安天周观察

主办：安天　2017 年 10 月 23 日 (总第 108 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天各地共迎十九大开幕　“不忘初心，牢记使命”

2017 年 10 月 18 日上午 9 时，中国共产党第十九次全国代表大会（以下简称“十九大”）在京开幕。习总书记代表第十八届中央委员会向大会作了题为《决胜全面建成小康社会夺取新时代中国特色社会主义伟大胜利》的报告。

■ 喜迎十九大同观开幕式

为能在第一时间迎接十九大的胜利召开并了解学习会议内容，安天各地的党支部组织公司党员和积极分子统一观看十九大开幕会。大家凝神收听，不时为总书记的报告热烈鼓掌。总书记的身影也让大家回忆起了去年 5 月 25 日习总书记视察安天并与安天人亲密互动的景象，每个人都心潮起伏。用掌声为党点赞，为伟大斗争、伟大工程、伟大事业、伟大梦想喝彩。

■ 奋斗一线保障安全

安天作为国家级网络安全应急支撑单位，参与了历次重大政治、社会活动的网络安全保卫工作，如十七大、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、一带一路峰会、金砖国家论坛等。

在十九大期间的网络安保工作中，安天投入了近两百名工程师，组成了以安天技术负责人肖新光作为总指挥，包括总体协调、事件研判、通报联络、威胁分析、现场处置等九个工作组共同组成的安保团队。按照国家网络安全主管部门、执法部门的要求和所保障的关键信息基础设施运维机构的需求，高度关注持续监测安全威胁状态，密切注意关键信息基础设施、党政信息系统和网站安全运行状况，随时进行风险排查研判上报和应急处置，以保证十九大会议的顺利进行。

■ 学习报告引发思考

在观看学习了习总书记的报告后，曾在去年 4.19、5.25 两次有幸向总书记汇报的安天技术负责人肖新光接受了多家媒体的采访。在采访中肖新光表示：

总书记将“网络安全问题”作为可以和“恐怖主义”、“气候变化”等相提并论的非传统安全威胁，体现了总书记对网络安全的一贯重视。中国网络安全工作者要枕戈待旦，持续努力。

总书记在报告中指出“更加自觉地维护我国主权、安全、发展利益”。作为中国的网络安全工作者，就是要用技术、产品和服务维护我国的网络主权、网络安全和国家与人民的发展利益。我们将按照总书记网络强国的号召和对科技创新的要求，进一步深化核心技术能力，为我国网络强国的建设，为实现“两个一百年的目标”，保驾护航。

总书记在报告中要求我们“坚持总体国家安全观”，“加强国家安全能力建设”，网络空间即是至关重要的非传统安全领域，网络安全能力是非传统安全领域的关键能力，也对政治、军事、经济传统安全领域有重大支撑作用。安天将按照总书记总体国家安全观的要求，从供应链、信息流等更广阔的视角完善自身的技术能力。

总书记在报告中指出要“加快军事智能化发展，提高基于网络信息体系的联合作战能力、全域作战能力”，并在报告中三次提及“军民融合”，“军民融合”为能力型网络安全企业实现在网络空间为国铸盾，提供了广阔天地。作为中国民企国家队，安天将坚定的投身军民融合，将自身安全防护技术转化为国家战略客户的防御感知能力。

■ “不忘初心，牢记使命”

成立十七年来，安天在威胁检测领域中执着探索、不断创新积累；牢记以提升用户应对网络空间威胁的核心能力、改善用户对威胁的认知为企业使命，服务客户，解决问题，应对威胁，保障安全。2016 年 5 月 25 日，习总书记视察了安天，在听取了汇报后，对安天人说，“你们也是国家队，虽然你们是民营企业”。这句话，不仅体现出总书记对安天工作的肯定，更表明他对安天的期许。

未来，安天将继续以“国家队”的坚毅信念匹配习总书记的要求和嘱托，以自身在威胁检测防御领域的技术优势，进一步深化核心技术能力的自我创新发展，奋力践行对国家的使命、勇于承担对网络安全领域的责任，为保障国家的网络安全事业不断奋斗，贡献力量。

上左：哈尔滨安天总部党员和积极分子观看十九大开幕会
上右：安天移动安全公司党支部观看十九大开幕会
下图：安天北京办公区党员和积极分子观看十九大开幕会

进行十九大网络安全保障工作的安天驻场工程师

进行十九大网络安全保障工作的安天驻场工程师

每周安全事件

类 型	内 容
中文标题	英飞凌 TPM 芯片存在弱 RSA 密钥，多家厂商受影响
英文标题	TPM Chipsets Generate Insecure RSA Keys. Multiple Vendors Affected
作者及单位	Catalin Cimpanu；BleepingComputer
内容概述	近日，一众主板上的英飞凌 TPM 芯片上存在不安全的 RSA 密钥，可能会导致设备存在遭受攻击的可能。TPM 指的是可信计算模块，这是一种用于安全密码处理器的国际标准，用于存储关键数据，如密码、证书和加密密钥。而在硬件层面上，TPM 是主板上的专用微控制器，提供硬件隔离防护，生成和存储验证信息，如密码、证书或加密密钥。近期英飞凌发布了公告表示其产品中产生了一系列弱 RSA 密钥，影响的产品是 TCG 系列的 1.2 和 2.0 版本，攻击者可以获取私钥，攻破 RSA1024 和 RSA2048 加密的信息。与此同时，英飞凌已经发布了固件更新并通知了相关的主板厂商进行整合更新。由于在许多商业笔记本、路由器和 IoT 设备中都有 TPM 的身影。
链接地址	https://www.bleepingcomputer.com/news/security/tpm-chipsets-generate-insecure-rsa-keys-multiple-vendors-affected/

