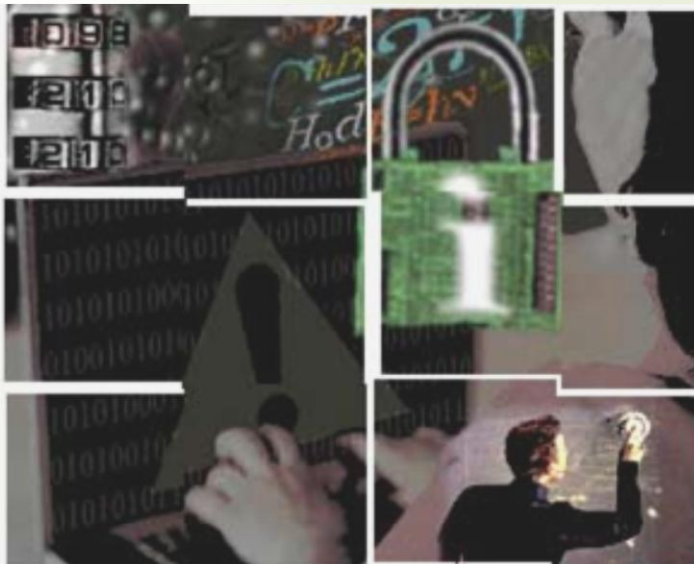


January 2010

# E-Newsletter



Association of  
Information Security Professionals



## Contents

- President's Message
- The "Revolution" in Rootkit Technologies
- The 2010 Job Outlook for IS Security Professionals
- Student Chapter's Corner
- Calendar of Events

Association of Information Security Professionals  
Tel: 6226 2567 ext. 18  
Fax: 6226 2569  
Email: [secretariat@aisp.sg](mailto:secretariat@aisp.sg)  
53/53A Neil Road  
Singapore 088891

I hope all of you have enjoyed a well deserved break and are raring to go to face the challenges in new year. The improving economic outlook augurs well for AISP as we move into our third year of existence. We will be stepping up our programmes for members and embarking on new initiatives to create greater value and branding for our members, and a more sustainable future for the Association.



To kick off the year, we have launched another Student Chapter with a signing ceremony on 22 January 2010 with the Institute of Systems Science ('ISS'). ISS is the sixth Institute of Higher Learning to form AISP Student Chapters. The others are Nanyang Polytechnic, National University of Singapore, Singapore Management University, Singapore Polytechnic, Temasek Polytechnic. In collaboration with ISS, we have rebranded our Academic Series as the AISP-ISS Technology Security Series. This rebranding reflects the partnership we have formed with ISS to enhance the popular half-day technical seminars you have been enjoying last year. With ISS, we aim to bring in more speakers with a broader range of topics to meet the needs of your professional development. Look out for announcements on the forthcoming events.

We will be launching our AISP certification examination and preparation course soon. When launched, AISP will provide the infocomm security community with a roadmap and path to obtaining Associate and Ordinary membership with us. This programme will be especially beneficial to those who would like to obtain an infocomm security qualification which takes into account Singapore's infocomm regulatory environment.

Our main event for the year would be the IDA-AISP Information Security Seminar 2010. This is our 2<sup>nd</sup> year in doing this highly successful Seminar, which has been scheduled for 22 March 2010. Look out for the information flyers coming your way.

Do join us for our 2<sup>nd</sup> AISP Annual General Meeting, to be held on 11 March 2010. Your strong support counts. Announcements of the AGM will be made nearer the date.

Last but not least, we look forward to you renewing your AISP membership and encouraging new members to join us. AISP can only succeed if it enjoys the strong support of the infocomm security professionals in Singapore. To reward you for your loyalty and support, there will be a lucky draw and you stand to win for yourself a Lenovo Ideapad worth \$699! In addition, members who renew will also be given a copy of Symantec Norton Internet Security 2010. Thanks to Symantec for sponsoring this gift!

Best wishes for 2010!

Gerard Tan  
President  
Association of Information Security Professionals

## History

In the early nineties, the first UNIX[1] rootkit begin to take the centre stage. Although they still exist till now, the evolution is not that great as compared to their Windows-based counterparts. However, it should be noted that Windows malware are direct descendents of DOS-based malware and are not UNIX predecessors.

DOS-based viruses appeared around 1990. Unlike UNIX rootkit, these DOS-based viruses simply hid themselves from the user and AV programs. This is similar in nature to the Windows Rootkit which relies on techniques such as intercepting system calls and masking malicious code by serving false data on either disk or memory content.

