

# Pwn2Own Pre-Game: Bug Hunting and Analysis 0x65, Assured Exploitation Training

New York City, January 31-February 3, 2012

Just in time to get warmed up for Pwn2Own, we are delivering a joint offering of the training courses “Bug Hunting and Analysis 0x65” by Aaron Portnoy and Zef Cekaj as well as “Assured Exploitation” by Dino Dai Zovi and Alex Sotirov.

The two-day “Bug Hunting and Analysis 0x65” training will take students through a crash course in reverse engineering, vulnerability discovery, and vulnerability analysis with a focus on server-side software vulnerabilities. The two-day “Assured Exploitation” course immediately follows and guides students through vulnerability analysis of browser-based memory corruption vulnerabilities and hands-on development of reliable exploits against Microsoft’s Internet Explorer 8 on Windows 7. Taken together, these two complementary classes will give students the knowledge and hands-on experience they need to discover, analyze, and exploit memory corruption vulnerabilities in major server-side and client-side Windows software.

Both courses will be delivered in the same professional training facility with pre-configured machines running VMware Player and custom training VM images. The training facility is located in Manhattan’s financial district, easily accessible by NYC subways, waterways, and helicopter.

## Registration

Class	By 1/06	By 1/27
Bug Hunting and Analysis 0x65 (1/31-2/1)	\$2500	\$3000
Assured Exploitation (2/2-2/3)	\$2500	\$3000
Both Classes	\$4000	\$5000

Each class is \$2500 per student if payment is received by January 6<sup>th</sup>, or \$3000 after. Sign up for both classes and save \$1000!

Early registration is recommended because the class size is limited and may be sold out. Please email [ddz@theta44.org](mailto:ddz@theta44.org) to register for one or both trainings or if you have any questions. We accept payment through both PayPal and Google Checkout.

## Bug Hunting and Analysis 0x65

This 2 day course is structured to impart upon the students the skills necessary to effectively utilize debuggers, disassemblers, and other tools to discover vulnerabilities in binary code. The curriculum will begin by introducing students to the tools and generic techniques that will enable them to actively participate in reversing applications during the rest of the course.

After gaining a basic understanding of the tools involved, the instructors will spend time walking students through case studies from patched vulnerabilities. That is, we will be choosing specific vulnerabilities and walking the students through the methodology used to verify them (debugging) and how the discoverer likely found them (fuzzing, static reverse engineering, dynamic instrumentation, etc). As each flaw is dissected, we will focus on how the student's arsenal of techniques can be extended to more easily debug applications and eventually discover similar bugs going forward.

We will then begin focusing on automating our tools to build a checklist that we can use to more efficiently reverse engineer a binary code base. We will walk through a complete audit of a default installation (latest version) of a popular enterprise server application culminating in the discovery of over 20 remote pre-authentication 0day vulnerabilities.

### Prerequisites

Prospective students should have basic x86 assembly fluency. Previous debugging experience is also required; Our debugger of choice for this class will be WinDBG. Programming experience is required, preferably in Python as the class will be developing IDAPython scripts to aid in RE. Our target platform will be Windows 2003, the student should be comfortable operating in this environment.

### Trainers

#### *Aaron Portnoy*

Aaron Portnoy is the Manager of the Security Research Team at TippingPoint Technologies. His group is responsible for reverse engineering vulnerability submissions to the Zero Day Initiative program, discovering new 0day vulnerabilities in enterprise software, developing tools to aid in these processes, and architecting competitions such as Pwn2Own. Aaron has discovered critical exploitable vulnerabilities affecting a wide range of vendors including, but not limited to: Microsoft, Adobe, RSA, Novell, Symantec, HP, IBM, SAP, and VMware. He has presented original research in the areas of reverse engineering and vulnerability discovery at conferences such as BlackHat, CanSecWest, BlueHat, RSA, and RECon. Additionally, Aaron has been an invited speaker at the National Security Agency, has

been referenced in several published books, and guest lectures on reverse engineering at the Polytechnic Institute of NYU each fall.

