



# Information Security in Law Firms



- Year 2003, in the second week of August, the Law Community of New York city experienced a real havoc in their information systems and network resources. Emails that appeared to come from legitimate addresses of known faces and regular establishments in the legal circle clogged everyone's mail box like crazy, only to steal more email addresses and multiply. The culprit was the email worm, 'Sobig'.
- Butera & Andrews, a Washington DC Law Firm, files a suit against IBM to seek unspecified damages and repayment of expenses incurred in investigating an intrusion and espionage in its email service and internal networks, allegedly carried out by an unnamed IBM employee. According to Butera & Andrews, the IP address of the computer traces down to an IBM facility in Durham, North Carolina.
- An Advocacy Group by name Center for Democracy and Technology, put out a list in March this year to shame those advertisers who employ Adware and Spyware in selling their products. The exposure took place in the wake of a suggestion for public humiliation as a punishment for companies using Adware to promote their products, by Jon Leibowitz, a commissioner of the U.S. Federal Trade Commission.

## The Current Threat Scenario

There are no two ways about the fact that America is a litigious society. In our civilized world, bitter battles are fought, won and lost in courtrooms, where Law Firms form the troops and battalions armed to their teeth and nails. In this business of trust and commitment, it's of paramount importance to safeguard your secrets, strategies and often times, highly critical and incriminating client information.

Nationwide implementation of federal judiciary's Case Management/Electronic Case Files (CM/ECF) is at its final stage in District and Bankruptcy courts. The new system would require Law Firms to convert Word documents into PDF format and log on to the Court's website to file them. Now, there are some Viruses and Worms that spread using PDF files as carriers and such a malicious document unknowingly uploaded by you, can create severe issues in the court's database.

One of the key concerns for Law Firms in United States is the presence of vulnerable systems in their networks due to the general lack of user awareness in Information Security issues and a significant presence of part-time staffs. A single user's carelessness can introduce a network or email worm in the internal network of a firm and it won't take much time before the Malware brings the entire organization to its knees.

Network hackers can easily sneak into the internal systems of a Law Firm as they perpetually scan the Internet for vulnerable systems to hack into and spy on. In a targeted attack with the help of a Black Hat, your opponent firm can get hold of some critical evidences that you were planning to present in the court, to prove the case against the accused. By employing new techniques, this data stealing can be done quite insidiously, leaving no traces behind.

Another menacing fact is that many breeds of Malware created by today's online crime syndicate also have the capability to sneak into and control targeted computers. Trojans, Backdoors and Bots that spread via emails, network sharing, web downloads and plain browsing, can be employed by a remote attacker to takeover information systems and do as he pleases.

Deadline for a Law Firm to complete a task is decided by the court and it's truly a do or die situation within that stipulated time. Unlike the timeframe given by a client, there is no scope for date creeping in here. If a worm capable of destroying all PDF and Word files enters in your internal systems the day before an important hearing in the court, you may not want to imagine the ensuing jeopardy!

Here is a lowdown on various types of threats that Advocacy Firms face in their online activities.

## **Onslaught of Virus, other Malware and Riskware**

### **Virus**

A typical computer Virus is a malicious program that destroys and alters files and folders, while replicating on its own. A virus usually attaches or inserts itself into an executable file or the boot sector of a disk.

### **Network Worms**

This Malware spreads via P2P File sharing, LAN, WAN and even over the Internet using file sharing programs. A worm wriggling into a vulnerable computer of a large network will send requests to all other machines in order to infect every computer across the business house.

### **Trojan**

A Trojan refers to a program or a file that may look harmless otherwise, but carries a malicious component in it. Regular Trojans do not replicate on their own but can be highly destructive, harm other applications and threaten your Data Integrity.

Many Law Firms have been seriously affected by the increased and more targeted attacks carried out by various Trojan families. A MicroWorld study in November 2005 revealed that 43% of Malware cases reported by Law Firms in US, UK, South Africa and India involved various breeds of Trojans.

