Defence in-depth for Cyber Security With Custom Anti-Virus Signature Definition

Markson Aigbodi, Karim Ouazzane, Daniel Mitchell, Vassil Vassilev
School of Computing, London Metropolitan University
maigbodi@yahoo.com, k.ouazzane@londonmet.ac.uk, daniel@lifelineit.net, v.vassilev@londonmet.ac.uk

Jun Li
Department of Oncology, University of Oxford
jun.li@oncology.ox.ac.uk

Abstract. Anti-virus software has been the main defence against malicious application and will remain so in the future. However the strength of an anti-virus product will depend on having an updated virus signature and the heuristic engine to detect future and unknown virus. The time gap between an exploit appearing on the internet and the user receiving an update for their anti-virus signature database on their machine is very crucial. Having a diverse multi-Engine anti-virus scanner in the infrastructure with the capability for custom signature definition as part of a defence in-depth strategy will help to close that gap. This paper presents a technique of deploying more than one anti-virus solution at different layers and using custom anti-virus signature from the ClamAV anti-virus software as part of a defence in-depth strategy.

Keywords: Anti-virus, ClamAV, Malware, defence in-depth, Portable Executable (PE), Cyber security.

1. INTRODUCTION

Malicious applications like virus, worm, Trojan, Spamming and phishing tools can infect and destroy information in a user's computer through means that the user utilizes in communicating on the internet. Email, File attachment, web surfing or file transfer on the internet either with a desktop or a smart phone are just a few of the many ways that potential harmful applications called Malware [1] can be introduced into the network.

It is widely agreed that it is much easier to destroy than to build. This is very true when it comes to building software applications that are useful and secure. Security and usability are at two different end of the spectrum. Most of the time security is sacrificed for usability and at the end of the day security only becomes a retrofit. The desire to meet market's demand has resulted in the development of software products that are full of security vulnerabilities and it takes only a short time before these holes are discovered and exploited [2].

It is true but sad that the information protection industry is always one step behind in the fight to protect the network and the device it supports from malicious application. In most of the cases the black hats community will discover a hole in an application and then look for ways to exploit that opening and before long the exploit are being sold to the highest bidder [3].

Whenever vulnerability is discovered in an application or operating system, attempt will be made by legitimate security engineers and black hats to exploit it and sometimes the exploit may appear on the internet. During the time it takes for the anti-virus companies to provide updates for their anti-virus signatures and software vendors to release patches the enterprise is at the mercy of the malware author. There are cases where vendors deliberately delay in producing a security patch for their products because of the high cost involved in providing an immediate patch.

At this crucial stage in malware history one can no longer rely and wait for software vendors and anti-virus companies to release patches and update their virus signature database. We need to take our destiny into our hand and provide our own custom security solution which may include the use of multi-Engine and custom anti-virus database definition which we can update, with our own malware definition and then layer it in a way to provide end protection at every point in the flow of data and information in the enterprise.

2. DEFENCE IN-DEPTH

Defence in-depth involves the building of different layers or barriers [4] of protection around an asset or group of asset in order to reduce the effect of exploitation. It involves the use of policies, operation, human, legal and technical elements [5] such that if one layer fails, is taken out or proven to be inadequate another layer of defence will prevent a complete breach. Although we always think of protecting information as it flows through the communication path, at may be more practical to deal with data and information security at the three possible stages of data and information, namely at rest, in motion and data at the perimeter[6]

Although the origin of defence in-depth is military with the use of a watchtower, walls, moat, and trenches to create a fortress, its application has found its way into information security whereby we are protecting an information zone which is the boundary or perimeter surrounding the flow of private data and information and the systems that process the information and data. This boundary has become very difficult to define and defend as it is always expanding and contracting.

Years ago the information security boundary could be a small office or group of offices within a geographical confine with properly defined perimeters. Today with the help of advance technology employees can carry out their businesses while telecommuting and their location could be at the airport, hotels, taxies or cafes. Given this expanding perimeter it has become difficult to employ traditional protective method.

Businesses have suffered greatly when mobile device containing sensitive data are lost or stolen. There has been case of theft of confidential information while employees are connected to public wireless access point.

A good real-world example where defence in-depth can be useful but rarely applied is in the protection of data that travel between various servers’ components in the enterprise. Most companies throw up a corporate wide firewall to keep intruders out. Then they will assume that the firewall is good enough and let their application server talk to their database in clear text [7].

Assuming that the data in question are important, what happens if an attacker manages to penetrate the firewall? If the data are also encrypted, then the attacker won't be able to get at them without breaking the encryption, or (more likely) breaking onto one of the servers that stores the data in an unencrypted form. If we throw up another firewall, just around the application this time, then we can protect ourselves from people who can get inside the corporate firewall. Now they'd have to find a flaw in some services that our application's sub-network explicitly exposes something we're in a good position to control. This is the main reason that defence in-depth is more of common sense or a best practice framework than a complete product.

