安天周观察

主办：安天　2017 年 9 月 25 日（总第 105 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

共推网安等保：安天亮相第六届全国网络安全等级保护技术大会

9 月 22 日，第六届全国网络安全等级保护技术大会在南京召开。本次会议由公安部网络安全保卫局、中央网信办网络安全协调局、国家保密局、国家密码管理局、中国科学院办公厅指导，公安部第一研究所主办，有来自政府部委、中央企业、各地网安、测评机构、安全厂商等共计 600 多人参会。安天作为支持单位之一参与了本次会议，安天研发副总裁王小丰在会上带来了题为《赋能用户 保障安全 安天的关键信息基础设施安全防护实践防护分享》的演讲。

《中华人民共和国网络安全法》自 2017 年 6 月 1 日起已正式实施，其中第二十一条规定了“国家实行网络安全等级保护制度”，标志着等级保护已进入 2.0 时代，也更加需要政府、企业、群众等多方力量联合发动，才能尽早实现我国建设网络强国的目标。本次会议旨在深入实施国家网络安全等级保护制度和信息通报预警工作，推进网络安全等级保护技术交流和工作开展，促进重要行业部门、网络安全企业、科研机构、专家及公安网安部门的技术交流与合作。

安天研发副总裁王小丰在演讲中介绍了关键信息基础设施面临的威胁与挑战，并通过三起关键信息基础设施遭受攻击的案例分析，指出关键信息基础设施面临攻击成本正不断下降、受损风险不断上升的挑战。WannaCry 事件的爆发和巨大的应急响应成本更说明我国关键基础设施仍旧脆弱，面临的网络安全形势极其严峻。从安天的视角，王小丰介绍了关键基础设施的有效防护手段，他表示急需建立在基于网络安全的“敌情想定”，以“抵近部署、集中感知、有效防护、快速响应”作为策略，提升关键信息基础设施的防护水平。

安天作为中国能力型安全厂商的代表之一，将积极参与网络安全等级保护的关键技术研发和技术手段建设，并将发挥自身能力，为构建并完善以保护国家关键信息基础设施安全为核心的网络安全等级保护技术支撑体系贡献自己的一份力量。

黑龙江省委网信办开展『网络安全知识进课堂』活动

9 月 18 日上午，2017 年黑龙江省网络安全宣传周在黑龙江大学正式开幕，本届宣传周为期七天。宣传周期间，黑龙江省委网信办组织相关网络安全企业，于 9 月 19 至 20 日开展以“网络安全知识进课堂”为主题的宣传活动。

黑龙江省委网信办将“网络安全知识进课堂”列入本次宣传周的重要环节，加大对高校师生及青少年的网络安全意识培养，提高对于网络威胁的防范能力，提升社会各个层面对于网络安全的关注程度。

本次“网络安全知识进课堂”宣传活动，来自安天、360、绿盟科技等多位网络安全行业资深讲师，联合哈尔滨师范大学、黑龙江科技大学等高校，进行网络安全知识科普讲解，高校学生积极参与互动，针对相关问题讲师答疑解惑。

此次活动加强了网络安全宣传教育的力度，为营造健康文明的网络环境从教育环节夯实了防线，在增强师生网络安全防范意识和自我保护技能方面都取得了良好的效果。

■ 新型 Android 恶意软件感染多款银行与社交媒体应用

近日，据外媒报道，研究人员发现一款新型 Android 银行恶意软件 Red Alert 2.0，允许黑客窃取用户敏感信息、劫持短信邮件，并阻止与银行、金融机构相关的所有来电呼叫。目前，Red Alert 2.0 已感染 Google Play 商店上超过 60 款银行与社交媒体应用。不过，与其他 Android 木马不同的是，该恶意软件是由开发人员从零开始编写。如果目标设备的 C & C 服务器被关闭时，该恶意软件可以通过 Twitter 保存所有数据信息。然而，当设备无法连接到硬编码的 C2 时，它可以从 Twitter 帐户中重新检索一台新 C2 服务器进行连接。研究人员表示，这也其第一次从移动设备的恶意软件中发现此类银行木马。（来源：ibtimes.co.uk）

