Knowledge engineering

Operation 'Red October': and it is Cyber Espionage

ANTONIO TETI

Red October, in the greater part of the collective imagination, identifies a famous film of the 90's in which Sean Connery interprets the Commander of a Russian submarine in flight from the Soviet Union. Today, it identifies something quite different from a prey fleeing in the ocean depths: a formidable 'digital hunter' of the Cyberspace …

Operazione 'Red October': ed è Cyber Espionage

October 2012. The researchers of the Kaspersky Lab Global Research & Analysis Team start up an intense research and analysis activity on threats coming from the network regarding the detection of certain informatics attacks targeting computer networks of various diplomatic facilities. Within a few weeks, the Kaspersky technicians notice a botnet [1] which is quite different from the others because of its pursuit of distinct espionage goals. It is immediately christened 'Red October', which brings to mind the famous film of 1990, 'Hunt for the Red October', directed by John McTiernan and based on the homonymous novel by Tom ClancyContrary to the film plot, however, which attributes the role of the 'prey' to a silent, futuristic Soviet submarine hunted by other submarines of the same Nation with intentions to destroy it, in the case of the 'malicious' Red October code (pin-pointed by the Kaspersky technicians), it is the 'malicious code' that assumes the role of 'hunter', but retains the same silence and aggressiveness of the film submarine. And, as far as we know, it seems that it has exercised this role for five long years, before being discovered by a series of accurate investigations begun in 2007. It should be mentioned that as of January 2013, it is still active.

[1] Botnet. It is a network formed by computers connected to Internet and infected by 'malicious' software able to damage an informatics system. A Botnet can be created thanks to the presence of security flaws in the computers or the network, or even for negligence on the part of the user or the administrator of the system. In this case, the computers are attacked and infected by informatics viruses that permit their creators to control the entire network from remote systems. The controllers of the Botnet can exploit the infected computers by launching distributed attacks of the type 'distributed denial of service (DDoS) against other systems in the Net and can conduct further criminal actions, at times, acting on commission by criminal organizations. The computers that make up the Botnet are called Bot (from RoBOT) or Zombie.

The name given, however, as the Russian company Kaspersky underlines is attributable to the place of origin of the network that triggered the cybercrime actions: Russia. But it should be noted that many of the servers that were protagonists of the attacks are spread throughout other European Countries, for example, Germany.
In the technical Report presented by Kaspersky, it appears that the attacks have spread like an oil slick from Asia to the United States, mainly against institutional structures, government, (particularly embassies), academic and, above all, research centers located prevalently in East Europe and Central Asia. The principal mission of the cyber criminals was aimed at: the gathering of information regarding the types of information systems which were the object of the attacks; the mobile devices connected to them (notebooks, netbooks, smartphones, iPads etc.); the different varieties of router appliances, and last, but not least, certain databases stored in the mass memory of the computer systems.
The technique used is the following: firstly, the crackers [2] gather a variety of useful information on the target to be hit, utilizing a technique of particularly sophisticated phishing [3] the spear phishing. It is a programme purposely developed to launch phishing attacks, but only after having first collected detailed information on the target.
A classic example of spear phishing is where the recipient of the attack receives an email from a 'noted' or 'known' sender (therefore, considered as harmless), in which seemingly authentic documents are attached concerning the receiver's work or personal life. Consequently, the e-mail assumes all the characteristics of a real and reliable message. Following this, a 'malicious code' (malware) [4] is introduced, appropriately created to conduct specific actions: steal data and information; block the systems; modify memorized data in the computers and cancel data and programmes etc. In this case, the malware code is structured to acquire the data contained in the various computers present in the network where it has been introduced, even striking the mobile telephone devices (smartphones) connected to them. According to statements

[2] Cracker. In the computer science environment, the term 'cracker' identifies a computer expert who uses his knowledge and technologies to bypass the barriers and systems of protection (hardware and software) to obtain advantages, most of the time, economic. Nevertheless, 'cracking' can be used for the purpose of military or industrial espionage, for fraud, or to supply and increase disinformation. The term 'cracker' is often confused with the term 'hacker', the meaning of which is considerable different. The 'hacker' is the individual who uses his knowledge to explore, evaluate or test a computer system, without, however, creating damage or inefficiency to the system.

[3] Phishing. It is a scam technique in the network through which an attacker thinks to deceive the victim by convincing him/her to supply sensitive personal information. One of the classic examples is that of sending email messages that imitate the web graphics of bank or postal sites. With this technique, the criminal tries to obtain from the unfortunate people, the usernames and passwords of access to the system

[4] Malware. In computer science 'malware' indicates any software realized with the scope of damaging a computer or a network of computer systems. The term derives from the contraction of the English words 'malicious' and 'software' and has, therefore, the literal significance of 'evil programme' or 'malignant code'

by the Kaspersky technicians, circa 3,000 devices have fallen into the Red October trap and highly confidential documents have been robbed from their memorized data.
One of the more disturbing aspects lies in the type of data files taken from the attacked systems: the stolen files would include those with the following extensions: eretxt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau, cif, key, crt, cer, hse, pgp, gpg, xia, xiu, xis, xio, xig, acidcsa, acidsca, aciddsk, acidpvr, acidppr, acidssa. It should be noted that the 'acid' extensions are related to a specific software application by the name of 'Acid Cryptofiler', which is utilized by many authorities and institutional organizations, among which the European Union and the NATO, and the French Département Maîtrise de l'Information (former Centre Electronique de l'Armement, CELAR). Therefore, it is plausible to believe that the Red October systems are able to decipher both the messages and the documents encrypted by Acid Cryptofiler.
According to the investigation conducted by the Russian company, there are four salient points on which the entire operation is based.

1. The attacks lasted for at least five years and were mainly directed against diplomatic and government agencies throughout the world. Much of the information gathered was used to make new attacks, as in the case of the theft of the credentials of access to the systems of users of a certain importance, which inserted in specific lists, were used to identify the access passwords to other systems located in different networks. An interesting particular lies in the 'piloting' system of the infected computers: to exercise their control, it was necessary to create over sixty domain names [5] and as many servers (network computers) spread throughout different Countries, of which a good part are located in Germany and Russia. Furthermore, it became necessary to create a C&C infrastructure (Command and Control) based on the functioning of a 'battery' of servers having the function of proxy [6] and VPN networks[7] (Figure 1) to conceal the IP addresses of the servers of command and control (mother ships), the point from which the directives for the attack actions emanates.