每周值得关注的恶意代码信息

经安天检测分析，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.omniscient.a[prv,exp,spy] 2017-10-18	该应用程为一款间谍应用，运行后会隐藏图标，后台窃取用户短信、联系人、浏览器记录、存储的图片、地理位置、通话录音等信息并上传至远程服务器，造成用户隐私泄露，并且存在私自下载行为。建议卸载。（威胁等级高）
		Trojan/Android.BgSpy.a[prv,rog,spy] 2017-10-16	该应用程序运行后隐藏图标，请求 root 权限，私自监听用户手机通话状态、监听用户短信箱，私自发送短信、拦截短信、获取用户手机号码、地理位置等信息并联网上传，造成用户隐私泄露和资费损失，建议不要使用。（威胁等级高）
		Trojan/Android.GhostFramework.a[fra,rog,exp] 2017-09-20	该应用程伪装成正常应用，安装无图标显示，后台通过云端推送广告、模拟点击广告、具有私自下载软件等恶意行为，造成用户流量消耗。（威胁等级高）
	较为活跃的样本	Trojan/Android.Triada.bl[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，并存在私自下载安装未知 APK，联网后会上传手机固件信息，建议卸载。（威胁等级高）
		Trojan/Android.FakeSexApp.e[prv,exp,rog]	该应用程序伪装成色情应用，运行会诱导激活设备管理器，隐藏图标，私自上传用户邮件地址，Google 账户信息及指定文件列表信息，下载恶意子包，访问钓鱼网址，警惕该程序造成用户隐私泄露和财产损失，请卸载。（威胁等级高）
		Trojan/Android.LockScreen.ap[rog,sys,lck]	该应用程序为测试应用，点击锁机后锁定屏幕，并删除系统文件，勒索用户付费解锁屏幕并恢复系统文件，造成系统破坏和手机的正常使用，建议卸载。（威胁等级中）
		Trojan/Android.Hqwar.h[prv,exp,rmt]	该应用程序伪装成正常应用，运行诱导激活设备管理器，访问钓鱼网址，窃取用户银行账户隐私，监听收件箱短信，上传到远程服务器，同时获取指令进行私发短信、群发短信、锁定设备、拨打电话、执行 USSD 指令等高危操作，造成用户隐私泄露和财产损失，建议卸载。（威胁等级高）
		G-Ware/Android.HiddenAds.cm[exp,rog]	该应用程序伪装成新闻应用，运行隐藏图标，后台推送广告，会造成用户资费消耗，建议不要使用。（威胁等级中）
		G-Ware/Android.E4ALocker.c[rog]	该应用程序测试应用，运行后锁定屏幕，并无实际功能，导致用户手机无法正常使用，建议卸载。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Windows SMB Server 远程代码执行漏洞（CVE-2017-11780）	Microsoft Windows SMB Server 远程代码执行漏洞（CVE-2017-11780）攻击者利用该漏洞可在目标系统上执行任意代码执行，如果攻击失败，会导致拒绝服务，对业务造成一定的安全风险。（威胁等级高）
	较为活跃样本	RiskWare[Downloader]/Win32.AdLoad.oa	此威胁是一种传播、下载广告软件的木马类程序。它可以在未经用户许可的条件下入侵用户系统，并窃取重要数据。安装其它恶意软件后可以使用户的电脑性能变慢。（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[DDoS]/Linux.Znaich	此威胁是一类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）

本年度重大云存储泄露事件

Kelly Sheridan / 文　安天公益翻译小组 / 译

继 Verizon，Deloitte 与 Dow Jones 之后，Accenture 的敏感云数据也遭到了泄露。

由亚马逊网络服务 S3 存储桶错误配置引发的云数据泄露是 2017 年令人担忧的问题之一。

RedLock CSI（云安全情报）研究表明，53% 的使用云存储服务的公司，曾无意间向公共网络泄露了一次或多次这种服务，这一比例从 5 月份的 40% 增加到 53%。研究人员还发现 38% 的公司的公共云管理账户曾遭到入侵。

该趋势表明，各种规模的企业以及企业将敏感信息委托给的第三方普遍存在安全问题。很多公司的云存储账户配置方法不当或者未对第三方公司的安全规则进行确认。因此导致客户数据泄露。

