



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

SIG² G-TEC Survey Research Paper

SIG² Survey on Microsoft Windows XP on Service Pack 2 Usage & Experiences

Principal Investigator: Cecil SU (csu@security.org.sg)

Author: Cecil SU (csu@security.org.sg)

30 September 2004

Introduction

Making the enterprise more secure and robust by managing the OS upgrade deployment is a major issue and concern for cross industries in Singapore. Microsoft has taken the wraps off of Service Pack 2 (SP2) for Windows XP [1]. On first thought, one might think that this is another general "bug-squasher" from the release. Things are different this time. The company claims that the free service pack adds proactive protection features that will help safeguard computers from hackers, worms and other security risks. Microsoft will localize the software in 25 languages by Q4 2004 and will distribute it to computer manufacturers, enterprise customers and consumers through downloads, retail installation, free CDs and on new PCs.

The arrival of SP2 gives enterprises large and small, running Windows 2000 added incentive to adopt Windows XP on new PCs, rather than waiting for Microsoft's Longhorn (next scheduled release) expected by 2006 [2].

SP2 includes a number of badly needed fixes [3] to the Internet Explorer browser that is built into Windows, including enhancements to help prevent pop-up advertisements and "phishing" attacks. Microsoft has also updated the simple firewall that was built into XP (now turned on by default) and is adding technology known as Data Execution Prevention (DEP) to prevent worms from spreading through buffer overruns, when run on PCs with NX-capable processors.

This survey aims to share the usage and experiences from some of the industries in Singapore that have started to at least experiment with the SP2. With this in mind, the survey was sent out to several correspondents in different vertical industries across Singapore to get a sampling of the experiences encountered so far.

The survey was conducted across eight different industries: financial securities, hospitality, retail, ASP, system integrator, consumer products, banking and education. The number of Windows clients deployed or to be deployed from the respondents were from 30 to approximately 40000 machines. The survey involved interviews with at least one senior executive or the IT security consultant in each organization

"IT Security...the Gathering. By enthusiasts for enthusiasts"



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

together with the input from the various divisions like the helpdesk and MIS operations within the organization who were involved with the testing, planning and deployment stages. The appendixes are representative samples of the replies we get from different segment of the industry

Observations

90 percent of the respondents view the SP2 update as providing safer browsing, enhanced security tools and improved user experience [4]. However, 10 percent have adopted to wait and see the reaction from the community of users before embarking on the update for the entire organization altogether. The general consensus here was that all in-house applications written on the Windows XP platform as well as third-party programs that are to be migrated to the SP2 should be given ample testing periods to ensure that they operate correctly.

Of those surveyed, 70 percent of the respondents were able to install third-party products directly out-of-the-box without any tweaking or manual adjustments. Some of these products include IBM Lotus Notes, MS Office for XP and Microsoft Visio.

Broken applications were among the most common issues reported with SP2 - something Microsoft has been warning users for several months - often an effect of changes in Windows XP's security settings. Some of the Cisco VPN clients were reported to have issues with SP2. Users also discovered conflicts with a number of other applications. For example, one of the in-house applications written by one of the securities company was slowed down by an SP2 feature that limits the number of simultaneous TCP connections a program can make to different IP addresses; something that would have blocked worms such as Sasser from spreading. Currently, the only fix appears to be a complicated workaround to change Windows' TCP/IP parameters. On the other hand, Symantec's AntiVirus Corporate Edition 8.0 requires certain ports to be opened on SP2 before it can work. Some of the other quirks include false alarms being triggered during normal Windows ftp command sessions [5].

Other applications that users reported problems with included remote debugging in Visual Studio.NET 2003, SQL Server 2000, Microsoft Access 2003, Novell BorderManager, Style XP, the Table PC's OneNote application, the Skype IP telephony program, Microsoft Baseline Security Analyzer 1.2 and the ATI graphics control panel.

