安天周观察

主办：安天　2017 年 6 月 12 日（总第 90 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

风雨十七载，我们在路上

——安天举办成立 17 周年纪念日活动

2017 年 6 月 6 日，是安天成立 17 周年的纪念日，安天各地通过视频直播的方式，召开全员大会，不忘启程的初心，树立前进的信心。

在过去的一年中，安天业务持续增长，员工人数不断增加，在全员大会上，安天创始人、首席技术架构师再次为大家全方位解读了《安天价值观读本》，从安天名字与LOGO的由来讲起，回顾了安天创业的历史，从企业口号的变迁看安天不同阶段的发展，并向大家强调了安天的底线和威胁驱动的能力的建设导向。安天始终坚持用户价值信仰，安天人始终走在奋斗的道路上，并始终以工程师来定位自己。他指出，“我们在路上”是安天当前的状态，并且将一直持续下去。同时他表示，安天目前正处于第三次创业时期，面对变革，安天要坚持做能力型安全厂商，坚持用户第一的信仰，为客户提供更优质的服务。

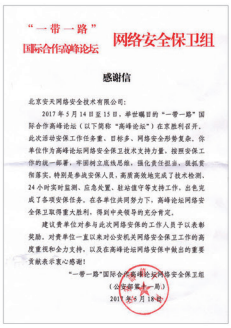
安天总裁胡忠华也在会上发表了演讲。他从安天的业务和经营等层面回顾过去一年取得的进展，但指出“革命远未成功”，他提醒大家要抓住机会，不断贴近客户、分析客户需求，树立灯塔式的解决方案。安天创立 17 周年，是又一个新的起点，面对新征程，安天信念不变，再次启航。

新型攻击技术：网络犯罪分子采用 PowerPoint 演示文稿传播恶意软件

近日，据外媒报道，安全专家发现网络犯罪分子正利用一种新型攻击技术传播恶意软件，即通过 PowerPoint 演示文稿诱导用户在系统中下载执行恶意代码。调查显示，当用户打开 PowerPoint 演示文稿时会看到标注“正在加载……请等待”字样的蓝色超链接。如果用户将鼠标悬停在该链接上，即使不点击也会触发 PowerShell 代码执行操作。一旦用户打开该文档，PowerShell 代码就会被连接至“cccn.nl”域名并下载执行负责传送恶意软件程序的文件。

安全研究人员表示，用户设备中受视图保护的安全功能会通知用户操作风险，并提示用户启用或禁用该项操作。此外，研究人员在分析此次攻击活动时还观察到网络犯罪分子利用该技术传播银行木马 Zusy、Tinba 与 Tiny Banker 新变种。（来　源：http://hackernews.cc/archives/10953）

安天收到“一带一路”国际合作高峰论坛网络安全保卫组的感谢信


“一带一路”国际合作高峰论坛　网络安全保卫组

感谢信

北京安天网络安全技术有限公司：

2017 年 5 月 14 日至 15 日，举世瞩目的“一带一路”国际合作高峰论坛（以下简称“高峰论坛”）在京顺利召开。此次活动安保工作任务重、目标多，网络安全形势复杂。你单位作为高峰论坛网络安全保卫技术支持力量，按照安保工作的统一部署，牢固树立底线思维，强化责任担当，狠抓重保落实，特别是参战安保人员，高质高效地完成了技术检测、24 小时实时监测、应急处置、驻站值守等支持工作，出色完成了各项安保任务，在各单位共同努力下，高峰论坛网络安全保卫取得重大胜利，得到中央领导的充分肯定。

现对贵单位对参与此次网络安保的工作人员予以表彰奖励，对贵单位一直以来对全国公安机关网络安全保卫工作的高度重视和全力支持，以及在高峰论坛网络安保中做出的重要贡献表示衷心感谢！

“一带一路”国际合作高峰论坛网络安全保卫组

（公安部第一研究所）

2017 年 5 月 18 日

5 月 18 日，“一带一路”国际合作高峰论坛网络安全保卫组向安天发来感谢信，感谢安天在“一带一路”国际合作高峰论坛（以下简称“高峰论坛”）网络安全保卫工作中做出的贡献。

“高峰论坛”是国际社会各方共享互利合作成果的盛会，也是加强国际合作，对接彼此发展战略的重要合作平台，因此，做好网络安全保障工作至关重要。安天在本次“高峰论坛”网络安全保卫工作中，按照安保工作的统一部署，高质高效的完成了技术检测、24 小时实时监测、应急处置、驻站值守等支持工作，出色完成了各项安保任务，有效保障了“高峰论坛”期间的网络安全。

