Vol. 6, No. 1, January 2015 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Addressing Advanced Persistent Threats using Domainkeys Identified Mail (DKIM) and Sender Policy Framework (SPF)

[1] Yusuf Simon Enoch, [2] Adebayo Kolawole John, [3] Zirra B. Peter
[1] Department of Maths & Computer Science, Federal University, Kashere, Gombe, NIGERIA
[2] Department of Computer Science, Southwestern University, Okun-Owa, NIGERIA
[3] Department of Maths & Computer Science, Federal University, Kashere, Gombe, NIGERIA
[1] simmypukuma@yahoo.co.uk, [2] collawolley3@yahoo.com, [3] zirrapeter644@gmail.com

ABSTRACT

Securing an organization is an increasingly difficult challenge. Attacks are growing in complexity, and the rise of Advanced Persistent Threats (APTs), a type of targeted attack, has made organizations more aware of their vulnerability to attack. Companies have found themselves the target of APTs. APTs persistently collect information and data on a specific target using diverse techniques, examine the vulnerabilities of the target, and then carry out hacking using the data and examination result. An APT is very intelligent, as it selects a clear target and carries out specific attacks, this is unlike the traditional hacking attempts typified by experiences in the previous cyber-attacks which predominantly look to sniff for and steal credit card and other personal identify information. In this paper, we propose a tool that acts like an email gateway that monitors both inbound and outbound traffic for content, context and data integrity for both email and web communications. The proposed tool among other capabilities have the following abilities; inspect malicious web links and attachments in order to prevent initial infection, real time threat analysis capability, strong outbound web detection capabilities for detecting malicious behavior, ability to see inside encrypted traffic and attachment, strong endpoint data loss prevention capabilities to be able to see when most valuable data is leaving an organization. In developing the framework for the design of the proposed tool, the following approaches have been duly incorporated: (i) DKIM- an approach that uses a digital signature to authenticate domain names and the entire content of a message to demonstrate the sender's legitimacy (ii) SPF - An approach that defines which machines are allowed to send mail on a network. The results revealed from exhaustive experiments conducted indicate that the proposed system is able to filter approximately 73% targeted attack.

Keywords: *APTs, Attack, DKIM, Security, Phishing, SPF, Reconnaissance*

1. INTRODUCTION

Advanced Persistent Threat (APTs) is one of the most difficult challenges faced by the anti-virus community. APTs have made headlines in the last few years for breaching some of the most well-known enterprise networks [1]. The term Advanced Persistent Threat was first coined by United States Air force in 2006 to describe the complex cyber-attacks against specific target over a long period of time [2]. It was employed by nation states to penetrate other nation's network for security secrets and other defense data, it is unlike the previous cyber-attacks that went after credit card and other personal identify information.

APTs employ far more sophisticated tactics than other types of attacks. They combine advanced technology with traditional intelligence gathering to gain entry to a network. They then stay hidden for long periods scoping out where targeted data resides and where vulnerabilities exist, and then develop customized attacks to breach these vulnerabilities and seize sensitive data. These blended and stealthy methods circumvent traditional network security that protects against known cyber threat signatures [3].

The methods developed for an APT don't always end with one attack. These techniques are often copied and applied by other perpetrators against other targets, including organizations of all sizes. Eventually, these techniques may be commoditized and turned into malware kits that are readily available to common hackers for a nominal cost [4].

In this respect, the life cycle of an APT may extend for many years beyond its original target and victimize hundreds or thousands of other targets. The figure below shows the exploit code from Aurora APT announced in 2010, which has since been detected on thousands of other sites.