Greg Hoglund, a well known member of the security community including the Black Hat Society is a seasoned author on the subject of computer security and computer hacking. He was one of the pioneers that manage to build a tool that can hide data in the system by combining various techniques for evading system protection features in Windows. His result was published in the e-magazine PHRACK [2] (Issue 55).

A Windows programming guru named Jeffrey Richter, disclosed techniques for intercepting system calls in user mode in his book titled “Advanced Windows”[3] and its fourth edition titled “Programming Applications for Microsoft Windows”[4]. These techniques were widely used by malware that appeared after that.

Technique to intercept system calls at a lower level (i.e. the kernel mode) was disclosed later in two books titled “Undocumented Windows 2000 Secrets” [5] by Schreiber and “Undocumented Windows NT” [6] by P. Dabak. These were the cutting edge techniques at that time.

The table depicts the various malware tools that were released over the years.

Year	Name of tool	Remarks
2000	He4hook [7]	It is not malicious but has the ability to hide files and It works in kernel mode.
2001	NTRootkit [8]	Hacker tool, used after an attacker has gained admin access to a Windows NT/2K system.
2002	Hacker Defender [9]	It can be used to hide files, processes and registry keys with flexible settings in the configuration file. It works primarily in user mode.
2003	Vanquish [10]	It can be used to hide files, directories and registry keys. It has a malicious payload and it logs passwords. It works in user mode.
2003	Haxdoor [11]	It is a backdoor that uses rootkit techniques to conceal its presence in the system. It also works in kernel mode.
2004	FU [12]	It introduces a new technique based on modifying the system structure itself, rather than modifying access to the system. It works in kernel mode.



## The “Revolution” in Rootkit Technologies

This article describes briefly past and present rootkit technologies and discusses briefly what can possibly lie ahead for rootkit technology. This article focuses mainly on Windows-based rootkit as they are the most common and they pose a serious threat to Windows OS users. Readers are encouraged to follow the links to the technical details and read them up in depth if they are interested.

For a start, we will define the term Rootkit. Rootkit is defined as a program or application that circumvent standard system mechanisms by using stealthy techniques to hide system objects such as files, processes, drivers, services, registry keys, open ports and network connections etc.

## New Technologies

The year 2006 is an important year as an advance technique based on hardware-based virtualization is widely publicized and the claim is that such technique is not easily detectable. There were three such proof-of-concept rootkit that were publicized: SubVirt [13], BluePill [14] and Vitriol [15].

Subvirt is a proof of concept virtual machine rootkit created by Microsoft Research and the University of Michigan. It pushes the limit for hiding malware to even lower level than the operating system itself.

Blue Pill is the codename for a controversial rootkit based on x86 virtualization technology that targets Microsoft Windows Vista operating system. Blue Pill originally required AMD-V (Pacifica) virtualization support, but was later ported to support Intel VT (Vanderpool) as well. It was designed by Joanna Rutkowska and was publicized at the Black Hat Briefings in 2006.

Another virtualization-based rootkit called Vitriol developed by Dino Dai Zovi, a security specialist, was also publicized at the Black Hat Conference in 2006. The difference between Vitriol and Bluepill is that Vitriol was developed based on the Intel VT (Vanderpool).

On a separate track, there were also researchers working on the detection of virtualization-based rootkit. Notable detection mechanism was the detection of OS running under the hypervisor control via the execution timing of certain instructions such as WRMSR which causes an exit from the guest operating system to the hypervisor. The decision factor is that the timing to execute the instruction on an operating system under the control of the hypervisor is higher than one without the control of hypervisor. This was presented by Nate Lawson, Thomas Ptacek and Peter Ferrie in Black Hat 2007 [23]. There were other approaches as well. This includes observing side-effects of execution on side channels such as translation look-aside buffers (TLBs) and processor-specific behavior (using processor errata). However, one important point to note is that all the documented techniques try to detect that the system is running under a hypervisor, but do not detect that the hypervisor is malicious.

While the hype on Virtualization-based rootkit was going on, researchers were also focusing on another area. They were called the bootkit, which is a rootkit that operate in the boot sector. This group of rootkit gains total control over the system while it is booting up. This technique can be traced back to the boot viruses that were dominant in the era of the DOS operating system. The first proof of concept rootkit targeting the boot sector was eEye Bootroot [16]. Vbootkit [17], a similar proof of concept, appeared later. Following this, there was also the Stoned Bootkit [22] which is a research and scientific bootkit by Peter Kleissner. It was presented in Black Hat USA 2009. The claim make by the Stoned Bootkit is that it had the capability to attack all Windows version from Windows XP up to Windows 7 and was able to bypass the TrueCrypt's full volume encryption. The rootkit out in the wild that was based on the bootkit concept is the Sinowal or the Mebroot[18]. Most AV solutions still have trouble detecting it.

