PROTECTION FROM ADVANCED TENACIOUS THREAT IN WEB APPLICATION

Lalita (M.Tech)
Monad University-Hapur, Uttar Pradesh

1. Abstract

Now days the number of web based attacks are increasing considerably. The advanced persistent threat, group of very skilled, sophisticated and well organization people used to exploit that vulnerability to inject some malicious code into the system to extract valuable information. These attacks are quite dangerous and hard to treat than other type of attacks. In order to protect our system we need to protected web application that will help attacker to launch their code into the system and remain undetectable for long period of time. The adaptive phishing and spear phishing technique, cross site scripting, SQL injection etc. are commonly known tricks used by attacker. In this paper, first we description a model that help to understand various attack vectors used for launching and triggering of APT attacks. Second describes a framework, which can be used as a roadmap to analyze, prevent and detect the APT activities inside the application, system and network.

2. Keywords

Advanced persistent threat (APT), Web Application Security, Cross site scripting (XSS), Cross site request forgery (CSRF), SQL injection Attack (SQLIA).

3. Introduction

Originated from the military sector, advanced persistent threats is another more sophisticated entity in cyber world. Advance Persistent Threat are pioneer attackers who are well organized, skilled and well-funded and emerges as most dangerous and fast growing security threat[2]. These attacks are hard to detect as security mechanisms bypassed with some proficient tricks that spoof victim or in many case identified but after execution for long period of time [1]. These attacks are impractical to prevent but may be refracted toward other target to make the attack unprofitable and difficult [2]. These techniques are used by intruders to grab sensitive information. Intention in such attacks may vary from monetary gain; gather victim's credential or other sensitive information. Intention in such attack may vary from monetary gain; gather victim's credentials or other sensitive information. The APT attacks are widely launched through email based tricks such as spear phishing that are further backed by some external technique of exploitation. APT attackers mostly use web driven exploitation starts from social engineering and phishing, takes advantage of economy of scales and breaks into as many sites as possible. Due to unawareness, insufficient training and ignorance of user creates back door entry for the attackers [3] using web application for example social networking web sites.

Employees are not restricted to access organization`s application from home to complete the pending work that attracts attacker towards reconnaissance [1, 2]. Phishing is
Another type of trick commonly used with social

engineering to obtain victim`s credentials that may help attacker to gain access into the system [4].Spear phishing attacks are reported as widely used trick by APT done through an email having malicious link, clicking on that link user may be redirected to malicious location /page or installs/downloads malicious program code in to the users computers [2,4]. An APT attack is extremely difficult to discover because it changes itself so much that it appears to be entirely new. These types of attacks are ultra-sophisticated, continuous and well organized. Fixing the past vulnerabilities won`t help preventing APT; Focusing on the existing vulnerabilities is very much required. Stealth a being covert and look as close to legitimate traffic are the main goals of attack and the difference is so minor that many devices cannot differ between them. Attacker just doesn't want to attack and leave but desires a long term access. APT`s can do insidious damage long before an organization knows that it has been hit. APT can use a range of tools, from common malware to complex, zero-day threat tactics to achieve their goals. The two categories of attacks that are quite common and dangerous to every web application are SQL injection (SQLIA) and a site scripting (XSS) attack [6].In SQLIA the attacker take advantage of programming flows and executes the malicious database queries which may lead to injection of malicious code into the system. In XSS the attacker executes the malicious code on victim`s machine by exploiting the inefficient or improper data validation check that may lead to injection of malicious code into the user machine [6], Cross site request forgery (CSRF) attack that used by APT to launch their code it occurs when A malicious site cause unwanted activities over legitimate web site and known as "sleeping giant", because on internet user fail to identify these attacks [7].

4. Related work

In recent past year`s lots of study has been carried out on advanced persistent threats by various, origination, institutions and researchers. The work presented in [1] gives information about APT but does not address its connection with web security threat. the study presented in [12]considers the phishing and spear-phishing attacks, proposed a detection model , this system will work in real time processing of traffic and monitoring but mitigation of web based attack are untouched. The study given in [11] provides good sense of existing techniques and their limitations for preventing these attacks. The indeed study focused towards network and system security, even it considers that application like web browser is crucial to attackers because of its extensible nature and requires an extra bit of security put across it. The study given in [13] adopts data leak prevention algorithm to improve prevention techniques against APT but new generation attacks and threats are more complex in nature, this paper talks about the detection of malicious codes but the attacks and threats are more complex in nature, this paper talks about the detection of malicious codes but the attacks by which these codes will be injected are not discussed. The model given in [3] gives good explanation on spear-phishing attack used by attacker to launch their code into the victim's machine or network but ignore other attack like SQLIA etc. the intended study in [14] is about the exploitation of zero day vulnerabilities and presented a framework that addresses the cyber counterintelligence processes used as toll to deal with such attack. Intrusion detection system with counterintelligence sensor and fingerprint database give desired protection but consideration of web flaws have equal importance to make this framework more robust.