■ 黑客利用 WSL 攻击 Windows 操作系统

近日，Windows 10 引入的 Subsystem for Linux(WSL) 功能，允许用户在 Bash 终端运行 Linux 可执行文件。研究人员近期报告了黑客利用 WSL 的新攻击方法，他们称之 Bashware 攻击。研究人员表示，现有的安全产品还没有适应去监视运行在 Windows 操作系统上的 Linux 可执行程序的进程，从而为网络犯罪分子打开了新的攻击大门，即利用 WSL 提供的功能躲避检测、运行恶意代码。目前，研究人员已在现有的杀毒软件和安全产品上测试了 Bashware 攻击，发现它能够躲避所有安全产品的检测。（来源：solidot.org）

每周安全事件

类 型	内 容
中文标题	系统清理工具 CCleaner 被植入后门，可能影响 200 多万用户
英文标题	Warning: CCleaner Hacked to Distribute Malware; Over 2.3 Million Users Infected
作者及单位	Swati Khandelwal；The Hacker News
内容概述	近日，据外媒报道，著名的系统优化工具 CCleaner 的某个版本被发现植入后门，大量使用该工具的用户恐将面临泄密风险。这是继 Xshell 后门事件后，又一起严重的软件供应链来源攻击事件。CCleaner 是一款免费的系统优化和隐私保护工具。主要用来清除 Windows 系统不再使用的垃圾文件，以腾出更多硬盘空间，并且还具有清除上网记录等功能。被植入后门的版本为 8 月 15 日上线的 5.33 版本 (CCleaner5.33.6162)。出现问题的版本是在 2017 年 8 月 15 日发布的，直到 9 月 11 日才从官方服务器上移除。由于该版本使用了有效的数字签名，因此截止到目前为止大多数安全厂商仍无法检测。CCleaner 总共拥有 20 亿次下载量，且每周的下载量超过 500 万，从发布日期到移除日期，可以估算该版本已经有将近 2000 万次数的下载量，这意味着有大量用户可能已经受到感染。
链接地址	http://thehackernews.com/2017/09/ccleaner-hacked-malware.html?m=1