### **Trojan Downloaders**

They download other Viruses, Worms and Trojans into the victim's machine from the Internet. According to the requirements of the Operating System, the downloader either launches the executable component or registers to enable its auto run.

### **Trojan Clickers**

This breed redirects victim's machines to specific websites or other resources on the Internet. They make this possible by tampering with Windows HOSTS file and rerouting regular web requests towards wrong websites. Trojan Clickers are widely used in increasing the hit count of specific websites or for launching Denial Of Service (DOS) attacks.

## **Pharming Trojans**

This breed is similar to Trojan Clickers, and is used in a deadly attack called 'Pharming'. While an attorney keys in the website address of a court in order to file a case document over the Internet, a hidden Trojan Clicker can redirect him or her to a spoof website that looks completely identical to the original, and loot your information.

## **Keyloggers**

Keyloggers remain silent in a compromised computer and capture usernames and passwords when a user logs on to websites of Financial Institutions, Banks and Credit Card Companies and the Information is then mailed to the author of the Malware. Some of the more evolved ones can take screenshots and capture mouse clicks too. This malicious code is a core component in Password Stealing Trojans.

Keyloggers can pose a dangerous threat to the Data Integrity of Law Firms. If they manage to steal the username and password of a Law Practitioner's email system, all of his or her mail communication can be spied on, day in and day out.

## **Backdoor**

This Malware is hooked into the victim's system by an intruder, in order to gain Access and Control of it. IRC channels are widely used by Backdoors to connect to the attacker and to be ready to take orders from the criminal in his far away hideout.

Using the Backdoor, the attacker can operate a compromised computer like his own desktop and execute commands. For an Advocacy Firm, a backdoor infection could cost its secret strategies, confidential files or highly sensitive forensic evidence to be used in litigations. 21% of Malware detected in Law Firms were seen possessing Backdoor capabilities, according to the MicroWorld study referred earlier.

## **Rootkit**

A Rootkit is used by malicious programs to hide running processes, files or system data, so that Security Applications may not detect their presence in the computer. They modify parts of the Operating System, install themselves as drivers or kernel modules to achieve deep penetration in the computer. It's the favorite hiding mechanism for many recent Backdoors and Trojans.

## **Spyware**

Spyware is a risky, malicious program typically bundled as a hidden part of freeware or shareware programs, downloaded from the Internet. It spies on user activities on a computer and sends that information over the Internet to the Malware author. Spyware eats up system memory, damages its functioning, sneaks into sensitive, Personal Financial Information like Credit Card numbers and passwords.

## **Adware**

Adwares are nasty software programs that pester your computer screens with countless pop-up advertisements. Often they push you to the limits in their attempts to make you visit certain websites, buy tacky products online or join scam services. Often they can cause system crashing while robbing of your computing resources and bandwidth, all the while being a perpetual nuisance.

## Specific Dangers in the Acrobat (PDF) Environment

As we've seen earlier, PDF is going to be a regular file format for Law Firm activities, after the implementation of CM/ECF. This file format too is vulnerable to Malware attacks and carriage. Some Viruses and Worms use PDF files as host for proliferation while other breeds delete all PDF files.

In the year 2001, a Worm named 'Worm.VBS.Peach' was found to be spreading by using a PDF file as a host. It comes with an embedded VB script and when you open a malicious document in Adobe Acrobat's full version, it shows an image with a puzzle game called 'Find the Peach'. The worm slips into your computer, while you click on a link to find the solution for the puzzle. VBS.Peach steals email addresses from the victim's address book and sends self copies to all ids.

The infamous Kamasutra worm, first detected by MicroWorld Technologies, destroyed PDF documents along with Word and Excel files on the 3rd of every month, in infected machines. The Worm came in the form of Pornographic messages titled 'Kama Sutra pics', 'The Best Videoclip Ever', 'School girl fantasies gone bad', 'A Great Video' and 'Arab sex'. It managed to lure many unsuspecting users to click on the attachment and download it, only to invite a time bomb into their computers, while the worm was also found to be spreading in networks via shared resources.

