Session 1
Introduction

Security Summer School

ACS/Ixia/Hexcellents

Motivation

- Why do we need security?
- What could possibly go wrong?
- What's the worse that could happen?

Security against whom?

Security against whom?

- Neighbors that sniff your Wi-Fi

Security against whom?

- Neighbors that sniff your Wi-Fi
- Script kiddies that try to bruteforce your SSH login

Security against whom?

- Neighbors that sniff your Wi-Fi
- Script kiddies that try to bruteforce your SSH login
- Disgruntled employees that know your network topology and all running services (and the ones that are not updated)

Security against whom?

- Neighbors that sniff your Wi-Fi
- Script kiddies that try to bruteforce your SSH login
- Disgruntled employees that know your network topology and all running services (and the ones that are not updated)
- Nation state actors that have exploits to undisclosed vulnerabilities in software you use

Security against whom?

- Neighbors that sniff your Wi-Fi
- Script kiddies that try to bruteforce your SSH login
- Disgruntled employees that know your network topology and all running services (and the ones that are not updated)
- Nation state actors that have exploits to undisclosed vulnerabilities in software you use
- Agencies that use quantum computers to break encryption

Security against whom?

- Neighbors that sniff your Wi-Fi
- Script kiddies that try to bruteforce your SSH login
- Disgruntled employees that know your network topology and all running services (and the ones that are not updated)
- Nation state actors that have exploits to undisclosed vulnerabilities in software you use
- Agencies that use quantum computers to break encryption

Security is relative: you need to establish the Threat Model.

Hacking timeline

Hacking timeline

- 1990s: phone hacking (phreaking)

Hacking timeline

- 1990s: phone hacking (phreaking)
- Early 2000s: hacking for fame or hacking to see the world burn (defacements, viruses)

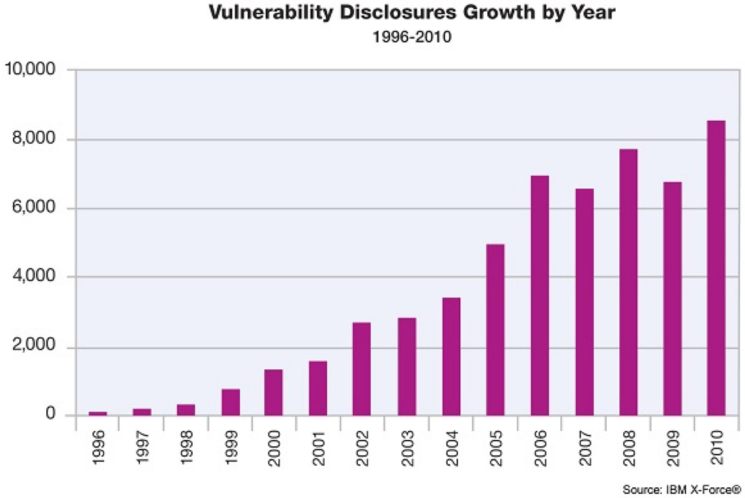
Hacking timeline

- 1990s: phone hacking (phreaking)
- Early 2000s: hacking for fame or hacking to see the world burn (defacements, viruses)
- Late 2000s: financially, philosophically, politically or morally motivated (spam, botnets, hacktivism)

