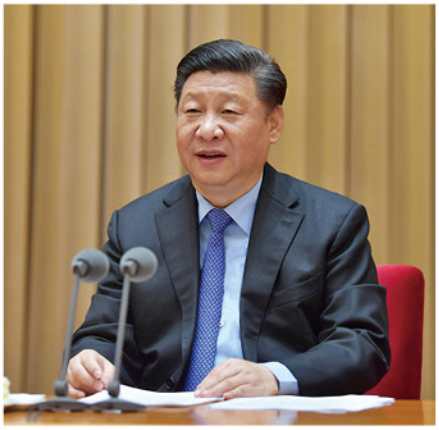
# 安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 04 月 23 日 ( 总第 132 期 ) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流


# 习近平总书记出席全国网络安全和信息化工作会议
# 安天第一时间组织学习总书记重要讲话精神



总书记讲话（图片来源：新华社）

全国网络安全和信息化工作会议 20 日至 21 日在北京召开。中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化委员会主任习近平出席会议并发表重要讲话。习近平总书记指出，党的十八大以来，党中央重视互联网、发展互联网、治理互联网，统筹协调涉及政治、经济、文化、社会、军事等领域信息化和网络安全重大问题，作出一系列重大决策、提出一系列重大举措，推动网信事业取得历史性成就。

安天集团是具有鲜明政治属性的市场主体，也是政治属性与经济属性的统一体，作为网络安全国家队，安天始终坚定正确的政治方向，主动对接党的领导，安天集团党委第一时间组织集团负责人、党员干部和核心技术骨干进行分组讨论学习，布置全员传达，大家对总书记讲话感到极大的鼓舞。

总书记讲话重申了**“没有网络安全就没有国家安全”**，强调了国家安全、社会安全和人民利益在网络空间的辩证统一。不仅强调**“加强关键信息基础设施网络安全防护”**的重要性，更进一步强化了**“落实关键信息基础设施防护职责”**的工作要求。

安天创始人、首席技术架构师肖新光在组织学习时指出，总书记在讲话中强调**“做到关口前移，防患于未然”**，对网络安全工作形成了方法要求和效果导向，将使网络安全防护的层次覆盖整个供应链场景和全生命周期，对解决网络安全防护的纵深性、有效性和态势感知的覆盖力与持续性至关重要。**“加强网络安全信息统筹机制、手段、平台建设”**、**“加强网络安全事件应急指挥能力建设”**等工作要求必将拉动网络安全领域的基础工程投入，以“超级工程”带动全面的能力提升。总书记讲话中明确提出了**“积极发展网络安全产业”**，将网络安全作为一个独立的产业层次予以强调，令安天人感到激动振奋！

安天学习讲话精神座谈会

安天研究院高级战略研究员张岩组织大家研讨了总书记对核心技术发展的工作要求。总书记再次强调**“核心技术是国之重器。要下定决心、保持恒心、找准重心”**，对研发自主先进核心技术，安天人的决心和恒心从未改变，但随着企业发展，重心同样需要阶段性校准。安天当前正在从威胁检测核心技术授权的上游企业，走向全面为我国高价值、高等级、高对抗场景提供动态综合防御体系的能力型安全企业。安天不能躺在持续研发十多年反病毒引擎技术的历史功劳簿上睡大觉，要厘清新使命要求所需的核心技术体系内涵，对接敌情想定，迅速全面强化体系化、实战化技术能力，打造具有系统性、前瞻性的技术新高地。

总书记讲话中强调**“网信军民融合是军民融合的重点领域和前沿领域”**。在总书记 4·19 讲话两周年之际，作为新型后备力量和新质作战能力建设的探索，结合军民融合发展战略和自身网络安全防护处置的专业特点和技术积累，在军地双方相关部门的指导和支持下，安天网络民兵分队宣告成立。

安天人一定要认真学习领会总书记重要讲话精神，把思想和行动统一到党中央关于网信工作的战略部署上来，以钉钉子精神把各项工作抓实抓到位。

## 一周简讯

- 黑客可利用 iTunes Wi-Fi 同步功能漏洞接管 iPhone
- 安全厂商揭示 DNS 劫持感染安卓手机恶意活动
- Google 电子邮件服务 Gmail 推出了邮件自毁功能
- Intel SPI Flash 曝出漏洞可删除 BIOS/UEFI 固件
- 思科 IOS 漏洞影响 Rockwell 多款工业交换机