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 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	RiskWare/Android.LuaHtml.a[exp]	该应用程序运行通过 LUA 脚本加载指定网站，如：秒赞、代挂、刷空间留言、破解、卡盟、博彩、色情等类型的网站，造成用户资费消耗，建议谨慎使用，避免上当受骗。（威胁等级中）
		G-Ware/Android.psmf.a[fra]	该应用程序用于制作虚假微信、支付宝等应用的转账、交易、账户信息记录的界面，易被用于恶搞、诈骗，建议不要使用。（威胁等级高）
		Trojan/Android.parsibagan.a[prv，exp，spy]	该应用程序伪装成系统更新程序，运行会隐藏图标，后台监听用户通话，私自录像、录音，窃取用户短信、联系人、通话记录、地理位置等信息并通过邮件发送至指定邮箱，会造成用户隐私泄露，建议不要使用。（威胁等级高）
	较为活跃的样本	Trojan/Android.Dendroid.g[prv，rmt，spy]	该应用程序运行会隐藏图标，接收远程指令，上传用户通讯录、通话记录、短信、位置、文件列表、微信聊天记录、百度账号密码等隐私信息，并私自执行拍照、录音、截屏、发送短信等恶意行为，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Dropper.n[exp，rog]	该应用程序伪装正常应用，运行会隐藏图标，加载恶意子包，频繁推送广告，造成用户流量消耗，建议不要使用。（威胁等级高）
		Trojan/Android.SmsSend.ne[prv，exp]	该应用程序运行会诱导用户点击按钮发送付费短信，私自拦截短信，造成用户资费损失，建议不要使用。（威胁等级中）
		Trojan/Android.Ztorg.c[prv，exp]	该应用程序包含风险代码，会联网上传设备固件信息，可能会私自下载子包、加载广告，该程序会造成用户资费损耗和隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.legal.b[prv，rmt，exp，spy]	该应用程序伪装成银行应用，运行会诱导激活设备管理器，接收短信指令，上传用户信箱、通话记录、位置等隐私信息，还会私发短信，造成用户隐私泄露和资费损耗。（威胁等级中）
		G-Ware/Android.HiddenAds.cj[exp，rog]	该应用程序运行后台加载恶意广告子包，通过通知栏推送、弹窗和加速球等模式展示广告，会造成用户资费消耗，建议卸载。（威胁等级低）
		G-Ware/Android.qqzan.b[rog，pay，exp]	该应用程序为虚假 QQ 刷赞、永久会员等业务的办理工具，欺诈诱导用户付费，会造成用户资费损失，建议谨慎使用。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft .NET SOAP WSDL 解析器代码注入漏洞 (CVE-2017-8759)	该漏洞影响所有主流的 .NETFramework 版本。由于主流的 Windows 操作系统都默认内置了 .net 框架，黑客通过 Office 文档嵌入远程的恶意 .net 代码进行攻击，所有的 Windows 系统及安装了 Office 办公软件的用户都会受到影响。（威胁等级高）
	较为活跃样本	Trojan[Dropper]/Win32.Agent	此威胁是一种以基因片段定性的木马类程序。该家族以捆绑安装为主要传播手段，将木马程序与正常软件捆绑，并将捆绑后的文件上传到下载网站中。（威胁等级高）
		Trojan[Downloader]/Win32.Adload	此威胁是一种具有下载功能的木马类程序。该家族可以在电脑中下载并安装其他程序，这些程序可能是恶意软件或恶意软件组件，从而导致用户电脑感染恶意程序。（威胁等级中）
		Trojan[Banker]/Win32.Banker	此威胁是一种以窃取网络银行敏感信息为目的的木马类程序。该家族通过恶意网站或已被感染的邮件进行传播。该家族可以监控用户的网络行为，在用户登陆银行网站时记录用户信息，并将所有收集的信息发送给攻击者。（威胁等级中）

IT 部门面临的十大挑战

Emily Johnson / 文　安天公益翻译小组 / 译

如今的 IT 行业与 20 年前截然不同，但似乎年复一年地面临着同样的挑战：人才和技能短缺，以及预算限制。虽然面临的挑战是一样的，但是解决方式有很大的不同。

新技术和方法，如云计算、DevOps 和数据分析，正在帮助 IT 团队解决诸如基础设施能力、项目优先级排序和客户理解等问题，其影响远远超过旧的解决方案。最近，InformationWeek 和 Interop ITX 对 400 名 IT 专业人士进行了一次调查，以更好地了解他们的优先事项、挑战，以及用来实现目标的技术和策略。

◆ 不能很好地理解外部客户

在 2017 年，“理解外部客户”方面的挑战很小。60% 的受访者表示，根本不存在或者根本不关心该问题。也许，这归结于当今客户创造了大量的数据，以及公司采用了先进的数据收集和分析工具以便更好地了解其客户。27% 的受访者表示，他们的公司已经在实施客户服务分析，另有 34% 的受访者正在评估或计划在未来 12 个月内实施客户服务分析策略。

◆ 没有良好的外包关系

45% 的受访者表示，为了应对 IT 人才短缺，他们将寻求使用更多的外包服务和承包服务，所以 IT 企业应该与外包承包商维持良好的关系，这一点很重要。幸运的是，在 2017 年 IT 面临的挑战榜上，该挑战是很小的。考虑到 IT 企业已经使用外包服务多年，这一点并不奇怪。

◆ 与其它部门的关系差

5% 的受访者表示，他们与其它部门的关系仍然是一个重大挑战。14% 的受访者表示与其它部门的不良关系正在阻碍 IT 创新。

◆ 不能提供创新的、与业务有关的想法

IT 部门面临该挑战的原因并不是因为他们缺乏好想法。我们的研究显示，只有 25% 的受访者认为 IT 技能不足阻碍了组织创新。近一半 (49%) 的受访者表示，他们受困于日常业务，47% 的受访者表示缺乏预算会妨碍创新。

