Press release
Paris, June 7th 2023

Cyber Extortion activity reached the highest volume ever recorded in Q1 2023 after a decline of 8% in 2022, reveals new Orange Cyberdefense report

- The shift previously observed in the geographical location of cyber extortion (Cy-X) victims continues to accelerate, moving from the United States (-21%), and Canada (-28%) to Southeast Asia region (+42%), the Nordics (+40%) & Latin America (+32%).
- Whilst Manufacturing continues to be the biggest industry impacted, the number of victims decreased (-39%), with a shift towards the Utilities sector (+51%), Educational Services (+41%) and Finance and Insurance Sectors (+11%).
- Businesses in 96 different countries were impacted by Cy-X in 2022, equating to nearly half (49%) the countries in the world. Since 2020 Orange Cyberdefense has recorded victims in over 70% of all countries worldwide
- Over 2,100 organizations in the world were publicly shamed as a victim of Cy-X in 2022, across an almost even distribution of business sizes.

Orange Cyberdefense, the specialist arm of Orange Group dedicated to cybersecurity, has today released a new report, Cy-Xplorer 2023, in which it provides a detailed analysis of Cyber Extortion (Cy-X) activity during 2022. Examining data from a total of 6,707 confirmed business victims, the findings show a fluctuation in the number of victims across different countries and industries, with attacks expanding to new regions. While the data shows a decrease of Cy-X victims (8%) in 2022, this reduction is short lived as the latest data shows the largest volumes to date in Q1 2023.

As Cy-X attacks continue to rise, the report suggests that 2022 was the year of 'distraction' and rebranding for some of the major Cy-X operations Orange Cyberdefense is monitoring.

Incident volumes spike as Cy-X activity broadens to impact previously unaffected countries

The geographical shift of Cy-X attacks has continued, as previously noted in the Security Navigator 2023, with a significant year on year increase (42%) in Southeast Asia, with Indonesia, Singapore, Thailand, Philippines, and Malaysia the most impacted. Simultaneously we have seen a decrease in victims in regions such as North America and Europe.

Previously we observed that countries are mostly targeted opportunistically, and the number of victims depends primarily on the number of organizations registered in a country. However, this general trend is changing as bigger western countries respond actively to the threat, and threat actors are forced to seek out new hunting grounds. As such, threat actors are focusing on regions where the level of risk seems lower for them, which could partly be due to a lack of proactivity from local governments.

The war in Ukraine has disrupted the Cy-X ecosystem as much as other areas in cyberspace

The data from the report shows that the war has had a noticeable impact on Cy-X, slowing down activities and causing threat actors to regroup before continuing their attacks.

Geopolitical tensions resulting from the Ukraine war has seen many countries firmly shifting their allegiance to one side or the other in the conflict, creating expectations that Cy-X patterns would follow suite. Indeed, our findings show that in 2022, 74% of all victims were from NATO countries. However, Cy-X impacting NATO countries decreased noticeably at the start of the war and continued to decrease as the war progressed. Activity during this time from pro-Russian threat actors did not result in a proportional increase in Cy-X victims among NATO member countries.

We observed a dramatic shift in Q1 2023 and especially March 2023, which shows a different trend, illustrated by the spike in threat actor activity. Whether this is going to continue is difficult to foresee.

Whilst we expected to see more organizations from NATO-member countries being impacted, we observed exactly the opposite. Non-NATO countries from regions such as Latin America (+32%), and Southeast Asia saw an uptick in victim numbers instead. How this is influenced by the political situation of the Ukraine war is not entirely clear, but it can be said with some confidence that the war has not spawned an increase in Cy-X incidents for NATO member countries so far as fewer are being impacted over time.

Threat actors changing tactics – moving from manufacturing to utilities and education

In 2022 manufacturing was the biggest industry impacted, with roughly one fifth of all victims within this industry. However, in 2022 we observed a decrease of 39% for the manufacturing sector, with the second half of 2022 showing a noticeably lower number of victims. One reason for this sharp decline is most likely the closure of the Conti group's criminal activities.

The educational sector has suffered much more in 2022 when compared to the year before, with an increase of 41%. And particularly at the hands of the Vice Society group. We saw an average of 10 organizations per month from this sector being publicly exposed on the dark web, with the top five countries impacted being the US, UK, Spain, France and Australia.

We also observe that the utilities sector saw an increase of 51%, but the actual numbers of observed victims in 2022 remained low (35 victims).

The report also highlights how the financial sector has seen an increase of Cy-X attacks, (+11%) with over 130 Financial Institutions becoming victims of Cy-X. 75% of all victims have under 1,000 employees.

With regards to business size, in 2022, we saw large organizations impacted the most, representing 36% of all victims, but small and medium organizations were not far behind. We recorded that 30% of all victims were small organizations, while medium-sized businesses made up 24%.

Attempts to disrupt Cy-X, an increased number of law enforcement activities

As a result of consistently high-impact attacks, governments worldwide are starting to take more action. Some forbid companies operating within their country to pay a ransom when demanded. In the USA, Australia and elsewhere, authorities have made several official statements condemning foreign threat actors. While still on the backfoot, law enforcement is catching up, increasingly disrupting threat actors' activities.

We also see positive developments in that law enforcement agencies and governments are taking action to disrupt this ecosystem through criminals' arrests, infrastructure takedowns, money seizures, international sanctions, development of decryptors for victims and 'hack back' activities.

"Whilst 2022 witnessed a slowdown in the growth of attacks, we can see from Q1 that it's not the time to become complacent. Our research shows that industry and government collaboration is the key to driving down malicious cyber activity, as Cy-X is not a problem that businesses can solve on their own. We are yet to see the true impact of geopolitical events such as the Ukraine war in cyberspace, but increased initiatives being put in place at a government level are essential if we are to tackle the ever-present risks posed by threat actors", says **Hugues Foulon, CEO at Orange Cyberdefense.**

"Despite the increase in victim numbers in the first quarter of 2023, there is hope that the continuous efforts to combat the Cy-X threat can yield more positive outcomes and victories this year. But to achieve this, we must pull together as an industry and keep sharing information about threats and attacks," said **Charl van der Walt, Head of Security Research at Orange Cyberdefense.** "We are seeing significant changes and trends in terms of victim distribution across countries and industries and we believe collaboration between the public and private sectors can be improved to demonstrate a united front in combating this type of crime.

Orange Cyberdefense has been consistently tracking cyber extortion activity since 2020 and has collected information on over 6500 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 services capabilities draw their strength from research and intelligence, which allows us to offer our clients unparalleled knowledge of current and emerging threats. With more of 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://orangecyberdefense.com/global/

https://twitter.com/orangecyberdef

About Orange

Orange is one of the world's leading telecommunications operators with revenues of 43.5 billion euros in 2022 and 136,000 employees worldwide at 31 March 2023, including 74,000 employees in France. The Group has a total customer base of 288 million customers worldwide at 31 March 2023, including 243 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. 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.

Orange and any other Orange product or service names included in this material are trademarks of Orange or Orange Brand Services Limited.

Press contacts :

Emma Goodwin : +44 7746 515 781 ; emma.goodwin@orange.com
Vanessa Clarke ; +44 7818 848 848 ; vanessa.clarke@orange.com