



# 软件安全性

公关 Yves ROUDIER I3S博士–

CNRS – UCA

[Yves.Roudier@unice.fr](mailto:Yves.Roudier@unice.fr)

[Yves.Roudier@i3s.unice.fr](mailto:Yves.Roudier@i3s.unice.fr)

# 软件安全性

- 这是关于软件安全性的入门课程
  - 高级概念
  - 某些攻击和防护方法的动手经验
- 我们还将在某种程度上考虑网络和硬件安全性
  - 如今，软件是分布式的，移动的或嵌入式的。
- 现在您知道如何编写代码，我们将看到如何破坏代码以及如何保护代码！
  - 了解软件漏洞
  - 安全需求工程和安全体系结构的概念

# 一句警告

- 不要在别人的系统上这样做！不要在Polytec h系统上执行此操作...
- 不要在野外这样做，既不是为了娱乐，也不是为了牟利！
- 骇客/破解是非法的（而且通常是不道德的）
- 本课程讨论漏洞，以使您了解必须对抗安全软件的攻击媒介
- ...您已经被警告过！
- *Le contenu de cet enseignement*成为无约束力的教学法。吹捧有用的儿子继续领导干部的公开竞争！

# 增强安全意识

- **理论**：攻击如何进行，软件保护的原理和机制是什么，等等。
- **实践**：进行一些攻击，编写安全代码，操纵安全库和用于安全测试的工具
- **心态**：学会以攻击者的身份思考，而不仅仅是以开发人员的身份思考：  
您需要了解如何破坏系统，然后才能创建安全的设计

# ( 暂定 ) 课程大纲

- 恶意软件和攻击 : 简介
- 软件漏洞1 : Web应用
- 软件漏洞2 : 低级别攻击
- 安全软件开发生命周期
  - 安全要求 , 风险评估和模型驱动的安全体系结构工程 , 密码学入门
- 安全编程
  - 安全目标和体系结构 , 访问控制 , 安全性和密码库
- 渗透测试 ( 安全测试 ) : 逆向工程 , 静态和动态分析
- 安全执行环境 , 可信计算 ( 完整性和机密性 ) , 安全软件部署

# 关于课程

- 幻灯片和实验室：在LMS Moodle ( Securite logicielle-EIIN727 ) 上可用
- 等级
  - 书面评估 ( 60分钟 )
    - 10月6 : 30%
    - 十二月1<sup>st</sup> : 40%
  - 论文介绍 : 30%
    - 论文将由3-4名学生组成
- 实验室不会评分
- 通讯技术
  - 通过Slack或电子邮件联系
  - 首选虚拟会议 ( COVID-19... )

# 夺旗（CTF）比赛

- 在线或本地CTF
  - 密码：2021年1月



# 完成本课程后...

- 卡斯帕
  - [https://www.dropbox.com/s/d5y2wxq4ej3a2on/CASPAR.pdf](https://www.dropbox.com/s/d5y2wxq4ej3a2on/CASPAR.pdf?dl=0)
  - SI5 /硕士2 ( 学徒制 )
- 安全课程：
  - 密码学与安全
  - 网络安全
  - 密码学
  - 安全和隐私3.0
  - Sécurité dans les réseaux
  - 安全应用程序网站

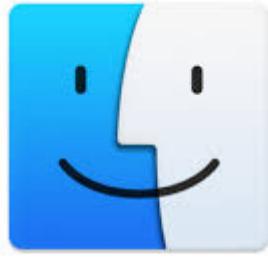
# 安全性：您为什么要关心？

- 安全影响我们的日常生活
- 您必须成为具有安全意识的用户
  - 使用软件时做出明智而明智的决定
- 您想成为一名具有安全意识的开发人员或安全顾问
  - 设计和构建安全的软件和系统
- 您可能想成为一名安全研究员
  - 发现安全漏洞并提出原始解决方案

# 安全性难以捕捉

- 网络安全
  - 周边保护（身份验证及更多）
  - 保护通讯
- 系统安全性
  - 安全策略（权限管理，访问控制/使用）
- 硬体安全性
  - 对处理器和内存的物理攻击
- 软件安全性
  - 软件漏洞
  - 信息流保护
  - 知识产权保护（模糊处理，指纹识别...）