Some security flaws have also been exposed In the Acrobat software. A Buffer Overflow vulnerability named CVE-2005-2470 was identified in a core application plug-in of Adobe Acrobat and Acrobat Reader, exploiting which Malware authors could crash the software and execute malicious code in the computer when you open a specially crafted PDF file.

## The Spam Trouble and Phishing Menace

The Center for Democracy & Technology, the Advocacy Group mentioned earlier, has done some extensive studies about Spam mails and they found that email addresses posted on the web and Chat Services are quickly harvested by spammers using an array of techniques to send large numbers of unsolicited mails to those addresses.

Wading through the clutter of Spam is one of the biggest challenges faced by employees of advocacy firms on a daily basis. And the real danger lies in accidentally deleting important and legitimate mails in that process. Bandwidth issues, Storage Concerns, Loss of Productive hours and Distribution of Malware are some other ramifications of Spam mails in organizations.

### Categories of Spam

A research by MicroWorld Labs in July 2006, reveals that the total number of worldwide spam mails per day stands at a staggering 25 billion. MicroWorld categorizes present day spam into segments given below along with their respective shares in the total.

Adult Content -23%

Consumer Products- 20%

Health -16%  
Finance- 14%  
IT and Internet-11%  
Phishing- 6%  
Education and Training-3%  
Others-7%

60 billion US Dollars is what the world lost by way of dent in productivity and wastage of technology last year as a direct and immediate impact of spam, while its second and third levels of impact on the economy could be much deeper and wider.

### **Phishing and Identity Theft**

Phishing is a form of online criminal activity using smart Social Engineering tactics to steal the identity of other people, in order to break into their personal accounts in banks, credit cards, auction websites and other financial institutions. Phishers attempt to acquire sensitive information such as usernames, passwords, PIN and Social Security Numbers by masquerading as a trustworthy person, business house or bank, working via emails, IMs or other channels of communication.

Phishing affects employees of Law Firms more on a personal level than in an official way. Their confidential personal financial information is at greater risk as Phishers improve their methods of deception and technology at astonishing speeds to prey on more victims and line their wallets.

## **Port Scanning for Network Hacking**

Port Scanning is the most popular reconnaissance technique used by attackers to identify vulnerable systems and services in a network. Many services work with TCP and UDP ports and there are as many as 6000 ports currently used in networking.

In Port Scan an attacker sends messages to targeted ports and based on the response it generates, probes deeper for vulnerabilities. TCP ports are targeted the most as they are connection oriented and normally give immediate response to the Intruder.

Some methodologies used in Port Scan are given below.

### **SOCKS Port Probe**

SOCKS is used in a network to facilitate sharing of Internet connection among multiple systems. There's a good possibility for erroneous configuration of some of these ports by a significant share of users, creating arbitrary sources and destinations. This helps a cyber criminal to hide his location and access the Internet through the victim's machine.

### **Stealth Scan**

Normal Port Scanning is done with the help of a series of packets rapidly fired at the host. Now, 'very slow scanning' can be used as a stealth technique to avoid detection. Another such method is called Inverse Mapping, where the attacker finds all hosts in the system by employing "host unreachable" ICMP-messages.

### **Fragmented Packet Port Scan**

This is done by breaking a TCP header into several IP fragments. Many firewalls can be tricked by this technique as they try to match the whole TCP header to identify an attempt of intrusion.

## **How to Defeat Security Threats and Protect Your Digital Assets?**

MicroWorld Technologies has developed the world's most advanced security solutions to combat various threats aimed at information systems. Its products eScan, MailScan and eConceal will provide a comprehensive, multi-layered protection for Law Firms, at the same time being easy to deploy and highly user friendly.

