安天周观察

主办：安天　2017 年 6 月 5 日（总第 89 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布《NSA 系列外泄军火级漏洞应对手册》

5 月 12 日 20 时左右，全球爆发大规模的 WannaCry（魔窟）勒索软件感染事件，该勒索软件迅速传播的原因是利用了基于 445 端口传播扩散的 SMB 漏洞——MS17-010。该漏洞利用工具原本是美国 NSA 下属的 Equation Group（方程式组织）使用的“网络军火”，在 2017 年 4 月 14 日的被黑客组织 Shadow Brokers（影子经纪人）曝光，而该勒索软件的攻击者或攻击组织在借鉴了该“网络军火”后进行了此次全球性的大规模攻击事件。

关于本次事件需要注意的是，WannaCry（魔窟）勒索者蠕虫仅利用了被曝光“网络军火”中的“永恒之蓝”(Eternalblue) 漏洞，Shadow Brokers（影子经纪人）曝光的“网络军火”中还有系列的漏洞及其利用工具需要关注和防范。同时，Shadow Brokers（影子经纪人）在 5 月 16 日再次发布声明，称其会在 6 月公布更多漏洞，鉴于以上原因，需要对当前已知的和未来将出现的威胁做好相应的防护和准备工作。

在面对各种严峻的安全风险时，除了通过有效的安全设计和使用安全产品形成防御能力之外，我们必须要做好合理的补丁策略、端口和应用的管理策略、边界的安全条件等基础安全工作。安天建议普通的桌面系统和不重要的服务系统在内部无法安装在线补丁的情况下，先安装基础补丁包，然后再安装无法安装的补丁包。因为基础补丁包体积较大，一旦出现大型的安全事故，由于大量用户进行下载，可能造成下载不成功的情况，因此希望网络管理员提前储备基础补丁包及重要补丁包。（具体操作流程请查看：http://www.antiy.com/response/Antiy_Wannacry_NSA.html）

安天蝉联 5 届 CNCERT “国家级”应急支撑服务单位

5 月 22 日 -24 日，第 14 届中国网络安全年会在青岛举行。安天首席技术架构师 seak、研发负责人王小丰分别就安天在威胁防御方面的认识和应对以及安天态势感知技术为内容发表演讲。同时，安天被授牌“国家级网络安全应急服务支撑单位”，这是安天连续 10 年、第 5 次蝉联该荣誉。

在过去的两年中，安天持续跟踪分析重大漏洞、恶意代码和 APT 组织的行动线索，发布内部和公开分析报告近百篇。在近期全球爆发勒索者蠕虫病毒 WannaCry 后，安天第一时间启动了“A”级灾难响应，上报主管部门，到达用户现场；第一时间发布深度报告，发布免疫工具和查杀工具，向公众发布“周一开机指南”和针对用户高频问题进行回复的 FAQ。在 CNCERT 发布的《关于防范 Windows 操作系统勒索软件 WannaCry 的情况通报》中，向公众推荐使用了安天的免疫、专杀工具、内存秘钥获取和解密工具等。这是安天作为国家级应急支撑单位和主管部门紧密合作、联合快速响应处置的最好体现。

安天的 5.25 一周年答卷

一年前的 5 月 25 日，习总书记在黑龙江调研时，来到安天视察。“你们也是国家队，虽然你们是民营企业”。殷殷期望，已经刻入安天人的心中。一年过去了，安天始终坚持以“国家队”的坚毅信念匹配习总书记的要求和嘱托，奋力践行对国家的使命、勇于承担对网络安全领域的责任。

在过去的一年中，安天始终站在应对安全威胁的第一线，针对“白象”等攻击完成分析溯源、针对“方程式”组织发布多篇深度分析报告。在近期的勒索软件感染事件中，安天第一时间响应，相继发布了深度报告、免疫工具、专杀工具、内存秘钥获取和解密工具等，并向公众普及处置方案。

安天坚持能力型安全厂商的定位和价值，坚持解决用户安全问题的信仰，直面安全威胁的信念和勇气，在安全威胁的感知、检测、防御、分析等方面，有多年持续积累。在过去一年，安天发起的关键基础设施防护百日研发大会战完成后，完善了包括威胁监测产品探海、终端防护产品智甲、威胁分析产品追影、和安天态势感知平台组成的产品体系。安天的全新态势感知系统围绕着资产和威胁视角展开，实现资产信誉评价和威胁认知，充分了解资产和威胁的关联，评价威胁对资产所造成的后果和风险。