# 软件无处不在（每个软件？）



Mac OS



操作系统

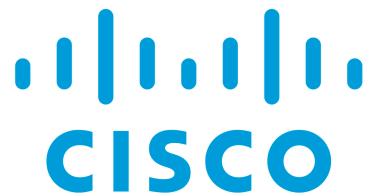


本机应用



网络应用

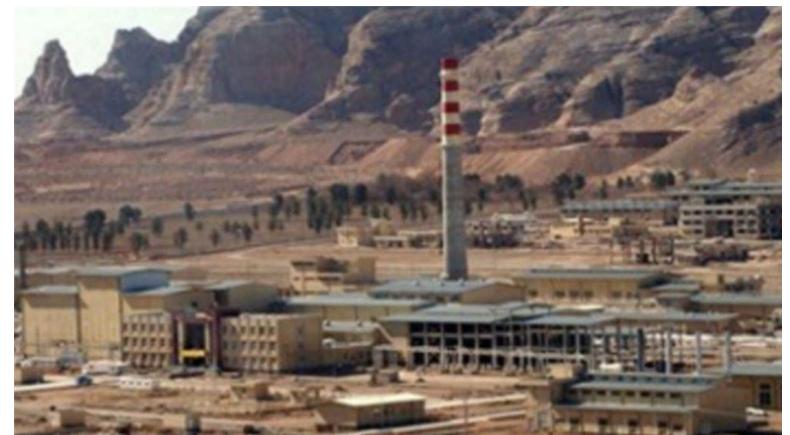
# 软件无处不在（ 每个软件？ ）



网络堆栈



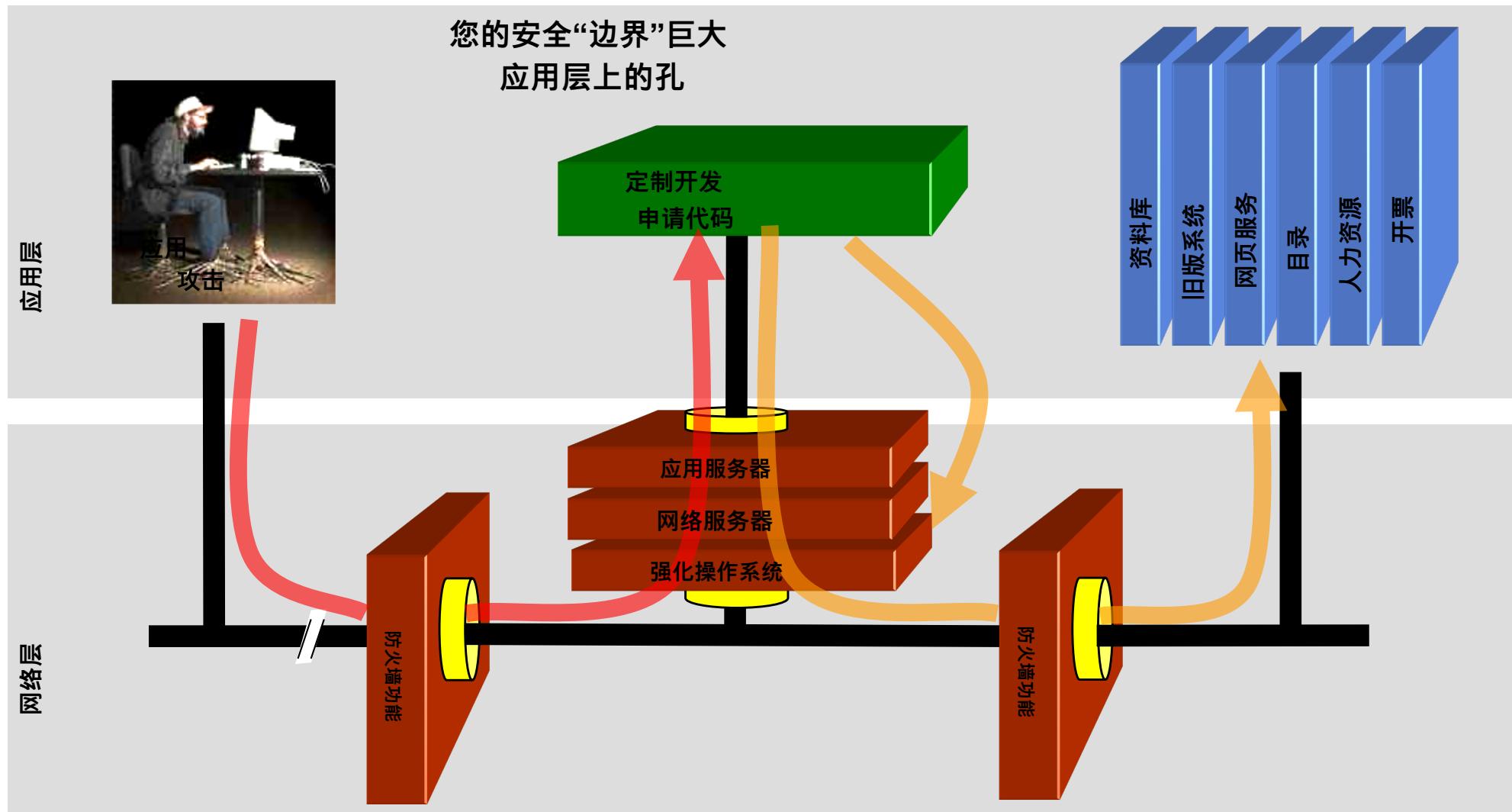
安全系统（ 智能卡，防火墙 ）



网络物理系统（ 物联网，车辆，工厂 ）

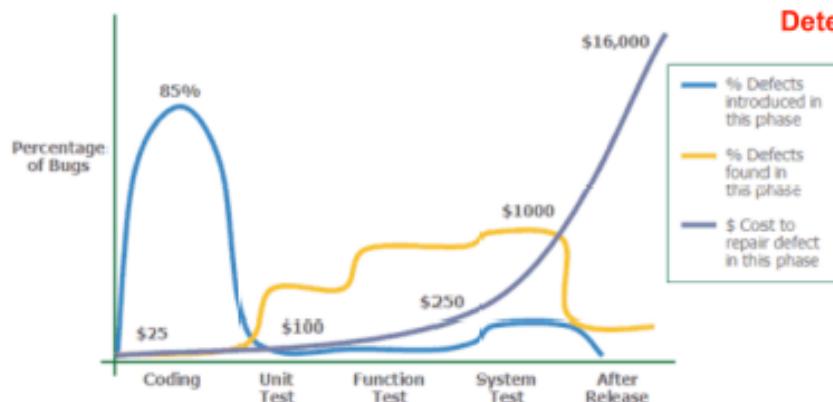
# 线条模糊：您的代码是安全的一部分

## 周长



# 软件与安全工程

- Multiple actors
- Separation of responsibilities
- Secure SDLC



"applied software measurement"  
Capers Jones 1996



# 易受攻击的软件

- 计算机系统仍然存在许多漏洞
  - 词汇：人为错误->错误（错误或恶意访问）->安全失败（漏洞）->利用（妥协）
- 技术因素
  - 太复杂了！
  - 错误的配置与逻辑故障
- 组织因素
  - 安全=成本中心！
  - 截止压力
- 人为因素
  - 设计师心态
  - 环境

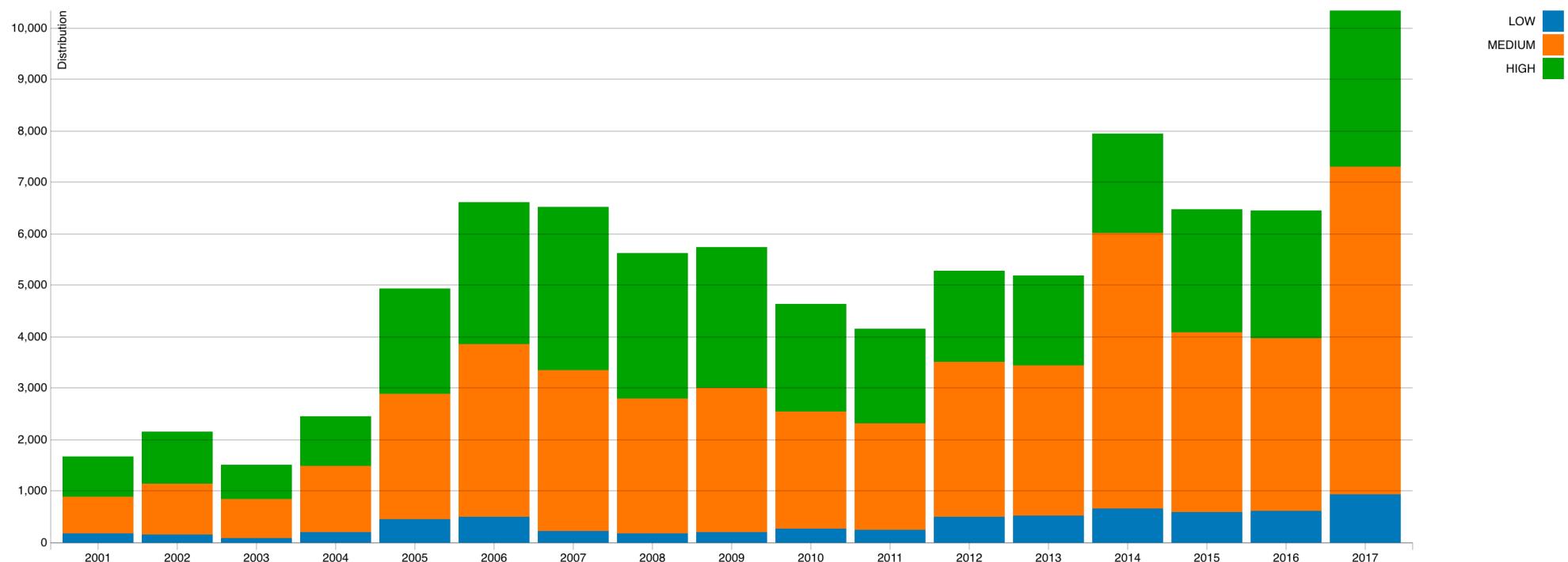
布鲁斯·施耐尔 (*Bruce Schneier*) 的法律 (根据科里·多克托洛 (*Cory Doctorow*) 的说法)：“任何人都可以发明出如此聪明的安全系统，以至于他或她都无法想像破坏它的方法。”

