软件安全—恶意代码机理与防护

C1 软件安全概论

彭国军

武汉大学国家网络安全学院

guojpeng@whu.edu.cn

提纲

1.1 信息与信息安全

1.2 软件安全威胁与来源

1.3 软件安全威胁的典型防护手段

1.2 软件安全威胁

- 信息系统面临的三大典型软件安全威胁
  - 软件缺陷与漏洞（正常软件）
  - 恶意软件：实现恶意目的
  - 非法破解，知识产权被侵害（正常软件）

1.2.1 软件缺陷与漏洞

- 软件缺陷（**Defect**），常常又被称作**Bug**
  - 指计算机软件或程序中存在的某种破坏正常运行能力的问题、错误，或者隐藏的功能缺陷。

- 缺陷的存在会导致软件产品在某种程度上不能满足用户的需求。

漏洞

- 漏洞，是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

软件漏洞

- 软件漏洞(Vulnerability)，是指软件在设计、实现、配置策略及使用过程中出现的缺陷，其可能导致攻击者在未授权的情况下访问或破坏系统。

典型软件类型

- 系统软件
  - Windows、Linux、Android、iOS...
- 应用软件
  - MS Office、Acdsee、QQ、迅雷、Acrobat Reader...
- Web软件等
  - 论坛、文章系统、博客...

软件漏洞带来的危害

- 软件正常功能被破坏
- 系统被非法控制和破坏
- 信息泄漏等

微软安全公告— MS14-052

- 最严重的漏洞可能在用户使用 Internet Explorer 查看特制网页时允许远程执行代码。
- 成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的客户比具有管理用户权限的客户受到的影响要小。

1 到 15 个公告，共 1211 个　　1　第 1 页，共 81 页

日期	公告号	知识库号	标题	公告等级
2014/9/9	MS14-055	2990928	Microsoft Lync Server 中的漏洞可能允许拒绝服务	重要
2014/9/9	MS14-054	2988948	Windows 任务计划程序中的漏洞可能允许特权提升	重要
2014/9/9	MS14-053	2990931	.NET Framework 中的漏洞可能允许拒绝服务	重要
2014/9/9	MS14-052	2977629	Internet Explorer 的累积性安全更新	严重
2014/8/12	MS14-051	2976627	Internet Explorer 的累积性安全更新	严重
2014/8/12	MS14-050	2977202	Microsoft SharePoint Server 中的漏洞可能允许特权提升	重要
2014/8/12	MS14-049	2962490	Windows Installer 服务中的漏洞可能允许特权提升	重要
2014/8/12	MS14-048	2977201	OneNote 中的漏洞可能允许远程执行代码	重要
2014/8/12	MS14-047	2978668	LRPC 中的漏洞可能允许绕过安全功能	重要
2014/8/12	MS14-046	2984625	.NET Framework 中的漏洞可能允许绕过安全功能	重要
2014/8/12	MS14-045	2984615	内核模式驱动程序中的漏洞可能允许特权提升	重要
2014/8/12	MS14-044	2984340	SQL Server 中的漏洞可能允许特权提升	重要

Microsoft 安全公告 MS14-052 - 严重

此主题尚未评级 - 评价此主题

Internet Explorer 的累积性安全更新 (2977629)

