Offensive technologies
Fall 2015

Lecture 0- Administrative Details

Fabio Massacci

https://securitylab.disi.unitn.it/doku.php?id=course_on_offensive_technologies

Course Objective

- ***Myths:***
  - Hackers are social outcast with "deviant" skills and do this out of bravery and spite for society
  - Bad things only happens to people who mess up and, as I'm not incompetent, this won't happen to me.
- ***Reality (concise version)***
  - Hacking is a professional activity performed by a wide varieties of actors
- ***Reality (extended version)***
  - '80s: hacker → security expert
    - Curiosity-driven, Interested in the technical aspects of the vuln
  - '90s: hacker → "script kiddie"
    - "How do I install linux to become an hacker", Batch attacks from a tool (e.g. se7en)
  - '00s: hacker → financially motivated criminal
    - Economic model and incentives behind exploit engineering
  - '10s: hacker → State actors
    - somewhere in between politics and theft
- ***Course Objectives***
  - Offensive technologies are a permanent characteristics of a technological society. It cannot be eliminated as it uses the very same "features" that make our society advanced.
  - The course guides students to understand the main economic, social and technological drivers behind malware development by governamental actors. Understanding them allows us to better identify methods to defend ourselves.

Course Structures

- ***Learning:***
  - Introduction
  - Black markets
  - Understanding how buffer overflow work
    - A"taster" to understand the intrinsic complication of modern software → Security Testing course
  - Data analysis, qualitative "coding"
  - Governamental Malware
    - General introduction, lectures from external experts
  - Legal aspects
- ***Presentations***
  - Each of you present its intermediate findings to the class
- ***Investigating***
  - Documents and email analysis and report for government malware, reporting statistics and "qualitative coding" of data (up to 15/30 grade points)
- ***Designing:***
  - Structuring knowledge describing a Government hacking as a business environment (up to 10/30 grade points)
- ***Producing:***
  - Redeployment of a government malware in the lab protected environment (up to 15/30 grade points)
- ***Feedback:***
  - Bonus 4 points if you addressed the feedback given to your team in intermediate presentations

Lecturers

- ***Main lecturers***
  - Prof. Dr. Fabio Massacci
    - Office hours by appointment in class
    - Can try your luck by email
  - Dr. Luca Allodi
    - Office hour by appointment via email
- ***Others***
  - Ms Martina De Gramatica
    - Qualitative research
  - Dr Cesar Bernardini
    - Buffer overflow tutorial
  - Industry guest speakers

Rules of Engagement

- ***Asking questions in class is always the best policy***
  - Your colleagues may be interested in the answer
  - Things are easier to explain
  - The prof gets hundreds email per day…
    - Today 9am – 14 am (66 emails and counting)
- ***Do your homework first***
  - "I can't bother to find the answer, I will ask the prof."
    - Q: "I don't remember to whom the deliverable should be submitted"
    - A: "read my slides"
- ***Write with "[OffTech-2015]" in the subject***
  - "important" is a no go
    - Got 57 in the last months
  - "urgent" is not better

Overarching Learning Objectives

- ***The course should develop and evaluate your abilities in***
  - Making value judgement
    - Decide which parts are important and which are not (this should be an important part of understanding which decisions are important to consider when security attacks are mounted by a varieties of actors).
  - Creativity
    - How to solve problems when not all steps are completely specified (this what you should try to replicate the deployment of the malware)
  - Ethics
    - Self explanatory?