[5] Names of domain. Domain Names System, DNS is a system used in Internet for the resolution of names of network nodes (hosts) in IP addresses (Internet Protocol Number) and vice versa. The service is realized through a database distributed in the network, consisting by the servers of the domain name server.

[6] Proxy server. A proxy server is a programme that interposes between client (user) and a server (network computer) and can be used in both local and for direct access to Internet. In the latter case, it is possible to have clients with a public IP address which connects them to a server with the proxy function, which handles the requests on their own behalf: the result is an anonymous connection for each client connected through the proxy.

[7] VPN (Virtual Private Network). A VPN is a technology that permits the connection between two private networks through the public network and was created, fundamentally, with the objective of installing an encrypted connection, and to increase, in this way, the productivity of the businesses. Through a VPN, it is possible to create a connection between the pc of a user and a VPN remote server, and all the data in transit

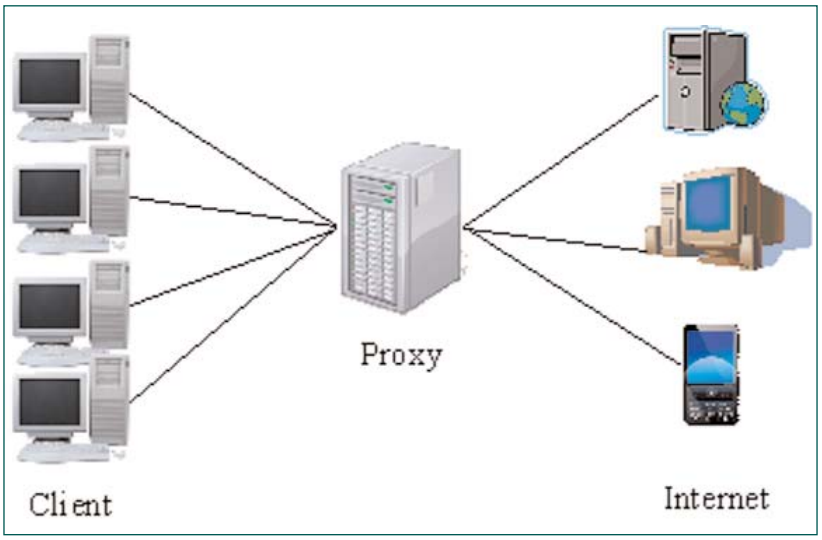

Figure 1 - *Proxy Communication*

2. The crackers of Red October have created a polyhedral multifunctional structure able to conduct attacks based on particularly effective and high performance techniques, but, especially designed to conduct cyber-Intelligence activities. Furthermore, the C&C system has shown to be particularly resistant to interception actions, as well as being extraordinarily effective in restoring the connection to the infected servers (which were protected by the defence systems of the victims) through channels of alternative communications.

3. Aside from the usual informatics systems (computers, servers and various work stations) attacks have been made on mobile devices, such as the smartphone (in particular, the iPhone, Nokia and the terminals that use Windows Mobile), but also the active devices of the network (particularly those of the Cisco Company). In addition, actions have been conducted of file extraction from removable mass memory storage, including the cancelled information, (but retrievable, thanks to the use of special software) still stored inside the infringed supports. Also, the email databases of many mail servers have been stolen (computers that manage the emails), as well as the data contained in numerous file-servers (computers used for the storage of data archives).

through Internet is sent into a virtual tunnel (tunneling), encrypted and not accessible to anyone. The VPN remote server then acts as a proxy server, concealing, therefore, the identity of the user. Very often this technology is used to transport the user's data to a location geographically different from the place of departure, which, many times, is subject to different laws.

4. The attacks also targeted certain application programmes of the Microsoft Office Automation. The use of three different exploits[8] employed to violate the following common-use applications was revealed: CVE-2009-3129 (MS Excel), CVE-2010-3333 (MS Word) and CVE-2012-0158 (MS Word). Some have already been known since 2010 (MS Excel) others appeared in 2012 (MS Word). In practice, the malware code was transmitted via email, as attachments of Word files, Excel and also in PDF format.
As far as the action of extracting information is concerned, at the moment of receiving the malware, activated by the opening of the document by the victim and exploiting the security vulnerabilities detected, a procedure of 'search and pick' is activated, which transmits instantaneously the information sought in the C&C system.
According to the updated data of Kaspersky of January 2013, the number of infected computers has risen above 300 (Figure 2). But the most critical aspect detected by the technicians of the Russian company lies in the extraordinary