发布日期： 2014 年 9 月 9 日

版本： 1.0

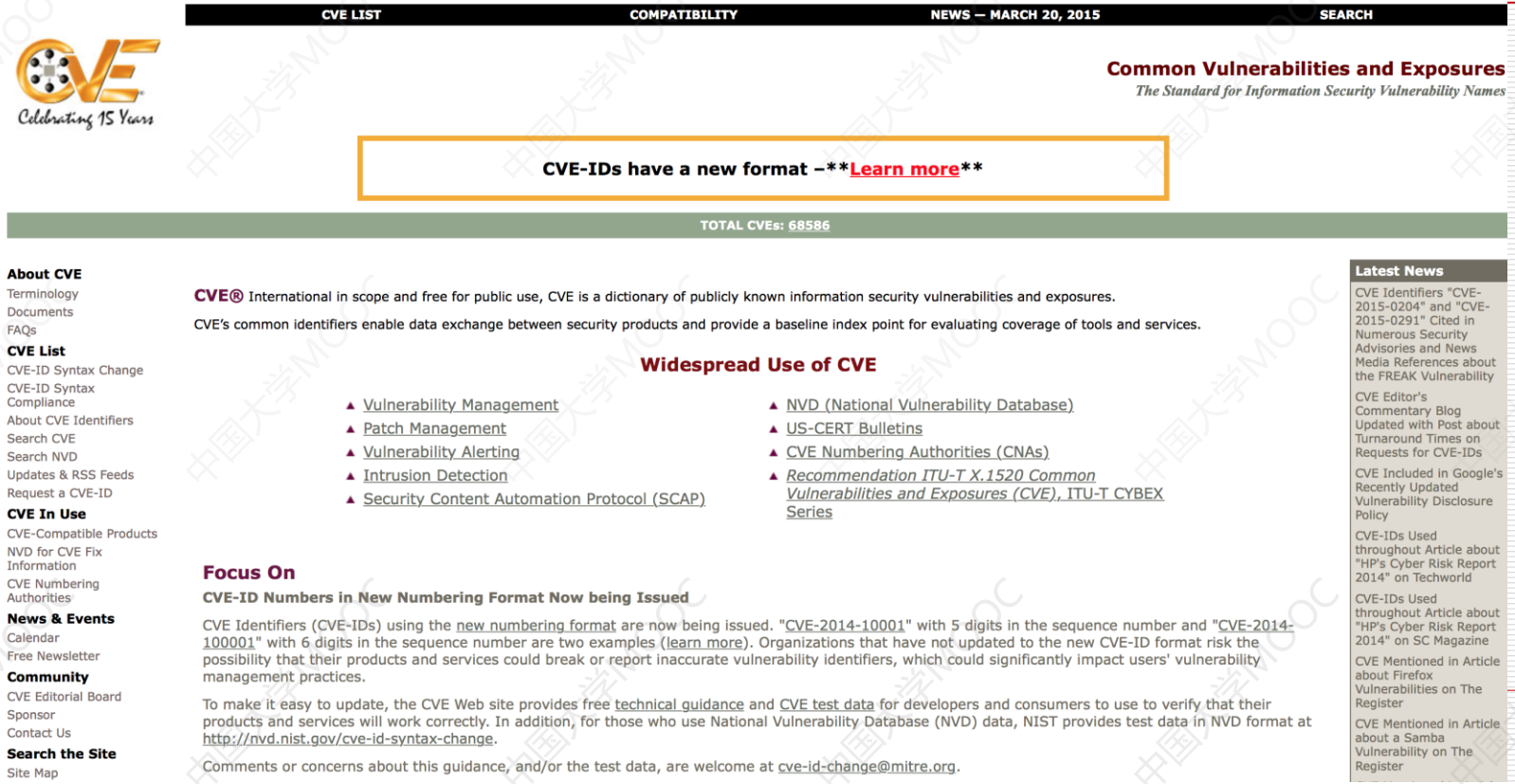
一般信息

摘要

此安全更新可解决 Internet Explorer 中一个公开披露的漏洞和 36 个秘密报告的漏洞。最严重的漏洞可能在用户使用 Internet Explorer 查看特制网页时允许远程执行代码。成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的客户比具有管理用户权限的客户受到的影响要小。

对于受影响的 Windows 客户端上的 Internet Explorer 6 (IE 6)、Internet Explorer 7 (IE 7)、Internet Explorer 8 (IE 8)、Internet Explorer 9 (IE 9)、Internet Explorer 10 (IE 10) 和 Internet Explorer 11 (IE 11)，此安全更新的等级为“严重”；对于受影响的 Windows 服务器上的 Internet Explorer 6 (IE 6)、Internet Explorer 7 (IE 7)、Internet Explorer 8 (IE 8)、Internet Explorer 9 (IE 9)、Internet Explorer 10 (IE 10) 和 Internet Explorer 11 (IE 11)，此安全更新的等级为“中等”。有关详细信息，请参阅“**受影响和不受影响的软件**”部分。

