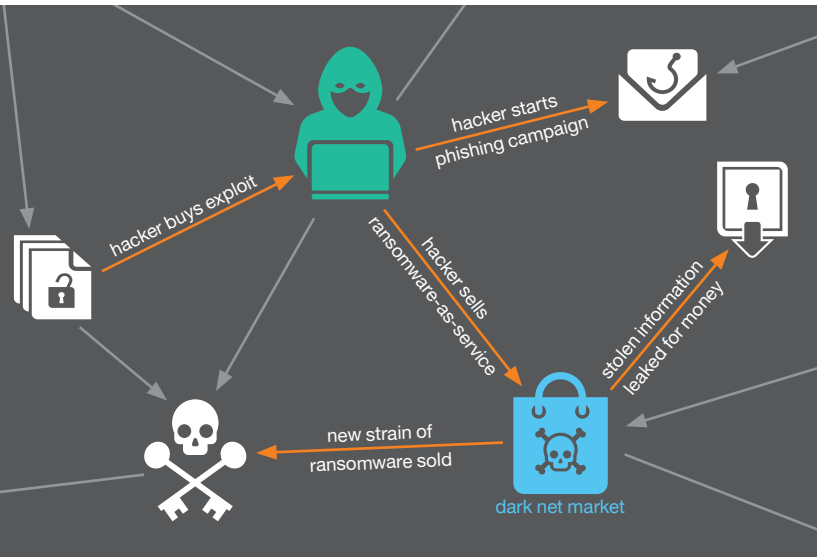
Read the full stories! Get your free copy of the Security Navigator on:
orangecyberdefense.com/navigator/

A look at the dark side

How does the cybercrime ecosystem work?

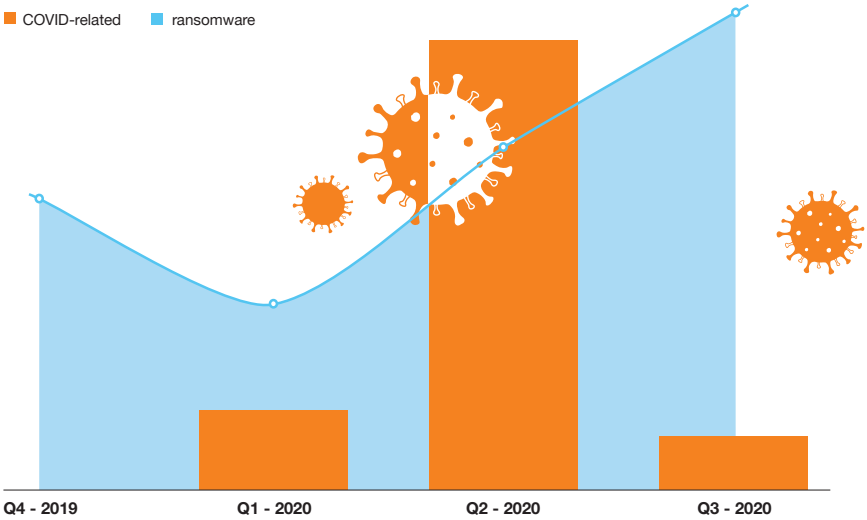
The cybercrime ecosystem hosts a range of players each with their own avenue of expertise and many ways to monetise products like malware, botnets, stolen information and other illegal goods and services. A true understanding of this ecosystem and its systemic drivers is essential to getting to the core of the cybercrime problem and developing a strategy that will enable us to strike it at its root.

One critical element of cybercrime, that is not as well understood as it should be, lies at the very root of the problem: the flow of money and value between different players in the cybercrime ecosystem.



What impact did COVID-19 really have?

Example: Ransomware activity



After a slight decrease during the first quarter of 2020, significant ransomware incidents have been trending upwards in our data steadily throughout the course of the year. Ransomware is carried by a combination of powerful systemic drivers that include insatiable demand, limited supply and the smooth flow of value.

In summary:

- Criminals may pivot to new disguises or lures based on 'hot topics'
- This does not trigger an overall increase in activity or change in basic attack schemes

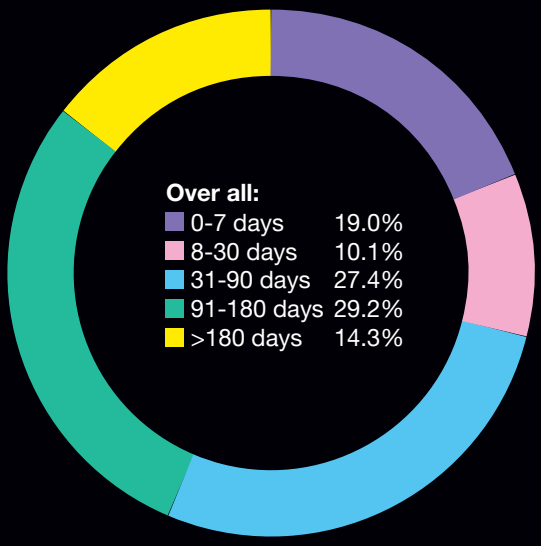
There are other major systemic factors and forces that have a much bigger influence on attacker behaviour than the COVID-19 pandemic or the fact that people are working from home.

When was your last patch-day?

A limited study we conducted across 168 security product vulnerabilities over the last 12 months reveals that, not only is the increased volume of these vulnerabilities a problem, but businesses are also taking too long to patch them.

We found that just 19% of vulnerabilities are patched within 7 days. However, the majority of 56.8% of these vulnerabilities are taking between 31 and 180 days to get resolved, and a deeply concerning 14% of vulnerabilities are still not addressed six months after notification.

In a recent advisory released by the U.S National Security Agency (NSA) titled 'State-Sponsored Actors Exploit Publicly Known Vulnerabilities' , they list the 25 known vulnerabilities in active use by state sponsored actors. Six of the them involve perimeter security technologies.



For more information check www.orangecyberdefense.com!