安天周观察

主办：安天　2017 年 10 月 16 日（总第 107 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布应对微软 SMB 漏洞（CVE-2017-11780）免疫工具及响应手册

近日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft Windows SMB Server 远程代码执行漏洞（CNVD-2017-29681，对应 CVE-2017-11780）。远程攻击者若成功利用漏洞可允许在目标系统上执行任意代码，如果利用失败将导致拒绝服务。

CNVD 对该漏洞的综合评级为“高危”。综合业内各方研判情况，该漏洞影响版本范围跨度大，一旦漏洞细节披露，将造成极为广泛的攻击威胁，或可诱发 APT 攻击。

安天在 10 月 12 日 12 时首次发布了应对该漏洞的免疫工具及《安天应对微软 SMB 漏洞（CVE-2017-11780）响应手册》。安天提醒用户应警惕出现“WannaCry”蠕虫翻版，及时做好漏洞排查和处置工作，并建议用户及时安装相应的微软官方补丁；若由于相关原因不能及时安装，可利用系统防火墙高级设置阻止 445 端口的连接及网络共享，或下载安天 CVE-2017-11780 漏洞免疫工具进行免疫处理。

另外，安天智甲终端防御系统及探海威胁检测系统等产品对类似机理的漏洞均有检测防御安全策略。

手册原文　工具下载

安天获“北京市政务信息安全应急队伍”授牌

日前，在十九大网络安全保障动员会暨北京市政务信息安全应急队伍授牌仪式上，安天获授“北京市政务信息安全应急队伍”资质。政务信息安全社会应急队伍由北京市通信保障和信息安全应急指挥部办公室统一管理、北京市政务信息安全应急处置中心组织调度。在未来两年中，安天将为北京市政相关单位提供网络安全应急支撑服务。

本次会议上还发布了关于做好党的十九大期间网络安全保障工作的重要通知。通知要求，北京市政务信息安全应急队伍与各级相关单位即刻进入 24 小时备勤状态，确保十九大会议期间不发生网络安全事件，保证重要网络和信息系统绝对安全。

安天作为国家级应急支撑单位，是中国应急响应体系中重要的企业节点，在红色代码 II、口令蠕虫、震网、破壳、沙虫、方程式、白象、魔窟等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。安天多次在重大网络事故和网络安全事件的响应中发挥关键作用，曾参与十七大、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 峰会等重大活动的安保工作。

在目前的十九大网络安全保障工作中，安天将继续发挥在安全保障、应急响应等方面的技术和人才优势，提前将各类产品及工具准备好，对常见安全事件进行演练和培训，对安保人员的行为规范进行严格要求，以保证十九大会议的顺利进行。安天将一如既往，在维护国家网络安全工作中贡献自己的一份力量。

■ “KovCoreG”黑客组织使用虚假浏览器和 Flash 更新消息传播恶意软件 Kovter

近日，研究人员发现一个代号为“KovCoreG”的黑客组织长期在使用虚假的浏览器或 Flash 更新提醒消息来诱骗受害者安装恶意软件 Kovter。

该组织在 PornHub（一个色情影片分享网站）上通过恶意广告将受害者重定向到“紧急更新”的钓鱼网站页面。根据所使用的浏览器不同，受害者会收到不同内容的更新提醒消息。例如，使用 Chrome 浏览器和 Firefox 浏览器的受害者将收到要求下载浏览器更新的提醒消息，而使用 IE 浏览器和 Edge 浏览器的受害者收到的则是要求下载 Flash 更新的提醒消息。只要受害者点击“更新按钮”，就会下载安装恶意软件 Kovter 的 JavaScript（Chrome、Firefox）或 HTA（IE、Edge）文件。

（来源：https://www.bleepingcomputer.com/news/security/malvertising-group-spreading-kovter-malware-via-fake-browser-updates/）

