安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 01 月 29 日 (总第 122 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天、电信云堤联合发布《2017 全球僵尸网络 DDoS 攻击威胁态势报告》

近日，安天捕风小组与电信云堤联合发布了《2017 全球僵尸网络 DDoS 攻击威胁态势报告》。该年度报告主要以安天捕风蜜网和电信云堤流量监测数据为基础，针对 2017 年发生的僵尸网络 DDoS（分布式拒绝服务）攻击事件进行汇总分析。报告给出了 2017 年全球范围内僵尸网络发起 DDoS 攻击的事件分布、地区分布情况以及攻击情报数据，并对黑客的攻击方法、攻击资源、僵尸网络家族进行了详细分析。

从整体的攻击情报数据来看，全球 DDoS 僵尸网络全年攻击态势呈“山”形，其主要爆发在第二季度的 4、5、6 三个月；在比特币交易价格暴涨期间，大部分 DDoS 僵尸网络被更换为挖矿僵尸网络，所以第四季度处于相对低迷的阶段。

根据全球数据统计，2017 年，美国境内发起的 DDoS 攻击数量是最多的，占全球 DDoS 攻击总事件数量的 37.06%；而中国则成为了遭受 DDoS 攻击的重灾区，承受了全球 DDoS 攻击数量的 84.79%（占整个亚洲 DDoS 攻击量的 98.63%）。DDoS 攻击我国的事件，37.47% 来源于美国，27.77% 来源于我国国内，23.28% 来源于法国，10.17% 来源于韩国。

攻击者发起 DDoS 攻击事件采用的主流僵尸网络家族为 Xor（Xor_Ex 和 Xor_D）家族，其通过控制 Xor 家族僵尸网络发起的 DDoS 攻击占全球 DDoS 攻击的 51.04%。SYN flood 为目前攻击者使用的主流 DDoS 攻击方式，Xor、BillGates、Mayday 等大型的僵尸网络家族的攻击方式均以 SYN flood 为主。物联网（IoT）僵尸网络爆发式增长是 2017 年的趋势之一，由于 Mirai 开源导致众多 IoT 变种出现，同时传统的 Windows、Linux 僵尸网络家族也向 IoT 平台进行拓展。

2017 年僵尸网络活动的主要表现为：

· 以 Linux 僵尸网络为主流

由于 Linux 服务器所在环境带宽大、长时间在线、安全措施落后，该类僵尸网络具有稳定性且易形成规模化。

· IoT 僵尸网络大发展

开源 Mirai 导致物联网僵尸网络变种快速增加，同时传统的 Windows 平台家族僵尸网络发觉 IoT 的规模和攻击威力后，也快速向 IoT 平台演进。Jenki、台风等僵尸家族就是典型代表。

· 具有明显的趋利性

2017 年以来比特币等电子加密货币快速发展，僵尸网络作为网络犯罪组织的重要工具从 DDoS 攻击转到挖矿，Linux、IoT 僵尸网络成为 DDoS 攻击、挖矿的主流。

自 1998 年第一次真正意义上的 DDoS 攻击开始，其攻击带宽流量从 10GB、90GB，逐渐扩大至 300GB、400GB、800GB，如今已经以“T”级别来计算，DDoS 攻击几乎在以飞跃式的速度增长着。受到影响的设备，从一开始的单个服务器、区域性的多个服务器，扩大到针对某行业的整个服务、甚至差点瘫痪欧洲的网络；受到影响的范围从个人、小范围网络，发展到商业之间的竞争、国家金融服务，甚至国家之间的政治、军事行动等等。

从 DDoS 攻击的发展历程，我们不难看出，在如今这个虚拟网络已经嵌入我们现实生活的社会里，DDoS 攻击无疑是一个巨大的安全隐患。伴随着 DDoS 工具的廉价性、易获取性，以及各僵尸网络家族的快速增长，利用物联网设备组建僵尸网络发起攻击的现象日益严峻，与此同时，移动端的僵尸网络亦处于萌芽阶段，网络安全之路可谓任重道远。