Material used the course

- ***MalwareLab***
  - The dump is downstairs in Povo 2 for you to analyse
- ✓ ***Dump of emails → insights on internal procedures of gov malware development***
  - Who was the hacking team dealing with? What problems did their products have?
- ✓ ***Dump of bills → insight on actual clients and malware deployment.***
  - Is your own motherland government involved? If yes, how much and for what?
- ✓ ***Dump of source code → insights on malware operations***
  - Can you spot malware functionalities declared in the documentation in the actual code?
- ✓ ***Malware dump → actual malware you can try to install and test on the lab machines***

Responsible Study

- ***Material in the MalwareLab is sensitive***
  - Its content might be offensive to you (pornographic pictures, racist comments, disrespectful of your religious beliefs etc..)
  - It may create embarrassment or slander of individuals
- ***Malware is advanced tech***
  - Nobody really knows what it does (most advanced one even detect they are analyzed)
  - There are mechanisms in place to prevent you from exfiltrating the data outside of lab
- ***You must agree to the terms and conditions of this course before having access to the data***
  - Mlab is isolated from rest of infrastructure
  - You work **only** in the lab
  - You are **not allowed** to disclose information about any individual that you find during the analysis
  - Your final deliverable, as approved by the professor is the only public deliverable you are allowed to disclose to third parties

Offensive technologies
Fall 2015

Lecture 1

Introduction

Fabio Massacci

Question

- ***Will be offensive technologies there to stay?***
  - Hacking "expires" the idea "stays"
    - Well old things are still there…
  - Attacker style is importance for defense
  - If there is something that can be abused it will be abused
    - Motivation is important – cost has to be feasible – engineering
  - Same problem may apply for protection mechanism

Do you trust these organisations?

- ***S-TRUST Authentication and Encryption Root***
  - Deutscher Sparkassen Verlag GmbH, Stuttgart, Baden-Wuerttemberg (DE)
- ***NetLock Kozjegyzoi Tanusitvanykiado***
  - Tanusitvanykiadok, NetLock Halozatbiztonsagi Kft., Budapest, Hungary
- ***TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı***
  - Bilgilletişim ve Bilişim Güvenliği Hizmetleri A.Ş. ANKARA, Turkey
- ***CA 沃通根证书***
  - WoSign CA Limited, China

- ***To guarantee that a website is really what it claims to be?***

What's this?

- ***ONE webpage***
  - Plenty of ads
- ***Process***
  - We DON'T look at the ads
  - Only click on mail
- ***And download the program of the infosec conference***

What's this?

- ONE PDF file, essentially an image
- What happens if we open it?
  - Nothing
  - Acrobat Reader shows the image on the monitor

What's this?

- ***A photocopier***
- ***A printer***
- ***You send a file, and it prints***

What *really is* this? Just like that!

- ***Xerox computer to just print a file:***
- ***Intel Celeron - 733 MHZ – 128MB***

- ***NASA computer to land Apollo 16 to the Moon***
- ***AGC – 1 MHz – 4KB RAM***

What *really* is this?

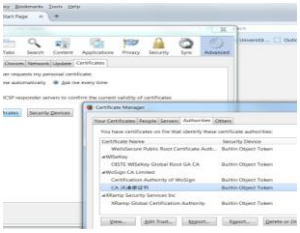
- ***That's a program containing***
  - at least 1682 instructions
- ***What happens when we open it?***
  - All instructions are executed
  - Not necessarily true that the result is displayed
- ***PDF language is Turing Complete***
  - **ANY** function can be written in PDF language
  - Opening a PDF file can seamlessly display an image and simultaneously solve small Fermat's theorem

What *really* is this?

- ***When we type www.libero.it o the browser, YOUR computer will:***
- ***Execute***
  - 186 local functions
  - 15 functions from ***external*** site
- ***Aggregate static contents from***
  - 676 websites of which
  - 370 external websites
  - 193 may be just images
- ***Aggregate dynamic content fr***
  - 8 advertisers (at least)
- ***Are all of these actions "good" ones?***

Who trusts these? Everybody.

