PRESS RELEASE

CYBERCRIME: CYBERSECURITY IN ITALY DETERIORATES IN 2022

In 2022, the Exprivia Cybersecurity Observatory recorded 2,600 cybercrime phenomena, almost double the figure for 2021. Hackers are increasingly successful at causing cyber incidents, which exceed attacks for the first time since the report was released.

14 February 2023 – If 2021 was an annus horribilis for IT security in Italy, 2022 was even worse. For the first time since the **Exprivia Cybersecurity Observatory** on IT threats in Italy was created in 2020, the number of IT incidents (i.e. successful attacks) exceeded the number of attacks. This is because of the lengthening time between an attack and an incident, the increasingly sophisticated techniques used by hackers, and the lack of awareness of internet-related risks among businesses and the public.

This emerges from the **last 'Threat Intelligence Report'** from **Exprivia** which considers 118 open sources (sites of affected businesses, public sites of national interest, online news agencies, blogs and social media) and which, in 2022, registered **2600** cybercrime phenomena, of which there were **1236** attacks, **1261** incidents and **103** privacy violations. This figure is almost double the **1356 for 2021** and more than quadruple the **605 in 2020**.

Five-hundred-and-forty-seven events occurred in Q4 2022 alone, with a progressive growth in December (which had 257) that made it the third month by the number of events after March and May.

"With incidents overtaking attacks in 2022, we can say with certainty that some incidents are due to hostile actions carried out by hackers in the previous two years **- comments Domenico Raguseo, Exprivia's Cybersecurity director***. Indeed, it's a big mistake to consider an attack as an action that begins and ends after a few minutes or a few days. In many cases, it is an undeclared war waged by an attacker who first studies their victim's weaknesses and vulnerabilities, then decides when and how to strike the final blow. Some attacks can last for years, and it is often difficult to trace an incident to a specific attack."*

In the report from the Puglia ICT Group – which promotes a culture of information security – **cybercrime** is confirmed as the hackers' main motive in committing malicious actions, with over 2000 in 2022, an increase of 73% over 2021. Starting in 2022 with the Russian-Ukrainian conflict,

cyberwarfare also joined the list of motives, with **157** recorded events. **Hacktivism** (criminal activities to promote a political or social cause) is particularly important, increasing by **139%** over 2021.

The **Finance** sector, with big peaks throughout 2022 and, in particular, in the first half of the year, remains the most affected sector with **939** cases (36% of the total and more than double the 428 incidents in 2021). According to Observatory experts, this figure is because financial companies, banking institutions, and cryptocurrency platforms managing large amounts of money are attractive targets for attackers. The **Software/Hardware sector –** one of the favourite targets during the pandemic **–** follows with **343** cases, a slight decrease from the 338 last year, while **Industry** is in third place with **280** incidents, followed by **Public Administration** (which rose from 120 to **260** cases) and **Retail** (from 118 to 172), which remain among the most vulnerable sectors.

Data theft still leads among the types of damage identified in 2022, representing 70% of recorded phenomena. **Economic damage** and **service interruption** are at a much lower but still significant rate (respectively 10% and 11% of the total). Among the most used attack techniques, **phishing-social engineering** is still out in front, with **1133** cases of soliciting on the internet or via email sent to distracted or unaware users, almost double the 627 for 2021 or 43% of the total for 2022.

Lastly, the Exprivia report notes a decrease in IoT devices exposed online in Q4 (-8%). The index on the ratio between secure and non-secure devices, processed by the Observatory, highlights greater vulnerability in southern Italy. However, for the first time, the relationship between the digital services analysed, and the vulnerabilities identified seems to see the entire country moving at the same speed.

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 Sebastiano
gianni.sebastiano@exprivia.it
T. + 39 0803382070 - F. +39 0803382077

Press Office

Sec Mediterranea
T. +39 080/5289670
Teresa Marmo
marmo@secnewgate.it - Cell. +39 335/6718211
Gianluigi Conese
conese@secnewgate.it - Cell. +39 335/7846403

Sec and Partners
T. +39 06/3222712
Martina Trecca
trecca@secnewgate.it - Cell. +39 334/1019671
Andrea Lijoi
lijoi@secnewgate.it - Cell. +39 329/2605000