完整报告详见

开源框架 Electron 爆严重安全漏洞，影响大量 Windows 热门应用

近日，外媒报道，流行软件构建框架 Electron 中存在一个严重的远程代码执行漏洞（CVE-2018-1000006），可能会影响大量热门桌面应用程序，比如 Skype，Signal，Slack，GitHub Desktop，Twitch 和 WordPress.com 等。Electron 表示目前只有 Windows 的应用程序会受到漏洞影响。

Electron 由 GitHub 团队开发，是一个基于 Node.js 和 Chromium 引擎的开源框架，允许应用程序开发人员使用 JavaScript、HTML 和 CSS 等 Web 技术为 Windows，MacOS 和 Linux 等构建跨平台的本地桌面应用程序。目前至少有 460 个跨平台桌面应用程序使用了 Electron 框架。

目前 Electron 开发者已经发布了两个新的框架版本来解决这个严重的漏洞，即 1.8.2-beta.4,1.7.11 和 1.6.16。并表示该漏洞只影响 Windows 应用程序，Mac 和 Linux 的应用不在影响范围内。

（来源：https://thehackernews.com/2018/01/electron-js-hacking.html）

每周安全事件

类 型	内 容
中文标题	新的 HNS 僵尸网络已经损害了 2 万多个物联网设备
英文标题	New HNS botnet has already compromised more than 20,000 IoT devices
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	最近，安全专家发现了其他物联网僵尸网络，其中大多数与 Mirai 僵尸网络相关，如 Satori，Okiru 和 Masuta，但是 HNS 僵尸网络有着不同的起源，不共享源代码。 Bitdefender 的研究人员发现 HNS 和 Hajime 僵尸网络之间的相似之处，与 Mirai 不同，Hajime 不使用 C & C 服务器，而是实现了一个点对点网络。 Hajime 比 Mirai 更复杂，它实现了更多的机制来隐藏其活动和运行过程，其模块化结构允许运营商在飞行中添加新的功能 HNS 恶意软件能够利用 Reaper 作为一系列物联网设备，目前的版本能够接收并执行数据类型的命令，如数据泄露，代码执行和对设备操作的干扰。 据专家介绍，该僵尸网络仍处于开发阶段，其中不包括 DDoS 攻击能力，这种情况表明它将被部署为代理网络。
链接地址	http://securityaffairs.co/wordpress/68194/malware/hns-botnet-20000-iot.html

每周值得关注的恶意代码信息

经安天【CERT】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

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	G-Ware/Android.FakeCD.a[exp,rog] 2018-01-22	该应用程序伪装清理工具，功能简单，调用第三方框架安装恶意应用，私自下载未知文件，造成用户资费损耗，请卸载。（威胁等级低）
		Trojan/Android.SpyCamcorder.a[prv,spy] 2018-01-22	该应用程序包含恶意代码，运行后可以无声无图拍照或者摄像，并联网上传隐私。造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.PornoLocker.a[rog,lck] 2018-01-24	该应用程序运行不断弹出主界面，勒索用户付费解锁，影响用户手机的正常使用，建议卸载。（威胁等级中）
		Trojan/Android.FakeWallet.a[fra] 2018-01-25	该应用程序伪装成电子钱包，诱导用户将电子货币发送到指定地址，造成用户财产损失，建议卸载。（威胁等级中）
		Trojan/Android.FakeBetternet.a[exp] 2018-01-25	该应用程序运行后伪装成 Betternet，诱导用户点击菜单按钮，私自发送短信，同时监听用户接收的短信，当短信包含指定内容时，会私自回复短信，造成用户资费损耗，建议卸载。（威胁等级高）
		G-Ware/Android.AdultSwine.a[rog,exp] 2018-01-25	该应用程序安装后隐藏图标，推送色情广告，诱导用户安装恶意应用，推送虚假通知，诱导用户安装推广应用，还会弹出虚假问答类广告通知，诱导用户输入个人信息，可能用于注册其他风险类服务，造成用户资费损耗，影响用户正常使用，建议卸载。（威胁等级低）
	较为活跃的样本	Trojan/Android.SpamSold.b[spr,exp]	该应用程序运行后隐藏图标，后台私自向所有联系人发送包含软件下载链接的短信，可能造成用户资费损失，建议立即卸载。（威胁等级高）
		Tool/Android.SmsCtrl.b[prv,rmt]	该应用程序短信监控类工具，安装后监控短信，远程接受短信指令控制，具有短信转发、监听来电、回拨电话等功能，可能造成用户隐私泄露，警惕恶意利用，建议卸载。（威胁等级低）
		Trojan/Android.FakeFB.p[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。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 内存破坏漏洞（CVE-2018-0812）	Microsoft Office 内存破坏漏洞，CVE 编号 CVE-2018-0812，攻击者可以利用这个问题在当前登录的用户上下文中执行任意代码。失败的利用尝试，可能会可引发 DoS 攻击。（威胁等级高）
	较为活跃样本	Trojan[Dropper]/Win32.SysDrop	此威胁来自一种可以释放恶意代码的木马程序。该家族样本运行后释放恶意代码，一般为 sys 格式，有一定威胁。（威胁等级高）
		Trojan[Downloader]/JS.JScript	此威胁来自一种具有下载行为木马类程序。运行该脚本后会执行里面的代码，链接网络下载恶意文件。通常以网页挂马和邮件进行传播。（威胁等级中）
		Trojan[Backdoor]/Linux.Gafgyt	此威胁来自一种木马类后门程序，运行在 linux 平台，主要功能为 DDOS 攻击、更新和下载等。通过扫描 SSH 弱口令进行传播。（威胁等级中）

