Cyberdefense

Press release

29 November 2023, 5:00PM GMT

Security Navigator 2024 reveals highest number of Cyber Extortion victims ever recorded, with an increase of 46% worldwide in 2023

- 129,395 detected incidents show a 30% increase YOY, resulting in 25,076 confirmed security incidents (19%).
- 37.45% of detected incidents originate from internal actors, whether deliberate or accidental.
- The VERIS 'Hacking' category remains in the top spot, account for almost a third of confirmed incidents (30.32%).
- Large enterprises (40%) are impacted the most by Cyber Extortion, followed by small organizations (25%) and medium-sized businesses (23%).
- New research finds a new levelling of physical and cyber battlefields, revealing a thin line between physical war and cyber (through hacktivism)
- Analysis of 2.5 million unique vulnerabilities reveals that majority (79%) are rated Medium or High, with nearly 1 in 10 critical (9.4%).

Security Navigator 2024 – Security incidents surge as testing teams work harder than ever

Orange Cyberdefense, the specialist arm of Orange dedicated to cybersecurity, launches today its annual security research report, the Security Navigator 2024. The report, which gathers, cross-references and analyzes data from a wide variety of sources*, paints a broad and complex picture of the world of cybersecurity, amplified by geopolitical, economic and social dimensions. With the environment more unstable and less predictable, it has become even more vital that organizations reduce their risk of exposure by understanding the threat landscape and how it can affect them.

The Security Navigator 2024 reveals that our Threat Detection teams processed 30% more events across the period, totalling to 129,395, of which 25,076 (19%) are confirmed security incidents. Of these, the threat action 'Hacking' remained the most prominent, accounting for almost a third of confirmed incidents (30.32%), followed by Misuse (16.61%) and Malware dropping to third (12.98%).

Whilst the volume of events has increased, the actual number of confirmed incidents decreased by 14% YOY. The Manufacturing sector (32.43%) is by far the largest contributor in terms of confirmed incidents, following the same pattern as past years. Retail Trade (21.73%) and Professional, Scientific and Technological Services (9.84%) completed the top three, responsible for over two thirds of the confirmed incidents we raised with clients.

As well as criminal opportunities, more and more threat actors are politically or ideologically motivated, with the aims of espionage, sabotage, disinformation and extortion increasingly intertwined. We report on the increase of Cyber Extortion (ransomware) victims worldwide, alongside a significant surge in Hacktivism linked to the war against Ukraine. Current geopolitical events have also politicized some Cyber Extortion actors, some of whom have become more politically driven.

2023 has seen the highest count of Cyber Extortion victims on record

The Cyber Extortion threat landscape continues to evolve quickly and the past 12 months saw the number of Cyber Extortion victims globally increase by 46%, marking the highest numbers ever recorded. Large enterprises were the victim in the majority of attacks (40%), with those employing more than 10,000+ people seeing a steady increase. This trend was exacerbated by a single threat actor, Cl0p, which exploited two major vulnerabilities in 2023. Small organizations make up a quarter (25%) of all the victims, closely followed by medium-sized businesses, with a share of 23%.

Large, English-speaking economies continue to account for the highest numbers of victims, with over half (53%) headquartered in the United States, followed by the United Kingdom (2nd, 6%) and Canada (3rd, 5%). However, we are starting to see a lateralization of the geographic distribution, illustrated by major YOY increases to victims in India (+97%), Oceania (+73%), and Africa (+70%).

During 2023, we found 25 Cyber Extortion groups had disappeared from 2022, 23 had survived from the previous year and there were 31 new groups we had never seen before. Of the Cyber Extortion groups that existed, over half (54%) had a life span of up to 6 months, 21% 7-12 months and 10% of all groups made it to the age of 13-18 months, highlighting the challenges faced by those attempting to disrupt a Cyber Extortion operation.

A new levelling of the physical and cyber battlefields, hacktivism as a powerful political tool

Over the past two years, there has been an evident increase of activity in the hacktivism space to support causes of a political or social nature. We report that attacks from hacktivist groups involved in the war against Ukraine, siding with either Russia or Ukraine, have reached record-high levels, with Ukraine, Poland and Sweden the most impacted by the pro-Russian hacktivists we track. This upwards trend is being exacerbated further by other geopolitical events which have sparked the creation of new groups, most recently spawned following the latest developments in the Middle East.