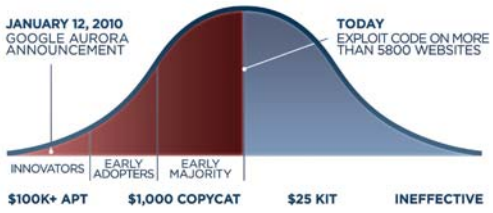

Fig 1: Graph exploits code from Aurora APT [5]

1.1 APT Attack Synopsis

APTs being intelligently crafted have over the years proven to be systemic and methodical in its operations. These can be codified in the following general steps[6]:

1.1.1 Reconnaissance

It is at this stage that the attacker conducts their research of gathering information about the target top-

ranking executives, they also identify vulnerabilities and the best targeting methods.

1.1.2 Preparation

Here, the attacker develops and tests attack tools and techniques.

1.1.3 Targeting

The attackers typically exploit end-point vulnerabilities in the network and/or target end users using social engineering and/or spear phishing to gain access to the network. Common attack methods include: emails with embedded links to websites with zero-day malware downloads; emails with file attachments in common formats like Office or PDFs that include zero-day attack code; infected websites of interest to key individuals identified by social media profiles; and social engineering to gain access to privileged user account info. These methods install custom attack code (e.g. malware) on a host.

1.1.4 Further Access

Infected hosts communicate back and forth with a command-and-control center (C &C). The C &C can remotely update malware, add new malware, and send commands back and forth to locate areas of interest on the network and open additional back doors to find targeted, valuable information.

1.1.5 Data Gathering

The malware gathers valuable data and sends it back to the attacker.

1.1.6 Maintenance

If new data valuable to the attacker continues to become available, the attacker will avoid detection by downloading new zero-day code from the C&C and remain on the network to steal additional information.

1.2 How Attacks are Perpetrated

Using data from social networks such as LinkedIn or Facebook, attackers can craft an email to a targeted user containing some attachment (PDF or ZIP) that entices the user to open it. This attachment could be named such that it would be of interest to their victim in the organization. The employee clicks on the attachment, the malware is inserted onto the users system and sends a signal outbound to a specific domain. This process is continuously repeated with slight differences tailored to the individual receiving the email.

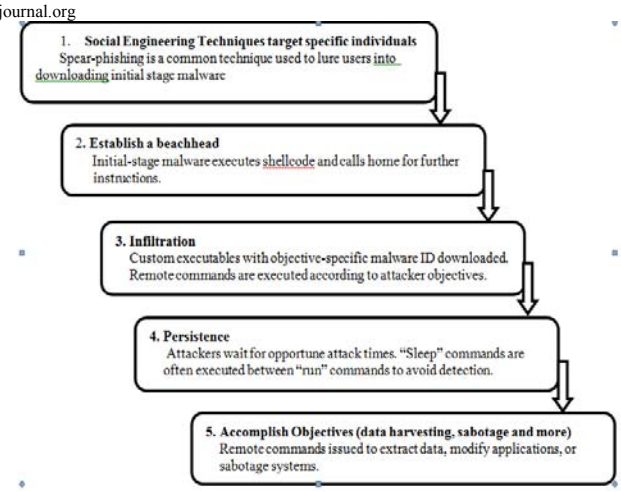

Fig 2: Typical APT Attack Steps

1.3 Problem Statement

An APT is very intelligent, as it selects a clear target and carries out specific attacks, this is unlike the traditional hacking attempts typified by experiences in the previous cyber-attacks which predominantly look to sniff for and steal credit card and other personal identify information [7].

Attackers recently use APTs to airstrike targeted enterprises for financial gains and other business information. This is done in order to steal lucrative intellectual property created from expensive research and to gain access to sensitive customers' data which could lead to business disruption and illegal transaction. APTs are craftier and more sophisticated than ever, using deceptive social engineering techniques to quietly penetrate organization to deploy customized malware that can live undetected for months.

Signature based detection system are ineffective in detecting APT, they are not scalable to the ubiquitous nature of organization networks, signature lacks the ability to identify completely new attacks or even significant variants of the same attack, therefore, a novel approach is required for combating such attacks.
Spear phishing is used as an entry point in an enterprise for launching APTs. In most time, email filters are not effective enough to identify well-designed spear phishing, therefore it takes only a single user to click and open an attachment for an APT to begin to execute its first phase of an attack.

