安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 02 月 12 日 (总第 124 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

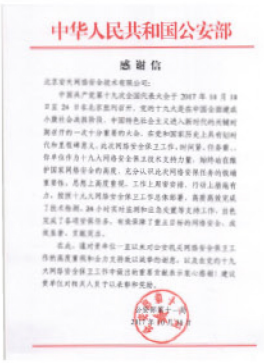
安天荣获党的十九大网上安保工作“优秀团队”称号

在近日由公安部主办的党的十九大网上安保工作优秀团队及个人表彰会上，安天武汉网络安全团队及安天黑龙江李柏松劳模创新工作室荣获党的十九大网上安保工作“优秀团队”称号。

中国共产党第十九次全国代表大会（简称党的十九大）于 2017 年 10 月 18 日至 10 月 24 日在北京召开。作为国家级网络安全应急支撑单位，安天为十九大提供了完善的网络安全保障服务。在十九大安保工作中，安天投入了近两百名工程师，组成了以安天技术负责人作为总指挥，包括总体协调、事件研判、通报联络、威胁分析、现场处置等九个工作组共同组成的安保团队。

安天作为国家应急响应体系的重要成员单位，参与了历次重大政治、社会活动的网络安全保卫工作，如十七大、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、9·3 抗战胜利日阅兵、G20 峰会、一带一路高峰论坛、金砖国家峰会等。此番再次获得行业管理机构的认可，是安天人的荣誉，亦是对安天在网络安全领域披荆斩棘、砥砺前行的勉励。

十九大期间，安天始终站在维护国家网络安全的高度，按照国家网络安全主管部门、执法部门的要求和所保障的关键信息基础设施运维机构的需求，高度关注持续监测安全威胁状态，密切注意关键信息基础设施、党政信息系统和网站安全运行状况，随时进行风险排查研判上报和应急处置，高质高效完成了技术检测、24 小时实时监测和应急处置等支持工作，有效保障了重点目标的网络安全，并收到了公安部第十一局发来感谢信。


中华人民共和国公安部

感谢信

自动化黑客工具 Autosploit 公开，大批 IoT 设备或将遭殃

名为 Vector 的研究人员在 GitHub 上发布了一款极具争议性的工具“Autosploit”，由于这款工具结合了“最可怕的搜索引擎”Shodan 和开源渗透测试工具 Metasploit，就连业余黑客也能借助该工具轻松入侵易受攻击的 IoT 设备。安全研究人员、渗透测试人员和“红队”（Red Team）使用的工具常常引发争议，因为他们将此类工具进行组合，将其自动化。而别有用心的人也会利用这些攻击发起恶意攻击企图。AutoSploit 就是一款自动化利用远程主机的工具，它能自动发现易受攻击的 IoT 设备，然后自动利用漏洞向目标发起攻击。Vectra 的安全分析负责人克里斯·莫拉莱斯解释称，Metasploit 降低了黑客实施入侵的技能门槛，Shodan 则可搜索任何暴露在互联网上的联网设备，将这两种高度自动化的工具相结合大大降低了黑客入侵的门槛，Autosploit 使入侵变得极其容易。这款工具令他非常担心 IoT 安全，据他预测，将会有一大波 IoT DDoS 攻击和加密货币挖矿活动汹涌而至。恶意攻击者只需编辑所使用的 modules.txt 文件，便能添加更多模块。

（文章来源于 https://www.easyaq.com/news/1891006161.shtml）

尊敬的读者：

2018 年春节即将来临，《安天周观察》于春节期间休刊两期，恢复出版时间为 2018 年 3 月 5 日。感谢所有读者对《安天周观察》一直以来的支持与关注！

祝大家春节快乐！

2018 年 2 月 12 日

安天发布《盗号木马“jLog”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注意到，一种新型利用CVE-2017-8759漏洞的盗号木马在网络中开始传播，当用户打开携带有恶意代码的文档时，就会触发漏洞，联网下载盗号木马源代码并编译运行。该木马会执行窃取计算机信息，盗取Firefox、Chrome浏览器密码等操作，对用户的计算机安全产生了较大的威胁。

“jLog”盗号木马利用Office文档作为传播载体，该文档在打开时会联网请求一个png格式的文件，该png文件是一个精心构造过的用于触发漏洞的文件，其文件内包含着一段混淆过的C#代码，漏洞触发后该段代码被C#编译器编译运行，释放jar木马文件，再由C#程序运行jar木马。该木马的运行需要Java环境，依赖jdk 1.8版本，也就是说如果jdk版本低于1.8或没安装jdk，该木马就运行不起来。由于Java的跨平台性，该木马支持Windows/SunOS/Nix/Mac多个操作系统。其运行后会检测当前木马程序是否需要更新，如果有更新就运行更新模块。随后会收集计算机名、当前登录的用户名、国家、cpu信息、主板信息、网络ip信息、jdk版本信息、内存信息、操作系统信息等，并在后台将这些信息发送到指定邮箱中。还会实现打开键盘记录器记录键盘操作、截取当前计算机屏幕、修改注册表项实现开机自启等功能。

