安天周观察

主办：安天　2017 年 9 月 4 日（总第 102 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天携手中国移动集团落地信息系统定级备案和安全整改加固工作

安天中标中国移动通信有限公司政企客户分公司信息系统定级备案项目，安全服务能力再一次被中国移动认可。

随着《网络安全法》的正式执行，明确要求关键基础设施运营者对其运营的网络具有安全保障责任和义务。按照中国移动集团公司对业务系统安全专项整治行动工作方案的整体工作部署情况，要求各单位对本单位所运行的所有正式上线网络和系统按照工信部通信网络定级备案实施细则进一步落实定级备案、符合性评测和风险评估等工作要求，确保网络单元全覆盖，定级备案及时、准确。

针对本项目，安天从信息服务业务系统的业务及应用安全、网络安全、设备及软件系统安全、管理安全和特定业务相关要求等方面对 20 个需定级备案的系统进行安全符合性测评，同时为提升移动政企分公司整体网络安全，为政企分公司提供包括安全监测、渗透测试、代码审计、安全加固、安全培训等服务，使信息服务业务系统在满足符合性测评的同时，又能做到实时发现安全漏洞，以及时应对安全威胁。

安天拥有大量安全服务项目经验，技术和服务具有以下两方面优势：

1. 技术优势

威胁风险分析：基于多年的技术积累，安天具有对高级持续性攻击事件和恶意代码的监测发现、跟踪和分析处置能力，具有对威胁的优先感知能力。

取证追溯：安天能够通过威胁情报的深度分析和追踪溯源，针对威胁迅速定位攻击源和安全取证。

2. 服务优势

针对项目目标和内容，通过现状分析和专业的评估工具，充分利用技术优势，制定切实可行的整改加固方案，包含定级报告、备案信息、符合性评测报告、整改报告、复测报告等全面完备的输出成果，实施可行性强。

助力湖南 共建网安

——安天协办湖南省互联网协会网络安全沙龙研讨活动

9 月 1 日，湖南省互联网协会网络安全专业委员会（简称“网安专委会”）成立大会暨首届湖南省互联网协会网络安全沙龙研讨活动成功举办。本次会议由湖南省互联网协会和湖南省互联网应急中心主办，安天作为会员单位出席了网安专委会成立大会，并作为协办单位参与了网络安全沙龙研讨活动。

本次网络安全沙龙研讨活动汇集了湖南省主要的运营商企业及网络安全企业的专家和领导，共同探讨“摸清家底，感知态势，携手保障网络空间安全”这一会议主题。在会上，来自安天的代表进行了题为《感知态势——传统防御体系如何应对威胁的演进》的演讲。他表示，安天通过端点有效防护、流量可靠采集、威胁深度分析，叠加自身领先的威胁情报平台，以保障态势感知系统的有效落地。

随着电信业务的不断发展，其对网络安全的需求也不断提高。安天依靠 17 年的技术和经验积累，在安全监测分析、事件深度分析、威胁情报获取及提供、应急响应、重大安保等方面均具有一定的优势和特长，可为运营商企业提供优质、可靠的安全服务，保障其网络安全、稳定运行。

■ 僵尸网络 WireX：黑客利用数十万安卓设备发动 DDoS 攻击

黑客继去年利用大量不安全物联网设备发动 DDoS 攻击后开始转向另一种极其流行且安全的设备展开新一轮攻击，即运行 Google Android 系统的智能手机与平板设备。调查显示，攻击者利用官方应用商店传播的恶意程序创建 Android 僵尸网络发动 DDoS 攻击。据悉，被称为 WireX 的僵尸网络在其高峰时最高控制 100 多个国家逾 12 万的 IP 地址。然而，当前各企业很难抵御这种 IP 地址遍布全球的 DDoS 攻击。研究人员表示，他们已在 Google 官方应用商店中发现 300 余款应用软件与僵尸网络 WireX 有关，其中多数应用主要提供铃声、视频或存储管理器等服务。目前，Google 经证实后紧急下架部分应用以减少目标设备沦为 DDoS 攻击的动力来源。（来源：https://arstechnica.com/information-technology/2017/08/first-known-android-ddos-malware-infects-phones-in-100-countries/）

