

## Trends of Spyware, Viruses and Exploits

This paper surveys spyware, viruses and exploits, collectively called malware. The first section discusses the objectives of malware. The second section addresses its anatomy and distribution mechanisms. Mitigation is addressed in the third section, and fourth section addresses the relationship between usability and risk mitigation.

### 1.0 Objectives of Malware

This portion of the research addresses the objectives of spyware, viruses and exploits. This portion takes the approach of first enumerating the objectives, with some historical context, and illustrates a taxonomy as put forth by a leading AV publisher.

We try to put the most innovative objectives first, and the more pedestrian last. We also show that the objectives are often combined.

### 1.1 Highly-specific targeted attacks (cyberwar, espionage)

In a talk this author attended, Hal McConnell - Retired NSA, and National Cryptologic Museum Docent, spoke to the Blackhat 2000 audience on "Threats from Organized Crime and Terrorists" in which he described both a cyber-surveillance project conducted by the National Security Agency, and a counter-attack against the NSA computers performed by their surveillance target. The counter-attack took NSA systems offline for three days, according to Mr. McConnell.<sup>1</sup>

Interestingly, major media had previously reported on the then-mysterious three-day outage of the NSA systems, and one online journal reported the following disinformation:

"WASHINGTON (CNN) -- U.S. government sources say there is no indication that the crash of an important spy computer operated by the super secret National Security Agency was caused by sabotage or the Y2K glitch."<sup>2</sup>

Though first disclosed to be used in 2000, the threat posed by targeted virus attacks has recently re-surfaced as described by in the context of industrial espionage. In July of 2005, Israeli police working in conjunction with British authorities arrested 18 people in connection with a custom-written virus used for industrial espionage.<sup>3</sup>

Antivirus publishers rely on both networks of honeypots, and statistics derived from their antivirus software, to identify new forms of malware.

This reliance created the vulnerability wherein low-volume, targeted viruses could safely be addressed to targeted entities; the honeypots would not detect these because they are not widespread, thus would not generate entries in the publishers' databases.

The ramification of this type of attack is that mitigation measures, mentioned in this paper, would not suffice in mitigation. In the absence of wide distribution of the code, antivirus firms do not have the ability to generate signature files for the targeted viruses. Corporations, relying on AV software and other generally-available countermeasures, do not have the capability to defend against these targeted viruses.

## 1.2 Digital Rights Management

One of the first viruses ever reported was the Brain virus of 1986 which originated in Pakistan. Reports of its purpose differ among journals; however the BBC reported that its purpose may likely have been an anti-piracy measure on the part of its authors.<sup>4</sup>

DRM measures today still often employ malware variants. For example, Sony has recently come under scrutiny for utilizing rootkit technology in its attempts at DRM. Their work is a watershed in the area of spyware, and has garnered the attention of the Department of Homeland Security w/r/t its ramifications. Comments from DHS Assistant Secretary of Policy warned industry leaders against utilizing DRM-objective spyware in any way which undercuts the security of the US Critical Infrastructure.<sup>5</sup>

Similar to the targeted objectives of the NSA virus, the Sony DRM eluded the signature databases of AV vendors until it was brought into the attention of mainstream media by [www.sysinternals.com](http://www.sysinternals.com)

## 1.3 Malware for profit

### ▪ Denial of Service attacks

Stacheldraht, as analyzed by Dave Dittrich, showed that one of the late-1990's objectives of malware was denial of service attacks.<sup>6</sup> The program Stacheldraht was later incorporated into many rootkits.

Remote control was incorporated into stacheldraht. The programming practice of incorporating remote control with denial of service capability was also demonstrated by the Windows-based Sub-7 Trojan.