每周安全事件

类 型	内 容
中文标题	全球知名的技术与市场调研公司 Forrester 遭遇黑客入侵
英文标题	Forrester, one of the most influential research and advisory firms was hacked
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	近日，技术与市场调研公司 Forrester 的安全专家发表声明，宣称公司网站系统已遭黑客入侵，黑客试图通过窃取客户登录凭证后接管公司网站、下载客户市场调研文件。不过，好在研究人员及时发现后立即对其进行拦截。研究人员表示，虽然黑客利用该途径窃取了客户调研报告，但目前并没有证据表明客户机密数据、财务信息，以及员工私人数据已被访问或公开。公司内部数据都是网络间谍手中的重要筹码，即可以访问与客户和项目相关的敏感信息。
链接地址	http://securityaffairs.co/wordpress/64016/data-breach/forrester-data-breach.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 8 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.Triada.bj[exp,sys]	该应用程序包含恶意代码，运行后加载恶意子包，推送广告，并存在私自下载、联网上传用户手机基本信息等行为，建议立即删除。（威胁等级高）
		Trojan/Android.emial.gi[prv,exp]	该应用程序运行后私发短信，监听收件箱短信并转发，同时上传收件箱短信，造成用户资费损耗和隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.Metasploit.c[prv,bkd]	该应用程序为重新打包的游戏应用，植入了后门程序，可以被远程控制，会窃取用户手机各项隐私信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		G-Ware/Android.FakeAV.n[pay,exp]	该应用程序伪装成杀毒软件，运行时会诱导用户付费，不具备实际杀毒功能，会造成用户资费损失，建议不要使用。（威胁等级低）
		Trojan/Android.FakeGoogleSys.e[rog]	该应用程序伪装成 Google 服务，会将指定服务放到前台执行使其不被 Android 内存管理销毁，警惕该程序配合其他木马使用，给用户手机带来安全风险。（威胁等级中）
		Trojan/Android.Locker.o[rog,sys,lck]	该应用程序伪装成 QQ 强制登陆工具，运行申请 root 权限，其后私自安装锁机程序，置顶界面，影响用户手机的正常使用，建议不要使用。（威胁等级中）
		RiskWare/Android.Triada.bk[exp]	该应用程序包含风险代码，动态加载第三方支付插件，会通过短信发送支付短信，建议谨慎使用。（威胁等级低）
		G-Ware/Android.Andut.b[prv]	该应用程序运行后加密上传用户 IMSI、手机号等固件信息，会造成用户隐私泄露，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	Dnsmasq 堆缓冲区溢出漏洞（CVE-2017-14492）	Dnsmasq 是轻型 DNS 转发器和 DHCP 服务器。Dnsmasq2.78 之前的版本在实现上存在堆缓冲区溢出漏洞，可使远程攻击者通过构造的 IPv6 路由器广告请求，造成拒绝服务或执行任意代码。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/Win32.Betload	此威胁是一类可以下载恶意代码的木马家族。该家族样本运行后连接远程服务器下载恶意代码并执行，会窃取用户信息并回传，具有一定风险。（威胁等级中）
		Trojan[Ransom]/Win32.Democry	此威胁是一类可以加密用户数据的木马家族。该家族样本运行后遍历系统文件并加密，它会在加密的文件名后面加上攻击者的邮箱地址，与其联系后才能获取付款以及解密的方法。（威胁等级中）
		Trojan[Downloader]/HTA.Locky	此威胁是一类可以下载勒索软件的木马家族。该家族样本是 Html Application 应用程序，运行后连接远程服务器下载 Locky 勒索软件并执行，会加密用户重要数据。（威胁等级中）