5. Attack Model

In this section we first describe the attack and later explain the corresponding defenses with the help of attack tree and defense tree concept. We introduce new model to understand how APT targeting the victim and what are the defense techniques to be used in an organization to cope up with the situation when an attack events occurs. This is a hybrid model suggested by Edward Amoroso and Bruce [8].

5.1 Attack Tree

We are explaining the attack of APT with the help of attack tree concept [8, 9]. These modeling help to understand about attackers, attack and their goal. Security assumption and where the best place of spending security budget. Figure 1 explains the attack for APT.

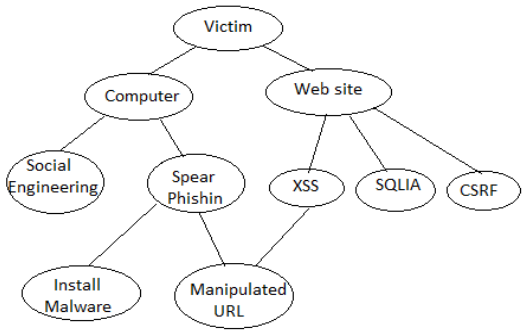

Figure 1: APT aimed to launch malicious code in Victim's machine

The above diagram shows how the victim can be targeted by APT to exploit in their own way. The above started model is based on the technique described by the Bruce Schneider [8], where leaf node are the describe result that might be helpful for the attacker to launch their malicious code. The round nodes are called attack nodes. The parent node is connected with is child node with an arrow, where the two arrows are connected with an arc shows AND relationships and arrows without an arch show OR relationship. In APT attack, the victim can be targeted in order to compromise the required information either through its computer or through its web site. In order to launch their malicious code APT uses some social engineering along with spear phishing, which is sending some malicious link on victim's email and due to ignorance he might click on that link which further redirect him to order location or install some malware in his machine. The victim can be targeted through in web site or any other web application that he may use. By exploiting the existing vulnerabilities of web site through SQL injection attack, XSS attack and CSRF attack, attacker got success to launch malicious code into the web server or other targeted machine. In SQLIA unintended database query execute on the database server lead to disclose sensitive information that may further lead to more dangerous and complex attack. These attacks may use separately or backed by one or more attacks. Now we propose a defiance tree model where each node I called as defense node which can be used as a countermeasure for corresponding attack tree.

5.2 Defense tree

We are explaining here the defense against APT attack with the help of tree based diagram. This is defense tree which is very similar to the attack tree figure 2 shows how various defense techniques might be useful as countermeasure of attack discussed in previous section. The attacks are shown with red ovals and defense show with green rectangles.

