

24 February 2007

By: Marius Oiaga, Technology News Editor



[The Coordinates of Windows Vista Security](#)

Microsoft's Stephen Toulouse gives an insight into security

Stephen Toulouse, senior program manager for the Trustworthy Computing Group was kind enough to give Microsoft's perspective on the security of Windows Vista. However, this mile-long interview covers a larger scope than Vista. You will be able to get an overall idea of the threat landscape for 2006 and 2007, along with the measures Microsoft had implemented in order to protect customers. The interview also covers Microsoft's relations with its security partners, the main security enhancements in Windows Vista, the principal security threat that users will face in 2007, the first service pack for Vista, and so much more...Just sit comfortably, grab a coffee, a large coffee, and enjoy. A large coffee because when I said this is a mile-long interview I was not exaggerating. I would like to use this opportunity to thank Stephen Toulouse and Margeau Lebeau for their patience and help.

Can you give us an oversight of the threat landscape in 2006 in comparison to 2005? What would you say is the backbone of cybercrime in the past year? It's an ever changing landscape, that's certain. In fact, to give an overview of the threat landscape, according to the Common Vulnerabilities and Exposures (CVE) list, the number of vulnerabilities is estimated to have doubled from 2005 to 2006 representing an increase in vulnerability reports across the industry. Social engineering is just one type of attack that has been evolving over the years and encompasses various ways in which criminals trick users into taking actions that reveal or provide access to personal information. According to the 2006 State of the Net study, published by Consumer Reports, phishing scams alone - a major form of social engineering - caused an estimated \$630 million in damage for the year, while the economic damage totaled by spyware infections reached \$2.6 billion. We see social engineering as the online threat that will most likely have the largest impact on users in 2007. So we're focusing of course on providing education and guidance, in addition to tools and technologies, that will help prevent these types of issues. **Without a doubt, Microsoft is at the center stage of the threat environment. In 2006 alone, McAfee has counted over 133 critical and important vulnerabilities spread across Microsoft's products. What has Microsoft done in order to reduce the volume of attack vectors in 2007?** When it comes to software vulnerabilities, it's important to understand that no one is going to get the code 100% correct. Software is a human endeavor and, as such, will always contain a certain amount of error to it. But that doesn't mean we don't try to do everything we can to reduce vulnerabilities and increase software quality. To help improve security overall, we continue to focus on engineering excellence and our understanding of the threat landscape. Through our Security Development Lifecycle we're working to keep the number of security vulnerabilities that ship in our products to a minimum. The SDL is our internal process that helps us develop more secure code. Just as an example of the real impact of the SDL on our products, the Security Intelligence Report released by Microsoft in November 2006, which correlates infection data from hundreds of millions of machines, shows that 54% of infected machines cleaned by the Malicious Software Removal Tool (MSRT) were Windows XP/XP1 (which did not go through the SDL) while Windows XP SP2 represented only 3.7% of the total infected machines. But again, knowing you can't get the code 100% right because no one does, what else can you do to help protect the user? That's where our "Defense in Depth" philosophy comes into play. And probably the best example of how that's going to benefit users in 2007 is Windows Vista. Windows Vista includes fundamental architectural changes that will help make customers more secure from evolving threats. Features such as Kernel Patch Protection, Internet Explorer 7's anti-phishing filter, Address Space Layout Randomization, and support for processor data

execution prevention features are just a couple of examples of underlying protections in the operating system that make it more resistant to attack. Our efforts have resulted in significant improvements in the security of our software, and we have every confidence that, together with our industry partners, we'll continue to meet the constantly evolving challenge to help our customers and the industry to become more secure.

According to Trend Micro's chief technology officer, Raimund Genes, a critical Windows Vista zero-day flaw has a price of \$50,000. VeriSign's iDefense Labs is offering from \$8,000 to \$12,000 for vulnerabilities in Windows Vista and Internet Explorer 7 together with functional exploit code. What is Microsoft's official position in relation to the commerce with vulnerabilities affecting its products? I think what you describe and what we've seen is that the industry is responding to the recent increase in focus by researchers moving away from the operating system and more broadly into all types of software by seeking new opportunities to improve the way that security information is gathered and shared to protect customers. The challenge, as always, is doing that while not aiding attackers. We're certainly aware of companies offering compensation for information regarding security vulnerabilities. Microsoft does not offer compensation for information regarding security vulnerabilities and does not encourage that practice. Our policy is to credit security researchers who report vulnerabilities to us in a responsible manner.

