An Intelligence based Model for the Prevention of Advanced Cyber-Attacks

Olawale Surajudeen Adebayo
[1]Computer Science Department, International Islamic University Malaysia, [2]CSS Department, Federal University of Technology Minna, Nigeria
[1]adebayo.olawale@live.iium.edu.my,
[2]waleadebayo@futminna.edu.ng, info@osadebayo.com

Associate Professor (Dr.) Normaziah Bintin AbdulAzeez
Computer Science Department, International Islamic University Malaysia
naa@iium.edu.my

***Abstract*— The trend and motive of Cyber-attacks have gone beyond traditional damages, challenges to information stealing for political and economic gain. With the recent APT (Advance Persistent Threat), Zero-day malware, and Blended threat, the task of protecting vita infrastructures are increasingly becoming difficult. This paper presents an intelligence based technique that combined the traditional signature based detection with the next generation based detection. The proposed model consists of virtual execution environment, detection, and prevention module. The virtual execution environment is designated to analyze and execute a suspected file contains malware while other module inspect, detect, and prevent malware execution based on the intelligent gathering in the central management system (CMS). The model based on Next Generation Malware Detection of creating threat intelligence for future occurrence prevention. The model takes into consideration the false positive and false negative among other lapses and benefits of the existing detectors.**

Keywords*— APT; Advanced Persistent Threat; Cyber Attacks; Next-Generation Security; Next Generation Threat

I. INTRODUCTION

Cyber Attacks are those kinds of attacks that are being perpetrated against cyber facilities for various dubious intents. The purpose of traditional cyber-attacks is for challenges and damages. However, modern attacks on the cyber facilities concentrate on financial and political gains. The traditional cyber threats like worms, Trojans, Viruses Social Engineering etc. known to traditional security defences can be easily detected by signature based defences. Today's cyber-attacks on the other hand are web based malicious events [17] that can easily penetrate traditional defences namely firewalls, Intrusion Prevention Systems (IPS), and Anti-virus software. Recent Next-Generation Cyber-attacks include Zero-day malware (new breed of malware that are unknown to defence and can use stealth technique to exist for a long period of time), Polymorphic malware (malware that constantly changed or morphed making the detection using signature-based defence difficult), Blended malware (combination of malwares of multiple types usually employed multiple attack vectors i.e. Nimda, Conficker, Code Red etc.), and APTs (Advanced Persistent Threat which is a sophisticated cyber-attack that employs advanced stealth techniques to remain undetected over times) [17]. The important cyber-attacks considered in this research are Malware and APTs (Andvanced Persistent Threats).

Next Generation Security is a security that is meant to deal with the recent next generation threats and cyber-attacks. New Generation Security is a defence strategy that capable of not only scanning and detecting but also preventing the feature escalation of occurrence of next generation threats like zero-day malware, polymorphic and blended malware. The features of Next Generation Malware However, modern attacks on the cyber facilities concentrate on financial and political gains. The traditional cyber threats like worms, Trojans, Viruses Social Engineering etc. known to traditional security defences can be easily detected by signature based defences. Today's cyber-attacks on the other hand are web based malicious events [17] that can easily penetrate traditional defences namely firewalls, Intrusion Prevention Systems (IPS), and Anti-virus software.

The next generation Malware Protection (NGMP) [17] involves scanning, inspection, detection, and prevention of next generation malware. NGMP also capable of inspecting dozens of file types including com, doc, docx, dll, exe, gif, ico, jpeg, jpg, mov, mp3, mp4, pdf, png rtf, vcf, others and not just exe, pdf, and dll files. It is expected not only to block the malicious code but also work cooperatively with other security features to protect the system. This might be a combination of various approaches and tools devoid of using root privileges and with low false positive. Next Generation Malware Protection works by suspecting a threat that has been classifying as malware by the detection system and create new intelligence automatically and distribute them to other NGMP appliances (those with central management system). It offers both a local GUI (graphical user interphase) and a centralized management system for centralized management, consolidated

threat monitoring, reporting, alerting and malware intelligence distribution.

