安天周观察

主办：安天　2015 年 9 月 14 日（总第 8 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加“网络与信息安全智库论坛”

8 月 31 日 -9 月 1 日，“网络与信息安全智库论坛”在上海社会科学院成功举办，会议主题为“网络与信息安全智库的挑战与机遇”，来自全国的权威政策专家、产业精英和专业人士，就信息安全智库发展、制度创新等议题献计献策。

论坛聚焦新形势下网络安全和智库的机遇与挑战这一议题，深入探讨“面向网络强国的信息安全智库发展”、“面向网络强国的信息安全制度创新”、“面向网络强国的信息安全产业变革”三大议题。

安天技术负责人参加并在论坛上发表了《赛博安全的支点—独立安全厂商的价值思考》的报告，报告解读了当前大国博弈的层次结构，通过 FireEye 等厂商对美国国家安全战略的支撑价值分析，提出了“独立安全厂商是大国赛博安全的支点”。同时还提出了我国在网络安全上存在一些认知盲点，如过度强调信息技术的短板，但又不在安全环节上有效布防；过度看重内容安全、网站安全，但对重要基础设施被入侵，信息被窃取的问题投入不足等。并对如何改善当前形势提出了个人建议。

【安天 CERT】发布

《利用路由器传播的 Dyreza 家族变种分析》报告

（第四版）

卡巴斯基和 FireEye 的产品中发现 0day 漏洞

9 月 9 日，漏洞研究人员分别在卡巴斯基和 FireEye 公司的产品中发现了一些安全漏洞，恶意攻击者可以利用这些漏洞来对用户进行攻击。

Ormandy 是谷歌公司的一名安全研究人员，这些年来，他披露了许多存在于其他软件开发商产品中的漏洞。

与此同时，另一名安全研究人员在美国时间的上周末发表了一份重要的声明，并表示他在 FireEye 公司的软件中发现了安全漏洞。（文章来源 http://www.csoonline.com/article/2980937/vulnerabilities/researcher-discloses-zero-day-vulnerability-in-fireeye.html）

报评

工程化能力是网络安全的能力之本

当前，网络安全技术和产业吸引了更多目光与关注，对于网络安全产业的发展和崛起，形成了很好的预热。同时这些关注与报道中，也带有把网络安全更多的解读为“渗透攻击”、“漏洞挖掘”、“硬件破解”等技术分支领域，带来一种网络安全将由个别天才黑客决定胜负的舆论导向。对单点渗透攻击、漏洞挖掘能力的推崇，无疑会让人更关注网络安全，有积极的一面，在网络安全长期没有获得真正重视的情况下，能够起到提升关注，吸引从业者的价值。但这不是网络安全的全部，网络安全的基础能力是“工程化能力”。

网络安全技术是因实际网络安全威胁的挑战应运而生，是以保障用户安全价值为核心诉求。安全的研究和能力要完成用户侧的转化，就是要转化为可在用户方部署与实施保障的实际产品与服务能力。工程能力由分为产品能力与支撑产品的体系能力和服务能等构成，涵盖了产品与体系设计、工程编码、测试改善、支撑体系体系的运维和相应的工作流程、前后台工程体系的接、协同、联动响应等问题。而无论是漏洞分析挖掘、还是渗透测试，最终也都要向实际的工程能力转化，才能达成用户实际的防护价值，同时及时对于漏洞分析挖掘和渗透测试等安全技术的分支，工程化也是使其事半功倍、能力系统化的唯一通路。

安天是一个草根起点的团队，即无天才 Founder，也无“大师”背书，安天的传统就是工程师文化，工程师文化的本质是解决问题的文化。安天培养的工程师团队的逆向思维，但更强调和强化架构和编码、研发能力。我们相信，工程化是安全能力之本，工程化能力依托产品工程体系和技术，依托工程师团队形成达成。用户普遍需要的是有效的安全产品和支撑保障。对一个工程师文化信仰的团队来说，任何不能转化为用户实际价值的能力，都不值得骄傲。就如同国土防御，固然需要特种部队。但其主体还是防御体系、装备体系和正规军，即通过产品体系所支撑起来的正规军。安全企业的荣誉感，不在于“我牛”、“我们牛”，而在于：服务用户，应对威胁，解决问题，保障价值。

每周安全事件

类 型	内 容
中文标题	黑客侵入火狐漏洞窃取敏感信息近一年之久
英文标题	Hacker had access to sensitive info about Firefox bugs for over a year
作者及单位	ZeljkaZorz，Help Net Security
内容概述	Mozilla 公司近日表示，一名攻击者从公司内部窃取了大量敏感的安全漏洞信息，并有可能借此向火狐用户发动攻击。该公司表示，他们早在 2014 年 9 月就证实了一些未经授权访问行为，但这类行为最早可以追溯到 2013 年 9 月。攻击者访问了 185 个未公开的漏洞，其中 53 个属于严重漏洞，43 个已经被修复。Mozilla 已经采取措施提高安全性，包括要求所有特权帐户重置密码、采用双因素身份认证技术等。
链接地址	http://www.net-security.org/secworld.php?id=18826

