https://cs155.Stanford.edu

CS155

Computer Security

Course overview

The computer security problem

- **Lots of buggy software**
- **Social engineering is very effective**
- **Money can be made from finding and exploiting vulns**.

1. Marketplace for vulnerabilities
2. Marketplace for owned machines (PPI)
3. Many methods to profit from owned machines

current state of computer security

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2018

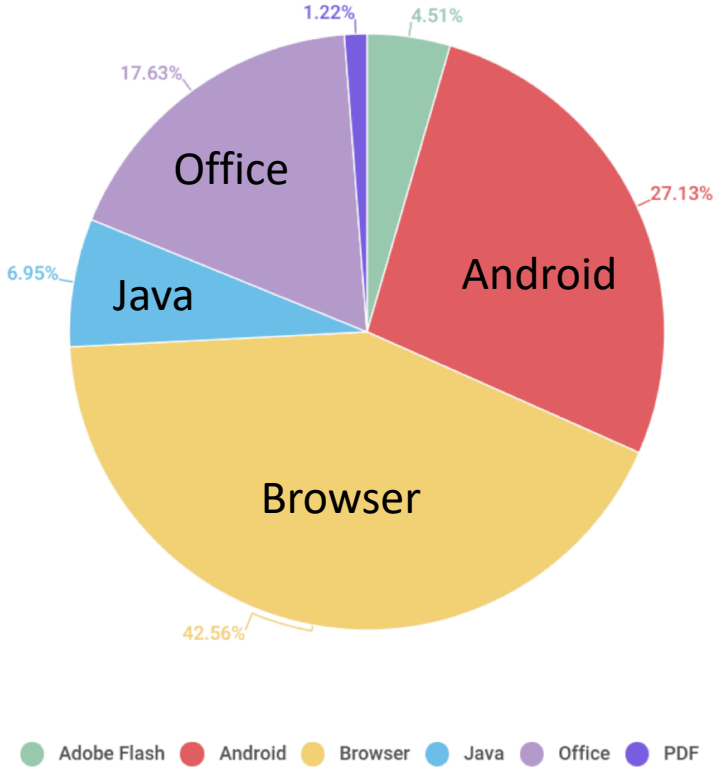
Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2019 All Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	950
2	Android	Google	OS	611
3	Ubuntu Linux	Canonical	OS	494
4	Enterprise Linux Server	Redhat	OS	394
5	Enterprise Linux Workstation	Redhat	OS	378
6	Enterprise Linux Desktop	Redhat	OS	369
7	Firefox	Mozilla	Application	333
8	Acrobat Reader Dc	Adobe	Application	286
9	Acrobat Dc	Adobe	Application	286
10	Windows 10	Mic[illegible]	OS	255

Screenshot

source: https://www.cvedetails.com/top-50-products.php?year=2018

Vulnerable applications being exploited



Source: Kaspersky Security Bulletin 2017

Introduction

Sample attacks

Why own client machines:

1. IP address and bandwidth stealing

Attacker's goal: look like a random Internet user

Use the IP address of infected machine or phone for:

- **Spam** (e.g. the storm botnet)

  Spamalytics: 1:12M pharma spams leads to purchase
  1:260K greeting card spams leads to infection

- **Denial of Service:** Services: 1 hour (20$), 24 hours (100$)