过去一年中，安天持续为公安、海关、水利、交通等部委行业提供安全服务与解决方案。特别是为我国重大的国防、军工科研成果提供了网络安全保障，包括载人航天、空间站对接等，安天产品和服务都提供了发射任务的完整保障；也为我国商用大飞机首飞的网络安全提供保障。同时，安天作为中国网络安全供应链体系的重要角色，在过去与未来持续为全球 100 多家合作伙伴的超过十万台网络设备、超过六亿部智能手机提供安全防护。

安天始终不忘总书记的期望和要求，始终牢记总书记的认可和嘱托，将以更大的决心和努力践行“国家队”的使命和担当，继续奋斗在网络安全领域的前线。

每周安全事件

类 型	内 容
中文标题	Terror EK 漏洞开发工具包新添指纹识别功能
英文标题	Terror EK rising in the threat landscape while Sundown EK drops
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	据外媒报道，相关安全人员发现，继 Stegano 漏洞开发工具包 (EK) 更新版本发布后，Terror EK 于近期也进行了优化完善，不仅可以指纹识别用户设备，还可针对特定漏洞侵入目标系统。黑客曾在各地下论坛以不同名称发布 Terror EK 售卖广告。相关安全专家表示，Terror EK 在恶意软件传播活动中主要利用 IE 浏览器、Flash 与 Silverlight 漏洞传播 Smoke Loader。此外，Terror EK 还参与了另一起攻击活动，即利用不同登录页面传播恶意软件 Andromeda。 此外，安全研究人员还发现，Terror EK 使用基于 cookie 的身份验证下载漏洞并阻止第三方访问。据称该方法不仅可以防止调查人员了解受害系统如何遭受感染，还可防止其他攻击者窃取这些漏洞。
链接地址	http://securityaffairs.co/wordpress/58058/malware/terror-ek.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 5 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.jianmo.co[rog] 2017-05-22	该应用为锁屏类病毒，点击后会置顶锁屏界面，要求用户联系指定 QQ 解锁，请立即卸载。（威胁等级中）
		Trojan/Android.SmsSend.mm[exp, sms]2017-05-23	应用运行会隐藏图标，私自发送短信到指定号码，造成用户资费消耗，建议立即卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.SmsSpy.u[prv]	该应用伪装成游戏作弊器，诱导用户填写游戏账号密码，通过短信窃取游戏账号密码信息，请使用正版软件，建议卸载。（威胁等级高）
		Trojan/Android.ProgOrder.a[spr, sms]	该应用是一个软件交易平台，通过订购短信来传播恶意软件，造成用户资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.SMSBomber.am[exp]	该应用为短信轰炸机供用户实施对指定目标进行短信轰炸，建议谨慎使用。（威胁等级中）
		Trojan/Android.hiddenspy.a[prv, exp, sys]	该应用是一个间谍程序，运行后加载恶意子包，获取远控指令，静默安装其他软件，窃取用户手机基本信息，造成用户隐私泄露和流量消耗。（威胁等级中）
		Trojan/Android.QQspy.bw[prv]	该程序伪装成热门应用相关工具，诱导用户输入账号密码并通过邮件转发，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.SmsListener.s[prv]	程序运行时监听来信并将之上传至服务器，这会造成隐私泄露，建议卸载。（威胁等级高）
		G-Ware/Android.Fakegupdt.da[rog, exp]	该应用感染恶意模块，运行后激活设备管理器，获取手机固件信息并上传，加载流氓广告，诱导用户点击下载，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Office OLE2LINK 逻辑漏洞 (CVE-2017-0199)	该 Office 漏洞在无需用户交互的情况下，打开 Word 文档就可以通过 hta 脚本执行任意代码。此漏洞的成因主要是 Word 在处理内嵌 OLE2LINK 对象时，通过网络更新对象时没有正确处理的 Content-Type 所导致的一个逻辑漏洞。（威胁等级高）
	较为活跃的样本	Trojan[Backdoor]/Win32.PassCV	此威胁是一种可以窃取用户信息的木马程序。该家族样本运行后连接远程服务器，接受攻击者的恶意操作，收集用户敏感信息并回传。（威胁等级高）
		Trojan[Dropper]/WinLNK.Agent	此威胁是一种具有软件捆绑行为的木马程序。该家族的样本在执行后会同时安装所捆绑的软件，被捆绑的软件通常具有广告或携带有其他恶意软件行为。（威胁等级中）
		Trojan[Downloader]/MSWord.Saguaro	此威胁是一种具有下载行为的 Word 宏病毒家族。该家族的样本在执行后会连接远程服务器，下载其他程序并接受进一步的控制。（威胁等级中）
		Trojan/Win32.HangOver	此威胁具有木马家族的共有特点。该家族的样本在执行后会连接远程服务器，上传信息，并从远程服务器接受进一步的控制，例如更新自身程序，接受控制命令并执行等。（威胁等级中）

