安天周观察

主办：安天　2016 年 10 月 31 日（总第 62 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天透过北美 DDoS 事件解读 IoT 设备安全

安天安全研究与应急处理中心（安天 CERT）在北京时间 10 月 22 日下午启动高等级分析流程，针对美国东海岸 DNS 服务商 Dyn 遭遇 DDoS 攻击事件进行了跟进分析。安天团队分析认为，此事件有一定的政治因素背景，涉及到 IoT(Internet of Things，物联网）设备安全等多种因素，在表象的 DDoS 攻击和 DNS 安全之外，依然有很多值得关注和研究的问题。

在本次事件中被广泛关注的 Mirai 的主要感染对象是物联网设备，包括：路由器、网络摄像头、DVR 设备。安天在此前跟进 IoT 僵尸网络跟踪分析过程中，发现如下包括 DVR、网络摄像头、智能路由器的品牌中有部分型号存在单一默认密码问题。

部分型号存在默认密码的设备品牌

安天 CERT 对 Mirai 源码进行了相应分析，得出 Mirai 事件相关源码主要包括两部分：

(1) loader：加载器，其中存放了针对各个平台编译后的可执行文件，用于加载 Mirai 的实际攻击程序。

(2) Mirai：用于实施攻击的程序，分为 bot（被控制端，使用 C 语言编写）和 cnc（控制端，使用 Go 语言编写）两部分。

安天的态势感知与监控预警系统可以对僵尸网络的样本传输、上线控制、攻击指令进行持续监控。除了 Mirai 相关事件外，我们也可以看到 IoT 僵尸网络对其他目标的攻击事件。

2014 年之前使用 Linux 系统的 IoT 设备被植入恶意代码主要通过扫描弱密码。但在破壳漏洞 (CVE-2014-6271) 出现后，互联网上也出现了大量利用该漏洞进行扫描植入恶意代码事件。根据当时安天蜜罐系统捕获的情况来看，破壳漏洞出现后，针对 Linux 主机入侵的事件呈现全面上升趋势。安天发现的首例通过破壳漏洞实际感染的事件是在 2014 年 9 月份。而后安天 CERT 陆续发了多篇 IoT 设备上的恶意代码分析报告如表 2 所列。

两年前，安天论述了“威胁将随‘互联网 +’向纵深领域扩散与泛化”的观点，并使用泛化 (Malware/Other) 一词来说明安全威胁向智能设备等新领域的演进，而正如我们所担心的那样，安全威胁在智能汽车、智能家居、智能穿戴，大到智慧城市中已经无所不在。

正因为此，这次针对 DynDNS 服务的大规模 DDoS 事件中，安天更重视其中暴露的 IoT 安全问题。尽管 DNS 的确被很多人认为是互联网的阿喀琉斯之踵。但我们同样不要忘记，互联网是依托 IP 地址联通的，而域名是为便于人记忆的原因而产生的。对于北美大型行业用户来说，其更多广泛采用 VPN 和 IP 地址链接，其基本系统运转并不依赖 DNS 的解析。也正因为此，如此大流量的 DDoS，尽管给网民访问网站带来一段阶段的不便，但其并不足以冲击北美社会运行和互联网的根基。从这个意义上看，这个事件的热度，更多来自媒体对公众感觉的放大，而其实际影响则相对有限。而更危险的行为是有针对性的、有放大效应的针对重要节点的威胁行动，特别是能够产生实体空间后果的威胁。

表 1　典型的 IoT 僵尸网络攻击事件

攻击起开始时间	样本家族（原厂命名）	攻击目标	攻击类型
20161022 9:36:48	Mayday 家族	203.195.*.*:15000 广州 X 讯	tcp flood
20161020 8:12:57	DDoS 家族	www.52***.com　X X阁	
20161020 1:36:20	DDoS 家族	www.ssh***.com/user.php 深圳X X X X X X公司	
20160109 18:52:35	Billgates 家族	121.199.*.*　杭州X X云	
20160905 10:57:00	Billgates 家族	59.151.*.*　北京X X通	