The practice of incorporating remote control into trojans provides a way of monetizing the virus-infected systems. Bot-farms are sold and leased for mass emailings and for DDoS applications. Farms of several thousand remotely controllable systems can be bought for a few hundred dollars. In November of 2005, the FBI / DOJ released information on the arrest and indictment of James Ancheta, whom the press release referred to as a "computer virus broker", and enumerated some of his specific profits from the monetization of malware.<sup>7</sup>

### ▪ SPAM

Though relaying email may sound to be an innocuous objective of malware, it is actually a multimillion dollar business. And here we look to Symantec's taxonomy of viruses:

Symantec ([www.symantec.com](http://www.symantec.com)) describes a "Damage" category in which they enumerate the capabilities of a virus's payload. As an example Symantec<sup>8</sup> describes the capabilities of W32.Nimda.E@mm as:

Payload:

- Large scale e-mailing: Emails itself out as Sample.exe
- Degrades performance: May cause system slowdown

- Compromises security settings: Creates open network shares

- **Keylogging/PII**

The acquisition of personally Identifiable Information, such as SSN's, Financial account information et al. are frequently the objectives of hostile code. Keylogger.Stawin is an example of one such virus. Other viruses in the multifunction category frequently include keylogging.

- **Product tracking**

As an example in the "product tracking" category of spyware, Compaq systems install an application called 'backweb' on the systems sold to consumers. Backweb is a lightweight web server. It uploads system data to Compaq's databases, and downloads messages and software from Compaq. It may be considered to be in a gray area of spyware, inasmuch as although Compaq does little to notify and end-user of its existence, Compaq does present data about it on its website. [http://www.hp.com/united-states/cpc/presario/connections\\_faq.html](http://www.hp.com/united-states/cpc/presario/connections_faq.html).

- **Surfing/Marketing data**

"Legitimate" firms such as Webtrends provide software which embeds web-bugs into pages created with their software. Wired with such bugs, the pages then provide updates to the Webtrends site, which feeds back aggregated information to the Webtrends subscriber.

- **Click fraud**

As new revenue models are created for internet usage, viruses are coded to exploit those revenue models. One Revenue model is pay-per-click, wherein clicks on ads return money to the web site which hosts the ads. Viruses are used to automate the hits, and compromised systems return hits for the users of the hostile code.

- **Pharming**

Pharming is a practice wherein unsuspecting users are directed to hostile sites which imitate a legitimate site in order to collect personally identifiable information such as financial resources. A method of pharming involves substituting host files on the target systems, such that DNS resolution of a legitimate site then points to a hostile site.

- **P2P functionality**

Virus code, like any code, is re-used while additional functionality is added to core functionality. P2P capability has been added to a number of viruses. The capability can be used for distributing hostile code, or even just for filesharing of any general type.

- **Multifunction objectives**

Novarg as an example of a multifunction virus enables mass e-mail (SPAM), plus DDoS capabilities, plus remote control.

In Symantec's taxonomy, it is shown as:

Payload: n/a

- Large scale e-mailing: Sends to email addresses found in a specified set of files.
- Deletes files: n/a
- Modifies files: n/a
- Degrades performance: Performs DoS against www.sco.com.
- Causes system instability: n/a
- Releases confidential info: n/a
- Compromises security settings: Allows unauthorized remote access.

#### 1.4 Malware for malice and publicity

- **File deletion**

File deletion is a capability used by many viruses, but often not a main objective. For example, in the Melissa series of viruses, only at version F was file deletion introduced. The “I love you” virus, on the other hand, used file deletion as its main objective.

- **Publicity/Props**

The motivation of virus authors trying to make themselves known is still prevalent today. MSNBC reported on a war of words which was coded into Netsky and Bagle. The Netsky code read: “Bagle – you are a loser!!!” and the Bagle virus code held the text: "Hey, NetSky ... don't ruine {sic} our bussiness, wanna start a war ?" <http://www.msnbc.msn.com/id/4422372/>

#### 2.0 Malware Mechanisms

This week marks the 20th birthday of the first virus that was introduced by Fred Cohan at the University of Southern California.<sup>9</sup> They were experimental and mainly for entertainment purposes. Since then, viruses have been evolving and becoming more sophisticated as well as malicious; they delete files, exploit operating systems’ and applications’ vulnerabilities. They can open doors for hackers to gain access to a computer or even a network.

According to Trend Micro’s Real-time Virus map which collects data from its free, online scanner for PCs, more than 15,000 PCs are infected with different types of viruses daily but this number is just a fraction from the real number of infected clients out there.<sup>10</sup>

#### 2.1 What is Malware?

Malware is a general term that usually refers to spyware, viruses, and exploits such as worms and Trojans. It is a program that performs malicious, unauthorized and unexpected actions. Below are some examples of the Malware we will be discussing.