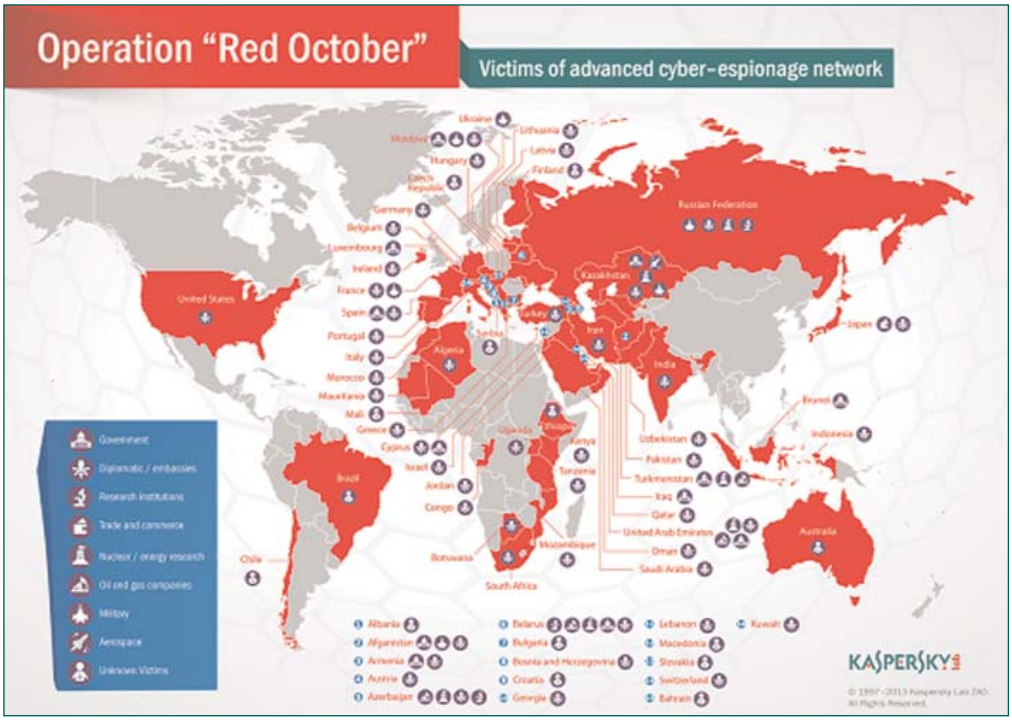

Figure 2 - *Victims of Red October*
(souce: www.securelist.com/en/images/pictures/klblog/208194085.png)

[8] Exploit. In computer slang serves to identify a code (programme) which, by exploiting a vulnerability of the system, allows the acquisition of privileges (complete access to the system) or to produce malfunctions to the system itself.

capacity of the Red October malware code to penetrate the computers and to withdraw all the access credentials (user name and password) stored inside them. It is further established that it is able to detect all the driver devices connected through interfaces of a different connection (USB, wireless, IrDA and Bluetooth) to the violated computers, thanks to the use of key loggers [9].
Since the practice of connecting smartphones and USB pen-drives to computers is now very widespread, we can deduce immediately what, in numerical terms, can be the extension of the entire operation of stolen data.
Once obtained, the data is included in 'dirty' packets (data packets that contain general and insignificant information) and transmitted to around 60 C&C servers, many of which are located in Germany, The latter, as a final action, communicate with the summit servers, defined also as 'mother ships', through the use of proxy, which takes charge of the transmission of the data in a completely anonymous way. "Everything is structured like an onion", says Rave Costin Raiu, 30 year-old head of a particular research team of the Kaspersky labs. He can count on the availability and efficiency of 34 'super' informatics technicians, spread geographically across the planet, but whom he directs from his office in Bucharest.
In an effort to discover the point of origin of Red October, Raiu created a specific programme to identify the victims of the 'malicious' code. It is a technique based on the assumption of addresses of the web servers that have not 'responded' to the attempts of access by the aggressors. In essence, Raiu tries to assume the identity (IP number) of one of the possible victims who has not yet been attacked, diverting the data traffic to his laboratory. It is a technique known as sinkhole [10] and enables the user to observe, in depth, the tunneling on the Net. After a few weeks 55,000 requests from contaminated computers were catalogued. "We were only able to access six out of the sixty 'Command' servers", Raiu said. "In other words, we were able to see only about 10% of the Net". To a great extent, these results are due to the interruption actions of Red October, carried out by the C&C servers to put the 'malicious' software in 'hibernation' for the obvious reason of defusing actions of interception. However, this must not lead us to suspect that the attacks are definitively terminated, given that Red October can be reactivated at any moment.
Another interesting aspect lies in the fact that after the access to the system, the malware code activates 1000 software applications with the sole purpose of conducting actions of Cyber-Intelligence. Raiu carried out a test in his labo-

[9] Key logger. In computer slang a key logger is a device of sniffing (activity of passive interception of data, hardware or software capable of intercepting everything a user digits on the keyboard of his own, or another person's computer.

[10] Sinkhole. A DNS Sinkhole, noted also as a sinkhole server. It is a Domain Name Server, which furnishes false information to impede the use of the names of real domains. The most common use is that of blocking the Botnets (a network formed of computers connected to the Internet and infected by malware, controlled by a single entity, the Botmaster, interrupting the DNSs used by a botnet. It is a technique that can be used for defence against attacks and to conduct them.

ratory to verify the effectiveness of these actions: after having infected a computer, the virus mapped the entire network of the laboratory and compiled a detailed list of all the informatics devices present, including the active devices of the network (switch, router, firewall, proxy). Subsequently it filed all the collected data, encrypting it in appropriate files. Then proceeded to assign a number for each of its victims (computers). Having terminated its work of analysis, cataloguing and memorization, the infected computer proceeded by putting in contact a series of servers deployed on the Internet network. It will be the latter to redirect the data packages to the mother ships.
Another interesting aspect is seen in the versatility and multi-functionality of the malware: in function of the type of hardware/software platform to attack, the infected computer utilizes the most suitable software, conducting simultaneous attacks on different systems. Therefore, the software proceeds with the search for passwords, particular documents, information contained in the databases, lists of information, tables etc. If lists of telephone numbers are found, certain software go ahead with attempts to access the mobile terminals (smartphones) trying to connect itself through Wireless, Wi-Fi, Bluetooth or by direct telephone calls. It is assumed that these 'malicious' applications are also able to copy the information contained in the mobile telephones, including the deleted information.
At this point, the following question could arise: how is it possible that during the 5 years of Red October's activities, the countless antivirus applications available on the market have not been able to detect the existence of this worm? [11]. A possible answer is given by Andreas Marx, Managing Director of AV-Test[12] well known German Institute specialized in informatics security, who says: "Red October infects only single computers in a very targeted way, while the anti-virus software, usually, concentrates on widespread common worms".
Red October has directed its attacks principally against Russia and other former-Soviet republics, but also many computers have been infected in India, Afghanistan and, in particular, in Belgium, where the NATO and the European Union have their headquarters. Fewer infections have been found in the United States, Iran, Switzerland and Italy. Infections have not been found in China and North Korea.
Moreover, it is singular that, according to the team of the Russian company, Red October presents striking similarities to the notorious 'malicious' codes Stuxnet, Flame and Gauss, which have, in fact, inaugurated in recent years, the era of the Cyber wars.

