Number of cyberattacks against organizations increases by 13%, with noticeable rise in attacks targeting mobile devices

- Significant increase in cyber activity puts further strain on stretched IT teams of all business sizes, particularly for small-medium sized business, that lack dedicated security analysis resources
- Report also finds wave of vulnerabilities and attacks against mobile operating systems

Research from Orange Cyberdefense, Europe's largest managed security services provider, today reveals that there has been a 13% increase in cyberattacks on enterprises over the past 12 months, with a rise in ransomware incidents and, for the first time, a noticeable wave of attacks against mobile devices.

The Security Navigator 2022 provides a detailed analysis of more than 50 billion security events analyzed daily over the past year (October 2020 to October 2021) by Orange Cyberdefense's 18 Security Operation Centers (SOCs) and 14 CyberSOCs across the globe.

Monitoring showed that of the 94,806 incidents flagged as being potential threats, analyst investigation confirmed 34,156 (36%) to be legitimate security incidents – a 13% increase on the year before. More than a third (38%) of all confirmed security incidents were classified as malware, including ransomware – an increase of 18% on 2020.

The report found that almost two thirds (64%) of the security alerts dealt with by Orange Cyberdefense analysts turned out to be 'noise' and did not represent a genuine threat - an increase of 5% on the previous year. The findings suggest that many organizations, particularly small and medium sized businesses, will require more resources to filter this massive amount of data for potential threats. The risk is that these businesses will become increasingly vulnerable to attack as the level and volume of activity continues to rise.

The Security Navigator also reports that mobile operating systems like iOS and Android in a business context are an increasingly popular target for exploits. Many of the activities appear to be related to commercial companies contracted by law enforcement and intelligence agencies. However, the vulnerabilities and exploits developed will likely not stay in that realm, but have in the past and will likely in the future find their way into the criminal ecosystem as well (mind the WannaCry attack of 2017).

Orange Cyberdefense predicts attacks targeting mobile devices are likely to continue on this upward trajectory. This is a development that security professionals will need to pay closer attention to. Mobile platforms are key in modern access protection concepts, namely multi factor authentication (MFA), which is commonly used in corporate environments to protect cloud access for instance.

Another key finding of the new Security Navigator is that malware, including ransomware, was the most common type of threat reported across the analysis period, with 38% of all confirmed security incidents classified as malware - an increase of 18% on 2020. Among the key malware trends are:

- A decrease in confirmed downloader activity (malware that downloads and runs other malware on affected systems) in November and December 2020 after the Trickbot botnet was taken down by law enforcement, and in January and February 2021, directly after Emotet was taken down;
- An inverse correlation between the stringency of Covid-19 lockdowns and the volumes of downloader and ransomware activity: the more stringent the lockdowns, the less of this activity, running contrary to the prevailing narrative that attacks increase when users work from home;
- Large organizations see more than double (43%) the amount of confirmed malware incidents than medium-sized businesses.

Hugues Foulon, CEO of Orange Cyberdefense, said: "Attacks like Solorigate show that even trusted software from reliable vendors can turn into a trojan horse for cunning attackers. Technology alone cannot be the solution to this problem. As our data shows, we have seen a 13% increase in the number of incidents in just one year, and these incidents keep increasing year on year. A large proportion of the tech-driven security alerts that our analysts deal with are just noise but this puts a tremendous strain on already stretched IT and security teams. Indeed, not all businesses have the means or resources to employ managed security services providers to help them sift through the 'noise' and find the actionable security 'signals'. We thus believe that security technologies can, and must, do better."

Security Navigator 2022 includes:
- 100% first-hand information from the 18 global SOCs & 14 CyberSOCs of Orange Cyberdefense, the CERT, Epidemiology Labs, Penetration Testers, Researchers, and more
- 18 pages of CyberSOC statistics
- 12 pages of World Watch/CERT observations
- Pentesting and CSIRT stories: including a case of possibly state-backed hacking and a red-team exercise
- Security deep-dives into the criminology of ransomware and analysis of 3000+ leak threats across 67 distinct actors involved with cyber-extortion
- Security predictions: shifting to "happy investments" by addressing three key areas of security in a different way

Download Security Navigator 2022 here: https://orangecyberdefense.com/security-navigator/

Press contacts :
Emmanuel Gauthier ; +33 6 76 74 14 54 ; emmanuel2.gauthier@orange.com
Vanessa Clarke ; +44 7818 848 848 ; vanessa.clarke@orange.com