An Innovative Custom Cyber Security Solution for Protecting Enterprises and Corporates' Assets

Karim Ouazzane*, Markson Aigbodi, Daniel Mitchell, Vassil Vassilev
School of Computing, London Metropolitan University
E-mail: k.ouazzane@londonmet.ac.uk, markson@lifelineit.net, daniel@lifelineit.net, v.vassilev@londonmet.ac.uk

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

Abstract
Anti-virus software has been the main defense 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 which is deployed in a custom proxy solution as part of a defence in-depth strategy.

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

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 (Norton, 2012) can be introduced into the network.

Security and usability are at two different end of the spectrum. Most of the time security is sacrificed for usability and 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 (BSI, 2012; Kim, 2012; Ryu et al., 2009; CRCR, 2008; TIB, 2004).

It is true but unfortunate 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 (Sophos, 2012).

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.

The era of big data is here and companies, even from small to medium scale companies are now dealing with data in the size of terabytes. Managing this Hugh amount of data in the face of new regulations and the financial implication of data loss has moved the emphasis from data accumulation to protecting these sometimes mission critical data. Backup and restore is the cornerstone of data protection and the first line of defense (Tom Petrocelli, 2005).

The main concern today is centred in the protection of data from eternal threats, but a large percentage of threats often come from people who are the actual custodian of data (CERT, 2012). This threat from the malicious insider within the organization tasked with managing computers and data repositories is often a difficult problem to address (Elisa Bertino, 2012). We cannot solve this problem with the same techniques used for external threats.

Insider threats are from people who are trusted by the organization, they possess the necessary authorization and often with elevated user rights. Due to the complex nature of the problem insider threats can be divided into three categories:

1. IT Sabotage which involves the use of information technologies to harm the organization.
2. Theft of IP which is the stealing of intellectual property from the organization and these include propriety software, strategies plan and customer information.
3. Fraud - the use of IT for the unauthorized modification addition or deletion of an organization data for personal gain (D. Cappelli, A. Moore and R. Trzeciak, 2012).

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.

The facade of enterprise security

It is easy to define a security approach that we think will provide adequate security. These solutions look perfect on the ground - employee security training, developing secure processes and implementing security technologies. These noble solutions have all met with failure as we still see them crumbling with the onslaught of cyber-attacks.

These facades of enterprise security result when a security solution does not fit into the defined security architecture. The security architecture is for enterprise security what a blueprints is for a properly constructed house. In other to have consistent security, security architecture must be properly defined. The current approach to security architecture is very generic, concentrating

primarily on what protocols can be used at a specific tier of the network without attention to identity of the user, application, type of data and data interaction.

Therefore to move from this ineffective risk mitigation driven solution, a security architecture will take into consideration the organizations network infrastructure, system architecture, applications, and data that needs to be designed, implemented and secured, processes, applications, user roles and users. (Aaron Woody, 2013)

The correct security architecture will result in an enterprise security solution that can be compared to a house that blends well with the external neighbourhood but provide a unique interior.

There are numerous vendors out there with hardware and software solutions that claim to provide complete security but fail when the threat is from inside. A custom enterprise security architecture that would be effective in combatting the malicious outside and insider threats would include the following attributes when implementing such a program (George j. Silowash, 2013).

1. Monitor Phone Activity Logs to Detect Suspicious Behaviors.
2. Monitor and Control Privileged Accounts.
3. Monitor and Control External Access and Data Downloads.
4. Protect Critical Files from Modification, Deletion, and Unauthorized Disclosure.
5. Disable Accounts or Connections upon Employee Termination.
6. Prevent Unauthorized Removable Storage Mediums.
7. Understand All Access Paths into Organizational.

Defense in-depth

Defence in-depth involves the building of different layers or barriers (Ahmad et al, 2012; Smith, 2003) of protection around an asset or group of assets in order to reduce the effect of unlawful exploitation. It involves the use of policies, operation, human, legal and technical elements (NSA, 2012) 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, it 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 (Dauch et al., 2009).