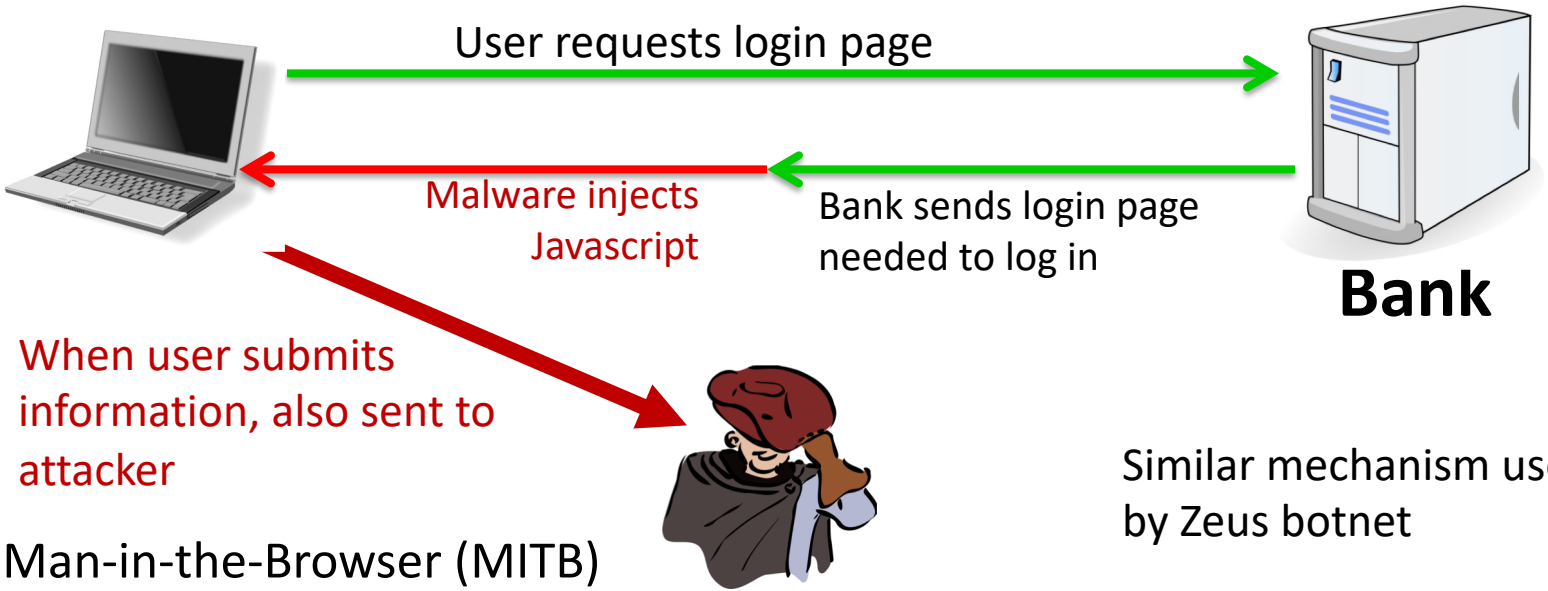
- **Click fraud** (e.g. Clickbot.a)

Why own machines:

2. Steal user credentials, crypto miners

keylog for banking passwords, web passwords, gaming pwds.

Example: SilentBanker (and many like it)



Man-in-the-Browser (MITB)

