安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 03 月 26 日 (总第 128 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布 2017 年安天移动安全年报

3 月 21 日，安天移动安全团队在官方博客上发布《2017 年安天移动安全年报——起承转合间的方兴未艾与暗流涌动》（以下简称年报），对 2017 年的移动安全与威胁状况进行总结，对威胁演进趋势做出预测。

自 2005 年起，安天便在每年年初公布年报，并分为“基础威胁年报”和“移动安全年报”发布。

安天移动安全团队 2017 年年报以“起承转合间的方兴未艾与暗流涌动”为主题，对应“起、承、转、合”，首先基于数据对移动安全的总体形势进行分析，紧接着梳理出 2017 年移动安全的焦点问题，之后对 2018 年的移动安全态势进行展望与预测，最后进行反思与总结。安天移动安全团队希望通过这份年报，不仅能够与移动安全行业从业者、移动互联网相关企业及相关专业技术人士分享过去一年移动安全的总体形势，传达团队过去一年的所见、所为及所思，更能够为任何需要或试图了解移动安全现状的用户提供一份令人信服的中立意见。

在移动产业发展的巨大变革过程中，信息安全的“攻”与“守”之道往往也是共生并进的。2017 年，移动安全和威胁对抗不断迈入新的阶段，而所谓“方兴未艾”与“暗流涌动”，也能够很好地体现于此。

（1）针对移动网络，除持续对普通用户信息安全造成影响的传统电信诈骗之外，更衍生出了基于仿冒应用、短信拦截马、短信蠕虫等针对智能手机用户的精准电信诈骗，且近年来俨然成为一种常态化威胁，新增的受害用户数量不可小觑；

（2）近一两年，随着 PC 端出现诸如 WannaCrypt0r 等目标明确、影响广泛的勒索软件，移动终端也出现了影响较广的加密勒索软件、隐私窃取及控制软件等，不仅对用户数据安全造成致命威胁，给用户带来各种形式损失，还可能使用户终端设备沦为僵尸网络节点，遭到攻击者的全盘控制，影响极为严重；

（3）部分商业利益或政治因素驱动的移动终端恶意软件（往往以潜伏的 APT 或类 APT 形式被发现）出现更为频繁，这些恶意软件往往具备攻击的精确性、战术性及较完善的攻击链逻辑，在考验基于“病毒特征库”启发检出机制及各方情报收集、分析及预警能力的传统威胁对抗模式的同时，可能导致较为重要的商业秘密或较高密级的国家基础设施信息持续性泄漏，且往往在发现时就已造成难以衡量的恶劣影响。

用户与互联网服务所共存的每一天正犹如“起承转合”，而其间既有移动安全领域新技术的“方兴未艾”，亦有对立面上攻击技术、黑色产业链等各方面的“暗流涌动”。纵观全局，移动安全在 2018 年的整体态势仍然不容乐观。

本年度的安天“基础威胁年报”承载了更多深入的思考，历经多个版本的修改，将于稍后发布。“移动威胁年报”完整报告可登陆安天移动安全官方博客（http://blog.avlsec.com/2018/03/5150/2017-annual-report/）或扫描下方二维码查看。

Windows 远程协助中存在严重漏洞 可导致敏感文件被盗

Windows 快速助手是一款内置工具，允许受用户信任的人接管其电脑（或者允许用户远程控制他人电脑）使得从世界任何地方都能远程帮助用户修复问题。快速助手功能依靠远程桌面协议（RDP）来建立共享权限的双方的安全连接。

趋势科技公司 ZDI 团队的研究员 Nabeel Ahmed 发现并向微软报告了一个存在于 Windows 远程协助（快速助手）中的漏洞（CVE-2018-0878），该漏洞可导致攻击者获取进一步攻陷受害者系统的信息。该漏洞影响微软 Windows Server 2016、Windows Server 2012 和 R2、Windows Server 2008 和 R2 SP1、Windows 10（32 位和 64 位）、Windows 8.1（32 位和 64 位）和 RT 8.1 以及 Windows 7（32 位和 64 位），并且能导致远程攻击者窃取目标设备的敏感文件，目前微软已经修复该漏洞。

微软解释称，“被盗信息可作为 HTTP 请求的一部分向攻击者提交。攻击者都无法强制用户查看受攻击者控制的内容，而是必须说服用户采取行动。”