Has Microsoft ever considered becoming a player on the market that trades vulnerabilities to its products? What are the chances that we will see a Windows Vulnerabilities Marketplace initiative from Microsoft? As I mentioned, Microsoft does not offer compensation for information regarding security vulnerabilities. Our policy is to credit finders who report vulnerabilities to us in a responsible manner. We believe the commonly accepted practice of reporting vulnerabilities directly to a vendor serves everyone's best interests, by helping to ensure that customers receive comprehensive, high-quality updates for security vulnerabilities with no exposure to malicious attackers, while the update is being developed. We have no plans to enter that market.

What price would you put on Microsoft buying zero-day vulnerabilities impacting its software and patching them before users are exposed to exploits? Again, we do not believe that offering compensation for vulnerability information is the best way we can help protect our customers. Our policy is to credit finders who report vulnerabilities to us in a responsible manner.

How will the threat environment evolve in 2007? On the consumer end, we believe that malicious attacks via social engineering will impact consumers heavily in the new year. Through social engineering, users are "tricked" into downloading or installing destructive software that can negatively impact their online experience and threaten their computer's level of security, leaving it vulnerable to potential attacks. While technology can assist, ultimately consumer education will be key in combating this type of evolving threat. Additionally, speaking in regards to the threat landscape as it pertains to business consumers, application-layer security threats continue to rise, and organizations are exposed to exploits and attacks from many different sources. Balancing the tensions among security, application functionality and broader access requires a flexible solution that provides rich application security and granular policy-based access. In response to this, we have developed a strong solution within the Forefront family of security products that brings together Service Level Agreement (SSL) virtual private network (VPN), Internet Protocol Security (IPSec VPN), application protection, end-point security, and strong granular policy controls, so companies can extend access to virtually all users and to all network resources with maximum security.

What has Microsoft done in order to safeguard its users from the threats emerging in 2007? As an industry leader, Microsoft recognizes our responsibility to help make the Internet safer. So what we concentrate on is our work with partners, customers, and governments worldwide to help create an environment in which adults, children, and organizations are more secure and can enjoy the full benefits of the Internet without concerns about their safety, privacy, or security. We can clearly see that customers today are facing a broader, more complex and diversely motivated threat

landscape. To address challenges like security, cyber-crime and children's online safety, we're investing in technology fundamentals that make our products more secure as well as new innovations in security technology that provide layered defenses against many kinds of threats. Microsoft understands it has a responsibility to help lawmakers and law enforcement agencies develop laws and policies to ensure online safety and privacy. In partnership with governments worldwide, we're helping to enact legislation that prohibits the distribution of deceptive email or spyware, protects individual privacy, empowers consumers and preserves the health and vitality of legitimate e-commerce. I think in general, Windows Vista and the newer products you are seeing coming out of the SDL, in combination with our security solutions and strong partnerships, are going to have a measurable impact on security in 2007. Of course I should also mention our world class Microsoft Security Response Center, which, should a new threat emerge that impacts customers, can mobilize all those partnerships worldwide to spring into action and protect users. **Generally speaking, end users are regarded as the weakest link in the security chain. Will users play an active role in protecting their computers and confidential data in 2007?**

Should they? That is an interesting question because people are starting to take "the user is the weakest link" as an axiom. As I have mentioned, malicious attackers are increasingly relying on social engineering methods to gain access to users' systems, personal and financial information. Data recently released in Microsoft's Security Intelligence report found that threats against consumers and businesses are continuing to become more targeted and motivated by financial gain. Social engineering was identified as one of the primary means of spreading malware, especially when sent over e-mail and peer-to-peer (P2P) networks. But here's the thing: you cannot state that the user bears part (or even all) of the onus of combating the threat without providing them the education and guidance to do so. We know that technology alone cannot stop the threat of social engineering because it's a technique that relies on tricking or manipulating a user to perform an action, and computers are meant to be used by their owners. We believe that to better protect their PCs from these types of threats, customers need to have help to understand the risks, have clear guidance for safe online behavior and use technology where it can help. In addition to the technological improvements in Windows Vista, Microsoft is committed to working with the industry to provide customers with guidance and resources to help identify and protect themselves from these types of attacks. More information is available at <http://www.microsoft.com/athome/security/email/socialengineering.mspx>