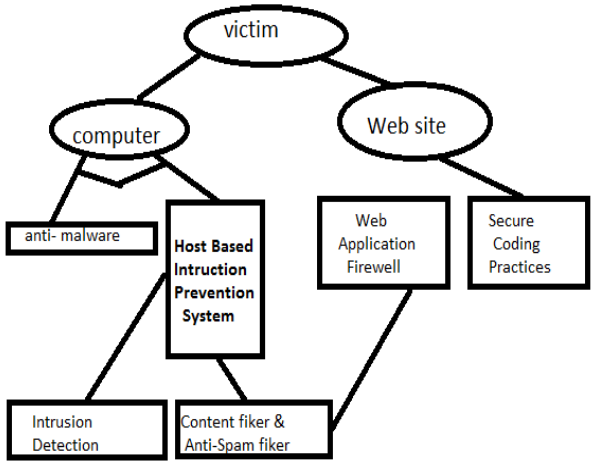

Figure 2: Victim aimed to defend against APT

The anti- malware and host based intrusion prevention system (IPS) WORK together in order to reduce the possibility of attack. They identify suspicious events through security mechanisms that have some abnormal activity, for example if an event occurs of file uploading of a large size in internal network that will be treated as suspicious event because in normal time no such event been reported in past history. For example active network traffic having known binary source code distributed in different packets. Content filtering methods are also useful in order to cope up with or suspicious URLs which is based on content screening and denies the access of web page or e-mail that is unexpected or deemed to objectionable. it is a part of internet firewall categories into two parts. One is web-filtering, used for screening of web page or site and other is email- filtering, used for screening of email for span and other network. it collects information from various parts inside the computer and network to analyses the possible malicious security event. the prevention of APT is difficult but can be detected and corrected by related security measures which comes by assessing , monitoring , analyzing , tracking and alarming against abnormal or suspicious events. The web application firewall provides security to web application against various threats commonly listed on OWASP top ten. It provides automated and adaptable security against SQLIA, XSS, and CSRF.

6. Protection Framework

In this section we intent a security chassis for web application from APT. Figure 3 shows our purpose model, mapping to attack and defense model as follows. Prevention and detection are two entities, works together provide complete protection. Prevention system gives it feedback to detection system collects input data for protection system.

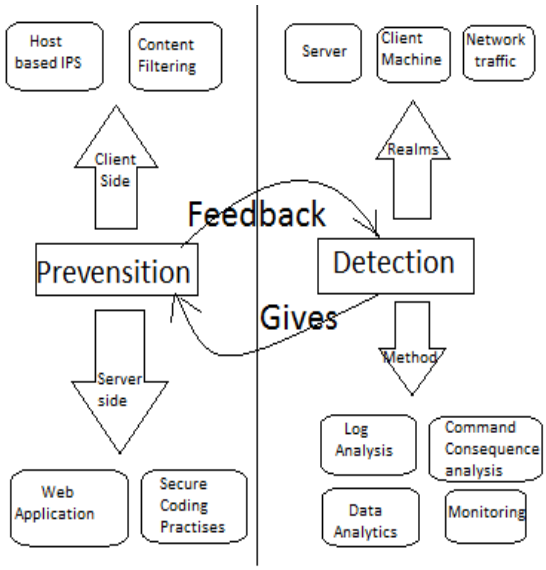

Figure 3: Protection Framework

6.1 Client side prevention

6.1.1 Host based IPS

It is a software system which is installed into the client machine and continuously monitors suspicious activities behavior of inbound traffic by analyzing signature, anomalies and protocols.

6.1.2 Content filtering

It is the technique realized by software system also called as content blocking. Content censoring and content control software. It denies any unintended contend discovered on the basis of policy and signature of content, especially inherited with web, email or some other ways.

6.2 Server side prevention

6.2.1 Web application firewall

It is software plug-in or content filter hat work on set of policies or rules governs whole HTTP communication. It performs comprehensive checks and validations for popular attacks such as SQLIA and XSS attack. By customizing in many other attacks can be accepted and stop its execution.

6.2.2 Secure coding practices

These are the guideline for the web application developers in orders to reduce vulnerabilities that come due to bad programming practices. For ex, to prevent the SQLIA, OWASP secure coding practice guidelines give few suggestions that always use prepared Statement. Callable Statement and stored procedure to execute database queries. Comply with these guideline does not provide full protection but the chances of attack would surely go down.

6.3 REALM

Detection requires location in which validation checks could be performed. We performed three locations. Where detection mechanism may perform its works .first is server, it could be an application server, web server, database server or combination of these. These locations are very crucial because its holds data that has very high level of sensitivity. Attacker aimed to target this location due to high probability of chance to get success their attack. Hence detection should focus on this area. Second is client machine, where signature or footprints of attack may found because APT target a particular individual, which is vulnerable and easy to exploit in comparison to other, to perform their malicious activity. the third is network traffic, one of the important realms in order to find out the malicious activity inside the network by analyzing the data packets, controlling , prioritizing and measuring the traffic to determine the root cause of attacks.

7. Methods

Here we propose the method to be used for detection APT attack. A deep log analysis gives us the senses on legitimacy of activities carried out and help to identify the malicious pattern. These patterns served as indicator to begin detecting the activity done by the attacker. Command consequence analysis is another method which is used to detect the attacks. Commands are set of instruction works together in order to complete a desired task. Commands are delivered in an ethical way that should not make any harm to the computer environment. Unethical delivery of command and its respective consequence create alert signal for the analyst to react accordingly.