安天作为网络安全应急服务支撑单位之一，多次在重大网络事故和网络安全事件的响应中发挥关键作用，曾参加过十七大、十八大、2010 年起的历届两会、北京奥运会、上海世博会、广州亚运会、2014 年 APEC 会议、抗战胜利 70 周年阅兵、G20 峰会等重大活动的安保工作，并荣获重大活动信息安全保卫工作突出贡献奖。安天会一如既往，在维护国家网络安全工作中贡献自己的一份力量。

每周安全事件

类 型	内 容
中文标题	漏洞扫描器 Nexpose 默认的 SSH 配置中启用了过时加密算法
英文标题	Nexpose appliances were shipped with a weak default SSH configuration
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，网络安全公司 Rapid7 的专家近期披露 Nexpose 漏洞扫描器出货时默认的 SSH 配置中存在一个安全漏洞（CNNVD-201701-424、CVE-2017-5243），可允许黑客利用过时算法实施密钥交换等功能。Nexpose 扫描设备能够帮助用户分析漏洞并减少黑客攻击。由于 Nexpose 启用了较弱及过时的加密算法，涉及硬件设备认证的攻击将更容易得逞。 专家提醒，具有 root 访问权限的管理员可在 Nexpose 中编辑 /etc/ssh/sshd_config 文件修复问题，以确保设备仅接受现代密码、密钥交换与 MAC 算法。而在更新配置文件后，管理员还需要验证是否已正确更改应用，任何配置遗漏或将触发服务器在重启时出现语法错误，从而导致连接失败。此外，安全专家还建议 Nexpose 设备的管理员需尽快更新系统应用、删除服务器对于过时加密算法的支持。
链接地址	http://securityaffairs.co/wordpress/59708/hacking/nexpose-appliances-ssh-flaw.html

每周值得关注的恶意代码信息

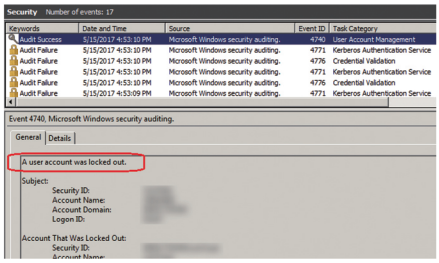
经安天检测分析，本周有 8 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

平台分类	关注方面	名称	相关描述
移动恶意代码	较为活跃的样本	Trojan/Android.emial.el[prv，fra]	该应用伪装成中国建设银行控件，运行后隐藏图标，后台获取手机收件箱短信上传到服务器，拦截用户短信并上传，同时包含风险短信模块，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.Triada.q[exp，rog]	该应用安装无图标，运行后获取 root 权限，私自下载应用并提权安装，后台推送流氓广告，造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.FakeFB.g[prv，fra]	该应用伪装成 Facebook，诱导用户输入账号密码并通过短信转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.emial.dv[prv，exp]	该应用伪装成移动积分应用，运行会监听短信，拦截短信，窃取用户短信信息，造成用户隐私泄露和资费消耗，建议卸载该应用。（威胁等级高）
		Trojan/Android.QQspy.ba[prv，exp]	该应用程序运行诱导用户输入 QQ 账号密码通过短信转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.aixunyun.a[prv，spy]	该应用程序为企业使用的监控类软件，运行后开启设备管理器，隐藏自身图标，获取设备 root 权限，能够删除用户资料、开启或禁用用户摄像头、获取用户地理位置、发送短信、安装未知应用等，如非自主安装建议及时卸载。（威胁等级高）
		Trojan/Android.LockScreen.b[rog，exp]	该应用无实际功能，开机自启动，运行后隐藏图标，上传短信、电话号码和设备信息，私自发送短信，删除短信，造成用户隐私泄露资费消耗，建议立即卸载该应用。（威胁等级高）
		Trojan/Android.FakeApp.bv[exp，prv]	该应用伪装成 YouTube 相关应用，安装后隐藏图标。会拦截用户短信，并无提示发送短信，可能造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 内存破坏漏洞（CVE-2017-2930）	Adobe Flash Player 是美国 Adobe 公司开发的一款广泛使用的、专有的多媒体程序播放器。Adobe Flash Player 中存在内存破坏漏洞，攻击者可利用漏洞控制受影响的系统，导致任意代码执行。（威胁等级高）
	较为活跃的样本	Trojan[Backdoor]/Win32.Zerot	Win32.Zerot 是一木马家族。该家族的样本在执行后会连接远程的服务器，上传所窃取的信息，并从远程服务器接受进一步的控制，例如更新自身程序，接受控制命令并执行等。（威胁等级中）
		RiskWare[Downloader]/Win32.Labuda	Win32.Labuda 是一个具有下载行为的木马家族。该家族的样本在执行后会连接远程服务器，下载其他程序并执行，并接受进一步的控制。（威胁等级中）
		Trojan/Win32.Gozi	Trojan/Win32.Gozi 是一种可以监控用户系统的木马家族。该家族样本运行后监控用户网络流量，窃取浏览器与邮件应用中保存的登录密码，还可以记录击键，修改注册表。（威胁等级中）
		Trojan[Banker]/Win32.IRCbot	Trojan[Banker]/Win32.IRCbot 是一种可以窃取银行密码的木马程序。该家族一般会利用高危漏洞进行传播，已有多个变种。样本运行后会修改多处注册表，以关闭杀毒软件、防火墙，降低系统安全性。该家族的核心行为是接受 IRC 远程控制，同时对文件进行上传下载、参与 DDoS 攻击等。（威胁等级中）

