

Interview: Lenny Zeltser of Savvis and SANS Institute

By Jamy Klein, MSIA, CISSP

According to Panda Labs over 25 million new pieces of malware were released into the wild in 2009. 2010 is expected to be even worse. In addition to sheer volume, malware is becoming more sophisticated and targeted as a result of the influx of organized crime and state sponsors into the realm of malware authoring. Due to this unsavory trend, the SANS Institute has developed a course, Reverse-Engineering Malware: Malware Analysis Tools and Techniques AKA FORENSICS 610, to help white hats that need essential malware analysis skills and also to prepare security professionals for the GIAC Reverse Engineering Malware (GREM) certification. SANS describes FOR610, as:

“Teaches a practical approach to examining malicious software that runs natively on Microsoft Windows, and covers web-based malware such as JavaScript and Flash files. You will learn how to reverse-engineer malicious programs using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out.”

In my work as a Security Engineer, I am frequently asked to analyze web sites and file downloads for potential infection. This course filled both a professional need and personal interest need for me in malware analysis. After attending the 4-day course (now officially a 5-day course) at SANS Security West 2010 in San Diego, I sat down with the course author and instructor, Lenny Zeltser (pictured), to discuss his background, the course and malware analysis in general.

[del.icio.us](#)

Discuss in Forums {mos_smf_discuss:/root}

vLive! from SANS is their live, online training platform.

This isn't a prerecorded study aid -- these are live classes with top instructors!

SEC504: Hacker Techniques, Exploits & Incident Handling (starting 11/9) taught by Bryce Galbraith and John Strand

SEC542: Web App Penetration Testing and Ethical Hacking (starting 12/6) taught by Kevin Johnson and Seth Misenaar

For 10% Off Everything SANS use Coupon Code: Connect_EHN10

Jamy Klein (JK): Please describe your background/history and how you became interested in malware research.

Lenny Zeltser (LZ): Alright. As part of my day job I lead the security consulting practice at Savvis, where I assist customers in designing and maintaining security of cloud-based IT infrastructure. I also spend a fair bit of time researching malware threats and associated anti-malware techniques. Pursuing this interest, I have been teaching malware-related courses at SANS Institute. I also volunteer as an incident handler at SANS Internet Storm Center.

When I graduated from college with a computer science degree, I worked on projects in system administration, then software development, and then some networking. I found information security at the intersection of these fields, and have been focusing on it ever since. In particular, I found the world of malware to be largely unexplored and especially interesting, which is probably why I have been pursuing malware-related projects. It's a lot of fun.

JK: For those unfamiliar with the FOR610 (GREM) course, how would you describe it?

LZ: The FOR610 course teaches practical malware analysis techniques. I've been working on it for a number of years, and recently expanded it from 4 to 5 full days. The goal is to provide people with interest in and perhaps some exposure to reverse-engineering malware to sharpen their skills in the context of a structured malware analysis framework. The course is written to be a springboard for people wanting to get started in this field. One of my primary goals for the course is to allow people who are non-programmers to perform malware analysis, perhaps at a beginner and intermediate level.

Editor's Note: See Review: SANS FOR610 Reverse Engineering Malware by Justin Kallhoff

JK: Why did you see a need to develop this course? Were you trying to fill a void?

LZ: Around 8 years ago I needed to analyze a malicious program found on a compromised Windows host. However, I couldn't find any details about how to do that in a structured manner. There were some useful tools, but no clear way to stitch them together into a comprehensive analysis framework. Presumably, anti-virus companies had this process figured out, but they are a closed industry, wishing to protect their intellectual property and maintain a competitive edge. So, I played with some tools, set up a lab, asked for help from people I know, experimented a bit more and wrote a paper on malware analysis approaches. That paper, still available on my website, was the starting point for the FOR610 course.

JK: What resources do you use for cutting-edge information on malware?

LZ: Is this for people who already have some basic understanding of this topic or for people who are just looking to get started?

JK: This would be primarily for people looking to get started.

LZ: So, there's this FOR610 course that I teach at SANS. [laughter] It's a good way to get started with not only understanding how to reverse-engineer malware, but also how malicious software works. I'm also collaborating on a new, somewhat less technical course, called Combating Malware in the Enterprise. It should be a good way to learn how to defend against malware threats.

Beyond learning through courseware, the various blogs that security companies maintain are an excellent source of information about malware. It's great to see anti-virus industries becoming more open, and now most of these vendors offer a blog that is filled with useful details. The few malware-related blogs that come to mind at this moment are from McAfee, Kaspersky, WebSense, but that is definitely not a definitive list.

Also, Twitter is a really active community for security professionals. It's actually a little bit surprising how many really interesting people and researchers, who have worked with malware, are on Twitter. They're sharing resources, sharing pointers to articles that they have written or have found. To get started, take a look at the list of Twitter malware people I maintain at <http://twitter.com/lennyzeltser/malware>. In a way, there are a lot of people on Twitter who act as narrators to whatever content is being published.

JK: For those starting out, what would be your recommended path for individuals to get their feet wet in malware research?

LZ: Find interesting pieces of malware at work, in your personal inbox, on the web… and analyze it. Blog on it. If you come across something that's cool, that's innovative, write about it and people will notice. Then you can say: "This is what I can do!” Of course, you need to take precautions to make sure you don't infect yourself. If you're interested in knowing how to take some first steps in this field, perhaps take a look at the introductory webcast I recorded at <http://zeltser.com/reverse-malware/malware-analysis-webcast.html>.

