

Exploitation of Android Mobile Malware in Phishing Modus Operandi: A Malaysia Case Study

Sharifah Roziah Mohd Kassim, Wira Zanolamy A. Zakaria & Nur Mohammad Kamil Mohammad Alta
MyCERT, CyberSecurity Malaysia
Level 7, Sapura@MINES, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
{roziah, wira, kamil}@cybersecurity.my

ABSTRACT

Phishing has evolved over the years with new techniques, beginning with simple URL manipulation, followed by vishing, then spear-phishing, causing huge monetary loss to financial institutions and Internet banking users around the world. Mobile devices are seen as a new perfect vehicle in phishing campaigns by attackers as they are widely and increasingly used. In this paper, we studied a phishing modus operandi that uses Android mobile malware, Zitmo, which is a variant of Zeus family, in operating successful phishing campaigns targeting Malaysians. This study includes analysis of the behaviour of this variant, its tricks and tactics in manipulating victims. The tools and codes that we developed to conduct the analysis and investigation for this incident are discussed in this paper. The result from this study proposes a mitigation and response recommendation for IT users and organizations in responding and mitigating phishing incident.

KEYWORDS

Phishing Campaign; Phishing Malware; Malware; CERT, Zeus, Zitmo

I. INTRODUCTION

In the age of mobile computing, smart devices and smart applications (or abbreviated as ‘apps’), users and businesses communicates seamlessly. From day to day, this mobile gadgets are getting more and more capable of doing the stuff that we normally do on a PC or notebook. This is of course supported by the existence of the Internet, which promotes the migration of many types of

businesses to move into the Internet realm. Fast interaction, availability, time and cost effective are some of the contribution factors for this scenario. We can see many types of services offered on the Internet, this includes banking, government, education, retails, entertainment, news, job-matching, cloud storage, to name a few.

Almost fifteen years back, we interacted with the online banking website for instance, by using a web browser on a PC or notebook. But nowadays, after the introduction of smartphone and tablets, there is an expanding trends of development of mobile applications or mobile apps that represents a new way of interacting with web applications. A smartphone or tablets preinstalled with a mobile banking app made personal banking even more easier. Any users that have access to Google Play Store or Apple Store, can install the app on their devices in order to assist them in their banking activities.

Malware, is a term coined from the word ‘malicious’ and ‘software’. It is a piece of software that are built with the intention to do harm to the user, network and computing resources including [1-5]. Mobile malware is not a newly created threat. It has been around since the Symbian age. In history, it is reported that a proof-of-concept malware named, Cabir, were released in 2004 [1]. Nowadays, with the increasing number of mobile devices consumers, mobile platform is becoming an interesting target for this kind of threat [6]. This is one of the reason on why there is a rapid increase in the number of reported malware cases. Malware poses one of the serious threat on the Internet [7]. Viruses, trojan

horses, worms, ransomware, backdoors, rootkits, spyware, adware and botnet are some examples of malware. Users and computer systems affected by malware would become the launch pad for the cyber criminal to do more harm such as stealing user credentials, financial information, spamming, executing distributed denial of service (DDoS) attack and so on [8].

Mobile malware only targets mobile platforms and usually came in the form of trojan mobile apps. This apps impersonates like a valid app such as banking and games but actually it is an app that have malicious intention towards the user, the device and the data within the device. Due to lack of security and technical awareness, naïve users would be easily fall into victim for this kind of app. Besides that, it is also quite hard to identify which one are the true and clean app from a pool of apps in the repository.

Meanwhile, phishing is a form of social engineering attack that is mainly being used by cyber criminals to steal customer’s information and money. It has become one of the most popular deceiving technique used by them to commit cybercrime [9]. The approach used by this kind of threat depends mainly on the assumptions that a user of IT systems will always be the weakest point in computer security. Financial gain is not their only objective. Nowadays, phishers also aiming for users’ data, social network account credentials, access to email inboxes and so on [9]. This is part of their effort to harvest for more contacts to spread their spam and phishing activities or even sell the information at the underground markets.