勒索软件觊觎备份：四种保护方法

Rod Mathews / 文　安天公益翻译小组 / 译

备份是防御勒索攻击的最佳方式，但它们也需要保护。

今年勒索软件来势凶猛。保守估计，WannaCry 和 NotPetya 两起重大攻击造成了数亿美元的损失，而网络犯罪分子则继续瞄准用户的系统和数据。

防御勒索软件的最佳方法是备份数据并设置经过充分测试的恢复过程。定期备份数据并能够快速检测勒索软件的公司能够在最短的时间内恢复数据和运作。

在某些情况下，擦除程序伪装为勒索软件，给出类似的赎金要求。在这些攻击中，即使受害者支付赎金也无法取回文件，此时从备份中恢复数据就更加重要了。

因此，勒索软件背后的网络犯罪分子开始瞄准备份过程和工具。一些勒索软件，如最近的 WannaCry 和较新版本的 CryptoLocker，删除了微软 Windows 操作系统创建的卷影副本。

在 Mac 系统上，网络犯罪分子从一开始就瞄准了备份。研究人员在 2015 年发布的第一个 Mac 勒索软件中发现了不完整的功能，它针对 Mac OS X 操作系统的自动备份工具 Time Machine 所使用的磁盘。

该策略很简单：加密备份，个人或公司就很可能会失去恢复数据的能力，更有可能支付赎金。攻击者已经不满足于感染单个工作站，他们不断升级攻击力度，旨在摧毁备份。

以下四个建议可以帮助企业保护其备份免受勒索攻击。

1、谨慎使用网络文件服务器和网络共享服务

网络文件服务器使用简单，它的两个属性使得可以通过网络访问的“home”目录成为集中数据并轻松备份的热门方式。但是，当暴露于勒索软件面前时，这种数据架构存在严重的安全漏洞。大多数勒索程序加密连网的磁盘，因此受害者的 home 目录也将被加密。另外，运行像 Windows 这样存在漏洞且经常被攻击的操作系统的任何服务器都可能被感染，这将导致每个用户的数据都被加密。

因此，任何拥有网络文件服务器的公司都需要将数据备份到单独的系统或服务中，并测试系统的恢复能力。

云文件服务也无法免疫勒索攻击。2015 年，一家为儿童演员及其父母提供信息的公司 Children in Film 遭到勒索攻击。该公司广泛使用云服务，包括一个常见的云盘。根据 KrebsOnSecurity 网站的一篇文章，在一名员工点击恶意电子邮件链接的 30 分钟内，存储在云盘中的 4000 多个文件被加密了。幸运的是，该公司的备份提供商能够恢复所有的文件，虽然恢复过程花费了将近一个星期。

根据云服务是否提供增量备份或容易管理的文件历史记录，恢复云中的数据可能会比恢复现场服务器中的数据更加困难。

2、实现备份过程的可视化

公司越早发现勒索软件感染，就越有可能防止重大的数据损坏。备份过程的数据可以提供勒索软件感染的预警。加密数据的程序会在备份日志中留下痕迹。随着每个文件的本质改变，增量备份将会突然“爆炸”，而且加密的文件不能被压缩或重名剔除。

定期监控重要的指标，如备份过程中的空间利用率，可以帮助公司检测勒索软件是否已经感染了公司内部的系统，并降低感染损害。

3. 考虑解决方案

如果勒索软件能够直接访问备份映像，那么阻止它加密公司备份将非常困难。因此，一个提取备份数据的专用备份系统将能够防止勒索软件加密历史数据。

通过将备份与正常操作环境分离并确保备份过程不在通用服务器和操作系统上运行，备份可以有效防御攻击。基于最常用的操作系统（微软 Windows）的备份系统容易受到攻击，使得企业更难保护备份数据。

4、定期测试恢复过程

最后，除非可以快速可靠地恢复数据，否则备份也不是什么好办法。一些勒索攻击的受害者已经备份了数据，但是仍然不得不支付赎金，这是因为他们的备份计划不够细粒度，或者他们错误地认为已经备份了某些数据。