# 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | 英特尔发布新技术，利用内置 GPU 扫描恶意程序 |
| 英文标题 | Intel to Allow Antivirus Engines to Use Integrated GPUs for Malware Scanning |
| 作者及单位 | Catalin Cimpanu |
| 内容概述 | 英特尔在 RSA 2018 安全会议上发布了几项新技术，其中一项功能是把病毒扫描嵌入了一些英特尔 CPU 的集成图形处理器上。<br>这项新技术的名称是英特尔加速内存扫描 (Intel Accelerated Memory Scanning)。英特尔表示，这项新功能让杀毒引擎减少 CPU 利用率，为其他应用程序腾出资源，同时，使用嵌入式 GPU 还会节省电池寿命。Windows Defender 的商业版本 Microsoft Windows Defender Advanced Threat Protection (ATP)，已经使用该功能。<br>除了加速内存扫描外，英特尔还推出了另外两项新技术。一是英特尔高级平台遥测技术，这是一种将平台遥测与机器学习相结合的工具，可加快威胁检测。思科表示思科 Tetration 平台将部署这项新技术，该平台为全球数据中心提供安全保护。二是 Intel Security Essentials，它是一系列可信根硬件安全功能的集合，部署在英特尔的 Core，Xeon 和 Atom 处理器系列中。 |
| 链接地址 | https://www.bleepingcomputer.com/news/security/intel-to-allow-antivirus-engines-to-use-integrated-gpus-for-malware-scanning/ |

# 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.wehefibi.a[prv,rmt,spy]<br>2018-04-16 | 该应用程序运行后隐藏图标，接收远程指令上传用户短信、联系人等信息，还会监听拦截指定短信并私自回复，造成用户隐私泄露，建议卸载。（威胁等级中） |
| | | Trojan/Android.SIMSpy.a[prv,exp,spy]<br>2018-04-18 | 该应用程序是间谍件，接收短信远程控制，上传联系人、通话记录、短信、应用安装列表等隐私，造成用户隐私泄露，建议卸载。（威胁等级高） |
| | | Trojan/Android.KevDroid.a[prv,rmt,spy]<br>2018-04-18 | 该应用程序运行后，在后台接收控制命令，窃取用户短信、联系人、通话记录、浏览器记录、地理位置等隐私信息，私自下载恶意 apk、拍照、摄像，并将用户隐私信息上传至服务器，其包含的恶意代码会利用用户手机漏洞进行提权，造成用户隐私泄露，危害用户手机安全，建议卸载。（威胁等级高） |
| | | Trojan/Android.Powersaving.a[exp,bkd]<br>2018-04-19 | 该应用程序包含风险代码，留有后门，会访问网络下载其他风险应用，可能给用户造成极大的安全隐患，建议卸载。（威胁等级高） |
| | | Trojan/Android.qpoe.a[prv,spy]<br>2018-04-20 | 该应用程运行后隐藏图标，窃取用户短信、联系人、照片等隐私信息，还会私自录音并上传，还可能会下载未知文件，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级中） |
| | | Trojan/Android.FakeJioCoin.a[prv]<br>2018-04-20 | 该应用程运伪装电子货币应用，无实际功能，运行后诱骗用户输入用户名、手机号码和电子邮件地址等个人信息，造成用户隐私泄露，建议卸载。（威胁等级中） |
| | 较为活跃的样本 | Trojan/Android.TelegramIR.b[prv,rmt,spy] | 该应用程序伪装成系统应用，运行后会隐藏图标，是其他间谍软件的功能子包，会保存录像和截屏文件，可能造成用户隐私泄露，建议卸载。（威胁等级中） |
| | | G-Ware/Android.FakePoloniex.b[rog] | 该应用程序伪装 Poloniex 应用，运行跳转指定网址，警惕该程序私自访问推广链接或钓鱼网址，造成用户资费损耗或隐私泄露，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 | WebLogic Server WLS 核心组件反序列化漏洞（CVE-2018-2628） | Oracle 发布了一个高危的 Weblogic 反序列化漏洞，漏洞编号为 CVE-2018-2628。攻击者可以在未授权的情况下，通过发送特殊构造的 T3 协议数据，获取目标服务器的权限，最终实现远程执行任意代码。（威胁等级高） |
| | | Trojan[DDoS]/Linux.Znaich | 此威胁是一可以发动分布式拒绝服务攻击的木马家族。该家族样本基于 Linux 系统，运行后向指定目标发起 DDoS 攻击。（威胁等级中） |
| | 较为活跃样本 | Trojan[Dropper]/Win32.Pincher | 此威胁是一种具有捆绑功能的木马类程序。该家族从用户系统窃取重要数据和信息，并把它发送给攻击者。该家族将恶意代码注入到被感染系统，并防止用户访问 Windows 的注册表文件。（威胁等级中） |
| | | Trojan[Ransom]/Win32.Cryptor | 此威胁是一种可以加密用户文件并勒索赎金的木马家族。该家族样本运行后遍历系统磁盘并加密文件，向用户勒索赎金以解密，有一定威胁。（威胁等级中） |
| | | Trojan/Win32.Carberp | 此威胁是一木马类程序。该家族专门用于盗取银行信息。运行后能够感染硬盘的主引导记录，对包括使用 EV-SSL 的 HTTPS 在内所有类型的网络流量进行控制，在被窃取的信息发送到金融网站之前就被传送到远程服务器上。（威胁等级高） |

