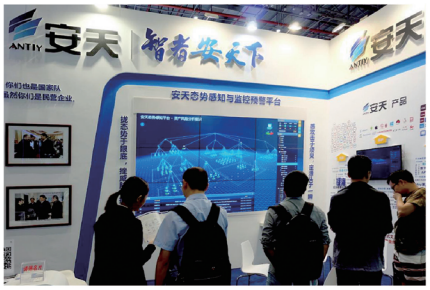
安天周观察

主办：安天　2017 年 9 月 17 日（总第 104 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天亮相 2017 年第四届网络安全宣传周

9 月 16 日，以“网络安全为人民，网络安全靠人民”的 2017 国家网络安全宣传周开幕式在上海举行。同期，由中央网信办、上海市人民政府指导，上海市互联网信息办公室主办，国家工业信息安全发展研究中心、上海市信息安全行业协会承办的“2017 网络安全博览会暨网络安全成就展”也在上海国家会展中心开展。

这已经是安天连续第四届参加网络安全宣传周活动。为响应习近平总书记在 4·19 网络安全和信息化工作座谈会上提出的“全天候、全方位感知网络安全态势”的要求，在本次博览会上安天带来了安天态势感知与监控预警平台的展示。该平台以安天的探海威胁检测系统（网络）、智甲终端防御系统（端点）、镇关威胁阻断系统（边界）等产品为探针，融入流量监测、端点扫描、主机蜜罐、主机检测、移动端检测五类安全数据。平台可面向安全监管部门、行业用户、关键基础设施管理机构、大中型企事业单位提供情报监测与预警、威胁检测与感知、深度分析与处置、安全业务管理与呈现的多角度安全业务与服务，实现网络安全态势全景感知和有效防护。平台的展示吸引了多位来宾驻足参观。



安天展台

安天以提升用户应对网络空间威胁的核心能力、改善用户对威胁的认知为企业使命。在不断提升自身技术能力的同时，也以自身独特的方式进行网络威胁与防护的科普与宣传。在本次博览会上，安天展位为大众带来了兼具知识性和趣味性的新版原创“威胁通缉令”扑克牌，吸引了来宾的关注。“威胁通缉令”定期更新，多年来将数百种计算机病毒进行形象化的表现，辅之以相关威胁和防护的解读，普及防病毒知识。这种体验式的互动，不仅有助于公众具象地认识安全威胁，也可以帮助一般使用者提高网络安全意识，掌握基本的计算机病毒知识。

本周，各地也将陆续开展网络安全宣传周的相关活动，活动将持续至 24 日。除上海外，安天也在哈尔滨及内蒙古等多地参与了当地的宣传周活动。安天技术负责人出席了黑龙江省网络安全宣传周开幕式，并进行了题为《关键信息基础设施的有效防护》的演讲。同时，作为宣传周活动的一部分，“安天网络空间安全学院”也在安天公司正式揭牌，为黑龙江地区的网络安全人才培养、建设贡献力量。

威胁通缉令

■ D-Link 850L 无线路由器 10 处零日漏洞被露

近日，安全研究人员 Pierre Kim 近期发现网络设备制造厂商生产的 D-Link 850L AC1200 双频 Gigabit 无线路由器（A、B 两个版本）存在 10 处零日漏洞，允许攻击者在拦截流量、上传恶意固件并获取 root 权限时远程劫持与控制受影响网络，致使所有连接设备遭受黑客攻击。

目前 10 处漏洞均未被修复。据悉，虽然 Pierre Kim 于去年发现并报告 D-Link-932B LTE 路由器存在多处高危漏洞，但并未引起公司重视。随后，类似事件于今年 2 月再次发生，研究人员发现 D-Link 产品存在 9 处安全漏洞。

不过，公司仍未作出任何响应。因此，Pierre Kim 此次发现漏洞后选择公开具体细节并呼吁 D-Link 能够妥善解决此类问题。（来源：http://thehackernews.com/2017/09/d-link-router-hacking.html）

■ 蓝牙协议被曝 8 处零日漏洞，逾 53 亿物联网设备易遭 BlueBorne 攻击

近日，据外媒报道，研究人员此前在蓝牙协议中发现 8 处零日漏洞，允许黑客远程操控 Android、iOS、Windows 与 Linux，甚至使用短距离无线通信技术的物联网设备。

目前，这些漏洞影响逾 53 亿受害系统，其中包括所有运行 9.3.5 或更旧版本的 iOS 设备、运行时间超过 Marshmallow(6.x) 或更旧版本的 Android 设备、运行 Linux 版本的数百万智能蓝牙设备，以及商业与面向消费者的 Linux 平台（Tizen OS）、BlueZ 与 3.3-rc1 系统。据悉，安全公司第一时间将漏洞上报至谷歌、苹果、微软、三星与 Linux 基金会。