On daily basis, Malaysia CERT (MyCERT) receives many reports regarding IT security related incidents from within our constituency. This also includes incidents regarding phishing and malware attacks. In this paper, we analyzed two types of malware that infects Android-based smartphones and Windows-based computers, simultaneously to deceive users to click on unsuspecting APK and phishing URL. The malware made callbacks to a Command & Control Server (C&C) and provide TAC number information to the C&C server. The TAC number is used by the attackers to login to victim’s online

banking account for unauthorised online banking transaction. The significance of this case study is that the use of a computer malware to generate a phishing website and a mobile malware to spoof TAC number information, a much improvised technique from the traditional technique.

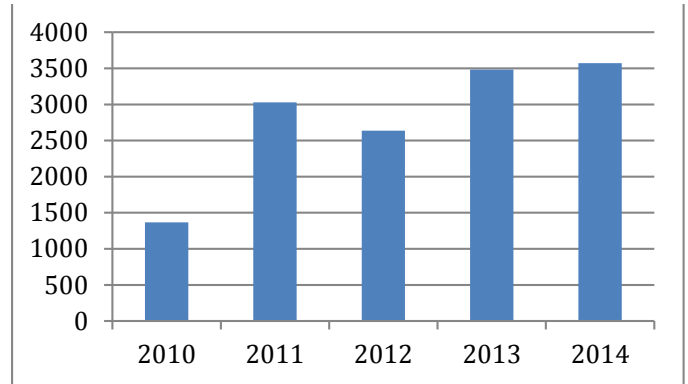


Fig. 1. Statistics for reported phishing incidents in Malaysia from 2010 to 2014 [11].

Similar phishing modus operandi using Zitmo mobile malware targeted Internet banking users had been observed in Poland by CERT Polska [10]. In Poland’s case, when a user, whose machine was infected, tried to access her internet banking site was greeted with a message that instructed her to install “E-Security Certificate” application on her Android phone. This “certificate” was nothing more than a malware capable of forwarding short messages to the attacker. As the attacker had a login, password to the banking transaction system (this is because initially the user machine had to be infected) and could access the SMS one time password it was easily possibly for the attacker to initialize an unauthorized wire transfer from the victim’s account. This is to say that the modus operandi is not specifically localized in Malaysia but widespread.

The key findings from this case study is that the use of Zeus family and its new variant, Zitmo mobile phone malware, targeting Malaysian internet banking users, with ATSEngine to dynamically inject a code in the victim’s browser while browsing a legitimate online banking website and managing the “drops” in full

automatic way. This paper is conducted with the objectives as mentioned below:

- a) *To unfold a new phishing technique that uses mobile malware as the vehicle in a phishing modus operandi.*
- b) *To propose mitigation plan that can be useful for industry practitioners in mitigating phishing incidents.*
- c) *To inform the public and financial institutions about phishing attacks by studying and unveiling new techniques used in the modus operandi.*

This paper is organized as follows. Section II discussed some overview about phishing threat. Section III discussed about the steps that involves in a banker malware attack. Section IV discussed about the malicious APK analysis and findings. Finally, Section V concluded the study and discussed some possible future works.

II. BRIEF OVERVIEW OF PHISHING

Phishing has become a global threat, affecting financial institutions, economies and end users around the world. Phishing has been in the wild for more than a decade long evolving with new techniques and modus operandi. Generally, phishing is referred to the act of getting personal or banking credentials via electronic means by masquerading as a legitimate entity from potential victims. This is supported by APWG, phishing is a criminal mechanism employing in both social engineering and technical subterfuge to steal customer's information and financial credentials.