表 2　安天部分与 IoT 安全有关的事件分析报告

发布时间	报告
20140926	Bash 远程代码执行漏洞“破壳”(CVE-2014-6271) 分析
20140929	“破壳”漏洞相关恶意代码样本分析报告
20150113	DDoS 攻击组织肉鸡美眉分析
20150901	利用路由器传播的 DYREZA 家族变种分析
20150915	黑客用 HFS 搭建服务器来传播恶意代码
20161024	Trojan[DDOS]/Linux. Znaich 分析笔记

网络安全威胁泛化与分布图（引自安天 2015 年网络威胁年报）

每周安全事件

类 型	内 容
中文标题	新加坡继美欧后遭受 IoT 设备僵尸网络 DDoS 攻击
英文标题	Singapore Telco Blames Recent DDoS Attacks on Compromised IoT Devices
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，新加坡三大电信公司之一星和 (StarHub) 表示，近期连续两次遭受到网络攻击，造成其部分宽带用户的网络中断，攻击者所用手段与近期造成美国东海岸和欧洲部分地区大面积网络瘫痪的攻击方式极为相似。该公司表示，已分析了中断的网络日志，发现其域名服务器 (DNS) 遭受了“故意并且可能是恶意的”分布式拒绝服务 (DDoS) 攻击。 星和在新闻发布会上表示，两波攻击均来自公司自己用户的机器，“用户被感染的机器变成了‘僵尸’机器，反复向星和的 DNS 发送请求。”星和首席技术官 Mock Pak Lum 称，宽带路由器和网络摄像头等设备被攻击者利用来发动攻击。
链接地址	http://news.softpedia.com/news/singapore-telco-blames-recent-ddos-attacks-on-compromised-iot-devices-509673.shtml

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	名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.sdali.a[rmt, prv] 2016-10-24	该应用程序伪装 Flash Player，运行后强制用户给予设备管理器权限，并隐藏图标，窃取用户 IMEI 号，手机号，固件信息等隐私信息并上传至相关网络服务器。从该网络服务器接收远程控制命令进行获取用户短信，开启 USSD 服务等行为。造成用户隐私泄露和资费消耗，建议卸载。(威胁等级高)
		Trojan/Android.PornAd.a[rog, exp]2016-10-25	该应用会伪装成系统应用，安装后无图标，运行后会加载显示色情广告，私自下载色情应用，频繁弹窗诱导用户安装，造成用户资费损耗，建议不要安装。(威胁等级中)
		G-Ware/Android.Dowgin.a[exp, rog]2016-10-27	该程序为资讯类应用，运行后会私自下载恶意 apk，伪装成系统升级诱导用户点击安装。该 apk 会私自下载推广应用，造成用户流量资费损耗，建议立即卸载。(威胁等级低)
		Trojan/Android.KksSpy.a[prv, spy] 2016-10-27	该程序是一款间谍程序，会收集用户收件箱及通讯录隐私信息上传，同时包含发送短信、删除短信、删除联系人等风险代码，避免造成隐私泄露和资费损耗，建议立即卸载。(威胁等级高)
	较为活跃的样本	Trojan/Android.FakeFlashPlayer.r[rmt, exp, rog]	该应用会伪装成 Flash Player，程序运行后会请求激活设备管理器，隐藏图标，私自联网获取数据指令，并执行解析指令发送指定短信、访问指定网址、推送应用、设置拦截短信等行为，造成用户资费消耗，建议卸载。(威胁等级中)
		Trojan/Android.Slocker.c[rmt, prv, exp]	该应用运行后会激活设备管理器，隐藏图标，私自发送短信，接收远程指令，窃取用户手机固件信息、短信和联系人信息，同时劫持用户界面，弹出虚假银行支付界面诱导用户输入银行卡信息，并将信息上传，造成用户隐私泄露和资费损耗，建议不要安装。(威胁等级高)
		Trojan/Android.Rootnik.h[rog, sys]	该应用会伪装成正常应用，运行后会隐藏图标，后台会私自下载恶意应用和提权工具，并静默安装。会造成用户资费损耗，建议不要安装。(威胁等级高)
		Trojan/Android.Mobilespy.v[prv, spy]	该应用是一款间谍、监控类应用软件，会通过联网获取关键代码。并会伪装成 Googleplay 商店，运行后隐藏自身图标。监听用户手机短信、电话、联系人等各种隐私信息、并静默安装未知应用。建议立即卸载。(威胁等级高)
		G-Ware/Android.Triada.n[exp, prv, rog]	该程序会伪装系统应用，收集设备位置、安装列表、通话时长等隐私信息联网上传，获取反馈数据后会加载子包推送广告。避免造成资费损耗和隐私泄露，建议卸载。(威胁等级低)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Linux 内核出现本地提权漏洞 CVE-2016-5195	Linux 内核的内存子系统在处理写时拷贝 (Copy-on-Write) 时存在条件竞争漏洞，会导致破坏私有只读内存映射。如一个低权限的本地用户能够利用此漏洞，获取其他只读内存映射的写权限，会进一步导致提权漏洞。(威胁等级高)
	较为活跃的样本	Trojan[Downloader]/Win32.CWS	此威胁是一种具有下载行为的木马类程序。这种木马可以很容易的 被保存在网页的服务器，感染那些访问网站的计算机，并嵌入到其它免费软件中。该家族会通过互联网潜入用户电脑，或以电子邮件的附件的形式进行传播。(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，同时把它发送给攻击者。该家族将恶意代码注入到被感染的系统中，并会防止用户访问 Windows 的注册表文件。(威胁等级中)
		Trojan/Win32.Comeli	此威胁是一种木马类程序。它会获取用户系统信息，存取用户数据，执行恶意操作。部分变种可以下载间谍软件在系统中运行。当执行完这些恶意操作后，木马会删除自身。(威胁等级中)