CVE—“公共漏洞与暴露”平台



CNVD & CNNVD


登录 免费注册
CNVD
国家信息安全漏洞共享平台
CHINA NATIONAL VULNERABILITY DATABASE
首页
热点关注
漏洞列表
补丁信息
安全公告
统计查询
研究报告
工作体系
统计数据
高级搜索
成员单位工作贡献排名（2015-03-16 - 2
1,000
900
800
700
600
500
400
300
200
100
0
奇虎360
天融信
启明星辰
安天
恒安嘉新
北京神州绿盟科技
漏洞查询
证书查询
漏洞报送
漏洞跟踪
热点推荐
热点新闻
> More
关于GNU glibc函数库存在缓冲区溢出高危漏洞（“幽灵”漏洞）的情况公告 2015-01-29
微软披露影响所有Windows版本的高危漏洞 2014-11-18
关于GNU Bash存在远程代码执行漏洞的情况通报 2014-09-26
关于Internet Explorer VGX.DLL远程代码执行漏洞的安全公告 2014-04-28
关于Apache Struts 2存在补丁绕过漏洞的情况公告 2014-04-24
关于OpenSSL存在高危漏洞可被利用发起大规模攻击的情况通报（4月9日结果） 2014-04-09
上周最受关注漏洞
漏洞标题
点击数
1 phpMoAdmin任意命令执... [1286]
2 724CMS SQL 'ID'参数S... [1226]
3 IBM API Management信... [1226]
4 Apache mod-gnutls证书... [1208]
5 automount权限提升漏洞... [1201]
漏洞信息
补丁信息
> More
漏洞名称
点击数
时间
多个产品SMM本地代码执行漏洞 29 2015-03-27
漏洞趋势
周 月 年
2015-03-16 - 2015-03-22
50
45


中国国家信息安全漏洞库
China National Vulnerability Database of Information Security
首页
漏洞信息
补丁信息
业界新闻
漏洞提交
查询统计
分析报告
常见问题
合作伙伴
CNNVD 服务
基本服务
CNNVD漏洞基本通报服务，主要为用户提供漏洞信息基本通报服务（含Top5最受关注漏洞及信息安全漏洞月报）及与CNNVD相关...进入服务
1 2 3
业界新闻 更多..
利用Instagram API制 ... 03/27
黑客利用PDF生成 ... 03/27
SELinux防御被轻易 ... 03/27
朝鲜否认与韩国 ... 03/27
12306图片验证码被 ... 03/27
黑客可通过电脑 ... 03/27
分析报告 更多..
信息安全漏洞月通报(2015年2月)
信息安全漏洞月通报(2015年1月)
信息安全漏洞月通报(2014年12月)
信息安全漏洞月通报(2014年11月)
信息安全漏洞月通报(2014年10月)
信息安全漏洞月通报(2014年9月)
网站简介 更多..
中国国家信息安全漏洞库，英文名称
*China National Vulnerability Database
最受关注漏洞
1 厂商：X.Org 发布日期：2015-03-23
漏洞名称：X.Org libXfont 安全漏洞
漏洞编号：CNNVD-201503-409
补丁
2 厂商：OpenSSL 发布日期：2015-03-20
漏洞名称：OpenSSL'EVP_DecodeUpdate'函数整 ...
漏洞编号：CNNVD-201503-404
补丁
3 厂商：IBM 发布日期：2015-03-19
漏洞名称：IBM Rational DOORS Next Generation和 ...
漏洞编号：CNNVD-201503-357
补丁
4 厂商：Adobe 发布日期：2015-03-16
漏洞名称：Adobe Flash Player 资源管理错误 ...
漏洞编号：CNNVD-201503-321
补丁
5 厂商：Cisco 发布日期：2015-03-16
漏洞名称：多款Cisco产品授权问题漏洞
漏洞编号：CNNVD-201503-308
补丁
其他漏洞信息 更多..
CNNVD-201503-588 WebGate eDVR Manager ActiveX C ... 2015-03-27
CNNVD-201503-587 Websense TRITON AP-WEB 安全漏 ... 2015-03-27
CNNVD-201503-586 Websense TRITON和V-Series 跨 ... 2015-03-27
CNNVD-201503-585 Websense TRITON和V-Series 安 ... 2015-03-27
CNNVD-201503-584 Citrix Systems Command Center ... 2015-03-27
CNNVD-201503-583 Citrix Systems Command Center ... 2015-03-27
CNNVD-201503-582 Red Hat JBoss RichFaces 安全 ... 2015-03-27
CNNVD-201503-581 Cisco Mobility Services Engine ... 2015-03-27
CNNVD-201503-580 Cisco IOS XR DHCPv4服务器拒 ... 2015-03-27
CNNVD-201503-579 Cisco IOS和IOS XE Service Dis ... 2015-03-27
漏洞提交
漏洞提交须知
提交漏洞
站内搜索
请输入相关关键字
搜 索
补丁信息 更多..
1. CNPD-201503-0261 openssl-1.0.2a
2. CNPD-201503-0260 openssl-1.0.1m
3. CNPD-201503-0259 openssl-1.0.0r
4. CNPD-201503-0258 openssl-0.9.8zf
5. CNPD-201503-0253 openssl-1.0.2a
6. CNPD-201503-0247 requests_2.3.0-1ubuntu0. ...
Flash 已过期