2. RELATED WORK

In 2012, Trend Micro conducted a research on APT, in which they analyzed APT-related spear-phishing emails from February to September and found that 91% of targeted attacks involve spear-phishing emails. And therefore, reinforce the belief that spear phishing is a primary means by which APT attackers infiltrate target networks.

In 2011, security firm RSA suffered a breach via a targeted attack. Analysis revealed that the compromise began with the opening of a spear–phishing email [4]. That same year, email service provider Epsilon also fell prey to a spear-phishing attack that caused the organization to lose an estimated US$4 billion [8].

RSA Laboratories and Professor Ron Rivest of MIT developed a graph-based model that predicts APT attack vectors that countermeasure multiple attack vectors with minimal impact on an enterprise [9]. This particular model depicts avenues of attack (red arrows) and remediation (line cuts/green boxed text) for APTs exploiting compromises in an FTP server alongside a social engineering attack using malware (figure below).

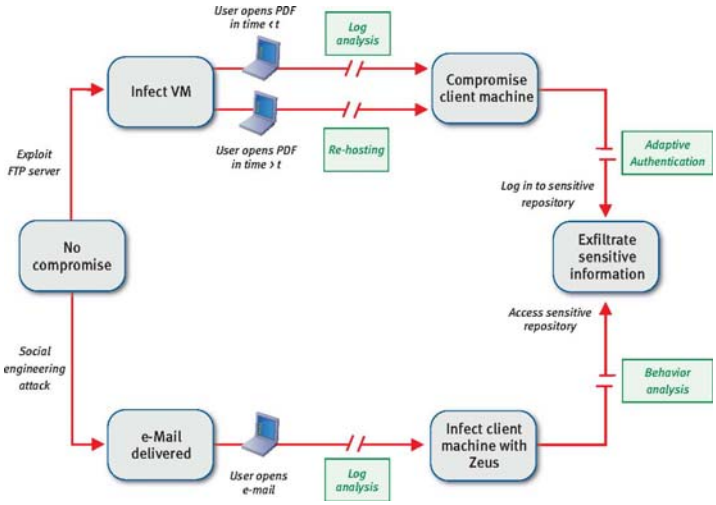

Fig 3: Graph-based model for predicting APT attacks [9]

On the other hand, [6] proposed an attack model for the detection problem as well as methodology to implement the detection system on a generic organization network by using a prototype multiprocess implementation of Map Reduce. They introduced the attack pyramid model and provided an APT detection framework that takes into account all the events in an organization.

Curry et al. [9] developed theoretical models to help organizations devise defenses for known APT techniques by employing game theory principles. Their threat models were used to identify which parts of an IT environment need to be strengthened, either through additional security precautions or complementary tools.
Binde et al. [10] considered four distinct countermeasures to the advance persistent threat, the approach they took included well known signature based methodology, manual analytical practices, statistical tactics and correlation concepts, as well as automatic leak prevention.

3. METHODOLOGY

In this section, we describe our approach, explain how we collected emails for testing and describe our evaluation methodology. Further explained employed DKIM and SPF and their integration as implemented in the proposed system.

3.1 Domain keys Identified Mail (DKIM)

Domain Keys Identified Mail is a signature/cryptography-based email authentication framework that provides a method for validating an identity that is associated with an email message during the time it is transferred over the Internet. It provides email users with an additional level of protection against email forgery. Below, we give a synopsis of the operational elements of DKIM adopted.

3.1.1 Identity that is Authenticated

DKIM allows the signer to choose any Domain Name, which is indicated in the DKIM Signature: header field of the message. Whether that Domain Name is related to another identifier in the message, such as the From: or Sender: fields, is a separate decision.

