Cyberdefense

Press release
5th December 2024 / 8.00 AM GMT

Security Navigator 2025 reveals Europe as top target for hacktivism, with groups shifting focus to cognitive warfare

- One pro-Russian hacktivist group claimed over 6,600 attacks since March 2022, with 96% targeting Europe countries, and attackers focusing on influencing public perception and trust over direct technical disruptions.
- Hacktivists were responsible for 23% of sophisticated “category 2” attacks that directly target OT. 46% of these attacks resulted in “manipulation of control” as an impact.
- Small businesses have seen a 53% YoY increase in cyber extortion (Cy-X) incidents, with medium-sized businesses close behind with a rise of 52%.
- AI has a dual role in cybersecurity, enhancing threat detection while being actively exploited within social engineering attacks. GenAI software vulnerabilities also pose significant risks.

Security Navigator 2025 – Cybersecurity landscape in Europe at a critical juncture

Orange Cyberdefense, the specialist business unit of Orange dedicated to cybersecurity and leader in cybersecurity services in Europe, today launches its sixth annual international and multi-industry investigative research, the *Security Navigator 2025*. It uses extensive data analysis to provide a detailed view of the cybersecurity landscape, shaped by geopolitical conflict and the increasing sophistication of threat actors. As threats to critical infrastructure and public trust continue to evolve, the report emphasises the need for European organizations to strengthen their defences against a rising tide of politically motivated cyber-attacks.

The *Security Navigator 2025* reveals that one prominent pro-Russian hacktivist group targeted Europe – primarily Ukraine, Czech Republic, Spain, Poland, and Italy – with 96% of their attacks, marking the region as their primary focus. The report also shows that Europe is the second most impacted region by Cy-X, with victim numbers increasing by 18% YoY. The most affected European countries are Italy (19%), Germany (19%), France (16%), Spain (13%) and Belgium (8%). In the Nordics, Cy-X activity has grown at a rapid pace, with a 38% increase in victim counts.

The report notes that this audacious pro-Russian hacktivist group, which is one of the most active, has conducted over 6,600 attacks since early 2022, mostly targeting symbolically

important European entities. Hacktivist groups are increasingly recognizing the power of cognitive attacks, skilfully using technical disruptions not only to create direct impact, but to manipulate public opinion, undermine trust in institutions, and destabilize societal confidence. By attacking election-related systems and other symbolic institutions, these groups aim to draw attention to the political and economic issues they consider important, creating fear, uncertainty and doubt. This strategic shift shows how modern hacktivists target perception as much as infrastructure, posing a unique challenge for organizations tasked with protecting both physical assets and public trust.

Despite hacktivism focusing on Europe, North America is not unscathed in this year's report. North America, dominated by the US, was the most impacted region globally by cyber extortion, with a 25% YOY increase in cases. The US also experienced the highest concentration of targeted OT attacks, accounting for 49% of all incidents. This trend reinforces the region's position as a top target for financially motivated threat actors but leads to questions about why hacktivists are avoiding it . The *Security Navigator 2025* surmises that this may be because they fear repercussions from the nation.

Hacktivists Extend Reach to Operational Technology Systems

Another emerging concern is hacktivist activity targeting OT systems, critical for operating essential infrastructure in the manufacturing, energy, healthcare and transportation sectors. The Security Navigator 2025 attributes nearly 1 in 4 (23%) of sophisticated attacks targeting OT to hacktivists. As such attacks have typically been associated with state actors, the growth of hacktivism reveals a new level of sophistication and risk to critical infrastructure.

46% of OT cyber-attacks resulted in 'manipulation of control,' which means that the adversary managed to manipulate the physical process. The utilities sector has been heavily affected, with the report finding that it suffered 46% of attacks that directly targeted OT systems. This highlights the continued vulnerability of OT systems to politically motivated cyber-operations.

Hugues Foulon, CEO of Orange Cyberdefense, stated, *"Cyber threats have become a critical barometer for anticipating global geopolitical tensions. The insights generated by our cyber teams provide a fresh and robust perspective on international disruptions and their operational impacts on society*.

"The Security Navigator 2025 underscores an urgent need for coordinated defensive strategies across Europe and beyond, including enhanced incident response measures, strengthened OT protections, and proactive monitoring of public channels to counter the unique blend of cyber extortion, hacktivism, and cognitive warfare facing European organizations," said Foulon.

Cyber Extortion's Rising Toll on Small and Medium Businesses

The report highlights a worrying increase in cyber extortion impacting SMBs, with a 53% YOY rise in incidents targeting small businesses. The compounding effect of 'revictimization' – where stolen data is reused in multiple extortion campaigns – further amplifies these organizations' financial and psychological toll. SMBs now account for over two-thirds of all observed cyber extortion victims.

Critically, SMB cyber security may also impact large organizations as the first are often part of their supply chain. An incident at a small player can lead to a cascade of disruptions throughout the chain.