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 (Barnum & Gegick, 2012).

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. As the attacker is moving through the host and network looking for holes to exploit there will surely be artefacts left behind no matter how meticulous the attacker may be. With a proper audit system in place the keen system administrator can be notified in realtime whenever suspicious activities are registered. When Microsoft spent time in implementing first class auditing in it core operating system it was thinking of auditing as part of a defense in-depth strategy (Shimonski, 2012).

Defence in-depth can be applied in any area where there are data flows and a perfect example is packets moving through the network. With the packets flowing between different points, 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 (Aigbodi, 2010).

As shown in the figure below the software architecture is made up of components which cover 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.

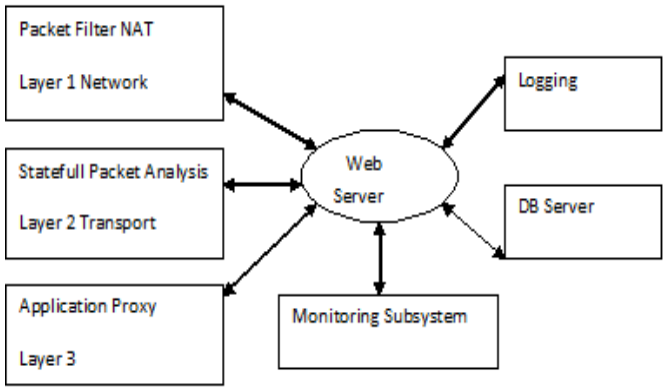

Figure 1. Defence in-depth on Network Packet and Protocol Stack.

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:

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

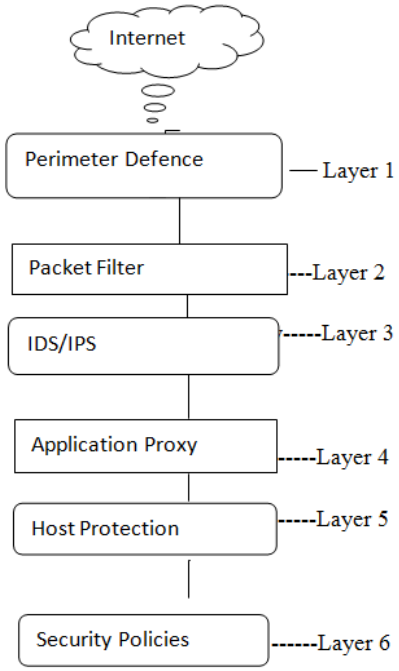

Figure 2. A typical Defence In-depth Structure.

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*" (Convery & Trudel, 2012).

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 is a technology that offers a layered solution to the Microsoft network (Stanek, 2012). It is a multi-layered suit of products 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 products 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 how defence in-depth can be applied in the enterprise to protect against portable executable files (PE) and how a custom antivirus signature can be placed in different parts of the enterprise software to detect malicious executable files - whether received as email attachment or delivered as embedded shell code in internet communication. Also, it is worth mentioning that there are different approaches for implementing a custom malware signature generating system; the approach is mostly dependent on the targeted layer of the application

protocol. For example (Perdiscia et al., 2013) uses network-level behavioural malware clustering to generate malware signatures.

Creating custom anti-virus signature

While most anti-virus software is proprietary 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., rar, zip, gzip, bzip2 and 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. It 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.

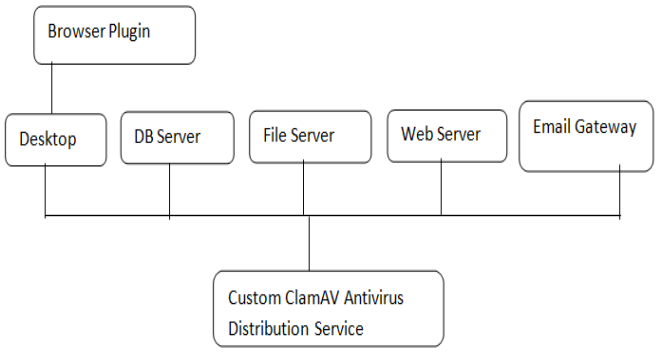

Figure 3. Distributed malware service.

