New Ways To Fight Malware

Muni Prashneel Gounder, Mohammed Farik

Abstract: Network security is vital in each field of today's reality, for example, government workplaces, instructive foundations, any business association and so forth. Information security is now top agenda for any computing environment ensuring safe transmission of information from sender to recipients. Dangers to data privacy are powerful and enhanced devices in the hands of attackers that could utilize the vulnerabilities of a system to degenerate, annihilate steal the sensitive data. This paper discusses latest trends and types of malwares, malware attacks techniques, method of propagation and detection additionally, it exhibits recommendations on various solutions are expressed to combat malware attacks. The primary beneficiaries of this journal are network engineers, network administrators, academics and students whose focus area is network security for research and development.

Index Terms: Malicious Software, Malware, Malware Detection, Ransomware

1 INTRODUCTION

Today in this modern era of digital computing software play a pivotal role in accomplishing business objective and automations. The ongoing challenge faced by most contemporary information technology professional is to protect and secure against all form of fraudulent malware. The term malware refers to malicious software intentionally deployed to intrude computing environment by exploiting vulnerabilities. Malware enthusiast code software with objectives of challenges to economic gain, destruction or closure of company or competitors, gain competitive advantage and seek revenge. Malwares are being targeted for mobile devices due to heavy dependence on mobile communication for services such as email and messaging, multimedia. For example, a publishing by UK independent shows that more than 30 has suffered severe infection with “Slocker” malware targeted at android operating system platform [1]. Techniques used by malware writers are code obfuscation and modification or inclusion of new behavior in the malware to improve strength and viability. Code obfuscation makes malware code obscure and unintelligible by malware detectors, reduces the size of codes making malware download time and deployment shorter and easier. In addition to this, code obfuscation can be categorized into be polymorphic or metamorphic. Metamorphic virus evades detection by hiding itself from detectors whereas polymorphic virus hides its decryption loops using code insertion and transposition to bypass detection [2]. Some of the recent and recurring computer malware includes computer Trojan, viruses, malicious mobile codes, worms, tracking cookies (spywares, adware, and crime wares), attacker Tools (Backdoors, Key logger, Rootkits, E-mail generator). Table 1 shows top ten malware worldwide, and in Fiji, New Zealand, and Australia reported by ESET Endpoint security for May 2017, http://www.virusradar.com/en/statistics/10 .

TABLE 1.0
TOP 10 MALWARE IN MAY 2017

Threat Name	Prevalence Level			
	Worldwide	Australia	New Zealand	Fiji
JS/Chromex.Submelius	11.65%	1.15%	1.44%	
JS/Adware.AztecMedia	9.14%	2.06%	1.82%	5.40%
JS/Adware.BNXAds	3.16%			1.61%
JS/Danger.ScriptAttachment	2.81%	7.99%	12.40%	
Win32/Adware.ELEX	2.67%			
LNK/Agent.DA	2.01%			8.85%
Win32/Bundpil	1.87%			8.27%
JS/Adware.Imali	1.82%			
HTML/Refresh	1.31%			
REG/Agent.AY	1.28%			
HTML/FakeAlert		17.14%	17.83%	
JS/TrojanDownloader.Nemucod		4.27%	1.35%	
Win32/RiskWare.PEMalform		1.78%	1.82%	
HTML/Scrinject		1.70%		
Win32/GenKryptik		1.64%	2.49%	2.53%
PDF/Phishing		1.24%	2.90%	
JS/Danger.DoubleExtension		1.12%		
MSIL/Injector.SCB			10.14%	
JS/Kryptik.BDX			1.31%	
LNK/Agent.DV				5.79%
Win32/Conficker				3.81%
Win32/Kryptik.FOZL				3.41%
Win32/Autoit.EB				3.36%
LNK/Agent.BZ				2.51%

This paper discusses various variants of malware in Section 2, followed by Section 3 highlighting malware propagation and attack techniques, followed by detection techniques in Section 4, few recommendations to combat malware attacks in section 5 and finally conclusion in Section 6.