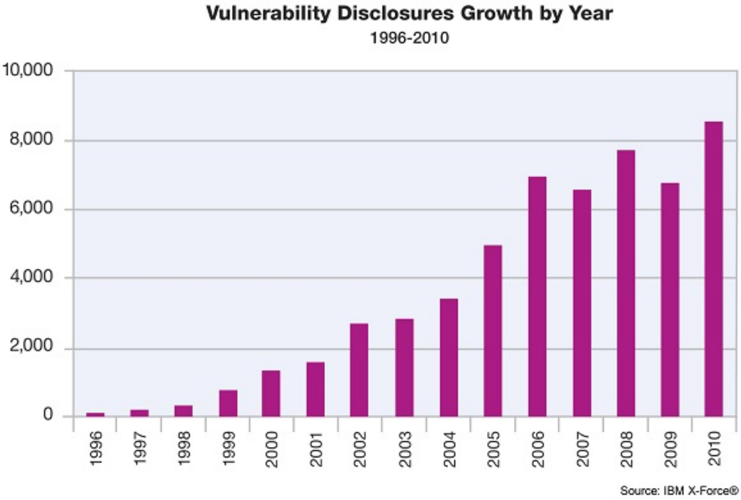
Hacking timeline

- 1990s: phone hacking (phreaking)
- Early 2000s: hacking for fame or hacking to see the world burn (defacements, viruses)
- Late 2000s: financially, philosophically, politically or morally motivated (spam, botnets, hacktivism)
- Now: cyberwarfare, intellectual property theft, Crimeware as a Service

Vulnerabilities on the rise



Vulnerabilities on the rise

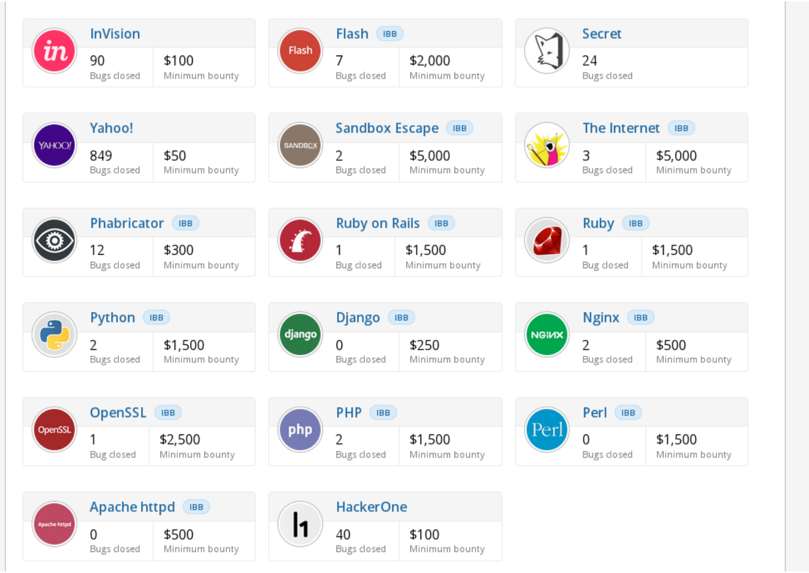


Security should be of paramount importance but we aren't getting safer.

The good

- Companies have started realizing how important security is
- These now offer bug bounty programs
- Yearly contests award researchers money for exploits in common software
- Hackers can try out their skills legally and make $$$$

