安天周观察

主办：安天　2015 年 9 月 21 日（总第 9 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加“2015 中国 – 东盟信息港论坛：网络安全”闭门会议

9 月 14 日，“2015 中国 – 东盟信息港论坛：网络安全”闭门会议召开，该会议邀请了 50 位来自中国与东盟各国的信息安全、网络安全和通信领域的政企高层和专家学者，就东盟与中国在网络安全领域的合作空间开展了深入的探讨。

安天技术人员以“AVL 检测引擎助力区域性安全产业与网络安全保障能力的本地化”为主题，提出了通过解决网络安全核心基础技术问题，如利用反病毒引擎授权等，发展安全产品外围能力，赢得发展网络安全核心技术的时间，进而建立本地化安全产业能力的建议。

安天代表在演讲中提到，东盟各国当前在资金和技术上的缺乏，使得在信息技术产品和核心技术领域要在短时期内有所突破十分困难。而当前网络空间的非对称性为东盟地区的网络安全构成极大的挑战。面对这些问题，应该以“外围助力”搭建本地安全屏障为契机，在短期保障信息安全的同时为“内核技术”的发展赢得关键时间。

【安天 CERT】发布

《大量 HFS 搭建的服务器被黑客利用进行恶意代码传播》报告（第四版）

非官方 Xcode 工具被植入恶意代码

9 月 14 日，国家互联网应急中心发布的“关于使用非苹果官方 Xcode 存在植入恶意代码情况的预警通报”，其中提到了开发者使用非苹果公司官方渠道的 Xcode 工具开发苹果应用程序（苹果 APP）时，会向正常的苹果 APP 中植入恶意代码。（文章来源 http://www.cert.org.cn/publish/main/12/2015/20150914152821158428128/20150914152821158428128_.htmll）

报评

穿透安全篱笆的“供应链”危机

上周，Xcode 给安全界带来了不小的震动。造成了巨大的影响，一些第三方渠道下载的 iOS 开发工具被插入恶意代码，XcodeGhost 直接把病毒代码嵌入了开发工具源头，造成开发者用此工具编译的软件都自动被装入了木马，从而带来了用户的数据主动上传。利用了这一“事半功倍”的新思路，躺枪应用不计其数。

对于安全界来说，从官方应急机构的提前预警，到多个厂商的接力分析，对于此事件接力式的分析也展示了网络安全界的集体力量。

如果对这一事件进行定性，我们将其称之为一起严重的供应链（工具链）污染事件，从目前来看其污染源是地下黑产，其穿透了若干道安全篱笆。值得深思的是，在今年 3 月份的时候斯诺登曝光的一份文档显示：NSA 曾考虑通过对 Xcode(4.1)SDK 进行污染，从而绕过苹果 AppStore 的安全审查机制，最终将带毒 APP 放到正规的苹果应用商店里。长期起来，国内安全的焦虑过多的集中围绕着 CPU 和操作系统的自主化展开，但有其他几方面问题没有得到足够关注。

Xcode 污染事件，正是通过工具链污染绕过了多个开放商的自我安全审核，与号称非常严格的苹果应用商店的上架审核。而大量开发商不坚持原厂获取开发工具，不审查工具的数字签名，暴露了 APP 领域的野蛮生长，忽视安全的现状。而这种被污染的 APP 到达用户终端后，并不需要依赖获取更高权限，依然可以获取大量有价值的信息。而同时，其也采用了类似于互联网客户端类似的信息采集聚合方式。而数据的聚合点，则位于境外的云服务平台上。

这一问题再度提醒我们，要跳出单点迷思，而从完整供应链、信息链角度，形成全景的安全视野、安全建模与评价、感知能力。同时，我们也要再度提醒我们需要警惕“建立一个完全自闭合的供应链与自循环的信息链方能安全自保”的小农安全观的卷土重来，在互联网和社会生活场景下，这本身就不可能实现。而中国政企网络的市场空间，完全不足以保证一个健康的闭环供应链的的有效生存，更别提其所必须要的安全性的持续改进。

同时，我们也需要看到，网络地下黑产的泛滥与无孔不入，其不仅将危害中国网民的安全，也侵害了中国国家安全，其让国家安全的防护边界变得模糊。因此在这一问题上投入更多的资源，进行更为强力、有效的综合治理，于国于民都非常必要。