##### **Virus**

A computer virus is typically a small executable code that can replicate itself. It can attach itself to other executable programs and can spread as files that are copied and sent out to different clients. The virus can do many things from displaying messages, images, consuming memory, and CPU processing power to destroying files, reformatting the hard drive or causing other damages.

**Trojan horse**

Trojans are programs that look harmless or desirable but it contain the malicious code that does damage to the system. Trojans frequently replicate themselves. Examples of this type of malware are:

- Remote Access Trojans which open backdoors for hackers to examine the local system
- Rootkits which also open backdoors and allow hackers to perform more activities.

**Worm**

Using security holes, a computer worm is software that replicates itself to other computer system via email attachments and network connections such as instant messaging software and peer-to-peer networks

**2.2 Anatomy of Malware**

We will discuss the anatomy of malware by breaking it down into three different areas. These areas are the creation stage, distribution methods and finally the malware payloads and triggers

**Creation stage**

With the availability of tools, technology and help out there, it is no longer difficult to write and distribute a malware to the public. Anyone with a computer, Internet access and some basic programming skill can create a malware.

In order to plan a successful attack, malware creator decides what target environment is and write specific code for that. Here are some typical examples:

Applications environment: Using other installed application to execute the malware.

Operating systems environment: malware takes advantage of un-patched systems using a known vulnerability or security holes to attack the system.

In addition to the target environment, malware creator also considers the object that it infects. Examples are:

Boot Sector: This refers to the MBR (master boot record). The malware will execute when an x86-based computer starts up, before the operating system is loaded.

Macros: This refers to applications that support macro scripting such as spreadsheet, word processor application. Execution of the macro script will activate the malware.

Scripts: This refers to scripting language files such as Java script, Visual Basic script.

Executable: This refers to typical executable files such as the ones with extensions such as .exe, .com, .dll, .sys, .ocx.

**Distribution Methods:**

There are different methods that malware uses to propagate and replicate to different computer system. The common methods are:<sup>11</sup>

*Via Email messages*

A popular mailing list can contain over 100,000 subscribers. Malware creator can create the malware, carefully plant it in the email with an attractive subject and send it out using one of many mass e-mailer programs that are widely available for a small cost or for free. Malware creator can use one of many free email accounts that is hard to trace back. In no time, the email that contains this malware arrives in thousands of mailboxes.

The human factor is usually the easiest target. Malware creators know this and usually take it into consideration and change the name of the executable files to include multiple extensions because most people know not to run EXE extension. Some examples are:

- Adding a non executable extension to executable file: myPic.exe changes myPic.jpg.exe or myPic.gif.exe
- Making the malware to screen saver format: screen\_saver.scr
- Embedding the malware to wma files.

Once it is executed, the malware may behave as expected by displaying text or images and in the same time spreading and infecting other files and computer.

Depends on the type of email clients and its vulnerabilities, some email clients can set off the executable when user opens the email / auto-execute. If it is a link, the file can be downloaded from a web server.

#### *Via Instant messenger*

Instant messaging is relatively new yet can be the next new breeding grounds for malware. According to computer researchers, because of its "scale-free" networks structure, it is highly susceptible to virus infections.

IM malware spreads itself, by using popular instant messaging service such as MSN, Yahoo, and AIM, to other instant clients using the file transfer feature of the program. User when click on the link that may contain the link that points to a different malware can be downloaded and executed on the local system.

#### *Via Network shares*

The most common spreading and propagation method that is used by malware today is via network shares.

Peer-to-peer: In P2P networks, users install a client program to transfer files privately. These channels are created using common port such as 80 thus bypassing firewall. Malware creator uses this transport mechanism to spread and infect computers.

Exploits: By using vulnerabilities and security holes, malware takes advantage of un-patched systems to take over a system. Malware then will replicate and spread to other computer systems.