Phishing activities were initially detected when they targeted the America Online newsgroup in the 1980s and during that time phishing was largely associated to the newsgroup. However, as motivation among hackers changes to money-driven rather than for fun, banks has become prime target to fulfil the motivation. Since then, various techniques began to evolve such as using

emails in order to trap users into a fake website to disclose their credential.

Cyber criminals used techniques such as tricking victims through email and spam. Usually, phishing attacks happen from email in order to trap users into a fake website to disclose personal information. Some of the well-known phishing techniques that had evolved over the years are:

- a) *URL Manipulation* – also known as HTTP manipulation, is a set of attacks against web-based systems specifically focusing on attempts to gain access to unauthorised information based on a direct manipulation of the URL [12]. This is one of the earliest technique used in which the phisher attached a phishing URL that is almost similar to a legitimate banking website in a phishing email. When the user clicks on the deceptive link, it opens up the phishing website instead of the website mentioned in the link. One of the anti-phishing techniques used to prevent link manipulation is to move the mouse over the link to view the actual address.
- b) *Vishing* – is an abbreviation for the word 'voice phishing'. It is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward. Sometimes referred to as 'vishing', the word is a combination of "voice" and phishing. Voice phishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations known to the telephone company, and associated with a bill-payer. Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals. Some fraudsters use features facilitated by Voice over IP (VoIP).

c) *Social media* - with more and more people actively engage on social networks, phishers are also moving a step ahead, targeting even larger number of people as their victims. Social media becomes more effective to lure more victims users tend to “follow” popular people and people they are familiar with that deceives them into clicking phishing website or malicious links. In addition, where a social network uses URL shorteners heavily that makes differentiating a suspicious and legitimate link is difficult.

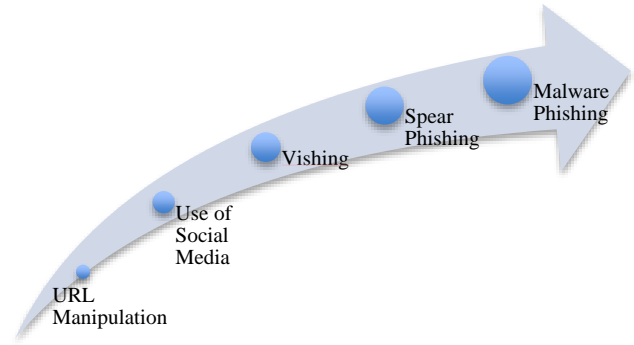


Fig. 2. Evolution of phishing techniques.

d) *Spear phishing* - it is associated to targeted attack and is largely used in Advanced Persistent Threats (APT) attacks. For example the phishing activity targets Top-Level Management such as the Chief Executive Officers (CEO), Chief Financial Officers (CFO) and Chief Technology Officers (CTO). Attackers may gather personal information about their target to increase their probability of success.

e) *Malware phishing* - this is a latest technique we observed in our constituency that is gaining popularity among attackers. In this technique, malware is used as a vector in the modus operandi and is being used actively in large scale phishing campaigns. With the increase in mobile phone usage, malware phishing has moved one step ahead targeting mobile phone users. Mobile phone users are lagging in terms of keeping their mobile phones up-to-date with patches compared to computer users. This lagging and ignorance is seen as a vast opportunity for attackers.

III. TAXONOMY OF A BANKER MALWARE ATTACK

The source of data for this case study is obtained from the MyCERT’s incident report database. The data is carefully handled to preserve its confidentiality and integrity. Several reports were received from the Malaysia constituency regarding a phishing campaign that targets Malaysian Internet banking customers. Our analysis found out that this campaign uses the Zeus banking malware family as its Modus Operandi for this campaign. Attacker will infect victim’s computer with Zeus banker malware which will then injects fake contents or page while a user is browsing a legitimate online banking website. Based on our investigation, we found out that the campaign only targeted Android smartphones and vulnerable Windows OS computers. The mobile malware has been discovered since late September 2010 but it is the first time being used in malware campaign targeting Malaysian Online Banking users.