然而，安全研究人员近期利用上述漏洞构建了一组攻击场景“BlueBorne”，允许攻击者完全接管支持蓝牙的设备、传播恶意软件，甚至建立“中间人”（MITM）连接，从而在无需与受害者进行交互时访问设备关键数据与网络。不过，要想快速实现攻击，除受害设备的蓝牙处于开启状态外，还需在攻击设备连接范围内。（来源：http://thehackernews.com/2017/09/blueborne-bluetooth-hacking.html）

每周安全事件

类 型	内 容
中文标题	.NET 0day 漏洞被用来传播 FinFisher 病毒
英文标题	NET Zero-Day Flaw Exploited to Deliver FinFisher Spyware
作者及单位	Eduard Kovacs；SecurityWeek
内容概述	近日，微软在本月安全更新中修补的漏洞中的一个 0day 漏洞被黑客用来传播 FinFisher 恶意软件，目标针对俄语用户。该漏洞安全专家向微软报告，漏洞编号为 CVE-2017-8759，它影响的是 .NET 框架中的 SOAP WSDL(Web 服务描述语言）解析器。攻击者可以利用漏洞远程执行代码，让目标用户打开特制的文档或应用程序。 在 FireEye 观察到的攻击中，黑客利用多个恶意文件利用漏洞，在最终部署有效 Payload(FinFisher) 之前会下载多个组件。微软认为攻击与黑客组织 NEODYMIUM 有关联，NEODYMIUM 去年使用 Flash Player 0day 漏洞传播 FinFisher。今年早些时候，安全厂商注意到一个名为“BlackOasis”的黑客，通过 Microsoft Office 零日漏洞 (CVE-2017-0199) 传播 FinFisher 恶意软件。
链接地址	http://www.securityweek.com/net-zero-day-flaw-exploited-deliver-finfisher-spyware

每周值得关注的恶意代码信息

经安天检测分析，本周有 8 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

平台分类	关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.ssaid.a[prv，rmt，spy]	该应用程序安装无图标显示，后台接收远控指令，窃取用户短信、联系人、通话记录、手机基本信息、手机程序安装信息、聊天软件信息、地理位置信息、邮箱账号、浏览器记录、SD 卡数据等隐私信息并上传至远程服务器，私自录音、拍照、拨打电话、拦截短信，造成用户隐私泄露和资费消耗。（威胁等级高）
	较为活跃的样本	Trojan/Android.Mobilespy.ak[prv，spy]	该应用程序伪装成系统应用，运行隐藏图标，窃取用户短信、联系人、通话记录、安装包等信息，上传用户的 WhatsApp 聊天记录到指定邮箱，造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.Triada.bc[exp]	该应用程序伪装 Google 更新程序，安装无图标，私自提权推送广告，静默下载安装未知程序，造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.SmsThief.bj[prv，fra，exp]	该应用程序运行会拦截短信，获取短信内容并存到本地 XML 文件中并上传到指定网址，会造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.b4aspy.i[prv，exp，spy]	该应用程序伪装成知名应用，包含恶意代码，会窃取用户照片、私自下载文件，造成用户隐私泄露和流量消耗，建议卸载。（威胁等级高）
		Trojan/Android.emial.gg[prv]	该应用程序运行隐藏图标，监听收件箱，通过邮件转发收件箱短信，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.FakeFB.l[prv，exp，fra]	该应用程序伪装成知名应用 Facebook，诱导用户输入账号和密码，然后将用户账号和密码通过短信发送给指定号码，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.SmsSend.nd[exp]	该应用程序运行私自发送含有特定内容的短信至指定号码，退出后隐藏图标，可能会造成用户资费损失，建议卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 内存损坏漏洞 (CVE-2016-7193)	当 Office 软件无法正确处理 RTF 文件时，Microsoft Office 软件中存在远程执行代码漏洞。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。（威胁等级高）
	较为活跃样本	Trojan[Ransom]/Win32.Locky	此威胁是一种可以加密用户文件并勒索比特币的木马家族。该家族样本运行后加密多种格式文件并向用户要求支付比特币解锁，有一定威胁。（威胁等级高）
		Trojan[Backdoor]/Win32.Dridex	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后可以连接远程服务器接受攻击者的恶意操作，可以删除文件、回传敏感信息等。（威胁等级中）
		Trojan[Dropper]/Win32.Pincher	此威胁是一种具有捆绑功能的木马类程序。该家族从用户系统窃取重要数据和信息，并将其发送给攻击者。该家族将恶意代码注入到被感染系统，并防止用户访问 Windows 的注册表文件。（威胁等级中）
		Trojan/Win32.Shifu	此威胁是一类可以窃取银行相关信息的木马家族，它可以注入系统进程，记录用户击键，并通过网络回传给攻击者。（威胁等级高）