#### *Via Network scanning*

This method is quite popular. It is said that when an un-patched computer connects to the Internet, it will likely be compromised in a very short time. Malware creator scans the open ports of a range of IP address and look for vulnerable computer to attack.

### Payloads and Trigger Stage

After a successful deployment malware can do any of the following, depending the on programmed trigger mechanism:<sup>12</sup>

Self execution: malware executes its attack by itself.

User dependent: user runs the program that will execute the malware.

Logic bomb: an action from user can trigger the malware.

Time bomb: malware can execute or stop on or after a certain date and time.

Upon execution, malware can do any of the common activities:

Install as Service: In the local system, the malware installs itself as a service. Because services are run before and after the user logs in or out, it can continue its own thing and also has better chance not getting detected by malware utilities program.

Register in startup key: In the local system, the malware places itself in one of the startup keys such as HKEY\_Local\_Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. This enables the execution of the malware every time user logs in.<sup>13</sup>

Data deletion / theft / corruption: malware quickly delete data on local hard drive or shared drives using the permission from the current user

System failure: malware attacks the application or operating system by finding their weakness and cause the system to shut down or malfunction.

Network bandwidth flooding: malware can send packets to multiple random or pre-programmed ranges of IP addresses using a pre-selected port. Other infected computer systems, in turn, will do the same thing. In no time, all traffic will be halted.

Backdoor opening: malware install backdoors for remote access such as setting up FTP. Malware creator then gains access to the system.

## 3.0 Mitigation

Thoughtful users have a myriad of options available in mitigating the effects of malware. These defenses are essentially divided into three areas; deterrence, prevention, or detection and response. They attempt to solve the problem by either good design or feedback; open-loop or closed-loop. Each of these areas, while providing unique resistance capabilities, is not without weakness. The shortcomings are inherent to their strengths.

Deterrence, for example, is primarily based on and limited by legal actions. Prevention strategies require a hardening of systems, potentially self-defeating as usability is diminished. Detection and response is predominately the arena of scanning products, an open-loop approach to an adaptive problem.

### 3.1 Deterrence

The ever increasing onslaughts are prompting enterprises to pursue legal actions as a form of deterrence. While this trend should reduce the motivation of attackers, in practice it is problematic. The interpretations of jurisdictional and legal issues show few signs of reaching sustainable clarity.

Recent legislation is the *Securely Protect Yourself Against Cyber Trespass Act*, also known as the SPY Act, the *Internet Spyware (I-SPY) Prevention Act* and the *Software Principles Yielding Better Levels of Consumer Knowledge Act*, unsurprisingly known as the SPYBLOCK Act.<sup>14</sup>

The U.S. House of Representatives has passed both the SPY Act and the I-SPY Act. While their long-term effectiveness remains in doubt, they do appear to be having the desired effect. Enterprises now have the option of taking legal action against entities for the damages resulting from non-secure products, particularly if the vulnerabilities are well known and continue to be neglected.

There remain areas of broad interpretation. While prohibiting the unauthorized installation of software may seem simple enough, what constitutes authorization? Court rulings such as *DeJohn v. The .TV Corporation International* and *Bruce G. Forrest v. Verizon Communications Inc. and Verizon Internet Services* have upheld the concept of click-wrap agreements - essentially allowing contracts to be consummated on a mouse-click.<sup>15</sup> Similarly, while prohibiting exploits may seem sensible, what defines exploits? One man's spyware may be another's legitimate product. These areas show no sign of being resolved in the near-term.

Even the idea of classifying legitimate vendors by an opt-in versus opt-out scheme suffers from shortcomings. Opt-out effectively implies that the burden is an individual to alert a potential sender that they do not want anything sent in the first place. But unlike telemarketers, there are an unlimited amount of Internet senders, rendering this scheme impractical.

A more effective opt-in scheme would be one where it is illegal to solicit recipients who have not explicitly requested an opt-in. Obviously this would have no effect on illegitimate senders.

### **3.2 Prevention**

Exploits can be limited through the use of network separation, the use of surety systems, change management, and a variety of other protective mechanisms.