[11] Worm. A worm is a particular category of 'malignant' code. Its major characteristic lies in its ability to self-replicate. It is very similar to a virus, but differs from this latter because it does not need other applications in order to propagate.

[12] www.av-test.org/en/home/

Cyber Intelligence: the new frontier of espionage

Vitaly Kamlyuk is a Belarusian of 28 years old, component of the 'special unit' of Kaspersky that contributed to the discovery of Red October. In an interview granted to the online German newspaper Der Spiegel [13], he says that from the attacks conducted emerged "… a special interest for information which was very significant at a geopolitical level". According to the Belarusian technician, it would seem that the Russian Embassy was the most coveted of the attacks. And as far as we are able to know, thousands of documents (we are speaking of terabytes of data), including 'classified' ones from the Foreign Ministry in Moscow, have fallen into the hands of the cyber spies. It seems that the silent digital submarine has spent its first five years sorting, analyzing, checking, assimilating and memorizing information of every kind and it's almost certain that the majority of its victims were aware of it. "Never before have we seen an attack conducted with such surgical precision", Kamlyuk says.

And this can be believed since the Company for whom he works is not able to accumulate additional information on the malware and why? Because 'the enemy is destroying the proof', thanks to the 'offline' state of the systems of control and piloting of the attacks.

As we have been able to understand, Red October belongs to the family of 'malicious' software (given the name 'Sputnik' by Kaspersky) able to infect the computers that utilize applications like Word and Excel, exploiting the hidden vulnerabilities. With about a thousand malwares strong, (grouped in modules), the Kaspersky researchers have catalogued at least 10 categories of damaging actions (modules) which can be targeted on the attacked computers:

1 Recon (Reconnaissance). These are modules planned to be used during the initial phase of the attack, after the phase of penetration of the informatics systems. Their principal purpose is that of gathering general information on the target, in order to be able to localize and identify the computers to infect; to estimate the potential value of the informatics data available and to define which other modules must be utilized later. These applications also handle the collection of further information capable of supplying interesting indications, such as: the chronology of the web sites visited; the credentials of access memorized in the browser cache (username and password), and any eventual FTP client settings [14]

[13] http://www.spiegel.de/international/spiegel/how-russian-virus-hunters-tracked-down-a-global-espionage-network-a-879467.html

[14] FTP Client. It is a software that allows the use of the file transfer function (File Transfer Protocol, FTP) to transfer files data from one computer to another.

2 Passwords. These are modules able to extract the credentials (username and password) from a series of programmes, among which the temporary folder protected by Microsoft Outlook (emails, address book contacts, appointments activities) and Agent Mail.ru, the most popular portal of free email, used by Runet [15]. Furthermore, these modules are able to gather the hash [16] of the Window accounts in order to penetrate any work station.

3 E-mail. In this category we find the modules to extract the messages and the data locally memorized by the client of emails such as Outlook and Thunderbird, but also for the remote connections (POP3) or on mail servers (IMAP). They are able to copy the addresses of the senders, of the recipients, the text of the messages and even the files contained within same, (the attached documents).

4 USB Drive. These modules are able to steal data from the units which are connected to the UBS interfaces (pen drive, mass storage devices, smartphones, pc, etc.). They can collect any type of files and can even acquire an entire file system [17], including the cancelled files

5 Keyboard. These modules are capable of registering the typing/keystrokes on the keyboard. They are programmes that register the letters and numbers that are typed, memorizing everything that is entered into the system, obviously including the private access credentials, even capturing the images projected on the screen (in this sense, the matching between applications and typing is automatic).

6 Persistence. They belong to the modules that proceed to the installation of payload codes [18] for various applications (Word, Acrobat Reader etc.) as

[15] Runet. It is a much used term that identifies the web sites and Internet domains attributable to Russia. It is often used by the media as a synonym for Russian network.

[16] Hash. In the informatics field it corresponds to a function that maps a string of arbitrary length in a string of predefined length. The hash functions play an essential role in cryptography and for the creation of digital signatures

[17] File System. In computer slang, it identifies a mechanism with which the files are organized and stored in a mass memory, like a hard disc or a CD-ROM. It also identifies the total of the types of data necessary for the memorization (writing), the hierarchical organization, the manipulation, navigation, access and the data reading.

[18] Payload. It is a runtime (moment in which a computer programme is performed) present in a computer virus that extends the functions beyond the infection of the system. Payload means, therefore, any fixed-time operation, random or activated by a command contained within a virus or worm. The action of Payload can be partial or total destruction of information, its unauthorized diffusion, the sending of emails to all the users of the contacts book and similar actions.

well as plug-ins [19] used to resume the control of previously compromised computers, which can be partially disinfected.

7 Spreading. These are modules that permit the scanning of the hosts (terminals connected to the network, usually a computer) of a local network, infecting them through the use of credentials already previously extracted or to organize attacks that are based on the points of vulnerability encountered. A typical example of attack is that directed against the routers [20] to acquire the routing tables of the data packages transmitted on the network.

8 Mobiles. These innovative and fearsome modules are able to copy all the information present in the smartphones that interface with a network using any mode of data transmission. Some modules can verify whether a device is 'jail broken' [21] and use the function to introduce malware.

9 *E*xfiltration. These are modules that intercept and extract all the data memorized on the mass storage devices of the FTP type server (computer identifiable as file server, used to convey and memorize various data shared on the network), to then relay it to C&C servers). Usually these modules are activated after the action of those modules that fall under the Recon category.

10 USB Infection. Even though there has not been any effective feedback on their ability, it seems that these modules were created to attack directly the USB units [22], sending viruses onto the devices connected via these interfaces.

The most particular fact about the Sputnik malware is the very high level of sophistication of the applications, an element which confirms the existence of an infrastructure of extremely highly specialized informatics technicians, directed by team leaders (in this case, Intelligence experts) able to supply precise indications on the type of actions that the applications must conduct, besides individuating the target to be hit.

[19] Plug-in. It is an autonomous programme that interacts with another programme to increase the functions (for example, a plug-in on a programme of writing that allows activating a function for which another programme is necessary).

