安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 01 月 08 日 (总第 119 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布《处理器 A 级漏洞 Meltdown（熔毁）和 Spectre（幽灵）分析报告》

安天安全研究与应急处理中心在 2018 年 1 月 4 日，针对刚刚披露出的英特尔等处理器芯片存在非常严重的安全漏洞，发布了 A 级漏洞风险通告，并发出提醒，该漏洞演化为针对云和信息基础设施的 A 级网络安全灾难。相关漏洞利用了芯片硬件层面执行加速机制的实现缺陷实现侧信道攻击，可以间接通过 CPU 缓存读取系统内存数据。漏洞 Meltdown(熔毁)因“融化”了硬件的安全边界而得名，漏洞 Spectre(幽灵) 因其手段的隐蔽性而得名。

安天在第一时间向管理部门提交威胁通报，并根据管理部门的要求进行深度的分析验证和应对工作。于 1 月 4 日发出了公开漏洞通告，并于 1 月 5 日上午 9 时更新了《处理器 A 级漏洞 Meltdown（熔毁）和 Spectre（幽灵）分析报告》。

鉴于相关漏洞机理较为复杂，涉及到体系结构、操作系统，特别是 CPU 的核心运行机制，为使主管部门和用户深入了解漏洞细节，做好防护，安天组织内部公益翻译和技术团队对披露这两个漏洞的长篇关键论文文献《Meltdown》和《Spectre Attacks: Exploiting Speculative Execution*》进行了翻译，于 1 月 4 日发布了《Meltdown》译文的初稿，并于之后进行不断更新。

此次被披露的漏洞是一个足以动摇全球云计算基础设施根基的漏洞，其意味着任何虚拟机的租户或者入侵成功了一个虚拟机的攻击者，都可以通过相关攻击机制去获取完整的物理机的 CPU 缓存数据，而这种攻击对现有虚拟化节点的防御机制是无法感知的。同时由于该漏洞的机理，导致其存在各种操作系统平台的攻击方式，因此尽管这一漏洞本身只能读取数据，不能修改数据，但由于其获取的数据中有可能包括口令、证书和其他关键数据，包括能够完整 Dump 内存镜像，因此该漏洞比一般性的虚拟机逃逸对云的危害更大。

尽管当前全球主要云服务商均在积极应对这一漏洞的影响，但鉴于这些云服务体系的庞大而复杂，以及大面积补丁本身所面临的复杂度和风险，漏洞利用 POC 已经发布并验证成功，因此这次漏洞修补已经成为一场时间赛跑。在此过程中，攻击者所获取到的数据，将会沉淀出对于关键数据和隐私泄露、登陆凭证被窃取导致连锁攻击等次生灾害。

鉴于大量政企机构和行业进行了私有云的建设，而私有云的安全防御和补丁升级可能更弱。因此后续需要深度注意利用该漏洞在私有云中进行的攻击。同时，该漏洞对于攻击桌面节点同样有巨大的攻击力，其大大提升了以浏览器等为攻击入口的攻击成功率。包括使传统的使用非超级用户来降低网络风险的安全策略失效。

当前已经公布的漏洞 POC 对 Intel 系列 CPU 有效，但鉴于相关执行加速机制是现代处理器的通用技术，因此所有处理器均需要分析相关风险。

安天紧急升级了 AVL SDK 威胁检测引擎，以支撑安天自身产品及使用安天引擎的用户对相关 POC 的检测能力。同时，安天智甲终端防御系统升级了主防机制，可对相关 POC 进行拦截。无论是在 Windows 系统还是在国产中标麒麟系统中，安天智甲均可对英特尔 Spectre (幽灵) 的 POC 进行检测。

图 1 安天智甲针对利用处理器芯片漏洞在 Windows 平台系统可有效防御

图 2 安天智甲针对利用处理器芯片漏洞在 Linux/ 国产操作系统均可有效防御

详细报告　公益翻译

- 1、CNVD 发布 CPU 处理器内核漏洞的安全公告
- 2、安天发布处理器漏洞熔毁和幽灵应急通报
- 3、微软发布 CPU 处理器内核漏洞的修复更新
- 4、Linux 内核将对 AMD 处理器禁用页表隔离修正
- 5、研究者披露 macOS 0day 本地提权漏洞
- 6、物联网渗透团队发布 2017 IoT 常见漏洞
- 7、俄罗斯黑客承认为情报部门开发 WannaCry