3.1.2 Authentication Mechanism

The responsible organization adds a digital signature to the message, associating it with a domain name of that organization. Typically, signing will be done by a service agent that is part of the message author's organization or delegated by them. Signing will be performed by message transport agent (MTA). DKIM permits signing with a particular domain name to be performed by authorized third parties, such as having an originating organization obtain a signature by an independent assessment (reputation) organization and affixing the signature to the message.

3.1.3 DNS Query Mechanism

DKIM envisions a new DNS resource record but defines a TXT record for initial use. It is placed under a special sub-domain of DNS, which is underneath the

domain name declared in the DKIM-Signature: header field. Any TXT records under that sub-domain name are only for DKIM use. The special portion of the sub-domain has a field, called the selector, which is used for key management. So the DNS query string has multiple fields, with only a portion intended to be used for actual reputation assessment. That is, a core domain name represents the organization. It is then combined with an administrative sub-name so that keys can be assigned more conveniently. This is necessary for control over signing by different individuals or systems, as well as for migrating to a new key.

The DKIM DNS record has some parameters for constraining its use to particular services or addresses. However the record only validates an existing signature. Publishing additional email signing practices (SP) for the domain is the subject of separate follow-on work.

Example:

Header from an email newsletter:

Received: from gombenet.demoibadan.com (HELO gombenet.demoibadan.com) (16.0.0.1) by mailserver.company.com with SMTP; 20 Jan 2014 19:53:28 -0000
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=demoibadan;
d=authorscompany.com;
h=From: To: Subject: Mime-Version: Message-ID: Content-Type: Date;
i=author@authorscompany.com;
bh=EMR7D1qC7ykz41K8ArLCt++IWxM=;
b=TGkNEq7fW4OIno/5DlX2qHDQeRmzhY+uiTzEcxu2
KIKC+4B7+i2olIWGZP9JBnOR4Ck6iAiidnRj
DLuc2QJh3ifDNPWJ6xYjiuE73ilCZfbtN0r2MVke9pRU
4aydBQ5DSCFS7YhUFB22CT70MutZkaDF
SZZpqI5vTlSWm9MI8PM=
Date: Mon, 20 Jan 2014 11:42:15-0500
From:"Author" <author@authorscompany.com>
To: Recipient@company.com
Subject: January Newsletter
Sender: authorscompany@demoibadan.com
Return-Path: bounce-4101674@authorscompany.demoibadan.com
Mime-Version: 1.0
Message-ID:
<20080324040103985572.328428@mx12.emailroi.com>
Content-Type: multipart/alternative;
boundary="==========_email ROI_=========="...

3.2 Sender Policy Framework (SPF)

SPF is an email validation system designed to detect and block forged or spoofed emails. This is done by verifying the sender's email server before delivering all legitimate email to a recipient's inbox. SPF allows an agency to specify which servers are allowed to send emails for their domain and makes this information available for recipients to check. This is achieved when the network owner creates an SPF entry in the Domain Name System (DNS) record for their domain. The SPF entry will contain a list of domains or valid IP addresses authorized to send emails for their domain.

When an email is sent to a network with SPF checking enabled, the recipient email server validates the sender's domain against the published SPF record. That is, it confirms that the IP address of the sending server is on the allowed list for the domain; if it does not match, SPF verification will fail. A synopsis of the operational elements of the SPF follows.

3.2.1 Identity that is Authenticated

SPF uses the IP Address of the SMTP neighbor and maps it to the Domain Name in the MAIL FROM Return command of SMTP (also known as "Return-Path:") and/or the HELO/EHLO SMTP command. The latter name is explicitly provided by the neighboring SMTP client host to label itself. It is probably more helpful to view the IP Address as the identity, with the mapping being useful for aggregating a number of different MTAs' IP Addresses under the same organizational reputation.