[20] Router. Corresponds to an electronic device which, within an informatics network, deals with routing the data, sub-divided into packages (data packages) among different networks.

[21] Jail breaking. It is a procedure that permits the installation on a device (type smartphone) applications which allow acquisition of programmes alternative to those present on the device (for example, alternatives to the App Store). After having made the jail break on the device, the users can install numerous applications, which are not available through the App Store.

[22] USB. Universal Serial Bus

In essence, it is simply inconceivable to consider that behind such a complex and detailed operation is hidden a puny little group of hackers searching for excitement, or an isolated group of independent cyber-criminals in the pay of the highest bidder. Behind Red October lies an impressive hierarchical infrastructure of a military kind; structured in sections, areas of expertise and personnel of different specializations, able to define specific objectives, target actions and objectives to be achieved. A complex infrastructure of these dimensions must also be able to count on a good deal of financing, indispensable for the acquisition of informatics devices of very high performance and particularly innovative.

It is also improbable that such a complex and huge structure could escape the attention of governmental and institutional bodies. Consequently, one has to deduce that an apparatus of Cyber Espionage, such as that which realized Red October, could not operate without the direct collaboration, if not absolute integration with governmental structures or organizations that operate in close contact with a State.

Who is behind Red October?

Red October can be considered the first authentic programme developed for actions of the spyware type, that is, able to conduct actions of espionage on the Net.

The most particular fact lies in its ability to steal 'classified' data and not common data banks of little interest. The suspicion that derives from this consideration is that behind this fearsome digital Intelligence instrument can be concealed the Secret Service of a Country particularly advanced in the Cyber Intelligence sector.

Although at this moment the 'customers' and the 'authors' of the attacks are still shrouded in mystery, some clues leak out from the code of Red October. First of all, between the lines of the programme, it is possible to read words like 'zakladka' (Russian term used to identify a bug), or 'proga (also Russian for the word programme), which hint that behind the group of developers of the 'malicious' code are hidden crackers of Russian nationality. Sergei Nikitin, informatics security expert of the Government of Moscow, believes that the programme was commissioned by "an Intelligence Service that hired programmers through forum in the Russian hacker community". But it could also be a simulated action to lead the analysts to completely erroneous conclusions.

The opening of a new market of professionals of the digital war is certainly not something new. The digital mercenaries (cyber-mercenaires), represent the new 'soldiers' of the international informatics terrorism of the third millennium. In preference to weapons and explosives, they opt for the keyboard and the mouse which, as well as being inexhaustible - unlike weapons - they are vastly more economical and guarantee damage that can be more effective and

devastating than the most sophisticated and costly weapons on the market.

But let's return, for a moment, to examine the architecture of Red October. If we analyze it carefully, we can reach the conclusion that it is the first operation that envisages the interaction between cyber-spies and cyber-criminals at a transnational level. Why? Let us try to understand this by retracing some of the focal passages.

First of all, let us start from the methodology of attack and infection. In September 2012, thanks to a vulnerability of the navigation browser of Internet Explorer of Microsoft ('IE zero-day' exploit), numerous computers across the world are attacked and the actions campaign of cyber-crime presents similarities to a previous attack which goes back to July of 2011.(figure 3)

In this 'campaign' of attacks, named 'Nitro' by Symantec, approximately 48 companies are infected and they are all operating in the sectors of chemicals, advanced materials and defence. Symantec identifies in 'Poison Ivy' the Trojan[23] author of the attacks and attributes the paternity to Chinese hackers.But

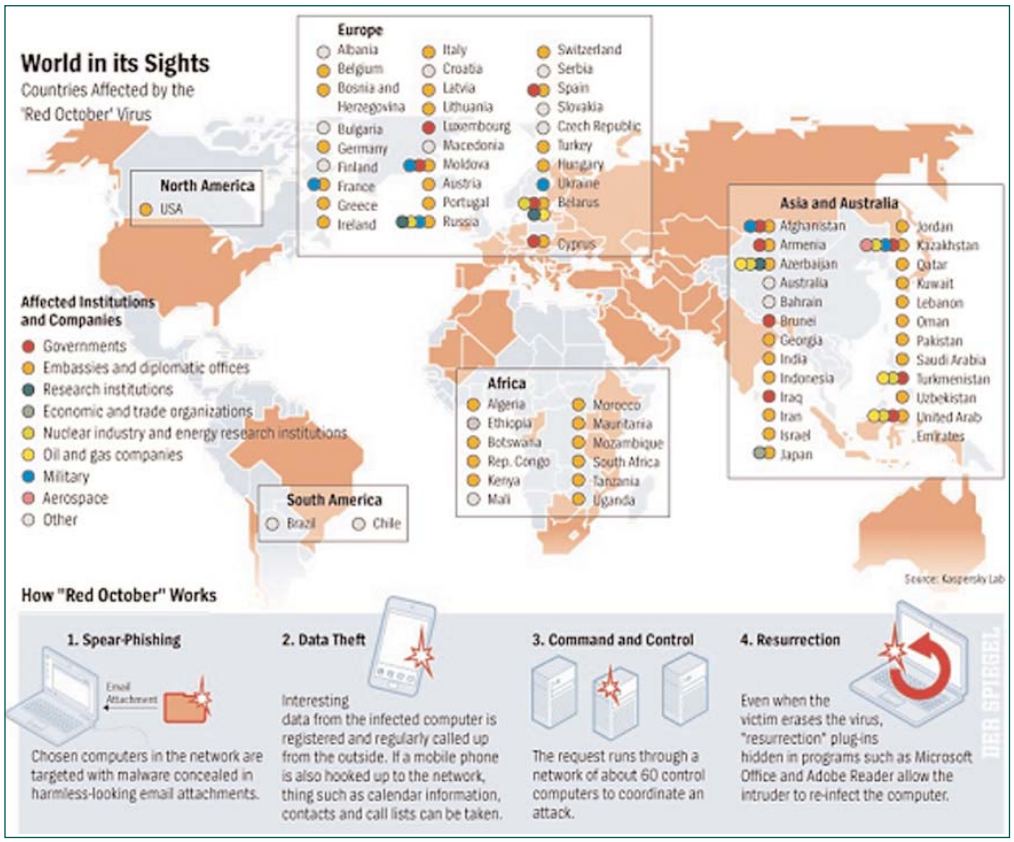

Figure 3 - *Countries affected by Red October*
(source: www.spiegel.de/international/spiegel/bild-879467-453013.html)

the People's Republic of China categorically denies that the attacks could have started from servers located in their Country.