乌云漏洞公布平台（404）

登录 | 注册

WooYun.org 加关注 13.2万

首页 | 厂商列表 | 白帽子 | 乌云榜 | 团队 | 漏洞列表 | 提交漏洞 | 安全中心 | 乌云招聘 | 知识库 | 公告

当前位置：WooYun >> 首页

WooYun支持在等级不够时使用乌云币提前查看漏洞

最新提交 (58)

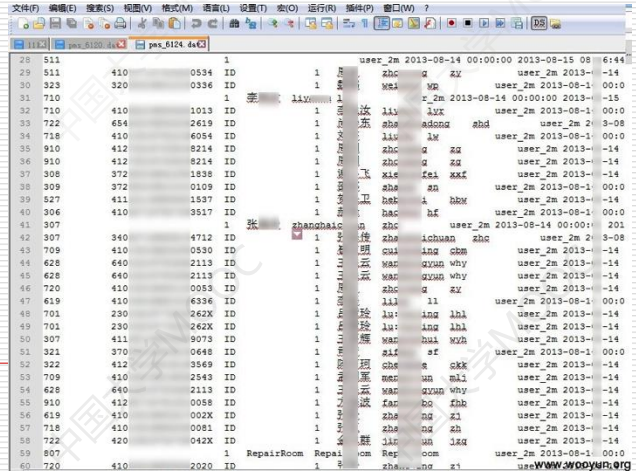
提交日期	漏洞名称	评论/关注	作者
2015-03-28	国家超级计算某中心某系统漏洞可导致内网漫游(点到为止)	17/39	管管侠
2015-03-28	一起飞一个弱口令引发的血案	0/1	路人甲
2015-03-28	易车某核心业务存在时间注入	0/0	Comer
2015-03-28	网站安全狗免杀神技+IIS6.0解析WebShell访问限制Bypass	2/18	RedFre...
2015-03-28	边锋网络某处SQL注入	0/1	路人甲
2015-03-28	Wecenter最新版注入之二（黑盒测试技巧）	2/19	Xser

最新确认 (1124)

提交日期	漏洞名称	评论/关注	作者
2015-03-28	美丽说另一站点MySQL盲注	0/1	lijiej...
2015-03-28	美丽说某站点MySQL报错注入(用户数据15万)	0/2	lijiej...
2015-03-28	和讯财经APP接口注射	2/6	greg.w...
2015-03-25	机锋网某dubbo未授权访问	0/10	路人甲
2015-03-28	拉手网部分商户信息泄露	0/2	咸鱼翻...
2015-03-28	拉手团购某分站存在post注入	0/3	路人甲

WooYun-2013-34935：

如家等大量酒店客户开房记录被第三方存储并因漏洞导致泄露



1.2.2 恶意软件

- “恶意软件”是指那些设计目的是为了实施特定恶意功能的一类软件程序。

- 典型的恶意软件种类：
  - 计算机病毒、蠕虫、特洛伊木马、后门、僵尸、间谍软件等。

恶意软件威胁

- **修改或破坏已有软件的功能**
  - 恶意软件运行之后，可以对同一运行环境中的其他软件进行干扰和破坏，从而修改或者破坏其他软件的行为。
- **窃取目标系统中的重要数据**
  - 数据库、文档、口令等（灰鸽子、上兴、Flame）
- **监视目标系统中的用户行为**
  - 对目标系统进行屏幕监视、视频监视、语音监听等
- **控制目标系统等**
  - Shell、屏幕控制、跳板等