# 2018 年的云迁移状态

Joe Masters Emison / 文　安天技术公益翻译组 / 译

**企业现在是时候停止找借口，并认识到为什么需要迁移到云端了。**

现在是 2018 年——为什么你的数据中心仍然有服务器？为什么不用云来做一切事情？为什么不为办公室所需的服务应用“软件即服务”（SaaS）方案，为什么不为所有的服务器和服务应用“基础架构即服务”（IaaS）方案？

对于许多企业来说，这些问题的答案如下：

- 太冒险！
- 太昂贵！

但这些并不是根本原因。大多数还未迁移到云端的企业未采取行动的原因是，企业的领导不理解迁移到云端的核心业务价值。而且，这通常是因为企业中没有人能够正确理解这种价值。

迁移到云的关键优势是为企业提供针对性、速度和灵活性。如果恰当地迁移到云，企业可以停止为不必要的功能提供人力或运行这些功能。

最佳措施是 SaaS，这其中的佼佼者是 Salesforce.com。这就是大多数销售主管选择 Salesforce（以及其他 SaaS 方案），而不再使用像 Act! 这样的安装软件的一个原因。它允许销售主管及其员工直接与一家在入职培训方面很专业、并为他们的核心工作提供支持的公司（Salesforce.com）合作。这远远优于让内部员工努力支持像 Act! 这样的软件（这些软件并不是他们编写的，他们并不太了解），以及处理安装、升级等问题。

如果恰当部署 IaaS 方案，企业可以执行相同类型的特定功能消除，比如硬件购买和安装（包括容量规划）、操作系统安装和持续硬

件维护等。IaaS 的进一步发展——例如容器和无服务器架构——允许企业进一步转向 IaaS 供应商，包括操作系统配置、软件修复和扩展应用程序。2014 年，一名前端开发人员（没有后端开发人员！没有操作人员！）可以在八个小时内构建一个支持数百万并发用户的应用程序。想象一下四年以后的现在能够实现什么！

下面，我们说说三个最常被提及的未迁移到云端的理由，并且讨论一下它们的真正含义。

## 太冒险

这是最常见的理由，也许是因为它的范围非常广泛。有时候风险在于“安全性”——通常围绕“我们的客户”对安全性的期望。有时候会担心运行该应用程序所需的特定操作系统和软件版本比 IaaS 中使用的版本更旧 / 不同。有时候是因为原来的系统是由不同的人创建的，而现在的员工不能很好地理解它们，无法确保在不破坏这些系统并导致停机的情况下迁移到云。而且，有时候风险意味着，“我们没有足够的时间来正确地研究和理解云迁移相关的内容。”

如果你处于这种情况，容器可能会很好地帮助你解决这些问题。如果你之前查看过 IaaS，发现虚拟机环境与你当前的环境差别太大，则特定范围的容器应该能够提供帮助。而且，你可以迁移到当前环境中的容器，然后再迁移容器。主要的云供应商已经帮助了许多这样的客户，如果你最近没有关注他们最新和最好的帮助迁移的工具，那么你应该关注一下。

## 太贵昂

利用云的企业能够有效地实现巨大利益，但他们在整个企业中使用云，而不是将其作为数据中心的“即插即用”替代品。云的业务敏捷性和针对性优势依赖企业改变其行事方式。

回到 Act! 类比：设想一个企业以使用 Act! 的方式使用 Salesforce.com——每个用户的帐户都与其他用户独立；所有用户都必须首先使用内部资源对 Salesforce 进行设置，每当出现更新时也要进行设置。这种情况下，企业将无法正确使用它。

为了正确地转向云，企业必须制定迁移到云后（post-cloud）的组织图以及执行策略。云应该能够实现快速和频繁的应用部署，这将增加与客户的反馈循环。云应该让企业自己的员工专注于业务问题，而不是围绕计算机架构执行无差别的繁重工作。