欺骗：一种令人信服的网络防御新方法

Ofer Israeli / 文　安天公益翻译小组 / 译

美国国家安全机构的防御者如何在捕获标识演习中使用虚假数据来挫败攻击者并遏制伤害？

我们生活在攻击向量不断增加的世界中。黑客们使用越来越粗暴的方法攻破边界防御，包括采用窃取的凭证和后门、网络钓鱼、间谍软件和恶意软件、暴力破解等等。一旦攻击者成功地攻破了网络，他们通常会有足够的时间造成重大损害。根据威瑞森《2016 年数据泄露调查报告》，只有 25％的感染持续“几天或更少的时间”，火眼公司 2017 年 M-Trends 报告显示，尽管检测方法持续改进，发现网络攻击的平均时间仍然长达 99 天，其中，47％的感染是由外部来源通知受害者的。

人们对欺骗方法（最新的网络安全方法之一）的认识正在增加。Gartner 称之为“威胁欺骗”，并预测 10％的企业将在 2018 年之前采用某种形式的网络欺骗手段。欺骗依赖于攻击者的一个漏洞，攻击者认为他们在网络上找到的信息是真实的，他们收集的数据是可靠的。

高级攻击者如何接近网络呢？首先，黑客使用各种工具和技术，有条理地收集数据、分析数据，并在整个网络中横向运动。最初，当访问网络时，他们会有一点困惑。他们不知道到了哪里，也不知道目标在哪里。通过反复尝试，他们构建了网络环境的映射：网络本身以及它的使用方式。例如，他们可能会从一个员工的电脑中发现 SharePoint 服务器的线索，由此找到有关的文件和名称，这有助于他们确定

下一步的行动。攻击者越高级，其横向运动方法就越复杂；横向运动越多，映射就越详细。这种迭代过程使他们最终能够找到并感染目标。

当攻击者在网络中运动时，捕获他们的一种常见策略是蜜罐。蜜罐看起来像 PC 或服务器，其理念是，当攻击者访问蜜罐时，蜜罐会发出告警，提醒 IT 人员发生了攻击。蜜罐的问题是它们的部署和管理很费时，所以使用相对较少，这意味着当攻击者访问蜜罐时可能已经发生了重大感染事件。

欺骗和“捕获标识”

威胁欺骗采取不同的方法。美国国防部门设立了一项“捕获标识”演习，以测试欺骗战略的有效性。一个团队作为攻击者，他们执行多次攻击以捕获和检索被防御团队保护的目标。攻击团队不知道对方部署了欺骗战略。然后，防御团队在端点、服务器和攻击面上引入了各种虚假数据。欺骗类型包括“分享欺骗”，“Windows 凭证欺骗”和“文件欺骗”。

为了部署欺骗策略，防御团队使用了两个组件：一个用来传播欺骗信息的服务器和一个陷阱服务器。作为低成本的无代理解决方案，欺骗策略对网络服务和性能几乎没有影响，并且具有高度可扩展性。这些欺骗策略部署在整个企业的现有工作站、笔记本电脑和服务器上，不需要特殊的硬件。

当攻击团队发动攻击时，他们会立即发现欺骗信息，这些信息正是他们在网络中横向运动所需要的。访问这些欺骗信息会触发陷阱服务器，它会提醒防御团队发生了攻击。陷阱服务器还对攻击源进行实时取证，帮助防御团队确定攻击者的目标，并提供可操作的证据和制品来帮助他们遏制攻击。

同样，一家面临越来越多金融威胁的大型国际银行也部署了欺骗策略来补充现有的网络安全工具，并增加一种新的、更直接的威胁检测能力。该银行采用与美国国防部门类似的方法，为共享文件夹、服务器、Windows 凭证、SWIFT 和其它网络系统部署了一系列欺骗方案。随着欺骗解决方案到位，银行实现了接近即时检测的目标，误报率很低。当告警被触发时，安全团队能够观察攻击者在网络中的横向运动，收集取证数据并监控攻击行动。这使得防御团队更具战略性，可在造成损害之前终止攻击。

网络犯罪分子将会越来越聪明，越来越大胆。为保护网络，要不断加强防御措施。欺骗方法是一种强大的、先发制人的、互补的防御解决方案。有关人员在负责保护网络和数据资产时，应该考虑欺骗策略。