### **eScan AntiVirus and Content Security**

eScan is the world's most powerful and advanced Anti-virus and Content Security solution that safeguards Workstations and Servers from all kinds of Malware, future threats, Adware, Spyware, Spam, Phishing mails and Other Content Security Issues.

eScan uses a revolutionary technology named MicroWorld Winsock Layer (MWL) to block security threats at the Socket Level itself, way before they enter your application level and thus saves the need for writing files to a temporary folder before scanning. Data packets coming at different TCP/IP ports are assembled at the MWL Layer and get scanned for Malware, there by making sure that threats are tackled in a preventive way.

MWL Technology forms a protective screen around your system that's always 'On', while you carry on with your activities on the computer. It empowers MicroWorld Solutions to comprehensively block and prevent all kinds of malicious code from entering into Information Systems.

### **Real-Time Malware Scanning with the Earliest Detection Record**

eScan checks e-mails and websites in real-time, including email and web traffic, to protect computers against Viruses, Worms, Trojans, Spyware, Adware, Keyloggers, Backdoors, Rootkits and more. It has the fastest and earliest updating database for detection and removal of all kinds of Malware including latest exploits targeting vulnerabilities in Operating Systems and other Software Applications.

### **Integrated Security Policy Enforcement**

eScan Management Console enables the network administrator to view and access the entire network architecture, including activities at different workstations. Features allow the administrator to distribute updates across the network, send Outbreak Alerts and Security Violation notifications and carry out remote installation and Uninstallation.

With the Centralized Security Management of eScan, even rouge systems can be managed and protected against Viruses and Worms.

### **Remote Administration**

This is a powerful feature of eScan that helps the Network Administrator access the "eScan Management Console" from a remote location. This will empower the Administrator to manage the security of an organization even while being away from the office.

### **Heuristic Scanning**

eScan employs a highly sophisticated Behavioral and Intention analysis method to identify unknown Viruses and Worms. This means eScan will proactively block even that malicious code which doesn't have a signature of it in the eScan's AntiVirus Database.

### **Rootkit Tracing and Removal**

eScan comes with the power to detect and remove Rootkit components in the system so that Worms and Trojans cannot hide their presence.

### **Powerful Protection against Spyware and Adware**

eScan has a continuously updated database of protection against Spyware and Adware that mushroom in many forms and names every passing day. The software also repairs damages done to the system by these Riskwares.

It gives options to block Active X controls, exploit codes and Trojan Droppers that target browser vulnerabilities, to make sure that no unwanted program is installed in your computer using deceptive ways.

### **Blocking Offensive and Non-Business Websites**

The process of website filtering works on the basis of occurrence of certain 'probable' words like sex, gambling, chatroom and alike, in webpages. In order not to block legitimate websites, eScan screens the web content on the basis of total number of such unique words appearing in a webpage. If the word count goes beyond a certain threshold level, then the website in question will be banned. For Law Firms, this gives the opportunity to streamline their web access and to block non-business websites.

### **Pop-Up Ad Blocker**

eScan stops pop-ups that plague your screen while you work on your computer. eScan's Pop-Up Blocker, unlike most pop-up blockers, does not make you wait for a window to appear and disappear, and this saves your bandwidth significantly. You can create a White List to allow Pop-Ups of specific websites and also use the 'hot key' option to temporarily allow pop-ups.

### **Privacy Control**

To protect your privacy and to prevent access to personal information, eScan erases links of visited sites and entries made in online forms. Features allow the user to schedule browser clean-up for Cookies, Plugins, History, Cache, and links to most recent files and images opened.

## **MailScan - AntiVirus and Content Security at Mail Server**

MailScan is the ideal AntiVirus and Content Security solution for Law Firms to safeguard their Mail Servers. Working at the Mail Gateway, MailScan scans and cleans emails that flow between all local users and emails between the Internet and Mail Server. It protects organizations against Virus, Worm and other Malware and stops Spamming and Phishing while providing total Content Security.