Next Generation Malware Protection creates intelligence using only metadata from infectious files. Hence, it prevents sensitive data from leaving the network. The web and email components of NGMP examine URLs for malicious contents and email attachments for APTs (Advanced Persistent Threat) respectively. The detail of Next Generation Cyber-Attacks Protection is discussed under the proposed model. The role of Next Generation Security in this research is to incorporate the next generation features technique of consolidated threat monitoring, reporting, alerting and malware intelligence distribution so as to ensure the detection and prevention of occurrence of malware.

APTs (Advanced Persistent Threats) are sophisticated network attacks in which an unauthorized person gains access to a network and stays undetected for a long period of time [52]. The intention of this attack is to steal information of target organization such as credit card processors, government information, and financial services information. Topmost in the APTs technique are Spear phishing and baiting for gaining initial network entry into the system in order to compromise the host system. Once the host network is compromised, APT process using slow-and-slow strategy to evade detection [17]. The word advanced in the term shows that attacker is an expert in cyber intrusion methods is capable of rafting custom exploits and tools, while persistent signifies that attacker has a long term objective and will persistently operate to realise its intention without detection and regard for time, the threat part shows that attacker is organized, funded, well trained, and highly motivated [17].

Common APTs are Operation Aurora (2009), Stuxnet (2010), and Flame (2012). Flame malware also known as Flamer, sKyWiper, and Skywiper. This APT was identified in May 2012 by the MAHER Center of Iranian National CERT, Kerpasky Laboratory, and the Budapest University of Technology and Economics [17]. The Flame attack is a malware developed by United State and Israel to wreck havocs to Iranian Oil Ministry computers by collecting intelligence for cyber-sabotage. This prompted Iranian officials to disconnect their oil terminals from the internet. Flame malware is characterized by including calling back operation to its command-and control servers to download other malware modules. It is about 20 megabytes in size, about 20 to 30 times larger than computer virus. Stuxnet (2010) is a highly sophisticated computer worm discovered in June 2010 used in conjuction with APT attack against Iranian uranium enrichment infrastructure. Stuxnet initially exploiting Microsoft Windows vulnerability and spread laterally in the network to ultimately reach targeted Siemens industrial software and equipment causing it to malfunction.

II. LITERATURE REVIEW

A malware is a computer program that has various kinds of malicious intents [16]. Some commonly known Malware categories are viruses, trojans and worms. Malicious programs present an incessant threat to the privacy and security of sensitive data and the availability of critical services at crucial point in time [1]. Advanced Cyber Attacks are those attacks which are either not previously known to the detector or combine several attack vectors using stealth techniques in order to attack system and evade attack. The major common cyber-attacks are APTs (Advanced Persistent Threats), zero-day malware, and blended threats. All these aforementioned attacks are term as next generation attacks because of their nature and technique of attack. These attacks require next generation based solution which is an intelligent driven.

Today, federal agencies are increasingly the victims of advanced persistent threats, often comprised of multi-staged, coordinated attacks that feature dynamic malware and targeted spear phishing emails [5]. On a weekly basis, over 95% of organizations have at least ten (10) malicious infections bypass existing security mechanism and enter the network [5]. While firewalls, next-generation firewalls, IPS, AV, and gateways, which rely on approaches like URL blacklist and signature, remain important security defences, they continue to be proven ineffective at stopping APT attacks [6]. APTs are dynamic attacks that exploit zero day vulnerabilities. APTs are also coordinated and often use multiple attack vectors, which can be delivered through websites or email, blended, or through application or operating system [6].

The dynamic stages explore by APT attacks include system exploitation (by compromising the system), malware download (i.e. keylogger, Trojan backdoor, and password cracker, or file grabber for respective different functions), callbacks and control establishment (communicating the owner through callback server), data exfiltration (by encrypting the data and send it to other machines outside the organization), and finally lateral movement (where attackers exploit additional vulnerabilities and gain access to important users, services, and administrative accounts) [6]. The 2013 Lieberman software survey that included nearly 200 IT security professionals in Las Vegas reveals that more than 74% of respondents are not confident that their network has never been breach by a foreign state sponsored attacks or an advanced persistent threats [4].