In this context, could you please comment on the risks associated with social engineering? The risks can be very large indeed. Through social engineering, users are often tricked or manipulated into downloading malware or giving confidential information without their knowledge. This becomes a privacy issue if the software tracks and/or shares personal information without the user's consent. Some forms of malware may also take advantage of a security vulnerability or have other negative security implications. Aside from the nuisance of a slow running or unstable computer because of malware, more serious results of social engineering could include:

- Unsolicited pop-up advertisements
- Changes to the user's system configuration (e.g., changing their default browser home page or search engine)
- Unauthorized sharing of personal information
- Configuring the user's modem to place unauthorized calls to a toll number (e.g. a 900#).

To combat this, users should first ensure that their PCs are protected from a security perspective by following the steps outlined on <http://www.microsoft.com/protect>. Protecting your PC is about understanding the risks, having clear guidance for safe online behavior and using technology where it can help. Microsoft recommends all users to follow the steps below to stay safe online:

- Use an Internet firewall. A firewall functions like a moat around a castle: It keeps your sensitive information in your computer safe from the outside world.
- Keep your Windows computer protected and up-to-date against potential threats; have Microsoft do this automatically for you each month through the Automatic Updates feature.
- Use an anti-virus product and don't let it

expire. Two-thirds of people don't have up-to-date protection, which leaves them vulnerable to the bad guys. Finally, use anti-spyware software so unknown people cannot lurk on your computer and potentially steal your information. Microsoft offers its anti-spyware protection, Windows Defender, free of charge.

Has Microsoft considered a weekly patch cycle in order to reduce the attack exposure of its customers? For a long time, that was exactly our policy. Up until 2003, security updates either came out the moment they were ready, or once a week on Wednesdays. Feedback from customers made it clear that the system did not represent the best method for combining the delivery of software updates with customers ability to roll them out efficiently. It is specifically the job of the Microsoft Security Response Center to deliver improved satisfaction for customers around security updates and incidents and based on that feedback from customers we moved to a monthly release cycle. However, we are always looking at ways we can improve our communications to help customers get timely and useful information to help them manage vulnerabilities and protect themselves against ongoing threats. We will continue to look for ways to improve our processes and offerings to ensure we are communicating with customers with authoritative and clear information as quickly as we can.

Can you provide our readers with a short description, in concert with an explanation of how the security features introduced into Vista and IE 7 have been adapted to enhance their protection and adapt to the threats of 2007? I would like you to address UAC, IE 7 Protect Mode and PatchGuard. Well, there is a lot of stuff there, almost too much to answer briefly. A short version would be that Windows Vista contains numerous security features that, working together, can help prevent malware from installing on a user's PC, and help find and remove malware if it has already been installed. It's important to note that with Windows Vista, we're taking a defense-in-depth approach to helping protect users from malware, which includes features such as User Account Control, Windows Service Hardening, ASLR and Kernel Patch Protection (aka PatchGuard). Additional technologies such as IE protected mode provide a safer browsing experience, and Windows Defender helps protect against spyware that might later try to download spyware, such as a rootkit, to a user's machine. In addition, the Malicious Software Removal Tool will run monthly on machines that have opted in to Automatic Updates and will remove prevalent malware such as rootkits, providing multiple layers of protection against this type of malware in Windows Vista.