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周 6 个移动平台和 9 个 pc 平台的恶意代码家族值得关注

平台分类	关注方面	名称与发现时间	相关描述
移动平台恶意代码	新出现的样本家族	Trojan[Backdoor]/Android.BaseBr 2015-08-31	用户打开该恶意软件后，软件提示更新，实际为后台安装恶意子包操作，安装后在用户毫不知情的情况下自动发送扣费短信并拦截提示短信，为用户强行订购多种 SP 扣费服务，导致用户资费损失。
		RiskWare[Monitor]/Android.SpyMo 2015-08-31	该应用是一款间谍软件，安装后无图标，并伪装成数据备份图标，使用户无法辨别是否为系统应用，获取用户的联系人、通话记录、短信记录，以及 GPS 位置信息，并上传到远程服务器。
		Trojan[Spy]/Android.Mogap 2015-08-31	该应用伪装成系统应用，运行后删除图标，激活设备管理器使用户无法正常卸载，拦截短信，接受短信指令控制将收到的短信息以邮件的形式上传，造成用户隐私泄露。
		Trojan/Android.Najin 2015-08-31	该应用以情色内容引诱用户安装，启动后私自下载其他安装包，并发送短信订阅服务，存在恶意扣费行为。
		Trojan/Android.Uten 2015-08-31	该应用运行时会连接远程服务器获取相应的扣费指令，执行发送扣费短信、屏蔽运营商回执短信、自动回复向其发送验证短信等操作。
		Trojan[Downloader]/Android.DorD 2015-08-31	捆绑在不同的软件上。上传各种隐私信息，如用户电话记录信息、短信记录信息、联系人信息且会下载恶意软件，上传或者下载的 url 都是储存在通过 DES 加密算法加密的文件中。
PC 平台恶意代码	重要恶意代码相关事件样本	Trojan[Downloader]/Win32.Upatre 2015 年 9 月 1 日	该恶意代码能够下载其它恶意程序，通常以电子邮件进行传播。目前以 Upatre 家族为载体的木马家族有 Zeus、Rovnix、Dyreza、勒索软件和僵尸网络等。(威胁等级：中)
		Trojan[Backdoor]/Win32.Dyreza 2015 年 9 月 1 日	Dyreza 家族非常类似于臭名昭著的 Zeus 僵尸网络，它们都是利用浏览器中间人攻击，当被感染的用户访问特定的网站，则会注入恶意 Javascript 代码来捕获用户所输入的账号密码等信息。
	新出现的 0day	FireEye 核心产品 0day 漏洞 2015-09-07	研究人员 Kristian Erik Hermansen 从 FireEye 核心产品中发现一个 0day 漏洞，会导致未经授权的文件泄露。他还提供了一个简短的触发漏洞的例子以及用户数据库文件副本。
		Samba 文件共享服务存在远程命令执行 0day(CVE-2015-0240) 2015-09-07	该漏洞可以允许一个恶意的 Samba 客户端发送一个特定的 netlogon 数据包给 smbd 获得 smbd 运行的权限，而 smbd 的默认权限是 root，从而导致未经身份验证的攻击者都可以远程利用这个漏洞获得 samba 服务器的控制权限。
	本周较为活跃样本	RiskWare[Downloader]/Win32.LMN.gen 2015-08-31	此威胁是一种具有下载风险程序行为的木马类程序。在未经用户允许情况下，下载、安装其它程序(包括其它恶意程序和风险程序等)到用户电脑。
		GrayWare[AdWare]/Win32.Linkury.a 2015-09-01	此威胁是一种有广告行为的木马类程序，它会在未经同意的情况下下载并安装多个程序。如 IE 搜索条，推广的软件程序等。
		Worm[Net]/Win32.Allaple.e 2015-09-03	此威胁是通过网络传播的蠕虫类程序。其运行后复制自身到系统目录，衍生大量病毒文件。利用漏洞进行传播，可以盗取用户敏感信息。
		Worm[P2P]/Win32.Sytro.o 2015-09-03	此威胁是利用网络进行传播的蠕虫类程序。运行时复制自身到系统临时目录下，伪装成游戏注册码生成器，探测网络环境，传播自身。
		Virus/Win32.Nimnul.a 2015-09-04	此威胁是一个感染类病毒程序，主要感染 windows 可执行程序和 HTML 文件。具有 hook 系统函数、DLL 注入和感染可移动存储介质等功能。