WannaCry 带来的五个安全教训

Ericka Chickowski / 文　安天公益翻译小组 / 译

安全行业应该采取更多的措施，以保护其系统和数据免遭网络勒索。

近日，WannaCry 攻击的影响范围和严重程度引发了人们对勒索软件的恐惧。该蠕虫以迅雷不及掩耳之势在全球传播。

5 月 12 日，共有 74 个国家的 4.5 万个系统遭到感染。根据欧洲刑警组织的统计，目前，该勒索软件已经感染了 150 个国家的 20 万个系统。虽然安全研究人员发现了可以利用的 killswitch(攻击开关)，但是攻击者迅速发布了新变种，每小时能够感染 3600 个系统。

我们不应忽视 WannaCry 带来的灾难，可以由此得出一些宝贵的经验教训。

教训 1：漏洞和补丁管理极为重要

打补丁，打补丁，打补丁。重要的事情说三遍。几十年来，这一直是安全专家的口头禅，而 WannaCry 攻击再次证明了这一点。该蠕虫之所以能够迅速蔓延，是因为全球运行着无数不受支持或未打补丁的操作系统。

eSentire 首席技术官马克・麦卡德尔 (Mark McArdle) 说：“我们希望各组织能够改变不良的打补丁习惯。微软甚至发布了针对 Windows XP 和 2003 的应急补丁，这说明了该事件的严重性以及在生产环境中部署过时的操作系统的巨大风险。”

教训 2：未知资产易被利用

WannaCry 感染很好地证明了攻击者能够轻松地攻击在不一致的资产管理中被丢失或遗忘的系统。

RiskIQ 的高级产品经理史蒂夫・金蒂 (Steve Ginty) 说：“攻击者通常会发现未知、无保护和不受监控的资产，并将其用作攻击向量。对于大型企业来说，这类资产通常很容易被黑客和威胁组织找到。因为它们不受监控，所以攻击者可以自由进出。为了保护自己，企业需要知道攻击者从防火墙外面能够看到什么。”

教训 3：网络分段能够有效降低风险

由于许多技术问题，许多组织难以更新旧版和嵌入式系统。许多医疗设备运行旧的 Windows 操作系统，由于政府法规以及医疗机构自己的担忧 (在更新过程中导致系统中断)，这些操作系统难以更新。

Tripwire 漏洞研究团队安全研究员克雷格・扬 (Craig Young) 说：“在许多情况下，设备永远不会更新，或者是因为操作系统不再受支持，或者是因为内存、存储和处理限制导致设备无法使用最新的软件进行有效的操作。最后，我认为许多医院管理人员并没有认识到在医疗设备上使用过时软件的危险，只要设备能够运行，就不必打补丁。这种心态极大地损害了医院的安全。”

这种现象说明，许多组织应该采取额外的控制措施 (如网络分段)。Veriflow 联合创始人兼首席技术官布赖滕・戈弗雷 (Brighten Godfrey) 说：“如今，完全断开网络的机器通常没有任何用处，但是我们应该对网络连接进行必要的限制。网络分段需要严谨的网络架构，特别是在防火墙，路由器和其他设备的配置不断变化的复杂环境中。严格的网络验证方法可以帮助确保预期分段不断实现。”

教训 4：网络攻击带来现实影响

说到医疗，世界各地的安全专家应该深思的问题是：网络安全已经不仅仅是保护数据了。当攻击发生时，会对病人的生命和肢体安全产生影响。

Imperva 首席产品策略师泰瑞・雷 (Terry Ray) 说：“随着许多医疗设备连接到互联网，一些设备被 WannaCry 感染导致无效也并不奇怪。”

针对英国国民健康服务中心的攻击导致其运作被迫终止，这威胁到了人们的身体健康。WannaCry 攻击带来的后果是真实而严重的。

教训 5：很容易忘记“可用性”

在信息技术风险管理的三脚凳 (机密性，完整性，可用性) 方面，许多安全机构经常忘记“可用性”。据 Cyence 研究人员估计，WannaCry 对公司造成的业务中断损失将超过 80 亿美元。

Cyence 首席技术官兼联合创始人乔治 (George Ng) 指出：“WannaCry 造成的业务中断很可能是该攻击最重要的部分。组织会遭受业务中断、收入损失和其他损失，即使能够修复感染，也需要花费一些时间才能恢复生产力。”