Advanced Persistent Threat is also threating the security of Control systems, which include supervisory control and data acquisition (SCADA) systems, which are devices and networks used electronically control various important

infrastructures like electricity generation and transmission devices, water valves devices, [2] fuel pumping devices, fuel onshore and offshore equipment etc. As these facilities and technologies are being operating in conjunction with the internet, there is a great tendency to be exposed to advanced persistent threats and hence a need to continually provide an improved cyber-defence technology. Recent attacks targeting Canadian government officials, French government officials, RSA, and elements of the European Union have all been linked to APTs [14]. However, it is pertinent for security professionals to note that the same APT strategy used by nation-states for strategic gain are now being used by cybercriminals to steal data from businesses for financial gains [14].

ISACA [7] undertook the study of the Advanced Persistent Threat (APT) Awareness in the fourth quarter of 2012 and found out that market has not really changed the ways in which it protects against APTs. This research identified that network perimeter technologies such as firewall, anti-malware, and antivirus as still being used for protection against APTs. The Google Aurora attack in 2010 revealed that APTs are not just government threats. On the verge of discovering Google Aurora, large-scale breaches of cyber-attacks followed and made international headlines. RSA's 2011 breach was classified as being caused by an APT and, of course, awareness of Stuxnet and Flame is followed and alarming [7].

Whereas many APT players have resulted to tactical web compromise as a delivery vector, it is obvious that spear phishing via email-based attachments or links to zip files remain prevalent with several threat actors, especially when paired with lures discussing current media events [8]. Ned Moran and Alex Lanstein [8] identified a numbers of spear phish as follows; "Admin@338" designed to hamper APAC Government and U.S. Think Tank, the Naikon Lures discovered on March 9, 2014, which is a malicious executable entitled the "Search for MH370 continues as report says FBI agents on way to offer assistance.pdf .exe" (MD5: 52408bffd295b3e69e983be9bdcdd6aa), it was seen circulating in the wild and was identified via forensic analysis, as Backdoor.APT.Naikon, the Plat1 Lures was discovered on March 10, 2014, and seen as another sample that exploited CVE-2012-0158, titled "MH370班机可以人员身份信息 .doc", which roughly translates to "MH370 Flight Personnel Identity Information". This malware that is dropped by the malicious Word document, was detected as Trojan.APT.Plat1, begins to beacon to 59.188.253.216 via TCP over port 80, the Mongall/Saker Lures was another sample leveraging the missing airliner theme and was seen on March 12, 2014.

Florian S. et al [7] adopt a white list approach with anomaly detection technique. The anomaly detection technique keeps the track of system events, event dependencies and occurrences and uses the events to learn the normal system behaviours over time. John R. et al. [8] developed a novel graph analytic metric that can be used to measure the potential vulnerability of a cyber-network to specific types of attacks that use lateral movement and privilege escalation such as the well-known Pass The Hash, (PTH). Josephine M. Namayanja paper characterized the behavior of large, evolving networks, in terms of central nodes to identify patterns that may be conducive to persistent threat structures over time and geo-spatial regions. This approach is use to monitor central nodes to determine Consistency and Inconsistency (CoIn) in their availability across time periods. This approach also identifies the time periods and spatial regions associated with CoIn [9].

In order to gain initial access to the victim's networks, the attackers started with a targeted spear phishing attack against the company [3]. The attackers use this spear-phishing method through social media in order to conduct reconnaissance and theft of confidential proprietary information [13]. R. M. Amin's dissertation surveys and categorizes existing email filtering techniques, proposes and implements new methods for detecting targeted malicious email and compares these newly developed techniques to traditional detection methods [15]. Masahiko Kato et al. discuss the modeling of target information systems as well as various attacks, in order to clarify the impact of Advanced Persistent Threats (APTs) and to enable efficient planning of defense strategies to counter APTs [10]. Paul Giura's model of the APT detection problem and methodology implementation on a generic organization network aimed to address the problem of modeling an APT and to provide a possible detection framework [15].

Mordehai Guri et al. [12] present the work-in-progress of OpenAPT, a community supported, open-source advanced malware development and documentation framework that provided researchers code-samples and documentation of malware and set of APT mechanisms to compile and test against their new security mechanisms. Merete Ask et al. [11] takes a closer look at APT, beyond the hype to shed light on different aspects of APT and as such provide a paper that can be a source for peers looking for a broad, yet collected, source of information on the topic.