3.2.2 Authentication Mechanism

SPF uses path registration. A site that is validating a message receives it from a neighboring MTA. It uses the IP Address of that neighbor and the Domain Name in the SMTP MAIL FROM Return and/or the HELO/EHLO commands for the message. Validation consists of finding the IP Address registered under the Domain Name.

Querying on the MAIL FROM Return command is mandatory, according to the SPF specification. Querying the HELO/EHLO command is recommended.

3.2.3 DNS Query Mechanism

The owner of the MAIL FROM and/or HELO/EHLO Domain Name registers a record in the DNS that contains the IP Address of each MTA that will be the closest neighbor to a validating MTA that is authorized to send mail on behalf of the domain. When the validating site queries the DNS for the domain in the MAIL FROM Return command, it will find that the neighboring MTA's IP Address is registered under it. This means that the Address is authorized to send email containing that Domain Name in the MAIL FROM and/or HELO/EHLO commands.

SPF defines two choices for recording information in the DNS. One defines a format to be applied to the existing, general-purpose TXT RR record. The other is a new SPF RR record. Because it has proved challenging to obtain widespread deployment and use of new DNS RR records, it is common to define an interim alternative, such as the SPF specification has done. One issue with having different standards specify different definitions for TXT content is distinguishing which application service applies to a particular record. SPF

identifies its TXT records by including a v=spf1 parameter inside.

Whether coded as a TXT or SPF RR, the SPF DNS record is intended to be a rather flexible means of publishing a variety of email service practices information rather than only for registering authorized systems. This includes registering addresses that are not authorized, alternate mechanisms that are authorized, and even recursive references that derive authorization information from other records. This flexibility can make it challenging to create records that accurately reflect the policies of a registering organization. Consequently administration software has been developed to facilitate the process of specifying a SPF DNS record for the most common configurations.

Example:

Header from an email newsletter:

Received: from gombenet.demoibadan.com (HELO gombenet. demoibadan.com)(16.0.0.1)
by mailserver.company.com with SMTP; 20 Jan 2014 13:46:22 -0000

Date: Mon, 20 Jan 2014 11:42:15 -0000
From: "Author" <author@authorscompany.com>
To: Recipient@company.com
Subject: January Newsletter
Sender: authorscompany@demoibadan.com
Return-Path: bounce-4101674@authorscompany.demoibadan.com
...

The validating MTA will extract the MAIL FROM and HELO/EHLO domains as authorscompany.gombenet.com and demoibadan.com respectively. When the validating MTA queries DNS for these domains it receives the following SPF record for both domains:

v=spf1 ip4:10.0.0.1 mx ~all

The validating MTA then compares the neighboring MTA's IP address from the Received: header to the IP address or addresses in the SPF record and determines that the neighboring MTA is authorized to send email for the Domain Name in the MAIL FROM and/or HELO/EHLO commands.

4. THE PROPOSED FAIR PRIORITY MAC(FP-MAC) PROTOCOL

This paper presents a novel approach for combating APT using Domain Keys Identified Mail and Sender Policy Framework. Both mechanisms were selected in order to thwart many of the threats inherent in using either protocol. For example, messages that break the DKIM authentication process can still be authenticated via SPF. Likewise, a forwarded message that fail SPF authentication can still be appropriately authenticated using DKIM. The combined use of the two protocols reduces the number of false positives and can increase the receiving network's confidence in authentication, to the point of being willing to start blocking messages that fail both authentication processes. In addition, this strategy enables companies to have their messages authenticated at ISPs that only support one of the two protocols, as ISP support of both protocols is not currently available in many cases [11]. ISPs today have not yet implemented blocking/failure based on authentication results. Furthermore, DKIM is transparent and compatible with existing email infrastructure and has no dependency on the deployment of any new internet protocols. DNS is used as Database because of its convenience; the infrastructure is already deployed and has proven to be stable and scalable.

