高级持续性威胁与防范

Vincent Cim

OWASP

The Open Web Application Security Project

议题

OWASP
The Open Web Application Security Project

I. 什么是APT(高级持续性威胁)

II. APT攻击案例学习

III. APT 攻击手段与方法

IV. 如何防范

APT相关新闻

OWASP
The Open Web Application Security Project

Operation Aurora

Description of
On January 14,
was used as an
Microsoft has si

Operation Auror
Microsoft Intern
to download and
targeted users a
connected those
intellectual prop

What is McAfe
Upon learning o
content signatur
advice on the M

NEWS

Chinese Night Dragon Attack Hits Energy Companies

Since 200
McAfee

On February 10, 2011 by P
The world's energy compa
control of internal servers

The attacks, which started
operating system vulnerab
issues such as oil and gas

Oil companies are

effort, and has updated sig
have seen in these attacks

Once one system has bee
Gh0st and zwShell to expl
can eventually be extracte

McAfee has confirmed five
companies are affected –

BUSINESS CENTER Mar 19, 2011 1:10 am

RSA SecurID Hack Sho
APTs

By Tony Bradley, PCWorld

RSA revealed in an open letter posted to its website that it
that data was stolen which could potentially compromise it
the RSA network is an example of a new breed of security
longer and going after bigger payoffs.

SIMILAR ARTICLES:

- Lockheed-Martin Attack Signals New Era of Cyber Espionage
- 6 Security Trends to Watch For
- How to Stop Hack Attacks In One Easy Step: Whitelisting
- Privacy Watch: Two Passwords Double Your Privacy
- A Hidden Security Threat: Beware the Office Multifunction Printer
- Hacktivism Trumps Money as Motivation for Denial-of-Service Attacks

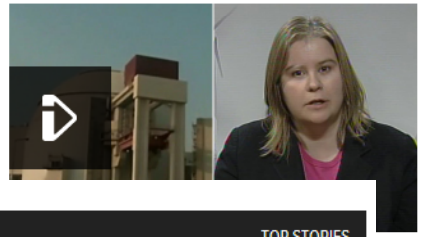
RSA describes the atta
(APT). Tim 'TK' Keanir
APTs represent a sign
landscape. An APT att
funded attackers going

Keanini warns, "This p
attack could be really
for mercenaries. Being
go to the black market
the capability to break
SecureID infrastructure
worth a lot of money fo
reasonably big time wi

Two-factor authenticat
preferred method of providing stronger security than is pr
by a username and password alone. One of the most com
methods of two-factor authentication is to use a key fob o
which provides a randomized code you must enter in addi
the username and password in order to authenticate and

Stuxnet worm hits Iran nuclear plant staff computers

A complex computer worm has infected the personal computers of staff at Iran's first nuclear power station, the official IRNA news agency reported.



However, the operating system at the Bushehr plant - due to go online in a few weeks - has not been harmed, project

GIZMODO TOP STORIES

HACKING

Operation Shady Rat Is The Largest Cyber Attack Ever Uncovered

If it wasn't true before, it's definitely true now. Hacking isn't just for giggles, it's a major threat to international security.

BY KELLY AUG 3, 2011 12:31 AM

Share

GET OUR TOP STORIES
FOLLOW GIZMODO

什么是高级持续性威胁

OWASP
The Open Web Application Security Project

NIST给出的详细定义

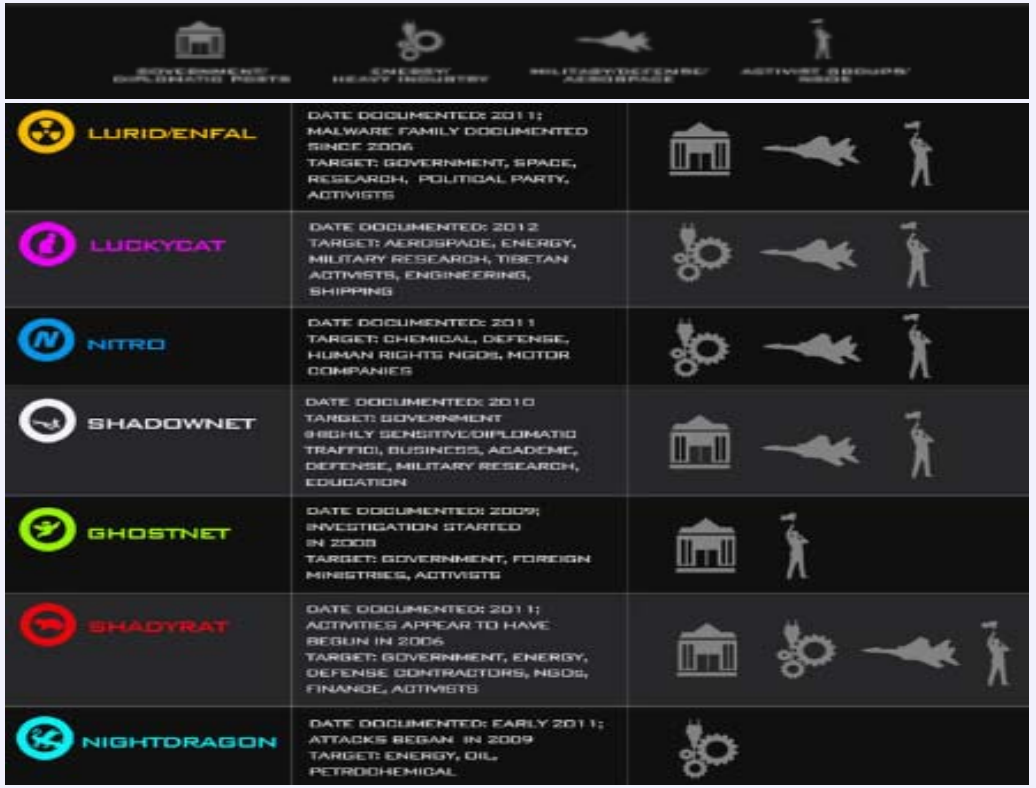
“精通复杂技术的攻击者利用多种攻击向量(如：网络，物理和欺诈。)借助丰富资源创建机会实现自己目的。”这些目的通常包括对目标企业的信息技术架构进行篡改从而盗取数据(如将数据从内网输送到外网)，执行或阻止一项任务，程序;又或者是潜入对方架构中伺机进行偷取数据。