Statistics

Of the organizations surveyed that have already started to roll-out SP2 (totalling 70 percent), only 10 percent indicated that there were no problems with the updates. Out of these, 60 percent indicated that they have had minor issues with the updates. The rest of the 30 percent of the respondents claimed that they had major issues with the updates.

"IT Security...the Gathering. By enthusiasts for enthusiasts"



On these major issues encountered by the respondents, 80 percent reported that the major issues dealt mostly with the in-house applications which were not tested at all with SP2.

The remaining total 30 percent of the respondents were still either in their trialing, UAT or testing phases, and were not ready for deployment as yet.

Advice

While Microsoft is characterizing SP2 as a "critical" upgrade and encouraging all XP users to upgrade to it as soon as possible, many IT managers in Singapore are holding off from pushing SP2 to users' desktops until they are able to thoroughly test its effect on custom and third-party applications.

For home users, Microsoft has provided enough reasons that they should install SP2 [6]. There are a few informative links that home users should also probably take note prior to updating their systems to verify for incompatibilities [7].

Most respondents have advised that organizations planning to deploy SP2 should evaluate SP2 as quickly as possible. Find those incompatibilities, and then figure out a workaround that makes the existing solution work. But realize that security is the priority. Do the right thing going forward, and the system will pay back by keeping the precious data safe the next time a Slammer-type attack occurs. Windows XP SP2 will make the system more secure, if the users let it. But if they ignore or put off this release, they will only be hurting themselves in the long run.

An interesting point to note is that, despite the public availability of SP2, Microsoft has also recently published a toolkit allowing IT managers to temporarily block SP2 from installing before they are ready for it [8].

Background & Planning

Of those surveyed, a total of 80 percent responded that they will start deploying SP2 in Q4 2004. The remaining 20 percent has either opted for Q1 or Q2 2005. The testing period for SP2 seemed to be the only agreeable timeline for all respondents, which is more than one month. The duration of the testing period lasts anywhere between one to 3 months.

Organizations that have tested SP2 during the testing phase can consider deploying the upgrade it in four to six weeks, if their applications have proved compatible and no major issues were reported. The deployment duration from the respondents for the entire SP2 exercise is anywhere between 5 days to 2 months, with the longer period happening in phases throughout the organization.



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

Mainstream enterprises should plan to wait at least two months after SP2 ships before beginning deployment, and should favor testing on PCs with NX-enabled processors that support the DEP function (available now from Advanced Micro Devices and in Q4 2004 from Intel). Testing on NX-enabled machines will ensure that running in physical address extension (PAE) memory mode does not break any applications or drivers. Organizations that test on non-NX PCs will have to repeat testing on NX PCs.

Large organizations should also consider host-based intrusion prevention products — such as Cisco Security Agent, Network Associates Enterscept, Sana Security, Determina, Platform Logic and Immunix. These enterprises will still need third-party personal firewalls for all laptops. Many consumers and some small businesses will find the Windows XP firewall included in SP2 sufficient.

Most users, however, have said that they had a positive experience overall with the update, with particular favorites being the popup blocker in Internet Explorer, the Security Center and improved integration of wireless technologies such as Wi-fi and Bluetooth.



Appendix A – Survey Contributor

Industry : Systems Integration

Observations

Nos.	Question	Response / Comments
1	How does you the ITSEC professional or your company/industry view this update?	The update looks like Microsoft has thought about security. It does seem to have lots of user-enhancement features for people on-the-go (WiFi and Bluetooth).
2	What are those software that you tried which worked out of the box with the update?	Some of our in-house biometric applications. Most of the Microsoft Office suite and Microsoft Visio applications worked fine.
3	What are those software that you tried but need some minor tweaking to work? Describe them if possible.	A couple of in-house products would need to be re-packaged (re-worked).

