Press release
Paris, 25 November 2022, 3.00 PM CET

Security Navigator 2023 shows Cyber Extortion dominates landscape as 40% is malware, attackers target Europe and beyond, and SMEs, manufacturing and the public sector particularly exposed

- Companies of all sizes faced attacks, with malware representing 40% of CyberSOC (Detection and Response operation centers) incidents.
- 99,000+ investigations show an increase in incidents of +5% YoY; averaging 34 incidents per month/per customer – more than one security incident per day per organization.
- There is a clear shift in the geographical location of Cyber Extortion (Cy-X) victims. From 2021 to 2022 a decrease is observed in the number of victims from North America (-8% in the USA, -32% in Canada) offset by an increase in Europe (+18%) the UK (+21%), the Nordics (+138%) and East Asia (+44%).
- Small business[i] in particular dealt with malware incidents (49%). Manufacturing is the most impacted sector for Cyber-Extortion, and Public Administration deals mostly with incidents attributed to internal origins (66%).
- Almost half (47%) of all security incidents detected by our CyberSOCs originate from internal actors, whether deliberate or accidental.
- For the first time, Security Navigator 2023 includes anonymized, proprietary data on the patch levels of almost 5 million mobile devices, illustrating the differences between Android and iOS vulnerabilities landscape.

Security Navigator 2023 - Incident volumes continue to rise though pace has slowed

Orange Cyberdefense, the specialist arm of Orange Group dedicated to cybersecurity, has today launched its annual security research report, the **Security Navigator 2023**, available from 1st December. Amongst other things, this year's in-depth analysis examined 99,506 potential incidents that were investigated and triaged by our CyberSOC teams, an increase of 5% from the 2022 report. While this year's report shows encouraging signs that the pace of incidents is slowing, several factors are still a cause for global concern.

This year's report suggests that cyberbattles are being won in some areas. However, a plethora of challenges remain.

For example, our data shows that businesses are still taking 215 days to patch a reported vulnerability. Even for critical vulnerabilities, it generally takes more than 6 months to patch. Indeed, our ethical hacking teams report a 'Serious' (Critical or High) issue in almost 50% of all the tests they conduct.

We are seeing Cyber Extortion impact businesses of all sizes across the world. 82% of observed Cy-X victims were small businesses, an increase from the 78% we measured last year.

While some of our teams observed a marked slow-down in cybercrime during the onset of the Ukraine war, the intensity soon increased again. We see significant increases in Cyber Extortion also: over the last six months, for example, the number of Cy-X victims in East Asia and South East Asia grew by 30% and 33% respectively.

Cyber-extortion remains the dominant form of attack but victim location is clearly shifting from North America towards Europe, Asia and emerging markets

Ransomware and cyber extortion attacks continue to prove a major threat to organizations globally, and as such featured regularly in Orange Cyberdefense's World Watch threat advisories throughout the year. Notable spikes in news about ransomware occurred in March and April, resulting from Lapsus$ activity and Conti leak events, as well as concerns about the war on Ukraine.

Simultaneously, 40% of the incidents processed by our CyberSOCs involved Malware.

There is also a clear and visible geographical shift occurring, illustrated by Cy-X victim volumes decreasing by 8% in North America and 32% in Canada, but increasing in Europe, Asia and emerging markets. From 2021 to 2022 victim volumes increased in the European Union by 18%, in the UK by 21%, and by 138% in the Nordics. East Asia saw an increase of 44% and Latin America 21%.

We also observe dramatic shifts in the makeup of active criminal groups. From the top 20 actors observed in 2021, 14 are no longer in the top 20 in 2022. After Conti disbanded in Q2 2022, we observed Lockbit2 and Lockbit3 become the biggest Cyber Extortion actors in 2022 with over 900 victims combined.