APT的特点

- 会长时间重复这种操作;
- 会适应防御者从而产生抵抗能力;
- 会维持在所需的互动水平以执行偷取信息的操作。

遍布全球的Gh0st Net

- [APT]具有确定具体目标用户在一个单位或组织根据工作职能或推定获取信息的能力。
- [APT]可以使用被动监测网络流量达到情报搜集目的。让这些机器平时可以为攻击者提供一个攻击的跳板，从而诱发灾难性的后果。
- [APT] 拥有成熟的技术手段和上传的方法以及隐蔽的远程接入软件，建立深入且持续访问而不容易被检测和发现。



议题

OWASP
The Open Web Application Security Project

I. 什么是高级持续性威胁

II. APT攻击案例学习

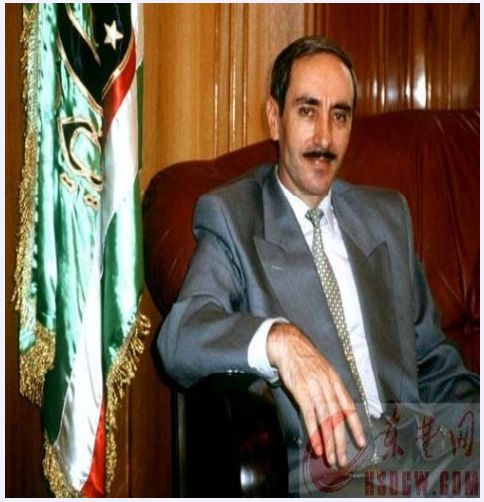
III. APT 攻击手段与方法

IV. 如何防范

不得不提及的历史

OWASP
The Open Web Application Security Project

4月末注定是不平凡的日子，20日是希特勒的生日，22日是列宁的生辰。而1996年的4月21日，



- 前苏联空军少将，车臣独立之父
- 公开羞辱叶利钦
- 逃脱三次追捕

- 海事卫星电话
- 每次谈话不超过5分钟
- 最后一次通话15至20分钟（与莫斯科通话）

- 前苏联SU-24战斗攻击机
- 起飞-发现目标-发射导弹-摧毁目标需要8分钟。

Operation Aurora

