MALWARE FOR MOBILE DEVICES AND THEIR SECURITY

PhD, Ştefan IOVAN[1,2], Student, Ramona MARGE[3]
[1] The West University of Timişoara, Computer Science Department, ROMANIA
[2]Railway Informatics SA, Bucharest, ROMANIA, stefan.iovan@infofer.ro
[3]Oradea University, Mathematics Faculty, ROMANIA, ramona.marge@yahoo.ro

Abstract: *One of the most interesting theories launched in the software industry presents the following aspect: software applications alter purposes, consumption behaviors and everything related to motivation. And this is extremely obvious where mobile phones replace personal computers by the numerous applications offered by the mobile gadgets to users. Companies adopt complex security solutions, but hackers use more and more the concealment technique, creating a complex code difficult to analyze. The more complex the concealment, the longer it takes until the antivirus solution neutralizes the malware code, leaving hackers enough time to steal more money. Experts explain the danger behind the loan tenders sent as spam, especially if users reply, and experts also give some useful tips for users to prevent them from becoming the victims of these merciless financial organizations and Internet scams [1, 2]. The paper presents certain aspects regarding computer/cybernetic attacks on company data, information, applications, systems, with the help of mobile devices. The subject is vast and generous and this paper will discuss only aspects from the field of cybernetic security.*

Keywords: mobile devices, mobile applications, device malware, banking Trojans, Android vulnerabilities;

1. Introduction

We will present the results of an analysis regarding the scenery of threats for mobile devices. In 2016 almost 145000 new malware programs were detected for mobile devices, three times more than in 2015 when 40059 samples were discovered. In 2017, the malware programs identified are almost 190000 malware samples for mobile devices.

98.1% of the total of malware files for detected mobile devices was created to attack devices which operate on the Android operating system. Approximately 4 million malware applications were used by cybernetic hackers for spreading mobile malware on Android devices. Between 2015 and 2016, 10 million applications were detected containing malware for Android.

The first five countries with the largest number of attacked users: Russia (40%), India (8%), Vietnam (4%), Ukraine (4%) and Great Britain (3%). In 2015, the malware samples for mobile devices targeted the users' money. The number of malware alterations for mobile devices created for phishing activities, information theft related to bank cards and for money theft from bank accounts increased almost 20 times. 2500 infection attempts with banking Trojans were blocked [3].

Banking Trojans are by far the most dangerous type of mobile malware for users. A part of the threats detected in 2015 were oriented towards money theft from bank accounts rather than from the account for the victim's mobile device, which significantly increases the potential losses.

The vulnerabilities of the architecture of the Android operating system and its increasing popularity are important aspects which supported the evolution of the number of banking Trojans for Android in 2015. The cybernetic hackers seem to be extremely focused on this

method of making money: at the beginning of the year there were only 67 known banking Trojans, but until the end of 2015 *Kaspersky Lab* owned 1321 individual samples.
Today, most attacks which use banking Trojans target users from Russia and from The Commonwealth of Independent States. However, it's highly unlikely that this situation lasts, due to the special interest of the cybernetic hackers for the users' bank accounts, the activity of the banking Trojans for mobile phones is estimated to increase in other countries too in 2016. We already know about *Perkel*, a Trojan for Android which targets clients of many European banks, as well as the Korean malware program *Wroba*.
Hackers use more and more the concealment technique, creating a complex code difficult to analyze. The more complex the concealment, the longer it takes until the antivirus solution neutralizes the malware code, leaving hackers enough time to steal more money. The methods used to infect a mobile device include the compromise of the valid sites and the spreading of malware programs through online alternative and bots stores (bots usually proliferate by sending text messages with malware elements to the contacts from the victim's contact list).
The Android vulnerabilities are used by hackers to consolidate the rights of malware applications, which significantly extend their abilities and make the elimination of malware programs more difficult. In order to elude the process of inspecting the code's integrity when the user installs an application, the hackers use the *Master Key* vulnerability.
Due to the fact that eliminating an Android vulnerability is possible only by receiving an update from the device's manufacturer complicates the situation even more. If a smart phone or tablet was launched more than a year ago, it's likely that the device is no longer kept by the manufacturer and the vulnerability patches are no longer supplied. In this case, the only help comes from an antivirus solution.