# 易受攻击的软件

- 剥削与远程访问一样古老
  - 随着计算机系统无处不在的主要问题
  - 暴露于远程访问（例如互联网）会导致剥削
  - 1973年-鲍勃·梅特卡夫（Bob Metcalfe's）*RFC 602*：“小心地将烟囱挂在丝袜上”（关于ARPANET中的安全性问题）
    - “许多人仍然使用容易猜到的密码：他们的名字，名字缩写，他们的主机名向后拼写，一串容易按顺序键入的字符”

# 软件缺陷

<https://web.nvd.nist.gov/view/vuln/statistics>

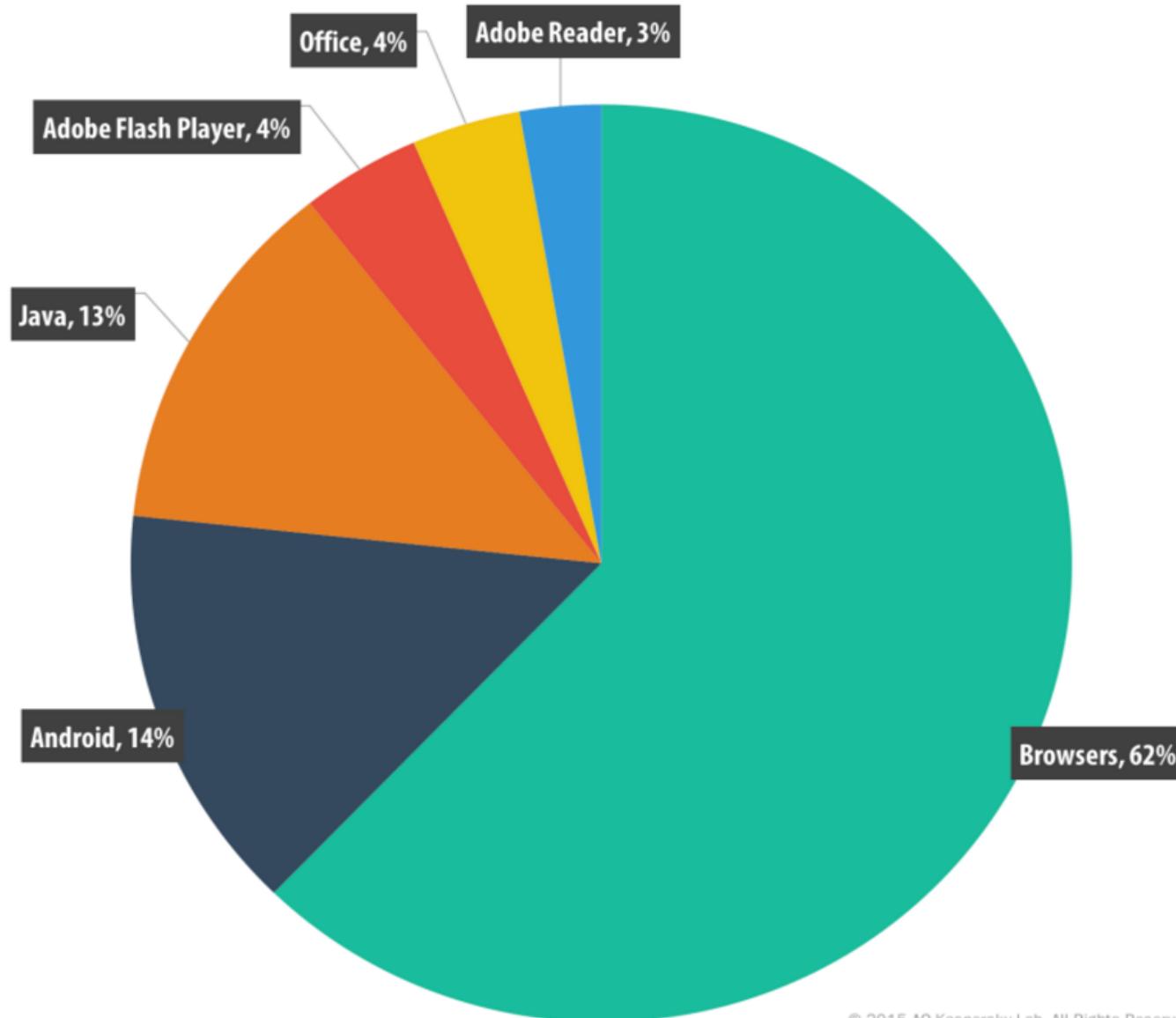


- 随时间变化的CVSS严重性分布

# 漏洞披露 ( 2015 )

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	<a href="#">Mac Os X</a>	<a href="#">Apple</a>	OS	<a href="#">385</a>
2	<a href="#">Iphone Os</a>	<a href="#">Apple</a>	OS	<a href="#">376</a>
3	<a href="#">Flash Player</a>	<a href="#">Adobe</a>	Application	<a href="#">313</a>
4	<a href="#">Air Sdk</a>	<a href="#">Adobe</a>	Application	<a href="#">246</a>
5	<a href="#">AIR</a>	<a href="#">Adobe</a>	Application	<a href="#">246</a>
6	<a href="#">Air Sdk &amp; Compiler</a>	<a href="#">Adobe</a>	Application	<a href="#">246</a>
7	<a href="#">Internet Explorer</a>	<a href="#">Microsoft</a>	Application	<a href="#">231</a>
8	<a href="#">Chrome</a>	<a href="#">Google</a>	Application	<a href="#">187</a>
9	<a href="#">Firefox</a>	<a href="#">Mozilla</a>	Application	<a href="#">178</a>
10	<a href="#">Windows Server 2012</a>	<a href="#">Microsoft</a>	OS	<a href="#">155</a>
11	<a href="#">Ubuntu Linux</a>	<a href="#">Canonical</a>	OS	<a href="#">152</a>
12	<a href="#">Windows 8.1</a>	<a href="#">Microsoft</a>	OS	<a href="#">151</a>

