|  |  |  |
| --- | --- | --- |
| * Draft the history and background on why study malware | Michael Gergely | Nov. 11 |
| * Draft present-day examples of teaching the making of malware | Christopher Sigouin | Nov. 11 |
| * Draft thoughts on future Internet security if malware is taught | Evan Cahill | Nov. 11 |
| * Draft handout and interactive activity | Ashley Patterson | Nov. 11 |

=====================================================================================

**PEOPLE WHO ARE TEACHING MALWARE**

* Intro
* George Ledin
* John Sullins
* John Aycock

**IMPORTANCE ON ETHICS IN EDUCATION ON MALWARE**

* Intro
* Reasons why
* Example Methods

**EXAMPLE COURSE OUTLINE**

* Intro
* George Ledin Course
* John Aycock Course
* Possible Video? ( John Aycock talking about malware course )

=====================================================================================

**PEOPLE WHO ARE TEACHING MALWARE**

**Intro**

**SCRIPT (LEAD FROM HISTORY TO PRESENT):**

Malware has now placed us into a position where we need to consider other alternatives. A few people of education have realized this and have introduced new methods of learning in the fields of computer science. Their main goals are common in nature. To teach how malware works so that can better prepare our future professionals. Let’s take a look at them now…

**George Ledin**

Professor of the Computer Science Department of Sonoma State University

**SCRIPT:**

A professor in the computer science field who is a trailblazer on malware design and defense education. His course is called “Computer Security and Malware“at Sonoma State University in California. He has been subject to the media for some time due to his involvement with the course. Antivirus companies have shunned him calling “him” the nuisance instead of the malware that they aim to prevent. On the other side, Ledin believes that antivirus products are of no worth whatsoever.

**Dr. John Sullins**

Assistant professor at Sonoma State University (partnered with George Ledin)

**SCRIPT:**

Dr. Sullins responsibilities lie in teaching computer ethics to classes alongside Mr. Ledin. He specializes in philosophical issues of artificial intelligence/robotics, engineering ethics, philosophy of technology, and more. He is also a certified Military Master at Arms and winner of the 2011 Herbert A. Simon Award. Professor Ledin and Dr. Sullins agreed before beginning the curriculum that ethics would need to be stressed given the circumstances of the content.

**John Aycock**

Associate professor of the Computer Science Department at the University of Calgary

**SCRIPT:**

Professor John Aycock teaches a course developed in 2004 called “Spam and Spyware” that we will highlight later on. At the time of its development it was the only one known in existence. Similar to Ledin’s theory on learning the development process of malicious code, Mr. Aycock believes the more that is known about malware, the better prepared we will be to defend against it. Also that places of higher learning should be more responsible for handing out education on this subject matter as it is very difficult to find specific resources alone.

**IMPORTANCE ON ETHICS IN EDUCATION ON MALWARE**

**Intro**

**SCRIPT:**

Before we dive into the courses offered by some of these professors, we will look at the side requirements that are essential to them. Ethics. Dangerous knowledge is how John Sullins describes the act of malware programming and in cases where it’s taught requires special consideration on ethics. Learning the art of malware in his words require firewalls of both technical and moral nature.

**Reasons why (Why do we need to learn about ethics?)**

**SCRIPT:**

Why is this necessary you might ask? Consider from the brief history we looked at and what capabilities some of the malware possessed. If you were taught a method on how to bypass every single antivirus program created, would you be tempted to create the software and utilize it for your own purposes? Depending on your own morals the direction is either way. In order for education to be successful with its malware teaching endeavors, ethics must reinforce the minds of students who will be planted deep in its roots.

Working with malware even for the best of intentions still requires someone to think like the developer who created it. Human nature would say the more you think like a person who developed a program to steal information or break security measures, the more your own judgement changes. A skill ethics can develop is to keep those two worlds separate in one’s own mind.

**Example Methods**

**SCRIPT:**

Basic concepts:

Starting place for students is the ACM Code of Ethics. This is a code that contains 24 crucial statements describing ethical issues a professional may come across in his or her IT career. The code uses a set of guidelines that complement the statements directing how one should proceed upon confronting an issue. Think of it as a programmers “Prime Directive “if you’re a star trek fan. There are areas that the code still may not cover completely so other theories are lectured such as utilitarianism, deontology, human rights, and the unified common goods approach as described by James Moor. These in turn also have their own good and bad areas so other systems are used to cover them.