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高级威胁的检出。

高级威胁

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述高级威胁进行有效检测，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、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。

最终依据静态行为鉴定器、智能学习鉴定器将文件判定为疑似高级威胁。

◆ 概要信息

文件名	c3444be8618346d4ed36eb06291fb2e53ce3e8961f94e35c3417681a070dd916
文件类型	Document/Microsoft.RTF[:Rich Text Format]
大小	628 KB
MD5	ACC6BBE8742E42200B68F5C3A1116A3C
病毒类型	疑似高级威胁
恶意判定 / 病毒名称	Trojan[Exploit]/RTF.CVE-2017-8759
判定依据	静态分析

◆ 运行环境

操作系统	内置软件
Windows XP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 危险行为

行为描述	危险等级
延时	★★★

◆ 常见行为

查找指定内核模块	★
创建特定窗体	★
获取计算机名称	★
获取驱动器类型	★
请求加载驱动的权限	★
获取系统内存	★★
查找特定窗体	★
获取主机用户名称	★
独占打开文件	★
获取系统版本	★★
获取 socket 本地名称	★
连接网络	★
查找浏览器进程	★★

◆ 监控预警

PID	创建
1608	C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE
1212	wuauclt.exe

为何说网络自动化不是“职位杀手”

Michael Bushong / 文　安天技术公益翻译组 / 译

自动化网络运营的价值不在于削减人员成本。

目前流行着这样一个观点：随着企业 IT 采用自动化技术，网络工程师将会失去工作。该观点的前提是，自动化能够帮助公司减少昂贵的运营成本（即高薪网络专家）。现有的认证工程师将被相对低薪的软件通才替代。

然而这并不是自动化的价值；自动化的关键在于协作。自动化在两个事物的边界上是最有用的，如两个人、两个系统、两个企业等。当需要协作时，自动化能够自动传递信息，以减少协调活动所需的时间。

世界末日论

当然，有些人将自动化视为灾难。要想充分利用自动化，企业需要变换员工队伍并撤销某些职位，用低薪的通才取代高薪的专家。他们说，尽管自动化有助于提高灵活性，但真正的好处是可以减少与需要人工的基础设施的交互次数。

通过完全消除这些工作流程，可以减少支撑基础设施所需的人员数量，而且不会对运营产生什么影响。“世界末日论”很快就被推翻了。

自动化在于节省时间而非按键

自动化的主要价值不是简单地减少按键或使命令更容易输入。有些人认为自动化的主要好处是将复杂的按键序列实现快速和高度的自动化，而且不会出现人为错误。但是同样的好处可以通过设立码字团队获得。

例如，连接到服务器需要服务器和网络团队之间的协调，所需的按键并不是特别复杂的。公司启动服务器所花费的时间主要在于协调工作和对提议的更改进行审查。

如果这些活动实现自动化，将不再需要

协调，而这正是自动化的最大效益所在。

自动化在于壮大企业而非降低成本

认为“自动化会消除工作”的人们还犯了一个更加根本的错误。

哪种程度的自动化能够减少人员投入？要注意：这可不仅仅是一些脚本化的工作流程。公司将不得不改变他们的工具，引入 DevOps 类型的框架并利用关键的编程和系统技能。

问题在于这将需要几年的时间来准备。在准备就绪之前，公司需要进行双重投资：在构建新的运营框架的同时支撑着旧的基础设施。

增加运营成本（OpEx）的真正原因并不是在短期内降低成本，而是改变成本能力（cost-capacity）曲线。公司正在扩大规模，并且意识到他们不能随着应用和用户需求线性地增加员工队伍，因此他们开始追求先进的自动化。如果企业目标是改变成本曲线，为增长做好准备，那么企业不大可能裁员，因为随着企业壮大他们仍然需要人才。

通才和专家

然而，高度自动化的未来确实意味着基础设施的设计、部署和维护方式会发生变化。采用自动化技术的公司最终将从以设备为主导转向以架构为主导，甚至以运营为主导。

今天，大多数企业都是以设备为主导的，而大型云提供商则是以运营为主导的。前者是指逐个设备地指定行为，随着自动化的深入发展，这种方式将演变为以架构为主导，并最终演变为以运营为主导。另一方面，大型云提供商做出关键的运营决策（如数据建模、数据收集和 API 策略），这些决策塑造了体系架构，最终形成了部署的设备。在这个世界上，设备及其配置和命令从属于更广泛的运营架构。

然而，仍然需要有人知道路由器和交换机是如何工作的。

只有像网络工程师这样的专家才能理解网络协议和故障排除。那些认为可以撤销这些职位来大规模削减成本的公司是在拿他们的基础设施玩俄罗斯轮盘游戏。（译者注：Russian roulette，俄罗斯轮盘是一种残忍的赌博游戏，其规则很简单：在左轮手枪的六个弹槽中放入一颗或多颗子弹，任意旋转转轮之后，关上转轮。游戏的参加者轮流把手枪对着自己的头，扣动板机；中枪的当然是自动退出，怯场的也为输，坚持到最后的就是胜者。旁观的赌博者，则对参加者的性命压赌注。）他们可能在好几次扣动扳机后仍然活着，但是夜路走多难免会碰到鬼，他们总有一天会需要专家人才。