2. Cybernetic threats for mobile devices

The prognosis for cybernetic threats for 2015 was confirmed and experts concluded that all the three main forecasts regarding final users have been confirmed. Therefore, the experts stated that cybernetic hackers will target:

- The users' privacy **-** leading to a larger popularity of VPN or Tor services. The number of users who targeted Darknet in their attempt to protect their personal data increased. However, besides the good faith users, Tor continues to attract *"evil forces"* – anonymous networks which can camouflage the malware activity, performing trading activities on illegal sites and money laundering. For example, experts detected the first Trojan for Android, which uses a field from the pseudo-area *.onion* as control and command center.

- The users' money. Experts expected that cybernetic hackers will continue developing tools to collect money. Their expectations were confirmed by detecting *Trojan-SMS.AndroidOS.Waller.a*. It is capable of stealing money from the *QIWI* e-wallets belonging to the holders of infected smart phones. The Trojan targets only users from Russia, but it is capable of extending anywhere, the e-wallets being managed by SMS. The cybernetic hackers also used standard approaches such as Trojans for mobile platforms, which steal money with the help of malware spam. In this case, the range is much more extended – for example, *Faketoken*, the Trojan for mobile platforms affected users from 55 countries, including Germany, Sweden, France, Italy, Great Britain and USA. The number of Trojans – tracked in a trimester – for the mobile banking systems almost doubled – from 1321 to 2503.

- Bitcoin. Experts expected the significant growth in the number of attacks which target the users' *Bitcoin* wallets, the bitcoin reserves and the exchange platforms. Many incidents which confirmed this forecast were recorded. Among the most notable is the attack

over *MtGox*, the largest exchange platform for *Bitcoin*, the attack on the personal account and the *Reddit account of the MtGox CEO, Mark Karpeles*, and its use to publish *MtGox2014Leak.zip*, which proved to be a malware capable of searching and stealing the victims' *Bitcoin* wallets.

In the attempt of adding to the illicit winnings, the cybernetic hackers infect computers and use their resources to generate more digital currency. *Trojan.Win32.Agent.aduro*, the 12th most frequently detected malware instrument online is an example of Trojan used in this type of action. In the first trimester of 2014, a major cybernetic espionage incident was recorded – *Kaspersky Lab* published a report about one of the most advanced threats, called *The Mask - Caretto*.

The main target was the confidential information belonging to the state agencies, embassies, energy companies, research institutes, private investment companies and activist organizations from 31 countries. According to the researchers, the complexity of the tool set used by the attackers and a series of other reasons suggest that it might be a company sponsored by a state [1].

Besides the new incidents, we noticed a follow-up of the companies which appeared to be terminated. For example, after the cybernetic hackers closed all the known command servers involved in the *Icefog* operation, a Java version of the threat was detected. The previous attack mainly targeted organizations from South Korea and Japan, but the new version had only targets from USA, judging by the tracked IP addresses.

33.2% of the users from the world confronted with at least one web-based attack in the first three months – a decrease with 5.9% in comparison to the same period from last year. 39% of the neutralized web attacks were enacted with the help of web malware resources located in USA and Russia; the total number for the two countries was higher with 5% than the first trimester. They were followed by Netherlands (10.8%), Germany (10.5%) and Great Britain (6.3%).

2.1. Android malware applications

Android - the operating system for mobile devices – has over 10 million malware applications, according to researchers in recent reports. The researchers declared that by the end of 2014, they discovered over 20000 individual malware samples for mobiles in Google Play and other resources, used and repackaged under different applications.

On 30th of January 2014, the official Google Play market offered 1103,104 applications. Researchers identified 10 million problematic applications, taking in consideration that cybernetic hackers also use valid Android software to transport their malware codes.

Researchers reported that the number of malware samples increased with 34% from one year to the next. Two months before, the researchers recorded over 148000 malware samples in one month. Until that date, researchers collected 8260,509 individual malware installation packages. For example, the total number of malware samples from the *Kaspersky* collection (an antivirus company) is 148778, 104421 being discovered only last year.

The most outstanding element from the mobile malwares in 2013 was *Obad*, which was spread through different means, including a default botnet. Android smart phones infected with *Trojan-SMS.AndroidOS.Opfake.a* are used as multipliers, sending text messages which contain malware links to each person from the contact list of the victim's device.

