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 defense 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 defense in-depth strategy.

Keywords: Anti-Virus, Clam Antivirus (ClamAV), Cyber security, Defence In-Depth, Malware, Portable Executable (PE)

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.

DOI: 10.4018/ijeei.2013070104
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 (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 (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 (Cappelli, Moore & 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.
Related Content

Legal Empowerment as Social Entrepreneurship: The KwaZulu-Natal Cases of Bulwer and New Hanover
[www.igi-global.com/chapter/legal-empowerment-as-social-entrepreneurship/135347?camid=4v1a](www.igi-global.com/chapter/legal-empowerment-as-social-entrepreneurship/135347?camid=4v1a)

An Integrated Business Model Innovation Approach: It is Not All about Product and Process Innovation
[www.igi-global.com/article/integrated-business-model-innovation-approach/51591?camid=4v1a](www.igi-global.com/article/integrated-business-model-innovation-approach/51591?camid=4v1a)

Women Entrepreneurship across Nations: Opportunities and Challenges
[www.igi-global.com/chapter/women-entrepreneurship-across-nations/139879?camid=4v1a](www.igi-global.com/chapter/women-entrepreneurship-across-nations/139879?camid=4v1a)
Pushing the Right Buttons?: A Critical Exploration into the Effects of Social Media as an Innovative E-Entrepreneurship Method of Recruitment for Enterprises
Anthony Lewis, Brychan Thomas and Gwenllian Marged Sanders (2013).
International Journal of E-Entrepreneurship and Innovation (pp. 16-37).
www.igi-global.com/article/pushing-the-right-buttons/100359?camid=4v1a