Ahmed 警告称，“XXE 漏洞可针对那些真的以为自己在帮助别人解决 IT 问题的个人发动大规模的钓鱼攻击。提供帮助的人完全没有意识到这个 .msrcincident 邀请文件能够导致自己的敏感信息被盗。”

除了修复微软于本月推出的其它严重漏洞问题外，强烈建议 Windows 用户尽快安装 Windows 快速助手的最新更新。

（文章来源：https://thehackernews.com/2018/03/window-remote-assistance.html）

每周安全事件

类 型	内 容
中文标题	AMD 证实处理器漏洞报告完全属实 将在数周内推出补丁
英文标题	AMD Confirms RyzenFall, MasterKey, Fallout, and Chimera Vulnerabilities
作者及单位	Catalin Cimpanu
内容概述	AMD 公司官方证实了 3 月 12 日由以色列 CTS 实验室披露的 RyzenFall、MasterKey、Fallout 和 Chimera 漏洞完全属实，且表示将在未来几周推出补丁。 具体来讲，MasterKey、Fallout 和 RyzenFall 漏洞影响 AMD 平台安全处理器（PSP）。它是一款安全的层叠式芯片处理器，类似于英特尔公司的管理引擎（ME），和硬件层面的其它 AMD 处理器分离，通常处理的是安全数据如密码、加密密钥等。Chimera 漏洞影响的是用于管理处理器、内存和外围设备进行通信的 AMD 芯片集（主板组件），该漏洞可导致攻击者执行代码并将错误信息中继到其它组件。 此前由于 CTS 实验室披露漏洞的流程并不标准，因此很多安全专家认为 CTS 发布的报告旨在操纵 AMD 股票，因此认为报告中含有错误或具有误导性的问题。
链接地址	https://www.bleepingcomputer.com/news/hardware/amd-confirms-ryzenfall-masterkey-fallout-and-chimera-vulnerabilities/

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	新出现的样本家族	Trojan/Android.crtici.a[prv,rmt,spy] 2018-03-19	该应用程序伪装系统应用，接收远程指令上传用户通话记录、联系人、短信、照片等隐私信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Pal4u.a[prv,spy] 2018-03-20	该应用程序伪装成 GooglePlay，运行隐藏图标，请求激活设备管理器，后台窃取用户短信、联系人、通话记录、位置等隐私信息并联网上传，造成用户隐私泄露，建议卸载。（威胁等级高）
		RiskWare/Android.NsAds.a[exp] 2018-03-20	该应用程序运行私自推送通知栏广告，创建桌面快捷方式，诱导用户点击，会造成用户流量资费损耗，请谨慎使用。（威胁等级中）
		G-Ware/Android.FakeJioUpdate.a[rog] 2018-03-22	该应用程序伪装程序更新，无实际功能，诱导用户分享指定链接、可能用于刷单行为，还会推送广告，建议卸载。（威胁等级低）
	较为活跃的样本	Trojan/Android.SmsSend.ok[exp]	该应用程序包含恶意代码模块，程序运行会私自发送短信，造成用户资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.FakeGoogleSys.f[exp,prv,rog]	该应用程序伪装 Google 服务，安装无图标，联网上传用户固件信息、安装列表信息，下载指定文件，造成用户流量资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.nbank.e[prv]	该应用程序运行后监听用户通话，替换拨打号码以及监听用户短信，上传用户设备信息、通话信息以及短信信息，造成用户资费消耗和隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.FakeSystem.u[exp,rog]	该应用程序伪装系统应用，运行请求激活设备管理器，隐藏图标，可能后台推送 Google 的广告，造成用户资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.FakeGSSpy.b[prv,rmt,spy]	该应用程序是一款间谍软件，运行后隐藏图标，后台私自加载漏洞利用程序进行 root，接收远程控制指令，窃取用户短信、联系人、通话记录、地理位置、浏览器记录、QQ 和微信社交软件信息记录，并将隐私信息上传至服务器，私自录音、拍照、拨打电话、下载未知 apk。造成用户隐私泄露和危害手机安全，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	微软 Office 内存损坏漏洞导致远程命令执行 CVE-2017-11882	微软在例行系统补丁发布中，修复了一个 Office 远程代码执行的严重漏洞，编号 CVE-2017-11882。该漏洞类型为缓冲区溢出，位于 EQNEDT32.EXE 组件。受害用户打开恶意的 Office 文档时，无需交互，就可能执行恶意代码。（威胁等级高）
	较为活跃样本	Trojan[Spy]/Win32.Montp	此威胁是一种木马类间谍程序。该家族能够通过记录键盘击键、截屏、检索运行的应用程序和列表来监控用户活动。该家族会将获取的机密信息发送到远程服务器或指定的电子邮件地址。（威胁等级高）
		Trojan[Downloader]/Win32.Donn	此威胁是一种可以下载并安装恶意代码的木马家族。该家族样本运行后，会在未授权的情况下下载安装其他恶意程序，而且会修改注册表。（威胁等级中）
		Trojan[DDoS]/Win32.Fram	此威胁是一种可以进行DDoS攻击的木马类程序。通常为DDoS生成器生成的木马类程序，有一个或多个攻击地址，也可能是等待服务器发送攻击的 IP 或域名地址。（威胁等级中）