显然，这些都是很重要的教训。我们需要花一些时间将这些教训变成有意义的行动。

原文名称	5 Security Lessons WannaCry Taught Us the Hard Way
作者简介	Ericka Chickowski，专注于信息技术和业务创新，为 Dark Reading 撰写安全领域的文章。
原文信息	2017 年 5 月 18 日发布于 Dark Reading 原文地址 http://www.darkreading.com/attacks-breaches/5-security-lessons-wannacry-taught-us-the-hard-way/d/d-id/1328914?
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 Ramnit 家族分析报告》

近日，安天追影小组在梳理网络安全事件时，发现一个 Ramnit 僵尸网络家族，该木马运行于 Windows 平台，首次出现于 2010 年。经分析，该病毒作者借鉴 ZeuS 源代码进行修改，修改后生成的病毒迅速扩散，在短短三四年时间，木马感染超过百万用户。直至 2015 年，通过一些执法机构、ISP 和安全公司的共同努力，追溯到了大部分控制服务器，才使得 Ramnit 病毒得到遏止，但仍有少部分木马存活下来，在该病毒被遏制 9 个月后，监控设备发现大量 Ramnit 家族传播证据，表明该家族病毒再次卷土重来。

安天追影团队对该家族的样本进行分析发现：

1. Ramnit 家族具有较完善的窃密模块

该样本监控网页浏览活动，检测特定网页，主要是针对银行网页提取 cookie，因获取到 cookie 后则可不登录直接对网页进行操作，故对银行网站危害较大。该样本还具有扫描计算机硬盘的功能，并从中窃取文件，同时还能捕获 FTP 登陆凭证以及为攻击者提供远程控制权限。

2. Ramnit 家族具有持久威胁

相对于普通木马，Ramnit 家族病毒具有更高的潜伏性，木马运行后会在系统目录中释放大量复制体，并具有自启动、禁用高版本系统的权限管理、伪装成系统进程等能力。木马还会将自身副本植入计算机内存，通过对系统进程的数据替换隐藏，达到潜伏在系统中不易被杀软查杀的目的。

3. Ramnit 传播途径多样

该家族样本早期可通过文件感染作为传播途径、随后通过在受入侵的网站和社交媒体页面上托管开发工具包、在公共 FTP 服务器放置恶意软件等方式进行传播。

经过对 Ramnit 家族的分析发现，该家族已经危及全球范围，损坏广大用户的利益。安天提醒广大网络用户，要提高自身的安全意识，对于来源不明的邮件，不要轻易打开，禁用办公软件宏功能，及时更新系统最新补丁，安装杀毒软件，对于一些“未知来源程序”中所谓的杀软误报不要轻信，定时查毒、备份重要文件，以防止感染木马，损害自身利益。

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：可疑进程名称、关闭 UAC、修改注册表键值，使与系统安全相关的设置失效、禁用指定服务、允许防火墙例外、关闭防火墙、增加 winlogon 自启动项、释放 PE 文件、获取驱动器类型、访问文件尾部、查找指定内核模块、填充导入表（疑似壳）、遍历进程、复制自身文件、增加 run 自启动项、自启动。

根据动态行为（默认环境）得出该文件具有以下行为：可疑进程名称、其他进程写入可疑数据、注入其他进程、增加 winlogon 自启动项、关闭 UAC、修改注册表键值，使与系统安全相关的设置失效、禁用指定服务、允许防火墙例外、关闭防火墙、释放 PE 文件、查找指定内核模块、填充导入表（疑似壳）、获取计算机名称、打开自身进程文件、复制自身文件、获取驱动器类型、设置调试器权限、创建挂起的进程、访问其他进程内存、独占打开文件、增加 run 自启动项、遍历进程、访问 dns、连接网络、自启动。

文件名	0784E53B2F19069AE4101440C93FB311
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	503 KB
MD5	0784E53B2F19069AE4101440C93FB311
病毒类型	木马程序
恶意判定 / 病毒名称	Virus/Win32.Ramnit.am
判定依据	静态分析

危险行为

行为描述	危险等级	行为描述	危险等级
可疑进程名称	★★★★	关闭 UAC	★★★
修改注册表键值，使与系统安全相关的设置失效			★★★
禁用指定服务	★★★	允许防火墙例外	★★★
关闭防火墙	★★★★	增加 winlogon 自启动项	★★★★

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	★	获取驱动器类型	★
查找指定内核模块	★	访问文件尾部	★
遍历进程	★	填充导入表（疑似壳）	★★
增加 run 自启动项	★	复制自身文件	★★
自启动	★		

报告地址：https://antiy.pta.center/_lk/details.html?hash=0784E53B2F19069AE4101440C93FB311