2 MALWARE VARIANTS

2.1 Ransomware

A ransomware attack involves encryption of files on the computer making it inaccessible to user. This malware is transmitted as embedded AES encryption algorithm attachment with spoofed email which upon opening begins its payload to encrypt file contents. For instance, the “Surprise” ransomware discovered in 2016 used an AES-256 algorithm to encrypt files, and then RSA-2048 to secure each file's encryption keys with a master key and demanded 0.5 Bitcoin (~$200) for decryption keys [4]. Several attempts have been made by various antimalware to break ransomware cryptography and the success rate is very limited [5]. In

- *Muni Prashneel Gounder is a postgraduate student in Information Technology in the School of Science and Technology at The University of Fiji. He works for Fiji Airways as a Systems Developer.*
- *Mohammed Farik (Member, IEEE), is a Lecturer and Head of Department in Information Technology in the School of Science and Technology at The University of Fiji, Email: mohammedf@unifiji.ac.fj*

accordance to an analysis by ESET live grid, 25% of all cyber-attacks in UK are ransomware making UK the most prone country for ransomware attacks [6].

2.2 IOT botnets

Moreover, the second largest malware to affect the users in the year 2016 was IoT (internet of things) botnets which resulted in highest spike in Distributed Denial of Service (DDoS) of all time. This was accomplished with Mirai malware which automatically finds IoT devices such as routers, laptops, mobile phones to infect and transform into a botnet [7]. This collection of internet enabled devices then used to launch (DDoS) that transmit malicious junk traffic floods to target's servers. For instance, in just few weeks Mirai disrupted internet service for more than 900,000 Deutsche Telekom customers in Germany, and infected almost 2,400 Talk-Talk routers in the UK [8]. In addition to this, research published by SEC consult shows that 80 models of Sony cameras were vulnerable to a Mirai takeover [9].

2.3 SQL Injection and Phishing

In the year 2015, a reputable company in Fiji lost a total of US$65,000 for a purchase of good from Taiwan via an online portal [10]. SQL injection techniques in which malicious code were injected with in the genuine site was used to capture user's banking details and redirect to fraudulent site (cross site scripting) using *man-in-the-middle* browser technique. In another instance, total of 18 cyber laundering cases were investigated by Finance Intelligence Unit (FIU) between 2013 and 2015 [11]. The attacks was accomplished through email spoofing using malware Dridex which uses email attachments of word and excel to activate macros to download and activate Dridex without user intervention. Symantec detects these fraudulent email attachments as W97M.Downloader which specializes in stealing bank credentials via systems that has macros enabled in the office suite [10].

2.4 Virus

Computer viruses are programmed to infect and corrupt a host file or program. Viruses are programmed to execute payloads that perform malicious activities. For instance, benign programs may either display annoying message or consume computer memory halting execution of legitimate programs. Virus avoids detection as malware writers use techniques such as polymorphism, metamorphism, stealth, self-encryption and decryption, armoring to code and obscure from antimalware programs [2]. The main objective of virus programs is to cause destruction. One of the examples of these attacks is the *I LOVE YOU* virus which is considered to be the most to be the most dangerous virus ever recorded. This was propagated through social media links and email attachment show casing hyperlinks to as LOVE LETTER FOR YOU which upon clicking executed its payload to infect computers by deleting master boot record rendering computer unusable [12]. It is estimated the damage caused by this malware is around 10 billion US dollars.

2.5 Worms

On the other hand worms are both self-replicating and independent as it does not require a host to execute its payloads. Worms are programmed to propagate itself and execute disastrous payloads without any user intervention. The objective of programming worms is to waste system resources and gain unauthorized access to system [2]. In addition to this, worms can either be a network service that exploits network service vulnerabilities to gain unauthorized access and mass emailing worms that transmit bulk of unwanted messages flooding inbox and degrading system performance. According to Norton's published report, Slammer worm was one of the most ruthless worm ever recorded that resulted in downtime of Bank of America's ATM services, 911 service, DOS attack on 4 billion IP address on the internet, and cancellation of many flights due to online errors [13]. The worm propagated through the internet using UDP protocol and SQL buffer overflow techniques of IIS and database servers running on the internet.

2.6 Mobile Malware

Android continues to dominate the mobile malware, mainly because applications are free to publish on google play store and android is an open source operating system. A recent report published by Kaspersky named Mobile Malware Evolution in 2016 shows an alarming growth in mobile malware with 8.5 million malicious installation packages, mobile banking trojans with 128,886 and 261,214 non-banking mobile Trojans [14]. One of the contributing factors for mobile attacks is that smart phones and other mobile devices has late or no operating system updates that make it prone to advertising attacks that exploit super user rights such as Root account on android devices. Such privileges include permitting secret installation of other malware. Besides this, google play found itself as the host of mobile malware whereby cyber-criminals developed and published Trojan.AndroidOS.Ztorg.ad (steals login credentials) and Trojan-Ransom. AndroidOS. Pletor. d (ransomware for mobile devices) disguised as video, disk and memory cleaner apps [15].