Defence in-depth can be applied in any area where data flows and a perfect example is packets moving through the protocol stack such as the TCP/IP protocol stack. With the packets flowing through the stack different point, different routing decisions are made. Defence in-depth can be applied through a protection against any attempts to fool firewalls, intrusion detection system and other network protection device [8].

As shown in the figure below the software architecture is made up of proposed system which consists of three layers of protection between the public hostile network and the private internal network. The packet filtering component serves two special purposes; provides network address translation between the public and the private network and protects the perimeter between the outside public and the private inside. The filter can make decisions based on the source and destination address and the port.

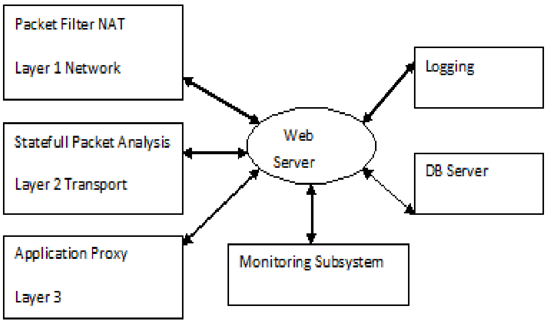

Figure 1 Defence in-depth on Network Packet and Protocol Stack

As shown in the figure below a typical defence in-depth strategy would usually be divided or grouped along the following security domain with six different levels where security can be applied and its effect monitor:

1. Policies and security awareness
2. Perimeter.
3. Internal Network.
4. Host.
5. Application.
6. Data and information.

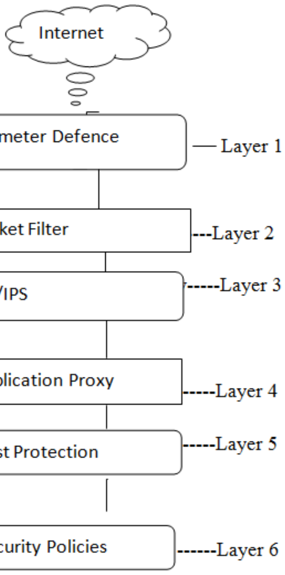

Figure 2 A typical Defence In-depth Structure.

Implementation of defence in-depth can be seen in every area where there are people and information systems with a connection to the public internet. From small and medium scale companies, large corporations and even governments' critical infrastructures and existing SCADA systems are being restructured to fight against the effect of cyber terrorism using defence in-depth strategy. There are also products' vendors that provide security solutions with this holistic view of security protection to the entire enterprise although they may not use the term - 'defence in-depth'.

Cisco has been in the forefront of providing defence in-depth solution to major companies that are required by legislation to provide transparency in business. Cisco provides such businesses with a defence in-depth solution using its commercial product and sometimes that of its partners based on their solution called SAFE - *"Security Blueprint for Enterprise Networks"* [9].

SAFE is not a product but a best guideline from cisco providing best practise information to interested parties in terms of designing and implementing secure networks. It takes a layered approach to security where a failure of one security system is not likely to lead to the compromise of the network resource.

Microsoft Forefront technology is a product that offers a layered solution to the Microsoft network [10]. It is a multi-layered suit of product that which include the following:

1. Forefront for Office Communication Server.
2. Forefront Identity Manager.
3. Forefront Endpoint Protection.
4. Forefront Threat Management Gateway.
5. Forefront Unified Access Gateway.
6. Forefront Online Protection for Exchange Server.
7. Forefront Protection for Exchange Server.
8. Forefront Protection for SharePoint.

With this group of product a defence in-depth solution can be built to provide complete protection for end computers, communication and collaboration servers and enterprise networks.

While the above two examples are commercial products with a heavy high price tag that is way off the league of some companies like those of non-profits, small and medium scale companies, the principle can be applied using open source solutions.

This paper will demonstrate that implementing a complete defence in-depth strategy is still possible with companies that do not have a budget and resources like the giant enterprises. We shall demonstrate that how defence in-depth can be applied in the enterprise in protecting against portable executable files [PE] and how a custom antivirus signature can be placed at different positions in the enterprise to detect malicious executable files whether received as email attachment or delivered as embedded shell code in internet communication.

3. CREATING CUSTOM ANTI-VIRUS SIGNATURE

While most anti-virus software is propriety and closed to modification we do have a few open source anti-virus solutions that can be used for our intended purpose. In this paper we are using the popular cross-platform Clam Antivirus (ClamAV) which is an open source antivirus software from Sourcefire. ClamAV prides itself as having been the first to identify a signature for 2003's MyDoom Virus allowing it to be detected and eradicated earlier than any commercial virus solution.