Enterprises can employ risk-avoidance strategies. They can refuse to run products that are known to be susceptible to exploits. They can, for example, choose to employ hardened systems in lieu of the Microsoft platforms. Paradoxically, enterprises are trending towards the increased, not decreased, use of Microsoft systems. Some organizations, for example, have created vulnerable environments by replacing closed systems such as hospital equipment and Teller machines (ATM) with networked Windows systems.

Of course, risks would be minimized with preventative thinking. The infection by an Internet virus implies that the system was accessible from the Internet to begin with. Network zoning and separation are reasonable mitigation approaches.

Another mitigation approach is establishing a separation of user data from externally facing applications. Once periodic checkpoints of the data are established, it becomes trivial to rollback to a known uncompromised checkpoint.

Another recent trend is the use of augmented authentication mechanisms. These systems limit the extent to which unauthorized software can access unrelated information. The keyring system combined with access control lists (ACLs) used by OS X is such a system. If application A is compromised, only information available to application A is compromised. Windows XP has a somewhat analogous mechanism called CredUI that allows for the secure storage of passwords.

Recommended Windows based spyware defense strategies<sup>16</sup>:

Preventative Strategy	Strengths	Weaknesses	Relative Cost
Gateway Protection	Centrally controlled	Does not address mobile devices	Low
Workstation Protection	Protection includes mobile devices	Significant overhead to maintain	Medium
Combined	Centrally controlled and addresses mobile devices	Overkill for some environments	High

Disabling ActiveX or replacing Internet Explorer with a less vulnerable browser is another strategy to consider. This alternative is also a less than perfect approach. ActiveX is sometimes required by websites and IE may even be embedded in the operating system. Again, the balance between usability and security must be weighed.<sup>17</sup>

### 3.3 Detection and Response

The security industry has been slow to address the spyware problem. Nor does there appear to be spyware products designed for large organizations. At this time, the process of removing spyware requires multiple approaches and can be more of an art than science. Spyware has shown itself to be remarkably resistant to complete removal.<sup>18</sup> There do remain, however, actions that can be taken.<sup>19</sup> They are imprecise and require changes in organizational cooperation and behavioral buy-in.

The following table represents available options.

Tool Options	Policy Options
Antivirus Desktop Firewall Anti-Spyware tools	Configuration management tools (CMDB, archived redo-logs) Firewall and gateway filter policies Registry and browser policy restrictions Thin-client with disposable browser sessions Port blocking Specialized user training

All the security in the world cannot always and completely protect an organization. Signature based virus detection, for example, is becoming increasingly obsolete.<sup>20</sup> The introduction of Instant Messaging and its own set of problems are trending negatively. The proliferation of wireless brings its own dimension to these challenges.

It is clear the most important long-term initiatives for an enterprise to adopt are:

- **Forewarned is forearmed.** The amount of threat and vulnerability information can be overwhelming to the point it is ignored. Enlisting a third-party security intelligence firm can improve the signal-to-noise ratio while providing customized advice on specific threats.
- **Improvise, Adapt and Overcome.** Good design is not enough. Looking for a static set of predefined conditions like signature matching or comparing for known vulnerabilities is insufficient. Feedback mechanisms are necessary. For example, detecting zero-day problems require a profile of normal activity, and then responding when that activity strays outside of normal baselines.
- **Strengthen the weakest link.** The weakest element of any security initiative is the human element. While acceptable use policies (AUPs) are a good start, it is not enough. Cultural change, in the form of experiential learning, accountability and disciplinary action, should be included in any security program.<sup>21</sup>
- **Share the Burden.** Even if a business process is outsourced, the liability and publicity resulting from a breach will fall squarely on the owner’s shoulders. Ensure partners are subject to stringent contractual security requirements.

For the private user, the following long-term activities would apply:

- **A little education goes a long way.** Ignoring the problem has not worked. By accepting the burden of understanding the problem, users can avoid the most common mistakes.
- **You are likely already infected.**<sup>22</sup> Install quality malware scanning software. Note that no single program does it all.
- **Avoid re-infections.** Install quality anti-spyware and virus protection software.
- **Be proactive.** Lock down Internet Explorer. Place bad sites on a restricted zone. Consider an alternative browser such as Opera or Firefox. Consider outbound filtering and blocking.