Statistics

Nos.	Question	Response / Comments
1	What is the percentage of updates without problems?	15 % that came straight out of the box
2	What is the percentage of updates with minor issues?	55% of third party related software
3	What is the percentage of updates with major issues?	30% of vendor-related and a few non-critical in-house products

Advice

Nos.	Question	Response / Comments
1	What advice would you give to corporate users regarding this update?	As a home user, if you can wait, then wait for a stabler release of SP2. Not unless you would need the functionalities in SP2 then would it be worth updating.
2	What advice would you provide to corporate users regarding this	This update should be deployed only after careful consideration, planning and testing by



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

	update?	the IT or MIS groups. Preferably this should be updated via SUS.
--	---------	--

Background & Planning

Nos.	Question	Response / Comments
1	What is your industry?	System Integrator
2	What is the size of your WindowsXP installation?	Approximately 1000 clients
3	What is the deployment deadline you have for this update?	Q4 2004. Started in Q2 2004.
4	What is the testing period you have given / are giving to SP2?	3 months for in-house applications 1 month for third-party products
5	What is the deployment duration?	6 months in total (1 week per department)



Appendix B – Survey Contributor

Industry : Securities (Finance)

Observations

Nos.	Question	Response / Comments
1	How does you the ITSEC professional or your company/industry view this update?	Feature-packed in terms of security and hardware-based (blueetooth and wi-fi). Possibly this is one update to install (if concerned about security for home users) but corporate users should take note of broken applications.
2	What are those software that you tried which worked out of the box with the update?	MS-Excel, MS-Word from the Windows Office XP worked perfectly fine.
3	What are those software that you tried but need some minor tweaking to work? Describe them if possible.	System became 3 times slower after VMWare 4.5.2 was installed with SP2. Results inconclusive if this was because of VMWare of SP2. Skype IP telephony application has intermittent issues. MSBA 1.2 hangs after scanning.

Statistics

Nos.	Question	Response / Comments
1	What is the percentage of updates without problems?	Still testing. So far estimated 15% – 20%.
2	What is the percentage of updates with minor issues?	Still testing. Approximately 65% - 70%.
3	What is the percentage of updates with major issues?	Still testing. Possibly around 10% - 15%.

Advice

Nos.	Question	Response / Comments
1	What advice would you give to home users regarding this update?	The built-in firewall tool should be sufficient for most home users. It would need a higher capacity machine and memory.



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

2	What advice would you provide to corporate users regarding this update?	Engage third-party firewall tools. Apparently the MS-Windows firewall had some minor issues.
---	---	--

Background & Planning

Nos.	Question	Response / Comments
1	What is your industry?	Securities (finance)
2	What is the size of your WindowsXP installation?	100 windows clients
3	What is the deployment deadline you have for this update?	Not yet. To begin testing / UAT in Q3 2004.
4	What is the testing period you have given / are giving to SP2?	Two weeks to a month.
5	What is the deployment duration?	One week.



Appendix C – Survey Contributor

Industry : Finance

Observations

Nos.	Question	Response / Comments
1	How does you the ITSEC professional or your company/industry view this update?	Necessary
2	What are those software that you tried which worked out of the box with the update?	Most 3 rd party applications
3	What are those software that you tried but need some minor tweaking to work? Describe them if possible.	Some custom applications which use older DLLs.

Statistics

Nos.	Question	Response / Comments
1	What is the percentage of updates without problems?	95%
2	What is the percentage of updates with minor issues?	4%
3	What is the percentage of updates with major issues?	1%

Advice

Nos.	Question	Response / Comments
1	What advice would you give to home users regarding this update?	Must have but some apps may not work initially.
2	What advice would you provide to corporate users regarding this update?	Same as above.



