PRESS RELEASE

CYBERSECURITY: FROM COVID TO THE RUSSIA-UKRAINE CONFLICT, IT THREATS HAVE INCREASED IN 2022

According to the Exprivia CyberSecurity Observatory, the first quarter of the year in Italy saw worse figures compared to 2021. In March, there was a peak in damage associated with the international crisis: fake news on the conflict and humanitarian aid campaigns is serving as a new avenue for criminal activities.

5 May 2022. From the pandemic to the military conflict, a new and alarming leap in the phenomena of crimes perpetrated on the internet in the first quarter of 2022, the worst in the last two years. This has been brought to light by the latest Cyber Threats **Report from the Exprivia Cybersecurity Observatory which**, between January and March, recorded 806 cases in Italy **including attacks, incidents and privacy violations**, a sharp increase compared to the average of the previous quarters.

Specifically, approximately **78% more cases were observed compared to the last quarter of 2021** (when 454 phenomena occurred), with 213 events in January, 207 in February and 386 in March, the month with the greatest impact in which criminals exploited the situation of international instability especially linked to the war between Russia and Ukraine. According to the Exprivia Observatory, which takes 113 public sources into consideration, in these first few months of 2022, besides online banking and purchases, which led the rankings, the Russian-Ukrainian war emerged **as an opportunity to target victims**, with frequent deception concealed behind fake news about the conflict or fake humanitarian aid campaigns.
The Report shows that between January and March there were **408 attacks, 379 security incidents** (successful attacks), **and 19 privacy violations**. The ratio between incidents and cyber attacks has therefore continued to increase rapidly, fuelling the perception that, despite investment in security in recent years, the number of hackers is rising and they are increasingly effective, causing damage mainly linked to the **theft of data** and **money**.

"In the past two years, events with a high political and economic impact and related social tensions have allowed criminals to exploit opportunities such as Covid or, recently, the conflict between Russia and Ukraine to deceive victims, in most cases for profit," comments **Domenico Raguseo, Cybersecurity Director for Exprivia**. *"In the immense digital ecosystem that we inhabit, it is not easy to pinpoint the causes and geographical origins of cybercrime; if an attack is developed for a designated victim, it could also affect others, and if a malware is used for a specific purpose, it could*

soon become the property of other criminals who will use it for different purposes. As such, at the moment we are also experiencing the first harm caused by the military conflict online, and in the coming months the consequences could be even more severe."

According to the Exprivia Observatory, in the first quarter of 2022 the **Finance** industry – which includes banking institutions, insurance companies, cryptocurrency platforms – was the one to experience the highest amount of criminal phenomena (**286** cases, over a third of the total), with a peak of 161 cases in March alone, including credit card data theft, access to bank accounts and requests for money. This was followed by the **Public Administration**, with **109** cases including attacks, incidents and privacy violations, more than **tripling compared to the cases experienced in the last quarter of 2021**. In third place, with **91 cases, was the Software/Hardware sector**. This includes companies in ICT, digital services, e-commerce platforms, device and operating systems, which mainly fall prey to theft of data, such as access credentials or sensitive information. The report showed a jump in cases in March, with a **figure more than double that of January and February**.

"Cybercrime reporting on the sources analysed in our Report is growing, including as a result of the increased critical nature of the digital services on which we depend. The greater the impact and duration of the incident or simply of the attack, the less likely it will go unnoticed," observes Raguseo. *"Even in mass media, the visibility and relevance of cybercrime have been increasing in tandem with the new vulnerabilities exploited by criminals."*

Among the techniques most used by cybercriminals is **phishing**, a method of luring victims through deceptive emails or through social networks, **with 389 phenomena and an 80% increase compared to the last three months of 2021**. On the other hand, an exponential increase (+102% compared to the last quarter of the last year) has been observed in the use of **malware** – with **372 cases** – as an attack method to steal sensitive information, mainly by spying on users' banking activities. One should also not underestimate malware, which is causing serious reputational and financial harm by encrypting the data of various organisations and companies in order to ask for cash ransoms.

PRESS RELEASE

Exprivia

Exprivia is the head of an international group specialized in Information and Communication Technology able to address the drivers of change in the business of its customers thanks to digital technologies.

With a consolidated know-how and a long experience given by the constant presence on the market, the group has a team of experts specialized in different technological and domain fields, from Capital Market, Credit & Risk Management to IT Governance, from BPO to CyberSecurity, from Big Data to the Cloud, from IoT to Mobile, from networking to business collaboration up to the SAP world. The group supports its customers in the Banking & Finance, Telco & Media, Energy & Utilities, Aerospace & Defense, Manufacturing & Distribution, Healthcare and Public Sector sectors. The offer includes solutions consisting of own and third-party products, engineering and consulting services.

Today the group has about 2,400 professionals distributed in 7 countries worldwide.

Exprivia S.p.A. is listed on the Italian Stock Exchange on the Euronext Milan (XPR) market.

The company is subject to the management and coordination of Abaco Innovazione S.p.A.

www.exprivia.it

Contact

Exprivia SpA

Investor Relations
Gianni Sebastian
gianni.sebastiano@exprivia.it
T. + 39 0803382070 - F. +39 0803382077

Press Office

Mediterranean Sec
T. +39 080/5289670
Teresa Marble
marmo@secrp.com - Cell. +39 335/6718211
Gianluigi Conese
conese@secrp.com - Cell. +39 335/7846403

Sec and Partners
T. +39 06/3222712
Martina Trecca
trecca@secrp.com - Cell. +39 333/9611304
Andrea Lijoi
lijoi@secrp.com - Cell. +39 329/2605000