一周简讯

- 勒索软件 BitPaymer 攻击英国 NHS
- 印度尼西亚数千台 ATM 机器因卫星问题而离线
- Google 错误劫持 BGP 路由，导致日本断网
- 研究者称可入侵零售支付系统修改价格
- 新型勒索软件 Defray 瞄准教育医疗机构展开网络钓鱼攻击

安天 CERT 搜集整理，详情请见：

每周安全事件

类 型	内 容
中文标题	研究人员发现影响主流浏览器扩展系统的 2 个漏洞
英文标题	Unpatched Flaws Affect Chrome, Firefox, and Safari Browser Extension Systems
作者及单位	Catalin Cimpanu；BleepingComputer
内容概述	近日，研究人员发现影响到诸多主流浏览器扩展系统的 2 个漏洞，影响范围覆盖了 Firefox、Safari、Chrome、Opera 等。 攻击者利用这些漏洞，可以导致用户安装的插件和扩展暴露——这些信息可用于用户画像，用作广告之用，甚至揭露隐藏在 VPN 或 Tor 背后匿名用户的身份。其中一个漏洞影响到基于 Chromium 的浏览器，包括 Chrome、Opera、Yandex 等，如 Firefox、Edge、Vivaldi 等浏览器也用了 WebExtensions API，但研究人员没有测试。WebExtensions API 通过插件中 manifest.json 进行访问控制，避免已安装的插件暴露。另一个漏洞名为 URI 泄露，影响到 Safari 的扩展系统。Safari 的扩展不采用 manifest.json 来限制扩展文件访问，而针对每个浏览器会话生成一个随机 URL，用户使用浏览器时才可访问。
链接地址	https://www.bleepingcomputer.com/news/security/unpatched-flaws-affect-chrome-firefox-and-safari-browser-extension-systems/

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 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	较为活跃的样本	Trojan/Android.QQspy.v[prv,exp]	该应用伪装成 QQ 相关应用，诱导用户输入账号和密码并短信转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.Downloader.dg[fra，exp]	该应用伪装成红包助手插件，诱导用户点击下载恶意应用，造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.HiddenAds.bj[exp]	该应用运行后会隐藏图标，后台推送广告，造成用户资费消耗。（威胁等级中）
		Trojan/Android.oxti.y[exp]	该应用运行会隐藏图标，后台频繁访问色情网址，造成用户的手机流量损耗。（威胁等级中）
		Trojan/Android.SmsSend.lp[exp]	该应用无实际功能，程序运行会隐藏图标，私自发送指定短信，造成用户资费消耗。（威胁等级中）
		Trojan/Android.Fobus.b[prv，rog]	该应用伪装成游戏应用 Machinarium（机械迷城），包含广告插件，运行后强制用户通过设备管理器申请，同时存在拦截未接短信、获取用户位置信息等行为，建议卸载。（威胁等级高）
		Trojan/Android.Triada.af[exp]	该程序运行隐藏图标，私自下载恶意子包，造成资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.HiddenAds.bk[exp]	该应用为广告插件，运行后会删除自身图标，并推送广告，可能造成用户流量损失，建议卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Foxit PDF Reader 任意文件写漏洞 (CVE-2017-10952)	Foxit PDF Reader 是一款小型的 PDF 文档阅读器和打印程序。Foxit PDF Reader 在实现上存在任意文件写漏洞，能让攻击者在目标系统写入任意文件，攻击者可以利用该漏洞获取代码执行能力。此漏洞位于 saveAs 函数。（威胁等级中）
	较为活跃样本	Trojan[Backdoor]/Win32.FinFish	此威胁是一类可窃取用户信息并回传的木马家族。该家族样本运行后连接远程服务器，收集系统信息并回传，运行后会自删除。（威胁等级中）
		Trojan[Downloader]/Win32.Pfoenic	此威胁是木马类家族程序。该程序的样本执行后进行文件下载并静默安装，同时在任务栏和桌面上创建游戏『超霸传奇』的快捷方式。（威胁等级中）
		Trojan[Dropper]/Win32.VB	此威胁是一种使用 VB 编写的捆绑类木马程序。该家族的特点是使用 VB 语言编写。该家族通过与正常软件捆绑在一起，或是由捆绑生成器生成捆绑文件等方式进行传播。（威胁等级中）
		Trojan/Win32.Bublik	此威胁是一种以窃取用户敏感信息为目的的木马类程序。该家族样本运行后，会安装恶意浏览器工具栏和扩展工具，引起搜索结果重定向等问题。该家族通过电子邮件或捆绑安装等方式进行传播。（威胁等级中）