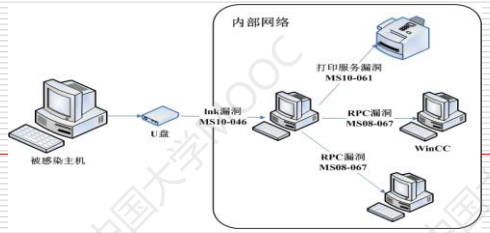
功能被破坏：武汉千余出租车计价失灵

- 2008年8月8日凌晨0时许，武汉市千余辆的士的计价器突然死机，导致人车停岗四小时。

浙江在线08月22日讯 8月8日凌晨零点起，杭城约有1100辆出租车计价器发生病毒感染，集体失灵。次日，等候维修的出租车陆续聚集在杭州市质量技术监督检测院外，形成了近3公里的“长龙”。这一天不仅仅是杭州的出租车计价器出了问题，武汉、厦门等地的出租车也遇到了这样的尴尬。这次出租车集体中毒事件让不少当天准备打的出行的市民受到影响，并且引起了人们广泛的关注。

Stuxnet(超级工厂病毒)：破坏伊朗核电站铀浓缩装置

- 2010年7月大面积爆发。
- Stuxnet病毒被多国安全专家形容为全球首个“超级工厂病毒”。
- 该病毒已经感染了全球超过 45000个网络，伊朗、印尼、美国等多地均不能幸免。
- 其中，以伊朗遭到的攻击最为严重，**该病毒已经造成伊朗布什尔核电站推迟发电**，60%的个人电脑感染了这种病毒。



