PRESS RELEASE

CYBERSECURITY: EXPRIVIA PRESENTS NEW REPORT

HACKERS GETTING MORE SKILLED, SECURITY INCIDENT TRENDS ON THE RISE

The Software/Hardware sector remains one of the main targets for hackers. Starting this quarter, the analysis of attack techniques present in the MITRE ATT&CK® framework has been introduced.

XXX– The number of cyber attacks in Canada in the third quarter of the year remains steady, with a resurgence of security incidents. This is highlighted in the new 'Threat Intelligence Report' compiled by **Exprivia's Cybersecurity Observatory**, which considers 55 open sources including websites of affected companies, national public interest sites, online press agencies, blogs, and social media.

According to the report from the ICT group, between July and September, there was an approximate **2% increase in cybercrime phenomena**, with a total of **171** cases, compared to **167** in the previous quarter. Specifically, there were 102 attacks (down 5% from 107 in the previous quarter), **68 incidents** – successful attacks – with a 19% increase compared to the 57 previously recorded security cases, and one **privacy breach** (down 67% from three in the last quarter).

'Compared to the previous quarter, there is a growing trend in security incidents and an almost unchanged number of attacks. Despite a consistent number of attacks, a trend of increasing incidents is not a good omen, especially in light of December, notoriously dominated by consumer fraud. We advise companies to pay great attention not only to what might happen but also to what has happened, knowing that an attack has a lifecycle of months, sometimes years. The number of attacks and incidents forces us to advance in the analysis of these events. To combat crime, we can no longer just focus on the technique predominantly used in the attack, but we must understand when, how, and why the technique was used in constructing the attack. To do this, we have decided to refer to MITRE ATT&CK® which classifies all the known attack techniques used in various stages of an attack. This allows us not only to understand that phishing is the most used technique, but also to comprehend when phishing is utilized. It's not surprising that phishing is used in the victim identification phase, but also during the initial access. If we often receive emails and do not understand their meaning, it does not always mean that the sender has sent a wrong email, sometimes it may mean that there is an activity aiming to recognize the targets of a possible attack,' ***comments Domenico Raguseo, Director of Cybersecurity at Exprivia****.*

For the experts at Exprivia's Cybersecurity Observatory, committed to promoting cybersecurity culture also through training courses, the sector most targeted by attackers in the third quarter returns to being **'Software/Hardware'** (ICT companies, digital services, e-commerce platforms, devices, and operating systems), with about **37% of the cases (64)**. In second place is the 'Finance' sector (financial companies, banking institutions, or cryptocurrency platforms) which increased from 22 phenomena in the second quarter to **37**. The **'Retail'** sector, the market that includes sales activities by a company to the final consumer, follows, increasing from 21 cases recorded between April and June to **19 cases**.

Data theft maintains the lead among the main **types of damage** caused by hackers with **78%** of **total cases** (134). Data theft involves the illegal storage or transfer of personal, financial, or proprietary information such as passwords, software codes, algorithms, and processes causing serious consequences for affected individuals or organizations. In second place is the demand for **money**, with a **percentage increase of about 44%** compared to the previous quarter. Following this is the **service interruption** (the stoppage of normal functioning of a network, an application, or a software service) with a **57%** reduction compared to the previous quarter.

In the third quarter of 2023, there has been an increase in attacks via **malware** (malicious software that compromises or disrupts the use of devices), which topped the list with **120 cases** compared to 94 recorded between April and June 2023. Meanwhile, the number of attacks via **phishing/social engineering**, which involves the online or email luring of distracted or unaware users, remained almost unchanged as the main type of attack, accounting for **10% of total cases** (18 incidents compared to 21 in the previous quarter, **a reduction of about 14%**). Specifically, there has been an exponential increase in **ransomware** with **37** recorded cases, malicious software that encrypts the files of the victims' systems, with the aim of demanding a ransom through the extortion of money to restore access.

According to Exprivia's report, **cybercrime** continues to be the primary threat to network security in Italy, accounting for over **90%** of the incidents (163) relative to the total. **Hacktivism** (criminal activities aimed at promoting a political or social cause) follows at a significant distance with about **4%** of the cases (6).

Finally, **data breache** (security violations involving destruction, loss, modification, unauthorized access, or disclosure of personal data) account for approximately **1%** of the total detected events.

PRESS RELEASE

Exprivia

The Exprivia Group, specializing in Information and Communication Technology, is among the leading players in digital transformation.

Backed by a wealth of expertise gained in more than 30 years of constant presence on the national and international market, Exprivia employs about 2,400 people in six countries around the world using a team of experts in different areas of technology and digitization: from Artificial Intelligence to Cybersecurity, Big Data, Cloud, IoT, BPO, Mobile, Networking and Collaboration, entirely presiding over the SAP world.

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

The company is subject to the management and coordination 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