Volume XXI 2018
ISSUE no.1
MBNA Publishing House Constanta 2018

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Frequently used methods in the preparation of the informational attack

To cite this article: Radu Moinescu, Dragoș Glăvan, Scientific Bulletin of Naval Academy, Vol. XXI 2018, pg. 97-102.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-18-I1-014

Frequently used methods in the preparation of the informational attack

Radu MOINESCU[1], Dragoș GLĂVAN[2]

[1] Ph.D. Student, Military Technical Academy – Systems Engineering for Defense and Security Doctoral School
E-mail: radu.moinescu@gmail.com

[2] Ph.D. Student, Military Technical Academy – Systems Engineering for Defense and Security Doctoral School
E-mail: dragos.glavan@gmail.com

Abstract. Once with the development of WEB technologies, more attention has been paid to information originated from Internet websites being complementary to information obtained from other sources of interest. Specialized structures have been set up to collect, analyze and capitalize this information, theoretically and methodologically based on concepts and principles. Thus, definitions have been formulated for what Open Source Information (OSINF) and open-source intelligence (OSINT) are. This paper presents the stages and technological methods applied for an informational attack.

1. General considerations

In the last decades of the twentieth century, increasing the degree of IT&C in all fields (political, military, economic, cultural etc.), as well as increasing the use of information in solving human problems, made the information an important resource with multiple meanings and benefits for any human activity.

The existence of electronic and automation means in information processing for the management of different systems is a very important issue with profound implications in human society. At the same time, through the diversification of activities and the development of the information system in any field of activity, due to the specialized functions, the means of collecting the information are of great importance.

Cyber space is an important and inexhaustible resource for information available to anyone. With the development of WEB technologies, intelligence services have begun to pay special attention to this information due to their complementary character with information obtained by other methods, and have created specialized structures for their collection, analysis and capitalization, theoretical and methodological concepts, notions, concepts and principles, thus defining definitions for what is Open Source Information (OSINF) and Open Source Intelligence (OSINT).

One of the first concerns in this context is the German Federal Intelligence Service (Bundesnachrichtendienst - BND), which has established since 1990 a distinct structure for the exploitation of open sources. It monitors the media in the countries of interest to gather OSINF and conducts the activity of identifying and exploiting the secondary open sources.

In the USA, the Office of the Community Open Source Program Office (COSPO) of the Central Intelligence Agency (CIA) has been established since 1994.

The collection of information from open sources is not an illegal activity and can be done by anyone, but if this information is properly exploited, it can be strategic, operative and tactical in scope, goals and objectives.

Strategic character – refers to the long-term evolution of a process, system, or other area of interest that can be constituted from both basic and professional information; it is necessary to make decisions and prepare overall plans, designed to carry out actions for the achievement of strategic goals and objectives (Fig. 1).

Operative character – refers to data necessary for decision-making and the preparation of plans for short periods of time and on small areas / areas, designed to carry out actions for the achievement of operative level goals and objectives.

Tactical character – refers to data necessary for decision-making and the development of plans for immediate periods of time and hours / spaces, to reduce actions to achieve tactical goals and objectives, as well as data to be pursued bringing the necessary corrections into the decision-making act during the actions, preventing, eliminating and limiting the negative effects, as well as a series of current problems.