付款被劫持

楚天都市报

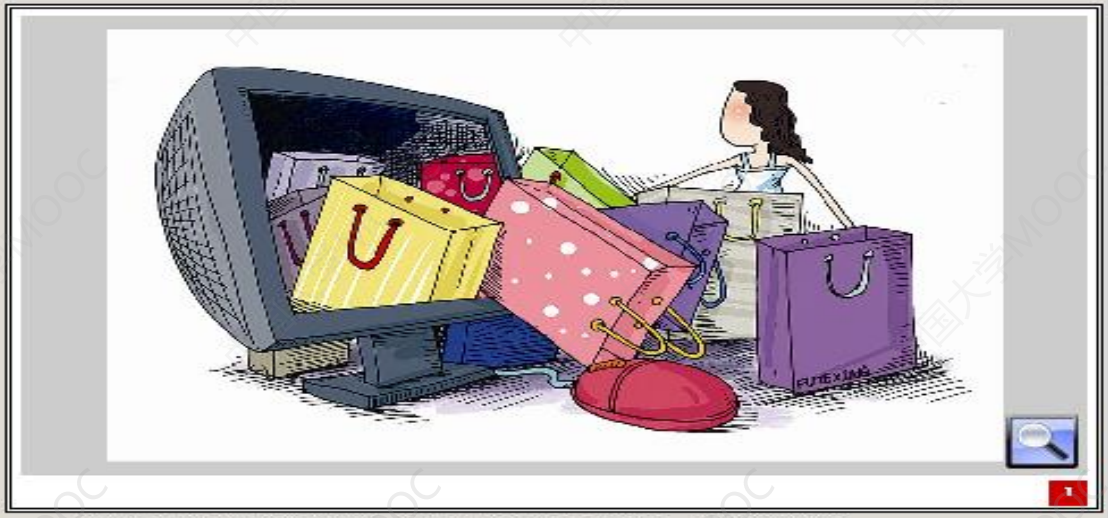
2010年9月13日 星期一

返回首版 | 版面导航 | 标题导航 | 最小化 | 退出

日期检索： 文章搜索

2 2010/09/13 网购黑客陷阱调查·案例

图文：网购货款被黑客劫至陌生账户



本报记者王昱晔 张泉 见习记者夏宇 统筹：记者杨向明

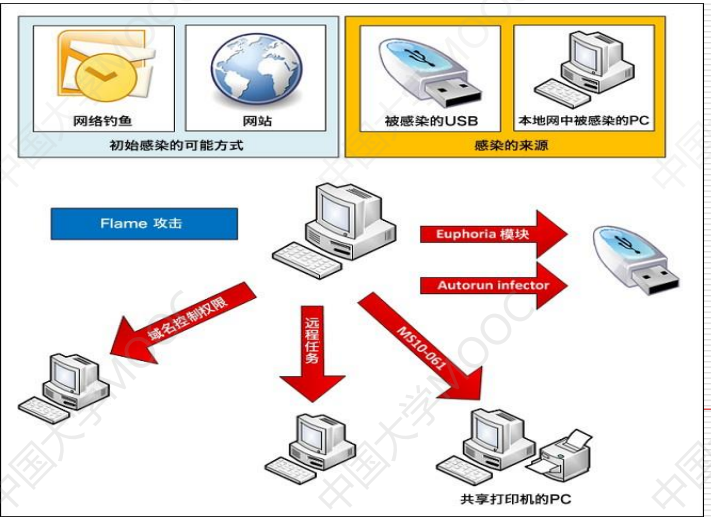
网上购物因其便捷、实惠、安全，已成为人们特别是年轻一代的生活方式之一。然而，武昌顾先生的亲身经历则提醒大家，网购在安全性方面亦可能存在漏洞。

机密数据泄漏

- 中国机密遭境外网络间谍围攻（攻击、策反和传输）：
  - 中原某军工科研所彭某：**国防科工委办公厅的中秋贺卡**（参与中国海军潜艇科研项目的大量军工科研项目的资料泄露）
  - 湖南某大学孙某（参与北方某军工院校重要军工项目）：**国际学术会议的电子邀请函**（重要军事武器项目资料泄露）
  - 能源化工某领域西南地区学术带头人周某：**朋友的电子贺卡**（涉及22个省的多个重大能源化工项目资料泄露）

Flame（火焰）

5 种加密算法，3 种压缩技术，至少 5 种文件格式，65万行代码，编写复杂。卡巴斯基实验室表示，要全面了解Flame病毒，可能得花上10年时间。



“网络重武器”火焰病毒攻击伊朗能源设施

发布时间:2012-5-30 13:39:09

俄罗斯电脑病毒防控机构卡巴斯基

Flame病毒体积较大 全面了解需10年

来源：腾讯科技　编辑：userz　发布时间：2012-05-29 15:34　浏览：　发表评论

北京时间5月29日消息，据国外媒体报道，俄罗斯**反病毒公司**卡巴斯基实验室(以下简称“卡巴斯基”)近日表示，一种名为“Flame”的恶意间谍软件已在中东和北非部分地区得以大范围传播，该病毒已经或即将造成的巨大危害不可忽视。

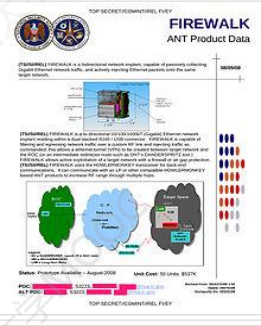
该病毒由卡巴斯基首先发现，并根据该病毒内部代码所含字样，而将其命名为“Flame”。卡巴斯基称，Flame实际上是一个间谍工具包。至少过去两年中，Flame病毒已感染了伊朗、黎巴嫩、叙利亚、苏丹、其他中东和北非国家的相应目标计算机系统。

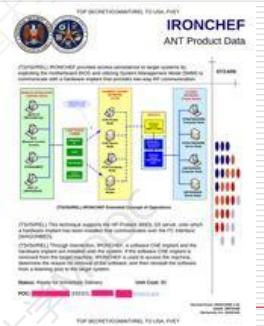
破坏＋窃取

- 三大恶意软件攻击目标互补：
  - Stuxnet ：破坏伊朗核设施（2010年被发现，4个系统漏洞，＋2个WinCC漏洞）
  - Duqu：窃取伊朗工业控制系统数据（2011年被发现）
  - Flame：窃取伊朗石油部门的商业情报。（2012年5月被卡巴斯基发现，部署于至少4年以前）

