PRESS RELEASE

NEW CYBERSECURITY REPORT BY EXPRIVIA: SUMMER BREAK FOR CYBERCRIME, COMPUTER THREATS DECLINE IN ITALY BETWEEN JULY AND SEPTEMBER

However the report drawn up by the ICT Group Cybersecurity Observatory showed that despite the summer decline, the situation is worse than in 2021.
The IT security index for IoT devices is improving in the South.

28 October 2022.Cybercrime takes a break. Cyber attacks and incidents decreased in the summer and the gap between the first and the second has slightly reopened: signs that show how cybercrime moves in parallel with economic activity.

This is what emerges from the Exprivia Cybersecurity Observatory's new report, **the 'Threat Intelligence Report' on cyber threats in Italy,** which between July and September **2022 recorded 251 attacks, 203 incidents** - or successful attacks - and **27 privacy violations**.

There was a clear decrease in observed phenomena (481 in total) compared to the 766 in the previous quarter, with a 34% decline in attacks and 43% in incidents, with no significant change in privacy violations.

The report drawn up by the ICT Group in Puglia - which takes into consideration 113 open sources (sites of affected companies, public sites of national interest, online news agencies, blogs and social media) - finds that **87% of the phenomena** is attributable to activities related to **cybercrime**, now the top motivation for attackers for seven quarters. At a clear distance are hacktivism - or rather online civil disobedience actions - (about 8%), and data breaches (about 6%).Cyber warfare, which was added to the list of motivations for hackers with the outbreak of the conflict between Russia and Ukraine, registering a surge in the second quarter of 2022, has collapsed dramatically, almost disappearing in the third (-96%).

While **online banking** stands out among the opportunities used by attackers, there is also a **security alert** - a real trap to deceive users who are induced, for example, to provide confidential information - followed by **purchases made online**.

"After a period in which cyber threats had grown continuously, during the summer months there was a considerable reduction in cases and a widening of the gap between attacks and incidents - **commented Exprivia Cybersecurity Director Domenico Raguseo**. *However, comparing third quarter 2022 to the same period last year we see a significant worsening of the situation, and we*

believe the figure for the second quarter is more related to a summer "break" than to an improved defensive capacity of the ecosystem. In fact, we fear that early 2023 may hold many pitfalls".

Despite the reduction in cases compared to previous months, the third quarter of the year **is In fact significantly worse than the same period in 2021 (with a growth of 76%), when there were 273 phenomena recorded**.

According to the Exprivia Observatory, the **Finance** sector - which includes banking institutions, insurance companies and cryptocurrency platforms - remains the one most targeted by attackers, despite registering a downward trend on to the previous quarter, with 177 cases detected between July and September. In second place is the **Software/Hardware** sector, and therefore ICT companies, digital services, e-commerce platforms, devices and operating systems, with 71 cases in contrast with 130 in the previous quarter. This sector showed an increase in September that coincided with the resumption of economic and commercial activities.
The **manufacturing** sector is confirmed in third place with 55 cases, while the **Public Administration** remains in line with the previous quarter (48 cases), marking a significant downward trend in the pace of the phenomena, which had accelerated during the most acute phase of the Covid-19 pandemic.

Between July and September, **phishing/social engineering** returned to being the top attack technique, with 248 cases, which, however, confirmed a downward trend over the course of the year. **Malware** i.e. attack vectors aimed at stealing sensitive information, follows (172 cases, down 45% compared to the previous quarter), while **DDOS attacks** (malfunction or interruption of IT services) went from 112 cases in the second quarter to just one case registered in the summer months.

The Exprivia report also shows that the number of IoT devices has grown by 6% in Italy, and the new indices developed by the Observatory show a strong recovery in the South in the ratio between safe and unsafe devices. The relationship between the digital services analysed and vulnerabilities identified throughout the national territory has also improved, with greater intensity in the North, which still lags behind the Centre-South since the digital services available to the public continue to be targeted more by hackers.

In addition to the devices analysed by the Observatory (such as video surveillance cameras or printers), **medical equipment**, of which only 8.6% is vulnerable, **turning out to be less at risk than other categories, is also included in the analysis.**

"In the last quarter there has been a greater awareness in the South of the damage that ineffective management of IoT device security can cause - **continues Domenico Raguseo** - *compared to what has been shown in the past. This also gives us hope for the Observatory's work, which aims to raise awareness on issues related to the culture of cyber security, not only for businesses, but also in individual ecosystems".*

Exprivia, which recently obtained the Cybersecurity Made in Europe certification assigned by the National Committee for Cybersecurity Research and promoted by the European Security Organisation (ECSO), presented the report during the 'Apulia Cybersecurity Forum', four days of events organised by the ICT Group on the subject of cyber security.

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

PRESS RELEASE

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