底线

如果企业的目的是降低成本以获取竞争优势，则他们不适合向这一推动更大的灵活性的技能转型投资。自动化不会压缩企业 IT 员工队伍。

但是网络工程师的角色正在改变。聪明的操作员会发现扩展他们的技能——掌握系统级设计和一些编程技能——将使他们在新的世界里更受欢迎。当然，新增加的工作可能会青睐通才，因为公司正在将软件和网络结合起来，以推动自动化成为现实。

原文名称	Why Network Automation Isn't a Job Killer
作者简介	Michael Bushong。Michael Bushong 是瞻博网络公司企业云营销副总裁
原文信息	2018 年 2 月 2 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/networking/why-network-automation-isnt-job-killer/23268880
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。

每周安全事件

类 型	内 容
中文标题	研究人员将美国国家安全局 (NSA) 的 EternalSynergy、EternalRomance 和 EternalChampion 移植到 Metasploit 上。
英文标题	Researchers ported the NSA EternalSynergy, EternalRomance, and EternalChampion to Metasploit
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	RiskSense Sean Dillon（@ zerosum0x0）的安全研究员移植了 Rapid7 Metasploit 这三个据称从 NSA 连接的方程式组中被盗的黑客工具。 研究人员修改了这些漏洞，并将它们与最新的 Windows 版本相结合，并将它们合并到 Metasploit 框架中，他们应该在基于 x86 和 x64 架构的所有未修补的 Windows 版本上工作。 这三个漏洞是黑客船员影子经纪人在 2017 年 4 月泄漏的 EternalSynergy，EternalRomance 和 EternalChampion。这些工具后来被用在野外的几次攻击中，例如，在恶意软件 Bad Rabbit 勒索软件攻击中使用了 EternalRomance 漏洞。 移植到 Metasploit 的版本可用于自 Windows 2000 以后的所有 Windows 版本。
链接地址	http://securityaffairs.co/wordpress/68768/hacking/eternalsynergy-eternalromance-eternalchampion-metasploit.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	较为活跃的样本	Trojan/Android.emial.gj[prv]	该应用程序为拦截马，伪装成中国移动诱骗用户，获取设备管理器权限，私发短信，后台拦截短信并上传，泄漏用户隐私，请立即卸载。（威胁等级中）
		Trojan/Android.Mobilespy.aj[prv]	该应用程序运行后会获取用户的短信信息及联系人信息，并将短信信息及联系人信息上传到指定网址，可能会造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.BKspy.b[prv,exp]	该应用程序伪装正常应用，运行拦截用户短信接收指令，通过邮箱发送用户手机的图片、联系人、短信、证书等信息，造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.Vitamio.b[exp]	该应用程序包含风险代码，运行跳转推广页面，诱导用户点击下载，造成用户流量资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.LockScreen.ao[rog,lck]	该应用程序运行自动将手机调节最大音量，播放色情音频文件，可能会造成用户的尴尬和恐慌，而后置顶勒索界面，勒索用户付费解锁，建议卸载。（威胁等级中）
		Trojan/Android.Fakegoogleplay.c[exp,sys]	该应用程序伪装正常应用，运行隐藏图标，关闭 WIFI，访问重定向网页，通过加载 JS 脚本，执行 WAP 计费，造成用户资费损耗。（威胁等级高）
		Trojan/Android.spymessage.f[prv,exp]	该应用程序伪装成号码定位系统，私自拦截、上传短信，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.PhoneTools.b[prv,spy]	该应用程序为手机监控工具，安装无图标，运行无明显提示，应警惕该程序被恶意利用，窃取用户、短信、通话记录、位置信息，造成隐私泄露。（威胁等级中）
		Trojan/Android.CPUMiner.c[exp,rog]	该应用程序运行诱导激活设备管理器，隐藏图标，上传设备 cpu 等参数信息，后台私自挖矿，会占用设备内存，同时造成损耗，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 远程代码执行漏洞（CVE-2018-4878）	Adobe Flash Player 远程代码执行漏洞（CVE-2018-4878），攻击者可以将恶意 Flash 文件嵌入 Office 文档、网页，或者桌面应用，当用户打开时便会受到攻击。Adobe 已经确认了该漏洞的存在。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/Win32.VB	此威胁是一种以 VB 语言开发的，具有下载功能的木马类程序。该家族程序就会在系统启动时自动运行。通常是从网页中下载或是捆绑正常程序。这种类型的恶意代码通常会在用户访问具有漏洞的网站时感染计算机。（威胁等级中）
		Trojan[Backdoor]/Linux.Gafgyt	此威胁是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）
		Trojan[Backdoor]/Win32.Agent	此威胁是一种木马类后门程序，是一个通过代码基因来定性的木马类程序，家族变种之间具有相同或者相似的源码和核心技术。它可以连接远程服务器接受攻击者恶意操作，包括下载与更新其它恶意代码、添加删除系统文件、窃取用户敏感信息等。（威胁等级高）