Returning to the exploit 'IE zero-day', Symantec confirms in a communique[24] that the utilization of the vulnerability should be viewed in the context of the continuation of the Elderwood project. Showing up for the first time in 2009, with attacks directed against Google (Operation Aurora), Elderwood is a platform rich in malware, capable of attacking multiple targets aimed at the intrusion of the systems and the theft of data. The Elderwood objectives have all been individuated within the supply chain and services in the Defence sector, reaching as far as the government sites attached to them.Figure 4

As far as the attacks are concerned, no exceptions are made for those organizations that protect human rights or the non-government organizations (NGOs) that have active contacts or interactions with government structures of the Defence.

As far as the attacks are concerned, no exceptions are made for those organizations that protect human rights or the non-government organizations (NGOs) that have active contacts or interactions with government structures of the Defence.

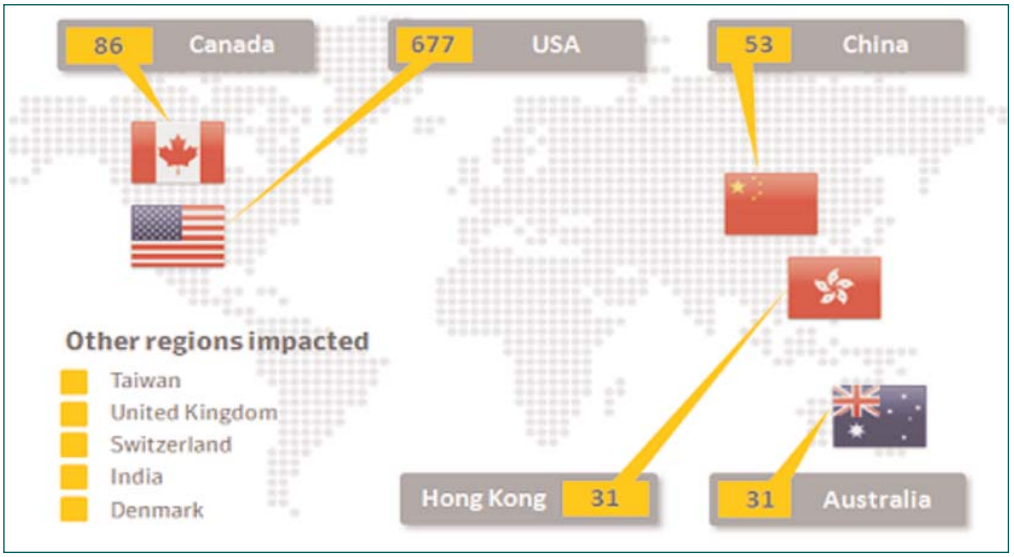

Figure 4 - *Number of files used for attacks carried out by Elderwood worldwide*
(source: www.symantec.com/connect/blogs/elderwood-project)

[23] Trojan. Trojan or Trojan Horse is a kind of 'malignant' code that hides its functionalities within an apparently useful programme. Therefore, the user who installs, unknowingly, an apparently innocuous, well-known programme, installs and perform also the 'malignant' code that nestles inside.