最后，公司应该通过监控或反恶意软件防御措施尽早发现勒索攻击，使用专门的系统来分离备份数据和潜在的受感染系统，并定期测试备份和恢复过程，以确保数据受到妥善的保护。

原文名称	Ransomware Will Target Backups: 4 Ways to Protect Your Data
作者简介	Rod Mathews，Barracuda 副总裁兼数据保护业务总经理。
原文信息	2017 年 10 月 4 日发布于 Dark Reading 原文地址 https://www.darkreading.com/endpoint/ransomware-will-target-backups-4-ways-to-protect-your-data/a/d-id/1330029?
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]/Win32.Togapy 攻击情报报告》

近日，网上出现一篇《西方红玫瑰和辣条先生黑产组织深度分析报告》，文中详细描述该黑产组织主要使用的木马类型和盈利方式等，其中也提到有关“辣条先生”的DDoS木马的传播和感染分析，但并未对其家族鉴定和攻击情报进行分析报告。

安天捕风小组对前期监控捕获的hfs（HTTP Files Service）进行对比排查，确有在2017年7月19日捕获该hfs站点及其所有样本数据。对捕获该站点的样本进行分析鉴定，其中的DDoS样本为Trojan[DDoS]/Win32.Togapy家族。Togapy家族主要实现的功能是利用“肉鸡”做跳板对自定义目标执行DDoS攻击，其中主要实现的DDoS攻击类型为tcp flood、udp flood、dns flood、icmp flood、http flood这5种攻击类型向量。

在对该家族40天的监控里，共捕获到该家族的各个C2（控制节点）向“肉鸡”发送的攻击指令351672次，共695起事件。其中主要使用http flood攻击，占54.2%（377次）；其次是tcp flood攻击，占40.3%（281次）；syn flood攻击占4.1%（28次）。

在695起攻击事件中，操纵Togapy家族的C2主要部署于境外，且Togapy家族的695起攻击事件的攻击目标基本集中在国内的沿海省份，而受害者对象主要是非法网络博彩网站（例如：http://13ff8.com/main.html，https://www.4hgvip.com/main.html，http://www.xczx188.com/），色情网站（例如：http://www.2016mj.com），当然还有少部分游戏服务器和其他行业网站。从Togapy的攻击目标分析，也侧面表明目前DDoS僵尸网络地下黑产主要攻击对象着重于灰色地带的“黄”、“赌”产业方向，因为这些行业本身就属于非法行为并不受到国内法律保护，所以这些产业成为DDoS攻击攫取利润的主要攻击目标。

经过安天捕风小组的长期监控与跟踪发现，Togapy家族每天都在进行非法的DDoS攻击以获取更多的非法利益，已经严重威胁互联网安全发展，损坏广大用户的安全利益，也损耗互联网及设备资源。此外，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，不要轻易点击邮件中的网址，更不要轻易下载附件，以防止钓鱼邮件中的恶意代码的感染。

目前，安天追影产品已经实现了对该类木马家族的检出。

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、静态分析鉴定器、动态行为（默认环境）鉴定器、动态行为（Windows7）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、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（默认环境）得出该文件具有以下行为：使用cmd删除自身、访问免费域名、删除自身、延时、打开自身进程文件、释放PE文件、复制自身文件、获取驱动器类型、查找指定内核模块、获取主机用户名称、查找浏览器进程、访问dns、连接网络、获取CPU信息。

文件名	./e9ba3f25b5908faaf3c3dfb29c00e3df.danger
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	53 KB
MD5	E9BA3F25B5908FAAF3C3DFB29C00E3DF
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[DDoS]Win32.Togapy
判定依据	静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=E9BA3F25B5908FAAF3C3DFB29C00E3DF

◆ 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、Office 2003、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	★★★★
访问免费域名	★★★	延时	★★★

◆ 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	★	获取驱动器类型	★
释放 PE 文件	★	.....	.....

◆ 运行环境

操作系统	内置软件
Windows 7 6.1.7600 Build 7600	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	★★★★
访问免费域名	★★★	延时	★★★

◆ 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	★
复制自身文件	★	.....	.....