Special Interest Group in
Security and Information Integrity
(SIG^2)
<http://www.security.org.sg>

--	--	--

Background & Planning

Nos.	Question	Response / Comments
1	What is your industry?	Finance
2	What is the size of your WindowsXP installation?	100-150
3	What is the deployment deadline you have for this update?	All updated
4	What is the testing period you have given / are giving to SP2?	1 week
5	What is the deployment duration?	1 week



Appendix D – Survey Contributor

Industry : Hospitality & Retail

Observations

Nos.	Question	Response / Comments
1	How does you the ITSEC professional or your company/industry view this update?	It is a security-enhanced update on the OS level and some hardware-based update (NX-enabled) and WiFi / Bluetooth. The pop-up blocker is a great innovation by itself.
2	What are those software that you tried which worked out of the box with the update?	At this stage still trying other software used in previous MS-Windows (ie., 200) versions. Those tried with confidence include MS-Office XP suite.
3	What are those software that you tried but need some minor tweaking to work? Describe them if possible.	Novell BorderManager, ATI graphics control panel

Statistics

Nos.	Question	Response / Comments
1	What is the percentage of updates without problems?	10 % approx.
2	What is the percentage of updates with minor issues?	50 % – 60 % approx.
3	What is the percentage of updates with major issues?	40% - 50% approx. Most of these would possibly be from in-house apps that may need re-work on the security modules to be compatible with MSWinXP SP2.

Advice

Nos.	Question	Response / Comments
1	What advice would you give to home users regarding this update?	Wait for at least 2 months before trying out on your home machine. Backup all pertinent / crucial data before running update.
2	What advice would you provide to corporate users regarding this	Mandatory tests for all in-house applications until no major modules break.



Special Interest Group in
Security and Information Integrity
(SIG^2)
<http://www.security.org.sg>

	update?	
--	---------	--

Background & Planning

Nos.	Question	Response / Comments
1	What is your industry?	Hospitality & Retail
2	What is the size of your WindowsXP installation?	30 machines
3	What is the deployment deadline you have for this update?	Q4 2004
4	What is the testing period you have given / are giving to SP2?	More than 1 month.
5	What is the deployment duration?	Next 6-9 months on SP2.



Appendix E – Survey Contributor

Industry : Media & Publishing

Observations

Nos.	Question	Response / Comments
1	How does you the ITSEC professional or your company/industry view this update?	Adopt a "wait & see" attitude as the reviews for SP2 has not been promising
2	What are those software that you tried which worked out of the box with the update?	Symantec Anti-Virus, MS Office
3	What are those software that you tried but need some minor tweaking to work? Describe them if possible.	Not conclusive but there might be problems with some of our in-house programs.

Statistics

Nos.	Question	Response / Comments
1	What is the percentage of updates without problems?	50% (estimated)
2	What is the percentage of updates with minor issues?	30% (estimated)
3	What is the percentage of updates with major issues?	20% (estimated)

Advice

Nos.	Question	Response / Comments
1	What advice would you give to home users regarding this update?	To backup their data prior to the update in case there's a need to re-format the harddisk
2	What advice would you provide to corporate users regarding this update?	To wait for the completion and sign-off of tests on all in-house applications before deploying across the departments.



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

Background & Planning

Nos.	Question	Response / Comments
1	What is your industry?	Media / Publishing
2	What is the size of your WindowsXP installation?	3000 clients
3	What is the deployment deadline you have for this update?	End 2004
4	What is the testing period you have given / are giving to SP2?	3 months
5	What is the deployment duration?	2 months



Appendix F – Survey Contributor

Industry : Financial Services

Observations

Nos.	Question	Response / Comments
1	How does you the ITSEC professional or your company/industry view this update?	It is a great update but It will take time for Corporate to test SP2 with in-house software and produce patches/fixes.
2	What are those software that you tried which worked out of the box with the update?	IBM Lotus Notes 6i, MS Office for XP
3	What are those software that you tried but need some minor tweaking to work? Describe them if possible.	As there are some known problems with SP2, possibly some form of code re-work or recompilation needed for some of the in-house products.