OWASP
The Open Web Application Security Project

1.侦察

2.攻击google员工好友
控制了google员工好友主机

3.搭建一个伪相册站点
上面放置了IE 0DAY攻击代码

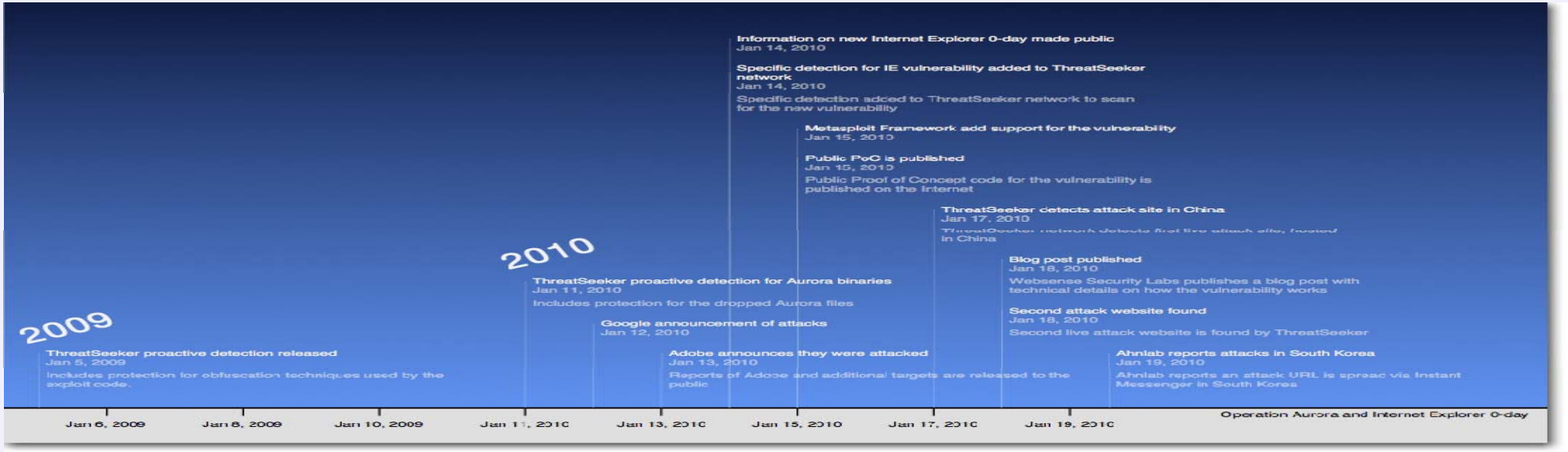
4.伪造google员工好友发IM
邀请打开恶意相册的URL

5.Google员工中招访问站点
攻击者控制google员工机器

6.攻击者利用google员工身份社工和渗透其他人员

7.攻击者通过多层渗透最后控制了gmail服务器

8.攻击者通过SSL加密把敏感数据传回



STUXNET

OWASP
The Open Web Application Security Project

1.侦察

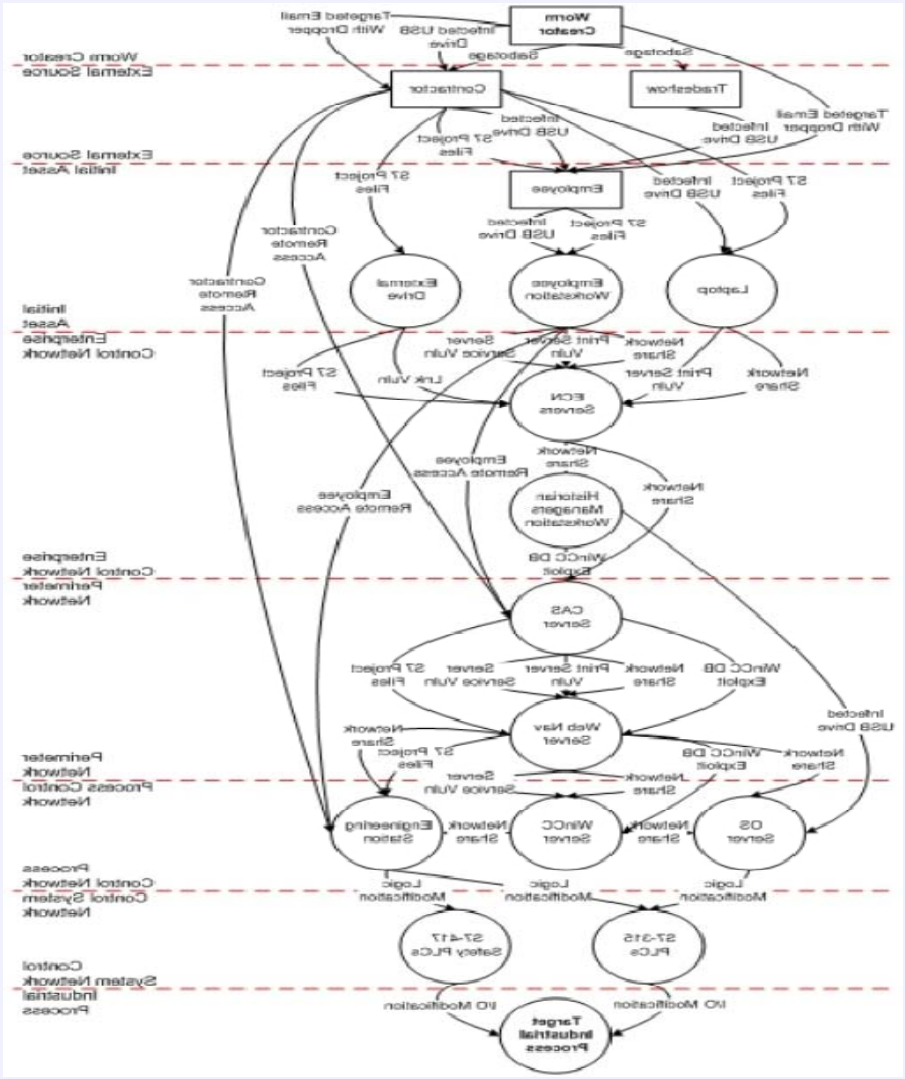
2.利用社工+0DAY攻击家庭主机

3.员工在家使用USB，利用0DAY感染USB

4.员工接入隔离的内网主机，利用0DAY感染内网主机

5.内网逐步渗透最后感染了核设施控制主机

6.篡改控制参数，导致无法产出关键物质



Night Dragon

OWASP
The Open Web Application Security Project

1.侦察

2.SQL注射攻击WEB服务器

3.上传伪装成图片的恶意代码到WEB服务器的员工交流区