国家背景的攻击行为日益突显，实力雄厚，组织性强

- NSA监听军火库－ANT：
  - 在全球网络中为情报部门开启“后门”，并植入间谍软件
  - 从计算中心到个人电脑，从笔记本到手机无一能够幸免

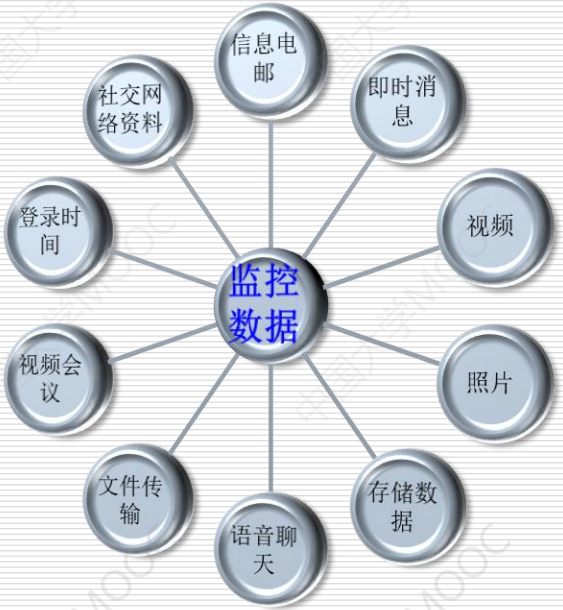




斯诺登与“棱镜”计划

- 斯诺登爆料：
  - “棱镜”窃听计划，始于2007年的小布什时期。
  - 棱镜包括两个秘密监视项目：
    - 监视、监听民众电话的通话记录，
    - 监视民众的网络活动。
  - 对中国的黑客 入侵
    - 对中国电信运营商的短信窃取
    - 对中国六大骨干网之一的教育科研网总节点清华大学的入侵等


PRISM
美国棱镜计划被指
监控隐私


监控数据
信息电邮
即时消息
视频
照片
存储数据
语音聊天
文件传输
视频会议
登录时间
社交网络资料


9大公司
微软
谷歌
雅虎
Facebook
Pal Talk
YouTube
Skype
AOL
苹果

❶美国监听计划披露及内容

“巧言”计划（blarney）：用来收集通过骨干网收发电子邮件或浏览互联网的计算机和设备的元数据。

“Xkeyscore”计划：范围最广的网络监听项目，150个地点监听700多个服务器，情报人员可以在未授权的情况下对个人的互联网活动进行“实施监控”。

“精灵”项目（GENIE）：美国侵入外国计算机网络，将恶意软件秘密植入世界各地电脑、路由器、防火墙，置于美国秘密控制下。

❶美国监听计划披露及内容

“涡轮”项目（TURBINE）：在线自动化系统收集大量恶意植入软件信息，并进行主动攻击。

“上游”（Upstream）项目：在承载互联网骨干通信内容的光缆上安装分光镜，复制其通信内容。

“碟火”（Dishfire）项目：存储了多年来全球各地的大量短信，以备需要时查看。

“金融情报组”（Tracfin）项目：则收集了大量的信用卡购物信息。

❶美国监听计划披露及内容

监控对象：NSA在欧盟总部和联合国总部安装监控和窃听设备，长达5年之久。

美国大使馆：80多个美国使馆开展监听计划，并且不为驻在国所知。
驻美大使馆及代表处（38个）：欧盟国家、日本、墨西哥、韩国、土耳其、印度。

将“秘密级”目录表把“情报优先考虑对象”分为一级到五级。

最重要的监听目标：中国、俄罗斯、伊朗、巴基斯坦、朝鲜、阿富汗。
反间谍工作“战略重点”：中国、俄罗斯、伊朗、古巴、以色列。

NSA vs 影子经纪人

美国国家安全局被黑 顶尖黑客工具打包售价5.65亿美元

作者：nana 星期三, 八月 17, 2016 0

分享:

黑客团伙"影子经纪人"宣称：已黑进美国国家安全局(NSA)"方程式"黑客小组，并盗取大量黑客工具和漏洞利用代码，将立即在网上出售！

卡巴斯基实验室将其发现的"方程式"黑客小组形容为高度复杂的威胁Actor，是前所未见的世界上最高端的网络攻击小组，就在你的身边，以"震网"和"火焰"病毒作者之姿傲视群雄。专家认为，方程式小组与NSA关联颇深。2015年，他们的大部分目标都集中在阿富汗、伊朗、印度、马里、巴基斯坦、俄罗斯和叙利亚。

