OAD
Osservatorio
Attacchi Digitali
in Italia

OAD 2020 Report - Executive Summary

The Digital Attacks Observatory in Italy, OAD, with this 2020 edition reaches the twelfth year of consecutive surveys on cyberattacks in Italy, and, as in the previous years, with the precious collaboration of the Italian Postal and Telecommunications Police.

OAD is the only independent online survey in Italy on intentional digital attacks on IT systems of companies and public bodies operating in Italy. The OAD survey does not provide for a predefined set of respondents, but allows potential interested parties full and free access to the online questionnaire, in a totally anonymous manner. Thanks to the number of responses collected and their balanced distribution between companies and public bodies of various sizes and belonging to various product sectors, the OAD survey provides an accurate picture of the cyberattacks in Italy.

The OAD 2020 survey took place during the Covid-19 pandemic, which made it even more difficult than in previous years to reach the respondents' minimum number necessary to obtain a consistent and credible survey. In order to better motivate the potential respondents, the 2020 questionnaire provided a reduction of the more technical questions, and a qualitative macro evaluation of the level of the cybersecurity of each Informatics System object of the answers provided. By means of these innovations and of the large promotion for the questionnaire compilation, it was possible to reach a sufficient number of answers, even exceeding the number of those received in the previous OAD editions.

The emerged respondents' pool covers all the product sectors, including Public Administrations, even if the majority of the respondents' companies belong to the ICT sector (30.8%). The 2020 pool is well balanced for the size of the organizations, in terms of number of employees, between those below 250 and the largest ones. It must be taken into account that in Italy 99.91% of enterprises are SMEs, Small Medium Enterprises, under 250 employees, and of these 95% are under ten employees. The OAD 2020 survey is therefore able to investigate on small and very small organizations, which are not normally considered in other cybersecurity surveys: 57.5% of respondents belong to structures with less than 250 employees, and of these 22.1 % under 10.

The OAD 2020 survey refers to the entire year 2019 and to the 1st quarter of 2020, when the Covid-19 pandemic exploded. This pandemic has been the trigger for a wide range of cyberattacks, mainly caused by the sudden - and in part unprepared - passage of many to agile working from home and to a strong use of every type of IT service on Internet, mainly derived by the mobility lockdowns imposed by the Italian Authorities.

For 2019, cyberattacks on Informatics Systems of the respondents' basin amounted to 46.6% of the total, and for the first quarter of 2020 to 44.8%.

The type of attack (what is attacked) most widespread in both the considered periods is the one aimed at access control systems (IAA, Identification Authentication Authorization), with 34% in 2019 and 28.2% in the 1st quarter of 2020. As diffusion among the respondents, the other 14 types of attacks follow, decreasing by a few percentage points among them, whose characteristics and impacts are detailed in the related paragraphs of the OAD 2020 report. Referring to the attack techniques (how to attack), all the seven attacks families considered in the 2020 questionnaire are widely used in the various types of attacks, even simultaneously.

The most widespread one, as an average on the various attacks detected by the respondents' pool, is the use of toolkits (rootkits, meta-exploits, etc.) for the identification and exploitation of vulnerabilities on the target system of the attack, with a 38.8 %, followed by the well-known malicious and unauthorized collection of information (social engineering, phishing, etc.) with 34.6% and the use of malicious code and scripts with 34.3%. The other considered techniques decrease with a few percentage points of difference between them.

The impacts of the most critical attacks are analyzed for each attack type, as well as their possible motivations and the recovery times required by the most critical ones.

In the 2020 OAD survey, all these attacks' characteristics vary for each type of attack, and the emerged results are described in the specific paragraphs dedicated to each attack type. At overall it emerges that:

- the impacts declared by the respondents are balanced between those irrelevant and / or easily resolvable with recovery in short time and at limited costs, and those very critical, which require expensive and long recovery actions, and that, in some cases, can cause business and customer loses; these two very different impact cases depend mainly on the security measures in place;
- the motivations of the cyber-attacks are mainly of an economic nature, therefore done for fraud and blackmail: the widespread diffusion of ransomware in Italy is a clear confirmation of these motivations.

The Informatics Systems considered in the 2020 survey and their cybersecurity are in the medium-high range and the emerged information show a relevant improvement in both technical and organizational measures, in comparison to the previous surveys. Few of the considered Italian Informatics Systems are based on Data Centers in Italy, most of the respondents' companies have medium-small Informatic Systems partly on premise and partly outsourced, with an increasing use of cloud services.

The high number of attacks detected in 2018, and the privacy obligations (GDPR) have certainly contributed to strengthening cyber security measures, and a further improvement comes from the growing use of cloud services, where usually there are high standard security measures.

Organizational measures for cybersecurity, historically lacking and neglected in Italy, have improved in terms of defining roles and separation of duties, of organizational policies and procedures, and of incidents management. These measures often are lacking in small organizations, and in general the cybersecurity awareness and competence are low, and mainly at the top level of the public and private organizations

In Italy, there is still a long way to go in terms of cybersecurity continual training and awareness. A formal and bureaucratic approach for the organizational procedures is still prevalent, which once defined, often do not find a possible concrete applicability, periodic updates and operational tests: an emblematic example is represented by the Disaster Recovery plans for which, several times, the required alternative ICT resources to be used are not forecasted and allocated and there also not provided periodic exercises and simulations of the possible disasters.

Cybersecurity management tools still have limited diffusion among the 2020 OAD respondents, in particular the most advanced ones based on artificial intelligence techniques.

The use of IoT, of industrial automation and of robotics systems, and also of systems based on blockchain techniques find a low number of respondents involved, which also derives from the limited percentage of their product sectors that should be the more interested in these systems: the manufacturing sectors, the logistics, the research and development centers and labs, the Local Public Administrations for territorial control, and so on. For these topics, the data that emerged from the survey are considered only as specific cases that contribute to the general values on the cyberattacks, but which cannot be still considered of reference at the Italian level.

The data provided by the Postal and Communications Police confirm the growing criticality of the cyberattacks and, above all, the difficulties in combating and suppressing cybercrime:

- in the protection of Critical Infrastructures, in 2019, the 1181 attacks detected more than doubled compared to those of the previous year, as well as the 155 investigations launched, and the only 3 people arrested; in the first quarter of 2020, 282 attacks were detected, 34 investigations were launched, but there were no arrests;
- in the fight against "financial cybercrime", fraudulent transactions in 2019 were blocked for a total value of € 21.3 million and € 18 million were recovered; in the 1st quarter of 2020 fraudulent transactions for a good € 20.2 million were blocked, practically reaching in 4 months what was blocked in the 12 months of the previous year, and € 8 million recovered; an indicator of the growth in attacks on financial transactions and services due to the very

large use of these online services caused by the mobility blocks imposed by the Covid-19 pandemic;

- in the fight against cyber terrorism in 2019, 36,000 websites were checked and 250 contents deleted; in the 1st quarter of 2020, 11,962 websites were checked.

To conclude, the OAD 2020 survey highlights a situation of cyberattacks of various types but all technically of ian high complexity and sophistication, with a slightly increasing spread in Italy compared to the trend that emerged in the twelve years of OAD surveys, but lower than the peak of 2018. Despite the proliferation of cyberattacks to varying degrees related to the Covid-19 pandemic, in the first four months of 2020 the general spread of attacks is at similar values to those of 2019: to be verified with the next OAD 2021 if there will be changes to this trend.

The Italian reality, made up of a very large number of small and very small organizations, does not make our country one of the most attractive for cybercriminals, but cyber warfare and massive attacks represent a growing and serious risk, as has already happened in part with the widespread of ransomware on computer systems whit a lack of or with low cybersecurity basic measures.
OAD 2020 notes a clear improvement and strengthening of digital security measures, both technical and organizational, even if the most modern prevention, protection and management systems that use artificial intelligence techniques are still embryonic in the respondents' basin.

The defense measures and techniques in use chase the increasingly sophisticated and smart evolution of attacks, but almost always late. The high density of vulnerabilities requires different approaches and new logics, with the aim of making all ICT systems interconnectable to the Internet intrinsically safe, by default and by design. But we are still a long way from this goal, and in order to decisively improve the concrete fight against continuous attacks and cybercrime, it is currently necessary to increase cybersecurity' awareness and skills at all levels, an effective collaboration between the police at world level, and primarily a real and large usage of the professional ethics both of those involved (supply side) and both of those who decide (demand side) on cybersecurity.