- ***S-TRUST Authentication and Encryption Root***
  - Deutscher Sparkassen Verlag GmbH, Stuttgart, Baden-Wuerttemberg (DE)
- ***NetLock Kozjegyzoi Tanusitvanykiado***
  - Tanusitvanykiadok, NetLock Halozatbiztonsagi Kft., Budapest, Hungary
- ***TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı***
  - Bilgiletişim ve Bilişim Güvenliği Hizmetleri A.Ş. ANKARA, Turkey
- ***沃通根证书***
  - WoSign CA Limited, China



Question - discussion

- ***Even with the basic assumption***
  - What's from inside is trusted
  - What's from outside is untrusted
- ***BUT in todays Internet this is not true***
  - Comes from inside→ Goes out → Comes back
  - Visualise a webpage = HTTP GET
    - HTTP GET = go out, deliver what you find, and what you find is an executable (for convenience)
  - E-mails come from outside etc. etc.
- ***We have too many powerful things that make our life nice, too powerful to control and lock them down and lock them out***

Attack delivery

- ***Type of infection is a function of attacker's goal:***
  - Botnet creation → simple form of control for limited functionalities
  - Virus/keylogger → credential theft /spoofing/ spam/ remote control
  - Full-fledged backdoors → monitoring / remote control
  - Ransomware → direct monetisation & low profile
- ***Regardless of what the attacker wants to do, he/she must have some level of access to the machine***
  - Remote control = long term avenue for the attacker to "valorize" the infection

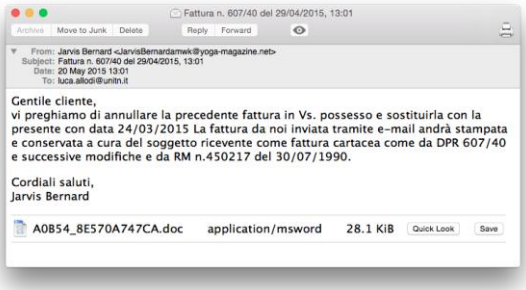
How does the infection happen?

- ***Human vector (social engineering) → user vulnerability***
  - The attacker convinces the user on doing something for him/her (e.g. install a virus masked as an anti-virus → fakeAV)
- ***Tecnological vector → software vulnerability***
  - Principal cause is that most systems are not capable of distinguishing "legitimate" input from "rogue" input (e.g. as provided by the attacker)
  - The system executes whatever's in memory.
  - Virtually any software has bugs that the attacker can exploit to deviate the execution of the software towards actions in his own agenda.
- ***Mixed: e.g. link on social network, link clicked by a user on a document, opening an email with a malware, IP connected camera with pre-loaded malware etc.***

Human vector: social engineering

- ***Attacker convinces the user to install a virus masked as a legitimate application***
- ***The example here is a fake antivirus product called "Win 8 Security System"***
  - User thinks it's actual AV
  - In reality it infects the system

Example of attempted infection



Technological vector

- ***The attack usually exploits some vulnerability in software***
- ***System is fed with computationally valid codes in input to a vulnerable software → code is executed***
- ***Several types of vulnerabilities***
  - XSS
  - Buffer overflow
  - SQLi
  - Privilege escalation
  - …
- ***More exercises and details in***
  - Network Security Course
  - Security Testing Course

Vulnerability examples

Vulnerability Summary for CVE-2012-2522

Original release date: 08/14/2012

Last revised: 11/02/2013

Source: US-CERT/NIST

Overview

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a malformed virtual function table after this table's deletion, aka "Virtual Function Table Corruption Remote Code Execution Vulnerability."

Vulnerability Summary for CVE-2015-3088

Original release date: 05/13/2015

Last revised: 05/26/2015

Source: US-CERT/NIST

Overview

Heap-based buffer overflow in Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allows attackers to execute arbitrary code via unspecified vectors.

Vulnerability Summary for CVE

Original release date: 05/13/2015

Last revised: 05/14/2015

Source: US-CERT/NIST

Overview

Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3053, CVE-2015-3054, CVE-2015-3055, and CVE-2015-3059.