We also note that these actors strike opportunistically. Almost 90% of all the actors we tracked claimed victims in the USA for example. More than 50% hit the UK. More than 20% of actors even hit Japan – a country with one of the smallest numbers of observed victims in our dataset.

Impact of the war in Ukraine

It is worth highlighting that during the first weeks of the war against Ukraine, we observed a decrease of up to 50% in cybercriminal activities targeting Polish clients, apparently due to criminals being distracted by the war and needing to regroup. However, activity returned to normal after a few weeks.

SMEs, manufacturing and public sector particularly vulnerable

Small-to-medium sized businesses

We report about 4.5x more small businesses falling victim to Cyber Extortion than Medium and Large businesses combined. As a proportion, however, Large businesses are still being impacted much more heavily.

Small-to-medium sized businesses are especially forced to deal with malware incidents, reflected in the 49% of confirmed incidents for this group this year (compared to 10% in 2019, 24% in 2020 and 35% in 2021). With average data breach costs estimated at $1.9 million for businesses with less than 500 employees[ii], SMEs may face the risk of going under due to these breaches.

Public Sector organizations

On a normalized basis, Public Sector contributes the 5th highest portion of incidents our CyberSOCs deal with. This sector also records the largest proportion of Social Engineering incidents in our dataset.

For most industries the majority of incidents we detect are triggered internally, but for our clients in Healthcare we attributed an astonishing 76% of incidents to external actors like criminal hackers and APTs (state-backed threat actor groups).

Manufacturing industry remains the most impacted industry in terms of victim count

The manufacturing sector remains the number one industry in terms of for Cyber Extortion (Cy-X) victim count, though our research shows it to rank only 5th amongst industries most willing to pay ransoms. We report that criminals are compromising 'conventional' IT systems, rather than the more specialized Operational Technology, and attribute this high number of victims primarily to poor IT vulnerability management. Indeed, our data shows that businesses in this sector take an average of 232 days to patch reported vulnerabilities. On this metric, only four other industries ranked worse than Manufacturing.

Critical vulnerabilities persist and delays in patching threaten security

Drawing on a brand-new dataset of vulnerability insights, researchers identified a concerning persistence of serious vulnerabilities on business IT systems, with 47% of confirmed vulnerabilities identified as 'critical' or 'high' severity. Critical vulnerabilities still took organizations more than half a year (184 days) to patch. Other vulnerabilities can persist for much longer, with data suggesting that many vulnerabilities, even critical, will never be patched.

IT vulnerabilities in manufacturing took an average of 235 days to be patched versus an average 215 days across all other sectors. In hospitals (within the Healthcare and Social Assistance Sector), IT vulnerabilities took an average of 491 days to patch. In the transportation sector, patches took an average 473 days.

The average time taken by our ethical hackers to discover a confirmed Serious (High or Critical) Finding was 7.7 days.

The human dilemma - Insider threat incidents outnumber external attacks across most industries while cybersecurity vacancies go unfilled

Organizations' employees remain at the frontline of a company's defense but can also represent their weakest link. For example, our report showed that:

- For the public administration, most incidents we dealt with were attributed to internal sources, whether deliberate or accidental.
- For our manufacturing clients, 58% of the incidents dealt with were classified as originating internally. For our "transportation and Warehousing" customers, the level is even higher - 64% of the incidents have their origins internally.

Our report enumerates how higher levels of security monitoring improve the efficacy of controls, but also generate more false positives and may result in more strain on security professionals. This in an industry struggling to fill over 300,000 cybersecurity job vacancies in EMEA alone[iii].

Mobile security: iOS vs Android

For the first time, Security Navigator 2023 includes proprietary data on the patch levels of almost 5 million mobile devices that we interacted with between September 2021 and September 2022. Third party research suggests that in 2021 both iOS and Android dealt with their fair share of vulnerabilities with 547 vulnerabilities reported for Android and 357 for iOS. 79% of Android Vulnerabilities were considered to have a low attack complexity (trivial for actors to exploit) compared with just 24% for iOS. 45 iOS vulnerabilities received a critical CVSS score compared to just 18 on Android.[iv]

The Navigator report examines serious vulnerabilities in both Apple and Android to determine how long it takes the ecosystem to deploy the required patch. In one iOS case we determine that it took 224 days for 90% of the Apple ecosystem to upgrade to the patched version. For both Android and iOS it appears that about 10% of the user base will never be properly patched.