The *Security Navigator 2025* also suggests that the traditional approaches to 'vulnerability management' are no longer fit for purpose, due to the large number of vulnerabilities security teams must handle, which takes them away from more meaningful work that would prevent a successful attack. This is especially true for smaller SMB teams.

Increased Aggression Against Healthcare and Beyond

As cyber extortion continues to increase globally, the report notes that it's also becoming increasingly 'cynical.' This year, there has been a 50% YOY increase in attacks targeting the Health Care and Social Assistance sector, ranking it as the fourth most impacted industry. Subsectors such as Ambulatory Health Care and Hospitals are now being frequently targeted, which points to a further erosion of the 'moral' restraints that previously protected these sectors.

Other sectors have also experienced a marked rise in Cy-X attacks this year. The top three most impacted industries have all seen significant increases: +25% for Manufacturing, +20% for Professional, Scientific, and Technical Services, and +65% for Wholesale Trade.

AI: A Double-Edged Sword in Cybersecurity

The *Security Navigator 2025* highlights AI as a powerful yet complex tool, with both defensive and offensive cybersecurity applications reshaping threat dynamics. Threat actors, including state-sponsored actors from countries such as China, Russia and Iran, are leveraging GenAI to create realistic phishing content, fake images and deepfakes to deceive large audiences, which is supporting their deployment of 'cognitive attacks.'

On the defensive side, the report found that AI is beneficial for detecting hard-to-identify threats. AI-driven systems have improved detection rates for advanced threats like 'beaconing' – a tactic where malware sends subtle, periodic signals to command-and-control servers – reducing incident response times by up to 30% as organizations use AI to identify and intercept these signals before damage can escalate. However, the report also warns about vulnerabilities in GenAI solutions and urges business to implement strict

access rights to sensitive data and systems, ensure isolation between tenants, and educate users about the risk of data leaks in prompts.

Charl van der Walt, Head of Security Research at Orange Cyberdefense, said, *"The story in this year's report is far bigger than statistics and technical details. It shines a light on a growing cynicism in the threat landscape as different threat actors seem less concerned about the potential of causing harm, and may even be more intent on inflicting it than ever before."*

About the Security Navigator

The Security Navigator is an international and multi-industry investigative research and a strategic guide to understanding changes in the cyber threat landscape and sharing recommendations for anticipating, responding to attacks and building the resilience of our societies.

For its sixth edition in a row, it draws on the intelligence capabilities of Orange Cyberdefense, its Cyber Threat Intelligence.

It brings together research and data from across more than 135,000 security events in 160 countries, 1,300 000 security vulnerabilities managed and 13,308 investigated cases of cyber-extortion since 2020, including 4,200 in the last 12 months. In addition, the data comes out of our 32 operational security centres and epidemiological labs around the globe, where Orange Cyberdefense's researchers have uncovered a year's worth of cybercrime activities, including the activities of a pro-eminent hacktivist group.

The Security Navigator goes to the heart of attacks - from the dark web and cybercriminal activities to hacktivist operations - and decrypts the mechanisms of cybercrime, while providing concrete solutions to improve threat detection, risk analysis and post-attack recovery capacity.

The Security Navigator combines rigorous analysis of first-hand global cyber research data with expert advice and actionable recommendations to guide public and private decision-makers through an ever-changing threat landscape.

It is a strategic and operational watch shared with the worldwide community, designed to strengthen the resilience of organisations and respond to today's geopolitical and economic challenges.

Security Navigator 2025 is more than just a snapshot of the threats.

It provides practical tools for action: methods for detecting attacks in their early stages, assessing their impact and organising a coordinated and effective response.

By combining expertise and in-depth threat analysis with actionable recommendations, it enables organisations to strengthen their resilience in the face of cyber-risks, while anticipating tomorrow's challenges.

The full Security Navigator 2025 report can be downloaded here :
https://www.orangecyberdefense.com/global/security-navigator

About Orange Cyberdefense

Orange Cyberdefense is the Orange Group entity dedicated to cybersecurity. It protects the entire threat lifecycle of 9,000 large companies. As Europe's leading cybersecurity services provider, **we aim to be the trusted cyber partner committed to creating value for all by delivering the safest digital space**. 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 30 years of experience in the field of information security, 3,000 multi-disciplinary experts and 36 detection centers spread around the world, we know how to address the global and local issues of our customers. Cybersecurity is a human journey, so we build a safer digital society by placing people at the core of our actions.

About Orange

Orange is one of the world's leading telecommunications operators with revenues of 39.7 billion euros in 2023 and 128,000 employees worldwide at 30 September 2024, including 71,000 employees in France. The Group has a total customer base of 292 million customers worldwide at 30 September 2024, including 253 million mobile customers and 22 million fixed broadband customers. These figures have been restated to account for the deconsolidation of certain activities in Spain following the creation of MASORANGE. The Group is present in 26 countries (including non-consolidated 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).
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 X: @orangegrouppr.