

Information Security for Windows Environments

Razvan Livintz
Communication Specialist, BitDefender

Corporate network administrators face daily challenges. They must fight phishing attempts, identity theft, reputation management and DDoS attacks, and at the same time, the risk of media exposure of the business if they get it wrong.

Top Five Obvious (and Usually Overlooked) Security Tips

Below are the top 5 most obvious security tips that Windows users might overlook.

Securing Your Assets (including Data)

The physical security of the company's computer infrastructure remains today one of the main risks of data leakage and information theft. Leaving the door of servers room open or the data center unattended while the administrator takes a cigarette break or a cup of coffee is the most probable scenario.

The same situation occurs when it comes to laptops. In July 2008 it was reported (1) that 658 MoD laptops had been stolen over the past four years, nearly double the figure previously claimed. It was also admitted that more than 26 memory sticks containing classified information had been stolen or misplaced since January of that year.

Strengthening Network Perimeter

Corporate networks should always be protected by firewalls, including client firewall. Microsoft Windows Firewall for instance, which is available with Windows XP SP2, offers enough security and, most important, can be centrally administered via Group Policy.

Since laptops are likely to be used in open, unsecured wireless environments, one should disable any files, folders and printers sharing, to prevent unwanted access from a potential intruder.

In situations where reliable connections are not available, for Wi-Fi access, then a combination of Wi-Fi Protected Access (WPA), anonymizers, as well as encryption may be adequate.

Ideally, one should use an encryption method which prevents file access as well as data interception. A Secure Sockets Layer/Transport Layer Security (SSL /TLS) protocol could provide enough security and data integrity for the Web-based communications over the Internet, such as the Web-based corporate e-mail.

For remote connections, Internet Protocol Security Virtual Private Network (IP Sec VPN), which creates a secure tunnel and encrypts all digital traffic between the

¹ Government officials admitted 6 as reported by the BBC and Times Online.

remote machine and the corporate network, should be a must, especially when dealing with the access to the e-mail client, organization's database or other resources stored on the network.

Protecting Sensitive Information

Ideally one should disable the Guest account and auto-logon option and create access passwords for all the users registered within the same machine.

The use of Administrator account should also be avoided, unless it is really necessary for system updates and special installations. One could appeal instead to the convenient User Account Control (UAC) options available in Windows Vista and Windows 7 Beta.

Users should suspend the current session, either by locking the system or by logging off, when they are away from their machines.

Last but not least, the circumvention of electronic security could be a risk. Employees with different access level can easily print sensitive data that is otherwise restricted by hard policies of files and folders permissions.

Deploying Antimalware Suites

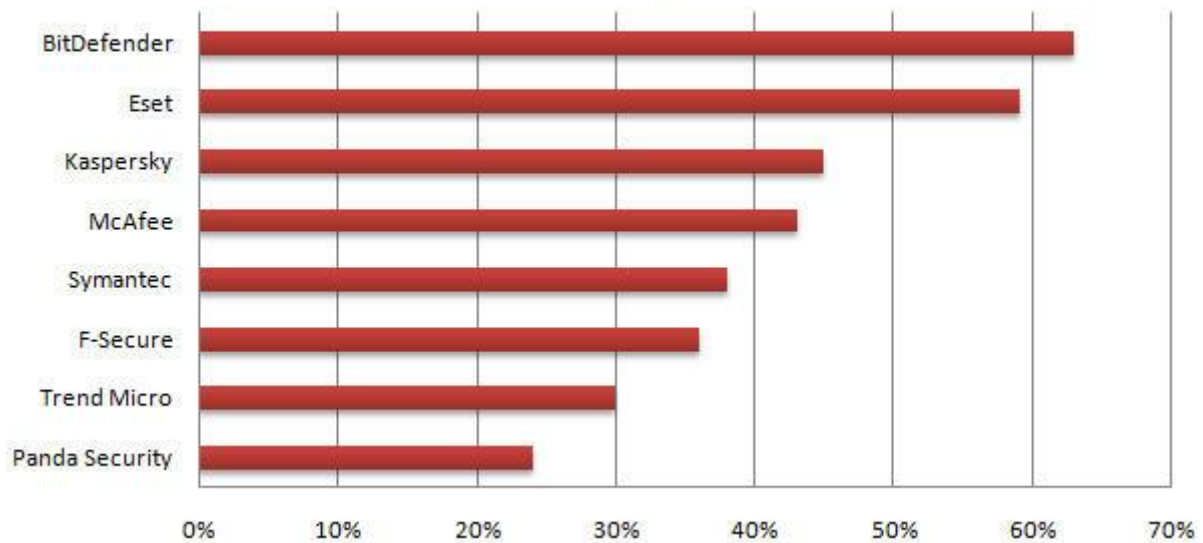
In the current malicious environment, the one fifth of the globe population connected to the Internet has to cope with approximate 2,000 new and mutated viruses per day, almost 50,000 phishing attempts per month and more than 1,000,000 hijacked computers that spread bots, rootkits and other malware during one year. More than 80 percent of these e-threats target Microsoft Windows-based systems.

