Cyberdefense

Press release
3 July 2024, 10AM CET

Cyber Extortion victims grow by a record 77%, with small businesses impacted 4X more often than medium and large businesses combined, reveals Orange Cyberdefense

- Over the last 12 months, 60 distinct threat actors impacted 4,374 new victims.
- Cyber extortion is a worldwide issue with businesses in 75% of all countries directly impacted since 2020, and 118 countries impacted in the last year alone.
- The healthcare and social assistance industry increasingly becoming a victim, experiencing the highest growth (+160% YOY).
- The impact GenAI may have on the cyber extortion threat is yet to be seen, concerns that it will enable the threat ecosystem to globalize.

Orange Cyberdefense, the specialist arm of Orange Group dedicated to cybersecurity, has today released its latest cyber extortion report, Cy-Xplorer 2024. Examining data from a total of 11,244 confirmed business victims, the findings show a steep increase (77% YOY) in the number of observable cyber extortion (Cy-X) victims over the past 12 months, with analysis suggesting the actual number to be 50-60% higher than what we directly observe, due to the dynamic and ever-changing nature of the cyber extortion ecosystem.

Majority of victims in predominantly English-speaking countries that dominate world economy

Cy-X is continuing to spread across the globe with victims recorded in 75% of countries since 2020. The USA, Canada, and the Great Britain have consistently recorded the highest number of victims, indicating that economic size, language, and business "culture" are key factors shaping the regional demographics of our victim dataset. Aside from being the most impacted region, the USA has also seen the fastest growth at 108%, followed closely by Great Britain and Canada at 96% and 76%, respectively. Other prominent growth regions included the Nordics and Africa, with growth rates of 78% and 100%, although off much lower starting bases.

Attackers "harvesting" victims, with patterns of opportunistic targeting

Whilst the term "big game hunting" is often seen in reference to targeted and sophisticated attacks against large, high-value targets, we have observed patterns of behaviours that suggest a much more opportunistic approach for most threat groups when it comes to Cy-X. As a result, we have observed that small businesses with less than 1,000 employees are 4.2X more likely to be impacted by Cy-X than medium and large businesses. We suggest that this is simply because there are so many more small businesses that get swept up in the "harvest" as attackers attempt to hit whoever they can.

Healthcare victims reveal a “moral tipping point” for attackers

Businesses in the manufacturing industry continued to be the most impacted globally by Cy-X (21%). However, in the past 12 months, for the first time, we saw healthcare and social assistance industries join the three most impacted sectors, seeing the highest growth rate at 160% YOY. Historically, through the COVID-19 crisis, and up until recently threat actors have shown some degree of "moral restraint," with healthcare being an industry that attackers explicitly avoided due to their moral compass and fear of political consequences. However, it appears to suggest that even this fragile political finesse is fading as this worrisome trend picks up pace. For instance, LockBit took credit for compromising two significant US healthcare institutions -Carthage Area Hospital and Claxton-Hepburn Medical Center, amongst others, and the ALPHV/BlackCat group, claimed a significant attack on Change Healthcare. There are further examples in the full report.

Re-victimization emerging as a new trend, exacerbated by the major increase in victim count

Our research has found over 200 occurrences of revictimization, which has been on an upward trajectory since 2023 and appears to be accelerating. In Q1 2024 there have already been 39 re-victimizations and this trend is expected to continue, with our research finding some victims posted up to three times on a Dedicated Leak Site. Additionally, there are incidents of victims being posted by different threat actors with a long delay between them, indicating an active attempt to re-attack and extort victims anew.

GenAI is a red herring as cyber threats evolve beyond social engineering and phishing

Our data suggests that AI is not significantly impacting Cy-X. The concerns for GenAI are instead that it could allow the threat ecosystem to globalize – by providing the language and cultural tools attackers need to reach across language and cultural barriers that have, until now, potentially shielded some economies from greater impacts.

Threat groups and ‘action’ by law enforcement

Despite the takedown and disruption of prominent cyber extortion groups such as RagnarLocker, ALPHV/BlackCat, and LockBit by law enforcement, there has been no noticeable decrease in victim count. The research has shown the general volatility of the Cy-X actor ecosystem, showing one-third of all actors we track will “disappear” each year, while an equivalent number of new actors are identified annually. It also suggests half of all identified threat actors will disband or rebrand in under 6 months.

“We are seeing a measured rise in the pace at which Law Enforcement is responding to meet the Cy-X threat but as victim numbers surge at an alarming rate, with new tactics being deployed and moral restraints dwindling, it’s an ongoing battle that’s further complicated by the decentralized and fragmented ecosystem”, said **Hugues Foulon, CEO at Orange Cyberdefense**. “Small businesses are increasingly falling victim to the crime and we see a real need for all organizations to join forces and play their part by working together and taking actions that will increase the cost for attackers.”

“The emergence and acceleration of re-victimization is a concerning trend that we are following closely. Whilst perceived as an unsophisticated crime, the impact is profound and exposes organizations to several forms of harm as they remain in the grip of the

criminal ecosystem," said **Diana Selck-Paulsson, Lead Security Researcher at Orange Cyberdefense**. "Cybercrime is borderless and as threats continue to evolve alongside the emergence of new technologies such as GenAI, we must continue to adapt and be prepared for the globalisation of the threat ecosystem".

Orange Cyberdefense has been consistently tracking cyber extortion activity since 2020 and has collected information on over 11,200 victims to date. The full methodology can be found in the report here

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.
https://www.orangecyberdefense.com/

About Orange

Orange is one of the world's leading telecommunications operators with revenues of 39.7 billion euros in 2023 and 129,500 employees worldwide at 31 March 2024, including 72,500 employees in France. The Group has a total customer base of 282 million customers worldwide at 31 March 2024, including 243 million mobile customers and 21 million fixed broadband customers. 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) 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 X: @orangegrouppr.

Press Contact : Emma Goodwin – **emma.goodwin@orange.com** - +44 7746515781