Similar mechanism used by Zeus botnet

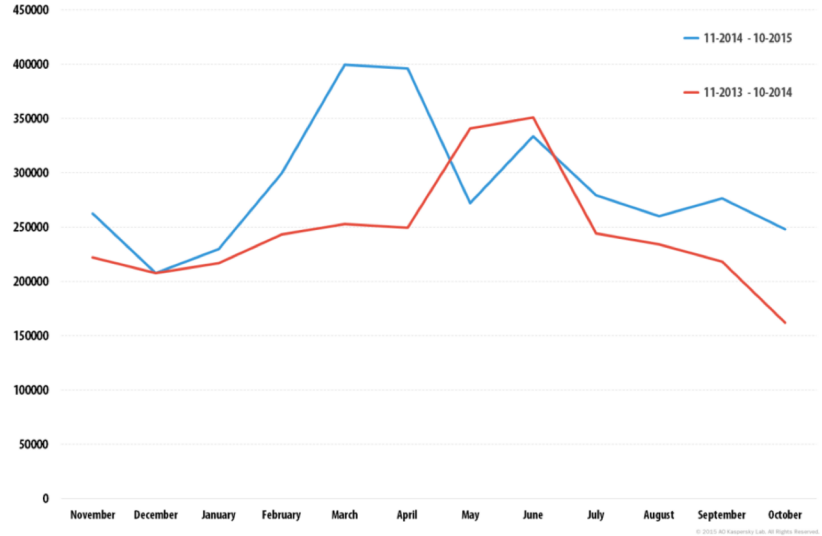
Lots of financial malware

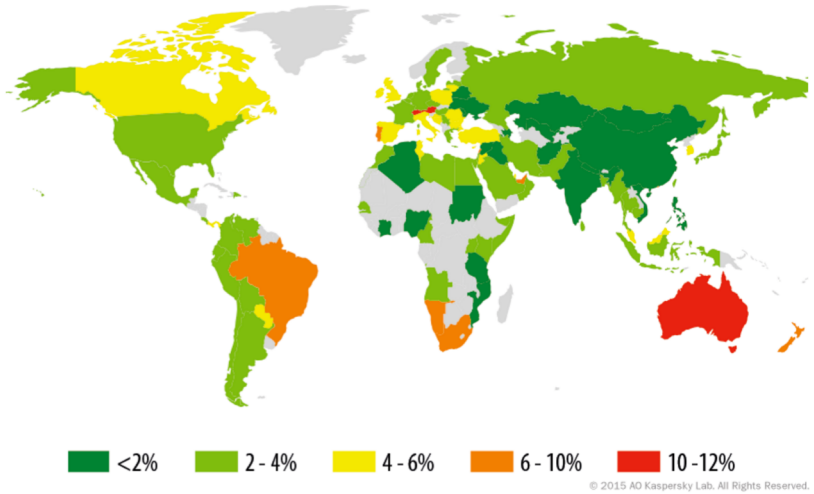
1	Trojan-Spy.Win32.Zbot
2	Trojan.Win32.Nymaim
3	Trojan.Win32.Neurevt
4	SpyEye
5	Trojan-Banker.Win32.Gozi
6	Emotet
7	Caphaw
8	Trickster
9	Cridex/Dridex
10	Backdoor.Win32.Shiz

- records banking passwords via keylogger
- spread via spam email and hacked web sites
- maintains access to PC for future installs

Source: Kaspersky Security Bulletin 2017

Users attacked: stats





≈ 300,000 users/month worldwide

A worldwide problem

Source: Kaspersky Security Bulletin 2015

Why own machines: 3. **Ransomware**

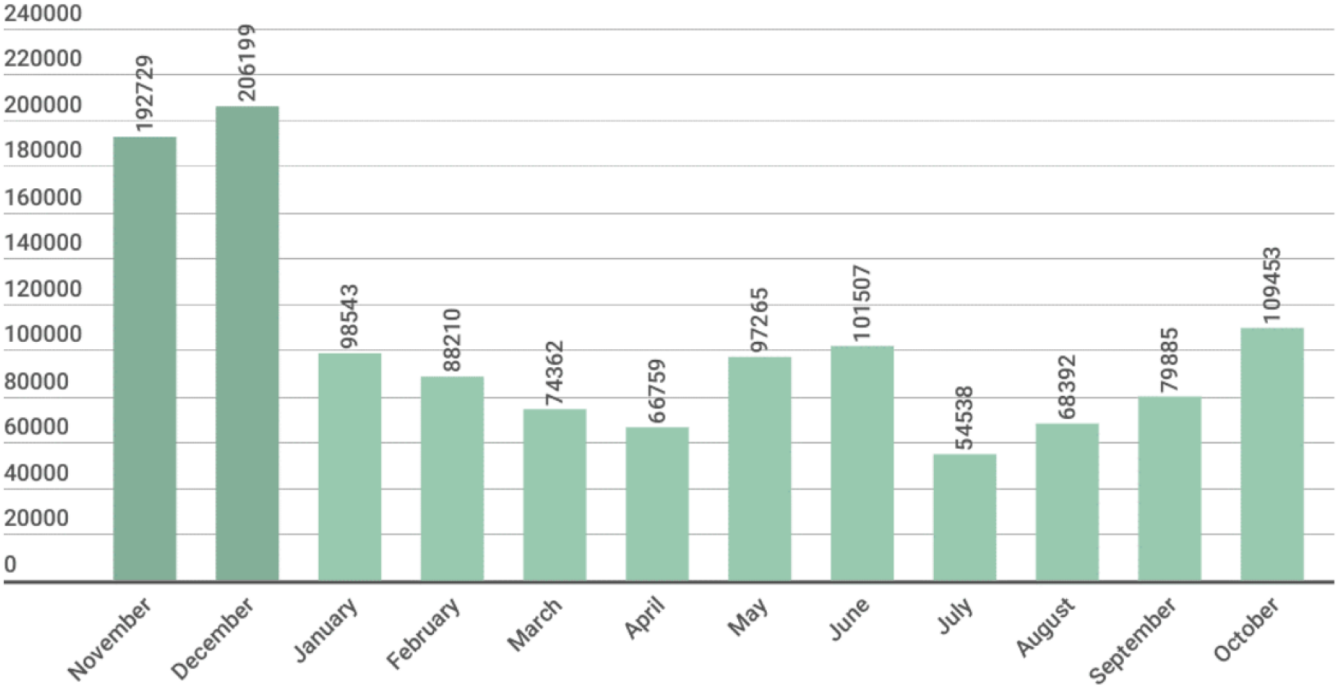
	Name	% of attacked users**
1	WannaCry	7.71
2	Locky	6.70
3	Cerber	5.89
4	Jaff	2.58
5	Cryrar/ACCDFISA	2.20
6	Spora	2.19
7	Purgen/GlobeImposter	2.11
8	Shade	2.06
9	Crysis	1.25
10	CryptoWall	1.13

a worldwide problem

- Worm spreads via a vuln. in SMB (port 445)
- Apr. 14, 2017: Eternalblue vuln. released by ShadowBrokers
- May 12, 2017: Worm detected (3 weeks to weaponize)