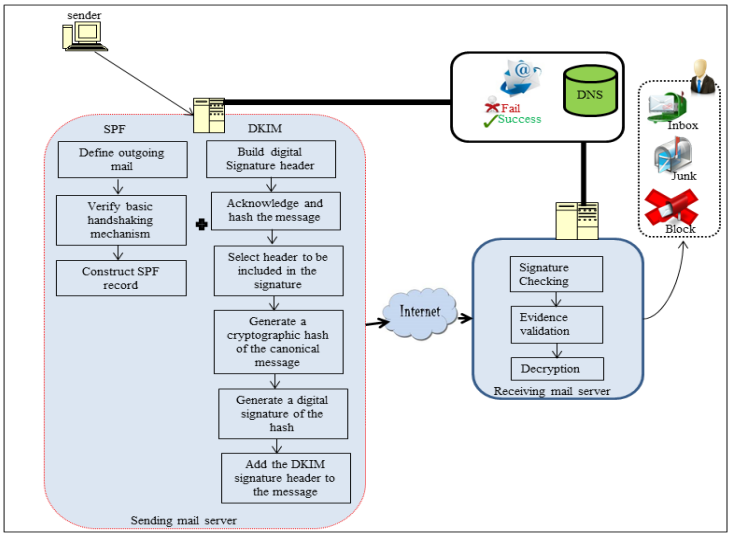

Fig 4: The Proposed Hybrid Architecture for combating APT

4.1 Operational Procedure

We present the operation of the proposed system as a 10-step simple procedure described below.

i. The sender composes a message and hits 'send,' which causes the message to be transmitted to the sending mail server.
ii. The sender server publish public key in DNS and then sum using SHA256 [12] [13] is calculated on selected header for sending an Email. SHA256, hash algorithm is used to generate a cryptographic hash for the undisputed message. A hashing algorithm takes a variable length data message and creates a fixed size message digest.
iii. The sender server generates a digital signature of the message using a public key encryption scheme called RSA [14]. Then the signer signs the hash using the RSA encryption algorithm in the signature header, and adds it to the beginning of the message header fields.
iv. Finally the encrypted content will be added in the DKIM header. The Sending Mail Server identifies the recipient, processes the message, constructs the message headers, and sends the message to the recipient's mail server.
v. The receiver server now look-up the public key using DNS, decrypts the hash value and verifies the received sum and also verify handshaking connection.
vi. The Receiving Mail Server processes the incoming message.
vii. It then queries the sender's DNS entry for the relevant authentication information, which it uses to validate the authentication.
viii. The Receiving Mail Server uses the authentication information to validate the incoming message.
ix. The receiver's back end processing combines the results of the authentication with any relevant reputation data and content filtering to determine whether the message will be delivered to the recipient's inbox, Junk folder, or whether it will be blocked completely.
x. Finally, the recipient will be able to access the message the next time email status is updated, assuming it has not been block.

5. RESULTS AND DISCUSSION

We created an e-mail account (dayo.demoibadan.com) within a specific domain name and forge some other email addresses from another domain (e.g. simon.demoibadan) to have the same domain name as the earlier (demoibadan). We created and sent different illegitimate mails to dayo from simon using phishing email generation tool. We succeeded in sending over 264 mails. We selected 200 electronic mails randomly from our corpus of mails created. To confirm the actual domain from which the e-mail originated, we pick the received "from:" and "mailed-by:" at the header view of the mail. We run the e-mails through specific open-source email and domain tracers such as IP Lookup [15] and email Tracer. We obtained and confirmed the result.