JK: Do you think that honeypots are effective learning tools for those interested in malware research?

LZ: Yeah. I think right now honeypot is a very exciting field from a researcher's perspective. We have seen the first generation of honeypots fall. Fortunately, new tools that are more useful and easier to maintain are coming to light. People are taking another look at honeypots. There are some really exciting honeypot projects out there… A good

starting point is probably those that the HoneyNet Project distributes.

Whatever you set up with a honeypot, it's a great way to look at learning. You'll see what attackers are doing, you can get access to fresh malware. What you'll find is going to be real— not theoretical.

JK: What future trends do you think we will see in malware?

LZ: Well malware in general is becoming more difficult to analyze. After all, as defenders improve their tools and techniques, so to malware authors increase the sophistication of their creations to keep up with the arms race. So I imagine the trend will continue. I suspect we'll see an increased use of rootkits to conceal the presence of malware.

I think malware will start targeting mobile devices more than it has in the past. Right now, more and more users are starting to adapt mobile devices, because they're becoming more powerful. The mobile applications are going to be very vulnerable, because they'll be less mature than those we're running on traditional servers and workstations. It's kind of interesting to see how that develops.

Also I think you might see more malware that resides purely in memory without touching the file system. If you stay in memory, you're harder to detect, harder to analyze.

JK: What do you think is the most significant challenge in malware analysis right now? What do you think it will take to combat the challenge?

LZ: Packers continue to be a challenge, because they really slow you down. But we're starting to figure out how to deal with packers, especially with malware analysis that makes use of memory forensics. Even with a complex packer, at some point, malicious code will need to be unpacked partially in order to run. If you keep catching it at the right time in memory, you can grab it from memory and examine it. There's a lot of research going on that's automating the use of unpacking techniques, so we're getting better.

Another challenge is trying to figure out how to deal with the sheer volume of malware samples that organizations are seeing. It's the increased quality of attacks, and they are coming from different parties. Given the volume, there might not be enough time in the day to analyze each of them with the same rigor.

So, I think we'll need to figure out how to deal with malware in a large volume. We will need to automate some techniques; there will be a need to also triage and figure out how to prioritize the efforts, so when you have an incident you can do malware analysis, manually or interactively. [Analysts] will need to be very careful about what they choose to work on, because their time will be limited.

JK: What are your favorite tools for research/analysis?

LZ: The tools mentioned in my REM [Reverse Engineering Malware] course, many of which are in REMnux.

Note: REMnux is a Linux distribution built and maintained by Lenny for the purpose of providing a pre-built analysis and reverse engineering environment.

JK: There has been a lot of press lately about Advanced Persistent Threats (APT). What are your thoughts on the subject? Is there significant reason for concern or has the media exaggerated the risk?

LZ: The advanced persistent threat is a big concern, of course. In addition, it is a very juicy tidbit for the media to hang onto. So has it been overwhelmed, or overblown? It may have been mischaracterized, and nowadays everything that may look remotely like it is targeting organizations, people think it's APT. So I think media might… mischaracterize some of the [events] as APT. You also have a lot of companies, and individuals, adopting the term APT and talking about it, even though they don’t personally get involved in handling APT.

JK: Would you agree that the APT has more to do with bad actors that are targeting the organizations than the actual pieces of malware being used?

LZ: Well, yes. APT is really focusing on the threat agent that uses various techniques, including malware, to maintain a presence in the targeted organization. So yes, malware is just a tool that allows the individuals using it to achieve their goals.

JK: What other training would you recommend for people trying to learn the field of malware analysis, besides your own course?

LZ: People typically ask me how to get into this field or how to proceed as a professional malware progression engineer or an antivirus researcher. The unfortunate answer is it's a bit hard to get into this field, because most companies that I have seen want to hire experienced analysts, which I'm not sure I agree with necessarily.

There are a lot of advantages to finding somebody who's really smart, who understands the basics, and then training him in your ways. What I've seen is there are only a few companies who are willing to do that. If you look at the job postings out there, they want you to be able to demonstrate that you have not just the basic skills, but also have some experience analyzing malware.

So it's a bit of a catch-22. A lot of people who are doing this kind of work found themselves in this field by accident. And

because they were in another job and had to do something related to antivirus engineering, they ended up getting their experience that way. So practically speaking, my recommendation is to get to first learn about the essentials by just reading articles, web chats, papers, playing with things on your own. Then get the formal training to fill in the gaps in your understanding.

JK: In closing I would like to thank Lenny for taking the time out of his busy schedule to share his insights with EH-Net's readers. Having personally attended Lenny's course, I cannot recommend the class and his instruction enough. If your daily duties involve malware analysis or you are even just interested in analyzing malware, Lenny's GREM course should be on your short list.

Jamy Klein is a full-time Information Assurance professional with Qualcomm, Inc. Prior to Qualcomm, he worked as an Information Security Officer for a government agency, as an Information Technology Security Specialist for a major west coast hospital, a fortune 500 insurance and financial company, at an educational institution, and a large credit union. As a result, he has worked in nearly all areas of information assurance and has worked within nearly all major regulatory frameworks. Jamy holds a B.S. in Networks and Telecommunications and a M.S. in Information Assurance from Capitol College, where he is also an adjunct faculty member in the Information Assurance Program. Additionally, Jamy holds various industry certifications including CISSP, GPEN, GCIH, GCFW, GSEC, RHCT, MCP, A+, and ITIL.