施耐德电气开发软件 Unity Pro 发现重大漏洞

Tom Spring / 文　安天公益翻译小组 / 译

近日，施耐德电气正在处理，其旗舰工业控制管理软件 Unity Pro 上发现的重大漏洞，这一漏洞允许黑客在其工业网络上远程执行代码。

这一警报是由一家行业网络安全公司 Indegy 发出的，安全公司发现了该漏洞并于近期发布了关于漏洞的报告。Indegy 的首席技术官米勒·甘德斯曼称该漏洞存在重大隐患，敦促所有使用 Unity Pro 软件的用户更新到最新版本。Unity Pro 运行基于 Window 系统的计算机上，用于管理和编程全世界数百万个工业控制器。

甘德斯曼告诉 Threatpost 记者：“如果运行 Unity Pro 软件的 Windows 个人计算机 IP 地址可以访问网络，那么任何人都可以利用该软件在硬件上运行代码”。这是打开了访问的潘多拉魔盒，所以，黑客可以利用已有的控制器为所欲为。

Indegy 表示该漏洞存在于 Unity Pro 上名为 PLC 模拟器的组件中，用于测试工业控制器。

甘德斯曼说：“黑客想要在 ICS 物理环境中访问是为了影响实际的生产进

程。包括阀门，涡轮、离心机以及智能仪表”。利用这种访问权限，黑客可以用它改变工业控制系统的制药配方或者关闭城市电网。

甘德斯曼近期在亚特兰大举行的 2016 工业控制系统安全大会上展示了他的研究，他说发现该漏洞大约是 6 个月前，并私底下告诉了施耐德电气公司，随后施耐德电气给该漏洞打了补丁。根据 Indegy 的说法，该漏洞存在于所有使用施耐德电气控制器的控制网络。

根据施耐德电气表示：“他们在 9 月 14 号承认存在漏洞，并给用户发送通知。该漏洞可能会执行任意代码远程下载补丁项目文件到 Unity 模拟器上”。

根据由 Indegy 发布的关于该漏洞的简报表明，Indegy 对该漏洞的研究与 Unity Pro 允许所有用户直接在任意安装了该软件的电脑上远程执行代码实情相符，拥有调试特权。

Indegy 指出该漏洞不会要求在 ICS 网络下入侵控制器，因为工业控制器没有认证且工业通讯协议没有加密。Indegy 说且不论在使用的 SCADA/DCS 应用，如果施耐德电气控制器被部署，将用于工程工作站。所有与该攻击相关的虚拟进程都会被 PLCs 控制。