Specific to the technologies you asked me to break out: User Account Control (UAC) makes it much easier and much more convenient for a user to run under a restricted user account. In previous versions of Windows, everyone was running as administrator, which of course could allow a malicious piece of software installed through social engineering to take any action it wanted to on the system. UAC is designed to help move the industry down to running with lower privileges on the operating system, and through elevation prompts, elevate only as needed and then drop back down. Internet Explorer 7 Protected Mode is a new way of running IE with restricted privileges also, so that software installed or viewed through the browser by default doesn't have the administrator rights it used to have. This again, it makes it more difficult for malware to impact the entire system. Kernel Patch Protection allows us to provide increased reliability, consistent performance, and additional levels of security for 64-bit Windows by preventing unauthorized software from modifying or patching the Windows kernel using unsupported methods while it's running. Kernel Patch Protection works by providing extensibility that allows potential extensions to be planned for, reviewed and tested thoroughly during product development. Instead of allowing multiple parties to directly modify kernel instructions and data structures in undocumented and unsupported ways, providing supported mechanisms and APIs will strengthen the security, performance and reliability of Windows Vista.

What role has the Security Development Lifecycle played in bulletproofing Vista? I think I might have answered this pretty thoroughly above, but Windows Vista is the first client-based operating system to go through the complete SDL from start to finish. Although no operating system is 100% secure, Windows Vista includes fundamental architectural changes that will help make

customers more secure from evolving threats, including worms, viruses, and malware. These improvements minimize the operating system's attack surface area, which in turn improves system and application integrity and helps people more securely manage and isolate networks.

Symantec is considering taking control over the UAC. Will Microsoft permit that? In fact will Microsoft permit any independent security provider to interfere with the functionality of any of the built-in security features in Vista, except disabling Windows Defender? We cannot speculate about what Symantec's technology may or may not do, but we look forward to hearing more from them about the solutions they are building on top of Windows Vista to help provide greater protection for customers. Based on customer feedback, we believe UAC is a good solution to get users to easily run with a more restricted user account than in the past. Standard user restrictions will help limit the impact of malware attacks, installation of unauthorized software, and unapproved system changes by making it easier to use Windows without administrator privileges. But, if the user decides they do not want to run UAC and they would rather run a third party solution that provides similar functionality, they do have the choice to disable it. Microsoft views security partners as critical to our effort to protecting customers as we can't do this alone. In following the feedback from our customers that Windows Vista should dramatically increase the security of the computing experience, we recognized that existing security solution providers were a key resource in helping to ensure not only that Windows Vista is the most secure Windows version to date, but to help maintain the user choice in selecting security solutions that best meet their needs. In fact, the development of Windows Vista has offered an unprecedented level of access and input from security vendors. Through our Secure IT Alliance and events such as the Microsoft Security and Safety Summits, we have worked closely with our security industry partners throughout the development of Windows Vista and have incorporated their feedback throughout the design of the product. We have been engaged with the industry and will continue to work with the industry through Windows Vista launch and beyond.

Microsoft recently published a list of approximately a dozen security providers that will deliver security solutions for Vista before the operating system's customer availability. Will support be equally available for 32-bit and 64-bit versions of Vista? In fact, what is the status of Microsoft's collaboration with third-party developers in relation to the APIs for x64 Vista? We're very pleased with the global security partner support we have received on Windows Vista as partners are critical to the success of our platform and the security of our customers. To date, Symantec, TrendMicro, McAfee, Sophos, CA, ContentWatch, GRISOFT, IMSafer, Kaspersky Lab and Panda Software International, PixAlert and SafeBrowse.com have all announced their intent to release security solutions for the Windows Vista platform. I have not reviewed every solution to determine the 32bit vs 64bit coverage, but I can say that a variety of vendors are indeed providing solutions for both. Regarding our collaboration with security vendors, in December we delivered the first set of draft Windows Vista APIs. Designed to help security vendors extend certain functionality in the Windows kernel on 64-bit systems, the draft APIs will not disable or weaken the protection offered by Kernel patch Protection (KPP). Additionally, we wanted everyone who develops software on the Windows platform to understand our criteria for providing the API's, and we shared a framework for which we use to help evaluate the types of APIs that will be developed and when they will be delivered. So far, the feedback from the ISV engineers we've been working with is good! It is clear that everyone recognizes the need to get ahead of security threats by making the operating system more secure and by providing defense-in-depth for customers. While significant progress has been made, this is an ongoing process, and we're going to continue working with ISVs to build trust in computing and provide a secure kernel environment.