人工智能的容器化

Hamid Karimi / 文　安天技术公益翻译组 / 译

人工智能 (AI) 可以自动执行重复性任务，减轻经常困扰决策者的单调工作。但它仍然不能替代最佳安全实践。

人工智能有望转变静态和动态安全措施，从而大幅降低企业风险。将安全策略转化为操作代码是当今敏捷 DevOps 面临的一项艰巨挑战。面对不断演变的攻击工具，构建预防性防御需要大量的上下文数据，如历史数据、预测分析和高级建模。即使这样的工作已经完成，SecOps 仍然需要基于现场威胁情报的反应式、近乎实时的响应来增强它。（译者注：DevOps 是 Development 和 Operations 的组合，是一组过程、方法与系统的统称，用于促进开发 [应用程序 / 软件工程]、技术运营和质量保障 [QA] 部门之间的沟通、协作与整合。SecOps 从 DevOps 的概念延伸和演变而来，其核心理念为安全是整个 IT 团队 [包括开发、运维及安全团队] 每个人的责任，需要贯穿从开发到运营整个业务生命周期的每一个环节。）

虽然目前人工智能更多的是炒作，但是由大数据集的元分析 (使用相关性和统计数据) 所驱动的机器智能 (也称为预测性机器学习) 能够提供切实可行的措施以减少人为干预决策的需要。

这种应用程序的典型副产品是创建行为模式，可以在策略存储中共享基准或策略修改。这种影响超越了 SecOps，可以为更广泛的 DevOps 集成提供动力。应用人工智能可能会破坏企业过程，有时必须在拆除分析和基于规则的模型的背景下进行权衡。

人工智能的应用必须建立在共同安全责任的原则之上。基于这种模式，安全不再是专业人士的事儿，它影响着企业运营和业务基础，技术人员和企业领导者 (首席安全官 [CSO]，

首席技术官 [CTO] 和首席信息官 [CIO]) 将接受保护数据和公司资产的连带责任。一些严厉的法规，如欧盟《通用数据保护条例》规定的处罚条款，起到了一种强制性作用。

关注特定领域

企业与其将人工智能视为一种万灵药，不如将其应用在能够提高效力的特定领域。有一些特定用例为 AI 的部署和演进提供了更加肥沃的土壤：云计算、微分段和容器就是很好的例子。即使在这些类别中，共享所有者也必须识别技术的复杂性来平衡部署 AI 的愿景和风险，同时避免完全忽视它的代价。（译者注：microsegmentation，微分段，是一种减少 LAN 网络段上站的数目以改进性能的技术。）

正如最近公共云服务近乎崩溃一样，数据流的东西向和南北向架构有其危险性。历来对容量和扩展的重视使我们获得了巧妙的计算模型，其中包含许多抽象层。在抽象的情况下，我们基本上删除了经典的堆栈模型，因此为其增加安全性是一个严峻的挑战。

此外，关注重点已经从基础设施的细节转移到应用程序隔离开发，这催生了这样的期望：容器和 web 微服务中的地理应用也可以独立保护，同时维护自动化和可扩展的中间件。超大规模计算依赖于分布式区域的毫秒可用性，它不仅依赖基础设施，而且越来越依赖微分段和基于容器的应用服务——这种现象的长期成功取决于人工智能。

