安天周观察

主办：安天　2017 年 2 月 27 日（总第 77 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

2016 中国网络安全大事件发布会召开 安天代表作会议发言

2 月 21 日，由中国计算机学会计算机安全专业委员会和新华社《经济参考报》互联网 + 周刊联合主办的 2016 中国网络安全大事发布会在公安部一所圆满召开。此次活动采用专家组评选和网络投票的方式，评选出 12 件 2016 年中国网络安全大事件。2016 年 5 月 25 日，习近平总书记视察了安天，在本次评选中，“习近平考察民营网络安全企业”入选了 2016 中国网络安全大事。

发布会上，安天安全服务负责人李波参加了本次发布会，在会上分享了安天人向总书记汇报的难忘记忆，表达了安天努力成长为网络安全国家企业坚定使命愿景。总书记视察期间，安天负责人汇报了安天的威胁检测引擎等核心技术的突破决心和研发历程；介绍了威胁检测引擎核心技术研发的端点防护、流量监测、深度分析产品和解决方案，以及其在相关部委与关键基础设施中的应用情况；演示了安全威胁捕获、分析、溯源和态势感知，以及利用超算资源，实现对关键信息基础设施的仿真模拟和防护演练工作。在听取了汇报之后，总书记对安天负责人说，“你们也是国家队，虽然你们是民营企业。”安天会按照总书记“网络安全要整体设计、加强合作，在相互学习，相互切磋，联合攻关，互利共赢中走出一条好的路子来。” 的指示，在国家信息安全主管和职能部门的指导协调下，与国内能力型安全友商加强合作协同，共筑我国网络安全的防御能力和体系。

由安天建设的黑龙江省网络安全检测与分析技术重点实验室通过备案

近日，黑龙江省科技厅公布第一批 52 家黑龙江重点实验室名单，依托安天建设的黑龙江省网络安全检测与分析技术重点实验室通过备案。

安天是专注于威胁检测防御技术和先进解决方案的网络安全厂商，依托在下一代威胁检测引擎、网络威胁检测、威胁分析与鉴定、终端威胁检测与防御、网络威胁阻断、威胁取证、APT 纵深防御解决方案、网络安全态势感知等方面积累的技术和能力，安天建设了黑龙江省网络安全检测与分析技术重点实验室，并已运行和对外开放 2 年以上。

近年来，实验室共承担 8 项科研项目，其中 1 项 863 计划，1 项国家重点研发计划，3 项 242 计划，1 项发改委信息安全专项，1 项省科学基金项目；荣获 19 项国家级、省级及市级等奖励。

安天入选 2016 年度国家知识产权优势企业

近日，安天入选国家知识产权局认定的“2016 年度国家级知识产权优势企业”。

自安天创建之初，就非常重视知识产权工作，建立起比较完备的知识产权体系。安天专注威胁检测防御领域的核心技术研发和积累，围绕终端和网络场景下的威胁检测、APT 的检测分析、安全分析能力与支撑体系、工控和其他新场景的安全等形成了自己的核心技术布局，并进行了大量专利申请。截至 2017 年 2 月，安天已向国家知识产权局提交专利申请 525 项，已获得授权专利 158 项，并有一项关键专利获得了中国第十七届中国专利优秀奖。

一周简讯

- 安全厂商发布勒索软件 CryptoMix 免费解密工具
- 微软发布安全更新解决 Adobe 任意代码执行漏洞
- 新型安卓勒索软件要求受害者口述解锁代码
- 韩亚航空遭到黑客攻击导致网站暂停服务
- Swift 编写的 MacOS 勒索软件 Patchers 被发现
- 研究人员发现 Siklu 无线设备远程代码执行漏洞
- 研究人员发现硬盘 LED 可泄露物理隔离网络数据
- Chrom 警告：部分网站提示下载字体实为恶意攻击

安天 CERT 整理，详情请见 http://bbs.antiy.cn

黑客通过控制麦克风窃取超过 600GB 的数据

近日，研究人员曝光了利用麦克风窃取情报的网络间谍行动。攻击者从大约 70 个目标窃取了超过 600GB 的数据，这些目标包括了关键基础设施、新闻媒体和科研机构。攻击者首先向目标发送钓鱼邮件，恶意程序隐藏 Microsoft Word 文档中，一旦感染目标之后利用恶意程序控制设备的麦克风去记录对话、屏幕截图、文档和密码。