# 易受攻击的应用程序被利用



资料来源：《卡巴斯基安全公告》 2015

# 恶意软件和攻击

# 恶意软件：恶意软件

- 恶意软件=恶意软件（作为攻击媒介的软件）
  - 垃圾邮件
  - 拒绝服务
    - 服务：1小时（20 \$），24小时（100 \$）
  - 点击欺诈
  - 窃取凭证和密码
    - 例如：目标攻击（2013），≈140M CC号码被盗



# 恶意软件 : 恶意软件

- 术语
  - 特洛伊木马 : 允许未经授权的用户远程访问
  - 病毒 : 旨在传播的计算机程序 ( 需要人工干预 )
  - 蠕虫 : 不需要人工干预
  - 广告软件 : 运行应用程序时的广告
  - 间谍软件 : 监视和收集要在没有用户了解/同意的情况下传输给第三方的信息
  - 勒索软件 : 要求勒索以防止数据删除 ( 加密和/或传输到其他磁盘 )
  - 僵尸网络 : 在攻击者控制下的 ( ro ) bot / 僵尸计算机网络 , 用于进行攻击或发送其他媒介

# 恶意软件：一些趋势

- 病毒，蠕虫和僵尸程序如今更加隐秘
  - 2008-2009 Conficker感染了2千1百万个Windows服务器
- 勒索软件正在上升
  - 最初是弱威胁（从软件中恢复了加密密钥）
  - 现在使用最新的非对称加密技术
- 移动恶意软件激增
  - 银行应用程序，特别是
- 从主流网站下载驱动
- 动态且高度混淆的恶意软件
- 浏览器插件
- 误导性应用

# 恶意软件：一些趋势

- 主流网站上的SQL注入
- 恶意广告：用户重定向到恶意网站
- 恶意软件比以往任何时候都更为普遍，导致地下经济
  - “ MPack是以商业软件的形式出售的（售价在500到1000美元之间），并且由其开发人员提供技术支持并对其所利用的软件漏洞进行定期更新。”
  - 多达数百万台计算机的僵尸网络—黑客之间的控制权也存在争议
  - 独特且有针对性的恶意软件样本呈指数增长

# 许多金融恶意软件

- 1 Trojan-Downloader.Win32.Upatre
- 2 Trojan-Spy.Win32.Zbot
- 3 Trojan-Banker.Win32.ChePro
- 4 Trojan-Banker.Win32.Shiotob
- 5 Trojan-Banker.Win32.Banbra
- 6 Trojan-Banker.Win32.Caphaw
- 7 Trojan-Banker.AndroidOS.Faketoken
- 8 Trojan-Banker.AndroidOS.Marcher
- 9 Trojan-Banker.Win32.Tinba
- 10 Trojan-Banker.JS.Agent

- 
- 大小 : 3.5 KB
  - 通过电子邮件传播附件
  - 也可以在家用路由器上找到

# 勒索软件

## You Have Been Hacked!!!

All your personal files have been encrypted, and your passwords and info have been copied to an offline server. To get your files and passwords back, send "0.25" bitcoin to the bitcoin address below. Failure to pay by March 1st 2017 will result in loss of ALL data and your passwords and info will be leaked to the public.

Google "How to buy bitcoin" or follow the steps below.

1. Click here to open "<https://www.coinbase.com/signup>"
2. Signup and buy the amount requested below.
3. Send bitcoin to the address below.
4. Wait until Payment is verified.

Once the payment is verified all your data will be decrypted and this program and the offline server will self destruct.

**Warning! Any Attempt to get rid of this program or rebooting your machine will result in the loss of all your data and your passwords and info will be posted online!**

Pay the following amount of bitcoin to the bitcoin address below

Amount: 0.25

Address: 1BcNd6eQ5vgzb7eRnV5ddpW1TBP7eNiwLb

Useful Resources

[Easy guide to buy bitcoin](#) [Full list of encrypted files](#) [Full list of passwords](#) [Decrypt 1 file for free](#)



Awaiting payment

# 勒索软件

## Restoring your files - The fast and easy way

To get your files fast, please transfer [1.0 Bitcoin](#) to our wallet address  
[1LEIPgvh6S9VEXWV2dZTy1SRd7e9B1bWt3](#). When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

## What we did?

We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world ([Encryption - Wikipedia](#)). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!

If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.

## Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

<https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5>

## Why we do that?

We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more the half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. **I personally have lost both my parents and my little sister in 2015.** The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. ([Syria War in Wikipedia](#))

Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people. We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.