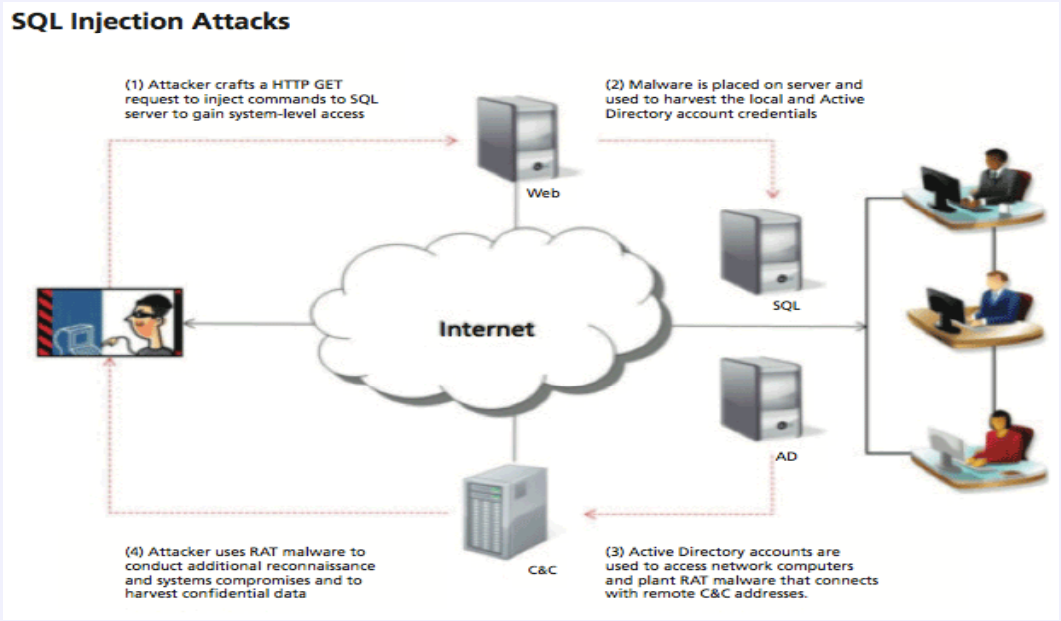
4.等待内部员工访问WEB服务器

5.利用WEB恶意代码攻击员工个人主机

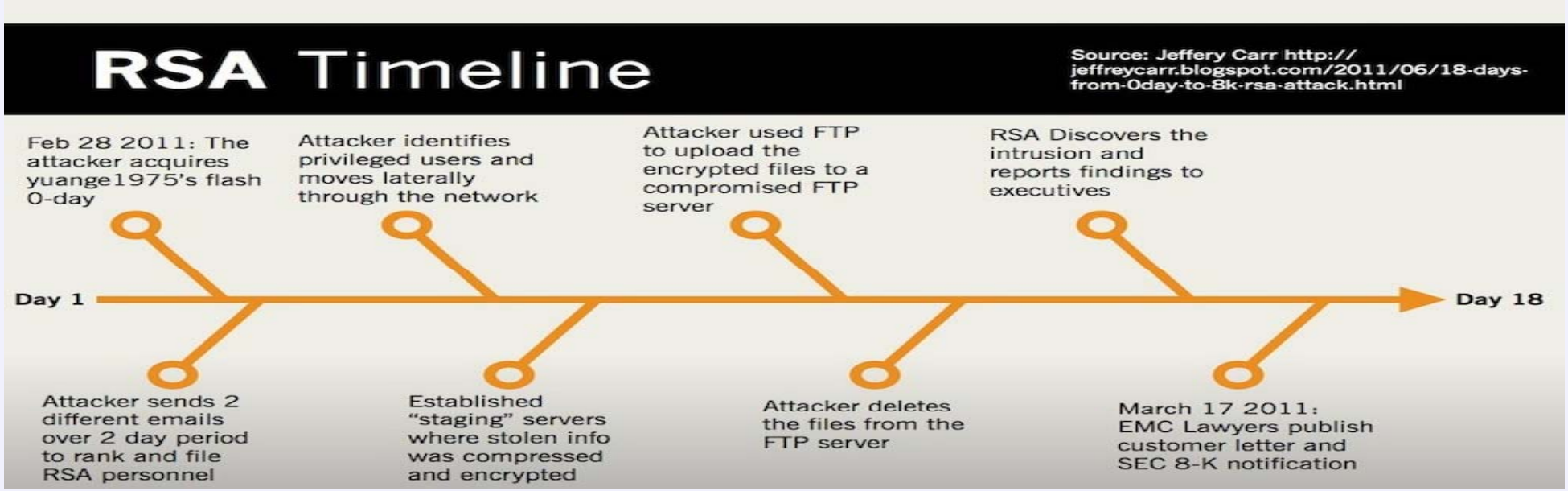
6.利用社交、钓鱼、暴力破解渗透高级员工

7.获得内部服务器核心资产

8.个人端加密传回敏感信息



RSA



1.侦察：

2.发送财务为主体的社工邮件，包含FLASH 0DAY

3. 财务员工打开中招，攻击者控制财务人员主机

4.攻击者利用财务员工身份社工和渗透其他人员

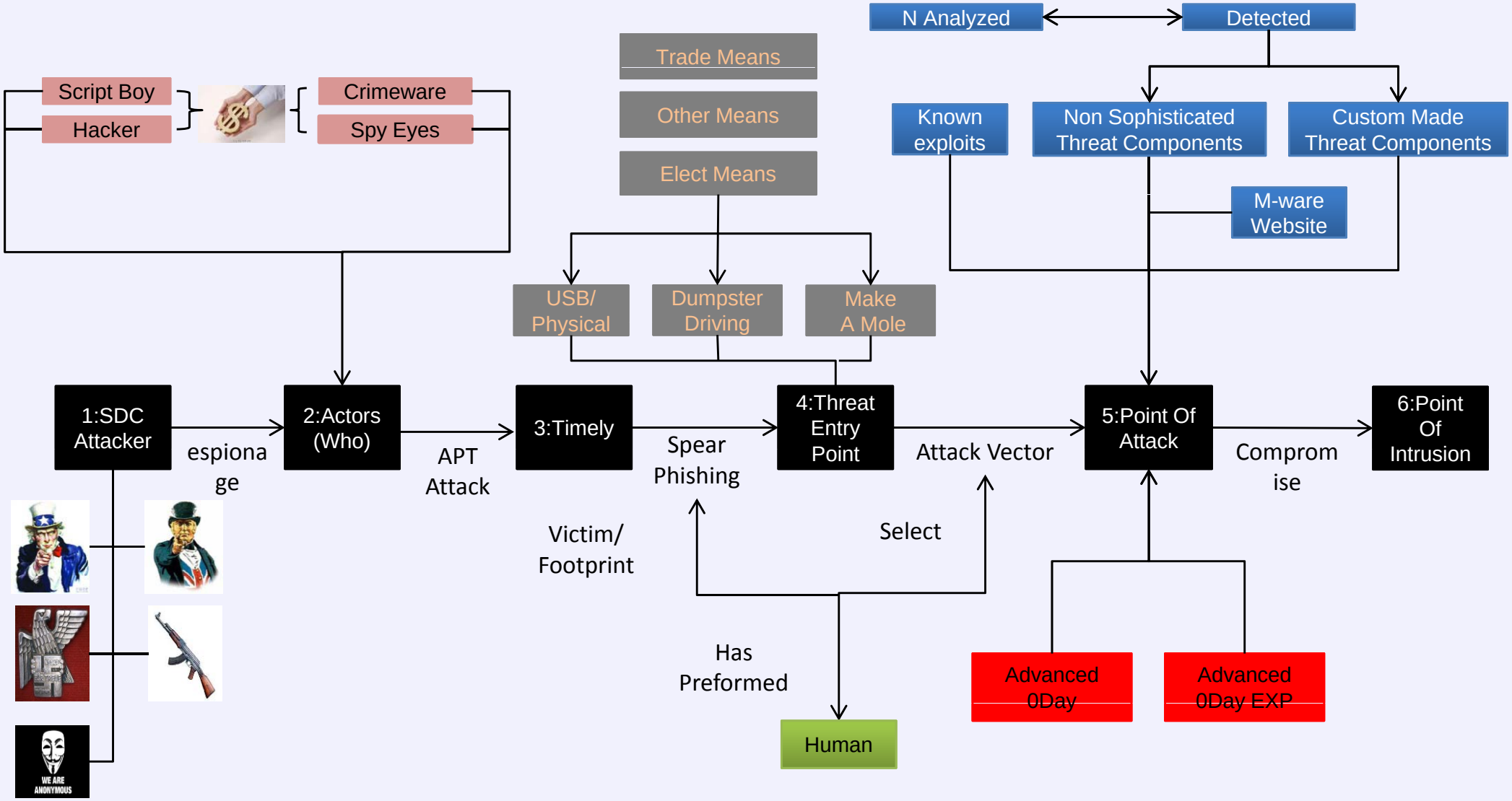
5.攻击者获得令牌服务器访问

6.攻击者将敏感数据加密传回

7.攻击者利用令牌信息对使用RSA令牌的国防部军火承包商攻击

案例分析APT Attack Model

OWASP
The Open Web Application Security Project



议题

OWASP
The Open Web Application Security Project

I. 什么是高级持续性威胁

II. APT攻击案例学习

III. APT 攻击手段与方法

IV. 如何防范

APT分析

- 从广义的角度进行归纳分析，它包含了：
  - 间谍
  - 社会工程
  - 0day
  - 恶意攻击者
- 从情报收集的角度来看，其实相似的手法已经存在很多年：