2.7 Trojan horse

Moreover, a Trojan horse malware that disguise itself to perform a legitimate function prior to installation but later exposes unauthorized access to system. For instance, Trojans emulate original attributes of a legitimate program such as login prompt capturing and transmitting user password for unauthorized system access [2].

2.8 Malvertising

Furthermore, adware also known as advertising-supported software, plays, displays and download advertisement automatically to computer after installation of damaging programs [17]. The malicious software has the advertising module embedded that captures user internet browsing data mainly user credentials to hack into financial sites such as online banking. Some freeware such as free games on the internet, free software packages comes with built in adware modules. According to latest report released by RiskIQ shows that 2 billion pages and 15 million mobile apps per day are blacklisted due to malicious adwares [18].

2.9 Logic bomb

A logic bomb is malware that lies dormant embedded within a legitimate program until a condition is met to trigger its payload. This malware are normally programmed by developers of program [19]. For example, a programmer may develop a database trigger to delete employee human resources data should his or her employment status be changed to terminate. A classic example on such attack was

in mid of year 2013 where a cyberattack wiped hard drives and master boot record of computers for banks and broadcasting companies in South Korea [20]. This resulted in outages of most machines with in the network with errors “Boot device not found. Please install an operating system on your hard disk.” In addition to this, there were outages on most ATM’s preventing account holders from withdrawing cash using ATM services. Beside this, the logic bomb incorporated a module that searched for remote connections and used stored credentials to access and delete master boot record from remote Linux servers [20].

2.10 Spyware and Rootkits

Spyware is designed specifically to monitor user’s internet activities, to capture information without their consent. Spywares collects information such as credit card number, frequently access sites and bank account numbers. In addition to this, it also changes setting on the computer, maliciously controls the computer remotely resulting in slower computer connection setting. Rootkits are designed to gain administrative access to computer system without detection by the system administrator to adjust computing resources illegally. Computer resources such as BIOS, Kernel, and Boot loader are main targets of rootkits. A latest rootkit published by researchers in Fortinet blog that sit inside programmable logic controllers (PLC) which modifies commands before it is transmitted to other units transforming into malicious commands [21]. The rootkit is named “Harvey” which changes the LED and HMI states of the PLC without changing the external input / output.

2.11 Backdoor

Furthermore, backdoor is an unauthorized entry point to the system coded by developers of the system that listen for commands using network protocols to allow remote connection the system. Upon gaining access to the computer, the hacker then collects confidential user data, changes systems settings and crashes the system. An example of one such attack was in December 2015 where BlackEnergy backdoor was used to implant a KillDisk Trojan making systems unbootable [22]. This resulted in power outages for half of the homes. Another recent backdoor attack was on Linux Mint release of 2016 where the hacker implanted a backdoor that maliciously sent confidential information such as financial details, usernames and passwords about the user to the attacker [23].

2.12 System Vulnerabilities

On the other hand, these malware attacks are a result of system vulnerabilities. The most common vulnerability is source code exposure which a result of poor programming, exposing information such as connection strings through the use of user executable script. For instance, buffer overflow whereby the user submits more data that the system is designed to handle causing system crash to allow unauthorized access to install and execute malware.

3. MALWARE PROPOGATION AND ATTACK TECHNIQUES

3.1. Method of Propagation

Malwares are disseminated either by self-propagation or through user interaction. Malwares such as worms does not require any user intervention and is capable to copy itself and self-execute. On the other hand, viruses that rely on host and user or a host program for its execution and propagation. Other malwares may use internet as medium for its transmission. Mobile malware use mobile phone network on the internet for propagation which is defeated using internally built defense mechanism on the mobile phone. In addition to this, direct pair wise communicating resources such as Bluetooth, WI-Fi and infrared expose the device mobile malware propagation.

3.2. Attack Techniques

There are several approaches to malware infection namely, entry point obfuscation, code integration, code insertion, register renaming, memory access reordering and session hijacking. Firstly, in entry point obfuscation the virus hijacks control of the program after execution and overwrites program import table addressees and function call instruction [17].Secondly, in code integration virus embed itself with a legitimate program that requires disassembly of target. Malwares append virus code either by modifying the entry point of the program or inject its code into unused sections of program code. Malwares undertake two essential methodologies on mobile devices by either creating new process dispatch an attack or diverting program flow to execute a malicious code. Malware attacks using the technique of new process creation to execute its malicious code requires user operation. For example, actions such as user downloading software from the internet or opening a received message from the user that creates a new process without user’s knowledge. The newly created process incorporates a program descriptor describing the address content, execution state and security context, that differs from that of the parent process which invoked the new process [17]. In contrast to this, malware attack techniques on mobile devices use program flow redirection to execute malicious code. This technique is targeted for open source based OS and application framework by exploiting the stack buffer overflow such as Linux based smart phones.