## 为什么要拥有机器 : 3。 勒索软件

1 Trojan-Ransom.HTML.Agent

2 Trojan-Ransom.JS.Blocker

3 Trojan-Ransom.JS.InstallExtension

4 Trojan-Ransom.NSIS.Onion

5 Trojan-Ransom.Win32.Cryakl

6 Trojan-Ransom.Win32.Cryptodef

7 Trojan-Ransom.Win32.SnoCry

8 Trojan-Ransom.BAT.Scatter

9 Trojan-Ransom.Win32.CrypMod

10 Trojan-Ransom.Win32.Shade

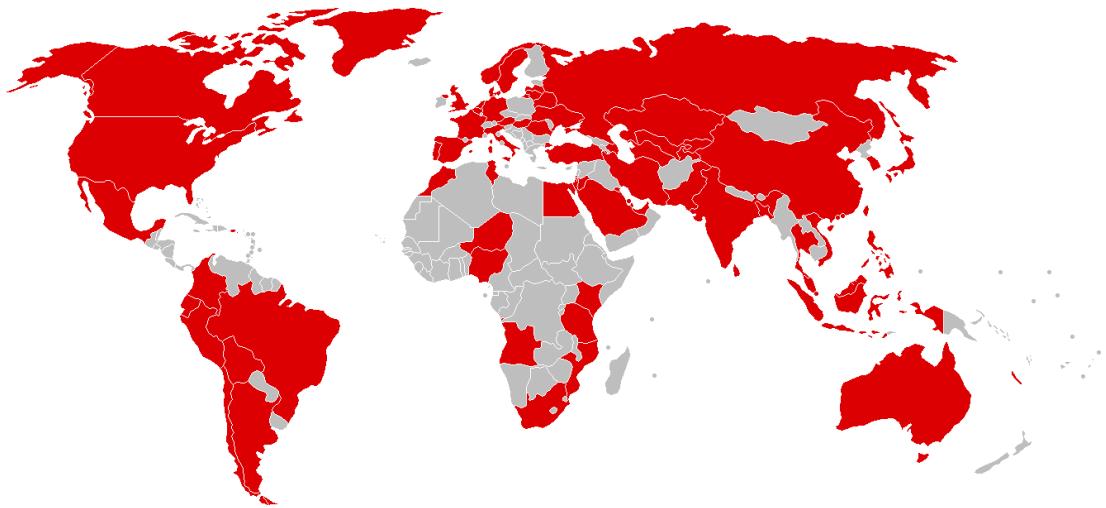
CryptoWall ( 2014- )

- 针对Windows
- 通过垃圾邮件传播

≈2015年有200,000台机器全球性  
问题。

# 想要 ( 2017年5月 )

- 全球网络攻击  
在Windows上
- 感染超过  
拥有230,000台计算机  
超过150个国家
- NHS ( 英国 ) , 雷诺  
（ 法国 ） , 德国铁路  
（ 德国 ） , 西班牙电信  
（ 西班牙 ） ...
- 杀死安全研究人员发现的Switc  
h URL  
  
马库斯·哈钦斯 ( Marcus Hutchins )

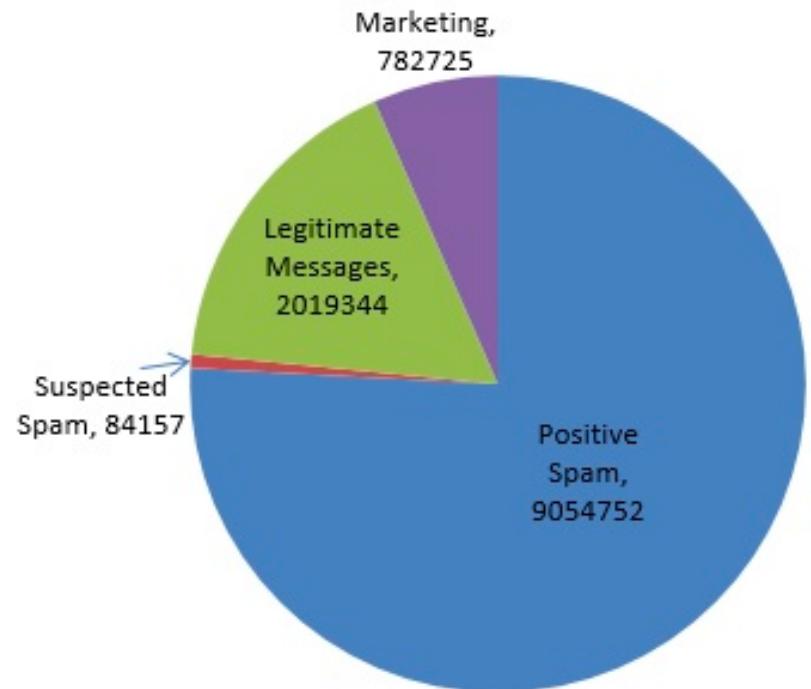
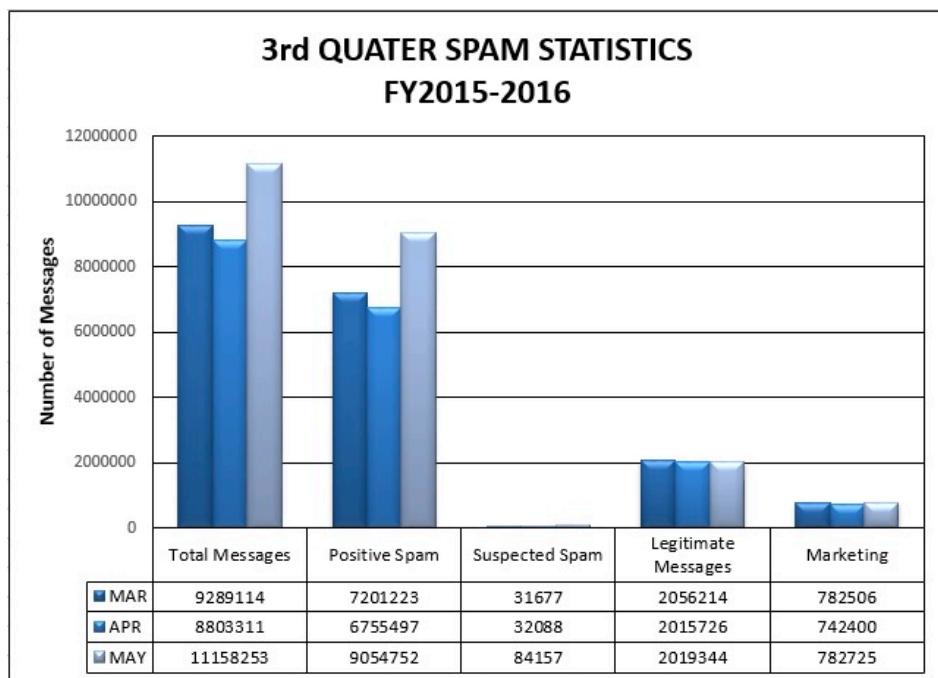