幕后	国家/组织	国家/组织
潜伏者	特工	木马
传递网络	情报网	botnet
手段	无线电发报	远程控制
中转站	欧洲、东南亚。。。	欧洲、东南亚。。。

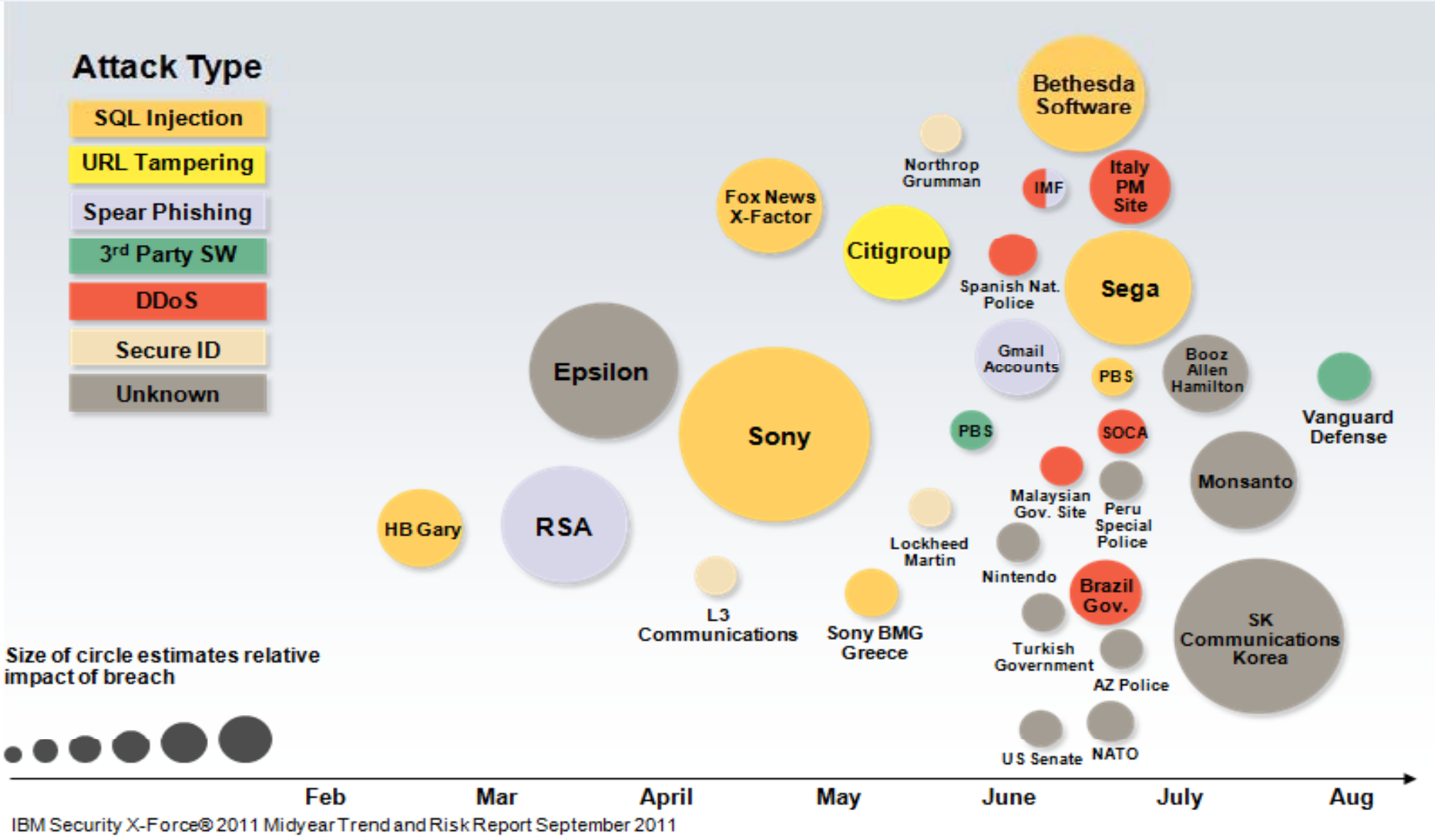
APT攻击与传统方式的对比

OWASP
The Open Web Application Security Project

威胁特点	普通攻击	APT攻击
财政支援	资金充足	资金充足；可能拥有政治资源
对象	可能的最大受众	特定组织
利用零日漏洞	不常见	常见
目标	几乎纯粹是经济性的	经济性、干扰运营、获取机密数据以获得某种利益
机会型	通常如此	否。具有明确定义的目标
执行耐性	少有	无疑
社交工程	是	是，但目标及其具体和明确
修改/定制常见恶意软件	是	是
攻击工具协调	很少超出传统混合型威胁范围	大范围；运用的工具可能因各运作步骤的结果而异
数据收集方法	通常是前行夺取	井然有序并且不引人注意
调查	少量；在有效负荷和传输机制方面	大范围；包括应用、政策最佳实践、雇员利益等
将感染扩散到其他系统	通常攻击任何易受攻击的系统	是，但更具策略性，可能会遵循规划好的路径，并在不同系统上充分利用不同的工具

