

Unlock Advice from a Top Security Expert

May 1, 2005
Stephen Ibaraki

Stephen Ibaraki, I.S.P., Director Network Professional Association Board and Canadian Information Processing Society Board, shares an exclusive interview with the universally regarded security authority, Jack Sebbag. [About Jack Sebbag>>](#)

[Cover Page>>](#)

Executive Corner

- [A Letter from the President](#)

Upcoming Events

- [Upcoming Microsoft and Windows IT Pro Chats](#)
- [Tech•Ed 2005: Birds of a Feather Sessions](#)
- [TechNet Briefings](#)

Get Linked Up

- [This Month's Links: Get detailed system information with this freeware, and more...](#)
- [Submit a Link](#)

Focus of the Month:
The IT Community

- [New Magazine for IT Pros](#)
- [Unlock Advice from Top Security Expert](#)
- [Get Recognized for your Community Contributions](#)

Culminis Happenings

- [Culminis Member Organization Leader Andy Goodman gets Published](#)

Special Offers

- [TechNet Magazine: Free Issue Promotion](#)
- [Learn More About Our Sponsors and Affiliates](#)

Register to receive updates and specials from the Culminis Compass. Enter Email here:

[Sign up](#)

[Q/A: Introduction](#)

[Q/A: Major types of malicious code and other threats](#)

[Q/A: Other forms of attacks such as DDOS](#)

[Q/A: How threats evolve and what to look for in the future](#)

[Q/A: Why anti-virus software is unable to handle today's threats and effectiveness of IPS software](#)

[Q/A: Security best practices for consumers and enterprises](#)

[Q/A: Growth Opportunities for IT Professionals](#)

[Culminis on Security](#)

[About Jack Sebbag](#)

Q: Jack, with your extensive background in security issues, we are fortunate to have you provide your in-depth insights into the evolving security threat. Thank you for taking the time out of your busy schedule to do this interview.

A: Stephen, thank you for the opportunity to share my views on this very important topic of the evolving IT security threat. This issue is receiving a lot of attention at all levels of management. It's no longer just the IT managers issue when a piece of malicious code can take out a production line, erase a company's financial data, or take down its e-commerce site so that customers can't place orders. This has gone from being a backroom issue to a boardroom related issue and receiving attention at all levels of management.

Q: Can you define the major types of malicious code (or malware) and other threats: viruses, worms, Trojans, exploits, key loggers, mailers/mass-mailers, social engineering, phishing, spam, Adware, Spyware, cookies, ...?

A: Many people are familiar with the traditional virus attacks using mass mailer techniques. This form of attack propagates via attachments in emails that once opened propagate to other computers by harvesting the infected system's address book. The new attacks that we've seen in the past 12 to 24 months are the result of exploits of a known vulnerability in an operating system. Attacks such as Code Red, Nimda, Sasser, Nachi, etc. are all well known worms that caused a lot of damage. Unlike a mass mailer virus, a worm can propagate itself without the intervention of a user. The worm seeks out un-patched computers (computers that haven't applied the fix to the known vulnerability), spreading itself from computer to computer. As the pool of infected computers grows, the spread gains steam as there are a larger number of computers seeking out its victims... think of it as a growing army of infectors.

The threats I just described revolve around malicious code writers seeking a challenge to bring down as many computers as possible. The newer attacks, such as Phishing, Spam, Adware and Spyware are all motivated by financial gain. Phishing scams are emails using social engineering to trick people to provide confidential information such as bank account, credit card and other personal data to criminals seeking steel. Spyware are software applications installed on computers whereby the user, in most cases, has no idea it's been installed. In some cases Spyware is used to provide marketing data to company's looking to learn buying habits of internet users, internet usage information, etc... all for marketing purposes. More potent use of Spyware applications install keystroke loggers onto a computer. A keystroke logger actually dispatches all data being inputted into a computer; even screen shots of the person's computer to an unknown source using the information

for personal gain. Information stolen can include personal financial data, credit card information, etc...

Q: Can you define other forms of attacks such as DDOS (distributed denial of service attacks)?

A: A distributed denial of service attack is another type of attack used by cyber criminals for financial gain. A distributed denial of service attack commonly known as DDOS, is a flood of requests directed at single or small number of computers, for the sole purpose of rendering that system unable to handle any meaningful requests due to the overflow of requests being launched at it. This type of attack is used by cyber criminals to extort money from companies. Think of an online gambling website receiving a note that if \$50,000 is not paid by a certain date, then a DDOS attack will be launched on its website, making it impossible to run their prosperous online business. Most people pay the bribes to avoid these devastating attacks.