在 90 年代，我们认为虚拟局域网 (VLAN) 能够提供保护隔离，并且能够根据角色和责任提供高效的计算空间。这一愿景远未达到预期。微分段和容器是 VLAN 的后计算演进。他们带来了其他好处，例如减轻防火墙规则的压力；不再需要追踪指数级增长的规则 (这些规则在导致误报和漏报的情况下几乎没有可见性)。虽然总体攻击面和附带损害减少了，但是出现持续性入侵活动的可能性并未降低。AI 工具可以专注更小的数据子集并创建更好的映射，而不会影响用户的生产力或破坏分段计算的叠加概念。

这可以说是一举多得：企业可以查看所有可用的元数据，将其提供给 AI，然后将 AI 的输出结果发送给预测性分析引擎，并为正在进行的或即将开始的潜在攻击建模。我们距离实施另一个可能的步骤——机器对机器学习和安全措施 (机器可以观察和吸收相关数据并完善安全态势以保护自己免受预测到的攻击) ——还有几年的时间。

人工智能还可以在自动驾驶等其他新兴领域提供实质性的价值。汽车越来越像具有直接云命令和控制的计算机器。从基于模糊测试的离线建模到传感器数据的实时分析，我们可以依靠人工智能降低风险和责任。

人工智能不是万能的；然而，它可以自动执行重复性任务并减轻经常困扰安全决策者的单调工作。像其他安全创新一样，它将经历其演进周期并最终找到其合适的位置。与此同时，仍然没有什么能够替代最佳安全实践。

原文名称	The Containerization of Artificial Intelligence
作者简介	Hamid Karimi。Hamid Karimi 是 Beyond Security 业务发展副总裁。
原文信息	2018 年 3 月 16 日发布于 Dark Reading 原文地址 https://www.darkreading.com/analytics/the-containerization-of-artificial-intelligence/a/d-id/1331208
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《勒索锁机木马 MBRLock 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发现一例 Windows 平台的具有锁机功能的木马样本。该木马会绕过 360 监控，结束 360 实时监控程序，替换主引导扇区数据，并使系统重启。系统重启后，会显示勒索信息“yao mi ma gei 30 yuan jia qq2055965068”等待用户输入密码。

该样本启动后，首先安装各种钩子，拦截 Windows 消息，用户双击运行软件后会跳转到恶意代码的位置执行恶意代码。该样本根据不同的控制指令执行不同的操作。样本在编写时就已经在函数调用时确定了控制指令，在实际运行时不需要人为进行指令控制。其中指令 0x7d8 执行勒索软件的关键代码，指令 0.x7e8 分配内存用于存储勒索信息。该样本会将 360 相关的注册表值设置为 0，从而绕过 360 监控。该样本利用控制指令分配内存，将勒索语句和密码 ssssss 存储到内存中。该样本会将原主引导扇区的数据存储到第三扇区，将勒索信息写入主引导扇区，系统重启后便会读取主引导扇区的数据，然后显示勒索语句，等待用户输入正确的密码从而进入系统。该样本将自身复制到 C:\Program Files\System.dll，对样本文件进行多次读取、写入，删除样本文件的原数据。在 C:\Program Files\ 目录下创建 360.dll 文件，360.dll 文件是白文件，用来迷惑用户，掩饰 System.dll。最后该样本会调用 taskill.exe 结束 360 实时监控程序 360tray.exe，然后重启系统。

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恶意代码的检出。

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、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、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据动态行为鉴定器将文件判定为木马程序。

概要信息

文件名	dfc56a704b5e031f3b0d2d0ea1d06f9157758ad950483b44ac4b77d33293cb38
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	844 KB
MD5	7E179D064B2D20B4EA5E6D492ABF8F2B
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	动态行为

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
修改硬盘引导扇区，疑似感染引导区病毒	★★★★

常见行为

查找指定内核模块	★
创建特定窗体	★
打开自身进程文件	★
读取自身文件	★★
释放 PE 文件	★★
复制自身文件	★★
增加 run 自启动项	★
获取计算机名称	★
关机	★
查找特定窗体	★
自启动	★
疑似查找杀软进程	★★

文件扫描

文件名	文件 MD5
target.exe	7e179d064b2d20b4ea5e6d492abf8f2b
target.exe.dmp	bf73405180391e401b0f697830316125
360.dll	14b07f297b5b881d877c5e313355dd01