International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Detection and Prevention of Malicious Transfer of Sensitive Information

Marimuthu M
Department of Information Security and Cyber Forensics
SRM University
Chennai, India

Sujatha G
Department of Information Security and Cyber Forensics
SRM University
Chennai, India

***Abstract*— Web-based email services are useful for most of the communication between organizations, conversely they are considered as the common threat by which sensitive information leaves the organization. Businesses have completely utilized all form of information technology and networks in order to completely integrate all the activities. The data flow traversing the whole chain involves abundanttrustworthy and sensitive information; this could cause grave consequences if critical information is leaked.In spite of this hazard, many organizations license the use of web –based services on their systems. Employing a method to sense and thwart data exfiltration through these channels is crucial to defend an organization's sensitive documents.This study delivers a widespreadmethod for thwarting malicious transfer of sensitive information.Using squid proxy server and clam antivirus [1] also introduced a signer tool which helps to insert signatures into documents. These Signatures are used by the proxy to prevent documents from leaving organization.**

Keywords- Squid Proxy Server, Clam Open Source Antivirus, Signer Tool

I. INTRODUCTION

A Malicious insider trying to transfer sensitive information from organizations premises got lot of ways to transfer them.This comprises email services, cloud storage services and FTP servicessuch as Microsoft's SkyDrive or Google Docs that let documents to be uploaded or attached whether encodedor not. These internet services can present lot of challenges to organizations. The main challenge in many of these services is that the communications channel is encrypted; therefore the contents cannot be examined.

There are many reported instances in which online services played a vital role in a malicious insiders attack. From above the mentioned observations and other concernsthat we discuss later in this study, organizations must deploy some effective methods and processes to Prevent any unauthorized use of online services at the same Time the organization must allow the users with genuine needs to use the online services for file transfer.

In this paper, we explored techniques for examining contents of encrypted communications channels and offer methods to prevent sensitive data from being transferred out organizations premises. While this report precisely aims protected webmail services, the same technique are effective for online based mail services, such as Google Docs, Ubuntu one, SkyDrive, that allows users to upload file to whether encrypted or not.

We explore attempts by which transfer of sensitive data can be prevented using Squid proxy Server and Clam Antivirus for scanning the contents [1]; all of these are open source software packages. Also we introduced a Signer tool to assist organizations in signing sensitive documents with key words to prevent transfer of sensitive data.

The solution presented in this paper is not a silver bullet to thwart malicious transfer of sensitive information. This can considered as another layer of security solution that should be added to existing organization policies for risk mitigation

II. MITIGATING INSIDERS THREATS

We define a malicious insider as an employee or officer of an organization, institution, or agency. The term can also apply to an outside person who poses as an employee or officer by obtaining false authorizations. The attacker obtains access to the computer systems or networks of the enterprise, and then conducts actionsprojected to cause damage to the organizations

Malicious insiders are able act inside a group by taking benefit of weaknesses they find in current organizations policy. Security team must be aware of all these weaknesses and how an attacker uses these weaknesses to exploit the systems. This paper largely emphases on theft of information using web-based email services.

The forthcoming sections present the methods and practices an organization could implement to thwart insiders threat.These practices can be deployed in organization of any sizeand all the tools used open-source and public-domain tools since they are available to public free of cost.

III. The Man-in-The-Middle(MiTM) squid Proxy

The solution in this paper uses Squid proxy server to intercept and inspect the content of Encrypted communication networks (a type of MiTM "attack") using an automated mechanism [4]. Although it is technically possible to use this proxy server to examine and record

secure communications, doing so presents many lawful concerns.

The aim is to permit information security authorities to sense and thwart sensitive company information from being transferred outside of organizations premises through both clear text and encrypted means using an automated mechanism [4].

IV. THE INSPECTION PROCESS

In order to examine the web traffic, all the communication networks must be terminated at the squid proxy server, contents are analyzed, and again encrypted and sent to its destination server. Encrypted traffic cannot be examined by any other means

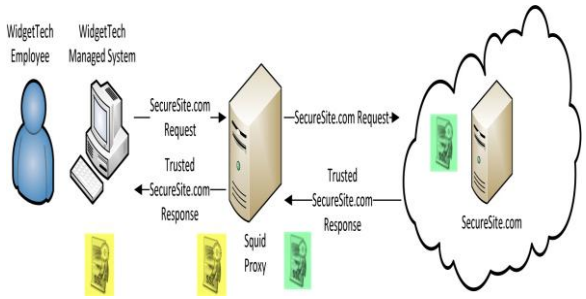

Figure: 1 Encrypted Traffic Inspection

In Figure 1, an employee requests use of organizations monitored system to request a protected website, such as SkyDrive. The monitored systems are designed to send all its website requests to a squid proxy server [2]. The squid proxy intercepts and makes request on behalf of its client. The encrypted web session is established between the proxy and the requested secure website

V. Self-Signed Root Certification Authority(CA)

A self-signed public/private certificate pair is mandatory to sign the dynamically created certificates as illustrated in Figure: 1. these self-signed certificates are usable for a set of period of time. Organization must think through how long the generated certificate is usable as a part of risk assessment and administration process.

