

CYBERSECURITY: FIRST EXPRIVIA REPORT FOR 2023

CYBERCRIME INCIDENTS DOWN IN ITALY, BUT THE SECURITY OF MEDICAL DEVICES WORSENS

The number of cases was down 44% during the period January-March compared to the prior quarter. However, the risk for radiology equipment, cardiac devices and microscopes connected online is up. Data theft is back to first place in terms of damage caused by hackers.

25 May 2023 – The year 2023 opened with an overall **decline in cyber threats** compared to the prior months, but **exposed devices in the network are up** and have **little protection**, particularly those used in **the medical field**.

This is what emerges from the new **"Threat Intelligence Report"** by the **Cybersecurity Observatory** of **Exprivia**, which looks at 122 open sources among the sites of affected companies, public sites of national interest, online news agencies, blogs and social media.

According to the report by the ICT Group in Puglia, cybercrime was down by 44% **between January and March** with **308** cases, compared to **547** in the last quarter of the prior year, with March alone accounting for nearly half of the cases (137). Compared to the same period of 2022, attacks were actually halved (-53%), with incidents down by over 70% and violations of privacy by 37%.

More specifically, during the first three months of the year, there were **192 attacks**, **104 incidents** - i.e. successful attacks - and **12 violations of privacy**.

"The number of incidents recorded compared to the past has indeed fallen; we had not recorded such a low number of incidents since September 2021 ", commented Domenico Raguseo, Cybersecurity Director at Exprivia. "However, we must become accustomed to cybercrime, especially at a time when network-connected devices are on the rise. At the same time, in fact, there is a growing risk of incurring threats that disrupt critical services such as those of the health sector. These results should act as an incentive to comprehend how to combat the phenomenon, with the only solution being to continue to invest in cyber security".

The report indicates that IoT devices connected to the network in Italy are up by 13% (around eight million), leading to a higher probability of being attacked by hackers, particularly in southern Italy. According to the assessment index of the Exprivia Observatory, the security of intelligent medical devices has worsened as well, such as equipment for radiology and magnetic resonance, microscopes or cardiac devices that are wearable and connected. A slight decline was also observed

PRESS RELEASE

in the level of security of services exposed online, increasingly vulnerable due to the increase in digital activities, from online payments to the sending of electronic prescriptions, with hackers compromising their retrievability or availability and causing inefficiencies in the systems.

According to experts of the Cybersecurity Observatory of Exprivia, committed to promoting awareness of cyber security including through training courses, the most targeted sector by hackers during the first quarter of the year was **Software/Hardware** (ICT companies, digital services, e-commerce platforms, devices and operating systems), with 99 cases. The **Public Administration** sector is second with 89 cases, up by 59% compared to October-December of last year, which recorded 56 cases; in third place with 31 incidents is the **Finance** sector (finance companies, banks or cryptocurrency platforms), which lost its top spot and recorded a 79% decline against the last quarter of 2022 (which had 150 incidents). These are followed by **Industry** and **Retail**, respectively with 22 and 14 incidents.

During the first quarter of the year, **data theft** was back to first place among the types of damage caused by hackers, accounting for 65% of total cases (201 incidents over a total of 308); however, this figure was down by over 50% compared to the previous survey (424). Data theft consists of the illegal storage or transfer of personal, financial or proprietary information such as passwords, software codes, algorithms and processes causing serious consequences for the persons or organisations impacted. With similar results, in second place, we have the **interruption of service** (halt of normal functioning of the network, of an application or of a software service) with 15% of cases, and requests for **money** with 13%, followed by the **violation of privacy** (4%), i.e. the disclosure of data by third parties without consent by the interested party.

In terms of types of attack, the most common was **phishing/social engineering**, i.e. the luring online or via email of distracted or inexperienced users, accounting for 47% of total cases (145 incidents compared to 193 the previous quarter); attacks through **malware** were also down, in second place with 88 cases compared to 170 recorded between October and December 2022.

According to the report, **cybercrime** is the main threat for network security in Italy, accounting for over 80% of cases (255). Quite a way behind are **hacktivism** (criminal activities to promote a political or social cause) with 13% (40 cases), and **data breaches** (security violations that involve the destruction, loss, modification, unauthorised access to or disclosure of personal data), accounting for 4% of the events detected.



PRESS RELEASE

Exprivia

The Exprivia Group, specialising in Information and Communication Technology, is one of the leading players in digital transformation.

Drawing on a wealth of expertise gained in over 30 years of constant presence on the national and international market, Exprivia employs around 2,400 people in six countries around the world, with a team of experts in various fields of technology and digitalisation: from Artificial Intelligence to Cybersecurity, from Big Data to Cloud, from IoT to BPO, from Mobile to Networking and Collaboration, covering the entire SAP world.

Listed on the Italian Stock Exchange since 2000 in the Euronext (XPR), Exprivia supports its clients in the Banking, Finance&Insurance, Aerospace&Defence, Energy&Utilities, Healthcare and Public Sector, Manufacturing&Distribution, Telco&Media sectors. The group's design capability is enhanced by a strong partner network, proprietary solutions, design, engineering and customised consulting services.

The company is subject to the management and co-ordination of Abaco Innovazione S.p.A.

www.exprivia.com

Contacts

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

teresa.marmo@secnewgate.it - Mobile +39 335/6718211

Gianluigi Conese

gianluigi.conese@secnewgate.it - Mobile +39 335/7846403

Sec and Partners

T. +39 06/3222712

Martina Trecca

martina.trecca@secnewgate.it - Mobile +39 334/1019671

Andrea Lijoi

andrea.lijoi@secnewgate.it - Mobile +39 329/2605000