When will Microsoft patch the vulnerability related to the Client Server Run-Time Subsystem? (this question initially had a different form but was adapted to better integrate in the context) The MSRC is currently investigating this vulnerability. Upon completion of this investigation, Microsoft will take the appropriate action to protect our customers, which may

include issuing a security advisory or providing a security update through our monthly release process, depending on customer needs. **Parental controls have become an indispensable security feature. What has Microsoft done in this aspect?** It's interesting to me watching my friends' children use the Internet. It really is a playground to them, perfect for exploration, learning and fun. As they get older, it's also where kids form social networks - sending e-mail and instant messages, posting blogs, creating personal Web pages, finding music and playing games. While these activities have many benefits, as we adults have found out, they may also be the source of serious issues involving personal safety, privacy, theft and computer security. There is now a significant amount of parents working for Microsoft, and it's been clear to us for some time that there were great things we could do in the products to make childrens' Internet experience safer. After extensive communication with parents, who told Microsoft that in addition to education and guidance, they want technology that can help make their children's online experiences more secure, we created the following: Windows Vista. We've built a parental control platform into Windows Vista, so parents can feel confident that their children are safe when they are working with their PCs. All your applications can plug into this platform, including instant messaging, browsing and gaming. Parents will be able to monitor and restrict when and for how long children can log on, which Web sites they browse on Windows Internet Explorer 7, and what applications they can run. Windows Live OneCare Family Safety. Formerly known as Window Live Family Safety Settings, Windows Live OneCare Family Safety is a free Web-based service that will aid parents in providing a safer experience for their children online by helping block inappropriate content and facilitating safer online communication. Windows Live OneCare Family Safety will offer customizable content filters that will block inappropriate content, a kids request line, reporting features and a contact list management tool, all of which allow parents to set standards for the types of sites that kids and family members can visit. Most important, Windows Live OneCare Family Safety is user-based, not PC-based, so the settings applied to each family member's account will remain intact anytime they log onto a PC equipped with Windows Live OneCare Family Safety software. The service will launch through a phased rollout beginning in 2006.

Is there something more that Microsoft wishes it could have done to increase the security of Windows Vista? There's always more we can do. Security will never be a destination, instead it's a journey. We remain confident that Windows Vista is the most secure version of Windows to date, however it's important to note that no software is 100% secure. Our goal is to give PC users the control and confidence they need so they can continue to get the most out of their PCs and have a safer and more secure computing experience.

Will Vista SP1 introduce anything new, security wise? When should users expect the first service pack for Vista? Thanks to comprehensive pre-release testing and the immediacy of services like Windows Update, service packs are becoming less relevant as a milestone of a product's maturity. It is too early to provide any firm date range for delivery, but we expect Windows Vista SP1 to be a standard service pack that will include security updates and hot fixes, as well as other limited changes focused on improving overall quality.

Where should consumers go to in order to access information about potential threats and about the products that will offer them the right protection? Microsoft offers free guidance and technology to help protect your PC at <http://www.microsoft.com/protect>.

Earlier this year, you said that "developers will never find all code-level security bugs, so you need other defenses." How true is this for Windows Vista? I've listed some of our defense in depth features in the previous questions, but I want to point out that that statement is true for all software, because no software is 100% secure. Additionally, on the user-level, even with the significant technological advances in an operating system like Windows Vista, techniques like social engineering rely on tricking or manipulating users to perform an action, something that technology alone cannot stop. Defenses such as general awareness of the threats that exist online are often invaluable in the prevention of social engineering attacks. While Microsoft has made several

improvements with Windows Vista to provide greater defense-in-depth protections, we continue to recommend four essential steps to help protect against malicious attacks including enabling a firewall, turning on Automatic Updates, and using anti-virus and anti-spyware software. If users choose, with the exception of anti-virus software, Windows Vista takes care of three of the four "Protect Your PC steps" for them. Microsoft does recommend that users install an anti-virus solution as well, whether a Microsoft or third-party solution.