Virtues in Security:

A concept taught to students are the three virtues on secure software. They are confidentiality, integrity, and availability (CIA). A particular CIA approved analogy on firewalls used to build systems is focused on as well, noting that it is questionable. This is due to the possibility of unknown perils from inside the system. The ethics on data level security are then discussed including the challenges that follow.

Ethical Hacks:

It’s advised that students should not just think like a goodie good but as a researcher striving to attain different methods that will work for humanity in the future. Also that defying limits and abilities of computer systems is not completely wrong. Innovation thrives on new discovery and a student may very well come across such a discovery. The main concern in the motivation of the student so concentration is applied to their virtues and personal motives. Students ultimately decide whether to take paths of good or evil based on these and not because they just do not choose to follow a basic code of conduct.

Assessments:

The reason why students choose a particular method based on their morals is examined. They are tested in two ways. The first is in a classroom through discussion and contemplation and the second method uses an exam process. While working on projects that involve awkard situations, students will be required to provide their own ethical reasoning for their choices. This is extremely important within the field of malware research.

**EXAMPLE COURSE OUTLINE**

**Intro**

**SCRIPT:**

Now that we have ethics covered we can take a look at the guts of the courses being offered by both Professor Ledin of Sonoma State and Professor Aycock with the University of Calgary. Both courses aim for the similar goals of advancing knowledge on malware to better defend against it. In the words of Professor Ledin:

“The goal is for students to use their knowledge of the “dark side” of programming to build future computer systems that are better equipped to guard against and even combat these malicious programs.”

**George Ledin Course**

Sonoma State University

CS 340 Course Description

Current methods for increasing security, protecting privacy, and guaranteeing degrees of confidentiality of computer records; ensuring computer installation safety; protecting software products; preventing and dealing with crime; value systems, ethics, and human factors affecting use and misuse of computers. Discussion of recent technical, legal, and sociopolitical issues influencing computer security problems. Prerequisites: CS 215 and CS 252, or consent of instructor.

**SCRIPT:**

// INFORMATION HERE ON THE COURSE

Some of the student projects completed in Professor Ledin’s course and a description on what they are capable of.

**Student Projects Completed**

**SCRIPT:**

FORK BOMB ( demo on Windows Vista )

Software that places copies of itself within memory. It continually does this until the machine has lost all resources and cannot function any longer. The replication process it goes through is called a “fork”. Most operating systems that were tested by the student failed to contain the malware. It was mentioned though that the Linux OS and versions of BSD were able to limit the number of processes running to prevent its destructive function.

COOKIE MONSTER( demo on Windows Vista )

A virus that takes advantage of no exploits on the Windows Vista OS. The malware is ran voluntarily by the user and asks to a cookie. The user is given a choice of yes or no. If yes is provided the program goes dormant but comes back after a minute or so and reasks the same question. If no is provided then the malware proceeds to wipe the complete Windows Registry from the computer without alerting the user in any manner. Upon reboot the computer affected will advise that the

KEYLOGGER

This malware was programmed to hide on the computer system. If a user suspected an infection and attempted to open a registry editor or command prompt the software would automatically close the application as soon as it started.

FORUM FLOODER

This application would generate users by automated process on a web forum. It could log into the forum system, bypass a captcha and confirm the email send to it. Once multiple users are created under it, each one could be used to post continuously to the forum basically “flooding” it with messages until the web server itself runs out of space. Very similar to DDos attacks utilizing a botnet.

**OPEN SOURCE MENU OF ANTI-WORM COUNTER-MEASURES**

**SCRIPT:**

A project in development by students with the help of Professor Ledin. On this website he advises that anyone from any universities are eligible to assist in the project for programming, review or even test its capabilities.

**John Aycock Course**

Computer Science 528 Spam and Spyware

Spam and other unsolicited bulk electronic communication, and spyware. Legal and ethical issues. Countermeasures and related security problems. Course Hours: H(3-0)

Prerequisite(s):

Computer Science 313 and 457 and consent of the Department.

**SCRIPT:**

Now a brief look at the course called “ Spam and Spyware “ offered by Professor John Aycock at the University of Calgary. There are many parts to this course so we very briefly summarize each part and what it entails. We then take a look at the assignments that a student would be required to complete.

**SCRIPT:**

* Introduction (3%) ( Laboratory protocol, Legal Agreement, Professionalism )

Lab Protocol is about behaviour in the lab. Applied to students, teachers and anyone involved in its maintenance. Treatment of the lab is like a biohazard area. Legal Agreements signed by the students. Professionalism due to imagery that is found in the same environments of spam and spyware. Students are warned ahead of time to deal with it appropriately.