每周安全事件

类 型	内 容
中文标题	宾夕法尼亚假日酒店信用卡信息遭恶意软件盗取
英文标题	Malware targets credit cards used at Pennsylvania Holiday Inn
作者及单位	AdamGreenberg，SC Magazine
内容概述	里程碑酒店管理公司(Milestone Hospitality Management)已通知曾入住哈里斯堡地区赫尔希酒店的客人，他们的信用卡信息遭恶意软件盗取，数量不详。被盗取的个人信息包括：姓名，信用卡账号，有效日期以及CVV编码等。该恶意软件感染了该酒店的房产管理计算机系统，个人信息可能已经被盗取。 目前该酒店正采取措施进行修复，并加强系统安全。所有受到影响的客人已经接到通知，并对其提供一年的信用卡监测和身份重建服务。
链接地址	http：//www.scmagazine.com/malware-targets-credit-cards-used-at-pennsylvania-holiday-inn/article/438597/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周8个移动平台和6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
移动恶意代码	新出现的0day	iOS 9以下AirDrop中存在严重漏洞 2015-9-16	该漏洞可以允许攻击者在iOS 9以下版本的苹果系统中秘密地安装恶意软件。对此用户没有任何的解决办法，无论用户采取怎样的措施，攻击者都可以替换掉用户的应用程序。(威胁等级高)
	新出现的样本家族	Trojan[Backdoor]/Android.Wroba 2015-9-10	该木马运行后激活设备管理器、隐藏图标。接收短信指令，根据指令拦截指定短信，伪造新版本通知下载恶意apk同时卸载正常程序，上传手机用户隐私信息至远程服务器地址。(威胁等级中)
		Trojan/Android.Zalyt 2015-9-15	该木马为一电池管理软件，会上传用户地理位置信息、imei、imsi、sim卡运营商信息等，还可能会监控短信收发内容并上传。(威胁等级中)
		Trojan[Backdoor]/Android.Cajino 2015-9-11	该木马通过预留的后门，推送指令，执行收集并上传用户手机中的照片、联系人、短信等，给用户造成了隐私泄漏和资费损耗。(威胁等级中)
		Trojan/Android.Koler 2015-9-08	该木马运行后在用户解锁屏及运行其它应用会以非法浏览色情为由不断弹出警告信息，提示用户需缴罚款后才能解除，其行为极为流氓同时会恶意勒索用户产生高额费用。
		RiskWare[Monitor]/Android.AnSmCon 2015-9-09	该木马安装无图标，初次运行会监听解锁广播，弹出设置界面，执行私自上传短信箱、通话记录等操作，泄露用户隐私。(威胁等级中)
		Trojan/Android.Xshqi 2015-9-09	该木马以“XX神器”作为伪装，诱骗用户安装并点击运行。监听并拦截短信，并将短信内容通过短信和email方式发送给恶意代码作者，泄漏用户隐私。(威胁等级中)
	较为活跃的样本	Trojan[SMS]/Android.Agent.sn	该木马运行后隐藏图标，会接收远程指令，向指定号码发送包含用户IMEI等信息的短信，联网上传用户通讯录等信息，并且还可以接收指令进行下载、安装和卸载apk，打开指定网页和拨打电话等操作。
PC平台恶意代码	新出现的0day	PowerPoint Silent Builder Exploit 2015-9-12	该漏洞允许将EXE & JAR转换成.PPS文件，它使用全新的编码，然后可以通过电子邮件发IM软件来进行传播。受影响的版本2003/2007/2010。(威胁等级高)
	活跃的格式文档漏洞、0day漏洞	CVE-2012-0158漏洞	该漏洞是一个栈溢出漏洞，在MSCOMCTL.OCX中存在错误，被利用来破坏内存，导致任意代码执行。主要通过电子邮件进行传播。(威胁等级高)
	较为活跃的样本	Virus/Win32.Virut.ce	此威胁是一种感染类程序。能够感染受损系统中的.exe和.scr文件。它还能通过连接IRC服务器来开启后门，允许远程攻击者在受感染计算机中下载并运行文件。
		Trojan[Downloader]/JS.Agent.hbs	此威胁是一个具有下载行为的JS木马程序。通常是嵌入到网页中，当用户访问带有木马链接的页面，则会通过JS木马进行下载其它恶意程序。(威胁等级中)
		GrayWare[AdWare]/NSIS.Adload.i	此威胁是一类广告件木马程序，一般通过捆绑其它文件进行传播。具有弹出广告，下载广告软件或是其它娱乐程序等恶意行为。(威胁等级低)
		Trojan[Dropper]/VBS.Agent.bp	此威胁是一种具有捆绑行为的木马程序。该家族会携带各种恶意软件，运行后会释放恶意软件并运行，窃取用户信息，占用系统资源，影响用户使用。(威胁等级低)