理解供应链网络攻击

Liviu Arsene / 文　安天技术公益翻译组 / 译

云计算和“一切即服务”（everything-as-a-service）提供商导致攻击面呈指数增长，尽管如此，托管公司仍然可以增强供应链安全。

数字化和网络互联导致当今的网络安全形势发生了巨大变化。其优势促使企业积极采用，但是相关的安全风险也引发了人们的担忧。“一切即服务”消除了传统的安全边界，并为企业可能无法识别甚至处理的新型网络攻击打开了大门。

如今，将资源转移到最终消费者手中涉及到使用复杂的供应商和服务网络来创建处理和分配商品的系统。第三方供应商通常能够在一定程度上访问其客户的网络，因此网络犯罪分子试图利用这些供应链这一点，再加上与关键内部基础设施相结合的先进软件堆栈，增加了攻击者攻破边界防御的攻击面。

信任经常被利用

云已经成为数字业务不可或缺的一部分，但云中缺乏适当的授权、追责和身份验证机制，导致了我们称为供应链攻击的安全威胁。采用云服务的企业必须定期评估外部审查计划和尽职调查流程。这种定期评估必须经过不断的迭代，以确定潜在的安全盲点，同时减少事件响应时间。

不幸的是，由于当前供应链存在固有的安全盲点，过去的几年里发生了一系列的供应链攻击，导致数百万客户的个人和私密数据遭泄。在美国零售巨头塔吉特（Target）攻击事件中，4100 万客户记录遭泄露，该事件是利用第三方对关键基础设施的访问权限执行供应链攻击的典型案例。

由于复杂的基础设施有时难以通过 IT 运营维护，因此使用可以在整个基础设施中远程部署的自动化工具对确保高效的供应链至关重要。不幸的是，这些工具——尽管是合法的——也可以被用作攻击企业的媒介，能够绕过标准的安全程序。CCleaner 是一个优化系统性能的热门免费工具，它被网络犯罪分子篡改并注入了针对技术和电信公司的恶意软件。由于 IT 运营部门在基础架构中广泛部署该工具，估计有 227 万个系统受到了该恶意软件后门功能的影响。

管理供应链风险

托管企业必须采用安全程序，不仅应涵盖内部基础设施，还应涵盖供应商、客户甚至合作伙伴。虽然内部 IT 和安全部门可能有强大的安全措施来阻止大范围的直接攻击，但是第三方合作者可能不会持有同样的信念。因此，在将供应商完全整合到内部基础设施之前，需要对其进行审查。

创建供应商管理计划的想法不错，可以从定义企业最重要的供应商开始。围绕基于风险的方法制定计划，可确保供应商不断得到评估且其政策与托管机构保持一致。

除了要求供应商及时通知任何内部安全事件之外，合作指南中还应包含定期安全报告，以定期评估供应商的安全状态。由于安全是一个动态和持续的过程，因此这些程序应该根据最佳实践和托管公司的安全要求不断进行更新和审查。