每周安全事件

类 型	内 容
中文标题	匿名意大利黑客入侵了超速摄像头数据库并接管了科雷吉奥的警察系统
英文标题	Anonymous Italia hacked speed camera database and took over the police systems in Correggio
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	匿名黑客入侵了意大利的一个超速摄像头数据库，这个行为主义者黑客控制了意大利科雷吉奥的一个当地警察电脑系统，并删除了包含超速摄像头的整个档案。根据 Gazzetta di Reggio 的说法，黑客还发布了内部电子邮件和文件。 匿名黑客通过科雷焦市警方的电子邮件帐户发送了一条消息。该消息宣布了黑客得到 Verbatel 公司开发的 Concilia 数据库和系统，还包括它们的下载链接和密码。 该消息包含黑客的屏幕截图，其中一个显示的一个 Windows 命令行可能与被黑客入侵的科雷焦市政警察有关。 有两名驾车人士抱怨说，他们收到了科雷吉奥的超速摄像头的罚单，尽管他们从未经过该地区，警方仍在调查此案。
链接地址	http://securityaffairs.co/wordpress/67378/hacktivism/anonymous-speed-camera-database.html

每周值得关注的恶意代码信息

经安天【CERT】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

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.JsLocker.a[rog,lck] 2018-01-01	该应用程序伪装色情应用，程序运行会判断是否有模拟器运行，请求激活设备管理器，隐藏图标，后台联网获取 js 脚本，置顶界面、显示用户通讯录、照片、位置信息等隐私，勒索用户付费解锁，影响用户设备正常使用，建议卸载。（威胁等级中）
		Trojan/Android.hyxSpy.a[prv,rmt,spy] 2018-01-01	该应用程序伪装系统应用，程序运行会隐藏图标，通过 socket 连接到远程服务器，获取指令并根据指令执行窃取用户短信、通话记录、通讯录、位置信息、拍照、录像、录音等隐私信息，造成用户隐私泄露，建议卸载。（威胁等级高）
		G-Ware/Android.FakeSpeedup.a[exp,rog] 2018-01-01	该应用程序为虚假应用，动态加载恶意子包，连接网络关闭 wifi，访问指定网址，同时加载 js 脚本可能用于刷单刷流量，造成用户流量资费损耗，请卸载。（威胁等级中）
		Trojan/Android.hungrysoftKR.a[prv,spy] 2018-01-03	该应用程序隐藏图标，实时上传用户的收发短信、通话记录、通话录音、地理位置，实时上传用户操作的几款常用社交软件的行为，造成用户隐私泄露，建议卸载。（威胁等级中）
		RiskWare/Android.Hcatam.a[exp,rmt] 2018-01-03	该应用程序伪装 Telegram，包含风险代码，运行后接收远程控制命令，会将用户添加到推广的群组或者聊天频道中，影响用户手机正常使用，存在一定的风险，建议卸载。（威胁等级中）
		Tool/Android.Haven.a[prv] 2018-01-04	该应用程序运行后会调用摄像头、麦克风等手机传感器，监听用户通话和环境信息，并将记录发送到主机或网站上。请谨慎使用，若非本人安装，请卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.Terbod.c[prv]	该应用程序伪装系统应用，诱导激活设备，后台利用 Telegram 提供的通讯接口窃取用户收件箱短信、联系人信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.migusms.b[prv,pay]	该应用程序安装无图标，运行后上传手机固件、电话号码等信息获取付费短信相关内容，后台拦截指定短信并私自回复和上传，造成用户隐私泄露和资费损耗，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	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[Downloader]/Win32.Cabby	此威胁来自一种具有下载行为的木马类程序。该恶意代码通过钓鱼网站、未知链接、下载黑客发布的免费软件及垃圾邮件附件等形式进行传播。（威胁等级中）
		Trojan[DDoS]/Win32.Mavros	此威胁来自一种可以实行 DDoS 攻击的木马家族。该家族样本运行后连接远程控制服务器并向其发送上线包，接受攻击者控制，有一定威胁。（威胁等级中）
		Trojan[Downloader]/MSWord.Steamilik	此威胁来自一类可以下载恶意代码的木马家族。该家族样本为 Word 宏病毒，运行后连接网络下载恶意代码并运行。（威胁等级中）
		Trojan[Dropper]/Win32.VB	此威胁来自一种使用 VB 编写的捆绑类木马程序。该家族特点是使用 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）