QakBot 又回来了

Chris Brook / 文　安天公益翻译小组 / 译

QakBot 是一种类似蠕虫的信息窃取恶意软件，从 2009 年开始活跃，如今再次浮出水面了。研究人员发现，该恶意软件与最近的大量微软 Active Directory(活动目录) 锁定事件有关。Active Directory 是微软的目录服务器，允许管理员从单个位置控制网络。管理员通常使用数据库来验证和授权用户。



近日，IBM X-Force 研究团队的 6 位研究人员表示，这是 QakBot 第一次执行锁定攻击，会导致用户无法访问受影响的域上的端点、公司服务器和网络资产。QakBot 利用一个投放器通过端点进行传播。该投放器会等待 10 到 15 分钟才执行，以此来规避沙箱或反病毒系统的检测。该投放器打开一个可执行文件，并注入一个 DLL，来覆盖原始文件，然后下载 QakBot 的载荷。

在过去，QakBot 恶意软件表现出类似蠕虫的功能，例如通过共享驱动器和可移动媒体进行自我复制。而此次，它一直通过网络传播，循环访问用户和域凭证来锁定用户的账户。该恶意软件使用不同的密码猜测方案进行登录，包括使用字典中的单词来猜测密码。

研究人员在近期发布的博文中说："QakBot 可能会收集受感染机器的用户名，并使用它来尝试登录域中的其他计算机。如果它无法枚举域控制器和目标计算机的用户名，就会使用硬编码的用户名列表。"

研究人员说："在某些域配置下，QakBot 的字典攻击可能会导致多次失败的身份验证，最终导致账户锁定。"

研究人员指出，QakBot 早就被证明善于规避检测了，而且具有持续性。它利用注册表运行键和计划任务来躲避系统重启和删除。利用注册表运行键，每次系统重启后，它都能够自动启动；而利用在 schtasks.exe 中编写的计划任务，它能够按时间间隔运行。

正是得益于这种持续性机制，QakBot 在 2011 年感染了马萨诸塞州的两个政府机构：失业救助部和职业服务部。这两个机构表示，W32.QAKBOT 有可能窃取了个人姓名、社保号、雇主识别号和电子邮件地址。

这两个机构指出："W32.QAKBOT 可能影响了失业救助部和职业服务部多达 1500 台电脑，包括一站式职业中心的电脑。"

这个恶意软件也与 2011 年投资和保险公司 The Hartford 的攻击有关，该公司员工用来远程访问 IT 系统的几台服务器遭到了攻击。

IBM X-Force IRIS 的全球研究负责人 Mike Oppenheim 在周一表示，虽然研究人员发现的大部分攻击面向医疗和科技行业，但是他们并不认为该恶意软件针对任何特定的行业。"目标组织和大部分目标银行位于美国。"

Active Directory 锁定只是 QakBot 攻击活动的副作用。研究人员说，QakBot 并没有失去窃取银行登录信息的诀窍。

QakBot 能够利用多种机制搭载受害者的银行会话。它利用浏览器中间人 (man-in-the-browser) 功能，从攻击者控制的域向网上银行会话中注入恶意代码。这样一来，攻击者就能够窃取用户击键、缓存凭证、数字证书和会话验证数据了。

Oppenheim 指出，Active Directory 锁定和银行攻击的方式相同。"在这两种情况下，QakBot 都是通过钓鱼邮件中的恶意链接到达目标机器的。" Oppenheim 说。"需要注意的是，这是一个复杂的犯罪组织，我们已经发现数百个受感染的设备与其 C2 中心通信了。该组织试图感染尽可能多的机器。他们感染了大量的基础设施，其 C2 服务器以小时为单位推出新的、稍微调整的 QakBot 版本，以增加他们的经济收益。"