#### 4.0 Risk Mitigation and its Effect on Usability

Organizations and home users want to protect their information. This information can be in the form of financial data, trade secrets, and customer data. This data more than likely is stored on a computer or server. Chances are that the computer or server are connected to a network that is directly connected to the Internet. The Internet is available to anyone with access. The challenge that organizations and home users face is determining how to protect this electronic information from the risks outlined in the first two sections of this paper. The preceding section outlined some methods available to mitigate the risks posed to organizations and home users. These methods however impose controls and parameters on the user which affect usability. This section will discuss the effects of information security risk mitigation measures on usability. We will review these effects within the contexts of internal security and perimeter security as well as in regards to organizations and home users.

#### 4.1 Internal Security

Gartner Research<sup>23</sup> concludes that information security is at greater risk from internal users versus external users. Internal users have direct access to an organization's data. In turn organizations have developed many information security policies and implemented many technologies to mitigate the risk to its data. Some of these technologies include:

- Complex passwords and short password expiration intervals
- Dual form authentication
- Biometrics
- Encrypted file systems
- Role based security
- Host based virus and spyware scanners
- Web usage filters and loggers
- Email usage filters and loggers

Information security policies will vary based on the industry, implemented technologies and industry compliance requirements. At the core of most information security manuals is a company's "Acceptable use Policy." This policy broadly defines what is acceptable and not acceptable use of technology resources within an organization. This policy typically references

an organization's disciplinary policy in the event that "not acceptable" use is deemed to have taken place.

While these mitigation strategies are placed in the best interest of the organization they can at times cause unexpected problems. These problems are encountered by both the users and the organization's staff whose responsibility is to monitor and enforce the information security technologies and policies implemented. The problems encountered by users are in the area of access and use of the protected information. Organizations that have data to protect will have some type of authentication mechanism. The basic method of authentication is establishing a unique password for all users. A large number of organizations have adopted the best practice of using strong passwords and forcing users to change them frequently. This poses a challenge for users who need to keep track of an increasing number of passwords and complexity. In turn users will opt to write the password down instead of remembering it. This is writing down of passwords is a security risk however it is a response to the controls placed in a user's environment. Once a user is authenticated on the network she has access to resources which she has been given explicit access to. Within the network the user is faced with a wide variety of additional security measures. These measures include role based security which defines what data the user has access based on her particular role. Role based security is also propagated down to the application that the user uses. The user can be denied access to data or system functions she needs access to if the security rules are not well designed.

Role based security can also be linked with the level of Internet access a user is granted. There are wide array of products that an organization can implement to filter sites with questionable content. Some of these products include Microsoft ISA Server, Surfcontrol Web filter and Websense Web filter. The challenges with these products are that some are based on keywords and others site definitions or both. Keyword based filters look for words within a site which are defined as inappropriate by the organization and block access to the site. The challenge with this setup is that the filter can block out legitimate sites if the keyword dictionary is poorly defined or not maintained. For example an investment bank might block sites with content including the word "Viagra" however this might not work in a healthcare facility where a doctor might be looking for a drug-drug interaction with the drugs "Zoloft" and "Viagra." Some products, specifically Surfcontrol's Web Filter uses categories to define sites to block. The challenge here is that this is manual process performed by Surfcontrol staff. The Internet is very dynamic and sites appear every day. This risk of missing a new site or mis-categorizing a site can lead to problems for the user. The same risks can be stated for email filters which filter emails using content keywords, attached file types and SPAM blacklists if the filter is designed to filter such traffic. It must be noted that web and email filters can be categorized as perimeter security however their effects directly affect usability and internal security.

Home users might not have all the challenges that users operating within an organization have in regards to usability issues. Home users also need to be concerned about viruses and exploits. Organizations might have the ability to setup automated virus definition updates and spyware scans on corporate PCs. Home users on the other hand might not have the expertise to setup such tasks on their PCs. Security software developers are aware that a majority of users might not comprehend all the risks posed to their data which in turn will lead to lack of understanding on how to apply security solutions. In response security software developers have designed programs that are user friendly and ready to run out of the box. This is beneficial to users if everything runs properly and the software packages are kept up to date. In the event something does go wrong with the software such as in the case of an expired antivirus license or corrupted installation a user might not have expertise to detect and correct the problem. This in turn exposes the user to risks.