HackerOne



InVision
90 Bugs closed
$100 Minimum bounty

Flash IBB
7 Bugs closed
$2,000 Minimum bounty

Secret
24 Bugs closed

Yahoo!
849 Bugs closed
$50 Minimum bounty

Sandbox Escape IBB
2 Bugs closed
$5,000 Minimum bounty

The Internet IBB
3 Bugs closed
$5,000 Minimum bounty

Phabricator IBB
12 Bugs closed
$300 Minimum bounty

Ruby on Rails IBB
1 Bug closed
$1,500 Minimum bounty

Ruby IBB
1 Bug closed
$1,500 Minimum bounty

Python IBB
2 Bugs closed
$1,500 Minimum bounty

Django IBB
0 Bugs closed
$250 Minimum bounty

Nginx IBB
2 Bugs closed
$500 Minimum bounty

OpenSSL IBB
1 Bug closed
$2,500 Minimum bounty

PHP IBB
2 Bugs closed
$1,500 Minimum bounty

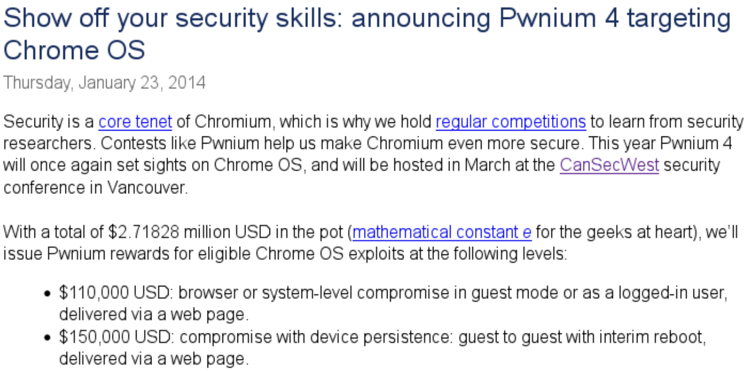
Perl IBB
0 Bugs closed
$1,500 Minimum bounty

Apache httpd IBB
0 Bugs closed
$500 Minimum bounty

HackerOne
40 Bugs closed
$100 Minimum bounty

Source: [1]

Pwnium



Show off your security skills: announcing Pwnium 4 targeting Chrome OS

Thursday, January 23, 2014

Security is a core tenet of Chromium, which is why we hold regular competitions to learn from security researchers. Contests like Pwnium help us make Chromium even more secure. This year Pwnium 4 will once again set sights on Chrome OS, and will be hosted in March at the CanSecWest security conference in Vancouver.

With a total of $2.71828 million USD in the pot (mathematical constant e for the geeks at heart), we'll issue Pwnium rewards for eligible Chrome OS exploits at the following levels:

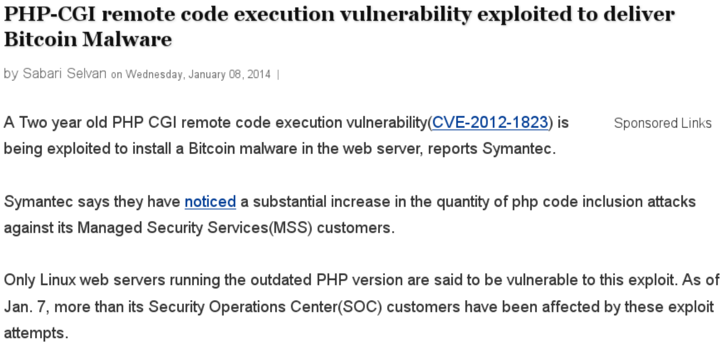
- $110,000 USD: browser or system-level compromise in guest mode or as a logged-in user, delivered via a web page.
- $150,000 USD: compromise with device persistence: guest to guest with interim reboot, delivered via a web page.

Source: [2]

The bad

- Malware
- Ransomware

PHP bitcoin miners



PHP-CGI remote code execution vulnerability exploited to deliver Bitcoin Malware

by Sabari Selvan on Wednesday, January 08, 2014 |

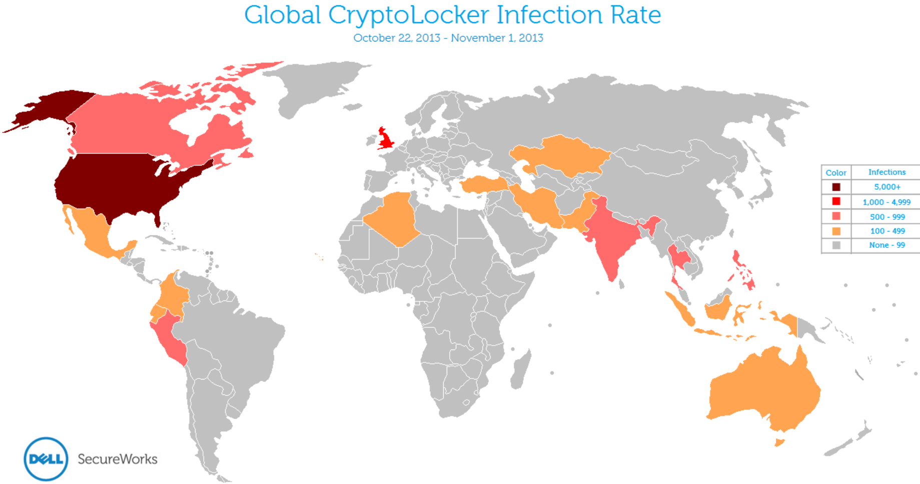
A Two year old PHP CGI remote code execution vulnerability(CVE-2012-1823) is being exploited to install a Bitcoin malware in the web server, reports Symantec.