WannaCry ransomware

Ransomware in 2017: # users attacked



Source: Kaspersky Security Bulletin 2017

Why own machines:

4. Spread to isolated systems

Example: **Stuxtnet**

Windows infection ⇒

Siemens PCS 7 SCADA control software on Windows ⇒

Siemens device controller on isolated network

More on this later in course

Server-side attacks

- Data theft: credit card numbers, intellectual property
  - Example: Equifax (July 2017), ≈ 143M "customer" data impacted
    - Exploited known vulnerability in Apache Struts (RCE)
  - Many similar (smaller) attacks since 2000
- Political motivation:
  - DNC, Tunisia Facebook (Feb. 2011), GitHub (Mar. 2015)
- Infect visiting users

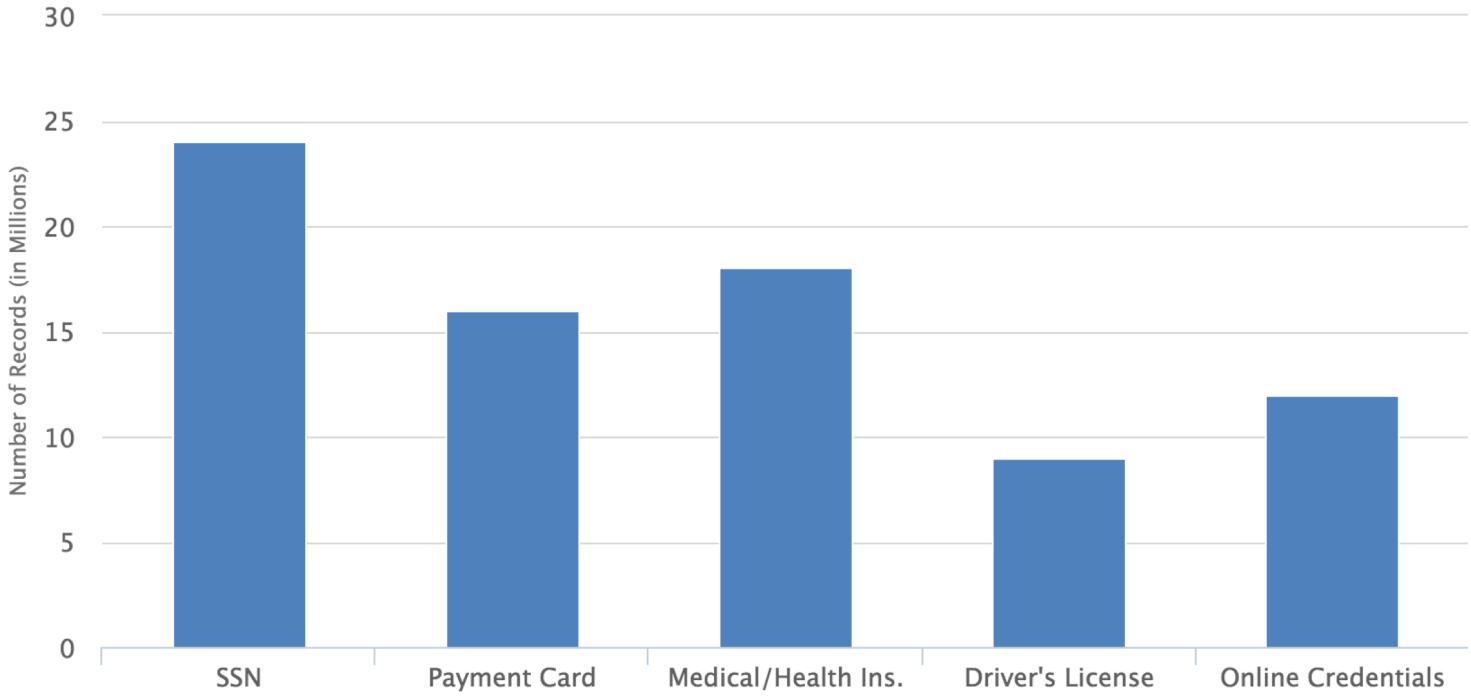
Infecting visiting users: Mpack

- PHP-based tools installed on compromised web sites
  - Embedded as an iframe on infected page
  - Infects browsers that visit site