2018 年将会影响企业的六项热门技术

Cynthia Harvey / 文　安天技术公益翻译组 / 译

新年伊始，很多技术专家会对未来 12 个月内可能发生的事情进行预测。由于某种原因，2018 年出现了比以往更多的预测。我们收到了许多 IT 专家对网络、存储和数据中心趋势的预测。

可以肯定的是，2018 年又将是 IT 基础设施快速发展的一年。本文将介绍基础设施专家应该关注的六个关键技术趋势。

人工智能和机器学习

德勤公司在其《2018 年技术、媒体和通信预测》报告中指出，“2018 年，大中型企业将加大对机器学习技术的使用力度，使用该技术的实施和试点项目数量将比 2017 年翻一番，到 2020 年又会再翻一番。”

基础设施专家需要部署和管理硬件来支持人工智能和机器学习的扩展使用，他们会发现机器学习工具可以帮助他们更好地完成工作。例如，许多最新的安全软件都集成了机器学习功能，一些日志分析工具使用机器学习技术来改善故障排除，甚至防止 IT 问题的发生。

软件定义的基础设施

像“软件定义的网络”（SDN）这样的软件定义技术已经出现了很多年，许多专家认为它们将会被更广泛地采用。根据 IDC 的数据，积极推进数字化转型的企业将在 2019 年年底之前将数据中心和边缘地区的一半以上的 IT 基础设施转移到软件定义的模式。

软件定义的广域网（WAN）将是特别热门的增长领域，许多专家预测今年它将迅速进军企业。IDC 预测，到 2020 年年中它将成为主流。

软件定义的网络也可能会以有趣的方式与机器学习交叉。网络供应商 Inocybe

Technologies 的首席研发官约翰·赞诺斯（John Zannos）表示：“云、5G 和物联网的融合要求实现智能（机器学习）和自动化网络（软件定义的网络）。这些软件智能网络是改善从消费者与语音和视觉网络产品的交互，到 B2B 服务的基础。”

自动化

随着越来越多的企业采用 DevOps，他们比以往任何时候都更加依赖自动化。

数据中心提供商 Interxion 的产品管理总监鲍勃·兰德斯特洛姆（Bob Landstrom）表示：“新兴技术迫使数据中心运营商采用新方法来提高效率、可扩展性和冗余度。但是，技术的改变不会很快发生。因此，到 2018 年，数据中心需要利用自动化来提高效率。”

对于基础设施专家来说，采用自动化意味着学习新的工具和流程。从好的方面看，自动化可以帮助他们减少每天的手动工作量，将节省的时间用于更有趣的和关键的任务。根据 IDC 的数据，到 2021 年，超过 25% 的基础设施服务将具有自主管理能力，以加快业务流程并减少人为错误的风险。

DevSecOps

许多 IT 运营专家已经习惯了 DevOps 方法，但是现在他们可能需要采用更加安全的 DevSecOps 方案了。

ShiftLeft 公司首席执行官兼创始人马尼士·古普塔（Manish Gupta）在一篇博客文章中写道：“2018 年将是 DevSecOps 被广泛采用的一年，因为安全团队越来越依赖于使用下一代安全工具在开发周期中自动插入安全性。在持续集成 / 持续交付（CI/CD）中创建安全性建立在‘每个人都要对安全负责’的理念之上。”

如果 2018 年继续出现重大数据泄露事件，这种新的思维方式将变得越来越重要。

区块链

作为加密货币基础的分布式账本技术，区块链已经被广泛讨论，即将腾飞。

“在 2018 年，业界将围绕成立监管机构这一共同目标进行组织，以推动区块链和加密货币的广泛采用。这是推动这两项支付创新成为主流的第一步。”Paysafe 公司首席数字官提姆·瑟曼（Tim Thurman）说。

Forrester 公司的看法则比较悲观，它在《2018 年预测》中表示：“在 2018 年，言论和热情将继续限制区块链收益，但 30% 的概念验证将加速那些能够考虑其运营影响的公司的区块链技术发展。”