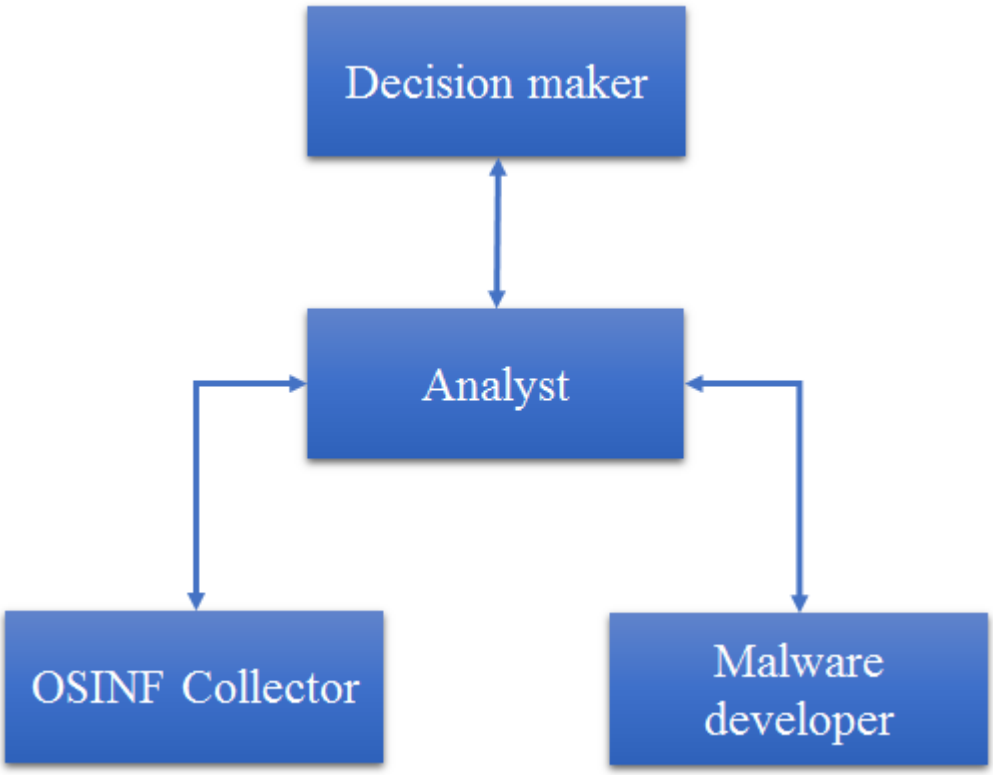

Fig. 1. Information flow in creating the malware

2. Social Network Analysis

Social Network Analysis (SNA) plays an important role in preparing computer attacks, especially those based on social engineering techniques, because it can provide valuable information on relationships and information flows between people, groups, organizations, IT systems, and other entities that process information and knowledge. Although it creates confusion between the concept of "social network" and "social networking" (Facebook, Instagram, LinkedIn, Twitter etc.), the latter provides the necessary resources for social network analysis through the data they provide. [1]

Often, ignorance or underestimation of the offensive collection and analysis capabilities of digital data, also available in the commercial, private sphere, makes it possible to recompose these information sequences in an intelligence product by interested entities. An important and frequent function of intelligence services is the constitution, periodic completion and maintenance of databases.

They consist of a great deal of relevant information about a variety of target objectives in any area of interest that can be activated when the situation that is created at a certain time so requires, as well as for monitoring.

By Social Network Analysis, stakeholders can easily set the starting point of an informational attack. Initial targets are studied though every information sequence for personal life, such as family and relational circle, preferences, passions, and then valued by specialized personnel, similar to making a puzzle, in order to create a psychological profile or to identify a main dominant of personality. This analysis identifies the best social engineering technique the attacker will address by exploiting human vulnerabilities such as sexual attraction, greed, vanity, credulity, convenience, compassion, or sense of urgency. The result of the analysis is a spear-phishing attack, a targeted phishing attack, characterized by personalizing the e-mail sent, impersonating a legitimate sender, and using techniques to avoid email filters, and persuading the victim to open the attached file or access a link.

Informational attacks based on Social Network Analysis can be of three types, depending on the attacker's goals:

- cybercrime activities aimed at: identity theft, financial information, theft of intellectual property or fraud;
- activities that serve the interests of some entities (competitors or intelligence services) and are aimed at: segregating data that is inaccessible to the public, theft of intellectual property and finding information and commercial secrets to generate unfair competition (competing products and services and their marketing etc.);
- hacktivism or actions by non-state terrorist entities generally pursuing, in the short term, damage or exfiltration of information (e.g. Wikileaks)

One of the most famous cyber-attack launched following the Social Network Analysis was in 2011 launched against RSA Security. The company was the target of a phishing attack that compromised a significant number of RSA SecurID token authentication devices. The attack was carried out by sending two different emails targeting four EMC employees (RSA mother company, later acquired by Dell Technologies on September 7, 2016). The emails had attached a malicious file called "2011 Recruitment Plan.xls" (Fig. 2) that used a zero-day exploit that facilitated the installation of a backdoor on the recipient's computer using an Adobe Flash vulnerability CVE-2011-0609. The backdoor allowed attackers to retrieve a large number of RSA employee's credentials, escalate privileges, and gain access to some systems that contained disparate data that putted together allowed attackers to compromise the RSA SecurID token devices. The data thus obtained was encrypted and exfiltrated through FTP to the attacker's command and control servers. [2]