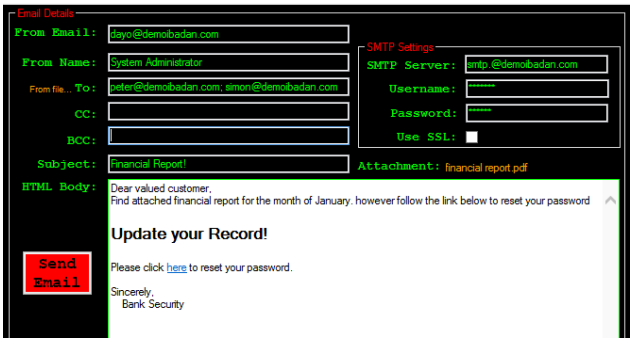

Fig 5: Screenshot of the system showing illigitmate mail/domain name

For effective testing and evaluation of the implemented proposed system, we used a lab environment on windows platform. The proposed system was implemented wholly in JAVA. We configured and tested our proposed system with the selected 200 mails from the same domain earlier sent plus 30 mails within the legitimate domain. The result of the test is shown below:

Table 1: Number of mails used

	Mails	Positive	Negative
Illegitimate	200	148 (True Pos)	52 (False Neg)
Legitimate	30	19 (False Pos)	11 (True Neg)

True positive: tool classified illegitimate mail as illegitimate

i. True negative: tool classified legitimate mail as legitimate
ii. False negative: tool classified illegitimate mail as legitimate
iii. False positive: tool classified legitimate mail as illegitimate

$$FalseNegRate = \frac{FalseNeg}{FalseNeg + TruePos} \quad (1)$$

$$FalseNegRate = \frac{52}{52 + 148} = 0.26 \quad (2)$$

$$FalsePosRate = \frac{FalsePos}{FalsePos + TrueNeg} \quad (3)$$

$$FalsePosRate = \frac{19}{19 + 11} = 0.63 \quad (4)$$

Table 1.0 shows the number of phishing emails flagged in the experiment and the total number of emails being flagged by both heuristics. From the table, we can see that we used 200 confirmed phishing emails and 30 confirmed legitimate emails for the experiment. Our hybridized system flag 167 emails representing 73% as being suspicious (spam), which was manually confirmed to be positive. On the other hand, 63 emails representing 27% were flagged as legitimate emails, however, it was manually confirmed that only 11 emails were legitimate while the remaining 52 emails were illegitimate.

The results revealed from exhaustive experiments conducted indicate that the proposed system is able to filter approximately 73% targeted attack. Therefore, the proposed hybridized system will be a useful tool for combating Advance Persistent threat.

6. CONCLUSIONS

There is currently no single standard that will solve the problems with targeted attacks and other fraudulent behavior [16] [17], it must be recognized that several standards must co-exist and work together in order to attain a formidable security that will frustrate attackers. That has been the aim of this paper to present a new approach in the overall process of eliminating the first stage of APT and other fraudulent behavior on the internet. DKIM and SPF have been proposed as a way to limit the risk of Advance persistent threat with hybridization of the two schemes. Our work shows the proposed model would improve the security of an organization and reduce targeted attack on a network.

Further research can address DKIM and SPF insensitive to reply emails. (for instance since some emails can be sent without valid DKIM Signatures).

REFERENCES

[1] Gamer T., Anomaly-based Identification of Large-Scale Attacks. Proceedings of the 28th IEEE Conference on Global telecommunications, pages6638 – 6643. IEEE Press Piscataway, USA, 2009.

[2] Bejtlich, R., What Is APT and What Does It Want? Tao Security. Accessed 1st June, 2013. Available http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

[3] ISACA, Advanced Persistent Threat Awareness: Study Results. Accessed 3rdMay, 2013. Available http://www.isacantx.org/Presentations/2012-05%20Lunch%20%20Advanced%20Persistent%20Threats.pdf

[4] Rivner, Uri, Anatomy of an Attack. EMC Corporation. Accessed 13th October, 2013. Available http://blogs.rsa.com/rivner/anatomy-of-an-attack/

[5] Websense. White Paper. Advanced persistent threats and other advanced attacks: Threat analysis and defense strategies for smb, mid-size, and enterprise organizations. Accessed 13th October, 2013. Available https://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf

[6] Giura, P. and Wang, W., Using Large Scale Distributed Computing to unveil Advanced Persistent Threats. Science Journal. Vol 1, No. 3, 2012.