Data analytics is digging out meaningful information from various pattern generated during communication. It uses statistical based approach to visualize the operation performed solely based on signatures, anomalies & policies [1]. In order to maintain effectiveness of detection requires to regular updating the signature database. A defined static policy governs the organization's traffic flow, identification any changes in the behavior of intended traffic and gives appropriate response against them. Monitoring of active data packets flowing though the network should be carried out continuously. Program code with in the application should have been monitored, by program like reference monitor, ensure the integrity of existing code and also while on

execution code does not do any harm [11]. If malicious codes cause damage to computer resource such as important files, software code, device drivers' etc. recovery is the only possible solutions. In this regard several tool are available in the market that could properly address and access the problem.

8. Methodology

The research paper is an outcome web application testing and auditing in which around 30 websites were tested for vulnerability which can be threat to both the web server and the end user. the testing results are solely based on attack performed and related response given by owner of web site. diagram based describe the type of attack performed on these sites and obtained knowledge between the impact and ease of attack. A chunk of website which had a responsible disclosure program was tested for the top 10 vulnerabilities and beyond. Vulnerabilities like XSS, CSRF, using servers with known vulnerabilities; SQL, click-jacking, authentication flaws were performed. A short glimpse of above vulnerabilities is given below.

8.1 XSS (Cross Site Scripting)

A cross site scripting is an exploit where the attacker injects a malicious code to a link that appear to be legitimate . this attacker than sends this link to the victim, which on being clicked executes the malicious code on to the victims system typically allowing the attacker to gather sensitive information about the victim. The vulnerability appears due to scripting flaws, code embedded inside HTML head or body to enhance page's dynamic loaded capabilities and extensibility of their features.

8.2 SQL Injection

In this attack the user sends his input in such a way that it gets executed with the original sql query as a part. This leads to unexpected behavior from the database. An attack r for can even bypass the authentication if the wasp is vulnerable to login SQL injection. A comprise in the database will lead to a hell lot of information disclosure.

8.3 Click jacking

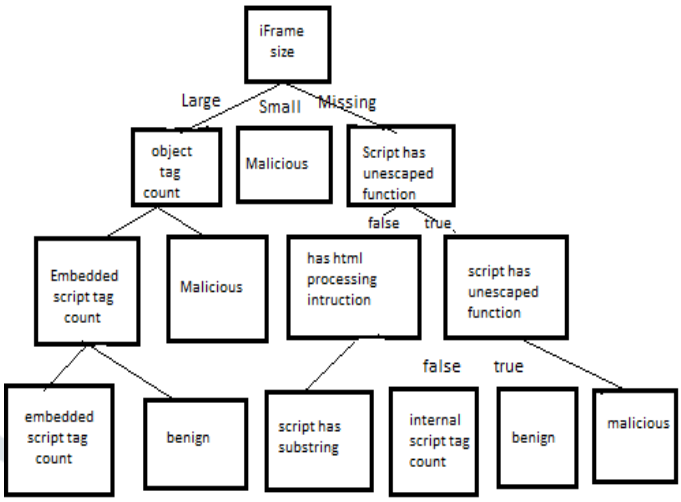

Figure 4: Decision tree [Source: [15]]

8.4 CSRF (Cross Site Request Forgery)

CSRF (Cross site request forgery) also called as one click or session riding or XSRF is an attack where in the attacker fools the victim browser into making a request the user didn't intend to. Fir any website your browser is who you are. The website recognizes you on the base of IP address of its traffics, header and cookies and links it request. The CSRF attacks hold the nix identity by manipulations the victim's browser into making request against a website on the attacker's behalf. The attacker relation to the site is immaterial; in fact the website never sees traffic from the attacker. Some people consider phishing attack as CSRF, although it can be part of one. In a phishing attack we manipulate the user into initiating a request from the browser whereas in CSRF forces the browser into initiating a request. It's not that the attacker has gained access to the victim browser but yes he had made the browser to something that the user is unaware of.

8.5 Using servers with known vulnerabilities

A kind of vulnerability where the server on which the web application is hosted itself vulnerable to attack. This vulnerability is possible in cases where the web server used is mostly outdated and several public exploit are available for the same. Revealing the specific software version of the server may allow the server machine to become more vulnerable to attack against software that is known to contain security holes.