间谍组织 Turla 利用卫星通信隐藏 C&C 服务器

Stefan Tanase / 文　　安天公益翻译小组 / 译

你有没有观看过卫星电视？你对多样的电视频道和广播电台感到惊讶吗？你有没有对卫星电话或卫星感到好奇，是什么让他们发出信号呢？ 这与卫星网络链路有密不可分的关系。当你身处于一个 APT 组织，你需要处理许多不同的问题。其中一个最大的问题，就是如何不断占用和拆卸用于指令和控制 (C&C) 的域名和服务器，但这些服务器由执法机关使用或被 ISPs 关闭。一些最先进的威胁源或使用商业黑客工具的用户已经找到如何解决拆卸问题的方法，就是使用卫星网络链路。

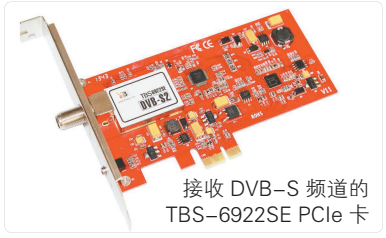
过去，我们曾看到三个不同的攻击源使用这样的链路来掩盖其操作，最有趣、最不寻常的就是 Turla 组织。Turla APT 组织，也被称为“Snake”或者“Uroboros”(都是顶级的 rootkit)，是至今为止最为高级的威胁组织之一。该网络间谍组织已经存在长达 8 年了，却很少被人知道，卡巴斯基实验室也是去年才发现 Turla APT 组织，该组织成员均说俄语，并且还发现其利用卫星通信中固有的安全缺陷来隐藏自己的位置和实施间谍活动。

Turla 集团之所以特殊，不仅仅是因为其使用工具的复杂性，如 Uroboros rootkit，又名“Snake”，还有通过内部局域网的多级代理网络绕过空气间隙的机制，其最精致之处在于卫星 C&C 机制。

据报道，自 2007 年以来，一些精英 APT 组织已经使用甚至滥用卫星链路来管理他们的业务，通常是 C&C 基础设施，Turla 就是其中之一。因为 C&C 服务器的真实位置和硬件无法轻易决定或物理捕获，卫星网络接收器可以安装在卫星覆盖面积的任意位置。Turla 组织劫持下游链接是高度匿名的且不需要有效的卫星网络订阅。

一开始，我们和其他研究人员都不清楚观察到的一些链接是否是攻击者购买的卫星商业网络连接，或者攻击者窃取了 ISPs 并在路由器通过执行 MitM 攻击来劫持流量。经分析，Turla 组织所使用的方法非常的简单和直接，并且高度匿名易于经营和管理。

Turla 组织所使用的简单方法就是 S21Sec 研究员 Leonardo NveEgea 在 2010 的 BlackHat 大会上介绍的劫持卫星 DVB 链接的方法。只需使用：卫星天线 (大小取决于地理位置和卫星)、低噪声块下变频器 (LNB)、专用的 DVB-S 调制器 (PCIe 卡，建议使用 TBS Technologies 公司的 TBS-6922SE)、电脑 (最好是 Linux 系统的) 这 4 种设备就可劫持卫星 DVB 链接。



接收 DVB-S 频道的 TBS-6922SE PCIe 卡

那么如何执行卫星网络劫持工作？为了攻击卫星网络链接，无论是卫星链接的合法用户还是攻击者自身的卫星天线都要指向特定的用于传播流量的卫星。攻击者会滥用卫星网络流量明文传输这一缺陷，具体的方式如下：一旦通过卫星的下游链接 IP 地址被检测出，攻击者开始监听来自互联网的数据包找到其指定 IP。当检测到这一数据包时，例如 TCP / IP SYN 数据包，他们识别其源并使用传统互联网线发回假的数据包 (例如 SYN ACK)。

同时，因为它流向未开放的端口，链接的合法用户忽略了此数据包，例如：端口 80 或 10080。这里需要强调，正常情况下，如果数据包遇到封闭端口，RST 或 FIN 数据包将被发送回源，表明没有想要的信息。然而，对于缓慢的链接，推荐防火墙和使用 DROP 数据包关闭端口，这也将造成滥用。