收集的情报上传到 Dropbox 账号。研究人员根据其使用麦克风和 Dropbox 而将这一行动称为 Operation BugDrop。大多数被感染的目标位于乌克兰，其余目标位于沙特和澳大利亚。（原文：http://www.cnnvd.org.cn/news/show/id/8192）

每周安全事件

类 型	内 容
中文标题	潜伏 11 年的 Linux 内核提权漏洞曝光
英文标题	CVE-2017-6074-a new 11-year old Linux Kernel flaw discovered
作者及单位	Pierluigi Paganini；SecurityAffairs
内容概述	近日，研究人员已经发现并确定了用来散播 Shamoon 的服务器。 Shamoon 恶意软件于 2012 年浮出水面，当时感染了全球最大石油生产公司沙特阿美 (Saudi Aramco)3 万个工作站，擦除了硬盘数据，使沙特阿美陷入恐慌。自那之后，攻击者不断完善该恶意软件，持续攻击沙特政府和行业的高价值目标，最近一次攻击发生在不久前。 目前，有关研究人员认为，他们已经破解了 Shamoon 操作人员使用的传播技术。研究人员可能知道攻击者如何让恶意软件进入系统，这为 IT 经理提供绝佳机会，以便 IT 经理在 Shamoon 破坏数据之前发现是否存在感染问题。
链接地址	http://securityaffairs.co/wordpress/56566/hacking/cve-2017-6074-linux-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 9 个移动平台恶意代码和 4 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.loader.a[exp，rog] 2017-02-20	该应用伪装成 Flash-Player，程序运行会隐藏图标，请求激活设备管理器，频繁弹出虚假界面诱骗用户开启辅助功能，后台连网私自下载安装指定的恶意应用，造成用户资费消耗。（威胁等级高）
		Trojan/Android.Femas.a[prv，exp，rmt] 2017-02-21	该应用程序伪装成其他应用，运行后隐藏图标，定期收取用户数据，上传设备信息、AppLists 等信息至服务器，同时执行远程命令进行下载伪装更新，造成用户隐私泄漏和资费消耗，建议及时卸载该应用。（威胁等级高）
	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，会造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.SmsThief.bf[prv，fra]	该应用伪装成中国邮政银行安全控件，运行后后台会获取用户收件箱的中国邮政银行相关短信并上传到指定服务器，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		G-Ware/Android.HiddenApp.x[rog]	该应用启动后会隐藏图标，开机启动，请求 root 权限，卸载指定应用，建议卸载。（威胁等级低）
		Trojan/Android.FakeSystem.h[exp，rog]	该程序伪装系统应用，运行后会隐藏图标，连网获取 URL 相关信息频繁访问，造成资费损耗，建议立即卸载。（威胁等级中）
		G-Ware/Android.Fakegupdt.cq[exp，rog]	该程序安装后无图标显示，连网下载恶意应用反射调用，后台推送广告，下载安装推广应用，造成资费损耗，建议立即卸载。（威胁等级低）
		Trojan/Android.emial.ep[prv，exp]	该程序伪装正常程序，运行诱导激活设备管理器，后台监听用户收件箱窃取用户短信，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Triada.ab[exp]	该程序伪装系统程序，安装后无图标显示，会私自下载安装应用，建议卸载避免造成资费损耗。（威胁等级中）
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 公司开发的一款是一种广泛使用的、专有的多媒体程序播放器。 Adobe Flash Player 中存在内存破坏漏洞，攻击者可利用漏洞来控制受影响的系统，导致任意代码执行。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Shell.Gafgyt	此威胁是一类使用 Shell 脚本编写的木马家族。该家族样本运行后关闭 iptables 防火墙，使用 Kill-9 及 Killall 命令结束多个进程，并使用 Busybox 下载恶意代码替换正常文件。（威胁等级高）
		Trojan[Backdoor]/Win32.Qakbot	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后连接远程服务器接受攻击者恶意操作，包括文件管理，进程查看等。（威胁等级高）
		Trojan[Downloader]/HTA.Locky	此威胁是一类可以下载勒索软件的木马家族。该家族样本是 Html Application 应用程序，运行后连接远程服务器下载 Locky 勒索软件并执行，加密用户重要数据。（威胁等级中）

