Press release
Paris, 10 December 2020

Orange Cyberdefense, the European leader in cybersecurity services, delivers its in-depth analysis of the state of threat in 2020 and shares its vision for 2021

- A constant volume of attacks even during the COVID-19 lockdown with an explosion of ransomware attacks linked to new business models
- An acceleration of IT transformation as a result of the COVID-19 pandemic, introducing new risks and security challenges: cybersecurity is now at the core of most businesses, requiring a new approach
- A cybercriminal ecosystem that has become more structured and professional as a result of huge potential rewards

Orange Cyberdefense publishes its annual report, the Security Navigator, which analyzes the evolution and changes in cyber threats. The data, collected between January and October 2020, comes from the 50 billion security events analyzed by Orange Cyberdefense's 17 SOCs and 11 CyberSOCs globally, the epidemiology laboratory, and the research center, as well as from expert reports and benchmark studies.

This 2021 edition provides a unique and comprehensive view of the cybersecurity ecosystem during the health crisis, which has hit all countries and companies.

"*With Security Navigator 2021, our customers and partners have access to our cyber threat analysis. It is based on recognized expertise in Threat Intelligence and on data collected around the world via the Orange Group's international network*," said **Hugues Foulon, Executive Director of Strategy and Cybersecurity activities at Orange Group**. He adds "*In a technical context and with organizations shaken by the Covid crisis, this Security Navigator provides a state of the threat that will usefully enlighten corporate decision-makers*".

Never before has it been more important to progress from a mode of crisis and reactivity to take back control of one's cybersecurity journey and build a safer digital society.

2020: the year of the COVID-19 pandemic

A clear observation: 2020, despite the crisis, has not been the year of a major explosion of cyberattacks except for ransomware actors who have changed their business models

The general slowdown of the global economy has not had a significant impact on the behavior of attackers. Cybercriminals used the COVID-19 theme opportunistically but relatively quickly; this subterfuge was abandoned in favor of more classic themes. For

example, attacks using COVID-19 as an object most likely represented less than 2% of the attacks recorded during April. The attackers' behavior was only superficially and temporarily modified during the crisis (pages 43 to 54).

There has also been no noteworthy explosion in terms of the volume of alerts but a trend towards attacks targeting users more, particularly via social engineering[1] (1% of attacks in 2019 vs. 5% in 2020). The most frequent incidents have been network and application anomalies (35%), user account anomalies (23%), and malware (20%) (pages 9 to 26).

Ransomware, a growing "data-centric" business

Ransomware was originally a relatively unsophisticated malware that, after penetrating the victim's IT system, encrypted all data. The victim can only retrieve the decryption key in exchange for a ransom payment. This type of attack was aimed primarily at small organizations or individuals who were easy to attack, lacked backups, and were willing to pay small ransoms for the recovery of their data. The development of cryptocurrencies, which facilitates transactions that cannot be easily traced back to the attackers, has enabled the rapid development of these attacks. This was clearly a mass-market business model, targeting any kind of victim. (page 46).
In 2020, ransomware groups have evolved their "business model" by monetizing not only the availability of data but also its confidentiality: in addition to seeing their data encrypted, companies are under the threat of having some of it publicly disclosed. An approach that allows for "big game hunting", where large companies are targeted, with ransoms amounting to millions of euros (pages 18 and 19; page 46).

Cascading vulnerabilities

Orange Cyberdefense experts' analysis shows the discovery of unusually high numbers of vulnerabilities within security products, particularly those essential to remote working. This growth can partly be explained by a "domino effect" or "cascade" in research: the discovery of one vulnerability leads to the discovery of another one within the same tool or the same vulnerability in other tools... This is a more positive observation than it might seem because it ultimately enables the security of these solutions to be strengthened. A point of vigilance: patching delays remain long. Our researchers analyzed 168 vulnerabilities within security products where patches were available over the last 12 months. Less than 19% of them were patched within 7 days and 56.8% of these available patches took between 31 and 180 days to be applied. More worryingly, 14% were still not implemented six months after being notified (page 36). Such delays can be exploited by attackers who will try to abuse every new vulnerability that is discovered.