APT攻击类型

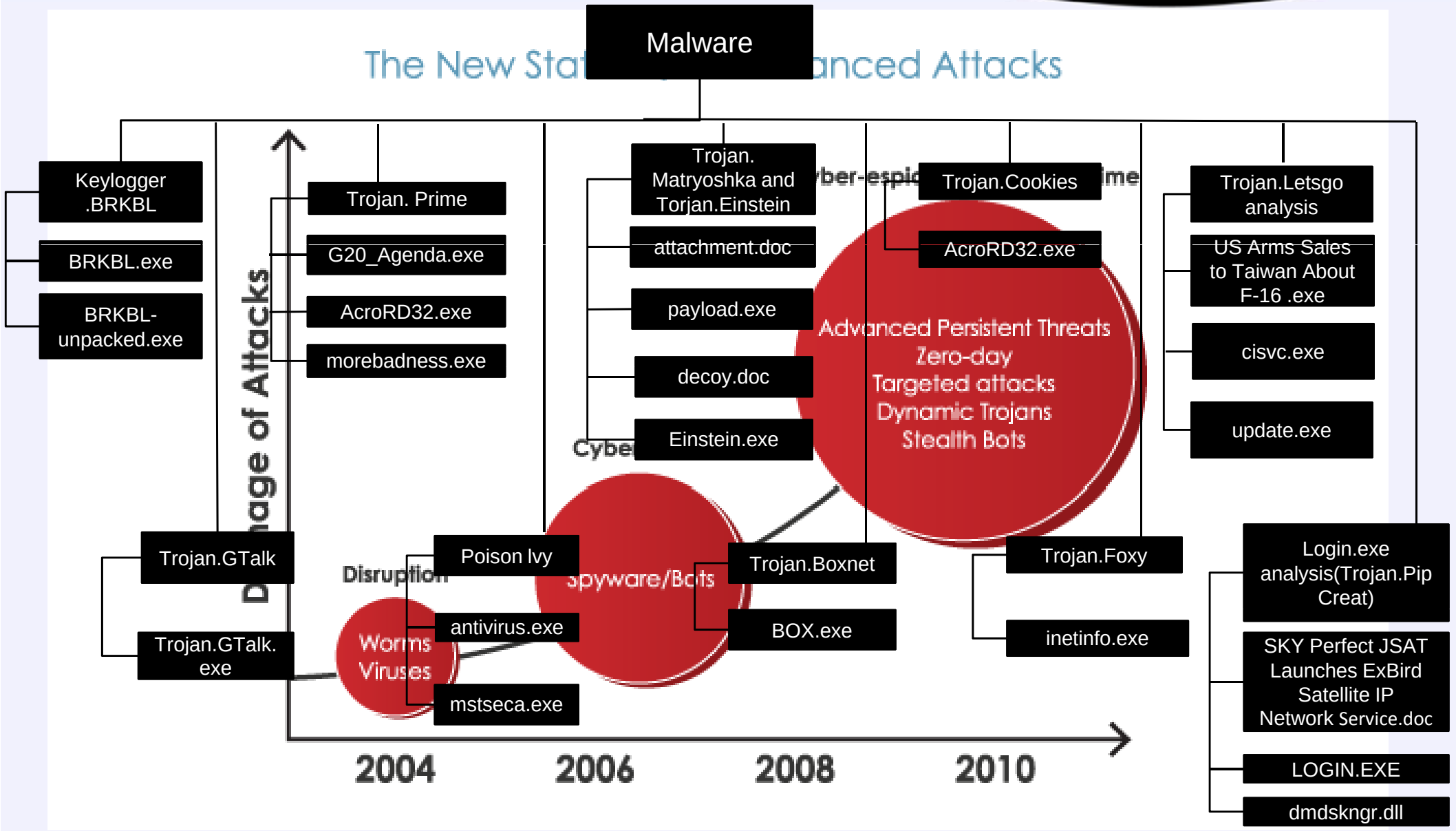
OWASP
The Open Web Application Security Project



IBM Security X-Force® 2011 Midyear Trend and Risk Report September 2011

恶意软件及其变种

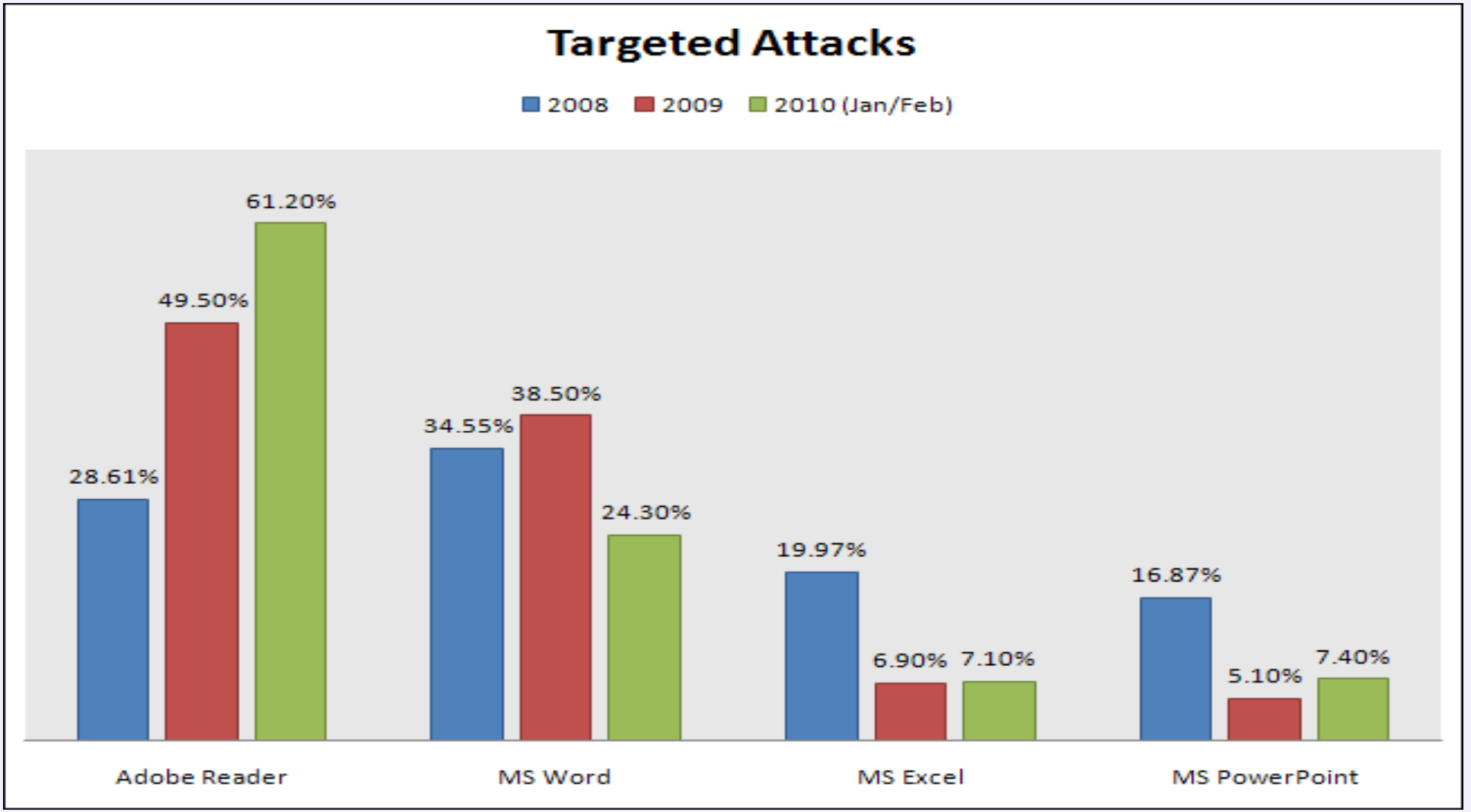
OWASP
The Open Web Application Security Project