III. METHODOLOGY

The method adopted in this research is combining the traditional detection with the next generation features in order to detect next generation cyber-attacks. The model consists of two main segments namely:

1. Next generation detector (Inspection, detection, Intelligent gathering, central management system, deployment system)
2. Signature based detector (virtual execution environment)

The details of these segments is contain in the proposed model section.

IV. CYBER ATTACKS THREAT VECTORS

The threat vectors of Advanced Persistent Threats include electronic mail (email) where APTs spear phish electronic mail. Advanced Persistent Threats can also attack the system through web-based threats where threats and malicious contents are hide within the communication protocols like HTTP, FTP, HTTPs, IRC and so on. The last vector is through file sharing from one medium to the other.

V. ECONOMIC DEMERITS OF APTS

Advanced persistent threat is a sophisticated and coordinated malware designed to execute advance attacks on a victim system ranges from gaining access to user system in an unauthorised manner to taking full control of the victim system. It can steal the information of an organization, having gain total or privilege access to the system. APT can also carry out political damages by deformation and modification of the victims data or website.

VI. PROPOSED MODEL

The proposed model shall consist of six (6) phases namely:

Inspection, Detection, Application Launching, Object Replay, Virtual Execution Engine (Dynamic & Static Analysis: virustotal, Classifier, Supervise learning, Event logger, Multiple file inspector, Filter), Prevention : Intelligence Gathering (Central Management System, Deployment Strategy (Inline or Out-of-bound)

Inspection
Application Launching
Object Replay
Virtual Execution Engine
Prevention

Start

Inspection

Programmatically mechanisms to inspect the network traffics for malicious code.
Inspects inbound and outbound traffic and file at rest for known threats, CnC callbacks and suspicious binaries or web pages to observe malicious behaviours.

Application Launching

Launches any application that is associated with the host targeted by the suspected threat. Blocks the connections

Triggers an alert if a known threat or CnC callback is detected.

Inspecting more than HTTP traffics i.e. FTP, and custom protocols.

Object Replay

Replays the object and observes a malicious behaviour using ***byte-by-byte capture and reconstruction of the traffic flow within the system***.

Replays corrupting root file,

Replays attacked application using heap spray, and calling back to a known infection URL (universal resource locator).

If the detected binary is determined to be benign, ***then***

event is logged in the event log and the system is reset

Else if zero-day malicious activity is observed, ***then***

protector captures the rest of the attack life cycle.

Virtual Execution Engine

Collector: collect the suspicious file from a capture module.

Multiple file inspector: scan and inspect most types of file format

Dynamic Analysis : through emulation where suspicious application code shall be examined during the execution time

Static Analysis: Virustotal

Classifier: trained to classify suspicious files to benign or malign using supervised learning technique of data mining.

Filter: programmatically built to filter a suspicious in order to ensure absolutely no false positive and false negative.

Event logger: This engine shall log an event associated with suspicious files.

Database: Suspicious files shall be stored into database probably SQLite.

Supervise learning

Prevention Module

Intelligence Gathering:

Loaded the malware binary

Recorded all malware-generated host and network activities

Generates threat intelligence to stop associated callback traffic across the network.

Raise priority alert

Record Malware Forensic

Creates new malware protection profile to block the now-known threats.

Forward new threat to the central management system (CMS) appliance, where it could be distributed to other appliances in the organization.

Deployment strategy

Deployment could be inline (active) or out-of-band (passive).

The out-of-band configuration is used for file sharing appliances to inspect file at rest and quarantine malicious file objects

Inline configuration is meant to identify and block advanced cyber-attacks like CnC (command and control) server and calling back and prevent future occurrences

Central Management System:

Storage and distribution of malware threat intelligence to some other detector appliances across the network.

VII. FUTURE WORK

The future research aims at examining various vulnerabilities being exploited by APTs in order to attack its host and conduct an hybrid way of analysing and classifying APTs. The analysis and detection strategies shall then be geared towards the development of a comprehensive algorithm that can help in the detection and containment of malware on the same platform.