Symantec says they have noticed a substantial increase in the quantity of php code inclusion attacks against its Managed Security Services(MSS) customers.

Only Linux web servers running the outdated PHP version are said to be vulnerable to this exploit. As of Jan. 7, more than its Security Operations Center(SOC) customers have been affected by these exploit attempts.

Source: [3]

Cryptolocker

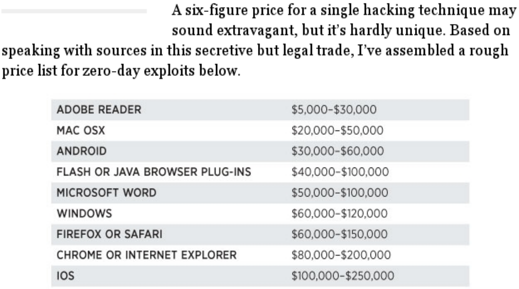


Source: [4]

The ugly

- Security is now part of warfare
- Stuxnet was the first to be termed a cyberweapon
- Based on four 0-day vulnerabilities

0-day market

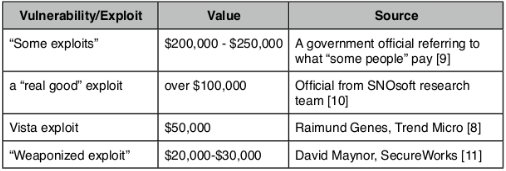


A six-figure price for a single hacking technique may sound extravagant, but it's hardly unique. Based on speaking with sources in this secretive but legal trade, I've assembled a rough price list for zero-day exploits below.

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

Source: [5]

0-day market



Vulnerability/Exploit	Value	Source
"Some exploits"	$200,000 - $250,000	A government official referring to what "some people" pay [9]
a "real good" exploit	over $100,000	Official from SNOsoft research team [10]
Vista exploit	$50,000	Raimund Genes, Trend Micro [8]
"Weaponized exploit"	$20,000-$30,000	David Maynor, SecureWorks [11]

Source: [6]

Where to start?

- “To know your Enemy, you must become your Enemy.” - Sun Tzu
- To be able to secure first learn how to attack

Course Outline

- Insight through OS interaction
- Diving into assembly
- Executable analysis (static & dynamic)
- Vulnerability discovery (manual)
- CTF I
- Vulnerability discovery (fuzzing)
- Weaponizing vulnerabilities
- Vulnerability prevention
- CTF II

Attack surface in dynamic analysis

- Loader, dynamic linker, libraries
- Files, sockets, shared memory
- Network communication
- Standard file descriptors
- System & library calls
- Address space
- Runtime environment

Demo time (after tutorials)

- We have a backdoored server
- We developed an exploit
- How does it work?

Resources

1. hackerone.com
2. blog.chromium.org/2014/01/show-off-your-security-skills.html
3. ehackingnews.com/2014/01/php-cgi-remote-code-execution.html
4. secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware
5. forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-expl
6. securityevaluators.com/knowledge/papers/0daymarket.pdf
7. www.zerodayinitiative.com
8. www.disclose.tv/action/viewvideo/157242/BBC_Horizon__Defeating_the_Hackers_HD