If the organization already has policy that defines how long a certificate for sensitive application is to be valid, then this time period should be used while creating certificates

VI. THE CLIENT CERTIFICATE

As stated in the earlier sections, there are numerous concerns to be addressed before creating client certificate. Predominantly the certificates validity must be determined before deploying [3]. The amount of time a certificate is valid directly affects how often the certificate must be renewed and how frequently the client side certificates must be deployed.

In smaller organizations, these concerns may not be serious, however for organizations that have thousands of computers; these concerns rapidly become a configuration management issue [3]. Moreover, every time a new certificate pair is created, the SSL certificate cache on the proxy server must be cleared and reinitialized. Hence, the organization must cautiously select a certificate that balances administrative overhead with risk.

VII. CLAM ANTIVIRUS WITH CUSTOM SIGNATURES

Clam Antivirus is a cross-platform antivirus software tool-kit able to detect many types of viruses [1]. One of its main uses is on mail Servers as server side email virus scanner.

Signatures are used in conjunction with the ClamAV antivirus engine on the proxy server to block selected documents from leaving the organization [1]. The concept behind this is all the sensitive documents signed with given signatures are falsely recognized as viruses and are therefore prevented from leaving organization.

There are several methods available for blocking file attachments. Pattern matching is based on case-sensitive strings. Clam AV scans for hexadecimal pattern in the files [1]. If the pattern is found Clam AV flags the file as virus and proxy server blocks the attachment from leaving. And it triggers an alert which sends email to security team. This pattern matching method will deliberately increases the number of number of strings to be included in Clam AV[1]. If the organization uses a distinguishingpattern for all files that are of sensitive nature, then the sum of signatures desired may be compact. For example, if an organization marks all the sensitive documents in the header and footer area of document using compulsory phrase such as “SENSITIVE DATA” then only one signature may be essential to block all the sensitive data. However, if a malicious insider alters the header of the file, by altering the single character, the signature is rendered useless

Some common file patterns are shown in the Table: 1 with their associated hex value. These hex values can be used for creating Clam AV signatures [1].

TABLE 1:

Plain Text	Hexadecimal Encoding
FOUO	464f554f
SECRET	534543524554
TOP SECRET	544f5020534543524554

VIII. DOCUMENT SIGNER TOOL

Microsoft office files are signed by unzipping the document, inserting two hidden properties into the document's custom.xml file, and zipping the document back up to its original location [7]. OOXML files can be unlocked to view and edit the modules parts that define the documents configuration and content. The custom.xml part of the document is located at docprobs directory of OOXML file, and holds any custom document stuffs added to the document [7].

The Signer tool alters the *custom.xml* file of OOXML files to contain "secret" custom property records that correspond to the tag. These entries are hidden in the sense that they are stored in the document's XML upon load or save but are not presented to the user for viewing or editing in Office (e.g., Word, Excel, and PowerPoint) user interfaces.

The goal of signing Office files is to add records to the *custom.xml* file that persist upon modifying and saving the file but not showed in the file's list of custom properties from within the Office application's Advanced Properties dialogs

IX. CONCLUSIONS

The need for retrieving web-based email services may be vital to business operations and for employee. Though, these facilities permit malicious insiders the capability to handover the sensitive information easily. Hence control is needed to balance organizational or employee requirements with the risk of losing sensitive data.

In this report we presented techniques that organization can employ to thwart access to attachment upload facilities offered by innumerable websites.

Signatures are added to files and these files are identified as sensitive and can be prevented from leaving organization while other information can flow freely.

REFERENCES

1. ClamAV. *About ClamAV.* http://www.clamav.net/lang/en/ (2012).
2. Microsoft. *Manage Trusted Root Certificates.* http://technet.microsoft.com/enus/library/cc754841.aspx (2012).
3. Microsoft. How to Force Proxy Settings via Group Policy.http://social.technet.microsoft.com/wiki/contents/articles/5156. how-to-force-proxy-settings-viagroup-policy.aspx (2012).
4. Squid-Cache.org. Squid: Optimizing Web Delivery. http://www.squid-cache.org/ (2012).
5. White House. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacyand Promoting Innovation in the Global Digital Economy*, February 2012 http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
6. E. Kowalski, et al., "Insider threat study: illicit cyber activity in the government sector", United States Secret Service & the Software Engineering Institute, Carnegie Mellon University, January 2008.
7. Office Open XML I: Exploring the Office Open XML Formats http://office.microsoft.com/en-in/word-help/office-open-xml-i-exploring-the-office-open-xml-formats-RZ010243529.aspx?section=12
8. M. Keeney, et al., "Insider threat study: computer system sabotage in critical infrastructure sectors", United States Secret Service & the Software Engineering Institute, Carnegie Mellon University, May 2005.