4. DETECTION TECHNIQUES

Malware detection can be categorized into analysis, classification, detection and containment of malware [17]. Classification techniques are used to catalogue malwares based on their instances making it easier to recognize the type and activities performed by a new variant. Analysis of malware involves identification of the instances of the malware using different classification schemes using the characteristics of known malware. Malware detection involves quickly concealing and validating any instance of malware to preclude further damages to the system. Finally, containment of the virus involves undertaking action to prevent escalation and damages to the system. Some malware detection techniques used are:

4.1. Signature-based malware detection

Signature based malware detection mainly used by antivirus whereby scanner scans for a sequence of byte within a program code to detect and report malicious code. Virus signature databases have to be updated regularly with latest definition of virus. Malware detection using this approach involves a syntactic level of code instruction by analyzing the code during program compilation [17]. This method however, is limited by ignoring the semantics of instruction that permits malware obfuscation during program run time. Zero day malicious exploit malware however evades antivirus detection which could be prevented using content analysis of the file to discover anomalous files.

4.2. Specification-based malware detection

This techniques use a special algorithm that incorporates semantics of pattern matching to address the deficiency of pattern-matching and provide high resilience to obfuscation techniques. For example, a *template T that* describes the behavior of malware containing sequence of instruction represented by variables and symbolic constants [17]. This approach is however is limited as attribute of a program cannot be precisely defined.

4.3. Behavioral-based detection

Behavioral-based detection performs surface scanning and also identifies the malwares action by generating a database of malicious behaviors. This is accomplished by studying dissimilar families of malware on target operating systems. Data mining technique classification is used to train support vector machines (SVM) to easily differentiate between malicious and non-malicious programs which makes it highly efficient to detect metaphoric malware.

5. RECOMMENDATIONS

One of the solutions to combat the rise in malware is to take proactive approaches rather than reactive. This could be accomplished through keeping the environment patched up and updated with latest firmware that fixes vulnerabilities in prior version of firmware. In addition to this, the signature database antimalware must be updated with latest definition provided by the vendor. There must be greater awareness in the organization on the recent threats and types of attacks a network environment is exposed to. For instance, when Fiji Airways was exposed ransomware attack, all employees were notified via Service desk to take precaution and consciously opening emails from known senders only. System administrator must ensure that firewall on device within the network is turned on and users are not able to disable it as firewall prevents hackers, viruses and worms and other malware from penetrating the system. Establishing and maintaining a security policy that successfully and proficiently bolster location and aversion of malware. Organization should train and prevent users from downloading unknown files from an unreliable source. This can be accomplished through the use of web filtering software that contains a predefined list of blacklisted sites and analyses the content of file prior to download. In addition to this, organization must implement and maintain an updated email filtering software that prevents malicious attachments and spoofed emails being sent to the user. Moreover, security should be implemented with infrastructure set up. One such implementation is allocation of different servers in different VLANS. For example, exchange server on VLAN 1 and DNS server on VLAN 2.

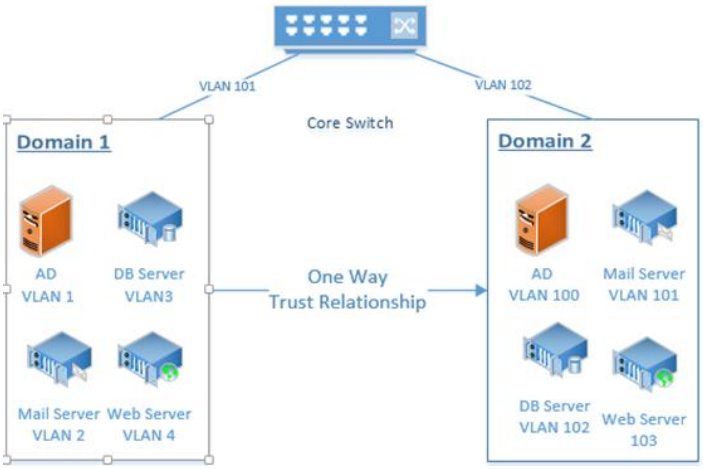

Fig. 1. *Infrastructure Setup to prevent propagation to entire domain segregated by different VLANs.*