[7] Yusuf, S. E., Adebayo, K. J. and Adetula, E. O., Mitigating Cyber Identity Fraud using Advanced Multi Anti-Phishing Technique. International Journal of Advanced Computer Science and Applications (IJACSA) Vol. 4, No. 3, 2013. pp 156 – 164. Accessed 27th January, 2014. Available http://www.thesai.org/Downloads/Volume4No3/Paper_25-Mitigating_Cyber_Identity_Fraud_using_Advanced_Multi_Anti-Phishing_Technique.pdf

[8] Matthew J. Schwartz, Epsilon Fell To Spear-Phishing Attack, InformationWeek. Accesed 13th October, 2013. Available http://www.informationweek.com/news/security/attacks/229401372

[9] Curry, S., Hartman, B., Hunter, P., Martin, D., Moreau, D.R., Oprea, A., Rivner, U., Wolf, D. E., RSA Security Brief: Mobilizing Intelligent Security Operations for Advanced Persistent Threats. Accessed 1st June, 2013. Available http://www.emc.com/collateral/industry-overview/11313-apt-brf.pdf

[10] Binde, B.E., McRee, R., O'Connor, T.J. , Assessing Outbound Traffic to Uncover Advanced Persistent Threat. SANS Technology Institute. Accessed 1st June, 2013. Available http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf

[11] BIT Security, Email authentication policy and Deployment strategy for Financial services firms. A publication of the bits security program February. Accessed 13th October, 2013. Available http://www.bits.org/publications/security/BITSEmailAuthenticationFeb2013.pdf

[12] Kashefa K. K, Saruladha.K, Packiavathy.M, A DKIM based Architecture for Combating Good Word Attack in Statistical Spam Filters. International Journal of Scientific & Engineering Research Volume 2, Issue 6, June-2011.

[13] Computer Security Resource Center (CSRC). Descriptions of SHA-256, SHA-384, and SHA-

512. Accessed 27th January, 2013. Available http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf on 27th January, 2014.

[14] Evgeny M., The RSA Algorithm Accessed 13th October, 2013. Available https://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf

[15] IP Lookup . Accessed 13th October, 2013. Available http://www.ip-tracker.org/

[16] Yusuf, S. E. and Longe O., "Hybrid Spread-Spectrum TCP for Combating Fraudulent Cyber Activities against Reconnaissance Attacks," The African Journal of Information Systems: Vol. 5: Iss. 2, Article 1, 2013. Available at: http://digitalcommons.kennesaw.edu/ajis/vol5/iss2/1

[17] Longe, Olumide Babatope, Yusuf, Simon Enoch, Egbedokun, G.G.O. and Adewole, O.A. , Scalable Knock Authentication Mechanism (SKAM) for Addressing TCP and UDP Probe Vulnerabilities in Open Network Ports. IEEE African Journal of Computing and ICTs. Vol 4. No. 1. June, 2011. pp 45 – 50. Available online at: http://www.ajocict.net/uploads/Longe__Yusuf__Egbedokun___Adewole_-_Scalable_Knock_Authentication_Mechanism___SKAM__for_Addressing_TCP_and_UDP_Probe_Vulnerabilities_in_Open_Networks.pdf

AUTHOR PROFILES

Yusuf Simon Enoch, is a Lecturer and a PhD Student, His research interest includes Network Security, Ubiquitous computing and ICT Diffusion in developing countries.

Adebayo Kolawole John, Ph. D. Student and also a Lecturer with Southwestern University, Nigeria. His main research interests include Intelligent Systems, ICT adoption and use, Computer Vision and Image Processing.

Dr. Zirra B. Peter, Lecturer and the current Head of Department, Mathematics and Computer Science, Federal University, Kashere, Gombe, Nigeria. His main research interests include Computer Security and Computer vision.