了解云优势的企业将有足够的资金进行迁移（企业将同时运行两个架构），处理从资本支出到运营支出的迁移，聘请合适的顾问，并适当地补偿其员工（包括现任和新任）。不理解这一点的企业可能永远无法采取行动，很有可能会被竞争对手扼杀。

## 是时候迁移到云端了

请在数据中心建立或部署新的应用程序，不要再找借口了。不将大部分或全部现有应用程序迁移到云中，没有什么好的理由——只有管理人员不明白他们的竞争对手将如何使用云来碾压他们。

| 原文名称 | The State of the Cloud 2018 |
| --- | --- |
| 作者简介 | Joe Masters Emison。Joe Masters Emison 是 BuildFax 的联合创始人。 |
| 原文信息 | 2018 年 4 月 9 日发布于 Information Week<br>原文地址 https://www.informationweek.com/cloud/the-state-of-the-cloud-2018/a/d-id/1331464 |
| 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。<br>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《使用“天堂之门”技术的挖矿木马分析报告》

近日，安天 CERT（安全研究与应急处理中心）发现一例使用了名为“天堂之门”（Heaven's Gate）技术的挖矿木马。该技术可使 32 位的载荷注入到 64 位进程中，虽然该技术在 2009 年就已出现，但在目前新出现的挖矿样本中仍极为少见。

在 64 位系统上运行该样本，其会运行一个记事本实例，带有挖矿的典型参数。在 ProcessExplorer 中查看内存中的字符串，可以清楚地看到它并不是一个真正的记事本进程，而是挖取门罗币的恶意代码。释放截荷的 Dropper 是 32 位，但它将有效载荷注入了 64 位的记事本中。微软官方的 API 并不支持这种注入，只允许从 64 位应用程序读取或写入 32 位进程程序，但不能反过来。

“天堂之门”技术在 2009 年首次被一位绰号为 Roy G. Biv 的黑客所提出。在 2015 年的博客文章中，Alex Ionescu 描述了这种技术的缓解措施。在 64 位版本的 Windows 上运行的每个 32 位进程都在被称为 WoW64 的特殊子系统中运行，该子系统模拟 32 位环境。我们可以将其解释为在 64 位进程内创建的 32 位沙箱。因此，首先创建该进程的 64 位环境。然后，在它内部创建 32 位环境。该应用程序在此 32 位环境中执行，并且无法访问 64 位部分。32 位进程本身无法看到 64 位部分，并且仅限于使用 32 位 DLL。为了向 64 位进程注入数据，需要使用适当函数的 64 位版本。32 位和 64 位代码执行可通过代码段的不同地址访问：32 位为 0x23，64 位为 0x33，于是可以使用汇编指令进行更改，这就是“天堂之门”的技术原理。

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。

最终依据静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

### 概要信息

| | |
|---|---|
| 文件名 | f9c67313230bfc45ba8ffe5e6abeb8b7dc2eddc99c9cebc111fcd7c50d11dc80 |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 810 KB |
| MD5 | 7B3491E0028D443F11989EFAEB0FBEC2 |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan[Spy]/Win32.Zbot |
| 判定依据 | 静态分析 |

### 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

| | |
|---|---|
| 查找指定内核模块 | ★ |
| 创建特定窗体 | ★ |
| 获取驱动器类型 | ★ |
| 获取计算机名称 | ★ |
| 请求加载驱动的权限 | ★ |
| 打开自身进程文件 | ★ |
| 读取自身文件 | ★★ |

### 文件扫描

| 文件名 | 文件 MD5 | 家族相似性 | yara 扫描 |
|---|---|---|---|
| target.exe | 7b3491e0028d443f11989efaeb0fbec2 | N/A | N/A |
| target.exe.dmp | c8b7ea7b3684aa4084bfb3f37854cc54 | N/A | N/A |
| Mesoderm.dat | d9fb36a081cffcfc3f8d91dd909e09f5 | N/A | N/A |
| System.dll | 3f176d1ee13b0d7d6bd92e1c7a0b9bae | N/A | N/A |
| petronel.dll | 437b11c6cce872c4c7e94b30e5812997 | N/A | N/A |

### UDP 信息

| 源 IP | 源端口 | 目的 IP | 目的端口 |
|---|---|---|---|
| 0.0.0.0 | 68 | 255.255.255.255 | 67 |
| 192.168.122.1 | 67 | 192.168.122.246 | 68 |
| 192.168.122.246 | 137 | 192.168.122.255 | 137 |
| 192.168.122.246 | 1025 | 192.168.122.1 | 53 |