Zeus family and its variant, Zitmo was used as the vector in this phishing modus operandi. Zeus, or Zbot is a well-known banking Trojan used by attackers to carry out malicious activities particularly related to stealing banking credentials. Zeus spreads primarily through drive-by-downloads and phishing campaigns. Victim may receive an unsuspecting email from a reputable organization, containing a link to the Trojan. Clicking on the link may infect any vulnerable computers.

Zitmo is a new variant of Zeus Trojan designed specifically for mobile phones. Zitmo is actively used by Zeus writers to defeat SMS-based banking two-factor authentication on several smartphones' platform. Our study indicated that the malware poses as a banking activation application Zitmo trojan spyware for Android and has the capability to make callbacks to a Control & Command (C&C) server owned by attacker, which includes sending banking TAC number information to C&C server. When a user is infected with ZitMo malware, his money is siphoned based on three phases as shown in the following diagrams. Fig. 3 shows the beginning phase of the malware infection. Victim generally opens an email that has a malicious attachment using a vulnerable, unprotected computer and gets infected. The malware is injected into legitimate system process and it monitors user's browsing activity.

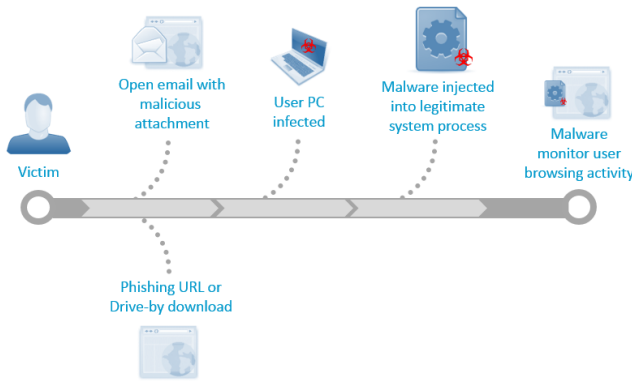


Fig. 3. Source of Zeus infection.

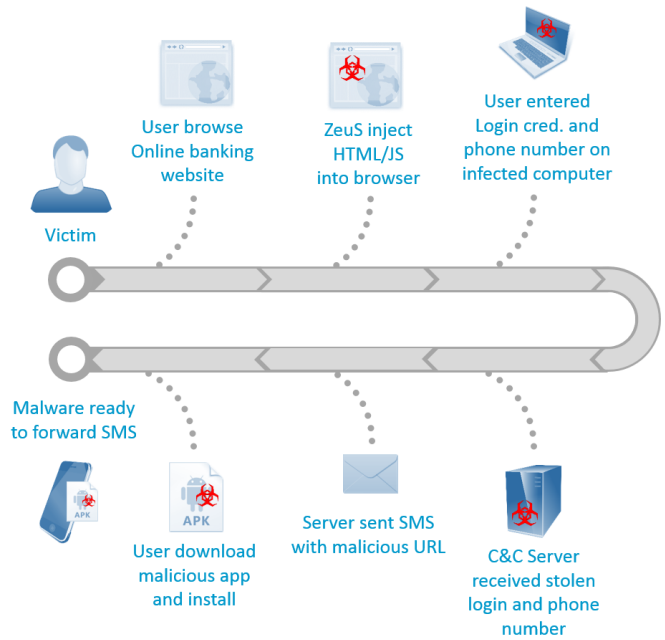


Fig. 4. Process flow of the malware infection.

Fig. 4 shows the ZitMo Infection Cycle. While victim browse a legitimate online banking website, Zeus malware injects a HTML/JS into the browser of the victim which prompts another page requesting victim to enter his mobile phone number and mobile phone Operating System. The information is sent to C&C server. Victim will receive a malicious APK through his mobile phone from the C&C server. Once the binary is executed, it installs the Zitmo malware. The malware is capable of forwarding a copy of SMS that has TAC number to the C&C server.