无论新的区块链举措是否长期存在，基础设施专家都应该了解该技术并准备好支持新的应用。

增强现实

随着相机和智能手机变得越来越强大，专家预测增强现实（AR）将会成为日常生活的一部分。也有许多专家认为 AR 将进入工作场所。例如，基础设施专家可以阅读 AR 教程，这些教程可以帮助他们在其数据中心部署和维护硬件。

原文名称	6 Hot Tech Trends That Will Impact the Enterprise in 2018
作者简介	Cynthia Harvey，Cynthia Harvey 是 NetworkComputing 网站的贡献者。
原文信息	2018 年 1 月 2 日发布于 NetworkComputing 原文地址 https://https://www.networkcomputing.com/data-centers/6-hot-tech-trends-will-impact-enterprise-2018/755072649
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《窃密木马 KOBI 样本分析报告》

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注意到一款新出现的 RAT 后门木马。该后门通过钓鱼邮件传播，欺骗用户点击下载邮件附件并执行压缩包内的恶意可执行文件。中招的用户主机会向攻击者 C&C 上传计算机用户常用语种、计算机名称、CPU 架构系统版本号、OEM 标识、系统时间时区、磁盘组织与容量信息等特征。样本拥有 TLS 反调试功能，使用虚假时间戳，能够截取屏幕、窃取浏览器和邮箱登录凭证、窃取用户本地文件和应用程序操作信息，利用 .NET 应用程序 Regasm.exe 和 VB.NET 编译器 vbc.exe 白名单绕过技术，来逃避杀软监测。

首先样本创建互斥量，通过注册表查询系统输入法，获取用户语言语种、计算机名、系统版本号、磁盘组织与容量信息、计算机系统 CPU 架构、内存和 OEM 标识。接下来解密资源段“DVCLAL”，结果为 C&C 域名“bio4kobs.geekgalaxy.com”。然后调用 GetDevicesCaps 捕获当前屏幕，使用 .Net 框架附带注册工具 Regasm.exe 白名单绕过 AppLocker 限制，逃避杀软监测，记录用户本地文件和应用程序操作行为，日志保存于 %APPDATA% 目录下 GUID 目录 Logs 文件夹中。样本运行后会连接 C&C，进程 Regasm.exe 连接到新的 C&C 主机使用 SecureVPN 掩盖自身真实 IP，数据传输过程皆被加密。经安天研究人员分析，样本作者在 geekgalaxy.com 下注册了大量子域名，geekgalaxy 为某免费子域名 DNS 提供商，类似于国内的“花生壳”。分析发现这款后门传播时间至少开始于 2015 年。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，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病毒样本的检出。

病毒程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述病毒程序进行有效检测，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、动态行为（window8）鉴定器、动静态向量提取引擎鉴定器、动态行为（WindowsVista）鉴定器、动态行为（window7）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、动态行为（WindowsServer2008）鉴定器、安全云鉴定器、动态行为（WindowsServer2003）鉴定器等鉴定分析。

最终依据智能学习鉴定器将文件判定为病毒程序。

文件名	5b51e96a00ebf611c87ceedd7e4d29ce56883b8d5e520c48bcab89c444fc5f93
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.08 MB
MD5	B1F9751B1DDA5766E9CEC983081FF0C0
病毒类型	病毒程序
恶意判定 / 病毒名称	Virus[Tool]/Win32.Ceeinject.TC!bit
判定依据	智能学习

◆ 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

◆ 常见行为

行为描述	危险等级		
查找指定内核模块	★	string1	C:\WINDOWS\system32\uxtheme
		string1	C:\WINDOWS\system32\MSCTF
		string1	C:\WINDOWS\system32\msctfime
		string1	C:\WINDOWS\system32\ole32

◆ 运行环境

操作系统	内置软件
Windows Vista 6.0.6002 Build 6002	默认、IE7、office 2010、Adobe Reader X

◆ 运行环境

操作系统	内置软件
Windows 7 6.1.7600 Build 7600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 常见行为

行为描述	危险等级	附加信息	
查找指定内核模块	★	string1	C:\WINDOWS\system32\uxtheme
		keypath	C:\WINDOWS\system32\MSCTF
自启动	★	ValueNeme	C:\WINDOWS\system32\msctfime
		Data	C:\WINDOWS\system32\ole32

◆ 运行环境

操作系统	内置软件
Windows 8.1 6.3.9600 Build 9600	默认、IE11、office 2013、Acrobat XI