◆ 没有对项目进行优先级排序的系统

一个有组织的 IT 商店是高效和富有创意的，如果 IT 团队没有流程和技术进行优先级排序，则他们很可能只能对拥有最大预算的项目做出响应。49% 的受访者表示他们已经采用或将会采用 DevOps：其中 14% 已经采用，20% 将在未来两年内采用，另外 15% 将在两年后采用。但是，DevOps 并不是唯一的选择。51% 的受访者不打算采用 DevOps，他们或者拥有自己的项目交付流程，或者正在寻找另一个模型或系统。

◆ 没有足够的 IT 基础设施能力

2017 年，存储和管理企业创建和收集的所有数据仍然是一个巨大的挑战。40% 的受访者表示，存储空间 / 数据的增长对其 IT 基础设施影响最大。受访者表示计划在 2017 年购买云服务，其它技术则侧重于 IT 培训和教育。他们还表示，云将在未来五年对企业产生最大的积极影响。

◆ 实施速度不够快

显而易见的是，这些挑战都不是独立的，它们相互影响。IT 部门正在努力实现足够快的速度来实现 2017 年的业务目标。一半的 IT 人员表示，他们困于日常运作，很难有时间和精力进行创新。

◆ 缺乏适当的 IT 技能

64% 的受访者表示，在 2017 年，没有适当的技能对他们的团队来说是一个中等挑战。42% 的受访者表示，相比于外部招聘，他们在员工再培训方面更加成功，帮助员工掌握云、移动或数据分析等新技术。而 37% 的受访者表示，他们在招聘和再培训方面并驾齐驱。大约五分之一的受访者表示，他们在招聘外界人士来满足技能需求方面更加成功。

◆ IT 预算不足以实现目标

55% 的受访者表示，2017 年的预算有所增加，但仍然不足以达成业务目标。在经过多年的削减和冻结之后，许多预算可能还在恢复之中。这可能就是“IT 预算不足以实现目标”的原因，是 2017 年 IT 部门面临的第二大挑战。

◆ 没有足够的 IT 人才

预算紧张和技能短缺是最大的挑战。60% 的受访者表示，他们在一个或多个 IT 领域存在人才短缺问题。25% 的受访者表示，人才短缺阻碍了 IT 创新。根据该研究，IT 技能差距导致的最大业务影响是 IT 项目延迟 (53%)，其次是劣质 IT 项目 (30%)。40% 的受访者表示 IT 招聘被冻结，14% 的受访者表示要雇用外包商和承包商，25% 的受访者表示他们正在聘请专业技术人员，而只有 14% 的受访者表示他们正在跨多个 IT 领域进行招聘。

报告的作者指出，解决人才短缺的一种方法是迁移到云服务提供商，他认为这能够减少人力要求。尽管 IT 部门面临各种挑战，但 65% 的受访者仍然认为 IT 业是一个伟大的职业，并会向年轻人推荐。

原文名称	Top 10 Challenges IT Faces Heading Into 2018
作者简介	Emily Johnson，InformationWeek 的数字内容编辑。
原文信息	2017 年 9 月 18 日发布于 InformationWeek 原文地址 https://www.informationweek.com/strategic-cio/top-10-challenges-it-faces-heading-into-2018/d/d-id/1329858? 9?

安天发布《Trojan[DDoS]/Win32.Nitol.M 病毒分析报告》

自从“EternalBlue”——MS17-010 漏洞在 4 月份被发布之后，5 月中旬该漏洞的自动化利用工具如雨后春笋般出现在地下黑产中并迅速传播，目前为止，安天捕风监控小组捕获到的“EternalBlue”自动化利用工具已有多套。“EternalBlue”自动化工具出现时就已经实现漏洞与各类型病毒相结合。从早期监控捕获到的“EternalBlue”与 Gh0st 远控结合实现 RAT(Remote Access Trojan) 自动化种植感染，到现在的“EternalBlue”与 Nitol.M 结合实现 DDoS botnet 快速自动化拓展“肉鸡”，都警示着：互联网安全形势越发严峻，为互联网安全保驾护航更是任重而道远。