网络安全：一场不对称的战争

Hal Lonas / 文　安天公益翻译小组 / 译

要想领先于攻击者，安全团队需要像犯罪分子一样思考、利用人工智能 (AI) 的能力发现恶意威胁，并停止担心机器学习会取代我们的工作。

在网络安全行业，我们都听过一句古老的格言：“防御者必须时刻警惕，而攻击者只需成功利用一个漏洞就行了。”

虽然令人生畏，但这正是网络安全行业每天都要面对的现实。我们面临着一场不对称的战争，不幸的是，我们的对手是一大批拥有各种武器的网络犯罪分子。

像其他战场一样，网络空间的不对称战争可以描述为：一方只需要适度投资来实现收益，而另一方则必须投入大量资金来维持足够的防御。在网络安全行业，恶意软件和勒索软件的作者和推广者是前者，而安全行业和潜在受害者是后者。这种投入时间和资源的不平衡导致这场战争是不对称的。

我们以 WannaCry 勒索软件攻击为例。这是一个简单的恶意软件，令人惊讶的是，它通过窃取的技术进行传播，感染了 40 多万台机器，攻击者几乎是毫不费力地实现了这一切。

网络犯罪分子富有创意，有能力测试新的攻击。同时，安全团队将资源投入到多层安全防御上，如网络分段和网络钓鱼培训。

这就出现了一个可怕的想法：当网络犯罪分子集中精力利用 AI 时会发生什么？

一旦攻击者掌握了 AI 技术，就会大规模渗透网络、窃取数据、传播能够导致设备瘫痪的计算机病毒。这可能会导致大规模军备竞赛，后果无法估量。足够聪明的 AI 能够清除电子邮件或网站被感染的迹象，这实在太可怕了。

虽然多态恶意软件 (到达新机器后发生变形) 有一些机器能力，但是这种恶意软件并非每日演变的。勒索软件几年前就出现了，到现在也没发生太大变化。我们经常看到受害者一次又一次地遭受同种类型的攻击。网络犯罪分子仍然可以用靠谱的工具制造混乱。

虽然我们无法预测网络犯罪分子下一步会做什么，但是一些人已经开始利用 AI 和机器学习来保护自己了。机器学习并非银子弹，但是它正在快速成为领先于犯罪分子，或至少能快速检测最新攻击类型的重要、必不可少的工具。它可以通过持续观察网络来提高安全性，并利用威胁研究团队的能力来创建一个整体大于各部分之和的解决方案。它设置一个基准，以帮助检测异常行为。但是想领先于攻击者，安全行业需要采取以下三个措施。