黑客通过常见的汽车小工具切断克尔维特的刹车

Andy Greenberg / 文　　安天公益翻译小组 / 译


安全研究人员卡尔·科修尔和伊恩·福斯特

汽车攻击演示说明，数字攻击者能够跨越汽车的蜂窝连接信息娱乐系统和转向/刹车之间的鸿沟。但是，一项新的研究表明，黑客有可能采用更简单的方法，用一些小工具就可以控制汽车的主要功能。

在8月中旬的Usenix安全会议上，加州大学圣地亚哥分校的一组研究人员演示了一种无线攻击汽车的技术。他们用一个微小的商用设备(一个2平方英寸的小工具)，把它设计为可以插入到汽车和卡车的仪表盘，然后连接到仪表板上，并向其发送设计好的短信，这样就能够发送命令到汽车的CAN(控制器局域网络，控制汽车的物理组件)总线，从而启动雨刷，启用或禁用它的刹车。

“我们得到了一些这样的工具，将它们逆向工程，发现它们有一大堆的安全缺陷，这些工具能够提供多种方式来远程控制任何与它们相连的汽车组件。”该项目的主管，加州大学圣地亚哥分校的计算机安全教授斯特凡·萨维奇说。

加州大学圣地亚哥分校(UCSD)在攻击中利用的设备是法国公司Mobile Devices生产的OBD2诊断工具，该工具在企业客户中(如旧金山的保险公司Metromile)广泛应用。在Mobile Devices的企业经销商中，研究人员详细分析了保险公司Metromile的设备，该公司向其客户发放这些名为Metromile Pulse的设备，客户将其插入仪表板的端口，这样就能够跟踪汽车，并按照英里数收费。该公司已经与Uber合作，向合同司机提供这些设备，作为折扣保险计划的一部分。

UCSD研究人员于6月份首次就该工具的漏洞问题联系了Metromile，保险公司告诉《连线杂志》的记者，他们以无线方式提供了该工具的安全补丁。“当我们发现问题后，以非常认真地态度予以对待，补丁已发送到所有的设备中。”Metromile首席执行官丹·普雷斯顿在一次电话采访中说，安全更新是由Mobile Devices开发的，Metromile将其发送给了客户。

研究人员认为，右图的这些Mobile Devices公司的2平方英寸的OBD小工具的问题还远未得到解决。他们还通知Mobile Devices其硬件存在安全隐患，但是却被告知该公司的最新版本工具不会受到攻击。然而研究人员使用搜索工具Shodan扫描了互联网，发现除了Metromile设备，其他的Mobile Devices设备也能够被攻击。这些设备主要位于西班牙，可能是在西班牙舰队管理公司和Mobile Devices客户Coordina中使用。《连线杂志》希望Mobile Devices就此发表评论并给出其主要客户清单，但是Mobile Devices尚未回应。

Coordina通过其母公司TomTom Telematics发表了一份声明，称其分析了研究人员的攻击，认为攻击仅适用于旧版本的工具，并表示正在努力取代少数的旧工具。该公司的常务董事托马斯·施密特还指出，其设备的SIM卡电话号码是不公开的，因此不能通过短信联系，所以TomTom Telematics方面认为不会遭受Mobile Devices OBD工具的短信攻击。UCSD研究人员反驳说：“我们已经能够通过暴力破解，在不知道SIM卡电话号码的情况下能够向设备发送短信。”但他们也承认没有针对Coordina设备进行实际测试。

UCSD研究小组表示，在研究Mobile Devices的设备时，发现了若干严重的安全漏洞。该工具激活了“开发者”模式，允许任何扫描到它们的人通过SSH(计算机远程通信的常用协议)访问它们，它们存储了同样的私钥，黑客能够立即提取这些私钥，从而获得这种设备的“root”访问权限。

Mobile Devices的设备也被配置为通过短信接收命令，这种协议几乎没有任何身份验证，只要通过某个电话号码向这些设备发送短信，任何人都可以重写其固件或向汽车发送命令。

需要明确的是，研究人员在测试中发现的漏洞不仅限于一种汽车。UCSD研究人员说，他们能够劫持任何使用Mobile Devices设备的现代汽车的方向盘或刹车，这不仅是某台汽车的问题。他提到了研究人员查理·米勒和克里斯·瓦拉塞克的研究，他们发布了能够用于攻击丰田普锐斯和福特翼虎的代码，攻击者只需要访问汽车的OBD2端口就可以了。Mobile Devices尚未详细说明开发什么补丁来响应UCSD研究指出的漏洞。