This was a popular practice in the PC (***P**ersonal **C**omputer*) threat scenery and it's a popular service offered in the underground economy of the cybernetic hackers. Researchers discovered that in most cases, the malware targets the financial information of the user, most

Android malware applications being developed in Russia.
For example, this was the case of the mobile version of *Carberp Trojan*, which originates from Russia. It steals the users' authentication data when they are transferred to the bank's server [4]. Last summer, researchers signed an agreement with the *Qualcomm*, the mobile chip manufacturer, for improving the "*inferior*" security of the mobile operating system of the smart phone.

2.2. Actual costs for phishing prevention

Avoiding future phishing attacks requires intelligent people and costly technologies to analyze the server journals. Within the *InfoSecurity Europe 2014*, people discussed the way in which the *BBC* organization faced an attack from the *Syrian Electronic Army*.
People admitted that most of the work involves matching the patterns. It requires very intelligent people and expensive technology. In order to face the incidents you must manage the journals therefore their storage and keeping is absolutely essential.
BBC externalized a large amount from IT, therefore it was extremely important to involve the contractors in the fight against an attack. *BBC* also has an incident commander, who takes quick decisions and is the main link with the external business teams.
The partnership with the contractors and other third parties in order to understand the environment and to have broader mapping services is very important. Security is a matter of technology and also people. In order to fight off future attacks, *BBC* created a *flag pole*. This allows the identification of a phish attack and the blocking of the phishing attack field and then setting a search to erase the phishing messages from the inboxes.
While this type of approach is suitable for desktops and laptops, it's necessary to keep in touch with the mobile users, considering that the mobile devices are generally outside the corporate IT control.

2.3. Credit spam – data theft, Trojans and Bible quotes

Experts explain the dangers behind the loan tenders sent as spam, especially if users reply and experts offer some useful tips for users to prevent them from becoming the victims of these merciless financial organizations and Internet scams.
Spam creditors are costly and dangerous. Small organizations and private creditors which are often not capable of competing on the same level as the marketing companies of large multinational banks often turn to organizations whose services prove to be much more expensive than mentioned in the advertising.
Regular online scams also include credit spam. In order to collect information about the victim, the credit spam pretends to offer assistance for acquiring a loan and requires a password of the online banking system, the inspection code of the card, the passport or the user's contact information. For example, this information may be used for concluding false documents.
The tools preferred by scam creditors are phishing and malware files. Phishing represents the attempt of stealing the user's financial information using false web pages which imitate the official request format of renowned banks and the attached malware files contain forms which imitate the request forms for loans or approved credit contracts.
If you replied, the inbox will be filled with more spam messages. Any reply to a spam e-mail, even if you don't intend to use the services offered in the advertising, gives the spammers certainty that the e-mail address is real and it's actively used (certain spammers send messages to randomly generated contact lists). Therefore, the number of advertisements sent

from the "*exposed*" e-mail account will increase significantly.
We notice that hackers turn to all kinds of tricks to deceive users [5]. Some senders pretend to be charity or religious organizations, which help people in need. Such messages may also include Bible quotes in order to seem more convincing.
Others want to attract potential clients, promising them large sums of money (sometimes up to a few millions of euro in cash), granted on a short period of time (from a few hours to a few days), without bonds or guarantees, without an income certificate and with minimum necessary documents. Any attempt of opening an attached contract may lead to the system's infection and the loss of the data stored on the hard disk.

2.4. Hotspots and free wi-fi present data risks

Sensitive information may not be sent through hotspots public wi-fi in order to prevent their theft, warned Europol. People must send personal data only through reliable networks. We initiate this warning due to the increase in the number of attacks performed through the public wi-fi.
We noticed an increase of the abusive use of wi-fi for information, identity, and password or money theft from users which use public or insecure wi-fi connections. We should teach the users that they must not send sensitive information while on an insecure wi-fi network, but from home, where they know the wi-fi network and its level of security.
Europolul, which helps coordinate the investigations regarding organized crime in Europe, assisted a few member states which discovered attacks performed on the wi-fi networks. The attackers did not use new techniques, but relied on popular approaches which try to deceive people to connect to a hotspot which is superficially to the ones from coffee-shops, restaurants and other public areas.
The attacks imply the fact that the data exchange in the case when people communicate with a bank or a store through the web or when they connect to social media sites may be captured by attackers. Everything sent by wi-fi is potentially risky and we have to be concerned with this as individual users and as police authorities.
The Europol warning comes only a few months after the European Parliament stopped the wi-fi public services, having discovered a "*man-in-the-middle*" attack being performed through the service. As it results from the name, in this type of attack, thieves try to place in between the users and a hotspot to collect all the data exchange between the two points.