## 4.2 Perimeter Security

Perimeter security is an organization's first line of defense against intrusions. An organization's perimeter is its outward facing network. An outward facing network is a network that is accessible to external entities. Web servers, email servers and web portals usually reside on an outward facing network. Perimeter security for an outward facing network is usually handled by a network security device or appliance such as a firewall. The firewall's sole purpose is to guard the perimeter and prevent intrusions or rogue code from entering. Firewalls accomplish this by using packet filters, antivirus detection, intrusion detection mechanisms and access control lists. These measures are effective in guarding against existing threats. In regards to new threats, the firewall must be updated and reviewed regularly so these threats can be identified and addressed.

Historically, organizations have placed a large focus on perimeter security. Organizations have invested a great deal of financial resources in network firewalls, intrusion detection and intrusion prevention devices. Unfortunately, firewalls and perimeter security devices give organizations a false sense of security. This is because most information security breaches are from internal sources as stated earlier in this paper. However perimeter security is a very important part of an organization's information security strategy. Usability issues with perimeter security are not necessarily directly felt by the end users except for the effects of web and email filters. Instead usability issues are felt by the system administrator who are tasked out to configure and manage these perimeter security devices. The devices and solutions which make up an organization's perimeter security must be configurable and adaptable to deal with new threats. The devices should also provide administrators with relevant and actionable information.

Mid and large size organizations' perimeter can be extensive however home users do not need such systems. Home users do need perimeter protection and thus the vendors who provide solutions for large organizations also provide home user versions of their products. Perimeter products geared to the home user have easily configurable settings presented in a user friendly interface. The interfaces are typically web based as in the case with NetGear's FVS318 Home Firewall. The security features included in these devices are not as extensive as their enterprise level counterparts. However it is still challenging for the lay user to understand all the risks that exist in the Internet and thus fully understand the proper implementation of a home firewall. A poorly configured firewall can be as dangerous as having no firewall at all.

The high availability of the Internet is a concern for home users in that there are a large number of sites with content which might be considered inappropriate to some users. PC based software firewalls and hardware based firewalls offer some protection but not to the degree that enterprise class systems provide. They provide protection by offering similar filtering capabilities however the burden is on the home user to configure the firewall based on their web browsing requirements. Online service providers such as America Online have a "Parental Controls" solution which relieves home users from this complicated task by offering a configurable control panel to manage all aspects of web content filtering. However, America Online users represent a small fraction of total Internet users. Microsoft's Internet Explorer comprises the majority of Internet browser use. While we suggested in the preceding section that an approach to mitigate risks with IE would be to disable ActiveX controls and setup browsing zones, this might be a challenging task to a lay user.

## 5.0 Conclusion

In this paper we have defined and discussed the objectives of malware. We also examined some of the mechanisms which are used by malware to accomplish its objectives. We also provide some risk mitigation strategies that organizations and regular users can use to protect themselves. Risk mitigation technologies however are not effective unless the end user can easily modify them to adapt to new threats. Additionally the risk mitigation solutions must also provide feedback to the user so she can react and take action where needed.

The nature of technology is very dynamic. Users are faced with new products and solutions too frequently to learn about them in any depth. Users are also faced with new threats on almost a daily basis. The amount of information to sift through can be daunting. It is however necessary to at least have a basic understanding of malware and its potential risks. This is also true of the available risk mitigation techniques and technologies. A user's best defense is indeed education.