Aside from possessing the ability to perform functions that can be found in other anti-virus products, it is the ability to create custom virus signature that makes clamAV standout. With ClamAV one can create new signatures and detect new threats to the enterprise. There is the added advantage that ClamAv can be installed to run side by side with other commercial product and if possible convert some signatures to clamAV virus signature format.

ClamAV was designed originally as an email attachment antivirus scanner to detect malicious email but it can also be used as a regular anti-virus. It can decompress archives (e.g., erar, zip, gzip, bzip2, cab) and scan Linux mailboxes (mbox, MailDir, and raw emails), and it supports on-access scanning on Linux and FreeBSD. However it has the ability to be used as a standalone malware scanner that can be deployed in any host whether as server or as a work station application with the ability to be run from the command line interface.

There are third party websites that specialize in providing enhanced ClamAV signatures against email messaging system from phishing, fake lottery, Ecard malware, Fake job, Porn and other general spam. They provide free daily signatures to the web community that are of quality standards which can be used for personal or commercial purposes.

As an anti-virus tool kit it becomes easy to build clamAV on any POSIX-compatible system with a C compiler and meshes perfectly well with any of POP3, Samba and web servers as well as any message transfer agent (MTA). These abilities of ClamAV make it a perfect candidate for a well thought out defence in-depth strategy.

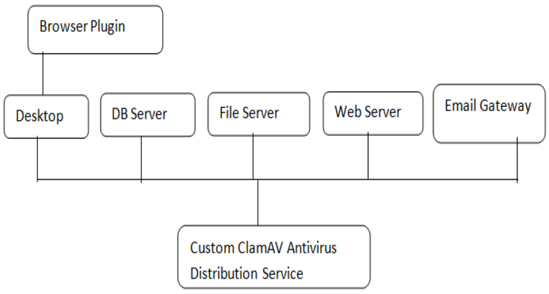

Figure 3 Distributed malware service

The figure above shows the different hosts in the network benefiting from a distribution of anti-virus service based on ClamAV. The service can be specialized based on the nature and type of server application. The case of the desktop computer is different from the others because due to encryption and encoding some malware may be able to invade network detection and its true intent becomes available only at the application endpoint which in most cases is the browser. With a browser plugging that can provide scanning capability when the file is open or decrypted the malware can still be discovered before it exploits the intended vulnerability.

The proliferation of malware has triggered the need for antivirus programs to detect, remove and protect the host computer from future infection. The job of the antivirus software is not made easier by the fact the malware's authors are getting smarter and more sophisticated. Antivirus programs are being attacked by malware, add to the fact that user can be tricked into running malicious programs even when such files are flagged by the antivirus as suspicious; the user ends up damaging the trust relationship between the host operating system and the antivirus software.

File scanning to match against existing virus signature is the main job of the antivirus software but due to its limitation in detecting zero day or future malware with no signature, behavioural analysis are being added to antivirus programs, however this analysis has its own weakness. First, one has to differentiate between normal behaviour and abnormal behaviour. This behavioural approach is difficult because we have both suspicious and malicious behaviour; when a suspicious behaviour is detected there must be further investigation to reduce false positives.

The best method to reduce false positive is to run the suspect file in an emulating or visualized environment to confirm its true nature and the author's intent. However we do not always have this luxury at our disposal hence we have to look for another alternative solution to the problem. The alternative approach used in this paper is to determine the true nature of the executable files by examining anomalies in the lower level attributes of the file [11].

The windows executable file format also known as PE/COFF (Portable Executable /Common Object File Format) files are by far the popular choice used by malware authors to distribute malicious applications to the desired destination. PE/COFF files include but not limited to the popular executable(.exe), dynamic link library(.dll) ActiveX controls(.ocx) amongst others.

When faced with these files it may become difficult to tell suspicious file from malicious files, but by examining the attributes of the file header and other attributes one can reduce the level of false positives.

Popular criteria include but not limited to files with,

1. TLS entries.
2. Resource directories.
3. Suspicious IAT entries.
4. Suspicious entry point sections.
5. Sections with zero-length raw sizes.
6. Sections with extremely low or high entropy.
7. Invalid timestamps.
8. File version information.

Armed with this information a security researcher can begin to collect information for a database of behaviour and heuristic for input into a custom ClamAV signature. The structure of the ClamAV signature format is given below;

SigName:Target:Offset:HexadecimalSignature

SigName is a unique string describing the particular signature, the Target field can range from 0-9 where,

0 = Any file type
1 = windows PE
2 = OLE
3 = Normalized HTML
4 = E-mail file
5 = Image file
6 = ELF
7 = Normalized ASCII
8 = UnUsed
9 = Mach-0 binaries

The Offset value can be anything from a wild card to specific offset in a file. The last part of the signature format is a hexadecimal hash representation of the particular string. ClamAV come with a command line tool called sigtool which can convert a string to hexadecimal representation.