VIII. RESEARCH'S BENEFITS

The benefits of the study of Advanced Cyber Attacks are enormous to the Muslim society as highlighted below:

1. Today's world is ICT and cyber driven global communities and therefore the security of these vital facilities should be guaranteed.
2. It will be recalled that in 2010 an advanced cyber-attack called Stuxnet was sent to attack Iranian oil and gas facilities, it was a prompt attempt by Iranian cyber experts that protect these vital facilities by disconnecting from internet. Therefore, Muslim world should be prepared ahead of cyber- attacks.
3. Education is vital most especially on the security of life and properties, and as said by the prophet (SAW) that a Muslim should seek for knowledge even if it requires going extra miles. Therefore, Muslim world should be educated and alerted on the consequences of cyber-attacks.

IX. RECOMMENDATION

The followings are some of the recommendations for the effective use of smartphone for the protection against malware:

A) The organization should ensure the inspection of inbound and outbound network before connection.

B) Download and Install software and application from approved and trusted sources.

C) Use of next-generation anti-malware software

X. CONCLUSION

This research reviews the existing literatures on the detection of Advanced Persistent Threats malware. The research examined several existing approaches in the analysis, detection and classification of this threat in a bid to identify weaknesses and propose consolidated approach. The research finally proposed a consolidated next-generation based approach that combines traditional signature based approach and next generation based detection strategies to provide efficient and effective algorithm for threats detection

TABLE 1. ADVANCED CYBER ATTACKS AND APTS

S/N	APTs	Detect	PE type	Initial Infection	Transmission	Key logon	Encryption	Purpose	Evasion
1	Duqu	Sep 2011	DLL	MS word	Manual	No	XOR, AES, CBS	Info G	True
2	Flame	May 2010	OCX	Unknown	Manual	Yes	XOR, Subs, RC4	Info Gathering	True
3	MiniDuke	Feb. 2013	EXE	Pdf	Manual	No	XOR, ROL, victims depend	Info Gathering	True
4	Night Dragon	Feb. 2011	EXE	Unknown	Manual	Yes	Victims depend	Info Stealing	True
5	Operation Aurora	Feb. 10 2010	DLL, EXE	Unknown	Manual	No	HTTP, Port 443	Info Gathering	
6	Red	October Oct 2012	EXE	excel, msword, java	Manual	No	XOR	Info Gathering	False
7	RSA breach	2011	EXE	Unknown	Manual	Yes	Unknown	Info Stealing	True
8	Stuxnet	June 2010	DLL	Unknown	Removable media, Network	No	XOR	destruction	Yes