- Features
  - management console provides stats on infection rates
  - Sold for several 100$
  - Customer care can be purchased, one-year support contract

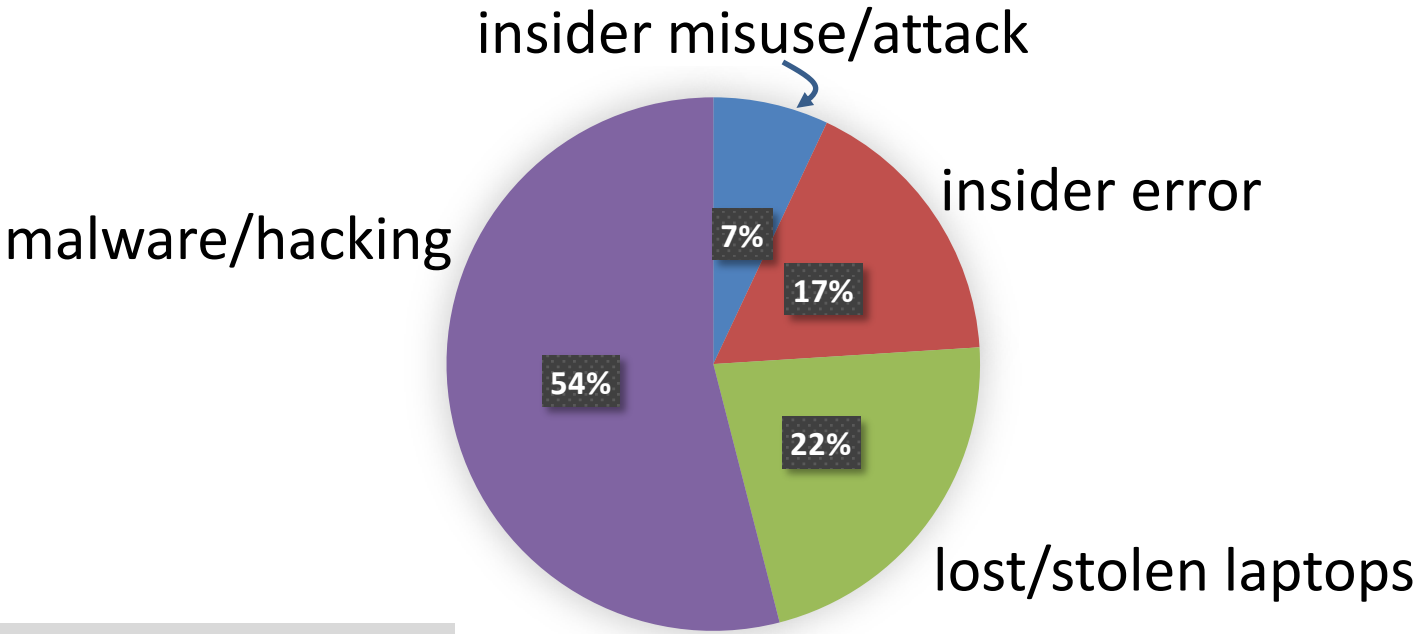
- Impact: 500,000 infected sites (compromised via SQL injection)
  - Several defenses: e.g. Google safe browsing

Types of data stolen (2012-2015)



Source: California breach notification report, 2015

How companies lose data



How do we have this data?

Source: California breach notification report, 2016

Insider attacks: example

Hidden trap door in Linux (nov 2003)

- Allows attacker to take over a computer
- Practically undetectable change (uncovered via CVS logs)

Inserted line in wait4()