The most efficient and effective solution for protecting networks, machines and data is to install a reliable antimalware solution. A comprehensive Security suite today will include firewalls, content filter, phishing and spam protection, as well as other protection tools, usually based on heuristic methods.

Security software vendors have introduced heuristics and behavior based technologies to detect new or mutated breed of malware, rather than using a list of known e-threats. This led to a drastic decrease of the time elapse between the launching of malware and the issuing of an antimalware signature update (also known as window of exposure). BitDefender's B-HAVE dynamic heuristic scanner, for instance, detects 63% of e-threats, without needing a signature (2).

² Proactive antivirus protection test available at <http://www.anti-malware-test.com/?q=node/39>.

Proactive antivirus protection test



Reinforcing Policies

The human factor and social engineering are, probably, two of the most important aspects to consider. Passwords and usernames are the core of every security strategy; but they are also easily to grasp.

According to a report by BERR (3) . the UK Department for Business Enterprise & Regulatory Reform . UK companies are becoming increasingly aware of the fact that their employees should be regarded as a potential vulnerability, and so need to be educated on security risk.

This is leading to a degree of management and fewer reported incidents. However, attitudes and controls in some companies mean that statistics are probably understated, BERR say that companies that carry out risk assessments are four times as likely to detect identity theft as those that do not. In addition the average seriousness of incidents has increased, so roughly a quarter of companies had a serious breach, the same as 2006. (3)

If possible, the use of Internet and other resources for personal purposes should be prohibited or at least restrained. The temptation of social networking Web sites, instant messaging, and chain letters represent the door for malware that usually exploits OSqflaws and bugs.

A simple dropper Trojan that an attacker conceals as a widget or banner ad on the users blog page can easily sneak into an insufficiently protected system. When the user accesses an e-commerce Web site or his company network from the compromised machine, the Trojan could steal the username and passwords, credit card numbers, as well as other sensitive data and send them to the remote attacker.

³ 2008 Information Security Breaches Survey

Although apparently harmless, we could include in the same category the removable media, such as CDs, DVDs or USB flash drives, which usually carry a disruptive payload. Probably the best example is to be found in the Conficker worm (also called Downadup or Kido), which made its first appearance late November 2008, exploiting the MS08-067 vulnerability in Microsoft's operating systems to spread unhindered in local area networks via USB sticks.

Top Five Obscure (and Hardly Considered) Safety Issues

Windows users may also encounter problems as a consequence of ignoring more elaborate security intrusions. Below are the top five less obvious security risks that Windows users often fail to notice due to their complexity and additional efforts that are required.

Client Security – Completing the Trust Circle

Unlike servers, which gather most of the focus of network administrators, especially in terms of security and defensive measures, Windows clients are not scrutinized with the same intensity. There are more of them which make maintenance more laborious and their flexibility makes even small company infrastructure, highly complex.