In Cansecwest Conference 2009 [19], a pair of security researchers from Core Security Technologies showcase method for infecting the BIOS with persistent code [20] that will survive reboots and reflashing attempts. Anibal Sacco and Alfredo Ortaega demonstrated a method for patching the BIOS with a small bit of code that gave them complete control of the machine. This was seen as an upgraded generation of Bootkit which is more persistent against operating system reinstallation. However, the technicality of implementing such a rootkit is significantly more complex.

## .What lies ahead?

As can be seen from the evolution of the rootkit technologies, we can see that the technologies have been slowly evolving and moving out of the jurisdiction of the operating system running on the physical machines. So what are the possibilities of future rootkit technologies?

For the foreseeable future when PC technology like the old-fashioned BIOS is being replaced by Extensible Firmware Interface (EFI) [21], all of the existing BIOS and boot sector rootkit, if they ever appear in the wild in the years to come, will become obsolete. By then, a new standard for booting operating systems will emerge. Coupled together with more frequent releases of new operating systems, we will see even more of the new boot virus. The reason for prevalence of such viruses could be that EFI provides the ease of developing a boot loading software or even to develop a boot virus. Another reason could be that the newer version of operating system is more secure and virus writer find it difficult to write viruses that operates from within the operating system.

As EFI brings more standardized support for hardware and possible support for features such as the Portable Executable (PE) format that is used in Windows for executables, it will be a matter of time before we have user-friendly development environment similar to Visual Studio for developing EFI-based application. I think the prevalence of boot virus will follow when EFI is much more established, especially in the initial years when it is widely used.

By looking at the emerging rootkit technologies so far, if we were to marry the two technologies together namely the virtualization technology and the persistent bios infection technique or even the new and emerging EFI technology, we can predict that this will potentially bring about a new chapter in the rootkit technologies in the future. By then, it will be possible to see an even more advanced rootkit than what we have now.

*Yong Zhen Shing works for a government agency in Singapore. He conducts research on cyber security and is recently focusing his research on malware and its evolution. He can be reached at [stanne@gmail.com](mailto:stanne@gmail.com)*

*Disclaimer: The information in this article has been made available for general personal use only and is provided without any express or implied warranty as to its accuracy or currency. All access to, and use of, the information is at the user's risk. Before relying on any information in this article, users should seek confirmation from the originating source. The provision of any URL or link is done for the convenience of reader of this article to gain more in-depth knowledge of the specific topics. Special thanks and credits are also given to the relevant owner of the materials stated in the references where information is being used for this article.*

## Reference

- [1] [http://www.rootsecure.net/content/downloads/pdf/unix\\_rootkits\\_overview.pdf](http://www.rootsecure.net/content/downloads/pdf/unix_rootkits_overview.pdf)
- [2] <http://www.phrack.org/>
- [3] <http://www.amazon.com/Advanced-Windows-Jeffrey-Richter/dp/1572315482>
- [4] <http://www.amazon.com/Programming-Applications-Microsoft-Windows-General/dp/1572319968>
- [5] <http://www.amazon.com/Undocumented-Windows-2000-Secrets-Programmers/dp/0201721872>
- [6] <http://www.amazon.com/Undocumented-Windows-NT%C2%AE-Prasad-Dabak/dp/0764545698>
- [7] <http://www.sophos.com/security/analyses/viruses-and-spyware/trojhe4hooka.html>
- [8] [http://vil.nai.com/vil/content/v\\_99877.htm](http://vil.nai.com/vil/content/v_99877.htm)
- [9] [http://www.carnal0wnage.com/papers/rootkit\\_for\\_the\\_masses.pdf](http://www.carnal0wnage.com/papers/rootkit_for_the_masses.pdf)
- [10] <http://www.comp.nus.edu.sg/~liangzk/papers/ndss08.pdf>
- [11] <http://www.f-secure.com/v-descs/haxdoor.shtml>
- [12] <http://www.f-secure.com/v-descs/fu.shtml>
- [13] [http://www.cs.uiuc.edu/homes/kingst/Research\\_files/king06.pdf](http://www.cs.uiuc.edu/homes/kingst/Research_files/king06.pdf)
- [14] <http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html>
- [15] <http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Zovi.pdf>
- [16] <http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-soeder.pdf>
- [17] <http://www.blackhat.com/presentations/bh-europe-07/Kumar/Presentation/bh-eu-07-kumar-apr19.pdf>
- [18] <http://www.f-secure.com/weblog/archives/00001393.html>
- [19] <http://cansecwest.com/>
- [20] <http://cansecwest.com/csw09/csw09-sacco-ortega.pdf>
- [21] <http://www.intel.com/technology/efi/index.htm>
- [22] <http://www.stoned-vienna.com/downloads/Paper.pdf>
- [23] [https://www.blackhat.com/presentations/bh-usa-07/Ptacek\\_Goldsmith\\_and\\_Lawson/Presentation/bh-usa-07-ptacek\\_goldsmith\\_and\\_lawson.pdf](https://www.blackhat.com/presentations/bh-usa-07/Ptacek_Goldsmith_and_Lawson/Presentation/bh-usa-07-ptacek_goldsmith_and_lawson.pdf)
- [24] <http://www.viruslist.com/analysis?pubid=204792016>