首先，安全人员要像网络犯罪分子一样思考。他们的主要动机很简单——赚钱。他们不断思考怎样用最小的行动产生最大的收益，因此他们非常喜欢网络钓鱼活动。他们可以轻松地发送数百万封电子邮件，将受害者重定向到伪造的网站并获得巨大的收益。网络犯罪分子可能会调整他们的方法，例如，伪装为技术公司而非金融机构，但是这些机制保持不变。第二，我们需要集成了 AI 技术的安全产品，利用 AI 固有的优势来发现恶意威胁。这些解决方案必须包含来自最佳威胁研究人员的情报和分析数据并发现进入企业的威胁的模型，这些解决方案可以是通用或特定的。最后，我们不用担心机器学习会取代我们的工作。真正的威胁来自于不利用机器学习，这种回避迫使最好的研究员疲于应付繁琐的工作，无法创造性地思考问题、预测新的攻击形式并进行防御。机器学习能够为研究员提供帮助，使他们腾出手来处理更重要的问题。

原文名称	Cybersecurity: An Asymmetrical Game of War
作者简介	Hal Lonas，Webroot 首席技术官。
原文信息	2017 年 8 月 28 日发布于 Dark Reading 原文地址 https://www.darkreading.com/vulnerabilities---threats/cybersecurity-an-asymmetrical-game-of-war/a/d-id/1329728?
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《加强壳的 MBR 勒索软件分析报告》

近日，安天 CERT(安全研究与应急处理中心) 的分析人员在梳理网络安全事件时注意到一种可以通过修改 MBR 在开机时锁定计算机以勒索用户的恶意代码。该勒索软件使用了多种反调试手段以阻止分析人员分析，而且它使用了 VMP 加壳软件进行保护，因此脱壳成为了分析人员极为困难的一环。

该恶意代码拥有“.txt.exe”的双后缀名，如果普通用户没有关闭文件夹选项中的“隐藏已知文件类型的扩展名”则很容易上当受骗而双击执行，样本在 XP 下直接运行后 MBR 被修改，重启计算机后会在屏幕上显示攻击者 QQ 号码及一个恶意代码随机产生的 5 位序列号，通过一个算法可以计算出相应的 6 位密码。而在 Vista 及以上操作系统版本执行的话需要 UAC 权限，因此分析人员猜测，该勒索软件还存在着前导文件用以绕过 UAC。

由于该勒索软件使用了 VMP 壳，因此需要带壳进行分析，首先需要在调试器中定位到函数 VirualProtectEx，在其地址处下断点，忽略异常处理并运行，直到堆栈中显示“PAGE_READONLY”字样，此时停止运行并取消断点。然后在 data 段处下断点，忽略异常处理并运行，在 0x401000 处可以发现密码算法及写入 MBR 的相应字符串。在随机生成 6 位序列号后，恶意代码将该序列号化作浮点数后与 6 相乘，结果与“123456”相加，最后得出密码。

近几年的勒索软件发展迅速，恶意代码也渐渐从拼技术转化为盈利第一，但计算机系统安全也不断提升，因此拥有加强壳、强混淆、反调试，绕过 UAC，绕过安全软件等一系列手段的恶意代码也不断出现。对于此类样本，安全研究人员也需要不断提升自身技术，在第一时间提升安全产品的能力。

此类勒索软件多以游戏客户端、外挂捆绑，在后台静默安装，故安天分析人员提醒用户，不要在不知名的网站下载文件，保持杀毒工具的实时监控，并定期做好重要数据备份工作。

目前该加 VPM 壳的 MBR 勒索软件样本已由安天追影威胁鉴定器检出。

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：

文件被页面手工提交发现，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：查找指定内核模块、创建特定窗体、查找特定窗体。

根据动态行为 (Windows7) 得出该文件具有以下行为：查找指定内核模块、创建特定窗体。

文件名	mbr 锁机样本
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.37 MB
MD5	BF287FFF2F626175BD54C65D2CBF7174
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.TSGeneric
判定依据	静态分析

◆ 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、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
查找指定内核模块	★	创建特定窗体	★
查找特定窗体	★		

◆ 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

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
查找指定内核模块	★	创建特定窗体	★

报告地址：https://antiy.pta.center/_lk/details.html?hash=BF287FFF2F626175BD54C65D2CBF7174