Q: How will the threats evolve and what should both consumers and enterprises be on guard for in the future?

A: With each attack the number of computers infected is larger and more dangerous. Malicious code writers use remnants of well known viruses or worms in order to travel faster and cause more damage. Future attacks will exploit known vulnerabilities quicker than in the past. If we think about the Nimda worm which exploited a known Windows vulnerability in September 2001, 336 days after Microsoft announced the vulnerability, versus the Sasser worm we saw in April 2004, whereby the known Windows vulnerability was exploited 17 days after Microsoft announced the potential exploit. Both of these worms caused significant damage to companies worldwide. As malicious code writers exploit vulnerabilities in a shorter and shorter period of time, it will give companies shorter timeframes to react, exposing them to substantial potential damage. Here's some food for thought...there are malicious code writers out there right now looking to exploit unknown and un-announced vulnerabilities. A zero day attack of this type can cause absolute chaos and infrastructure damage like we've never seen before.

Q: Perimeter firewalls and anti-virus solutions are no longer able to handle today's threats. Why is this so, and how effective are System or host firewalls and Intrusion Prevention Security software?

A: Anti Virus has done a good job in the past of cleaning infected machines after a virus has been launched. The problem now, with worms and viruses going global in minutes, an Anti Virus software which is re-active in nature is no longer enough. Organizations need to move to proactive technologies like Intrusion Prevention. Intrusion Prevention technology (IPS), like McAfee's network IPS Intrushield and host based IPS Enterecept, use signature based and anomaly (artificial intelligence) to proactively block attacks BEFORE they hit your infrastructure. This type of technology puts management back into patch management. Think about black Tuesdays when Microsoft releases its newest list of vulnerabilities...within a couple of hours, the IPS technology is ready to protect organizations against attacks exploiting these vulnerabilities. Companies can roll out the patches after appropriate Q&A and upon resource availability.

Q: Give us your security best practices for consumers and enterprises.

A: Consumers:

1) Invest in appropriate security technologies like Anti Virus, Desktop Firewall, Anti Spyware and Anti Spam. The investment can save you many hours of lost productivity or save you from potential cyber criminals.

2) Keep the software updated. It's not enough anymore to just buy the applications. The annual subscription renewals for maintenance are critical. Otherwise you won't have the protection against all the newest attacks.

3) Don't wait until being attacked before paying attention to what is needed to keep yourself protected.

4) Subscribe to ISPs (Internet Service Providers) who offer much of the needed protection like Anti Virus, Anti Spam, Intrusion Prevention, Anti Phishing, etc...

Enterprises:

1) Time to invest in proactive vs. reactive technology like Intrusion Prevention.

2) Make Vulnerability Management and Risk Management a regular part of your IT operations. Invest in tools that provide information on your security posture so that you can prioritize work to protect against the risks and threats that can have the most significant impact on your organization.

3) Try to reduce the number of consoles necessary to deploy, monitor and manage your best of breed security tools.

Q: What are the growth opportunities for security companies and security professionals? Where should IT professionals focus their training?

A: As we discussed, the threat will continue to evolve. The security professionals who continue to keep their skills aligned with the new and evolving threats will have an advantage.

Culminis on Security:

Culminis has formed the Culminis Taskforce on Building Security Awareness to develop recommendations for IT Pro User Groups and IT Solution Providers on how to build security awareness in the IT Pro Community, conduct monthly meetings to discuss and help resolve issues around building security awareness, and assist with security awareness efforts of Culminis Member Organizations and Sponsors. [Click here for more information>>](#)

About Jack Sebbag:

Jack Sebbag is the Canadian general manager and vice-president of McAfee, Inc. He joined the company In March of 2000.

Sebbag is responsible for the company's sales and marketing for all business units for the Canadian market place. As security threats evolve, McAfee® continues to help secure the networks of major Fortune 500 companies as well as government, health and education sectors.

Prior to McAfee, Sebbag spent 15 years with Canada's largest systems integration and outsourcing companies, EDS Innovations, focusing on the enterprise market space and turn-key solutions. There, he spent over 12 years as a senior territory sales representative and two-and-a-half years as Québec regional sales director.

Sebbag earned a Bachelor of Arts in Industrial Relations and Economics from McGill University in Montréal.