# 一些数字

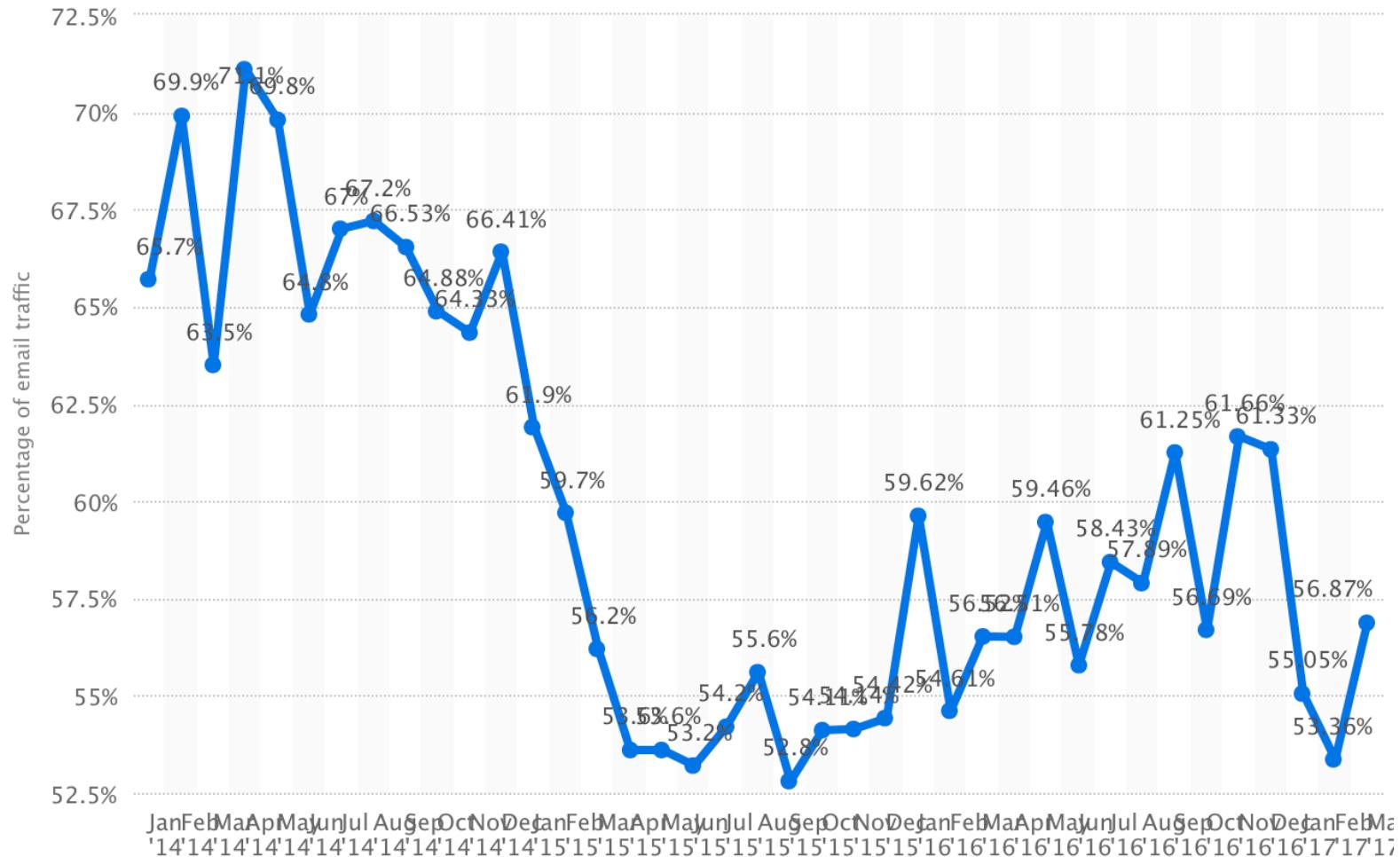
- “Rogueware业务”，PandaLabs，2010年
- “网络犯罪业务”，PandaLabs，2008年
- “基于网络的攻击”，赛门铁克，2009年
- 广告软件行业每年价值20亿美元 恶意软件行业每年价值1050亿美元
- > 80% 的电子邮件流量存在（或曾经是）垃圾邮件
- 连接到Internet的计算机中有50%-80% 被间谍软件感染
- 有些人使用僵尸网络（即被感染的计算机）每月赚取2万美元（！）。
- 一名26岁的老人通过垃圾邮件赚了2000万美元，然后在四年前被网络钓鱼者损失了20亿美元。

# 垃圾内容统计 ( 2016年5月 )

- 信息安全办公室 ( 埃尔帕索大学 )

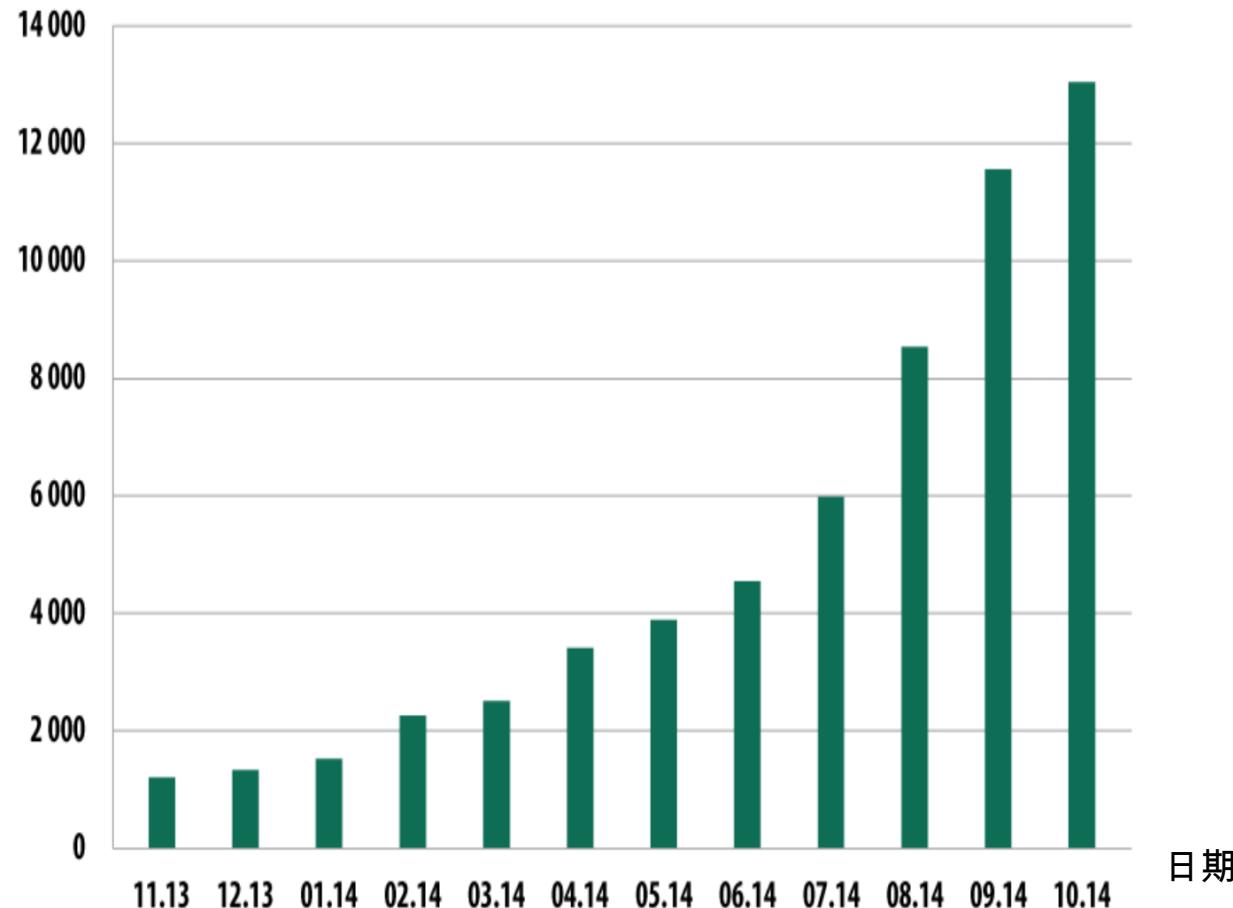


# SPAM数量占电子邮件流量的百分比



# 移动恶意软件

( 2013年11月 – 2014年10月 )