This reduces the impact of malware threats as it secures a VLAN from an infected VLAN by reducing propagation. In addition to this, the naming convention used to name servers and device on the domain should be complex which could not be predicted by attackers to launch DOS attack. For example a poor naming technique for naming mail server as exchange sever. Finally, create several domains with trust relationship amongst them. This could be done by segregating by use. Application used corporate wide and internal could be hosted in one domain whilst application that is used by a specific department and is open internally only on separate domain. This reduces the impact of compromise reducing the probability of entire network downtime. In addition to this, organization to implement an end to end disaster recovery solution whereby compromise on one site should automatically fail over to the DR site for continuous availability of systems and networks. Furthermore, for elimination of malicious adware's, ad hosting providers such as Google and Facebook should implement a content filtering in their hosting engines. These filters test and examine the advertisement for malicious code that gets pushed out to sites.

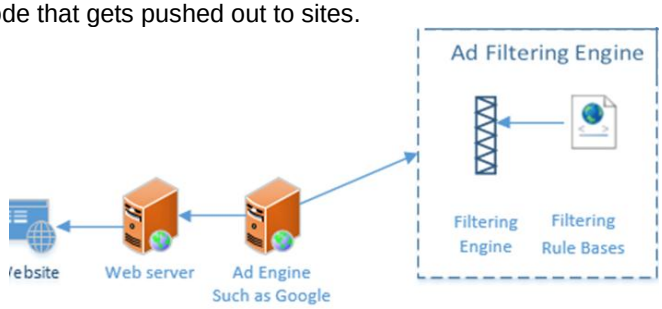

Fig. 2. *Infrastructure Setup to prevent propagation to entire domain segregated by different VLANs.*

In addition to this, should there be a breach caused by malvertisement, strong legal policies should be implemented to adware hosting providers hold accountable for the loss. Next, in the area of mobile malware since most mobile malware are transmitted through apps more stringent policies should be established for developers to publish their app for distribution and use on mobile platforms. For example,

implement multiple layers of authentication such as biometric, app signature and license to publish certification given by market operator's google (android) and Apple (IOS). Another solution proposed is to prevent all apps published to be publically available immediately. Rather it should be directed to holding or temporary area where it is tested and certified as non-malicious by vendors themselves before it is available for public use. Finally offloading security by deploying backend services for smartphones on cloud which is monitored and controlled by a third party provider complementing other security mechanism on the device.

6. CONCLUSION

Hence in a nutshell, with the rapid growth on malware proactive approaches must be undertaken to secure network computing environment. This review has discussed many variants of malwares and has suggested few solutions. It is clear that detection and prevention against malware is of paramount importance and new techniques needs to be developed to combat against new variants that exploits vulnerabilities in hosts.

References

[1] Sulleyman, A. (2017). If you have an Android, you need to read this. [online] The Independent. Available at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/android-malware-phones-infected-samsung-galalaxy-s7-nexus-5x-models-before-sale-a7626726.html [Accessed 26 Apr. 2017].

[2] Shah, T. (2014). Network Security- Virus Attacks and Defence using Antivirus Software. International Journal of Advanced Research in Computer Science & Technology, [online] 2(4). Available at: http://www.ijarcst.com/doc/vol2-issue4/ver.1/trupati.pdf [Accessed 17 May 2017].

[3] Panda Security Mediacenter. (2017). PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record - Panda Security Mediacenter. [online] Available at: http://www.pandasecurity.com/mediacenter/press-releases/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/ [Accessed 18 May 2017].

[4] Cimpanu, C. (2016). "Surprise" Ransomware Uses TeamViewer to Infect Victims. [Online] http://news.softpedia.com. Available at: http://news.softpedia.com/news/surprise-ransomware-uses-teamviewer-to-infect-victims-502006.shtml [Accessed 2 Apr. 2017].

[5] Ransomware and Businesses 2016. (2016). [online] Symantec. Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf [Accessed 2 Apr. 2017].

[6] Share, D. (2016). Shocking Statistics: 25% of all cyber-attacks in the UK are ransomware | Amazing Support. [online] Amazing Support. Available at: http://www.amazingsupport.co.uk/2016/07/25/25-of-all-cyber-attacks-in-the-uk-are-ransomware/ [Accessed 26 Apr. 2017].