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
            retval = -EINVAL;
```

Looks like a standard error check, but …

See: http://lwn.net/Articles/57135/

Many more examples

- Access to SIPRnet and a CD-RW: 260,000 cables ⇒ Wikileaks
- SysAdmin for city of SF government.
  Changed passwords, locking out city from router access
- Inside logic bomb took down 2000 UBS servers

⋮

Can security technology help?

Introduction

The Marketplace for Vulnerabilities

Marketplace for Vulnerabilities

Option 1: bug bounty programs (many)

- Google Vulnerability Reward Program: up to $31,337
- Microsoft Bounty Program: up to $100K
- Apple Bug Bounty program: up to $200K (secure boot firmware)
- Pwn2Own competition: $15K

Option 2:

- Zerodium: up to $2M for iOS, $500K for Android (2019)
- … many others

Example: Mozilla

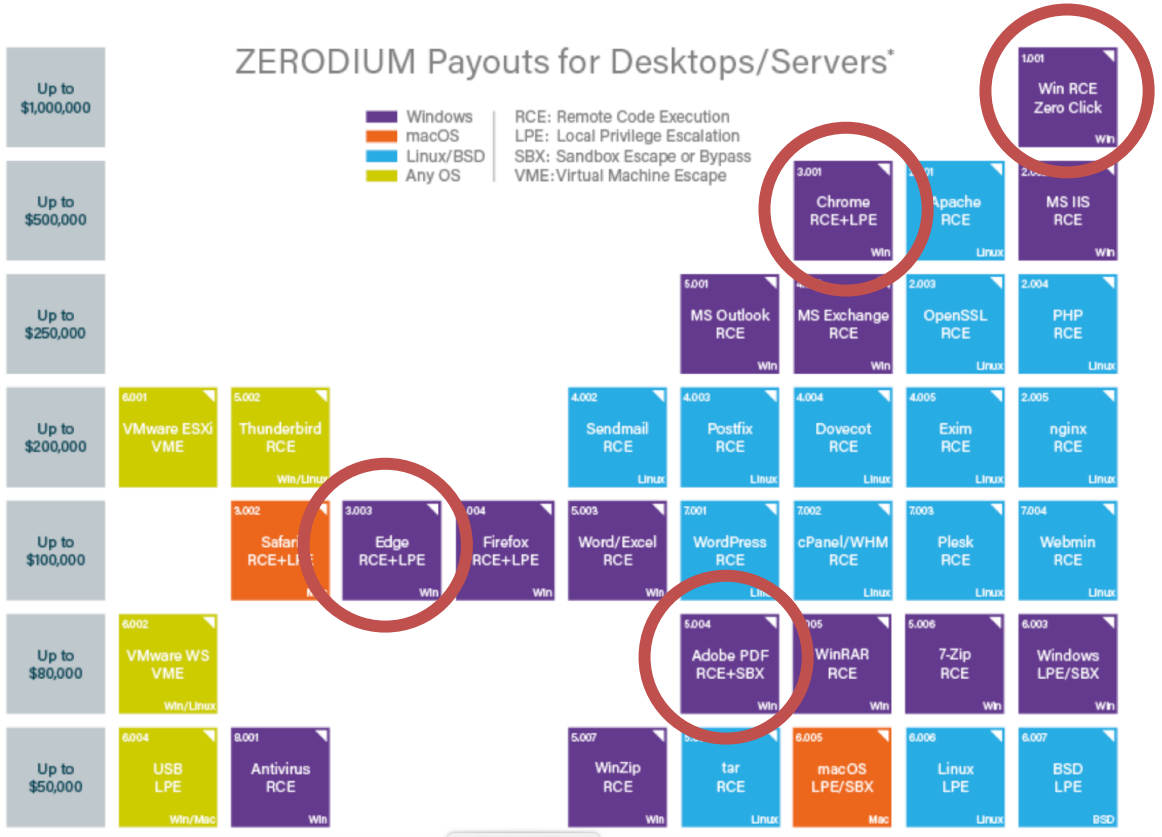