Fig. 5 shows how money stealing works. Cybercriminal logs in to a legitimate online banking website using stolen credentials. He makes unauthorised transactions and requests TAC number. The TAC number is sent to victim's mobile phone and Zitmo malware forwards the TAC number to the cybercriminal. They make use of the TAC number and makes unauthorised money transfer from victim's account. The stolen money is transferred to a mule account. The mule account holder will then transfer the money to the cybercriminal.

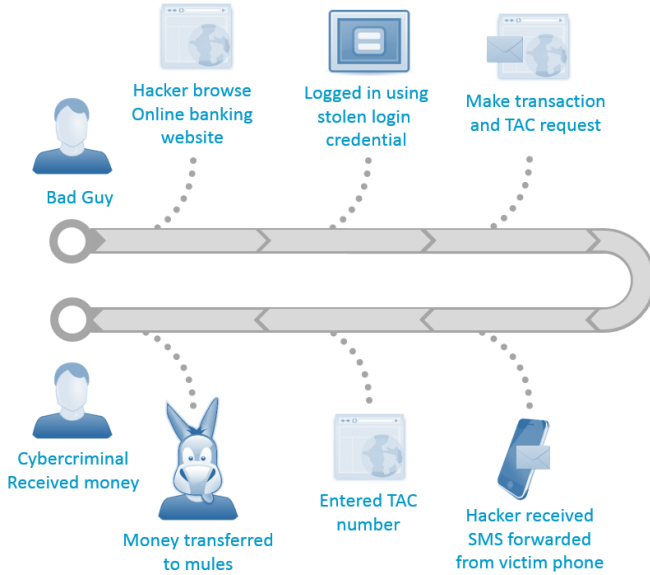


Fig. 5. Zitmo infection cycle.

IV. ANALYSIS AND FINDINGS

Several tools, combination of in-house developed and customized tools were used to analyze the malicious APK file. The tools are listed below:

- a) Droidbox (Android Emulator)
- b) MongoDB
- c) Nodejs
- d) Android SDK
- e) Apkinspector

For this work, four free APK analyzer sandboxes were also used to support our analysis:

- a) Andbox (developed by MyCERT)
- b) Anubis
- c) AVCeasar
- d) VirusTotal

ZitMo malicious android application has been used since its first discovery in September 2010. The source code uses very basic permission to access Android SMS read and sent. Thus, it is still

supported till the modern Android Operating System. Fig. 5 below shows a window in Android when a Zitmo malware successfully installed on victim smartphone, waiting for further instructions from attacker.

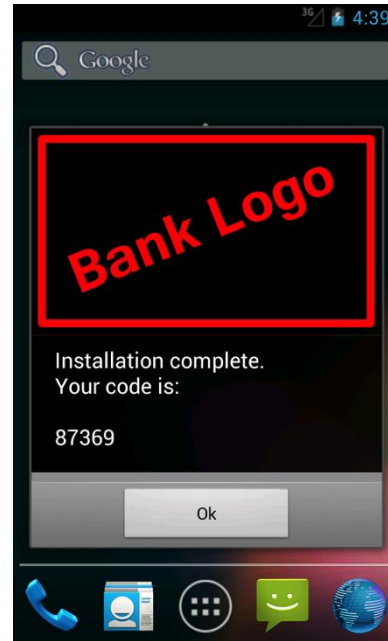


Fig. 6. Zitmo successfully installed on victim's Android based smartphone.

A. Analysis

We have done an analysis on this particular ZitMo APK using the following MD5 hash sample:

- 62cf8891b65550d13be7e7e1335ad03f

Upon activation, user will be prompted to install a "security certificate" through SMS containing download link of the malware (malicious APK). The ZitMo APK is an SMS interceptor. Upon running the application, malware will forward the selected SMS to the cybercriminal's phone number. As we traced the criminal phone number is + 7906810668. The following chronology describes the complete flow on how the cybercriminal performs illegal transactions using the malware below:

- a) As the phone is successfully infected, malware will immediately send an SMS

containing “hoo” to +7906810668 to acknowledge the criminal.