根据施耐德电气对该漏洞的描述，当 Unity 项目被编译为 x86 指令并加载到 PLC 模拟器上，该漏洞与其紧密关联。“它有可能通过重定向指令控制流使得模拟器执行恶意代码：通过在 Unity Pro project 可用空间植入任意 Shell 代码，然后下载执行模拟器的补丁项目”。

在美国工业控制系统网络紧急响应小组 9 月发布的一份报告中，官方断定上述问题一直困扰着工业控制系统和 SCADA 系统。

原文名称	Major Vulnerability Found In Schneider Electric Unity Pro
作者简介	Tom Spring，卡巴斯基《安全周报》的的副主编，报道科技新闻长达 15 年。
原文信息	2016 年 10 月 26 日发布于《安全周报》(Threatpost) 原文地址 https://threatpost.com/major-vulnerability-found-in-schneider-electric-unity-pro/121550/
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《Mirai 样本分析报告》

近日，安天追影小组通过整理安全事件发现了，一款以物联网设备为主要感染对象的命名为“Mirai”样本。在分析小组进行分析的过程中，发生了一起利用“Mirai”恶意代码进行攻击的 DDOS 攻击事件，受害方是为美国众多公司提供域名解析网络服务的 Dyn 公司。同时，受到影响的厂商服务包括：Twiter、Github、CNN、星巴客、纽约时报等知名网站。Dyn 公司称此次 DDoS 攻击事件涉及 IP 数量达到千万量级，其中很大部分来自物联网和智能设备，并认为攻击来自名为“Mirai”的恶意代码。

安天追影小组对 Mirai 的样本进行分析说明，经分析该样本为 ELF 格式，是运行在 Linux 操作系统上的恶意代码。该样本主要分为四个模块，分别为 Attack 模块、Kill 模块、Scanner 模块和 CNC 模块。

Attack 模块，会对某一批特定目标 IP（靶机）做永真循环的数据包发送，位于僵尸网络中的大量 Mirai 样本受控结点通力合作，具备对目标主机进行 DDoS 攻击的能力。Killer 模块，会禁止多个知名端口的服务，即关闭该进程并建立一个套接字绑定到该端口将其占用。Scanner 模块会针对 Telnet 登录口令进行猜解，尝试登录到某一其他设备上并控制该设备。CNC 模块的主要功能是远程命令和控制服务，是木马中常见的控制端服务程序，在 Maria 中的功能主要用于获取控制端的相关命令。

Maria 样本使用了很多隐藏自身的方法，以此保证自身不被轻易发现。对于大量重要的关键字符串，Maria 进行了加密，因为在文件中直接搜索加密前的明文字符串是不可见的，只有加载到内存后，需要使用时，才会调用解密函数将进行解密。

随着小到智能家居、大到智慧城市的物联网蓬勃发展，在线物联网设备数量大幅增加，该类设备一般没有经过严格的安全设计，恶意代码对其注入、进而利用其进行攻击的难度低于攻击桌面操作系。这起攻击事件也敲响了加强物联网设备安全防护的警钟。提高攻击入侵物联网设备的成本，以及加强物联网设备的安全威胁监测预警，是安天已经在进行的工作。

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，即可实现对上述木马程序进行有效检测，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、YARA 自定义规则鉴定器、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。

该文件具有以下行为：创建服务并绑定端口、禁止端口、远程下载、装载程序、创建套接字。

文件名	6B7B6EE71C8338C030997D902A2FA593
文件类型	BinExecute/Linux.ELF
大小	41 KB
MD5	6B7B6EE71C8338C030997D902A2FA593
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[DDOS]/Linux.Mirai
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

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=6B7B6EE71C8338C030997D902A2FA593

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
创建服务并绑定端口	★★★★★	禁止端口	★★★★★
远程下载	★★★★★	装载程序	★★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
创建套接字	★★		

◆ EXIF 信息

描述	值	描述	值
File Size	41 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	i386		