载体的种类

OWASP
The Open Web Application Security Project

PDF Based Targeted Attacks are Increasing

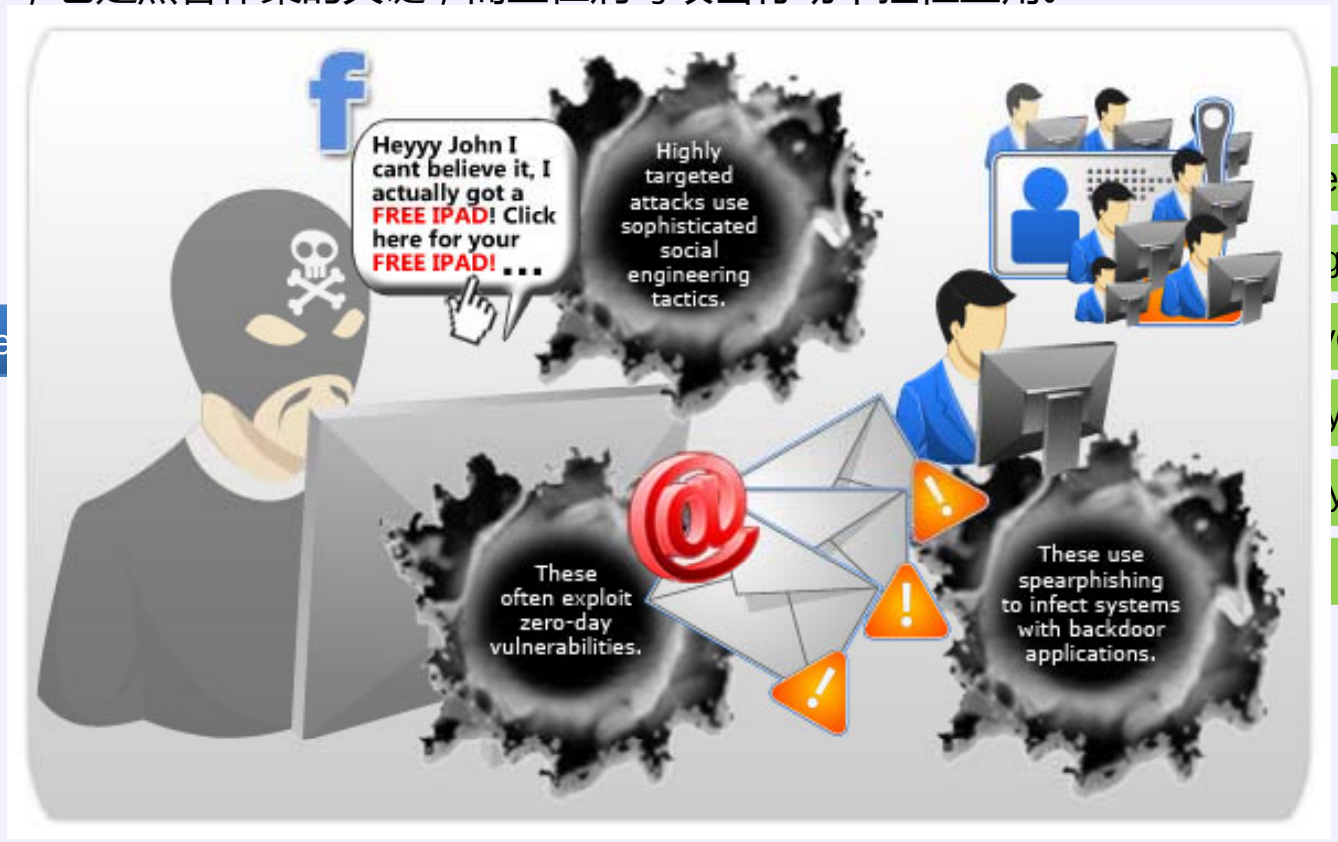


社交工程

OWASP
The Open Web Application Security Project

- 社交工程陷阱(Social Engineering)是种骗人的艺术，名词來自黑客出身的安全顾问 – Kevin Mitnick，它是一种引诱人们做出本意不想的行为，或是給出机密资料。
- 这种操控计算机使用者而非计算机本身的手法被称为「社交工程学」（ social engineering ）。在許多案例当中，它是黑客作案的关键，而且在病毒攻击行动中担任主角。