2020: a more mature cyber ecosystem

Today's threats do not replace yesterday's ones but add to them.

A rise in the general level of maturity has been observed: employees are more attentive to cyber issues. They have become aware of how critical the digital world is to their work and personal lives, and are more vigilant.

---

[1] Traps affecting users, including phishing and identity theft

This maturity affects all actors in cyberspace, and therefore also cybercrime, which is becoming considerably more structured in 2020. Being a cybercriminal has become a profession, at least in its organization (pages 57 to 65). Cybercriminals are joining forces to form specialized groups, collaborating and forming an interconnected network. They organize themselves like the companies they target and use known practices: customer service, Malware-as-a-Service, etc.

The democratization of new technologies and their security

The pandemic has put remote access technologies in the spotlight. Overall demand for these solutions increased by 41% in the second half of March and remains 22% above pre-pandemic levels (page 49). The shift to home working demands a greater security for endpoints (PCs, tablets, mobiles, etc.). Since the beginning of the pandemic, endpoints have become a critical element, and we have recorded a 500% increase in our managed endpoint detection and response (EDR) customers.

The other notable trend, which goes hand in hand, is the boost in cloud adoption, which offers companies greater responsiveness, lower investment, and flexibility. This migration to the cloud will require special attention to data security and user identity (IAM, strong authentication...).

Business investment in security products

In 2020, organizations seem to have adopted three behaviors:

- A wait-and-see attitude, limiting their IT security projects because of the need to focus on business survival
- Reviewing their IT architecture and the foundations of their security, especially those whose activities were at a standstill (e.g. airport sector).
- Focusing on targeted actions, in particular on securing critical points (mainly endpoints and remote accesses).

In terms of investment, 2021 Industry Analyst forecasts seem to show continuous interest from organizations for managed services (outsourcing security, in whole or in part, to a service provider).

Volume per business relates to size

We have recorded around 101 confirmed incidents per business for Small organizations, (compared to 63 in 2019). For Medium-sized organizations, the median number of incidents is 77 (vs. 266 in 2019) and 278 for Large companies (vs. 463 in 2019).

A point to clarify: more incidents does not necessarily mean less security. As small businesses have "caught up" and invested more in detection technologies, they are seeing their alert volumes increase (page 21).

What about 2021?

5G, launched this year in many countries, will bring its share of new uses and accelerate the development of the technologies and products. Some of these will be at the heart of the Industry 4.0. and smart cities in particular. We also anticipate an even more marked development of security solutions for IoT and for Industrial environments, with the necessary alignment of IT and OT (Operational Technology) teams. Orange Cyberdefense,

notably via its Demo Center in Lyon (France) which will be inaugurated in 2021, is committed to be a pioneer in the growing OT security landscape.

The appetite for the cloud, but also the adoption of new forms of connectivity such as SD-WAN, will remain a priority for enterprises, bringing new uses and new risks to cover.

In a context where the cyber-threats ecosystem is becoming increasingly structured, businesses need to be prepared for the number of attacks to continue to increase. The COVID-19 pandemic has generated unprecedented disruptions to society and the economy. It has fundamentally transformed the way we work and do business. As we are already seeing, many of these changes are turning into lasting improvements and mindsets are evolving. There has been a sharp increase in demand for cloud, network, and video conferencing security – remote working is here to stay.

Finally, another lesson from the COVID-19 crisis: the value of proximity. Although tech-driven, cybersecurity remains, above all, a matter of trust.

To find out more, download the Security Navigator 2021:
https://orangecyberdefense.com/global/security-navigator/

Press contacts:
Nathalie Chevrier, nathalie.chevrier@orange.com, + 33 6 48 52 75 83
Caroline Cellier, caroline.cellier@orange.com, + 33 6 07 25 00 06