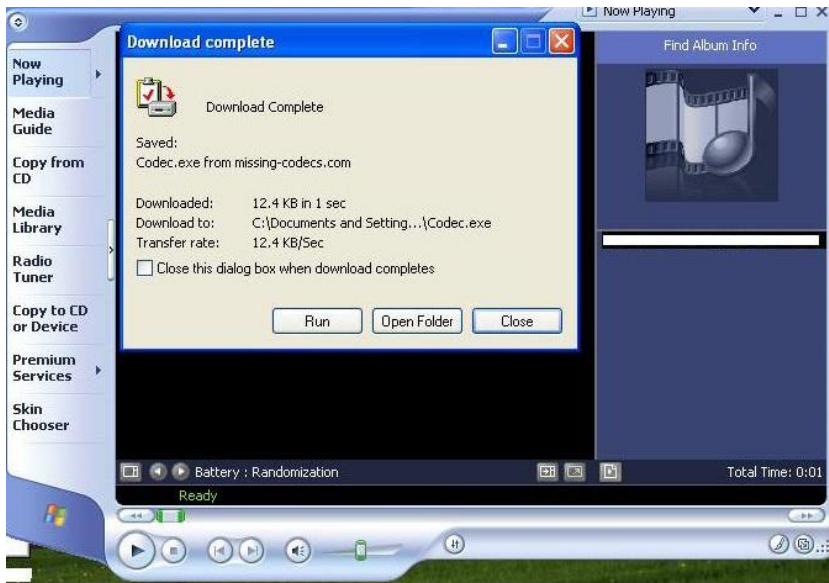
Client computers are technically the access gate to different types of sensitive content that normally resides on the server and cannot be otherwise retrieved. Even if it is almost impossible for one to connect a mobile HDD to a server and to start copying information, it is nonetheless very likely that one access the data stored on the server from a client machine and copies it on a USB stick, bypassing and breaking thus an entire set of policies.

One solution is the use of a Client Security configuration, such as the one BitDefender propose, which enables security policies to be set using pre-defined templates. It maintains mobile users' compliance with corporate security policies even while offline, while also integrating with Active Directory for an easy and flexible management process.

Bundled Vulnerabilities – Protecting from the Enemy Inside

The bundled vulnerabilities refer to applications that Microsoft ships with the operating systems. The (not so) harmless Windows Media Player, for instance, was the victim (or, if you prefer, the tool) for distributing one of the most prolific malware breeds.

Trojan.Downloader.Wimad.A, and its 3.26 percent, placed fourth in BitDefender's E-Threats Landscape Report, being responsible for the infection of 3.14% of the systems worldwide. Usually distributed via e-mail spam campaigns as a 3.5 MB .wma attachment bearing the name of some popular artist, the disguised Trojan automatically opens the Web browser in order to retrieve the appropriate codec, which is, in effect, another piece of adware . Adware.PlayMp3z.A.



Internet Explorer® is another bundled application heavily exploited by malware authors. For instance, in the latest BitDefender E-Threats Landscape Report, Packer.Malware.NSAnti.1 ranked the eight. This malware with worm functionality spreads via infected Web sites or through maliciously crafted autorun.inf files within removable devices. NSAnti corrupts Internet Explorer® behavior and steals user names and passwords for on-line games, such as Silkroad Online or Lineage.

File Permissions – The Devil in Disguise

Microsoft Windows file management system and its derivatives are frequently a burden for both administrators and users. Most files and folders inherit permissions from their parent folders. Once a folder is moved, it inherits the properties from its new parents.

On one hand this mechanism can help one to easily change an entire set of permissions by simply moving the files from one folder to another. What was once a collection of read-only files, now turns into a read-write one with just few mouse-clicks. On the other hand, this could become an ordeal when relocating large amount of files and folders, namely when moving them from a system volume to another one.

Hence, one should be extremely carefully and previously check the permissions status before handling sensitive data that could accidentally end up disclosed.

Background Services – The Skeleton in the Closet

By default, Windows enables and runs at startup several services that one might never need, thus occupying resources and creating potential security breaches. For instance, although the chances for one to use the Remote Desktop Help are minimal, Windows XP Media Center Edition enabled remote desktop by default. A Windows vulnerability allowed an attacker to cause the system crash.

Windows Update – Achilles' Heel

OS patches and updates represent another safety issue hardly considered. The continuously growing rate of Downadup infections in early 2009 revealed that the level of awareness is still low among users. Even when it means to constantly update their OS with the latest fixes against security flaws (the previously mentioned Microsoft RPC flaw was patched in October) or, to put it differently, to enable Windows or Microsoft Update.

The fact that the total number of compromised machines around the globe almost equaled Belgium's or Netherlands' population by the end of Q1 shows that security is not (yet) a major concern.

ENDS