We report that Europe was impacted by 85% of all hacktivist attacks seen in 2023, followed by North America (7%) and the Middle East (3%). We observe that most of the over-attacked countries are geographically relatively close to the war against Ukraine.

Our research has shown a continuous evolution towards ‘cognitive’ attacks, which seek to shape perception through technical activity. The impact has less to do with the disruptive effect of the attack or the value of the data or systems that are affected (e.g., stolen, leaked or destroyed) but with the impact that these attacks will have on societal perception. Not only do we witness cyber events that impact the physical world; we also observe physical events that illicit a direct cyber response from threat actors, thus in turn causing an escalation of those very same geopolitical tensions.

Most of the hacktivist attacks that we are observing are Distributed-Denial-of-Service (DDoS) attacks. Some hacktivist groups have developed strong DDoS capabilities, while others are noisy about their capabilities and impact, applying a language and narrative that is disproportional to their actual action (and impact).

Hacking remains in the top spot, with nearly a third of incidents we detect within our CyberSOCs

Based on the VERIS[1] framework, the threat action ‘Hacking’ remains the most detected type of security incident, accounting for almost a third of confirmed incidents with 30.32%, a significant increase on the 25% on last year. ‘Malware’ has historically been one of the two most detected true positive incident types. However, this year it has slipped to 3rd place, with just 12.98%. 'Misuse’ was the 2nd most raised Threat Action with 16.61%, almost exactly in line with last year’s report. Incidents

[1] Actions (verisframework.org)

categorised as ‘Error’ (7.33%) again take 4th place followed by ‘Social’ (7.15%) which completes the top five.

The data found 37.45% of detected incidents within organizations originated from internal actors, with the majority coming from external actors (43.6%). Of these, the end user device was the most impacted asset (27.7%), followed by the server (27.34%).

The efficiency of mature, established clients can be four times higher than that of new clients

The CyberSOC teams have noted that there is a strong correlation between the detection efficiency of a client account, and the degree of feedback we get from the client. We observe this year that the efficiency of mature, established clients can be four times higher than that of new clients who are just starting their onboarding journey with us, and we argue that this client maturity is strongly expressed in the frequency with which we receive feedback on incidents.

We also show that while the ‘quantity’ of incidents we report to our clients has decreased proportionally over the years, the ‘quality’ has increased. This is apparent for “unknown events” which decrease from 15.33% for customers that have been onboard 1-10 months to 4.10% for customers that have been onboard for 41-50 months. We argue that this is a function of detection tuning, more rigorous analysis, and other service enhancements. In addition, as our clients mature in the service they improve their ability to act on the events we raise with them and refine the process of providing us with feedback. With sufficient feedback we are able to perform intelligent tuning and thereby improve detection efficiency, in a repeating cycle.

A trusted partnership to define and implement cybersecurity strategies to meet organizations’ needs

“This year’s report underlines the unpredictable environment we face today, and we see our teams working harder than ever as the number of detected incidents continues to increase (+30% YOY). Whilst we are seeing a surge in the number of large businesses impacted by Cyber Extortion (40%), small and medium businesses together are making up nearly half of all victims (48%)”, said Hugues Foulon, CEO, Orange Cyberdefense.

“Together, with our customers, we are pursuing an unwavering policy of awareness and support for our increasingly interconnected world. We are adapting to new technologies and preparing for new threat actors by continuing to anticipate, detect and contain attacks when they emerge,” Foulon concludes.