原文名称	Deception: A Convincing New Approach to Cyber Defense
作者简介	Ofer Israeli，以色列网络安全公司 Illusive Networks 的创始人和首席执行官。
原文信息	2017 年 9 月 12 日发布于 Dark Reading 原文地址 https://www.darkreading.com/threat-intelligence/deception-a-convincing-new-approach-to-cyber-defense/a/d-id/1329839?
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。

安天发布《Poison Ivy 样本分析报告》

近日，安天 CERT(安全研究与应急处理中心) 的分析人员发现，臭名昭著的 Poison Ivy 远控工具的新变种开始利用 Office 文件 (Word、Excel、PPT) 进行感染和传播。当受害者使用 Office 软件打开文档时，文档中的恶意代码就会执行，进而将远控木马下载到主机上。安天分析人员捕捉到了用来传输 Poison Ivy 的文档，并对其进行了系统分析。

Poison Ivy 是一款有着悠久历史的远控工具，自 2006 年前后即在网络上广泛传播。彼时 Poison Ivy 以短小精干著称，虽然服务端体积较当时市面上的主流木马来说较小，但其功能却十分齐全，在黑客手中曾是一款实用性很高的木马。

Poison Ivy 的开发者一直保持活跃，不间断地推出具有新功能的恶意代码。这也就导致该远控木马被多次用于针对性网络攻击事件中。影响较大的有 2015 年对泰国政府展开的渗透和网络攻击活动，和 2017 年被研究人员披露的 APT 攻击活动。

本次发现的新变种，主要是利用 Office 文档的宏功能来进行攻击载荷的下载和运行。当用户打开 PPT 文档时，文件中的恶意宏代码会调用 CMD 执行 VBS 文件，下载名为 Thumb.bmp 的文件。该文件尾部衔接一个 PE 文件，即 Poison Ivy 服务端，一个 64 位的 .Net 程序。该应用程序使用了大量的对抗分析技术，不仅对内部字符串进行加密，还调用了大量的用于抗调试的 API，且创建线程进行系统环境的检测。在确定运行主机环境没有问题之后，攻击载荷会将 DLL 注入到 Svchost 进程中，开展进一步的工作流程。

除此以外，恶意代码还通过加密的配置数据，访问 PasteBin 获取 C&C 的服务器信息，这无疑增加了从流量侧发现威胁的难度。

随着抗调试、免杀技术的不断丰富，同时要求恶意代码检测的技术和方法能及时扩充。保持长时间持续对恶意代码的杰出检测能力，也是对反病毒厂商严峻的考验。

目前，安天追影高级威胁鉴定器已经实现对该样本的检出。

蠕虫程序

安天【追影威胁分析系统】无需更新病毒库，依据行为即可实现对上述蠕虫程序进行有效检测，以下为其自动形成的分析报告：

文件被页面手工提交发现，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、动态行为 (Windows7) 鉴定器、静态分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、静态分析鉴定器将文件判定为木马程序。

根据动态行为 (Windows7) 得出该文件具有以下行为：查找指定内核模块、创建特定窗体、获取驱动器类型、访问文件尾部、获取系统内存、打开自身进程文件、独占打开文件、设置文件属性为隐藏、获取计算机名称。

文件名	e7931270a89035125e6e6655c04fee00798c4c2d15846947e41df6bba36c75ae
文件类型	Document/Microsoft.PPTX[:PowerPoint 2007-2012]
大小	34 KB
MD5	6957BB720CD6AA0E9736026F58DA1210
病毒类型	蠕虫程序
恶意判定 / 病毒名称	Trojan[Downloader]/VBS.Agent
判定依据	静态分析

运行环境

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、ie9、office2007、flash、wps、FoxitReader、adobe reader

报告地址：https://antiy.pta.center/_lk/details.html?hash=6957BB720CD6AA0E9736026F58DA1210

其他行为

行为描述	危险等级	行为描述	危险等级
查找指定内核模块	★	创建特定窗体	★
获取驱动器类型	★	访问文件尾部	★
获取系统内存	★★	打开自身进程文件	★
独占打开文件	★	设置文件属性为隐藏	★★
获取计算机名称	★		

文件操作

操作	文件路径
新建	c:\users\ks32\appdata\local\temp\cvr5b96.tmp.cvr
新建	c:\users\ks32\appdata\local\temp\36023462.od
新建	c:\progra~2\micros~1\office\data\opa12.dat
新建	c:\2d8b650c36f44ef3a24575e53eb9ad9b\share\~$target.pptx