黑掉这么一个光环闪耀的黑客组织绝非易事，但也不是不可能的。影子经纪黑客团伙就已经搞了个网上拍卖，供感兴趣的实体竞价方程式小组的网络武器。

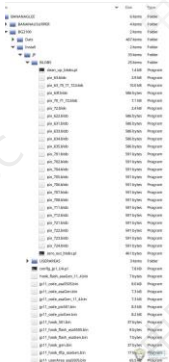
NSA被黑，或有可能成为第二个TheHackingTeam事件！

2016-08-16 Mickeyyyyy FreeBuf

事件概述

根据国外媒体的最新爆料，美国国家安全局（NSA）貌似遭到了黑客的攻击。这个黑客团伙声称他们入侵了"Equation Group"（方程式组织），并将他们从该黑客组织的计算机系统中所获取到的大部分黑客工具全部泄漏在了互联网上。

这一黑客团伙自称为"The Shadow Brokers"（影子经纪人），目前他们已经开始在网上逐步公开盗窃所



中情局vs维基解密

中情局数千份机密文档泄露：各种0day工具、恶意程序应有尽有

clouds 2017-03-08 +5 共1216545人围观，发现 22 个不明物体 资讯

维基解密最近再度获取到了数千份文件
具及其拥有的入侵能力。实际上，以近
具可能也就不算什么了。

本周二，维基解密曝光了8761份据称是
码），这些数据代号为Vault 7，文件日
该能够很大程度表现CIA的黑客技术和
Zero”（元年）。

维基解密创始人阿桑奇表示，文件显示出
失控”，以下为维基解密对此次曝光事件

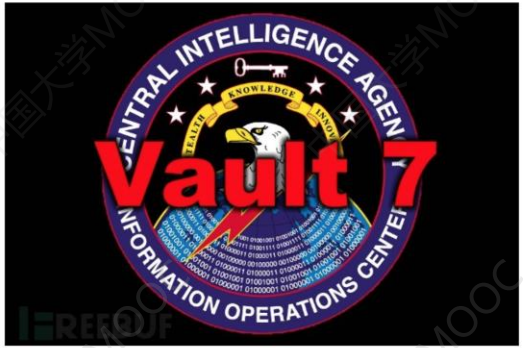
维基解密专题：CIA网络军火库-Vault 7:

FREEBUF 首页 分类阅读 文库 专栏 公开课 商城 企业服务 用户服务

曝光文件说明

维基解密称这些泄密文件来源CIA兰利总部网络情报中心（CCI，Center for Cyber Intelligence）与外网隔绝的高度机密局域网，文件不仅暴露了CIA全球窃听计划的方向和规模，还包括一个庞大的黑客工具库，网络攻击入侵活动对象包括微软、安卓、苹果iOS、OS X和Linux等操作系统和三星智能电视，甚至是车载智能系统和路由器等网络节点单元和智能设备。

维基解密进一步透露：这些文件中涉及的黑客工具既有CIA自行开发的软件，也有据称是得到英国MI5（军情五处）协助开发的间谍程序。其中包括恶意软件、病毒、特洛伊木马、武器化的‘0day漏洞’、恶意软件远程控制系统及其相关文件等。这些‘网络武器’的代码行数总计可达数亿之多，这就使其持有者完全有能力黑进CIA。目前，这些文件档案已经在前美国政府黑客和承包商间以未经授权的手段流传，维基解密得到的这些文件来自他们中的某人。



2001年以来，CIA获得的政治权利和资金预算远远超越了NSA，他们不仅成立了臭名昭著的无人机编队，还组建了一支具备全球入侵攻击能力的隐蔽黑客舰队，从某种程度上，与NSA的黑客攻击能力形成竞争。

2016年底，CIA网络情报中心（Center for Cyber Intelligence）下属的黑客部门已经雇佣了超过5000人参与其网络间谍行动，并开发了1000多个包括黑客系统、定制木马病毒、和其它“武器化”工具在内的间谍程序。至2016年，CIA黑客部门运行的代码量甚至比FaceBook还要多，这种规模让人吃惊，而也从某种意义上说，CIA成立了自己内部的“NSA”。

维基解密说，希望借这些曝光文件促成公众讨论：CIA的黑客能力是否已经超过他们所获得的授权？阿桑奇在一份声明中

1.2.3 软件破解

- 软件破解，即通过对软件自身程序进行逆向分析，剖析软件的注册机制，对软件的各类限制实施破解，从而使得非法使用者可以正常使用软件。

- 软件破解是对软件版权和安全的一个重大挑战。