Not all vulnerabilities are equal

- ***Publicly disclosed vulnerabilities → knowledge about the vuln is in the public domain***
  - Responsible disclosure
    - Vuln disclosed first to vendor
    - Vendor releases patch
    - Vulnerability is disclosed
  - "Not responsible" disclosure
    - Vuln is disclosed
    - Vendor gets to know it (word-of-mouth, sec researcher..)
    - Vendor (eventually) patches
- ***Privately disclosed vulnerabilities***
  - Somebody found the vuln
  - keeps info for him/her self
  - OR sells it to a few costumers
- ***Privately disclosed vulns also called "0-day"***
  - 0-day exploit is "Defined as computer language code written to take advantage of a particular vulnerability, which has been discovered but is not publicly known."
    - First definition in academic literature by Arkin in 2002.

Public vs private

- ***Two separate markets***
  - Public vulns → vendor pays researcher for finding it
  - Private vulns → rich player pays researcher to own exclusive information
- ***Vulnerabilities are information***
  - In theory: once the info is out, vuln is "replicable"
    - Private vuln → no value if disclosed
    - Public vuln → no value after publication
  - Not really true but disclosure still changes game
    - Engineering exploits is difficult → Black market tools only use an handful of disclosed vulns
    - High profile victims might be alerted by security → low profile victims may remain vulnerable

Alledged (1st time) price list for 0-days

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

- ***http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/***

Who buys into these markets?

- ***Allegedly (2nd time), mostly governments***
- ***Ok, but from whom?***
- ***Allegedly (3rd time), from private agencies that sell malware and exploits to governments***
  - Which governments?
  - Mostly oppressive ones (yes, allegedly, 4th time)
- ***Sample of agency names***
  - VuPEN (used to be in France)
  - Gamma International (UK/Germany)
  - Hacking Team (Italy)

Research on "private" tech

- ***Security "hacktivists" conducted research on "phishy" activities by these agencies***
- ***Most research done by CitizenLab***
  - 2015 EFF (Electronic Freedom Foundation) Pioneer award
- ***An example is FinFisher by Gamma International***
  - https://www.gammagroup.com
  - Headquaters in UK (Gamma group) / Munich (Gamma GmbH)

Gamma international GmbH

- ***FinFisher is a line of software products***
  - remote intrusion
  - surveillance
  - Typical "beach head" diffused through email campaign
- ***Sold exclusively to law enforcement and governments***
  - "Official" use
    - surveillance of criminals/prevention
  - Actual deployment (instance of)
    - surveillance of political dissidents in Bahrain

Gamma international (GmbH)

- ***FinSpy gathers information from the infected computer***
  - passwords
  - Screenshots
  - Skype calls
- ***Sends the information to a FinSpy command & control server.***
  - Researcher @ Rapid 7 traced C&C fingerprint
  - Binary analysis of malware samples → all belong to same family
  - https://www.virustotal.com/en/file/cc3b65a0f559fa5e6bf4e60eef3bffe8d568a93dbb850f78bdd3560f38218b5c/analysis/

FinSpy

- ***Disguises itself as a picture***
- ***Filename has Unicode Right-to-Left Override char (U+202e in unicode)***
  - Real name gpj.1bajaR.exe
  - Displayed name: exe.Rajab1.jpg
- ***An executable disguised as a picture***
- ***Different pictures for different samples***

FinSpy - delivery

FinSpy – Execution (1)

- ***Creates random dirname***
  - C:\DOCUME~1\User\LOCALS~1\Temp\\TMP44D8C9F9
- ***Drops copy of itself and launches***
  - C:\DOCUME~1\User\LOCALS~1\Temp\\driverw.sys
  - Driver already seen in other samples of FinFisher malware
    - Functionality unknown
  - New random dir to store screenshots, logs, etc. to send to C&C

FinSpy – Execution (2)

- ***Actual malware functionality upon reboot***
- ***Injects itself in winlogon***
  - Spawns legitimate processes and then replaces code image with malicious one (process hollowing)
  - Hooks on several system functions
  - Catches call and sends data to C&C