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.

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 alarms.

The best method to reduce false alarms 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 (Yonts, 2012).

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 are 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 alarms.

Popular criteria include but are 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 comes 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 signatures that can be tailored to the needs of the specific host and application.

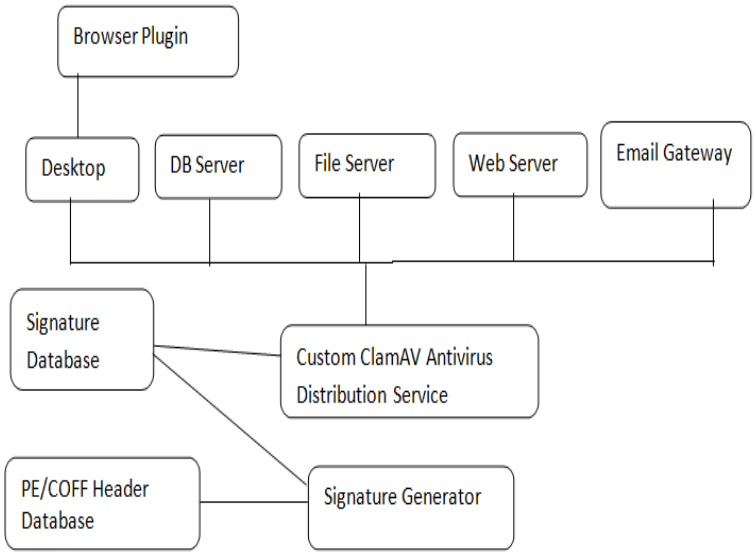

Figure 4. ClamAV Custom Antivirus Architecture.

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

plugin that can scan the URL and determine whether the site being visited is malicious, is another layer of protection. Although there are current browsers plugin 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 plugin could begin first by using ClamAV own support for Google Safe Browsing Database (Google, 2012) 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 plugin 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.

Custom proxy solution

All of the above services are good enough for the general public but when it comes to the more targeted attacks more is needed (Owasp, 2013; Bao & Cao, 2013). On a daily bases as more and more malicious applications and urls are detected, malware authors are coming up with new ways to exploit the software vulnerabilities. To cope with this ongoing onslaught it is ultimate requirements to install a security proxy solution that can ensure that exploit that goes unnoticed by protection mechanism like the safe browsing API can be detected before it exploits the web client browser. This is especially true of Advance Persistent threat (ADT) which is the latest and the most advanced form of attack and are proving very difficult to defend against. Protecting against these forms of attack may result in a complicated defence solution (Damballa, 2013). The problem with ADT is that they sometimes target the trust relationship that exist within the environment and are stealthier and more sophisticated using insidious social engineering techniques to quietly penetrate your organization forcing it to deploy customized malware that can live undetected for months (TrendMicro, 2013). The custom proxy solution could intercept both the request and the response between any internet applications. Any raw responses that may contain malicious content design to exploit vulnerabilities on the client browser are either removed or modified thus reducing their impact. The proxy solution could call any other security module to provided support and from time to time more modules could be added to deal with circumstances that affect the business. The authors have implemented a browser plugin in Firefox that adds a context menu to all URLs on the Firefox browser, enabling the user to personally send and receive information about any content which requires link enabling.

Conclusion

In this paper, a strategy to implement defence in-depth with custom anti-virus signature that can be deployed in a custom proxy solution 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. Future development could include design of special proxies not only for the Http protocol but for others that can be easily exploited.

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.

The problem dealing with the more recent advanced persistent threats and the complex nature of client side application would never go away. The design of custom application proxies that can be dynamically updated to provide client side protection to augment already existing security solution becomes a must. Implementing a sandbox environment for network aware applications to curtail the impact of any exploit is the holy grail of information security.