Statistics

Nos.	Question	Response / Comments
1	What is the percentage of updates without problems?	1%
2	What is the percentage of updates with minor issues?	0%, not a good indication as XP2 is only applied on users that do not run in-house applications.
3	What is the percentage of updates with major issues?	0%, , not a good indication as XP2 is only applied on users that do not run in-house application

Advice

Nos.	Question	Response / Comments
1	What advice would you give to home users regarding this update?	Home users should backup critical data files and only upgrade to SP2 if really necessary. The main positive advantages of SP2 would be the default firewall app and pop-up blockers
2	What advice would you provide to	Written guidelines in the upgrade/update policies.



	corporate users regarding this update?	Besides that, all updates will be implemented through SUS to manage required updates that will be pushed out to the users. A full-backup on essential applications/data and fully test XP SP2 with in-house applications/products before updating
--	--	---

Background & Planning

Nos.	Question	Response / Comments
1	What is your industry?	Financial Services (Software and Services) provider
2	What is the size of your WindowsXP installation?	120 clients regionwide (Asia Pacific excluding South Asia)
3	What is the deployment deadline you have for this update?	Q4 2004
4	What is the testing period you have given / are giving to SP2?	3 months
5	What is the deployment duration?	1 week



Appendix G – Survey Contributor

Industry : Consumer Products / Retail

Observations

Nos.	Question	Response / Comments
1	How does you the ITSEC professional or your company/industry view this update?	Microsoft has this time put lots of effort into security. It looks like a great update which may be the way to go for all releases of Microsoft. But as most may have noted, there are still some issues to be worked out in terms of compatibility of software across the board.
2	What are those software that you tried which worked out of the box with the update?	Most major mail, monitoring and office (spreadsheets, word-processing) software worked out of the box.
3	What are those software that you tried but need some minor tweaking to work? Describe them if possible.	Some in-house client and thin-client applications needed code re-work and re-compilation before re-deployment. A third-party corporate Antivirus program needed to open a certain port before it could work.

Statistics

Nos.	Question	Response / Comments
1	What is the percentage of updates without problems?	We can safely put 30 % to 40 % of third-party solutions.
2	What is the percentage of updates with minor issues?	About 30% to 40% of third-party solutions needed tweaking.
3	What is the percentage of updates with major issues?	Roughly 30% of our in-house applications on client-based environments needed code re-work on the access control modules.

Advice

Nos.	Question	Response / Comments
1	What advice would you give to home users regarding this update?	Be absolutely certain that you need all these enhanced security features and hardware gizmos like WiFi and Bluetooth. Most home



		users would probably need to upgrade their existing systems (as some older systems may not be able to enjoy the “improved user experience” without a much powerful box.
2	What advice would you provide to corporate users regarding this update?	Follow the heed of the IT Security department and deploy via SUS or pre-packaged deployment tools pushed down from the MIX/IT departments. Wait for the upgrade period, do not just jump ship.

Background & Planning

Nos.	Question	Response / Comments
1	What is your industry?	Consumer products.
2	What is the size of your WindowsXP installation?	5000 WinXP clients in SEA.
3	What is the deployment deadline you have for this update?	Already started. Deadline Regional deployment probably in H4 2004.
4	What is the testing period you have given / are giving to SP2?	Two months approximately.
5	What is the deployment duration?	In phases by divisions/departments.



Appendix H – Survey Contributor

Industry : Education (University)

Observations

Nos.	Question	Response / Comments
1	How does you the ITSEC professional or your company/industry view this update?	<p>Microsoft has released an update for Windows XP. This update provides safer browsing, better security tools and improved experience. This update known as the Windows XP Service Pack 2 (SP2) has been made available to the public.</p> <p>My company has been testing this Service Pack to ensure that our systems and applications run properly in SP2 environment. There are a few applications that has been identified that will not work properly with SP2. We are currently researching into this and are working with the vendors to address the issues.</p> <p>Windows XP SP2 is designed to enhance the Windows environment. It does not address any immediate vulnerability issue with Windows XP. As such, please refrain from downloading and installing it on your system. Doing so may render your system unusable.</p> <p>Our advice to users is not to download it for the time being. When it's ready, we will release it via our internal Automatic Update via SUS.</p>
2	What are those software that you tried which worked out of the box with the update?	Most of the software works out of the box.
3	What are those software that you tried but need some minor tweaking to work? Describe them if possible.	<p>Some CISCO VPN clients have issues with SP2. The solution is still being worked out with the vendor.</p> <p>False alarms are flagged with Windows FTP command sessions.</p>