Turla 组织使用的卫星网络链接通常持续几个月，但不会太久，不清楚它是否由于组织自我强加的操作安全限制，还是由于恶意行为被其他机构关闭。这种技术方法用于网络电路，实现依靠各种各样的 ISPs 和伪造数据包劫持下游带宽。这在技术上是容易实现，并提供可能比其他传统方法更高的匿名度，如租用一个 VPS 或黑一个合法的服务器。

实现这种攻击方法，初始投资少于 1000 美元，定期维护每年少于 1000 美元，该方法如此简单和廉价，但令人惊讶的是没有更多的 APT 组织使用它。尽管这种方法为运作提供了一个高匿名度，它更直接依靠的是防弹托管，多个代理水平或黑客攻击网站。最后，应该注意的是，Turla 不是唯一使用卫星网络链接的 APT 组织。曾经在卫星 IPs 出现过黑客团队的 C&C，以及 Xumuxu 组织的 C&C，近期的是 Rocket Kitten APT 组织。如果这个方法在 APT 组织或网络犯罪组织之间变得普遍，这将为 IT 安全和反情报机构带来重大灾难。

原文名称	Satellite Turla: APT Command and Control in the Sky
作者简介	Stefan Tanase，卡巴斯基全球研究和分析部门高级研究员。
原文信息	2015 年 9 月 9 日 Kaspersky Lab 发布，原文地址 https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

【安天 CERT】发布

《大量 HFS 搭建的服务器被黑客利用进行恶意代码传播》报告

近期，安天蜜罐——“捕风”系统捕获到一个下载者样本。该样本运行后访问一个由黑客搭建的轻型文件服务器 (Http File Server)。通过使用捕风系统进行追溯与关联分析，分析人员发现目前有很多使用 HFS 搭建的服务器，通过对其中一个下载服务器进行监控，其在线 6 天的总点击量近 3 万次，可见其传播范围极广。该软件的“傻瓜式”教程颇受低水平的攻击者喜爱，同时由于其架设方便，便于传播等特点，已被黑客多次恶意利用。经过安天 CERT 分析人员进行关联与分析发现，目前这种轻型服务器工具已普遍流行。

在报告中，安天 CERT 技术人员分析了这类黑客入侵数据库惯用的手法，而且捕获到了另外一种类似恶意代码下载服务器地址。

目前，随着“黑色产业”的巨大经济利益诱惑，商业化的黑客工具包的使用变得越来越流行。这种能够“短平快”地产出恶意代码的方式让新手的入门门槛越来越低，一个没有经验的新手通过短时间的工具学习，就能轻松掌握入侵计算机窃密的方法。不仅仅是黑客工具，就算是一个普通的，用于构建正常服务的工具也能被轻易地被黑客利用，比如，轻量级 Http 服务器 (Http File Server) 正以其架设方便、便于操作等特点受到越来越多用户的青睐。与此同时，黑客也能利用在云端搭建轻型服务器与使用动态域名相结合的手段使得恶意代码能够更广泛、隐蔽地传播。这种轻量、便捷的服务器工具将会被越来越多的黑客或者新手使用，这无疑会加速恶意代码的传播。

这种工具式的黑客技术，让恶意代码的生产周期变的更短。依托商业工具进行攻击降低了攻击成本，同时提高了检测难度和传播速度。这种难度小、门槛低、成本少的攻击手法将使互联网的黑色产业链变得更加鱼龙混杂，同时也给互联网安全带来更多的挑战。(报告原文：http://www.antiy.com/response/hfs.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，经过追影威胁分析系统分析。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。

文件名	A52B473888FA975D37048D5959533001
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	180 KB
MD5	A52B473888FA975D37048D5959533001
病毒类型	恶意程序
恶意判定 / 病毒名称	Trojan[Downloader]/Win32.Agent
判定依据	动态行为

◆ 网络监控

IP	IP 地址	端口
	118.193.207.213	1010

域名解析	域名	IP
	118.193.207.213	118.193.207.213

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：

访问异常端口；访问 DNS；检查摄像头；获取 CPU 信息；连接网络；填充导入表 (疑似壳)；获取 socket 本地名称；获取系统内存；遍历进程。

◆ 其他行为

行为描述	危险等级
访问异常端口	★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
访问 DNS	★	检查摄像头	★★
连接网络	★	获取 CPU 信息	★★
获取系统内存	★★	填充导入表 (疑似壳)	★★
遍历进程	★	获取 socket 本地名称	★

完整报告地址：http://antiy.pta.center/_lk/details.html?hash=A52B473888FA975D37048D5959533001