Novel vulnerability and exploit, new form of exploitation or an exceptional vulnerability	High quality bug report with clearly exploitable critical vulnerability$_1$	High quality bug report of a critical or high vulnerability$_2$	Minimum for a high or critical vulnerability$_3$	Medium vulnerability
$10,000+	$7,500	$5,000	$3,000	$500 - $2500

Marketplace for Vulnerabilities

RCE: remote code execution

LPE: local privilege escalation

SBX: sandbox escape



Source: Zerodium payouts

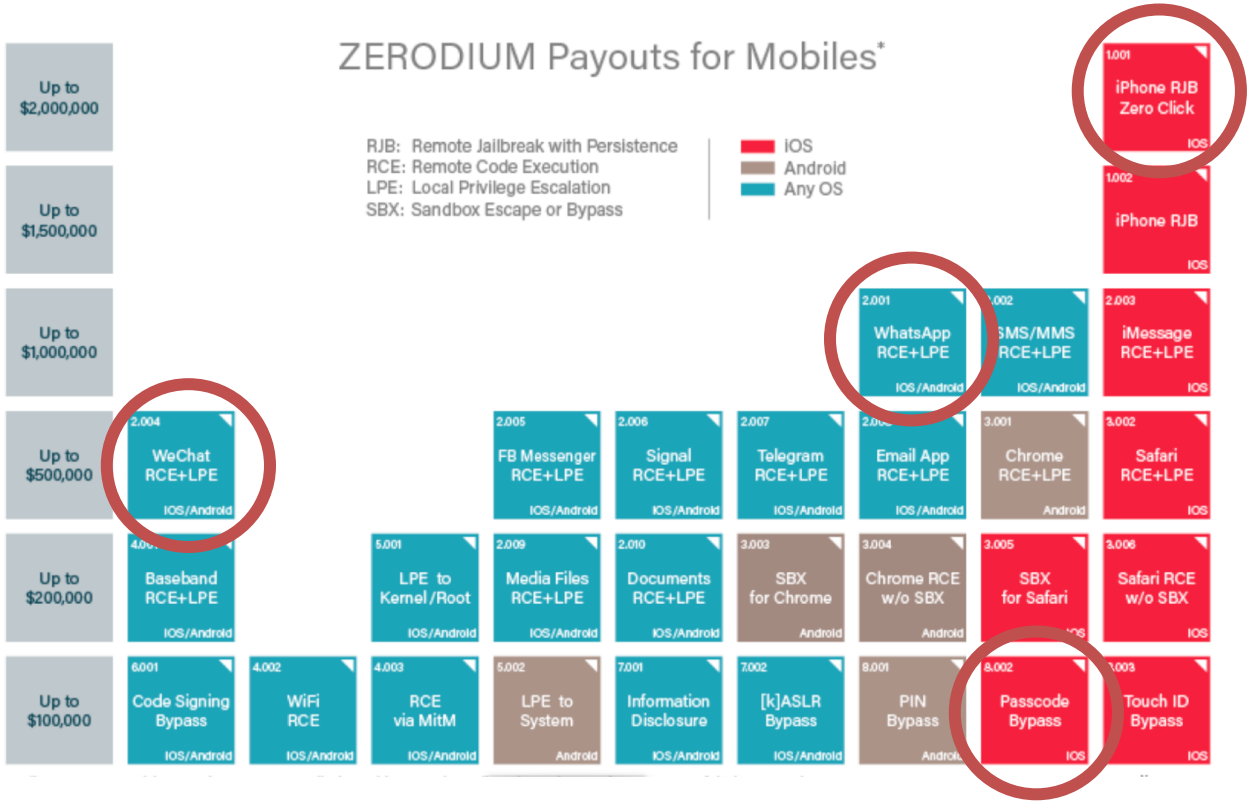
Marketplace for Vulnerabilities

RCE: remote code execution

LPE: local privilege escalation

SBX: sandbox escape

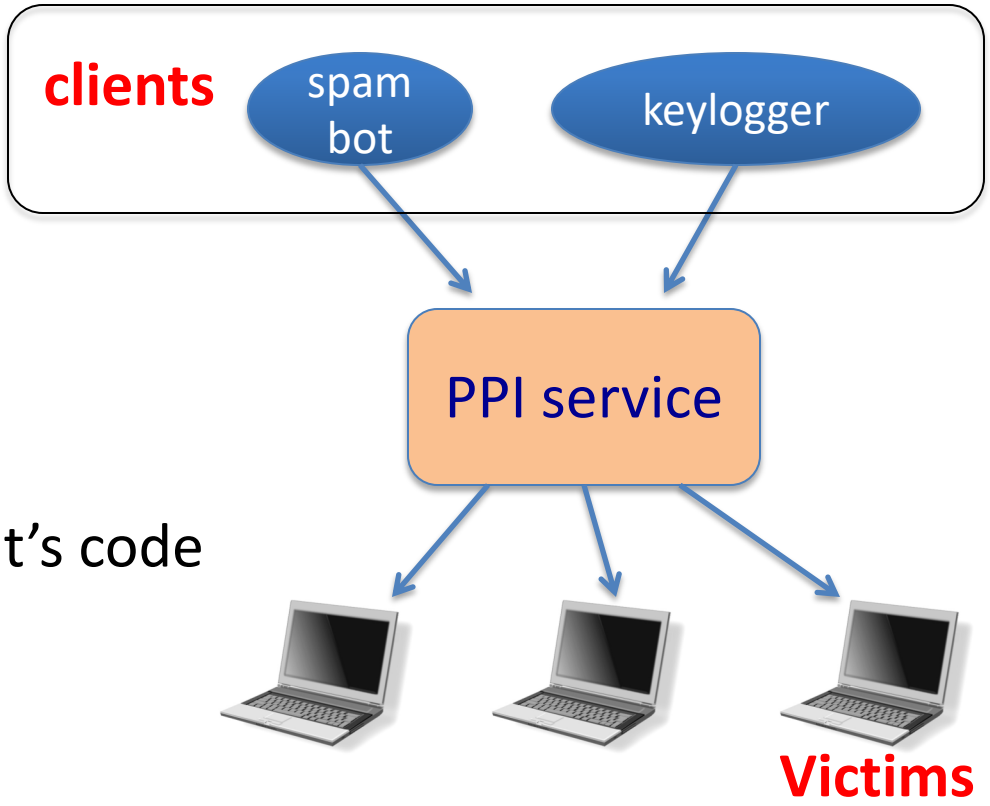
RJB: remote jailbreak



Source: Zerodium payouts

Marketplace for owned machines

Pay-per-install (PPI) services

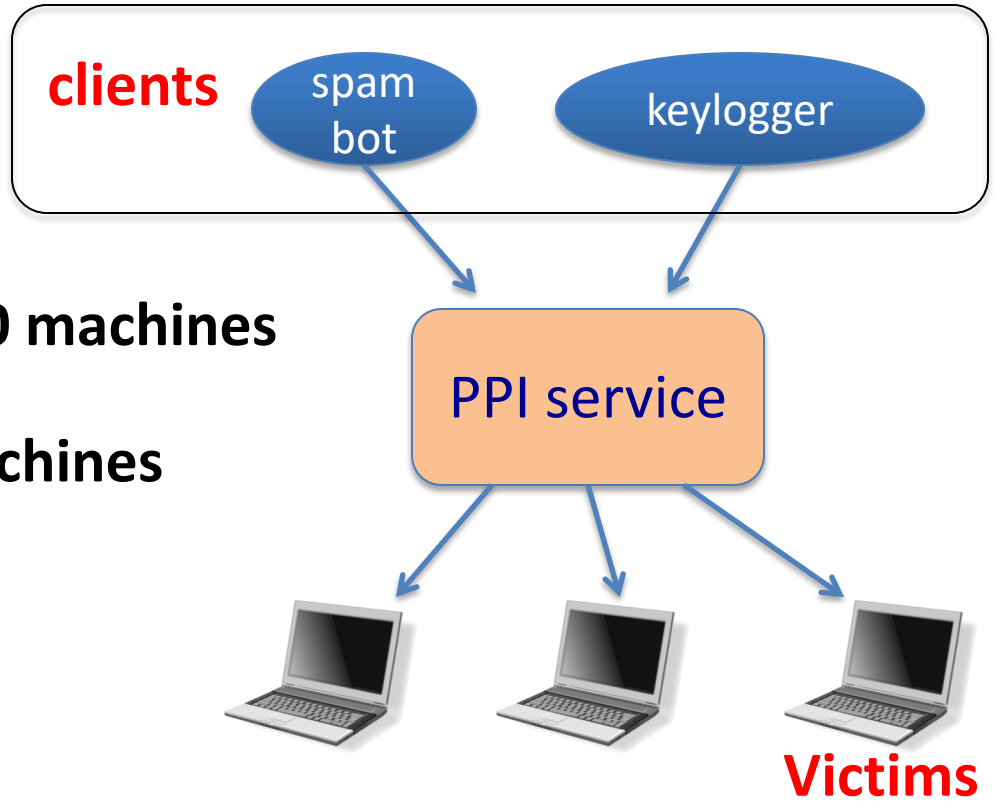


PPI operation:

1. Own victim's machine
2. Download and install client's code
3. Charge client

Source: Cabalerro et al. (www.icir.org/vern/papers/ppi-usesec11.pdf)

Marketplace for owned machines



Cost: **US - 100-180$ / 1000 machines**

Asia - 7-8$ / 1000 machines

Source: Cabalerro et al. (www.icir.org/vern/papers/ppi-usesec11.pdf)

This course

Goals:

- Be aware of exploit techniques
- Learn to defend and avoid common exploits
- Learn to architect secure systems

This course

Part 1: **basics** (architecting for security)

- Securing apps, OS, and legacy code
  Isolation, authentication, and access control

Part 2: **Web security** (defending against a web attacker)

- Building robust web sites, understand the browser security model

Part 3: **network security** (defending against a network attacker)

- Monitoring and architecting secure networks.

Part 4: **securing mobile applications**

Don’t try this at home !

Ken Thompson’s clever Trojan