Statistics

Nos.	Question	Response / Comments
1	What is the percentage of updates without problems?	It is not being rolled out yet.
2	What is the percentage of updates with minor issues?	It is not being rolled out yet.
3	What is the percentage of updates	It is not being rolled out yet.



	with major issues?	
--	--------------------	--

Advice

Nos.	Question	Response / Comments
1	What advice would you give to home users regarding this update?	<p>You can confirm whether you have SP2 installed via the Computer's Properties (i.e. click on file:\\c:\windows\system32\sysdm.cpl). It should indicate your current Service Pack level. Alternatively, you can check for the presence of alg.exe running on your system. It is the Application Layer Gateway provided by the windows firewall.</p> <p>Home users should install SP2 for the following reasons: http://www.microsoft.com/windowsxp/sp2/topten.msp</p> <p>There are a few informative links that home users should probably take note of in checking for incompatibilities or resolving incompatibilities:</p> <p>Authoritative reference: http://support.microsoft.com/default.aspx?scid=kb;en-us;884130</p> <p>Other references: http://isc.sans.org/xpsp2.php http://isc.sans.org/xpsp2summary.php</p>
2	What advice would you provide to corporate users regarding this update?	<p>For corporate networks, my advice is for SP2 to be properly tested with all used applications including third-party applications, customized applications and in-house applications. Corporate networks should rely on an automatic update mechanism such as Microsoft SUS for update via a corporate server so that there is a workflow mechanism for verification and approval of any updates or hotfixes before they are being rolled out corporation-wide. Because windows firewall blocks most incoming traffic by default, services that require opening services to receive such traffic would require customization of the windows firewall. In a corporate environment with a rather homogeneous network, such customizations are best rolled out via group policies.</p> <p>There are a few informative links that corporate users should probably take note of in checking for incompatibilities or resolving incompatibilities:</p> <p>Authoritative reference: http://support.microsoft.com/default.aspx?scid=kb;en-us;884130</p> <p>Other references: http://isc.sans.org/xpsp2.php http://isc.sans.org/xpsp2summary.php</p>



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

Background & Planning

Nos.	Question	Response / Comments
1	What is your industry?	Education
2	What is the size of your WindowsXP installation?	Approximately 40000
3	What is the deployment deadline you have for this update?	By end of Sep 2004
4	What is the testing period you have given / are giving to SP2?	Approximately 1 month
5	What is the deployment duration?	5 days



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

References

-
- [1] Windows XP SP 2 Official List of Features :
<http://www.microsoft.com/windowsxp/sp2/features.msp>
- [2] Windows XP Service Pack 2 Resources for IT Professionals :
<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.msp>
- [3] List of Security Updates included in Microsoft Windows XP Service Pack 2 (SP2)
<http://www.microsoft.com/technet/security/news/xpsp2.msp>
- [4] Deploying Windows XP - application compatibility :
<http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/depxpapp.msp>
- [5] Chew Keong's WinXP SP2 Firewall's FTP connection tracking :
<http://www.security.org.sg/gtec/honeynet/viewdiary.php?diary=20040913>
- [6] Top 10 Reasons to Install Windows XP Service Pack 2 (SP2) :
<http://www.microsoft.com/windowsxp/sp2/topten.msp>
- [7] Windows XP Service Pack 2 - Summary
<http://isc.sans.org/xpsp2summary.php>
- [8] Temporarily Disabling Delivery of Windows XP Service Pack 2 Through
Windows Update and Automatic Updates
<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2aumng.msp>

REVIEWED BY

Tan Chew Keong, Director G-TEC,
Vice-President, SIG²
chewkeong@security.org.sg

APPROVED FOR DISEMINATION BY

Aloysius Cheang, CISA, CISSP, GCIH
President, SIG²
aloysius@security.org.sg