* Definitions of spam and spyware (3%)

What constitutes spam and spyware. An overlook at all software to see if it would fall into the category. Official definitions are supplied later.

* Ethics (8%) ( General ethical theories, recognizing ethical problems, ethical decision making, sample ethical problems, professional codes of ethics and conduct, ACM code of Conduct, IEEE, Canadian Marketing Association )

Assumed that students have little to no training in ethics. Start with general ethical theories. Progresses into more specialized codes. Written ethics assignment is completed.

* Spam and spyware law (11%) ( Canada, Australia, United States )

Laws change rapidly. Examine existing and future legislation. Any cases of breaking laws are noted. Ethics are presented prior to any programming. This ensures a more secure environment by bringing attention to students on their possible actions.

* Spyware (23%)

Covers history, anti-virus and anti-spyware vendors, why it exists, how it gets onto a computer, spyware capabilities and countermeasures, keylogging defenses, startup hooks, hiding and forms of obfuscation, and much more

* Phishing ( 15% )

Teaches history, social engineering, specialized forms, url tricks, pharming methods, infrastructure for phishing, anti-phishing techniques, and much more

* Fraud (4%)

Advance fee fraud (419 scams), various types of online scams and money laundering

* Email (7%)

Mail system architecture, routing , DNS, SMTP transactions and mail envelopes and headers

* Spam (12%) Primer on spam while using real life examples, amassing email addresses, anti- harvesting techniques and harvester countermeasures, cleaning and verifying email lists, bulk email software techniques, open relays open proxies, zombies and much more
* Anti-Spam (15%)

Manual spam tracking methods, white and grey listing, tarpits, proof-of-work systems, sender policy framework, filter-evasion used by spammers and much more

ONE ETHICS ASSIGNMENT AND FIVE PROGRAMMING ASSIGNMENTS IN A SECURE LABRATORY

**SCRIPT:**

Five assignments are part of the Spam and Spyware course taught by Professor Aycock. One of which is an ethics assignment that is completed prior to the four that are programming based.

**SCRIPT:**

Assignment 1: spyware/offensive.

Writing spyware that installed a startup hook, changed the browser start page, and performed keylogging. Keylogging was directed at the capture of the username and password used in the web browser to access a ﬁctitious bank’s web site.

Assignment 2: spyware/defensive.

Students exchanged their spyware from the previous assignment. They then developed anti-spyware software that accurately detected, identiﬁed, and removed all spyware samples.

Assignment 3: spam/offensive.

Writing bulk mailing software that delivered messages directly to an SMTP server, optionally routing through an open proxy. Because laboratory constraints precluded us from sending a message to multiple recipients in any meaningful way, students instead sent multiple messages to one recipient. Spam and ham corpora (a subset of SpamAssassin’s public corpora [11]) were supplied for the students to transmit.

Assignment 4: spam/defensive.

Once the email was delivered to some lucky recipient, students developed a spam ﬁlter that sorted the recipient’s mailbox into spam and ham messages as accurately as possible.

**SCRIPT:**

Much detail is placed into both courses. [ LEAD INTO CONCLUSION FROM HERE ]

REFERENCES

CODE OF ETHICS - http://www.acm.org/about/code-of-ethics

WIKIPEDIA ( GEORGE LEDIN ) - http://en.wikipedia.org/wiki/George\_Ledin

GEORGE LEDIN WEBSITE - http://ledin.cs.sonoma.edu/

JOHN SULLINS WEBSITE - http://www.johnsullins.com/category/news

JOHN AYCOCK WEBSITE - http://pages.cpsc.ucalgary.ca/~aycock/

OPEN SOURCE PROJECT LEDIN - <http://www.cs.sonoma.edu/ledin/malware/pdf/WouldYouLike.html>

Aycock, J. (2006). Teaching spam and spyware at the university of c@ 1g4ry. *In CEAS.*

Wasp, J. (2008). The dark world of computer security. *Sonoma Insights, Fall*, 14-16.

John Aycock VIDEO

http://www.youtube.com/watch?v=qzrKSUsxFkM

PICS

http://www.sonoma.edu/newscenter/sullinswired.jpeg

http://www.cs.sonoma.edu/ledin/malware/images/George.jpg

http://www.ucalgary.ca/news/files/news/images/John\_Aycock-350.jpg