如何保护家庭摄像头

Matthew Rosenquist / 文　安天公益翻译小组 / 译

安装家庭监控摄像头有很大的好处，但也会导致隐私泄露和网络安全风险。用户希望在提高安全性的同时避免网络安全威胁。提供下面的三个建议，在用户购买、安装和配置家庭摄像头时予以参考。

风 险

家庭连网摄像头是网络犯罪分子的重要目标。最近发生了很多大型的物联网 (IoT) 攻击事件，黑客感染了数十万的物联网设备，并将它们纳入大规模僵尸网络。这些僵尸机器 (包括 IP 摄像头，数字录像机和家庭路由器等) 根据控制者的指令，将网络流量发送到指定的站点。大量的数据流导致目标站点崩溃，使其无法提供正常的服务。前不久针对 DNS 服务提供商 Dyn 的攻击使得美国东海岸大部分网站下线。攻击家庭设备已经成为网络犯罪分子的一个有效手段，家庭摄像头可能会成为黑客进行窥探的工具。

保护家庭摄像头的三大建议

1) 选择可靠的厂商

在购买摄像头时应充分的考虑，选择那些注重保护用户隐私和安全的厂商。在购买产品时不要被营销广告所吸引，而是去他们的产品网站看看。查看他们是否发布了安全更新，是否设立了安全小组，是否详细地说明了他们如何保护产品和服务。

没有什么产品能够永远安全，特别是物联网设备。重要的是厂商为保持客户的产品安全做出不断更新的维护。如果厂商开发安全补丁并向客户解释发现了什么漏洞，那么他们就是负责任的厂商。而用户要做的，就是及时为产品打补丁。

许多厂商不愿花精力去成立一个安全团队。如果厂商没有专业的安全团队，这意味着他们不太可能设计出强健的安全功能，意味着他们没有漏洞查找人员，没有补丁开发人员，没有验证补丁安全性的人员。

拥有安全团队的厂商应该公开讨论产品设计中的控制措施、测试标准、认证以及发现的漏洞。甚至有些公司设立了漏洞赏金计划，他们会奖励并关注那些发现漏洞的白帽黑客。

2) 设置在非敏感区域

监控摄像头是了解家庭情况的好工具。但是在某些时候，即使最好的产品也会有弊端和缺点。例如，摄像头放置在较私密的地方，可能会导致私人视频流出。所以，放置摄像头的位置至关重要。家门口、公共区域和婴儿房就是比较合适的地方。尽量不要放置在卧室、更衣室、浴室和其他私人区域。许多现代摄像头配备了麦克风和其他传感器。所以即使在公共区域，也要注意自己的言论。家庭摄像头便于设置，处理数据时也不麻烦。大多数家庭摄像头利用云服务存储数据，使用者可以随时随地查看。

但这也是致一个攻击点，所以要慎重考虑在云中存储哪些数据，避免让尴尬或私人视频出现在网上。

3) 更改默认密码

家庭摄像头有很多默认设置，便于用户轻松设置。大多数设置不需要修改，但更改默认密码至关重要！创建唯一的强效密码，将其备份在安全的地方。最危险的设置是，如果用户忘记了密码，会允许在摄像头上进行重置。很多物联网僵尸网络变种正是以大量采用默认密码的设备为目标，攻击者可以从网上找到这些密码，进而访问这些摄像头。一些厂商强制要求用户在安装时更改默认密码，其他厂商则不会这样要求。用户务必要更改默认密码，这会带来很大的不同。