不断审查技术、人员和流程——无论是内部还是供应商的——可以过滤掉容易被利用的、可能对托管企业和供应商造成毁灭性后果的供应链攻击。这一程序应涵盖从企业员工到与现有系统相结合的新技术、与安全事件响应有关的内部流程以及最佳安全实践的所有内容。

安全边界消失

强大的边界防御已经不足以保护安全了；安全团队必须考虑到数字化已经消除了所有的网络边界。虽然攻击面因此呈现指数增长，但是托管公司仍然可以采取一些措施来增强供应链安全，即使只是建立新的安全程序。

安全边界消失是“基础设施即服务”的必然结果，说明企业必须改变安全模型以应对新的威胁全景。如前所述，定期评估对于建立和保持强有力的安全形势至关重要，但这只是加强防御所需的安全控制措施之一。数字领域的网络犯罪层出不穷，因此组织必须建立严格的授权、验证和追责机制来保护关键数据并控制谁有权访问这些数据。

部署专门为物理、虚拟、本地部署或云中基础设施设计的安全控制措施也很重要。要想充分和成功地利用“一切即服务”的优势，数字化企业和大型组织必须实施针对其风险情况定制的分层安全方法。

原文名称	Understanding Supply Chain Cyber Attacks
作者简介	Liviu Arsene。Liviu Arsene 是 Bitdefender 的高级电子威胁分析师，拥有强大的安全和技术背景。
原文信息	2018 年 1 月 19 日发布于 Dark Reading 原文地址 https://www.darkreading.com/cloud/understanding-supply-chain-cyber-attacks/a/d-id/1330808
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《Trojan[DDoS]/Linux.Agent.g 分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时发现一例 Linux 平台的具有 DDoS 功能的木马样本，该木马会在 Linux 系统中添加自身为启动项，并开启后门线程，守护线程，远程下载线程等恶意行为。

木马启动后，首先将其工作目录写进环境变量，之后将加密的工作路径和需要用的 linux 命令通过异或解密。然后对比参数数值，如果参数数值等于 2 则删除文件并从开机启动项中剔除。如果参数等于 3 则向自身数据末端加入一串随机的字符串以改变 md5 值，之后分别复制到 /usr/bin、/bin、/tmp 目录下并执行。然后确定自己是否在指定的工作目录下，如果不是则继续改变 MD5 值，分别复制到 /usr/bin、/bin、/tmp 目录下并执行。接着将自身添加为开启启动项并写入环境变量。然后开启守护线程，后门线程，远程下载线程。后门线程先进行 DNS 请求，之后将主机的内存、cpu 等信息加密传送给 C&C 服务器，循环运行且从另一个域名通过 GET 请求下载文件并执行。最后循环执行以下操作：复制到 /usr/bin、/bin、/tmp 目录，运行、删除文件，保证不被轻易删除并等待接收控制端指令，恶意样本可构造 UDP、TCP ACK、TCP SYN 报文，用于发起 DDoS 攻击。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。目前，安天追影产品已经实现了对该类木马样本的检出。

木马程序

安天【追影威胁分析系统】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：

文件由页面手工提交，经由 YARA 自定义规则鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、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。

最终依据静态行为鉴定器、智能学习鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	98baaf902f5802eb3cde175fef1ca4661599b937c3695d9f0a4c6722ccf99619
文件类型	BinExecute/Linux.ELF
大小	596 KB
MD5	BAFC3E5E6C52E7159C95294502FD83EB
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[DDoS]/Linux.Agent.g
判定依据	静态分析
下次鉴定时间	约 2 周
首次发现时间	2018-01-23 10:39
末次发现时间	2018-01-23 10:39

◆ 文件元数据分析

描述	值
File Size	596 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

◆ 鉴定信息

鉴定器	YARA 自定义规则鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、静态分析鉴定器、智能学习鉴定器、安全云鉴定器
判定依据	静态行为鉴定器、智能学习鉴定器
文件来源	页面手工提交
来源标识	admin
用户自定义标志	无
来源 IP	127.0.0.1
时间	2018-01-23 10:39