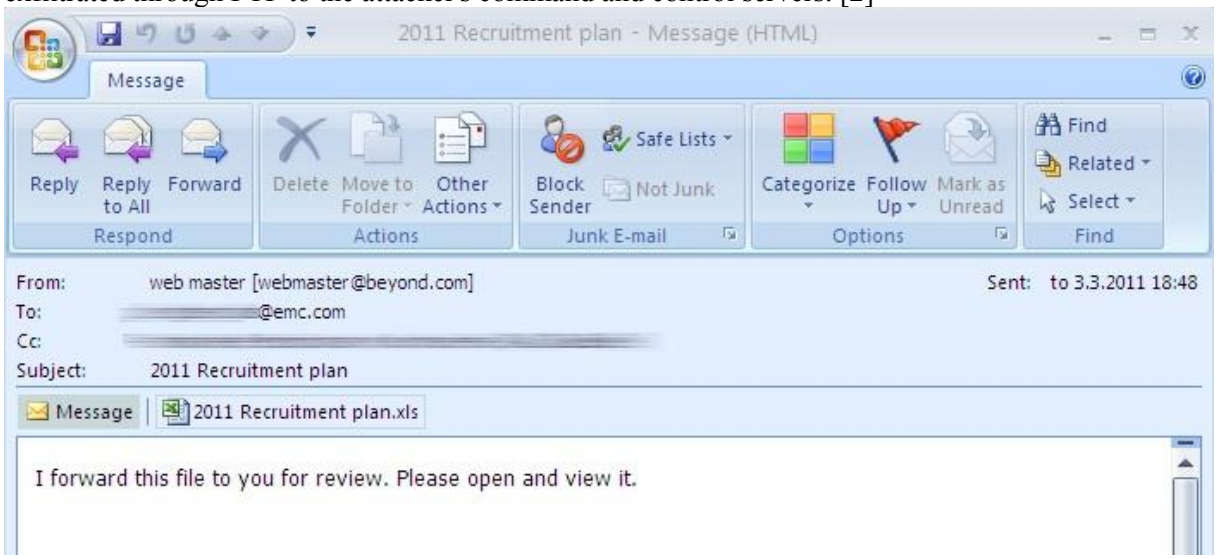

Fig. 2. RSA phishing e-mail

The attack was prepared by collecting online information such as employee and departmental lists, financial and planning documents available on the company's website. Although at the time of doing this paper we were unable to get a list of employees from the EMC website (probably removed by the company), we still managed to obtain this data by visiting the CrunchBase site (link https://www.crunchbase.com/organization/emc), a retrieval platform for information on industry trends, investments and public and private companies.

We can conclude here that an attacker becomes more credible than the more able to corroborate more target information.

3. Image interpretation

Often, an image is more appreciated than simple words, it can bring out much more detail, and when it is close to the moment of action it can highlight details of the last moment, changes etc.

Interpretation of images is one of the oldest preoccupations of intelligence services. Originally known as Photographic Intelligence - PHOTINT (information obtained from photo-video surveillance), it changed its terminology in the 1970s as a result of the evolution of sources and technologies from which images originated in Imagery Intelligence - IMINT. [3]

If in the beginning the imaging platforms were represented by surveillance balloons, used during the French Revolution, they evolved to satellite systems. Technological evolution and humanity's entry into the informational era has made the Internet also a platform for collecting multimedia information, and their interpretation can provide a quick and inexpensive means to plan and launch an informational attack.

Because some organizations work with sensitive information or manage critical infrastructure, their networks need to be isolated. Even if infiltration into these networks is feasible through the use of sophisticated methods of social engineering and the exploitation of zero-day vulnerabilities, internal recognition and lateral movement within these networks is done indirectly because there is no direct connection between attacker and compromised network. Here IMINT comes in, providing key elements about: how the target network is organized, the operating systems used, the software used to achieve the organization's goals, what certain IT systems are used in the organization etc.

The first advanced computer attack that refers to the use of images to model an informational threat is Stuxnet. Most computer security experts who analyzed the source code of this malware are of the opinion that the computer attack was modeled after analyzing photographs published on the Iranian presidency website and some footage made by an Iranian television on the April 2008 during the visit of the Iranian President, at that time, Mahmoud Ahmadinejad at the Nantz nuclear facility.