- b) Then, the cybercriminal will manually activate the malware by sending SMS containing “bra” word to the victim smartphone. Malware will respond with an SMS containing the “hooo” keyword.
- c) Using stolen online bank credential, cybercriminal will login to victim’s bank account to perform transaction and request for TAC number.
- d) An SMS of TAC number will arrive on victim phone and immediately forwarded to the criminal.
- e) Cybercriminal successfully completes the transaction and money is stolen from the victim’s account.
- f) Cybercriminal disable malware by sending SMS message “bre” to the victim phone. SMS will be no longer be intercepted. Table I below shows a list of commands used by this activity.

TABLE I. COMPLETE LIST OF ALL POSSIBLE C&C COMMANDS.

SMS	Type	Description
hoo	Response	Acknowledge infection of malware
bra	Command	Activate SMS interceptor service
hooo	Response	SMS interceptor service activated
bre	Command	Deactivate SMS interceptor service
haa	Response	SMS interceptor service disabled
call ado	Command	Listen for different administrative phone number

B. Persistence Mechanism

This malware also include a persistence mechanism, whereby the ZitMo APK will be launched when user boots up the phone or unlock

the screen. Fig. 6 below shows an excerpt of the source code that involved.

```

ActionReceiver.class
1 package com.security.service.receiver;
2
3 import android.content.BroadcastReceiver;
4 import android.content.Context;
5 import android.content.Intent;
6 import com.security.service.MainActivity;
7
8 public class ActionReceiver
9     extends BroadcastReceiver
10 {
11     public void onReceive(Context paramContext, Intent paramIntent)
12     {
13         if (("android.intent.action.BOOT_COMPLETED".equals(paramIntent.getAction()))
14             || ("android.intent.action.USER_PRESENT".equals(paramIntent.getAction()))) {
15             MainActivity.showActivityAndSendInit(paramContext);
16         }
17     }
18 }
    
```

Fig. 7. Code snippet of ZitMo persistence mechanism.

C. Indicators of Compromise

As for the Indicators of Compromise (IoC), the ZitMo APK file process package will appear as com.security.service (‘Bank name’ Certificate) as depicted in Fig. 7 below. Meanwhile, Fig. 8 shows the malware appearance in the process list.

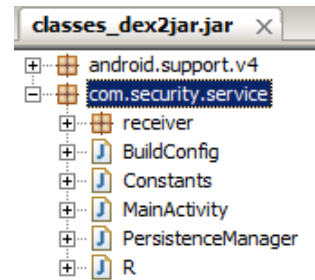


Fig. 8. Package name as shown on source code.


44.3		Certificate
2.5		Process
2.0		Process com.security.service
1.5		User u0_a60
1.0		PPID 588
0.5		Nice 0
0.5		Thread 11
0.0		Memory 37.6 MB / 6.4 MB / 4.2 MB
0.0		CPUTime 00:00
0.0		UTime 3
0.0		STime 0
0.0		Status Sleep
0.0		Start January 4, 2016 4:26:38 PM

Fig. 9. ZitMo as appeared on process list properties.

The malicious file package can be found at the following location:

- a) /data/app/com.security.service-1.apk
- b) /sdcard/Android/data/com.security.service
- c) /sdcard/Download/<bankname>cert.apk

The ZitMo APK required the following permissions in order to function accordingly:

- a) android.permission.SEND_SMS (send SMS messages)
- b) android.permission.RECEIVE_SMS (receive SMS)

D. Removal

The removal process can be done by go to the Android Application manager and find 'com.security.service' package name. Proceed with uninstall the package. The uninstall process will be remove the running process and the following file location:

- a) /data/app/com.security.service-1.apk
- b) /sdcard/Android/data/com.security.service
- c) /sdcard/Download/<bankname>cert.apk

Several mobile application antiviruses also have been able to remove the malicious ZitMo file including:

- a) AVG Antivirus for Android
- b) Avast! Mobile Security & Antivirus

V. CONCLUSION AND FUTURE WORK

Our primary contribution for this paper is the analysis of a new technique used in phishing modus operandi. The findings from this study will be used to propose a more effective response recommendation in responding and mitigating phishing incidents in the future.