The full Security Navigator 2024 report can be downloaded HERE

*Appendix: Key data sets

The Security Navigator report uses Orange Cyberdefense’s visibility and analysis of the current cybersecurity landscape by over 3000 experts, 18 SOCs and 14 CyberSOCs across the world. It takes into consideration countries including France, Belgium, Netherlands, Denmark, Germany, Norway, Sweden, United Kingdom and South Africa, looking at data between October 2022 - September 2023. It uses proprietary data sources (CyberSOC, Vulnerability Operations Center, Penetration Testing, World Watch Intelligence Data, Cyber Extortion Data Leak Sites, Telegram Chat Logs) and external data third-party sources. See more details below:

CyberSOC analysis

A broad data set is collected from across all the operational teams within Orange Cyberdefense, including 14 CyberSOCs, responsible for supporting customers around the globe. This includes Managed Threat Detection Services data from 1st October 2022 to 30th September 2023 using the VERIS framework for incident classification.

Cyber Extortion

Since 2020, we recorded 8,948 victims of Cyber Extortion that have been publicly listed on a 'leak site' on the dark web. This is just a partial view on the whole problem of Cyber Extortion because we note the victims that have been exposed on the dedicated leak sites, meaning that they have already reached the end of the Cyber Extortion attack chain, and Threat Actors have determined that there is some value in making the purported compromise public. We are very aware that there is a high dark number of victims that we simply don't know of.

Penetration Testers

This year's Penetration Testing dataset includes reports from two teams which reviewed 296 anonymized Penetration Testing reports for the period October 2022 through September 2023. Assessments are typically focused on specific customer requirements and scopes within the bounds of certain project types such as Internal, External, Web Application, Mobile Application Security, Red Teaming, API assessment, Configuration Review, and more. These can vary in complexity and time allocation and may require multiple Ethical Hackers to perform. For the most part the client determines the scope and extent of testing required.

Vulnerability scanning

The Orange Cyberdefense Vulnerability Operations Center offers access to experts that can guide clients to achievable outcomes based on relevant current threats and how that stack up against the exposure and potential risks a client's environment might face. The dataset is representative of a subset of clients that subscribe to our vulnerability scanning services. Assets scanned include those reachable across the Internet, as well as those present on internal networks. The data include findings for network equipment, desktops, web servers, database servers, and even the odd document printer or scanning device.

World Watch Intelligence analysis

Our World Watch service published 491 advisories for the period October 2022 through September 2023 averaging over 40 advisories per month – a combination of new and updates on previously covered topics. At a high-level, World Watch covers vulnerabilities and threats.

Reported Operational Technology Cyberattacks

We analysed 35 years of OT cyberattacks and added further context by seeing how they stand up when compared to proposed types and categories. This leads us to some findings that spark questions about the future of OT cyberattacks and whether we'll see a shift in type or category in the medium to long term. We then conclude with an example of how we think OT cyberattacks may evolve in the future.

About Orange Cyberdefense

Orange Cyberdefense is the Orange Group entity dedicated to cybersecurity. It has 8,700 customers worldwide. As Europe's leading cybersecurity service provider, we strive to protect freedom and build a safer digital society. Our service capabilities draw their strength from research and intelligence, which allows us to offer our clients unparalleled knowledge of current and emerging threats. With more than 25 years of experience in the field of information security, 3,000 experts, 18 SOCs and 14 CyberSOCs spread around the world, we know how to address the global and local issues of our customers. We protect them across the entire threat lifecycle in more than 160 countries.

About Orange

Orange is one of the world's leading telecommunications operators with revenues of 43.5 billion euros in 2022 and 137,000 employees worldwide at 30 September 2023, including 73,000 employees in France. The Group has a total customer base of 296 million customers worldwide at 30 September 2023, including 251 million mobile customers and 25 million fixed broadband customers. The Group is present in 26 countries. Orange is also a leading provider of global IT and

telecommunication services to multinational companies under the brand Orange Business. In February 2023, the Group presented its strategic plan « Lead the Future », built on a new business model and guided by responsibility and efficiency. « Lead the Future » capitalizes on network excellence to reinforce Orange's leadership in service quality.

Orange is listed on Euronext Paris (symbol ORA) and on the New York Stock Exchange (symbol ORAN).
For more information on the internet and on your mobile: www.orange.com, www.orange-business.com/, and the Orange News app or to follow us on Twitter: @orangegrouppr.

Press contacts :

Emma Goodwin : +44 7746 515 781 ; emma.goodwin@orange.com