该恶意软件已经运行了将近 8 年，貌似短期内也不会消失。

BAE Systems 的研究人员去年 4 月表示，QakBot(也被称为 Qbot) 应为 5.5 万起感染负责，其中 85% 的感染影响了美国的系统。当时，BAE Systems 网络威胁情报负责人 Adrian Nish 告诉 Threatpost，攻击者不断地重新编译代码并重新打包，以便规避检测。

IBM 的研究人员表示该恶意软件的隐秘性归功于位于东欧的开发人员。这些开发人员不时地将其下线，微调其代码、持续性机制、抗杀毒能力和抗研究能力。

研究人员说，攻击者的沉寂是一种有意识的决定，"可能是为了将攻击限制在最低限度，避免执法机构的调查。"

原文名称	QakBot Returns，Locking Out Active Directory Accounts
作者简介	Chris Brook，Threatpost 副编辑。
原文信息	2017 年 6 月 5 日发布于 Threatpost，原文地址 https://threatpost.com/qakbot-returns-locking-out-active-directory-accounts/126071/
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《IoT 僵尸网络 Dofloo 攻击预警报告》

近日，安天僵尸网络监控小组通过监控互联网地下黑色产业链某个组织使用的 HFS 站点捕获到一批 IoT(Internet of Things) 设备的“肉鸡”IP 数据信息。

目前，该批“肉鸡”数量已超 40 万，形成了一个庞大的 DDoS botnet，预计后期规模会大于攻击 Dyn 的 Mirai DDoS botnet，将严重威胁着互联网的安全，因此安天在此为您鸣起了安全预警警报！

该批数据已经确定是通过相关 IoT 设备厂商的默认密码进行爆破而来，进而植入 IoT 类型的木马，进行 DDoS botnet 的布控。截止目前，被扫描爆破的 IP 已超 40 万（仅花 2 天时间），而且这个数据还在持续增长，也就意味着要形成的 DDoS botnet 还在肆意增长，将对互联网安全埋下巨大安全隐患。

根据捕获的样本分析鉴定确定，被植入的木马为 Dofloo 家族木马。此前，在第 72 期《安天周观察》已经分析介绍过 Dofloo 的家族史，这是一个兼容 Windows、Linux、IoT 三大环境的 DDoS botnet，因此每个 C2 通常拥有非常庞大的“肉鸡”群，而且可实现反射、放大等多样 DDoS 攻击手法，因此其 DDoS 攻击破坏能力可见一斑，此次的大批量 IoT 设备沦为 Dofloo 家族的“肉鸡”更是“如虎添翼”。

将捕获到的“肉鸡”IP 进行 shodan 查询得知，涉及到的 IoT 厂商主要是以视频监控系统、路由器为主，且该批“肉鸡”分布十分广泛，主要集中在欧洲、印度、美国、越南、马来西亚、印度尼西亚、阿根廷、巴西、日本、中国等国家。如此规模的 Dofloo DDoS botnet 不敢想象后期爆发的 DDoS 攻击流量会有多大，但据统计拥有 10 万“肉鸡”的 Dofloo DDoS botnet 可实现超 600Gbps 的放大攻击。根据目前“肉鸡”集中分布于欧美及印度的情况，预测该 Dofloo DDoS botnet 后期爆发攻击的目标很可能就是欧美或者印度，所以在此为欧美印各安全同行们拉起安全警报。

这几年 IoT 得到了很大发展，但是 IoT 安全并没有跟上发展的步伐，各种高危漏洞层出不穷，加上漏洞难以修复，已经成为黑客的“盘中珍馐”。

安天提醒广大 IoT 设备厂商，要提高产品的安全防护意识，提醒产品用户及时修改默认登陆密码。

木马程序

安天【追影高级持续威胁分析系统】无需更新病毒库，依据行为即可实现对上述木马程序进行有效检测，以下为其自动形成的分析报告：

文件被内部组件发现，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、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、智能学习鉴定器将文件判定为木马程序。

文件名	def5b6170207bfdeef5ba453db3224b4
文件类型	BinExecute/Linux.ELF
大小	978 KB
MD5	DEF5B6170207BFDEEF5BA453DB3224B4
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Dofloo.c
判定依据	静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=DEF5B6170207BFDEEF5BA453DB3224B4

◆ EXIF 信息

描述	值
File Size	978 kB
File Type	ELF executable
MIME Type	application/octet-stream
CPU Architecture	32 bit
CPU Byte Order	Little endian
Object File Type	Executable file
CPU Type	Unknown (40)