UCSD研究人员萨维奇表示，虽然他们只是研究了某些设备，但是消费者和第三方OBD2设备厂商都需要考虑其汽车使用的设备的安全性。很多这种设备已经大量出现在市场上，已经发现了完整的远程漏洞利用代码，而且这些设备的管理很不规范，其使用也在越来越多，他认为还会出现其他问题。

原文名称	Hackers Cut a Corvette's Brakes Via a Common Car Gadget
作者简介	Andy Greenberg，Andy Greenberg是《连线杂志》的资深作家，研究领域涵盖安全、隐私、信息自由和黑客文化。
原文信息	2015年8月11日发布于《连线杂志》，原文地址 http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

【安天 CERT】发布

《利用路由器传播的 Dyreza 家族变种分析》报告

近期，安天 CERT(安全研究与应急处理中心)收到大量用户反馈，称其收到带有可疑附件的邮件，经过安天 CERT 研究人员分析发现，这是一类利用垃圾邮件进行传播和下载的木马家族 Dyreza 的变种，其目的是窃取银行账号和比特币。该变种通过 Upatre 下载者进行下载，下载 Dyreza 变种的服务器均为路由器。攻击者将入侵的路由器作为 Dyreza 变种的传播服务器，在路由器中存放的文件均为加密文件，此外，该变种还具有反虚拟机功能。

安天研究人员分析到，不法分子首先利用弱口令等方法入侵互联网中的路由器，在路由器中存放加载的恶意代码程序，这些恶意代码程序的后缀名包括：.AVI、.ZIP、.TAR、.RAR、.PNG、.PDF；然后通过散布带有社会工程学性质的垃圾邮件，诱使用户运行附件中的 Upatre 下载者，Upatre 下载者连接被入侵的路由器，下载路由器中存放的加密的恶意代码程序，在用户系统中解密后得到 Dyreza 木马。Dyreza 家族非常类似于臭名昭著的 Zeus 僵尸网络，它们都是利用浏览器中间人攻击，当被感染的用户访问特定的网站(这类网站通常为金融机构或金融服务的登录页面)，则会注入恶意 Javascript 代码来进行捕获用户所输入的账号密码等信息。Dyreza 家族新变种的主要功能是窃取用户银行账号和比特币。

安天研究人员联想到 2014 年 4 月份的 CVE-2014-0160(心脏出血)漏洞即可入侵大量的路由器设备。安天 CERT 判定，Dyreza 家族与 Rovnix 家族有着必然的联系，它们使用相同的 Upatre 下载者进行传播，并使用相似的下载地址。在本报告发布前，安天又捕获到一个更新的 Dyreza 变种，在传播方式上，它使用与 Rovnix 攻击平台相似的下载地址，都使用 WordPress 搭建的网站，或入侵由 WordPress 搭建的第三方正常网站。

安天 CERT 研究人员表示，Dyreza 家族木马通过入侵路由器的方式进行传播，恶意程序放置在路由器中很难被用户发现，而反病毒产品通常无法直接扫描路由器。因此，不要使用路由器默认的口令，修改为高强度的口令。定期更新路由器固件，修复已出现的安全漏洞。关闭 SSID 广播，防止 SSID 被嗅探。使用安全性较高的 WPA2 协议、AES 加密算法。禁用 DHCP，开启 MAC 地址过滤，仅允许绑定的 MAC 地址访问无线网络。(报告原文：http://www.antiy.com/response/dyreza.html)

恶意程序

安天【追影高级持续威胁分析系统】无需更新病毒库，即可实现对上述恶意程序进行有效检测，下为其自动形成的分析报告

该恶意程序由安天威胁检测系统发现，经过追影威胁系统分析。经由 BD 静态分析鉴定器、美国软件交叉索引(NSRL)鉴定器、可交换信息(EXIF)鉴定器、数字证书鉴定器、静态分析鉴定器、动态行为(默认环境)鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。依据动态行为鉴定器最终将文件判定为恶意程序。

该文件具有以下行为：删除自身；填充导入表(疑似壳)；读取自身文件；获取计算机名称；获取驱动器类型；打开自身进程文件；请求调试权限；释放 PE 文件；独占打开文件；遍历进程。

文件名	955D9364AE0AF753FC627D630883742F
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	492 KB
MD5	955D9364AE0AF753FC627D630883742F
病毒类型	恶意程序
恶意判定 / 病毒名称	Trojan/Win32.Yakes
判定依据	动态行为

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=955D9364AE0AF753FC627D630883742F

◆ 其他行为

行为描述	危险等级
删除自身	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
填充导入表(疑似壳)	★★	读取自身文件	★★
获取计算机名称	★	获取驱动器类型	★
打开自身进程文件	★	请求调试权限	★
释放 PE 文件	★	释放 PE 文件	★
独占打开文件	★	遍历进程	★