## 6.0 Works Cited

---

- <sup>1</sup> Hal McConnell, Luncheon talk at BlackHat Conference, Las Vegas, Nevada July 27 2000.
- <sup>2</sup> CNN.COM “US Intelligence computer crashes for nearly 3 days”  
<http://archives.cnn.com/2000/US/01/29/nsa.computer/> as visited 11/15/2005.
- <sup>3</sup> Techweb.com “Latest Online Menace: Custom Worms Built for Industrial Espionage”  
<http://techweb.com/wire/security/163702797> as visited 11/7/2005.
- <sup>4</sup> BBC.CO.UK “Computer Viruses now 20 years old” <http://news.bbc.co.uk/1/hi/technology/3257165.stm>  
as visited 11/18/2005.
- <sup>5</sup> Brian Krebs on Computer Security “DHS Official Weighs In on Sony”  
[http://blogs.washingtonpost.com/securityfix/2005/11/the\\_bush\\_admini.html](http://blogs.washingtonpost.com/securityfix/2005/11/the_bush_admini.html) as visited 11/18/2005.
- <sup>6</sup> Dittrich, David (1999). “The ‘stacheldraht’ Distributed Denial of Service Attack Tool”  
<http://www.sans.org/y2k/stacheldraht.htm> as visited 11/20/2005.
- <sup>7</sup> USAO/CDCA Press Release 11/3/2005 “Computer Virus Broker Arrested for Selling Armies of Infected Computers to Hackers and Spammers” <http://www.usdoj.gov/usao/cac/pr2005/149.html> as visited 11/20/2005.
- <sup>8</sup> Symantec.com Viruses & Risks -- <http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.e@mm.html> as visited 11/19/2005.
- <sup>9</sup> BBCNews, “[Computer viruses now 20 years old](http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/3257165.stm)” <http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/3257165.stm> . Retrieved on November, 2005
- <sup>10</sup> Trend Micro, “[Virus Map](http://www.trendmicro.com/map)”. <http://www.trendmicro.com/map> Retrieved on November, 2005
- <sup>11</sup> Danchev, Dancho (2004) “[Malware – It’s Getting Worse](http://www.windowsecurity.com/articles/Malware_Getting_Worse.html)”.  
[http://www.windowsecurity.com/articles/Malware\\_Getting\\_Worse.html](http://www.windowsecurity.com/articles/Malware_Getting_Worse.html) Retrieved Nov., 2005
- <sup>12</sup> Klinder, Bernie (2002) “[Computer Virus Primer for Network Administrator](http://labmice.techtarget.com/antivirus/articles/avprimer.htm)”  
<http://labmice.techtarget.com/antivirus/articles/avprimer.htm> Retrieved Nov., 2005
- <sup>13</sup> Grimes, Roger (2003). “[Life Cycle of an E-mail Worm](http://redmondmag.com/features/article.asp?EditorialsID=351)”.  
<http://redmondmag.com/features/article.asp?EditorialsID=351> Retrieved Nov., 2005
- <sup>14</sup> Cody, Jason Allen (2004). “[Congressional Attack on Axis of Internet Evil](http://practice.findlaw.com/tooltalk-1004.html)”  
<http://practice.findlaw.com/tooltalk-1004.html> Retrieved Nov., 2005
- <sup>15</sup> Samson, Martin (2005). “[Internet Law: Click-Wrap Agreement](http://www.phillipsnizer.com/library/topics/click_wrap.cfm)”  
[http://www.phillipsnizer.com/library/topics/click\\_wrap.cfm](http://www.phillipsnizer.com/library/topics/click_wrap.cfm) Retrieved Nov., 2005
- <sup>16</sup> Cohen, Fred (2005). “Enterprise Strategies for Defending Against Spyware.” Burton Group Research 7300
- <sup>17</sup> Friedlander, David (2004). “What to Do About Spyware.” Forrester Research 35770
- <sup>18</sup> Girard, John (2004). “Spyware Tales from the Analyst Files”. Gartner Research COM-23-2333
- <sup>19</sup> Pescatore, John (2004). “Preventing and Removing Spyware”. Gartner Research DF-23-1794

<sup>20</sup> Hallawell, Arabella (2001). "Signature-based Virus detection at the Desktop is Dying." Gartner Research SPA-14-0415

<sup>21</sup> Leong, Lydia (2004). "Companies Must Fight Spyware with Tools, Not Words." Gartner Research DF-23-2614

<sup>22</sup> Freidlander, David (2005). "Antispyware Adoption in 2005." Forrester Research 36312

<sup>23</sup> Baum, Fraga, Kreizman and Sood (26June2002). "Security Imperatives for Leaders in a Networked World" Gartner Research COM-17-1102