[24] *www.technewsdaily.com/16217-ie-zero-day-china.html*

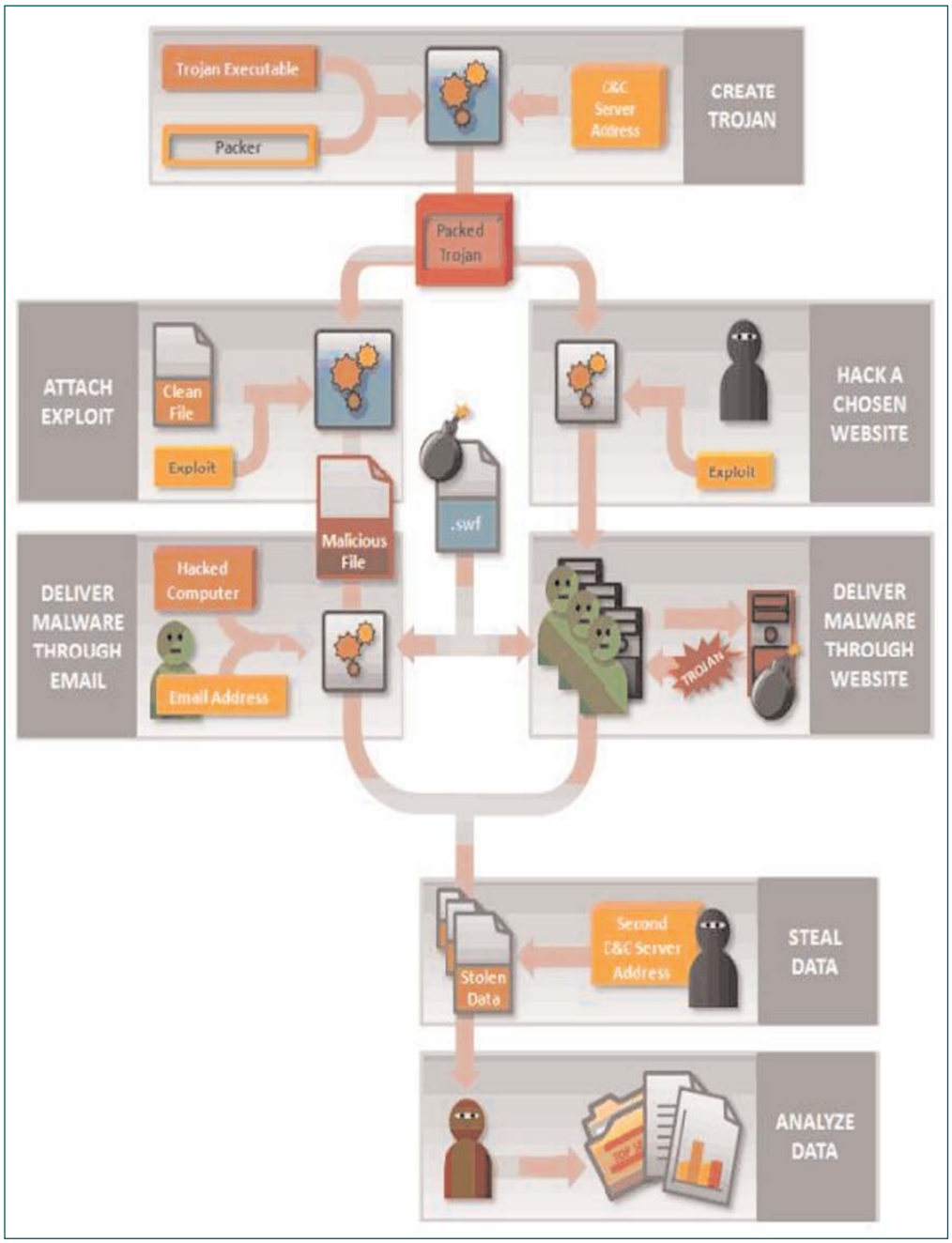

Figura 5 - *Operation of the Elderwood platform*
(source: www.symantec.com/connect/blogs/elderwood-project)

After this, all the information collected is analized. Another technique used to steal information, is that of the 'watering hole'. It functions according to the tested scheme of the feline that awaits its victim in the proximity of a water hole. The attacker tries to identify a web site particularly used by the victim. After he has identified it, he attacks, penetrates the victim's defences and injects the 'malicious' code.

The virus, which is programmed to identify its victim, awaits the moment that the latter accesses the web site. As soon as this happens, the virus attacks. Therefore, only at the moment the unfortunate user accesses the system, the virus activates a mechanism of penetration and bypasses the defense systems. Once the informatics system is violated, a new Trojan is activated, which spreads in a network between the computers connected to the victim.

The Elderwood group has conducted at least 678 attacks against 216 American organizations and 86 attacks directed towards Canadian organizations.

Many Australian (thirty-one), United Kingdom and Indian systems have been attacked, but this time China has not been excluded, with 53 identified attacks, of which 31 in Hong Kong alone.

Who then is behind the Elderwood project?

Is it an emerging Country that is trying to experiment its technological capacity or is it a skillful maneuver of 'intoxication' of the information on the virus victims?

In February 2013, Eugene Kaspersky, great patron of Kaspersky Lab, European leader in the development of solutions for informatics security and the management of threats, was nominated 'Influence of the Year 2012' by Channelnomics[25] for his vision and competence in the IT security and, perhaps, because he was able to install his applications on a pool of users that can boast the legendary 300 million threshold.

His curriculum (which can be acquired from the Network), certainly stands out for the Degrees he obtained in Cryptography, Telecommunications and Computer Science, but, perhaps, also because he achieved these academic qualifications studying in a British Institute, co-sponsored by the Ministry of Defence and the KGB.

Therefore, it is not particularly surprising that Kaspersky Lab is among the few companies authorized by the Federal Russian Security Services (FSB) to sell anti-virus security software to the Government and to the Agencies closely connected to it[26].

Furthermore, it should not be forgotten that it was his own company that analyzed the Stuxnet virus, which in 2010 infected the informatics sy-

[25] *http://channelnomics.com/*

[26] *http://mytech.panorama.it/kaspersky-putin-spie-kgb-pussy-riot*

stems of the Iranian nuclear power plants, blocking their function. After this last virus and its direct successors Flame and Gauss, suspicion lingers concerning possible collaboration between different Intelligence agencies of pro-Western government

Probably, it is precisely because of these fears of possible transnational alliances in the Cyber Defence, that news released by the Strategic Intelligence News[27] confirms the collaboration of Kaspersky Lab with the Kremlin in order to cope with certain attacks originating from African Countries (among which, Kenya), but that in reality, they seem to come from Countries hostile to the Russian Government.

A further oddity which can be added to this maintains that among the victims of Red October were some African Countries, such as Kenya, Uganda, Ethiopia, Chad, The Sudan and Eritrea. To make plain and simple speculations in the Intelligence sector, however, can lead to rapid and erroneous deductions. We must not forget that in the report of Red October victims, Russia appears at the very top of the list!

As is shown in Figure 2, it is clear that some Countries of South-East Asia (among which, China), were not given any attention by Red October.

But it is also true that neither were the informatics systems located in other Countries, such as Canada or Mexico, objects of attack.

In light of all this, President Barack Obama, on the 12th of last February, decided to sign a new executive order[28] to strengthen the informatics security at a national level.

The objective is to ensure that the United States companies, and, in particular, those of strategic importance, share a series of information produced by the federal agencies, on any recent informatics threats and the risks derived from the use of the digital technologies.

The programme Enhanced Cyber security Services will be extended also to the societies that work in the sector of the digital infrastructures, in order to expand efforts to combat cyber-crime

Nothing is what it seems!

It is, perhaps, the oldest rule of the Intelligence sector: nothing is what it seems. Probably on this very rule a more careful analysis could be based on the possible origins of Red October. The events, the information, the news that assails us daily and contribute to fill that information container that should transform itself into individual knowledge, often, instead, contributes to increase that mental confusion (information overload) that leads us to considerations and conclusions which are completely erroneous. And also in this case,

[27] *http://intelligencebriefs.com/?p=3308*

[28] *.www.corrierecomunicazioni.it/it-world/19607_obama-vs-cybercrime-ordine-esecutivo-sull-it-security*

the information available to us could be incomplete, distorted or conveniently manipulated to induce us to mistaken convictions.

Let us try to include a new element of analysis In June 2012, according to a Space Daily[29] report of 2012, South Korea accused North Korea of having activated an 'elite team' of hackers capable of stealing military secrets to foment public disorder within the Seoul Government. "North Korea is trying steal military secrets and paralyze our defence and information system, utilizing specially trained experts to intrude in our military information network". These are the words of the Defence Security Commander of the Seoul Government, Bae Deuk-Shik, in a security conference, adding that the North had tried to "foment social disorder, to paralyze our basic infrastructure through cyber-terrorism, which can cause enormous damage in a very short time".