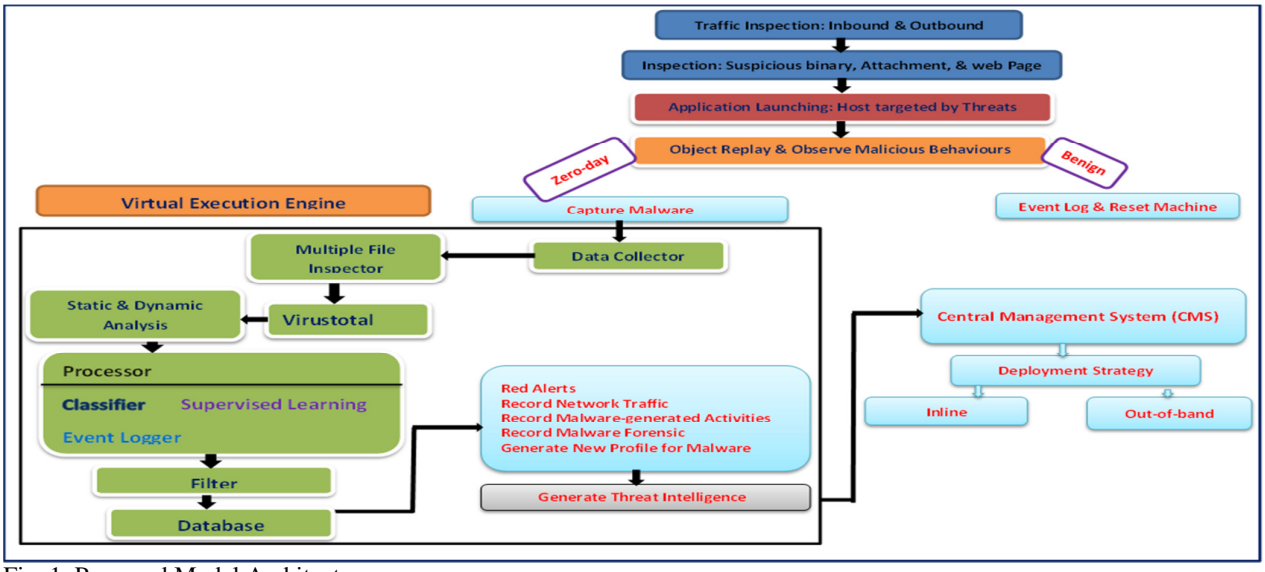

Fig. 1. Proposed Model Architecture

REFERENCE

[1] Adebayo, O. S, Mabayoje M. A, Amit Mishra, Osho Oluwafemi. "Malware Detection, Supportive Software Agents and Its Classification Schemes", International Journal of Network Security & Its Applications (IJNSA), Vol.4 (6), Pp.33–49,2012.

[2] Advanced Persistent Threat Awareness Study Results 2013. Available at www.isaca.org.

[3] Beth E. Binde, Russ McRee, Terrence J. O'Connor . SANS Technology Institute, Assessing Outbound Traffic To Uncover Advanced Persistent Threats, 2011.

[4] Commonwealth of Australia 2009, Cyber Security Strategy. Commonwealth Copyright Administration, Attorney General's Department, National Circuit, Barton ACT 2600 or Available at http://www.ag.gov.au/cca

[5] FireEye, "FireEye Advanced Threat Report – 2H 2011"

[6] FireEye Inc. Cyber Attacks on Government; How APT attacks are Compromising Federal Agencies and How to Stop Them, 2012.

[7] Florian Skopik, Ivo Friedberg, Roman Fiedler (2014). Dealing with Advanced Persistent Threats in Smart Grid ICT Networks. *International Journal of Smart Grid and Clean Energy (IJSGCE), Volume 1(1).*

[8] John R. Johnson and Emilie A. Hogan (2013). A Graph Analytic Metric for Mitigating Advanced Persistent Threat. *ISI*, Pg. 129-133.

[9] Josephine M. Namayanja, Vandana P. Janeja . Discovery of Persistent Threat Structures through Temporal and Geo-Spatial Characterization in Evolving Networks. *In IEEE Intelligence and Security Informatics (ISI,* 2013

[10] Masahiko Kato, Takumi Matsunami, Akira Kanaoka, Hiroshi Koide, and Eiji Okamoto. Tracing Advanced Persistent Threats in Networked Systems Automated Security Management, Springer, 2013

[11] Merete Ask, Petro Bondarenko, John Erik Rekdal, André Nordbø, Pieter Bloemerus Ruthven, Dmytro Piatkivskyi Advanced Persistent Threat (APT) Beyond the hype, Project report in IMT4582 Network security at Gjovik University College, spring 2013.

[12] Mordehai Guri, Tom Sela, Yuval Elovici. Poster: OpenAPT – Open-Source Advanced Persistent Threat for Academic Research, 2013. Available at http://www.openapt.org

[13] Nurul Nuha Abdul Molok, Shanton Changm, Atif Ahmad Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats. *Proceedings of the 8th Australian Information Security Management Conference,* 2010.

[14] Paul Giura, Wei Wang. A Context-Based Detection Framework for Advanced Persistent Threat. *International Conference on Cyber Security, 2012.*

[15] Rohan Mahesh Amin. Detecting Targeted Malicious Email Through Supervised Classification Of Persistent Threat And Recipient Oriented Features. A PhD dissertation, School of Engineering and Applied Sciences of The George Washington University, January 2011.

[16] Simon Meurer and Roland Wism¨uller (2012) "An Infrastructure for Permission-Based Filtering of Android Apps"A.U. Schmidt et al. (Eds.): MOBISEC 2012, LNICST 107, pp. 1–11. Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012.

[17] Victor Yap. "Conficker is Most Detected"

[18] Gartner Research "Email Security Focus Shifts to Address the Risks of Targeted Attacks and Data Loss", Peter Firstbrook, August 29, 2012.

[19] Ned Moran and Alex Lanstein Spear Phishing the News Cycle: APT Actors Leverage Interest in the Disappearance Of Malaysian Flight MH 370, March 24, 2014 Advanced Malware,Targeted Attack,Intelligence, Threat.