

Course Review: SANS SEC 569 Combating Malware in the Enterprise

By Jeff Georgeson

Your organization will get compromised! The convenience and ease-of-use that your employees and customers demand will expose your network to a plethora of compromises. As much as security paranoids, like myself, would like to completely lockdown our networks to prevent this, it is not practical. The next best thing is to do everything in one's power to minimize the number of incidents and recognize that, despite your best efforts, compromises will most likely happen. A well thought out plan and response is essential for an organization to minimize, contain, eradicate and recover from the damage a malware incident can cause. Lenny Zeltser's SANS Security 569: Combating Malware in the Enterprise is an excellent course to help you devise a robust malware incident response plan. It is a 2-day, in-depth course that extensively covers malware. For Lenny's full course, please read the review for FOR610 right here on EH-Net.

I went into this class having what I thought was an intermediate knowledge of the subject. I was very familiar with some of the topics and knew virtually nothing on others. No matter your knowledge of the subject matter, you will pick up a great deal from this class and definitely won't feel "out of your league." The review that follows discusses the course content at a high level and how this content pertained to me and my organization.

del.icio.us

[Discuss in Forums {mos_smf_discuss:/root}](#)

Free iPad 2!

From now through June 22, 2011, SANS will send you a free 16GB iPad 2 with Wi-Fi when you register and pay for one of the following vLive! courses:

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Learn how to assess and reverse-engineer malicious software with Lenny Zeltser and Michael Murr. Course starts July 25 and meets Mon./Thu. evenings.

MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam

Study the CISSP®'s 10 Domains and prepare to pass the exam with Ted Demopoulos. Course starts July 25 and meets Mon./Wed .evenings.

FOR408: Computer Forensic Investigations - Windows In-Depth

Learn the fundamental steps of computer forensic methodology with Michael Murr. Course starts August 23 and meets Tue./Thu. evenings.

NEW COURSE SEC660: Adv. Penetration Testing, Exploits, and Ethical Hacking

Model and analyze the most prominent and powerful attack vectors with Stephen Sims, Bryce Galbraith, and Joshua Wright. Course starts August 30 and meets Tue./Thu. evenings.

Use Promo Codes 05EH_iPad2BLK (Black iPad) or 05EH_iPad2WHT (White iPad)

Day 1: Discovering and Responding to Malware in the Enterprise

Day 1 started with the obvious question, "What is Malware?" SANS courses do good job of starting at a basic level. The instructors make sure everyone gets on the same page and up-to-speed for the topics discussed during the remainder of the course. This class was no exception. The section was designed for the novice. You could be brand new to the subject matter, and this section got the students to a knowledge level satisfactory for the rest of the course. Malware was defined, a few examples were given, and there was a brief discussion of the different types and forms of malware.

Much of the rest of the morning was devoted to an in-depth discussion of malware functionality and terminology. This was invaluable. Many real-world examples were given and described. Industry "buzzwords" were defined and many malware classifications and attack vectors were explained. What is the difference between a virus and a worm? What is a Trojan? What is a botnet? What are some of the ways they get on a system? These were all discussed in these sections. This was a great foundation and got everyone talking the same language.

A majority of the second half of Day 1 was spent on detection. This was the "Sherlock Holmes" section where you broke out your magnifying glass and started looking for clues many would overlook. Malware is designed to be difficult to detect. You have to know the signs of a compromise. You learned what and where to look for those signs. Some of the topics covered include: The different types, effectiveness and how malware authors avoid detection by various anti-virus programs, what and how to react to user reports of suspected compromises (hint: no questionnaires), what files are most commonly changed, what processes and network traffic abnormalities do you look for, the importance of routine critical file and webserver integrity checks and finally, what specialized malware detection tools are available.

By now you are asking yourself, "So great, I know what malware is and how to look for it. What the heck am I supposed

to do with it once I have found it?" The final section of the day, Containment and Eradication, covered this. Students were taught how to figure out the size of the outbreak once discovered and the different techniques used to contain it. This ranged from network isolation to user participation. The different ways of virus eradication were covered and how to restore the network to normal working functionality. Lenny not only taught the various techniques, but used stories and more real-world examples to further help you in understanding the criteria.

Day 2: Resisting Infections and Containing Malware Outbreaks

Day 2 was broken into 6 sections. The first section, Scalable Management Tools, showed various tools one can employ at an organization with hundreds or even thousands of systems. Different anti-virus strategies were discussed, and several third-party programs were introduced. However, a majority of the section focused on how to employ group policy on Windows, because it's most likely already installed and free in most organizations and "its power is vastly underutilized."

The second section covered Selecting Malware-Resistant Software. You can't combat malware, if the software being used doesn't work or is hard to administer. Lenny went over what considerations you should account for when selecting software; What is your operating system? 32-bit vs. 64-bit? What is the depth of installation? Is it easy to update? How is the anti-virus integration? What are vendor service and support levels?

The third section was Enterprise Patch Management (On a Budget). Every piece of software in your organization, no matter how well written, will most likely have some sort of exploit or vulnerability that will be found somewhere in the future. As a result, this software will need to be occasionally patched or updated. This section went into how to remediate these vulnerabilities. Patch management organization, reasons for test labs, Windows Server Update Services (WSUS), MSI packages and several more topics were discussed.

The fourth section went over restricting user processes. By placing certain restrictions on system, we could hope to block the spawn and spread of attacks. What privileges groups and/or users have and how they work is also covered. Should you whitelist? What are the different strategies to use? They were all discussed in this section.

The fifth section explored how to harden existing applications. This showed exploits and gave recommended settings on software that almost every system in your organization should have. Internet Explorer, Firefox, Adobe Acrobat and Microsoft Office were thoroughly discussed. This section was good in that not only did it show you how to handle these vulnerabilities at a system level, but also Lenny gave tips on how to handle the "political" hurdles of implementing these policies.

The sixth and final section, Restricting Malware-Related Network Traffic, covered network filtering. The first thing that came to mind here was firewalls. That was discussed, but there were so many other elements involved also. The pros, cons and recommendations for intrusion protection systems, proxy servers, DNS domain blocking, remote access gateways, IPsec and the built-in Windows firewall were explored.

Conclusion

A lot was learned in this course over the period of two days. You would definitely come away being more paranoid. Your eyes would be opened to the sheer multitude of vulnerabilities. The greatest thing I took away from it however, was the confidence to tackle the problem. It seemed like a giant insurmountable wall at the beginning. By the end, you're eager to take it on, because you have the tools and knowledge to attack back. In addition to the knowledge, this course, like many offered by The SANS Institute, kept you engaged and interested.

Jeff Georgeson

Information Security Consultant

Infogressive, Inc.

<http://www.infogressive.com>