MailScan works at "TCP/IP Port level" and hence does not require an additional machine to act like a gateway. It is based on the revolutionary MicroWorld WinSock-Layer (MWL) technology, the first of its kind in the world. At the Gateway, MailScan performs;

- Scanning of all e-mails for Viruses and other Malware
- Content control checks on the email body.
- Spam control using Real-time Black List, Sender Policy Framework, Non Intrusive Learning Patterns and other technologies.

### **Integrated Mail Security Policy Enforcement**

MailScan works on policy-based Rule-Sets. They have been categorized as universal and company specific. While universal Rule-Set is defined by default, company-specific Rule-Set is configured by Network Administrators of individual firms.

### **Real-Time Virus Scanning**

It Scans e-mails and websites for all breeds of Malware in Real-Time, in all inbound and outbound SMTP and POP3 mail traffic at the Mail Gateway itself.

### **Heuristic Scanning**

Sophisticated Heuristic Scanning to prevent newer Viruses, mutant variants and hidden malice in a proactive and pre-emptive manner.

### **Mail Traffic Management**

It gives you the option to define a selected list of users at the MailServer level, whose mails need to be scanned for restrictive content. Administrators can also block certain domains from sending or receiving emails.

### **Web Based Administration**

MailScan Administration Console can be accessed using a browser, thus enabling Remote Administration of the application.

### **Real-Time Content Scanning**

All incoming and outgoing messages are scanned in Real-Time for offensive words, Adult Content and expressions by pre-defined Security Policies. This way, administrators can control and restrict external and internal email content of employees.

### **Compression and Decompression**

Oversized files are compressed using standard file compressors. MailScan can be configured to create '.EXE' files or self-extracting zip files that are automatically decompressed at the recipient's machine.

## **Blocks Spamming and Phishing**

MailScan stops Spamming and Phishing using a combination of highly powerful technologies like,

### ***Real-Time Black List (RBL)***

RBL is a DNS Server that lists IP Addresses of known Spam sending machines. If the contacting IP is found to be in one of the blacklisted categories, the connection is terminated.

### ***MX/A DNS Record Verification***

The domain part of the email address is checked to see if it has a DNS MX (Mail Server) and/or A (IP) record as it is typical of spammers to use non-existent domains in their emails.

### ***Reverse DNS***

A reverse DNS check is performed to see if the connecting IP resolves to a valid domain name before accepting or rejecting the email.

### ***X-Spam Rules Check***

X-Spam Rules are Rules that describe certain characteristics of a mail and they are matched against the mail header, body and attachment to generate a score for each mail. If the score crosses a threshold value, then the mail is considered a Spam.

### ***Gray Listing***

A new email from an unknown sender is kept out for a certain amount of time before accepting it. The logic is that if it is a legitimate mail, the Mail Server will try to resend it while in most cases, spammers won't.

### ***Sender Policy Framework (SPF)***

Sender Policy Framework is a world standard that helps to prevent forgery of sender address, and hence works as a powerful mechanism to stop Phishing mails.

### ***Non Intrusive Learning Patterns (NILP)***

This is a revolutionary technology from MicroWorld that works on the principles of Artificial Intelligence to create an adaptive, self-learning mechanism in Spam and Phishing Control.

NILP is an advanced Bayesian Filtering method that can analyze each mail according to the Behavioral Patterns of the user and can take an informed decision based on that. Unlike regular Bayesian filters, this system doesn't need to be trained, has the capability to learn on its own and incorporates regular research feeds from the MicroWorld Server.

## **Attachment Control**

Powerful options to restrict certain attachments like EXE or COM from being sent or received via the Internet. The System Administrator of a Law Firm can restrict permissions given to employees to send out confidential information, thereby blocking attempts of espionage.