移动银行木马的兴起 ( 卡巴斯基安全公告2014 )

# 前所未有的规模 ( IoT )

## EXTRA-LARGE DENIAL OF SERVICE ATTACK USES DVRS, WEBCAMS

by: Elliot Williams

46 Comments

f t g+

September 26, 2016



Brace yourselves. The rest of the media is going to be calling this an "IoT DDOS" and the hype will spin out of control. Hype aside, the facts on the ground make it look like an extremely large distributed denial-of-service attack (DDOS) was just carried out using mostly household appliances (145,607 of them!) rather than grandma's old Win XP system running on Pentiums.

# 高级持续威胁 ( APT )

- 低频高冲击
- 针对性攻击，策略
- 复杂而协调
- 隐身攻击（在雷达下）
- 财务或工业收益不一定是即时的
- 攻击向量
  - 远程（传统向量）
  - 本地（USB密钥，共享磁盘，MITM攻击...）
  - 人类（鱼叉式网络钓鱼，论坛，社交网络.....）

# 黑客自行部署 基础设施

A screenshot of a web browser window showing a US-CERT alert page. The title bar reads "Avalanche (crimeware-as-a-service infrastructure)" and the URL is "https://www.us-cert.gov/ncas/alerts/TA16-336A". The page features the US-CERT logo and navigation links for Home, About Us, Careers, Publications, Alerts and Tips, Related Resources, and C'VP. The main content area is titled "Alert (TA16-336A)" and discusses the Avalanche botnet. It includes sections for Systems Affected (Microsoft Windows), Overview, Description, and a list of malware families. A mouse cursor is visible on the right side of the page.

**Alert (TA16-336A)**

Avalanche (crimeware-as-a-service infrastructure)

Original release date: December 01, 2016 | Last revised: December 14, 2016

Print Tweet Send Share

**Systems Affected**

Microsoft Windows

**Overview**

"Avalanche" refers to a large global network hosting infrastructure used by cyber criminals to conduct phishing and malware distribution campaigns and money mule schemes. The United States Department of Homeland Security (DHS), in collaboration with the Federal Bureau of Investigation (FBI), is releasing this Technical Alert to provide further information about Avalanche.

**Description**

Cyber criminals utilized Avalanche botnet infrastructure to host and distribute a variety of malware variants to victims, including the targeting of over 40 major financial institutions. Victims may have had their sensitive personal information stolen (e.g., user account credentials). Victims' compromised systems may also have been used to conduct other malicious activity, such as launching denial-of-service (DoS) attacks or distributing malware variants to other victims' computers.

In addition, Avalanche infrastructure was used to run money mule schemes where criminals recruited people to commit fraud involving transporting and laundering stolen money or merchandise.

Avalanche used fast-flux DNS, a technique to hide the criminal servers, behind a constantly changing network of compromised systems acting as proxies.

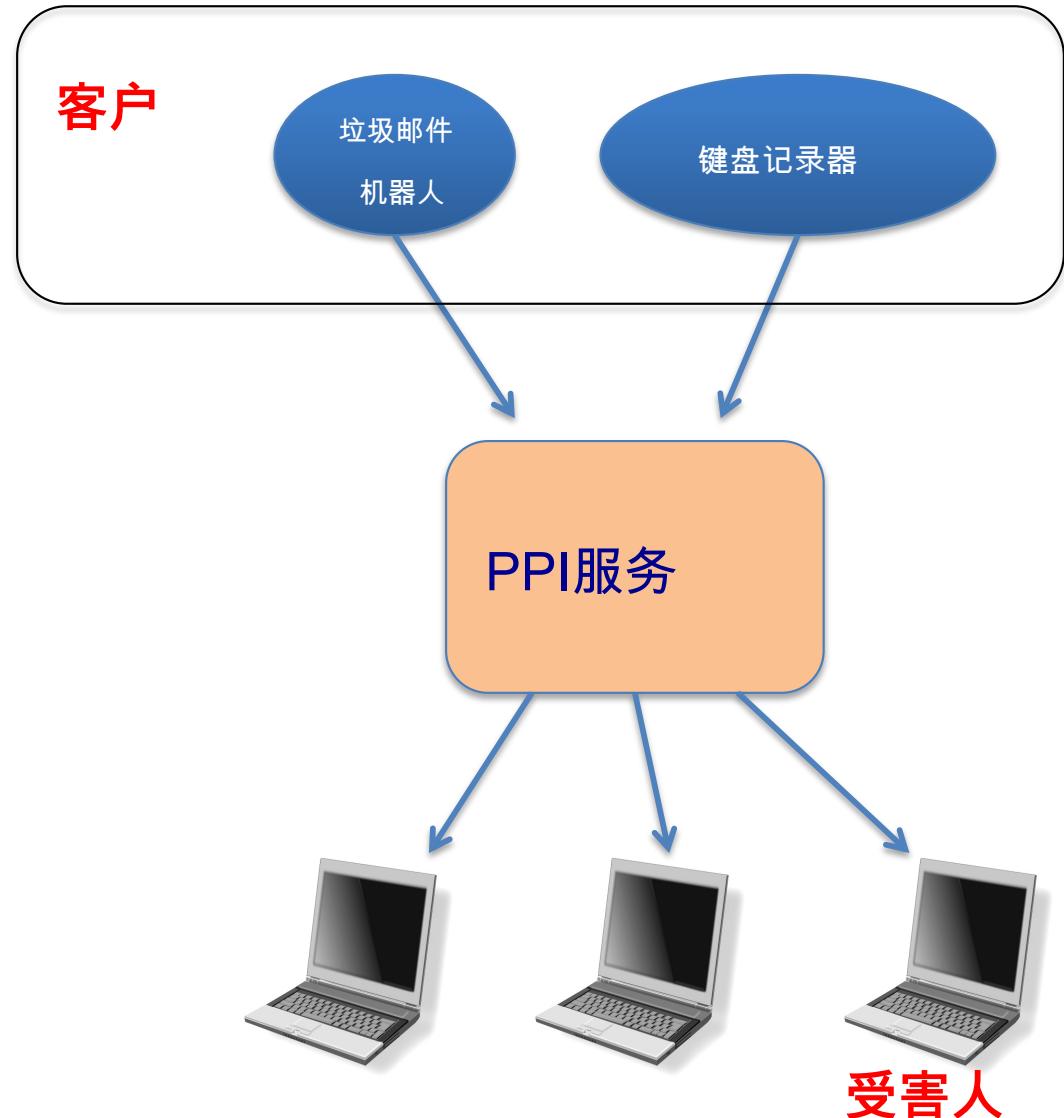
The following malware families were hosted on the infrastructure:

# 拥有机器的市场

每次安装付费 ( PPI ) 服务

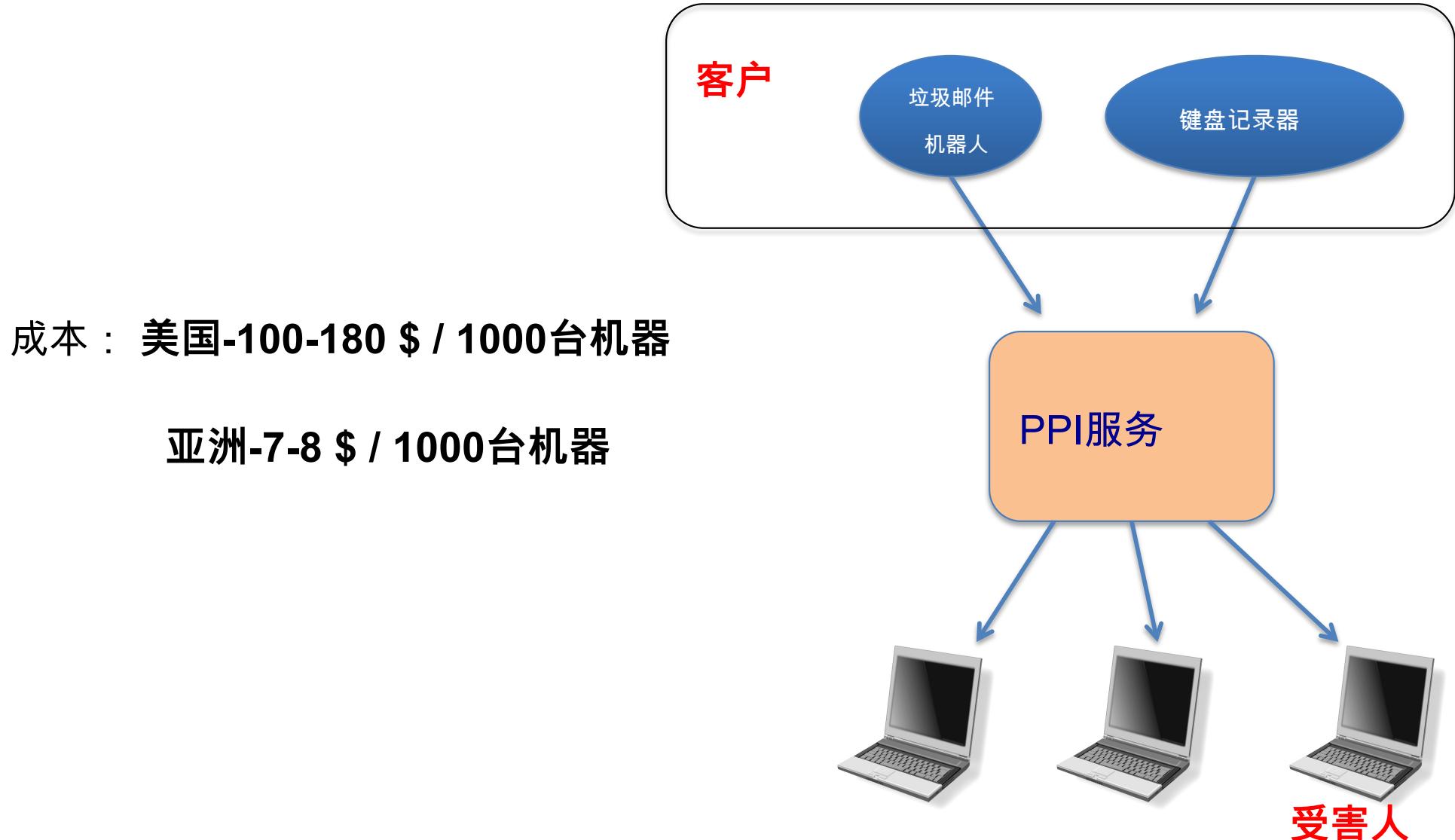
PPI操作：

- 1.自己的受害者的机器
- 2.下载并安装客户端代码
- 3.向客户收费



资料来源：Cabrallo等。 ( [www.icir.org/vern/papers/ssi-usesec11.pdf](http://www.icir.org/vern/papers/ssi-usesec11.pdf) )

# 拥有机器的市场



资料来源：Cabrallo等。 ( [www.icir.org/vern/papers/ssi-usesec11.pdf](http://www.icir.org/vern/papers/ssi-usesec11.pdf) )

# 漏洞市场

## 选项1：错误赏金计划（许多）

- Google漏洞奖励计划：最高\$ 20K
- Microsoft赏金计划：最高\$ 100,000
- Mozilla Bug赏金计划：\$ 7500
- Pwn2Own比赛：\$ 15K

## 选项2：

- 零日倡议（ZDI），iDefense：\$ 2K – \$ 25K

# 示例 : Mozilla

Novel vulnerability and exploit, new form of exploitation or an exceptional vulnerability	High quality bug report with clearly exploitable critical vulnerability <sub>1</sub>	High quality bug report of a critical or high vulnerability <sub>2</sub>	Minimum for a high or critical vulnerability <sub>3</sub>	Medium vulnerability
\$10,000+	\$7,500	\$5,000	\$3,000	\$500 - \$2500

# 一些参考

- 图书：
  - Gildas Avoine , Pascal Junod , Philippe Oechslin , Sylvain Pasini。信息安全，实践与实践。威伯特。
  - 罗斯·安德森。安全工程。威利。 ( <http://www.cl.cam.ac.uk/~rja14/book.html> )
- 会议：
  - 学术：安全与隐私（奥克兰）, CCS, Usenix安全, NDSS, ESO RICS, RAID, ACSAC, DSN
  - 非学术性的：DefCon, BlackHat, SSTIC, GreHack