家庭摄像头的为我们的现代生活提供了新的安全感和灵活性。但必须在这些好处和伴随的风险之间取得平衡。遵循这三个建议，可以更好地控制摄像头，使自己更加安全。

原文名称	Lovely. Now someone's ported IoT-menacing Mirai to Windows boxes
作者简介	Matthew Rosenquist，1996 年加入英特尔公司，在安全领域工作了 20 多年，专注于安全战略，衡量价值，开发具有成本效益的能力和组织。
原文信息	2017 年 1 月 4 日发布于迈克菲实验室 原文地址 https://securingtomorrow.mcafee.com/mcafee-labs/top-tips-for-securing-home-cameras/
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《僵尸网络 Gafgyt 家族分析》

近日，安天追影小组通过对 Gafgyt 家族涉及 IoT 领域进行深入分析及自动化监控发现该家族与 Mirai 家族一样在 IoT 领域属于相对活跃的僵尸网络恶意程序，其特性存在较多相似之处，Gafgyt 家族出现时间相比 Mirai 家族要早很多，不排除 Mirai 家族是在 Gafgyt 家族的基础上建立的可能性。Gafgyt 家族是在 2014 年 10 月开始被发现，一直以来，Gafgyt 家族保持着相对活跃的状态，从目前监控到的数据来看，其 DDoS 攻击目标基本针对于欧美国家。

Gafgyt 家族 Bot 程序主要功能分为 3 个模块：

1) Downloader 模块。通过样本硬编码的 URL 下载 Shell 脚本和其他附属样本，随后执行下载的脚本及样本，实现 Bot 程序传播；

2) Scanner 模块。Bot 程序在运行后，首先会向控制端发送首包，而这个首包和通常的 Botnet 病毒家族的首包存在比较大的区别。常见的 Botnet 病毒家族首包是包含系统配置等信息，而 Gafgyt 首包数据是“BUILD RAZER.”，控制端则通常回复“!* SCANNER ON”，命令被控端对随机网段进行 Telnet 弱口令扫描爆破，如果被控端发现有爆破成功，就会把 IP 及 Telnet 用户、密码数据向控制端发送，这也预示将增加一个潜在的僵尸网络被控端；

3) DDoS 攻击模块。Bot 程序在执行 Telnet 扫描爆破的同时，也在和控制端保持正常通讯，等待控制端的相关指令，例如 DDoS 攻击指令，Gafgyt 主要实现包括：SYN Flood、UDP Flood、UDP amplification、TCP Flood、RST Flood、Http Flood 这几种方式的 DDoS 攻击。

Gafgyt 家族的样本没有实现备份自身及自启动功能，通过 Scanner 模块与 Downloader 模块，即使受害者系统重启清除 Bot 程序，其它的僵尸网路节点同样可以通过 Telnet 重新登陆进而传播感染，使 Botnet 迅速拓展势力范围进而增加 DDOS 攻击威力，这一点 Mirai 家族与之非常相似。

安天追影小组对 Gafgyt 家族的监控仍在持续进行，每天都会发现新增的 C&C 且其大部分对欧美多个国家不同 IP 进行 DDoS 攻击，严重威胁互联网安全。安天提醒物联网设备管理者，若发现物联网设备被植入 Gafgyt 家族的恶意程序，只需要将设备重启，并将 Telnet 的用户密码更换即可。同时，也要避免使用弱密码，以免被黑客攻击利用。

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：

文件被网络威胁感知类设备发现，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、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。最终依据智能学习鉴定器将文件判定为木马程序。

根据动态行为（默认环境）得出该文件具有以下行为：执行 IP 网段 Telnet 扫描、疑似 DDoS Flood 流量攻击。

文件名	60B193AC62F64C78C517EF4228FD0038
文件类型	BinExecute/Linux.ELF
大小	139 KB
MD5	60B193AC62F64C78C517EF4228FD0038
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[DDoS]/Linux.Gafgyt
判定依据	智能学习

◆ 运行环境

操作系统	中标麒麟
内置软件	默认

报告地址：https://antiy.pta.center/_lk/details.html?hash=60B193AC62F64C78C517EF4228FD0038

◆ 危险行为

行为描述	危险等级
执行 IP 网段 Telnet 扫描	★★★★
疑似 DDoS Flood 流量攻击	★★★★

◆ EXIF 信息

描述	值
File Size	139 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)