The case study presented in this paper concluded three issues that need to be resolved in order to mitigate and prevent phishing activities around the globe:

- Financial Institutions: Need to improve two-factor authentication as TAC number can be spoofed by a mobile malware.
- Mobile phone and computer users: Need to increase on IT security awareness because of mobile phones and computers are vulnerable to this threat.
- Industry practitioners: Need to improve mitigation plan and response recommendation.

The crucial implication from this paper for industry practitioners is that the need for understanding the modus operandi used by attackers in successful phishing campaign and come up with an improved response to effectively mitigate the problem.

Our future work on this study would be to explore and study on the possibility of other smartphone platforms apart from Android such as iOS, Blackberry if it can also become a medium for such campaign and make comparisons with Android in terms of its behaviours, modus operandi and successful rate. This would require us to monitor closely latest phishing campaigns

and the latest techniques attributed to the campaign.

REFERENCES

- [1] Wikipedia: Mobile Virus. Retrieved from: https://en.wikipedia.org/wiki/Mobile_virus
- [2] Uppal, D., Sinha, R., Mehra, V., & Jain, V. (2014). Exploring Behavioral Aspects of API Calls for Malware Identification and Categorization. *2014 International Conference on Computational Intelligence and Communication Networks*, 824–828. doi:10.1109/CICN.2014.176
- [3] Wagner, M., Fischer, F., Luh, R., Haberson, A., Rind, A., Keim, D. A., & Aigner, W. (2015). A Survey of Visualization Systems for Malware Analysis. *EuroVis*. doi:10.2312/eurovisstar.20151114
- [4] Kramer, S., & Bradfield, J. C. (2010). A general definition of malware. *Journal in Computer Virology*, 6(2), 105–114. doi:10.1007/s11416-009-0137-1
- [5] Milliken, J., Selis, V., & Marshall, A. (2013). Detection and analysis of the Chameleon WiFi access point virus. *EURASIP Journal on Information Security*, 2013(1), 2. doi:10.1186/1687-417X-2013-2
- [6] Yang, W., Xiao, X., Andow, B., Li, S., Xie, T., & Enck, W. (2015). AppContext : Differentiating Malicious and Benign Mobile App Behaviors Using Context. *Proceeding of the 37th International Conference on Software Engineering (ICSE 2015)*, 303–313. doi:10.1109/ICSE.2015.50
- [7] Rieck, K., Trinius, P., Willems, C., & Holz, T. (2009). Automatic Analysis of Malware Behavior using Machine Learning. (18-2009), 1–30.
- [8] Chang, J., Venkatasubramanian, K. K., West, A. G., & Lee, I. (2013). Analyzing and defending against web-based malware. *ACM Computing Surveys*, 45(4), 1–35. doi:10.1145/2501654.2501663
- [9] Husak, M., & Cegan, J. (2014). PhiGARo: Automatic Phishing Detection and Incident Response Framework. *2014 Ninth International Conference on Availability, Reliability and Security*, 295–302. doi:10.1109/ARES.2014.46
- [10] Zitmo. Retrieved from: <http://www.cert.pl/news/tag/zitmo>
- [11] MyCERT. Statistics. Retrieved from: <http://www.mycert.org.my>
- [12] Sharma, Pratima & Nagpal, Bharti. A Study on URL Manipulation Attack Methods and Countermeasures. *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, 1353, Vol 15 Issue 1.