3. Conclusions

In the future, users may benefit from anti-malware extended protection abilities, including detection and blocking, constant analysis and retroactive remediation of advanced threats [7, 8]. This improved security tender represents one of the first results of the integration efforts from the security solutions, which extends the advanced malware protection for 60 million clients of *Cisco* solutions, large and medium companies.

The security solution uses vast security information networks, available in cloud. Therefore, they offer constant monitoring and analysis for the extended market, but also before, during and after the end of the attack process. By combining the expertise from the analytical field and the field of advanced threats with the Email and Web security solutions, clients benefit from visibility and control, as well as from a complex approach in facing advanced malware attacks.

The solution also includes the *Cognitive Threat Analytics* module, integrated in the portfolio last year as optional solution. *Cognitive Threat Analytics* is a very intuitive system

which uses the behavioral pattern and disturbance detection to indentify the malicious activity and to decrease the time for discovering the active threats from inside the network.

Adding advanced malware technologies to the *Web and Email Security* solutions, as well as the *Cognitive Threat Analytics* module to the present solution extended the ability to provide security solutions more oriented towards threats. This is possible by extending the coverage of the attack vector by providing advanced anti-malware protection anywhere a threat is present. By this integration, *Cisco* addresses the largest range of attack vectors from the extended market.

The multitude of attacks as well as the high level of complexity requires security solutions which offer constant monitoring, analysis and protection for the extended network before, during and after an attack [9]. By adding the *threat analytics* module, the solution offers a series of securities much more oriented towards threats, capable of providing malware advanced protection from cloud and the network to endpoint device, therefore addressing the largest range of attack vectors from the extended network.

References

[1] IOVAN, Şt. şi IOVAN, A.-A. (2016) *FROM CYBER THREATS to CYBER-CRIME*, Bucureşti: Editura Universitară, *Journal of Information Systems & Operations Management*, (***JISOM***), Vol. **10**, No. **2**, ISSN: 1843-4711, pg. 425 - 434;

[2] Adams, A. (2005). *Review: Cyber Ethics: Morality and Law in Cyberspace*, International Journal of Law and Information Technology, **13(2)**, 289 -291;

[3]] * * * , (2013*) Evoluţia malware-ului pentru dispozitive mobile: 3 tentative de infectare per utilizator în 2013,* http://www.agora.ro/stire/evolutia-malware-ului-pentru-dispozitive-mobile-3-tentative-de-infectare-utilizator-2013#_ftn1 (accessed in sep 2017)

[4] IOVAN, St. si MARGE, R. (2017) *Some Legal Aspects on Cybercrime*, Targu Jiu: "Academica Brancusi" Publisher, *Annals of the "Constantin Brancusi" University, Engineering Series,* Issue **3**/2017, (***CONFERENG 2017***), ISSN: 1842 – 4856, pag. 181 – 186;

[5] IOVAN, St. (2015) *Big Data Security Problems*, Proc. of 16th European Conference (***E_COMM_LINE 2015***), Bucuresti, Romania, ISSN: 2392-7240;

[6] IVANUS, Cr. si IOVAN, St. (2017) *Cybercrime in the European Union*, Targu Jiu: "Academica Brancusi" Publisher, *Annals of the "Constantin Brancusi" University, Engineering Series,* Issue **3**/2017, (***CONFERENG 2017***), ISSN: 1842 – 4856, pag. 187 – 192;

[7] Kaspersky Lab, (2016). *Kaspersky Internet Security – Multi - Device,* http://www.kaspersky.ro/internet-security-multi-device (Accessed in July 2016)

[8] IVANUS, Cr. si IOVAN, St. (2015) *Internet – The Foundation for the Future Societies Permanently Connected,* Proc. of 16th European Conference (***E_COMM_LINE 2015***), Bucuresti, Romania, ISSN: 2392-7240;

[9] European University Institute, (2013), *Code of Ethics in Academic Research* (2013 Edition), Italy: European University Press. Retrieved from http://www.eui.eu/Documents/ServicesAdmin/DeanOfStudies/CodeofEthicsinAcademicResearch.pdf (Accessed in August 2016)