Although the malware architecture, propagation, and how it managed to avoid security systems have been extensively studied, the way that made it possible to collect the logical or physical elements that have allowed the target to be reached has been briefly analyzed.

One of the first images to be analyzed (Fig. 3) comes from the Iranian Presidency website. At the bottom of the image you can see parts of monitors that show the exact configuration of the SCADA system. The green points at the top of the monitor represent the status of each cascade centrifuge. Since the optimum uranium enrichment level cannot be reached by a single gas centrifuge, it is necessary to connect a number of centrifuges in series, this process being called a "cascade". This image, correlated with the International Atomic Energy Agency (IAEA) reports on Iran, has created a clear image for the attacker on the configuration of the centrifuges.

According to Symantec's final report on Stuxnet, the malware code was scheduled to attack a hardware array of six groups, each group having 164 elements. [4] Another malware property, which shows that its authors knew exactly how the system was working and the structure of the target system was checking a condition that determined whether the malware was running on the correct target system, more precisely Stuxnet checked if the centrifuge frequency converter drivers were produced by the Iranian company Fararo Paya or by a Finnish company named Vacon. [5] The centrifuges at Natanz normally will spin at 1,000 Hz, and what the Stuxnet did was to spin up the centrifuges to either 1,400 Hz to be really fast, or slow them down to 2 Hz, to be really slow. And what would

happen is when they spin up really, really fast, the centrifuge will basically vibrate uncontrollably and just shatter, possibly creating a domino effect of centrifuges. The fact that Iran didn't seemed to bother to hide parts of the photographs or footage taken inside the nuclear facility, and by the contrary, were used as pride to show the technological achievement and this gave the attackers exactly the right information in the development of the malware.

Fig. 3. Iranian President Mahmoud Ahmadinejad Nantz visit (April 8, 2008)

Other images that facilitated the Stuxnet attack were the displays in front of the operators (Fig. 4) showing: the control loops of the SCADA system, the piping, the valves and the pressure sensors of the cascade. These images compared with the code of Stuxnet gives a good forensic evidence once again that the attackers had a clear image of determining the target.

Fig. 4. The Cascade Protection System monitoring application

There are two ways to collect information from images:

- gross - refers to basic information / details (space, individuals);
- refined - refers to sensitive information / details (information displayed on computer system monitors, presence of documents).

By gathering information in a rough way, there is interest in information about: the place where the photograph was taken, the location of the surveillance systems, the individuals working in that place. People captured in images will be subjected to a facial recognition process, and data from this process will be corroborated with other information from other sources.

The refined collection of information is the most important because it often provides technical information to be carefully analyzed.

IMINT can therefore play an important role in the preparation of an informational attack, in that the attacker can test the attack vector on a computer system almost similar to the target. At the same time, information from IMINT must be capitalized in a short to medium time, thus losing the tactical advantage.

4. Conclusions

The relationship between human and information is indissoluble. The value of information lies in the ability to reach the right moment and in a credible form to the authority or individual who will use it. Information gathering is an essential category in achieving an information attack. The more information an attacker has, the more likely that the attack to be successful will be greater.

It becomes more clearly nowadays that organizations increasingly may be harmed by informational attacks based on information from open sources. Using this information attackers can explore an unknown field where they can launch a „fire and forget" weapon.

References

[1] Mircea MITRUȚIU, *Analiza rețelelor sociale*, Timișoara, 2005, http://www.asecib.ase.ro/mps/Analiza_retelelor_sociale.pdf

[2] Kim ZETTER, *Researchers Uncover RSA Phishing Attack, Hiding in Plain Sight*, Wired.com, August 26, 2011, https://www.wired.com/2011/08/how-rsa-got-hacked/nother reference

[3] K. Lee LERNER, Brenda Wilmoth LERNER, *Encyclopedia of Espionage, Intelligence and Security*, vol. 2, Gale Publishing, 2004, ISBN 0-7876-7687-X

[4] Nicolas FALLIERE, Liam O MURCHU, Eric CHIEN, *W32.Stuxnet Dossier*, Version 1.4, February 2011, Symantec Corporation, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[5] Ralph LANGNER, *Stuxnet und die folgen*, Langner.com, Munich, August 2017, https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf