OAD
Osservatorio Attacchi Digitali in Italia

Rapporto 2018 OAD

a cura di M. R. A. Bozzetti

Executive Summary

SPONSOR

digitree · rithecyber · par-tec

In collaborazione con Polizia Postale e delle Comunicazioni

Indagine effettuata da

aipsi · malabo ICT Advisory

Media Partner

Reportec

The Observatory on Digital Attacks in Italy (OAD) arrives in 2018 at the tenth year of surveys on digital attacks in Italy. OAD 2018 has been realized by Marco R.A. Bozzetti with his company Malabo Srl, under the aegis of AIPSI, Italian Chapter of ISSA, and with the precious and effective collaboration of the publisher Reportec Srl and of the Italian Postal Police, who provided data for the report's last chapter and whose Central Director, Nunzia Ciardi, wrote the report's preface.

The 2018 OAD Report analyzes the intentional attacks, detected from 2016 to 2017 in Italy, to the IT systems of organizations of all sizes and sectors, including central and local public administrations. It is based on the elaboration of the answers received from a web questionnaire available online in the first half of 2018. Being free access to the questionnaire on the Internet, the sample emerged does not have strict statistical value, but, given the number of answers and the good distribution by size and by sector of the of respondents, it provides precise and contextual indications on the phenomenon of digital attacks in Italy.

The survey also identifies the prevention, protection and recovery tools used by respondents' IT systems to counteract and limit such attacks.

The respondents are mostly made up of companies belonging to the ICT sector (36%), to the services' sector (13%) and to manufacturing industry (13%), followed by lower percentages of organizations belonging to all the other sectors (classified according to ATECO), to which are added the Central and Local Public Administrations. In terms of number of employees, around 80% belong to organizations of up to 250 people, of whom 37.5% belong to those with up to 10 employees. The sample emerged is therefore well balanced between small and medium-large structures, with reference to the latest ISTAT statistic, for which 99.91% are SMEs, and among these 95.22% up to 9 employees.

The respondents of the 2018 questionnaire are 269, of which 20% consists of top managers, 19.22% CIO, 17% of third-party staff, 14% by personnel belonging to the organizational unit of information systems: only 5.19% of CISO, with this role formally defined in the organization chart. in Italy, this role is mainly performed in part-time among different other roles.

The OAD 2018 survey has redefined the taxonomy of digital attacks, clearly distinguishing the type of the attack (the what), referred to the attack's target, by the techniques for conducting the attack itself (the how).

The 2018 OAD questionnaire, for each type of attack (the what), put questions on the techniques of attack (the how), their frequency, impacts, motivations, recovery time. Among the types of attack the survey also considered industrial automation systems, robotics, IoT systems, blockchain-based systems.

The digital attacks detected in 2016 hit 41.57% of the respondents' IT systems, and in 2017 45.32 %. These percentages are in line with those of the OAD previous editions (mainly around 40%, although this comparison is purely indicative and non-statistical), and they confirm that 2017 was one of the years with more digital attacks.

The most common types of attacks among the respondents' ICT systems were:

- in 2016: network attacks (44.62%), followed by the physical theft of ICT devices or of their parts (33.33%) and attacks on the outsourced ICT systems (21.54%);
- in 2017: attacks on access control (39.39%), DoS/DDoS (29.22%), physical destruction of ICT devices or of their parts (28.57%).

Considering all the types of attack in 2017, the most used attack technique is the one that uses malware, scripts and OS commands. The use of autonomous agents (viruses) follows, but with a large gap, and with a decreasing percentage the use of toolkits. The collection of information, typically through social engineering,

is positioned to the penultimate place, an indicator that most of the attacks in 2017 took place mainly through technical tools and operating remotely.

The impacts following the most serious attacks are analyzed for each type of attack, as well as the possible motivations of the attackers and the recovery times required by the most serious attacks. All these insights change, and sometimes they are specific by type, but in general the following points emerge:

- the most widespread impacts include: a decrease of the level of the service provided to the customers and users, vandalism, sabotage, further attacks based on the information and the actions performed with the previous one; the spread of this last impact, which is also one of the most widespread motivations, shows that attacks are increasingly correlated with each other;
- the most widespread motivations include: blackmail / retaliation, fraud, use of the attack to make further attacks more and more serious;
- recovery times are for the vast majority within three days after the attack, even if in many cases the recovery requires only one day. In the most serious and complex cases, a full recovery can take even longer than a month.

The most feared attacks in the future are related, at least in part, to the most serious attacks suffered in 2017. The first ones are the attacks on access control, feared by 40% of respondents, followed by the theft of information from mobile devices and desktops, feared by 30%. DoS / DDoS, attacks on networks and unauthorized use of ICT systems are each feared by 20% of the respondents. Other types of attack are feared with lower and decreasing percentages. Referring to the attack techniques, the most feared one is malware-scripts-commands for about 50% of the respondents, followed by information gathering, typically through social engineering, for about 45%.

The 2018 survey detects also the security measures that the ICT systems of the respondents have implemented: these can be considered at a medium-high level concerning the ICT technologies, and at a medium-low level concerning the digital security, despite some element of excellence for both these topics:

- 45.59% of respondents utilizes highly reliable architectures;
- almost 20% have a Business Continuity Plan and 33.84% a Disaster Recovery Plan, but only 1/3 of those last have also the availability of the necessary technical infrastructures to deploy the DR when a disaster may occur on the informatic system;
- the operating systems of the servers and of the end user devices are mostly updated to the latest versions, and 45.59% use "hypervisor" operating systems for server virtualization;
- a little less than ¾ of respondents use housing, hosting and cloud for part or for the entire their informatic system;
- for ¼ of respondents the operational management of the IT system is automated.

The basic technical measures for digital security are not as widespread as they should on the whole sample, but they have some widespread and serious shortcomings, above all in the presence of the GDPR regulation. Some weaknesses include:

- for 37% of the respondents, the lack of a digital security architecture;
- the limited physical security measures for the protection of local ICT systems;
- for about 50% of the respondents, the access control systems are mostly based only on user ID-password; 37.88% use Active Directory or LDAP and about 13% use certificates and PKI;
- concerning the network security, almost half of respondent's IT systems use DMZ and firewall, 40% use VPN, 1/3 use URL filtering and ¼ use IPS / IDS;
- concerning the logical security of individual ICT systems, even if 94.46% use anti-malware and antivirus, only 34.85% provides systematic management of patches and software versions, and only

32% mange the system administrators' logs; this last activity is mandatory since 2008 for a directive of the Italian Privacy Authority;

- concerning security at the application level, even if 42.42% of respondents declare to use application firewalls (very high percentage, some responders may have confused them with the most widespread network firewalls), only 16.67% carry out the security check for the software code;
- concerning data security, safe back-ups are performed by 1/3 of the respondents, and just under 20% perform encryption to store critical information; encryption should extend a lot for protecting personal-sensitive data thanks to GDPR;
- concerning the digital security management and governance, the most common tools used by 27.7% of the respondents are the centralized monitoring and control systems; about 17% of the respondents use tools for the analysis of vulnerabilities; few advanced respondents, lower than 5%, use artificial intelligence systems for the events correlation and for the behavioral analysis of ICT systems and / or of their users.

The organizational measures for computer security in the companies of the respondents are less widespread (as percentages) and mostly less advanced and implemented than the technical ones:

- more than ¾ of respondents have in their organization who performs the basic activity of a CISO, but only 30% have formalized this role, that is essential for security and its management;
- approximately 1/3 have defined and are using organizational policies and procedures for the management of digital security, but less than 10% have defined a clear separation of duties for all the actors of the ICT department;
- 21.72% of responding companies do not carry out any type of training and awareness on digital security;
- there is still little interest in professional certifications on digital security: about 40% of responding companies are not interested and do not require certification either for internal professionals and/or ICT department or for ICT suppliers, and 14.65% of the respondents is not able to answer; for the companies interested, certifications are required more for internal professionals;
- the risk analysis is carried out by 45.39% of the respondents, a higher percentage than those found in previous OAD investigations, certainly due to the GDPR obligations for privacy: but in this context the percentage is still too low. 12% already have insurance coverage for ICT risks, and 10% have plans to subscribe one;
- 42.25% of respondents already perform auditing for their IT system and its security, and 9.15% have a plan for auditing in the next future. It is interesting to underline that auditing is performed by 73% of the structures with less than 250 employees, and of these about half are the very small ones with less than 10 employees.

The Italian Postal Police, which is in Italy the main responsible for the fight against cybercrime, has provided many interesting data on its activities, done both in 2017 and in 2016. These data are analyzed in the last chapter of the report (§11), and they show that:

- for the Critical Infrastructures, the attacks detected increased by 22.27%, the alarms by 369%, the reported persons by 7.34%;
- in contrast to the financial cybercrime, the blocked fraudulent transactions increased (in €) by almost 30%;
- in contrast to cyber terrorism, the reported people and those arrested increased both by 100%.

To conclude, the results of the present OAD survey confirm both the trends highlighted in previous OAD-OAI reports, and the latest international reports on digital security: 2017 saw a sharp increase in both massive and "targeted" attacks, increasingly sophisticated and sometimes with very serious impacts. The Italian

reality, made up of a very large number of SME, does not make our country one of the most attractive for digital criminals; but massive attacks may be an imminent and serious risk, as has already happened with the large spread of ransomware on systems not updated and without a complete back up. As expressed by the Director of the Postal and Communications Police in her preface "*Among the reasons that favor the spread of the cyber threat, in the endemic terms currently tested, figure the ongoing underestimation of aspects related to information security, and the consequent failure to set up an adequate technological defense*." Regulatory obligations, such as compliance with the GDPR for privacy, help to improve digital security measures: but this is not enough, if the awareness and culture of digital security do not grow in the country at all levels, mainly at the level of the top managers and of the politicians who legislate on cybersecurity.


AICA

aipsi


ASSOCIAZIONE
SPECIALISTI
SISTEMI
INFORMATIVI

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ASSOLOMBARDA

CENTRO RICERCHE
SULLA SCRITTURA
handwriting research center


CDTI

CTI
er
CLUB

ti
Liguria

ti

ClubTI

FIDA
INFORM

FTI
FORUM per la
TECNOLOGIA della
INFORMAZIONE

Grafobiometristi
italiani associati

IEEE computer society
Italy
Chapter

Inforav