With this signature format and the signature generating tool one can start to build a program that can create custom ClamAV signatures from header attributes that can be saved in a signature database and be distributed from a centralized location.

The figure below shows a custom ClamAV signature generator creating different antivirus' definitions that can be tailored to the needs of the specific host and application.

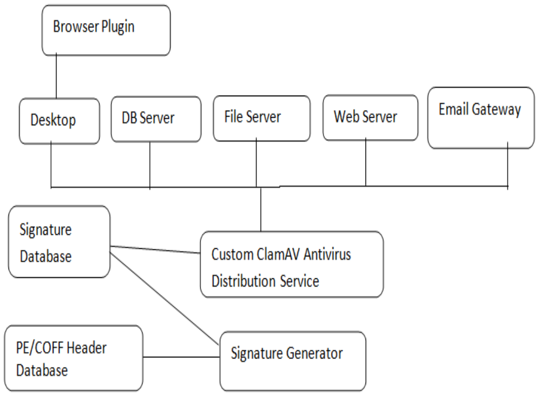

Figure 4 ClamAV Custom Antivirus Architecture

The design of a simple signature generating application is just the beginning to a world of opportunities. With the number of spamming and phishing sites increasing, having a browser plugging that can scan the URL and determine whether the site being visited is malicious, is another layer of protection. Although there are current browsers plugging from most anti-virus vendors, the messages these applications generate are so generic that the user is only warned about the nature of the site but no specific message that would enable the user to make an informed choice. With a custom anti-virus solution, the user can be provided with specialized information that will show the user the consequences of their actions.

The development of a browser anti-virus plugging could begin first by using ClamAV own support for Google Safe Browsing Database [12] which get updated regularly. This database is included with ClamAV and when enabled, it will provide the following added benefits;

1. Warnings that appear before the user clicks if it leads to malware-infected pages.
2. The plugging can have access to Google list of suspected phishing and malicious pages.
3. For companies with public sites it will prevent their sites from being used as a vector to infect visitors.

4. CONCLUSION

In this paper, a strategy to implement defence in-depth with custom anti-virus signature was presented to combat the ever changing landscape of protection from malicious application. The solution is not too difficult or expensive to design and the entire tool used is easily available and the technique has been in existence for some time. With this type of strategy the technique can be expanded to cover not only PE/COFF file but any other files' format or any other heuristic technology that the user may see fit to create a scanning engine.

One of the beauties of this solution is that it can be combined with any other anti-virus' solutions that may exist in the environment. With this technique, the security administrator or researcher can take the protection of the enterprise to the next level.

5. REFERENCES:

1. *Malware* Retrieved 10 December 2012 http://uk.norton.com/security_responce/malware.jsp

2. Patch Management and the Need for Metrics Retrieved 13 December 2012 from http:// buildsecurityin.us cert.gov/bsi/articles/knowledge/principles/347-BSI.html

3. *Hacker Selling Yahoo Exploit for $700* Retrieved 12 December 2012 from http://nakedsecurity.sophos.com/2012/11/26/hacker-selling-yahoo-exploit/

4. Smith C.L, (2003), "*Understanding concepts in the defence in-depth Strategy*", Proceeding on the 37th Annual International Conference on computing and Processing. Pages(s) 8-16.

5. *Defence in Depth A practical strategy for achieving Information Assurance in today's highly networked environments*. Retrieved 15 December 2012 from http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

6. Dauch k, Hovak A, Nestler R, "*Information Assurance Using a Defence In-Depth Strategy* " Proceedings on the CyberSecurity Applications & Technology Conference for Homeland Security, 2009, Page(s) 267-272

7. Sean Barnum, Micheal Gegick *Defence in-Depth* Retrieved 12 December 2012 from https://buildsecurityin.us cert.gov/bsi/articles/knowledge/principles/347-BSI.html

8. *Aigbodi Markson, Applied defence in-depth to intrusion detection prevention and control*. Msc Dissertation London Metropolitan University 10 January 2010.

9. Sean Convery, Bernie Trudel, *Cisco SAFE: A Security Blueprint for Enterprise Networks* Retrieved 16 December 2012 from http://www.cisco.com/en/US/prod/collateral/wireless/wirelssw/ps1953/product_implementation_design_guide09186a00800a3016.pdf

10. William Stanek *Microsoft Forefront: Achieving Defence in Depth with Forefront*

Retrieved 16 December 2012 from http://technet.microsoft.com/en-us/magazine/gg537286.aspx

11. Joel Yonts, *Attributes of Malicious Files*, Retrieved 16 December 2012 from http://www.sans.org/reading_room/whitepapers/malicious/attributes-malicious-files_33979

12. *Safe Browsing API – Google Developers* Retrieved 23 December 2012 from https://developers.google.com/safe-browsing/