9. Challenges

We have performed various web based attacks on 82 websites, exploit their web pages and got success in order to find a way where we can inject a malicious code of script. We have responsible disclosed those vulnerabilities to then that exists in

their web page distinguished by URL and discussed the framework that we proposed here in this paper to make a better protected environment on any organization. Out of 82 companies only 30 have acknowledge us, rest of them does not respond , some of them respond with a justification that identified flaws is not vulnerability and they do not feel that it could do any harm towards its security requirement. This framework is appreciated by everyone except few of them , status two big implementation issues, one is the times required and other is the budget.

10. Conclusion

This paper gives a good protection framework in order to protected web application from APT. our framework gives protection from 1) SQLIA, 2) XSS, 3) CSRF, 4) Spear – phishing, common attacks used to launch malicious code into the targeted machine or network. This paper could not be used see APT in different aspects that are not seen by others and gives a customized approach to deal with such attack or events. In future, we shall explain the implementation and related challenges of the proposed model and also provide statistics to prove its effectiveness.

11. References

[1] Paul giura and Wei Wang, "a context based detection framework for advanced persistent threat in"IEEE ASE international conference of cyber security "Washington DC dec-2012 pp. 69-74.

[2] Sam curry, Bret Hartman David Martin, "mobilizing intelligent security operations for advanced persistent threat "RSA security brief, February 2011.

[3] Nalin asanka gamagedara arachchilage, Melissa Cole " Designing a mobile game for home computer user to protect against phishing attack" Brunel university Uxbridge Middlesex

[4] Mahmood Khonji, Youssef Iraqi, Andrew Jones "Mitigation of spear phishing attacks: a context based authorship identification framework"6th International Conference on internet technology and secured transaction" from 11-14 December 2011, Abu Dhabi, United Arab Emirates pp 446-45

[5] Christian seifert, Ian welch , Peter Komisarczuk "Identification of malicious web pages with static heuristics" victoria university of wellington, P.O. Box 600, Wellington 6140, New Zealand.

[6] OWASP foundation (2003-2013) "OWASP top ten 2013" [online]available:https://www.owasp.org/index.php/Top_10_2013 -Top_10 Last modified on June 2013,Accessed

[7] William Zeller and Edward w. felten " cross-site request forgeries :exploitation and prevention " Woodrow Wilson school of public and international affairs , Princeton University revision 10/15/2008

[8] Bruce Schneier "attack trees" SANS network security Conference on UNIX and NT Network security , New Orleans , Louisiana . Wednesday, October 6th , 1999, Session.

[9] Allesander Bagnato, Barbara Kordy, Per Hakon Meland, Patrick Schweitzer "Attribute decortion of attack defense tree" TXT e-solutions, corporate research division, I-16100 Genoa, Italy. University of Luxembourg, Luxembourg SINTEF ICT, Norway. International Journal of Secure Software Engineering, volume 3(2), pages 1-35. IGI Global, 2012

[10] Shon Harris "CISSP"exam guide " sixth edition [ISBN 978-0-07-178172-2], January 2013 ,published by Tata mc- graw hill.

[11] Gary McGraw and Greg Morrisett2 "Attacking Malicious code : a report to the InfoSec research council " Reliable software technologies.Cornell University. Submitted to IEEE software and presented to IRC, May 1, 2011.

[12] Paul Giura and Wei Wang, "using large scale distributed computing to unveil Advanced persistent threat "in "IEEE ASE international conference of cyber security "Washington DC.[ISBN 978-162561-001-0] Dec-2012 pp. 1-13.

[13] Tarique Mustafa "Malicious data leak prevention and purposeful evasion attacks: An approach to advanced persistent threat (APT) management" founder & chief executive officer, nexTier Networks, Inc, USA in IEEE 2013 [isbn 978-1-4673-6195-8]

[14] Johan sigholm and martin bang "Towards offensive cyber counterintelligence adopting a target-centric view on advanced persistent threats" Department of military studies, Stockholm, Sweden in European Intelligence and security informatics conference 2013 [ISBN 978-0-7695-5062]

[15] Chistian seifret, lan welch, peter kmoisarczuk "identification of malicious web pages with static heuristics" victoria university of Wellington, New Zeland, IEEE 2008 [ISBN 978-1-4244-2603-4/08]