PRESS RELEASE

ONLINE SECURITY: IN THE SECOND QUARTER OF 2020, CYBER CRIMES INCREASED BY MORE THAN 250% COMPARED TO THE FIRST. ATTACKS PEAKED IN JUNE.

Exprivia's Cybersecurity Observatory also connected most of the reported phenomena in the second quarter of the year to the coronavirus. Over 60% of the incidents resulted in data theft. Industry is under attack after the lockdown.
Video surveillance systems are in danger.

30 July 2020 - The Covid-19 emergency in Italy has heavily affected cybersecurity even after the emergency. According to the second **report on cyber threats in Italy in 2020** developed by the **Exprivia Cybersecurity Observatory, June had the most attacks, incidents and privacy violations since the beginning of the year**, to the detriment of companies, individuals and the public administration.

Analysing 40 public information sources, it was found that between the first quarter of the year (when there were 47 attacks) and the second (171)**, the increase was more than 250% with a peak in June** (86 attacks), due to the increase in smart working, more connections to social networks during the emergency and the reopening of businesses immediately after the lockdown. Most of the attacks are related to the coronavirus emergency and over 60% of the incidents resulted in **data theft**, with triple-digit growth compared to the first quarter **(+361%)**, far exceeding both privacy violations (11% of cases) and financial losses (7%). Additionally, Exprivia's experts focus on the high risk for video surveillance systems targeted by hackers, which experienced a dangerous attack with the MIRAI malware already in the first quarter.

Domenico Raguseo, Exprivia's Director of Cybersecurity, confirms, *"During this period, several illegal sites have used terms such as 'Corona Antivirus' to introduce malicious software into the computers of their victims, compromising their operations.*" Raguseo added, "*Cybercrime has flourished mainly due to a lack of a widespread digital culture, including with individuals, and the inadequacy with which companies and public agencies protect sensitive data and IT systems. We also expect that video surveillance systems and IoT devices connected to the internet will also be at high risk for attacks in the coming months, which will not be adequately protected, facilitating illegal access."*

From the second report of the Exprivia Observatory, which promotes new training courses in the area of IT security for both business professionals and private users, it is also evident that in the second quarter in Italy **'hactivist' attacks**, i.e., hacker-style digital actions, **grew by 700%**, an emerging phenomenon often linked to international campaigns on highly topical issues such as "Black Lives Matter" and "revenge porn".

Furthermore, **scams conducted through phishing and social engineering quadrupled** (+307% compared to the first quarter, more than 37% of cases), which deceive the user by leveraging "bait" messages in e-mails or using subtle techniques in social networks to obtain financial information

(bank account or credit card numbers) or stealing passwords for services to which the individual subscribes. Also in the second quarter of the year, the **cyberattack method remains unknown in over 30% of cases** (53 more attacks in the second quarter), thus highlighting the urgent need to develop adequate security systems. However, 17% of attacks occurred through malware - malicious software or computer programs - that exploited the coronavirus to attract the attention of users. These include the "**Corona Antivirus**" or "**Covid-19 Antivirus**" programs, malware that allows cyber criminals to connect to the victims' computers and view the content, steal information or use it as a vector for further attacks. In addition, there is also the "CovidLock" ransomware - a type of malware that renders a system unusable and requiring the payment of a ransom to restore it - which targets Android smartphones when trying to download an app for updates on the spread of coronavirus.

In the second quarter of the year, 26% of the criminal initiatives were directed towards non-classifiable sectors and as many as 18% concerned multiple sectors; this is followed by the identified areas that have received the most attacks, the **Public Administration** and the **Cloud** (about 10% each of the total), whose platforms, even after the lockdown, continue to be stressed by remote working. The **Finance and Education sectors** still remain on the list of the most vulnerable areas (in particular, universities and schools engaged in exams in June), but there is a new entry for the **Industry sector, which in June marked a peak in attacks**, apparently connected to the reopening of many factories after the emergency period.

Other findings and useful data are contained in the report by the Exprivia Cybersecurity Observatory, available for download from the website www.exprivia.it, which also provides access to the list of courses organised for cybersecurity training.

(*) Source: https://www.enforcementtracker.com/

PRESS RELEASE

Exprivia

Exprivia is the head of an international group specialised in Information and Communication Technology, capable of directing drivers of change in the business of its customers thanks to digital technologies.

With robust know-how and significant experience from its constant presence in the market, the group has a team of experts specialised in the various technology areas and domains, from Capital Markets and Credit & Risk Management to IT Governance, from BPO to IT Security, from Big Data to Cloud, from IoT to Mobile, from networking to business collaboration, including SAP platforms. The group supports its customers in the sectors of Banking & Finance, Telco & Media, Energy & Utilities, Aerospace & Defence, Manufacturing & Distribution, Healthcare as well as the Public Sector. The offer includes proprietary and third-party solutions, engineering services and consultancy.

Following the acquisition of 81% of the share capital of Italtel, a historic Italian company that today operates in the ICT market with a strong focus on the Telco & Media, Enterprises and Public Sector markets, today the group has approximately 3,600 professionals in over 20 countries around the world.

Exprivia S.p.A. is listed on the Italian stock exchange on the MTA market (XPR).

The company is subject to the management and coordination of Abaco Innovazione S.p.A.

www.exprivia.it

Contacts

Exprivia SpA

Investor Relations
Gianni Sebastiano
gianni.sebastiano@exprivia.it
Tel +39 0803382070 - Fax +39 0803382077

Press office

Sec Mediterranea
Tel +39 0805289670
Teresa Marmo
marmo@secrp.com
Mobile +39 3356718211

Gianluigi Conese
conese@secrp.com
Mobile +39 3357846403

Sec and Partners
Tel +39 063222712
Martina Trecca
trecca@secrp.com
Mobile +39 3339611304

Andrea Lijoi
lijoi@secrp.com
Mobile +39 3292605000