Windows Vista's launch coincides with the Storm Trojan Outbreak. Do users have anything to worry about? It has been reported that this Storm Trojan outbreak was a large-scale attack launched via email spam that could have impacted users. We will continue to monitor the situation to ensure we can help protect our customers. To help mitigate such issues, Microsoft provides guidance on how customers can protect themselves from malicious attacks that take advantage of user interaction at <http://www.microsoft.com/protect>. For instance: As a best practice, users should always exercise extreme caution when opening unsolicited emails and/or attachments, or clicking on URLs from both known and unknown sources, to help protect themselves from attacks that require user action to execute. Follow all of the steps of the "Protect Your PC" guidance of enabling a firewall, applying all software updates and installing anti-virus and anti-spyware software. Customers who believe they have been attacked should contact their local FBI office or report their situation on www.ifccfbi.gov. If outside the U.S., people should contact the national law enforcement agency in their country for assistance. Customers who believe they are affected can contact Product Support Services. Contact Product Support Services in North America for help with security update issues or viruses at no charge using the PC Safety line (1866-PCSAFETY) and international customers by using any method found at this location: <http://support.microsoft.com/security>.

Can you give our readers additional information related to the Windows MessageBox Vulnerability? In this context, are there areas of the Vista's security that you feel might still need some work? Is there something else that you wished you could have integrated in Vista, security-wise? The MSRC is currently investigating this vulnerability. Upon completion of this investigation, we will take the appropriate action to protect our customers, which may include issuing a security advisory or providing a security update through our monthly release process, depending on customer needs. As I have mentioned before, no software is 100% secure. Security issues will exist even with more secure operating systems because the threat bar will continue to be raised. Hackers continually become more aggressive and that is why Microsoft has made Windows Vista more resilient across multiple layers and applied defense-in-depth measures to help protect users from vulnerabilities.

Is this an isolated case or has Microsoft identified and resolved other vulnerabilities in the operating system since November 30, 2006? As of February 19th, this is the only publicly confirmed vulnerability in Windows Vista, however it's important to remember that no operating system is 100% secure. Microsoft is committed to keeping the number of security vulnerabilities that ship in its products to a minimum as evidenced by the security improvements in Windows Server 2003, our focus on providing greater defense in depth and the ongoing work across the company - all of which help to deliver on Microsoft's vision of Trustworthy Computing. Microsoft requires internal use of the Security Development Lifecycle (SDL) for any product commonly used or deployed within an enterprise, any product that regularly stores, processes, or communicates financial or other sensitive customer information, and any product that regularly touches or listens on the Internet.

Does the fact that a few days before the Vista consumer launch, Microsoft has extended support for Windows XP Home Edition and Media Center Edition until 2014, give users the impression that XP is secure enough to continue to be used? Windows XP Service Pack 2 was a significant leap in the security of the Windows XP platform. However, it is important to note that the Windows XP base product was developed in a much earlier time in the threat landscape, and did not go through new advances like the SDL. Furthermore, it lacks many of the

architectural features that make Windows Vista a far more secure operating system. Customers can be confident undertaking broad deployment and use of Windows Vista today, and we encourage our customers to install Windows Vista now that it is available.

Would you say that the true measure of Vista's security will be defined by the sum of deployment practices and code quality? I'm very proud of Windows Vista and I believe that the true measure of Windows Vista's security success is already being attained. We have successfully released a product that is far more secure than any other operating system that we have ever released. Security researchers and security companies have had an unprecedented level of access and review of the code. I'm excited that it's out there now and people can put it to the test.

What are the risks associated with using pirated copies of Windows Vista? Consumers are at risk when they purchase (or download) software expecting it to be genuine. This can result in users subjecting themselves to potential identity theft, malware and other security threats that could be embedded in the software. Studies indicate that pirated software can install unwanted or malicious code, and some install Windows but leave the system vulnerable to take over of administrative rights so that it can be controlled or watched remotely. IDC research, commissioned by Microsoft, shows that users running counterfeit software have a 17% chance of getting a virus or Trojan that can slip through current anti-virus software. 25% of Websites that offer Windows at prices "too good to be true" attempt to install unwanted software such as viruses, spyware or Trojan Horses, many of which are too sophisticated for current anti-virus software.