IP	Operator	Routed to Country
117.121.xxx.xxx	GPLHost	Australia
77.69.181.162	Batelco ADSL Service	Bahrain
180.211.xxx.xxx	Telegraph & Telephone Board	Bangladesh
168.144.xxx.xxx	Softcom, Inc.	Canada
168.144.xxx.xxx	Softcom, Inc.	Canada
217.16.xxx.xxx	PIPNI VPS	Czech Republic
217.146.xxx.xxx	Zone Media UVS/Nodes	Estonia
213.55.99.74	Ethio Telecom	Ethiopia
80.156.xxx.xxx	Gamma International GmbH	Germany
37.200.xxx.xxx	JiffyBox Servers	Germany
178.77.xxx.xxx	HostEurope GmbH	Germany
119.18.xxx.xxx	HostGator	India
119.18.xxx.xxx	HostGator	India
118.97.xxx.xxx	PT Telkom	Indonesia
118.97.xxx.xxx	PT Telkom	Indonesia
103.28.xxx.xxx	PT Matrixnet Global	Indonesia
112.78.143.34	Biznet ISP	Indonesia
112.78.143.26	Biznet ISP	Indonesia
117.121.xxx.xxx	GPLHost	Malaysia
187.188.xxx.xxx	Iusacell PCS	Mexico
201.122.xxx.xxx	UniNet	Mexico
164.138.xxx.xxx	Tilaa	Netherlands
164.138.28.2	Tilaa	Netherlands
78.100.57.165	Qtel – Government Relations	Qatar
195.178.xxx.xxx	Tri.d.o.o / Telekom Srbija	Serbia
117.121.xxx.xxx	GPLHost	Singapore
217.174.229.82	Ministry of Communications	Turkmenistan
72.22.xxx.xxx	iPower, Inc.	United States
166.143.xxx.xxx	Verizon Wireless	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
183.91.xxx.xxx	CMC Telecom Infrastructure Company	Vietnam

Disclaimer

- ***Malware attribution is a very complicated problem***
- ***Can be based solely on***
  - Binary features
  - Behavioral analysis / implementation of techniques
- ***Hence the "allegedly this", "allegedly that".***
- ***Problem → malware analysis is hard because they are made to be understood by computers***
  - What if we had something made to be understood by humans?

The Hacking Team (HT) case

- ***The Italian group Hacking Team exposed***
  - Significant player in the market
  - Main product: Galileo RCS
    - remote control system
  - 400 GBs of exfiltrated data
    - Malware samples (computer can parse)
    - Source code in GIT repos (human can sort of parse)
    - Billing and emails (human can fully parse)
- ***Key question:***
  - what technology were they using, and to whom where they selling it?
  - Is the technology any good really?

Governmental malware: is it that sophisticated?

- ***FinSpy malware is not particularly complex***
  - No polymorphism
  - Delivery mechanism == email attachment
- ***What is the actual sophistication of the technology developed and deployed by these players?***
- ***From the HT dump:***

Invisibility test - Win7 32bit + Norton Security (Word Exploit): Exploit worked good, but after the infection the scout got detected at each logon and at each synchronization. The customer got distracted by [redacted] while I added the scout to the Norton's whitelist, so it could be upgraded to elite. After that, everything has been ok;

- ***"Good" guy distracts the victim while other guy whitelists the malware***
  - .. Lame
  - Is this really the nature of the game, or is there more to it?

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Additional Readings

- ***First academic paper mentioning 0-days (that I know of)***
  - O. Arkin. "Tracing Hackers: Part 1." *Computers and Security*, 2002.
- ***Insight in the market***
  - C. Miller. The Legitimate Vulnerability Market. *Workshop on Economics of Information Security, 2006*.
- ***Some different perspectives on cybercrime***
  - Nick Nykodym et al. "Criminal profiling and insider cyber crime." *Digital Investigation*, 2005.
  - D. Florencio et al. "Sex, Lies and Cybercrime Surveys". *Workshop on Economics of Information Security, 2006*.
  - J. Franklin. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants". *ACM Conference on Computer and Communication Security*, 2007
- ***A tutorial on the difficulty of attribution***
  - M. Marquis-Boire. Big Game Hunting: The Peculiarities of Nation-State Malware Research. *BlackHat USA, 2015.*