## **eConceal Firewall - Total Protection Against Network Intrusion and Hacking.**

eConceal is a powerful, highly advanced network Firewall designed to protect your internal network against attacks via the Internet. The firewall offers customizable security with user-defined rules for Packet Filtering and Access Control. eConceal Firewall allows a Law Firm to create Rules based on non-IP protocols such as ARP, whilst supporting multiple network adapter configurations.

eConceal manages and controls multiple channels of Internet access in a Law Firm based on default and user created Rules. These Rules function as filters by analyzing data packets to see if they fulfill the filtering criteria and then allow or block the access accordingly.

### **Port Monitoring**

eConceal prevents Port Scanning from network attackers and alerts you of any such attempts by Intruders. eConceal allows the user to specify Source and Destination ports, and Source and Destination IP addresses. This feature enables you to enforce Communication Control on specified ports and systems.

eConceal also helps you prevent intrusions by many Network Worms by restricting external access to vulnerable ports.

### **Network Data Filtering**

eConceal Continuously monitors and filters network IP and Non-IP Traffic so that no intrusion takes place into internal networks of Law Firms.

### **Active Connections**

This option shows details of all TCP connections on your system. Information like Process, Protocol, Local Address, Remote Address, Status and Start Time are given in detail.

### **Filtering Level**

It supports Application and Packet Level filtering. Application Level helps you set up Rules for a particular Application. Packet Level provides filtering for incoming and outgoing data packets

### **User-defined Rules**

The Firewall provides a powerful Traffic Filtering system with user-defined processing Rules. Users can define Rules according to their requirements and implement customized traffic filtering.

### **Preset Rules**

eConceal offers a set of pre-defined Rules that users can choose from, in order to enforce a total Access Control in the organization. The different types of rules are ARP, DHCP & BOOTP, DNS, E-mail, WWW, News, Net Bios, FTP, ICMP, ICQ, Telnet & SSH, IRC, MSN, and VPN.

### **Network Traffic Monitor**

This feature shows current data traffic on your system, including information regarding open programs and ports used in communication.

### **Stealth Mode**

eConceal gives you the power to surf the Internet invisibly, without letting other online users see you. When online, your computer constantly receives and responds to information requests from other computers. In stealth mode your computer will not respond to this flow of queries and requests, and there by reduces the possibility of system hacking significantly.

### **Comprehensive Logs**

The Firewall stores log information detailing programs involved in outgoing/incoming traffic, Communication Protocols used, Source and Destination IP addresses, direction of traffic, and action taken depending on Rules in force. In addition, it maintains an Event Log that details user events – e.g. changing security levels, loading Rules, firewall shutdown etc.

### **Real-time Traffic Monitoring Reports**

It provides clear, concise graphical and non-graphical reports on internal and external Data Traffic. Diverse reports based on Application, Expert Rule, Zone Rule, IP and Date are available along with graphs of different styles like Bar, Pie, Line and alike. These reports enable the Law Firm administrator to quickly analyze the patterns of data movement and to devise strategies based on that.

## **MicroWorld - The Future Tense of Security**

With eScan, MailScan and eConceal, MicroWorld provides a highly advanced, futuristic protection for your Digital Assets and Information Technology Infrastructure. At a time when legal work is getting increasingly computerized and Internet and emails are becoming basic necessities for the judicial process, it's vital for Law Firms to have a comprehensive, robust and ever evolving Security Strategy and Mechanism in place.

MicroWorld consistently delivers Security Solutions that you can rely on, in a business where stakes are truly high, by continuously improvising and innovating its Technology and Solutions.

Because for us and for you, trust is a common value.

## **MicroWorld Technologies**

MicroWorld Technologies ([www.mwti.net](http://www.mwti.net)) is the developer of the world's most advanced AntiVirus and Content Security software eScan for Desktops and Servers. Its gateway-level email security software, MailScan, is a comprehensive mail scanner for SMTP/POP3 Mail Servers. MicroWorld Winsock Layer (MWL) is the revolutionary technology underlying these products, powering them to several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready and Novell Ready. On the Network Security side, MicroWorld offers a powerful, futuristic network firewall branded as eConceal.

To learn more, kindly visit <http://www.mwti.net>.