Findings show that a higher proportion of iPhone users are at risk of being vulnerable when a security issue is first disclosed, due to the homogeneous nature of the ecosystem. Users migrate to a new version quickly, however, with 70% updating within 51 days of the patch being released. The more fractured nature of the Android ecosystem means that devices are often left vulnerable to more old exploits, while fewer may be vulnerable to new exploits.

"The last few months were particularly dense in terms of macroenvironmental events, nevertheless the cybersecurity ecosystem emerges more vigilant and united as a result. Cyberattacks are making headlines, and the war in Ukraine is a resounding reminder that our digitized world is also the field of virtual battles." said Hugues Foulon, CEO, Orange Cyberdefense.

"The encouraging overall slowdown in the number of incidents for our most mature customers (+5% compared to +13% the previous year) shows that we are able to win battles against malicious actors. However, these successes should not slow down our efforts in the fight against cybercrime. This year's results highlight the challenges faced by organizations of all sizes. Threats are evolving, becoming more complex, coming from all directions and underlining the importance of the work we will continue to do to adapt to the threat and support our customers in this fight," he concluded.

Security Navigator 2023 includes:

- 100% first-hand analysis by 2,700 experts spread across the world and Orange Cyberdefense's 17 SOCs, 13 CyberSOCs and CERT in 8 locations
- 28 pages of CyberSOC statistics
- Detailed analysis of the cyber warfare landscape and the cyber impact of the Ukraine crisis
- Brand new datasets from the VOC and penetration testing services, analyzing the scope and shape of vulnerabilities affecting organizations across industries
- Spotlight investigation into the threats and vulnerabilities impacting the manufacturing sector
- Brand new data into mobile security threats and vulnerabilities

Press can request the report in advance by contacting press.office@orange.com

About Orange Cyberdefense

Orange Cyberdefense is the Orange Group entity dedicated to cybersecurity. It has 8,500 customers worldwide. As Europe's leading cybersecurity service provider, we strive to protect freedom and build a safer digital society. Our services capabilities draw their strength from research and intelligence, which allows us to offer our clients unparalleled knowledge of current and emerging threats. With 25 years of experience in the field of information security, more than 2,700 experts, 17 SOCs and 13 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 sales of 42.5 billion euros in 2021 and 136,500 employees worldwide at 30 September 2022, including 75,000 employees in France. The Group has a total customer base of 286 million customers worldwide at 30 September 2022, including 240 million mobile customers and 24 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 Services. In December 2019, the Group presented its "Engage 2025" strategic plan, which, guided by social and environmental accountability, aims to reinvent its operator model. While accelerating in growth areas and placing data and AI at the heart of its innovation model, the Group will be an attractive and responsible employer, adapted to emerging professions.

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
Vanessa Clarke ; +44 7818 848 848 ; vanessa.clarke@orange.com

---

[i] Small business defined by Orange Cyberdefense are business with under 1000 employees
[ii] Ponemon institute 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses 2019
[iii] 2022 (ISC) Cybersecurity Workforce Study https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx
[iv] https://securityaffairs.co/wordpress/127240/hacking/apple-fixed-two-zero-day-2022.html
https://www.humansecurity.com/learn/blog/poseidons-offspring-charybdis-and-scylla
https://www.bleepingcomputer.com/news/security/2021-mobile-security-android-more-vulnerabilities-ios-more-zero-days/
https://about.fb.com/news/2022/10/protecting-people-from-malicious-account-compromise-apps/