Acknowledgement

The authors are grateful to LifelineIT (LifelineIT, 2012) and Technology Strategy Board (KTP, 2012) for the generous funding support.

References

Aaron Woody (2013) Enterprise Security: A Data-Centric Approach to Securing the Enterprise Packt Publishing February 22, 2013

Ahmad A., Maynard S. B. and Park S. (2012), *"information security strategies: towards an organizational multi-strategy perspective".* Journal of intelligent manufacturing; DOI: 10.1007/s10845-012-0683-0

Aigbodi M. (2012). *Applied defence in-depth to intrusion detection prevention and control*. Msc Dissertation London Metropolitan University 10 January 2010.

Bao H. and Cao Z (2013). *"Group–Proxy Signature Scheme: A Novel Solution to Electronic Cash"* Journal of Intelligent Systems. Volume 22, Issue 2, Pages 95–110, ISSN (Online) 2191-026X, ISSN (Print) 0334-1860, DOI: 10.1515/jisys-2012-0024, April 2013

Barnum S. and Gegick M (2012). *Defence in-Depth* Retrieved 12 December 2012 from https://buildsecurityin.uscert.gov/bsi/articles/knowledge/principles/347-BSI.html

Cappelli D., Moore A. and Trzeciak R. (2012) *The CERT Guide to InsiderThreats*. Addison Wesley. 2012

Convery S. and Trudel B. (2012). *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

CRC Report - "Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress," CRC Report RL32114, 2008.

Damballa "Advanced Persistent Threat" Retrieved 23 May 2013 from https://www.damballa.com/downloads/r_pubs/advanced-persistent-threat.pdf

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

Elisa Bertino (2012) *Data Protection from Insider Threats* Morgan & Claypool Publishers June 1, 2012

George j. Silowash (2013) *Insider threat attributes and Mitigation Strategies* http://www.sei.cmu.edu/reports/13tn018.pdf July 2013

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

Kim H. J. (2012). *"Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks,''* International Journal of Distributed Sensor Networks Volume 2012, Article ID 268478, 10 pages doi:10.1155/2012/268478

Knowledge Transfer Partnership (KTP) [online], available: http://www.ktponline.org.uk/ [accessed 18 January 2012]

LifelineIT [online], available: http://www.lifelineit.net/ [accesses 12 January 2012]
Malware Retrieved 10 December 2012 from Norton at http://uk.norton.com/security_responce/malware.jsp

National Communications System, "Supervisory control and data acquisition (SCADA) systems," Technical Information Bulletin (TIB) 04-1, 2004.

NSA - 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

Owasp "Defense in depth" Retrieved 7th April 2013 from https://www.owasp.org/index.php/Defense_in_depth

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

Perdiscia,B. R., Leea W., and Feamstera N. (2013). *"Behavioral Clustering of HTTP-Based Malware and Signature Generation Using Malicious Network Traces"* Retrieved 22 July 2013 from https://www.damballa.com/downloads/a_pubs/Usenix10.pdf

Ryu D. H., Kim H., and Um K. (2009). *"Reducing security vulnerabilities for critical infrastructure,"* Journal of Loss Prevention in the Process Industries, vol. 22, no. 6, pp. 1020–1024, 2009

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

Shimonski R. J. (2012). *"Auditing for Increased Security"* Retrieved 5th November 2012 from http://www.windowsecurity.com/articles-tutorials/windows_os_security/Auditing_Increased_Security_Part1.html

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.

Software Engineering Institute Carnegie Mellon University *CERT 2012 CyberSecurity Watch Survey How Bad is the Insider Threat?*

Stanek M. (2012). *Microsoft Forefront: Achieving Defence in Depth with Forefront* Retrieved 16 December 2012 from http://technet.microsoft.com/en-us/magazine/gg537286.aspx

Tom Petrocelli (2005) *Data Protection and Information Lifecycle Management* Prentice Hall September 23, 2005

Trend Micro "Only a Custom Defense Effectively Combats Advanced Persistent Threats", Retrieved 23 May 2013 from http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/index.html#understand-an-attack

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