Professor Lee Dong-Hun of the Korea University confirmed, during the forum, that also the Pyongyang Government had instituted a 'special unit', about 3,000 hackers strong, controlled and directed by the same leader of the Country, Kim Jong-Un.

But the Professor went much further, even affirming that "North Korea is the third most powerful nation in cyber-war in the world, after Russia and the United States".

It would appear, therefore, that China with its economic, scientific and infrastructural potentiality, is inferior to North Korea with regard to its structures, technologies and professionalism dedicated to the cyber-war.

According to what has been published in the international media from 2009 to 2012, many South Korean sites, with particular attention directed to those pertaining to the finance sector, (bank etc.) have been attacked by malware of the DDoS type[30], thanks to the cooperation of university students recruited in the University of North Korea.

Obviously, Pyongyang accuses Seoul of inventing the accusation. In the same year, between April and May, Seoul again accused North Korea, this time of having utilized radio signals for jamming actions.

It seems to be true, however, that for some years now, a core group of 'élite crackers', specialized in cyberware, has been in operation, and to this we can add the further cooperation of circa 10,000 graduates in the technical and scientific areas, who come from the Kim IL Sung University. The structure of 'élite' are to be found within the 'Room 39' (also known as Bureau 39, Division 39 and Office 39), a very secret organization directly responsible to the Pyongyang Government, specialized, above all, in audacious and reckless financial operations on the international markets. It would even seem that this structu-

[29] *www.spacedaily.com/reports/S_Korea_military_accuses_North_of_stealing_secrets_999.html*

[30] DDos (Distributed Denial of Service). In informatics, a Dos (Denial of Service) corresponds to an informatics attack which aims at the negation of a service. The functioning is based on the attempt to deactivate a service offered by an informatics system (for example, a web site). A variant of this type of attack is the DDoS which, functioning in the same way, tries, however, to conduct the attack utilizing numerous computer attackers which, together, constitute a botnet.

re, reporting directly to Kim Jong-Un, deal with multiple confidential activities, among which, the programme of the development of nuclear weapons. Nevertheless, the well-known isolation prevailing in North Korea almost totally impedes ascertainment of this information. It should be underlined that North Korea is another of those Countries that came out unscathed by the Red October attacks. In this regard, one could elaborate easy guesswork with respect to the paternity of Red October, but if we look closely at the geographic environments where the attacks took place, we can detect that also many Countries geographically situated in another continent were excluded from the cyber-attacks.

It is the case of the African Countries, which could be considered 'devoid of technology' because of their proverbial technological backwardness and chronic scarcity of means, but also in this case one risks committing a gross error of evaluation of the actual effective potential. Contrary to what one might imagine, for some time now, many African Countries have begun to organize for their entrance and, above all, their 'role' in the Cyberspace.

Already for several years, in many of those Countries considered 'hot' (from the Middle East to Africa), where the investments were mostly concentrated on the purchase of armaments and military technologies, a new voice is beginning to be heard in the balance of the national expenditure: the Cyber Defence.

Examples are not lacking: Kenya has announced[31] that it will assign to each user of the Network, a virtual identity to stem the growing phenomenon of cyber-crime. But Bitange Ndemo, Permanent Secretary of the Ministry of Information and Communications of Kenya, stated "We are moving rapidly towards the automation of all information, since the informative systems must be protected against certain people with bad intentions". He made this statement at the East African Cyber Security Convention of 2012, an event on informatics security where almost all the Countries of the African Continent participated with great interest. Ndemo also said that following the numerous informatics attacks suffered in the course of the recent months against banks and communication and data transmission companies, he is realizing an ecosystem of cyber security within the Communication Commission of Kenya (CCK), which has the mission of combatting the informatics threats coming from the Cyberspace.

But what should never be forgotten is that a Cyber Defence structure can also carry out actions of Cyber Intelligence. Many people think that the best way to address the problem of Cyber Defence is that of transnational cooperation. And it is precisely with this conviction that since 2011, the United States and the European Union have been experimenting the path of joint cyber-security. A first experience consisted in the realization of the 'Cyber Atlantic

[31] *www.businessdailyafrica.com/Corporate-News/-/539550/1624124/-/yi8poj/-/index.html*

2011' exercise, which saw the cooperation between the European Agency, ENISA (European Network and Information Security Agency) and the US Department of Homeland Security.

Altogether there have been 20 Countries involved in cyber-attack simulations, management of crisis scenarios from attacks on critical structures coming from the Net, theft of data from informatics systems, and attacks on energy infrastructures.

Other Countries, instead, are convinced of the contrary, i.e. that the sharing of technological resources and expertise, could be 'inconvenient' in an intrinsically unstable world, in which even the most solid collaboration or the historical bonds of friendship can fail or disappear because of additional needs tied to the continual changes that occur in the world at the economic, political and social level.

In conclusion, behind Red October there could lurk unidentified dark forces or, much more simply, synergic actions by Countries that are interested to steal information which they consider vital for their survival, in a world governed by the 'social-economic-productive globalization'.

Information is power, and to assume a position of importance at world level the continual acquisition of information is essential, which must be accompanied by the direct control of same.

But since information is becoming increasingly digitalized, one must be equipped with the instruments and human resources which are able to intercept it where it is produced and acquired: the Cyberspace

Bibliografia

http://www.spiegel.de/international/spiegel/how-russian-virus-hunters-tracked-down-a-global-espionage-network-a-879467.html

http://www.matthewaid.com/post/42178624483/red-october-spyware-system-used-sophisticated

http://www.csmonitor.com/USA/2013/0115/Digital-fingerprints-on-Red-October-spyware-point-to-Russia-or-do-they/(page)/2

http://www.technewsdaily.com/16373-red-october-spyware.html

http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

http://arstechnica.com/security/2013/01/why-red-october-malware-is-the-swiss-army-knife-of-espionage