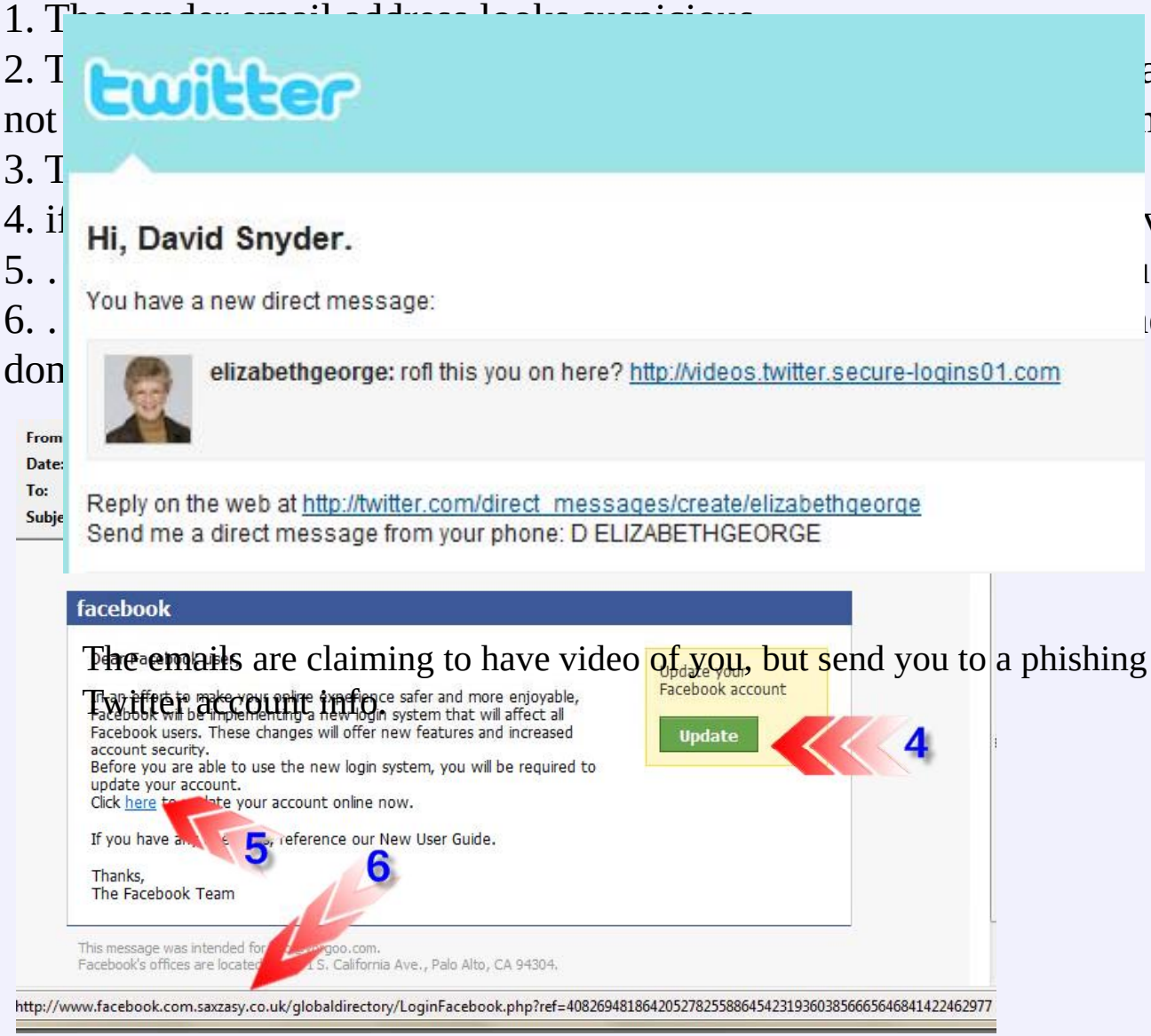
Social Engine



鱼叉式钓鱼

OWASP
The Open Web Application Security Project

1. T
2. T ace-book, in fact this address does not nail box.
3. T
4. it ver the
5. . ual…
6. . e scam sub-domain of a .co.uk don



The emails are claiming to have video of you, but send you to a phishing site to harvest your Twitter account info.

HTTP传染媒介

OWASP
The Open Web Application Security Project

- 并不是所有的攻击都是通过邮件来实现。
- 搜索引擎劫持和重定向
  - 搜索引擎每天返回数百万搜索结果，这也成为攻击者诱人的攻击目标。
  - 其中攻击者发动攻击或者传播恶意软件所使用的最普遍的方法就是引诱不知情的网络用户到包含恶意代码的网站。
  - 除了能够将用户直接带到恶意网站外，SEO中毒攻击还能够在受欢迎的合法网站使用跨站脚本攻击技术
- 服务溢出攻击利用
  - SWF on FF 0-day
  - SWF on IE 0-day
  - MS Vulnerability

VPN攻击

OWASP
The Open Web Application Security Project

- Gucci:前Gucci网络工程师创建了一个假员工账号来访问和控制公司电脑系统，他切断了Gucci服务器上邮件和文件的通道，Gucci因停产和修复还原的损失超过20万美金。
- DigiNotar:黑客入侵数字证书授权系统，分发超过500个欺骗性数字证书给顶级互联网公司，如谷歌，Mozilla和Skype.这次黑客攻击发生在六月初，但是DigiNotar直到7月中旬才发现。该公司在9月申请破产。
- Comodo:黑客分发欺骗性SSL证书给7个网页域名，包括谷歌，雅虎和Skype.
- 花旗集团：黑客访问了36万多个账号信息，查阅客户联系信息和交易历史，直接了曝光他们网站的安全漏洞。

议题

OWASP
The Open Web Application Security Project

I. 什么是高级持续性威胁

II. APT攻击案例学习

III. APT 攻击手段与方法

IV. 如何防范

历史的经验

OWASP
The Open Web Application Security Project

从反恐策略中学习

OWASP
The Open Web Application Security Project

- 英国自2003年以来，英国制定了打击恐怖主义的长期战略，又被简称为反恐4P战略，即：预防（prevent）、追踪pursue)、保护(protect)和准备(prepare)。
- 美国自911后不断的调整自身的反恐战略，提出了4项原则、8个目标、11个关注区域。
- 后拉登时代的新发布的反恐策略依然体现了任何敢于挑战美国霸权的国家、组织和个人，都将可能受到美国的制裁或彻底的消灭。

如何防范

OWASP
The Open Web Application Security Project

- 了解威胁是真实的存在于你的计算环境当中的。
- 承担自身计算环境保护的责任。没有那个国家有力量是能够保护互联网生态系统安全。
- 开始了解自身的存在的脆弱性和业务流程上的安全控制点。
- 知识共享充分利用。

意识	分级	控制	共享
◘ 确保您的领导了解APT的内容。 ◘ 沟通使用许多不同的渠道： ●年度强制性意识培训 ●特别活动，座谈会，日历，鼠标垫，衬衫 ●门户网站的文章 ●有针对性的培训 ◘ 有行政机制保障	◘ 输入、处理、输出 ●网络层 ●系统层 ●程序 ●数据 ◘ 简单可靠的ACL ◘ 进行区域隔离 ◘ 日志关联分析	◘ 建立符合业务需求的安全流程与制度 ◘ 各级人员具备相应的响应能力 ◘ 实时分析和捕捉有害的事件 ◘ 定义数据流控制矩阵	

Thank you