安天捕风监控对一则木马感染事件中捕获的样本数据进行了分析，发现了“EternalBlue”自动化利用工具以及 Trojan[DDoS]/Win32.Nitol.M 被控端木马。另外，发现被控端木马可通过该工具利用 MS17-010 漏洞进行自动化“肉鸡”拓展。

样本运行时会通过是否存在服务名称“.Net CLR”来验证样本是否初次运行，如果该服务名称不存在，则将样本备份到本地并创建服务以实现样本自启动，从而使其长期驻留受害系统。

“肉鸡”向 C2 发送的首包内容主要为系统版本和 CPU 配置及内存信息，并实时等待接收 C2 的远程指令，接收到 C2 的远程指令后首先对指令类型进行识别鉴定，然后分类执行，远程指令类型主要包含有 DDoS Attack、Stop Attack、Download Files、CMD Shell、Delete Service。通过配置解密分析，Trojan[DDoS]/Win32.Nitol.M 同样继承 Nitol 家族系列的风格，使用“base64+ 凯撒位移 + 异或”三重算法进行加密。

Nitol.M 主要实现的 DDoS Attack 类型有 syn flood、udp flood、icmp flood、tcp flood、dns flood、cc flood。结合 7 月 21 日捕获到的同家族版本进行监控获取的攻击情报中得知，近一个月中共发起 579 次攻击、185 起攻击事件，主要使用的攻击类型为：syn flood 占 57.3%，cc flood(http flood) 占 28.6%，icmp flood 占 11.9%，tcp flood 占 2.2%。

据了解，目前网上流传的“EternalBlue”自动化漏洞利用工具，通过 IP 网段自动化批量扫描，每天仍旧能入侵大量设备并植入病毒，这从侧面说明还有很多设备尚未升级系统及修补漏洞补丁。因此，安天提醒广大互联网用户安全、健康上网，安装杀毒、防毒软件并及时升级系统和修补设备漏洞。

木马程序

安天【追影威胁分析系统】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、数字证书鉴定器、动态行为 (Windows7) 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 BD 静态分析鉴定器、动态行为鉴定器、静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

根据动态行为 (Windows7) 得出该文件具有以下行为：使用 cmd 删除自身、删除自身、释放 PE 文件、复制文件到系统目录、创建服务、启动服务、查找指定内核模块、创建特定窗体、获取驱动器类型、自启动。

根据动态行为（默认环境）得出该文件具有以下行为：使用 cmd 删除自身、删除自身、打开自身进程文件、释放 PE 文件、复制文件到系统目录、创建服务、获取驱动器类型、启动服务、查找指定内核模块、创建特定窗体、获取计算机名称、请求加载驱动的权限、获取主机用户名称、设置调试器权限、遍历进程、连接网络、获取系统版本、获取 CPU 信息、独占打开文件、自启动、疑似查找杀软进程。

同时，该文件会对虚拟机、沙箱技术进行检测。

文件名	./C7D0827B6224B86F0A90FA42A8D39EDD
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	26 KB
MD5	C7D0827B6224B86F0A90FA42A8D39EDD
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[DDoS]/Win32.Nitol.M
判定依据	BD 静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=C7D0827B6224B86F0A90FA42A8D39EDD

运行环境

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、ie9、office 2007、flash、wps、FoxitReader、adobe reader

危险行为

行为描述	危险等级	行为描述	危险等级
使用 cmd 删除自身	★★★★	删除自身	★★★★

其他行为

行为描述	危险等级	行为描述	危险等级
释放 PE 文件	★★	复制文件到系统目录	★
创建服务	★	……	……

运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认、ie6、office2003、flash、wps、FoxitReader、adobe reader

危险行为

行为描述	危险等级	行为描述	危险等级
使用 cmd 删除自身	★★★★	删除自身	★★★★

其他行为

行为描述	危险等级	行为描述	危险等级
打开自身进程文件	★	释放 PE 文件	★
复制文件到系统目录	★★	……	……