PRESS RELEASE

EXPRIVIA PRESENTS THE NEW CYBERSECURITY REPORT: MORE CYBERCRIME INCIDENTS IN SIX MONTHS THAN IN THE WHOLE OF 2021

Research extends from the corporate perimeter to the individual, with printers and antivirus the targets most at risk. In the South, connected devices are less secure. The cyber-arms race continues as the Russia-Ukraine conflict carries on.

14 July 2022. A new report by Exprivia's **Cybersecurity Observatory on cyber threats** shows a big increase in Italy **with the first six months of 2022 exceeding the total for 2021. The first half of the year saw** 1,572 attacks, incidents and privacy violations in just six months, compared to 1,356 total cases last year**.**

Despite the growth curve over the entire six months, the report compiled by the Puglia-based ICT group - which includes 113 open sources (websites of affected companies, public websites of national interest, online news agencies, blogs and social media) - shows a slight decrease of around 5% in cases (766) **between April and June over Q1 2022** (when there were 806), but with a notable **peak in May**.
Between April and June, 381 attacks were reported, including 359 security incidents - meaning successful attacks - and 26 **privacy violations, 37% more than the previous quarter. Public Administration, Banking and Finance, and Healthcare were among the sectors most severely impacted** by the Data Protection Authority's sanctions.

"If on the one hand the slight decrease in the number of threats in Q2 suggests greater cyber security in the digital services that have evolved in recent years, on the other hand, overall cybercrime continues to grow at a very high rate," **comments Domenico Raguseo, Cybersecurity Director at Exprivia**. *"Moreover, for the first time, the Observatory has produced calculation indices that measure the impact of IoT devices on the security of the entire digital ecosystem, verifying whether the results of cybersecurity investments counterbalance those for digital development itself. At the moment, the analysis we start from shows a two-speed Italy, with connected devices much more at risk in the South than the North".*

Exprivia's new calculation indices show a lack of awareness in **Southern Italy** of the damage that ineffective cybersecurity management can cause to individual ecosystems, which are the ones most at risk (such as video surveillance cameras, printers, and even antivirus programmes themselves).

On the other hand, in the North, where more IoT devices are deployed due to the concentration of industries, devices are better protected but the digital services available to citizens are more exposed to vulnerabilities and under greater assault from hackers.

Between April and June, there was a huge increase in **DDoS attacks**, which disrupt the services provided by institutions, companies, public establishments, and malware, that is, attack vectors designed to steal sensitive information. Malware still tops the list of the techniques most used by cybercriminals in Q2 2022 (316 cases). **Phishing/social engineering** fell for the first time (-22%). This way of grooming via misleading emails or social networks dropped to second place, with **303 incidents** compared to 389 in the previous quarter.

In Q2, **cybercrime** remained the primary motivation for cyber attackers in Italy. **Cyber warfare** came second with 118 incidents, a fivefold rise over previous quarter (22) due to the continuing Russia-Ukraine conflict, increasing attacks on critical infrastructure. **Data breaches** (27) were in third place.

In the ranking of most affected sectors, cyber-attackers still favour **Finance**, up 14% (326 cases) compared to the first three months of 2022, accounting for 43% of the total number of attacks or 763. The **Software/Hardware** sector follows at a distance. This sector includes ICT companies, digital services, e-commerce platforms, devices and operating systems, which mainly suffer the theft of data, such as login credentials or sensitive information. Such cases rose by 40% (130) over the previous quarter, representing 17% of total attacks. The **Industrial** sector rose to third place, with 68 cases, while on 47 the **Public Administration** was **down 57%** presumably also thanks to government agency cybersecurity information campaigns, which seem to have increased awareness of how to better organise the implementation of appropriate security measures and controls.

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 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