# The 2010 Job Outlook for IS Security Professionals

The year-end bonus is in the bank, the festive season is over, and we are now all back to work with a vengeance. “Can I really face another year in this job?” Just as Mondays are bad news for most of us, January is surely the biggest “Monday” of them all. If past history is anything to go by, this is the beginning of a busy period for job hunters everywhere.

Happily for all of us this also coincides with a seasonal increase in job openings. With the New Year’s budgets and head counts approved or in progress, hiring managers and recruiters are now out to scour the market for the best talent to boost their ranks, to help them ease their own work burdens and, not least, to achieve their own MBOs as soon as possible.

In early 2010 there is going to be the added boost of a pent up demand left over from last year’s prolonged dry spell. Head count approval was hard to come by in 2009, however the work kept mounting up, users and clients still wanted quality service, perhaps even more so, and resources have been stretched paper thin. Most managers are eager to ease their own workload by bringing in more people. Moreover for 2010, more companies will be setting up their regional (even global) IT/IS facilities in Singapore (indeed they are already doing so) and a fair percentage of the positions on offer will be Information Security related. The first and second quarters of 2010 could be a good time for job hunters, as companies release frozen head count in anticipation of better things to come.

A quick look in the job basket shows that there are potentially more info-security related roles open than at any time since the bonanza year of 1999, during the pre-millennium last-minute panic period. Now we see requirements for generalists, analysts, consultants, specialists in application security, attack monitoring, compliance monitoring, incident response, forensics, privacy and data protection, cryptography, not to mention IS security project managers and middle and senior line managers for start-ups and established players alike.

Whilst 2009 saw a clear-cut retraction in the IS Security job market, 2010 certainly seems set for growth. How long it will last depends on the economy as a whole, and how well Singapore maintains its strong position in the global security league. Right now many companies are bullish about their expansion plans for their IS security teams in Singapore and this bodes well for AISP members in the months to come. Even if we are not job hunting as such, a buoyant job market and high demand for our services cannot be a bad thing. Maybe Mondays won’t seem so bad after all...



*This article has been kindly contributed by Andrew Sansom, AISP committee member. Andrew is a well-known international recruiter with over 20 years experience in the field, backed by 15 years as a leading IT professional in his own right. He has served on national committees in manpower-related areas for more than two decades.*



## Singapore Polytechnic- Another Student Chapter for AISP

AISP is pleased to announce that Singapore Polytechnic has joined to be AISP Student Chapter. We have signed an agreement with Singapore Polytechnic-School of Digital Media and Infocomm Technology on 1 November 2009.

Look out for more synergy between AISP and the Student Chapters.

# Student Chapter's Corner



## About Student Chapter

Since the inception of AISP, we understand the need to bring awareness to students in the infocomm studies about information security. AISP Exco has been very active in approaching various IHLs to create awareness and publicity about AISP.

Till date we have signed up with the following IHLs:

- National University of Singapore
- Nanyang Polytechnic
- Singapore Management University
- Temasek Polytechnic

## Student Chapter's Blog from Temasek Polytechnic



Have you wondered what do Information Security students learn from School?

Have you wondered what challenges they face in their competitions in Information Security?

Read all these from the blog of Temasek Polytechnic-Student Chapter. Visit website <http://tp-cds.blogspot.com>



# CALENDAR OF EVENTS

March						
Mon	Tues	Wed	Thurs	Fri	Sat	Sun
				1	2	3
4	8	9	10	11	12	13
14	15	<b>22 (Mon)</b> Events: IDA-AISP Information Security Seminar 2010		<b>11 (Thurs)</b> Events: 2 <sup>nd</sup> Annual General Meeting  Venue: SCS Resource Centre		
21	22			2		
28	29	30	31			