[7] NEWMAN, A. (2016). The Botnet That Broke the Internet Isn't Going Away. [online] Wired.com. Available at: https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/ [Accessed 26 Apr. 2017].

[8] Herzberg, B., Zeifman, I. and Bekerman, D. (2016). Breaking Down Mirai: An IoT DDoS Botnet Analysis. [online] Incapsula.com. Available at: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html [Accessed 26 Apr. 2017].

[9] Consult, S. (2016). Backdoor in Sony IPELA Engine IP Cameras. [online] Blog.sec-consult.com. Available at: http://blog.sec-consult.com/2016/12/backdoor-in-sony-ipela-engine-ip-cameras.html [Accessed 26 Apr. 2017].

[10] Shah, N., Sharma, A., Farik, M. and Pandey, S. (2016). Cybersecurity Situation in Fiji. TERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, [online] 5(7). Available at: http://www.ijstr.org/final-print/july2016/Cybersecurity-Situation-In-Fiji.pdf [Accessed 26 Apr. 2017].

[11] Deo, S. and Farik, M. (2016). Information Security - Recent Attacks in Fiji. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, [online] 5(12). Available at: http://www.ijstr.org/final-print/dec2016/Information-Security-Recent-Attacks-In-Fiji.pdf [Accessed 26 Apr. 2017].

[12] News, 1. (2017). Top 10 Computer Damaging Viruses in The World 2017. [online] Top 101 News. Available at: http://top101news.com/most-popular-top-10-list/2017-2018-2019-2020-2021/computer/computer-damaging-viruses-world-dangerous/ [Accessed 26 Apr. 2017].

[13] Norton_Team (2016). The 8 Most Famous Computer Viruses of All Time. [online] Available at: https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html [Accessed 26 Apr. 2017].

[14] Olenick, D. (2017). Mobile malware attacks hit new heights in 2016: Kaspersky Labs. SC Magazine US. [online] Available at: https://www.scmagazine.com/mobile-malware-attacks-hit-new-heights-in-2016-kaspersky-labs/article/641694/ [Accessed 26 Apr. 2017].

[15] Xentaurs. (2017). Report: 2016 saw 8.5 million mobile malware attacks, ransomware and IoT threats on the rise • Xentaurs. [online] Available at: https://www.xentaurs.com/2017/02/28/report-2016-saw-8-5-million-mobile-malware-attacks-ransomware-and-iot-threats-on-the-rise/ [Accessed 17 May 2017].

[16] Garnaeva, M., Wie, J. and Makrushin, D. (2015). Kaspersky Security Bulletin 2015. Overall statistics for 2015 - Securelist. [online] Securelist.com. Available at: https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/ [Accessed 26 Apr. 2017].

[17] Surajudeen, A., Mabayoje, M., Mishra, A. and Oluwafemi, O. (2012). Malware Detection, Supportive Software Agents and Its Classification Schemes. International Journal of Network Security & Its Applications (IJNSA),, [online] 4(6). Available at: https://www.idc-

online.com/technical_references/pdfs/data_communications/Malware%20Detection.pdf [Accessed 17 May 2017].

[18] RiskIQ. (2016). 2016 Malvertising Detection & Mitigation Report | RiskIQ. [online] Available at: https://www.riskiq.com/infographic/riskiqs-2016-malvertising-report/ [Accessed 26 Apr. 2017].

[19] En.wikipedia.org. (2015). Logic bomb. [online] Available at: https://en.wikipedia.org/wiki/Logic_bomb [Accessed 26 Apr. 2017].

[20] Zetter, K. (2017). Logic Bomb Set Off South Korea Cyberattack. [online] WIRED. Available at: https://www.wired.com/2013/03/logic-bomb-south-korea-attack/ [Accessed 18 May 2017].

[21] Apvrille, A. (2017). Security Research News in Brief March 2017 Edition. [online] Fortinet Blog. Available at: https://blog.fortinet.com/2017/03/24/security-research-news-in-brief-march-2017-edition [Accessed 26 Apr. 2017].

[22] Lipovsky, R. and Cherepanov, A. (2016). BlackEnergy Trojan strikes again: Attacks Ukrainian electric power industry. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/ [Accessed 26 Apr. 2017].

[23] Whittaker, Z. (2016). Hacker explains how he put "backdoor" in hundreds of Linux Mint downloads | ZDNet. [online] ZDNet. Available at: http://www.zdnet.com/article/hacker-hundreds-were-tricked-into-installing-linux-mint-backdoor/ [Accessed 26 Apr. 2017].