### **Zef Cekaj**

Zef Cekaj is a security researcher specializing in vulnerability reversing and discovery. He has reversed and documented hundreds of vulnerabilities and has a history of vehemently arguing with vendors over email regarding exploitability of bugs in their products. Consequently, he enjoys winning such arguments by demonstrating exploits on live systems. His primary interests are in the exploitation of server side vulnerabilities and mitigation circumvention. He is currently researching identified vulnerabilities in popular sandboxing implementations so that he may contribute to The Movement to Liberate Shellcodes (freetheshellcodes.net), of which he is a founder.

## **Assured Exploitation**

Many security professionals have mastered stack overflows and heap spraying, but these techniques are rarely sufficient when developing modern real-world exploits. Reliable exploitation on Vista and Windows 7 systems requires advanced techniques such as heap layout manipulation, return oriented programming and ASLR information leaks. This course focuses on teaching the principles behind these advanced techniques and will give the students hands-on experience developing real-world exploits.

The course will start off with an in-depth review of the exploitation mitigations introduced in modern operating systems. The instructors will demonstrate their limitations through simple examples and gradually develop the basic exploitation techniques into more complicated methods applicable to real-world exploitation. Unlike most other exploitation courses, we will focus on approaching exploitation as a creative problem-solving process rather than an exercise of applying cookbook techniques to common types of vulnerabilities. Most of the course will focus on the hands-on application of the material through exercises and leading the students through the development of reliable exploits for recently patched vulnerabilities in widely used software. Each student will finish the class with their own personally developed exploit for the Aurora vulnerability in Internet Explorer that evades ASLR and DEP and reliably exploits Windows 7.

This training will cover:

- In-depth review of GS, ASLR, DEP, SafeSEH and SEHOP exploitation mitigations
- Heap implementation details and manipulation of the heap state (including the Windows 7 heap)
- Building primitives for heap layout control in new applications
- Return oriented programming and shellcode development

- Implementing a universal bypass of DEP and ASLR in Internet Explorer 8
- Multistage stack pivots

## Prerequisites

Students are expected to be familiar with the basic exploitation techniques for stack and heap overflows on Windows, as described in the Shellcoder's Handbook and similar books. They should be comfortable using assembly level debuggers and have basic familiarity with reverse engineering. The material in this course is designed to be challenging, but we believe that with the help of our expert instructors any dedicated student will be able to master it.

## Trainers

### *Dino Dai Zovi*

Dino Dai Zovi, currently an independent security consultant and researcher, has been working in information security for over 9 years with experience in red teaming, penetration testing, software security, information security management, and cybersecurity R&D. Mr. Dai Zovi is also a regular speaker at information security conferences having presented his independent research on memory corruption exploitation techniques, 802.11 wireless client attacks, and Intel VT-x virtualization rootkits over the last 10 years at conferences around the world including DEFCON, BlackHat, and CanSecWest. He is a co-author of the books "The Mac Hacker's Handbook" (Wiley, 2009) and "The Art of Software Security Testing" (Addison-Wesley, 2006). In 2008, eWEEK named him one of the 15 Most Influential People in Security. He is perhaps best known in the information security and Mac communities for winning the first PWN2OWN contest at CanSecWest 2007.

### *Alexander Sotirov*

Alexander Sotirov is an independent security researcher with more than ten years of experience with vulnerability research, reverse engineering and advanced exploitation techniques. His recent work includes exploiting MD5 collisions to create a rogue Certificate Authority, bypassing the exploitation mitigations on Windows Vista and developing the Heap Feng Shui browser exploitation technique. His professional experience includes positions as a security researcher at Determina and VMware. Currently he is working as an independent security consultant in New York. He is a regular speaker at security conferences around the world, including CanSecWest, BlackHat and Recon. Alexander served as a program chair of the USENIX Workshop on Offensive Technologies and is one of the founders of the Pwnie Awards.