在下文中，概述了今年十大 AWS 泄漏事件（排名不分先后）。

Accenture

Accenture（埃森哲）公司留下了至少四个不安全 S3 存储桶并可供公开下载。Accenture 的疏忽泄露了验证凭证、机密 API 数据、数字证书、解密密钥、客户信息和其它可用于攻击 Accenture 及其客户的数据。

在四个被泄露的服务器中，最大的为 137GB，被配置为公共访问，并可供任何人输入存储桶网址进行下载。所有这些都包含了有关 Accenture 云平台和使用它的客户的高度敏感数据。

Viacom

Viacom（维亚康姆）是全球第六大媒体公司，价值 180 亿美元，内部访问凭证和其他重要数据被公开泄露，可通过 AWS S3 云存储桶下载。这可能让攻击者接管其 IT 基础设施

或互联网广告。

Booz Allen Hamilton

UpGuard 维克力发现情报和国防承包商博思艾伦汉密尔顿 6 万个文件可公开访问 S3 存储桶。大约 28GB 的数据缓存包括高级工程师凭证、美国政府系统密码，以及 6 个未加密的用于持有绝密设备清除权限的政府承包商的密码。

WWE

Kromtech 安全研究人员发现世界摔跤娱乐（WWE）存在一个大规模的、未设防的数据库。这些数据存储在 AWS S3 服务器上，它没有用户名或密码保护，任何人都可以访问该网址。研究人员发现了两个可公开访问的 S3 桶，估计约 12% 的信息被设置为公共访问。第一个不安全存储桶包含了几条 2014–2015 年客户的敏感信息，总记录数为 3065805 条。第二个存储桶包含了 2016 年和特定的欧洲客户。

Dow Jones

Dow Jones & Co 数据泄露了数百万客户的姓名、账户信息、物理和电子邮件地址以及信用卡号码的最后四位数字。这次泄露也影响了道琼斯风险和合规的 160 万项，这是一组在金融公司中使用的用于遵守反洗钱法规的规章。

RNC

RNC Deep Root 分析是一家数据分析公司，代表共和党全国委员会（RNC），通过一个不安全的 AWS S3 存储桶泄露了 1 亿 9800 万美国选民的个人资料。这些被泄露的数据包括生日、电话号码、自我报告的种族背景、家庭和邮寄地址以及党派归属等数以百万计的记录。

TigerSwan

TalentPen，一家负责处理新求职者的第三方供应商，因错误配置的 AWS S3 桶缺乏密码保护导致数以千计的美国个人数据被泄露，其中大部分是个人安全公司 TigerSwan 的简历和申请。

这个错误泄露了某些分级安全审查的绝密个人信息。在安全审查的顶部泄密揭露了联合国、美国特勤局、国防情报局、国防部和国土安全部所雇用的国防、情报、执法、语言和后勤专家的工作历史。

Time Warner Cable

Time Warner Cable（时代华纳有线）泄漏事件凸显了外包的危险，约对美国 400 万时代华纳电缆客户造成了影响。Kromtech 安全中心发现了两个 AWS S3 桶被全球通信软件和服务提供商 Broadsoft 泄露在网上。公司拥有 600 多家服务提供商，并支持数百万订阅用户。两个桶都配置为公共访问，因此使得任何人都可以在线访问数据。

ES&S

著名的投票机器和相关软件提供商 ES&S 错误配置的 AWS S3 桶被泄露并可以公开下载。此次错误泄露了 180 万芝加哥的个人信息，包括姓名地址、电话号码、驾照号码和部分社保号。泄露的数据库似乎是在 2016 大选期间，芝加哥选举委员会委员们创建的。

原文名称	Major Cloud Storage Security Slip-ups this Yea
作者简介	Kelly Sheridan，Dark Reading 副主编。
原文信息	2017 年 10 月 13 日发布于 Dark Reading 原文地址 https://www.darkreading.com/cloud/10-major-cloud-storage-security-slip-ups-(so-far)-this-year/d/d-id/1330122
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《利用 FLASH 漏洞传播的木马样本分析报告》

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发现了一个木马样本，该样本是一个利用了 Flash 漏洞 CVE-2015-8651 进行传播的病毒程序。CVE-2015-8651 漏洞是对内存执行相关操作的操作码在执行过程中访问地址的范围进行越界，导致整数溢出的漏洞。该木马利用此漏洞完成了对计算机信息的窃取等相关操作。

安天 CERT 拦截到的恶意代码实体运行后，首先会将自身打包的病毒代码解密拷贝到自身的运行空间，然后使用内存解析执行方式获取实际运行需要的导入表函数地址，对其代码空间中引用的函数地址进行修复。病毒代码经过了大量的代码混淆操作以增加分析人员的调试难度。解密出的样本首先创建 msiexec.exe 进程，以此来伪装自身恶意代码到合法进程中，并将 Shellcode 注入到该进程空间。注入到 msiexec.exe 进程的 Shellcode 代码根据保存的 API 名称 Hash 值获取到后续调用的 API 函数地址，然后判断 API 函数入口点代码类型判断是否需要对其进行间接调用。该木马会调用相关进程判断是否在虚拟机中运行，并在 C:\Users\ 用户名 \AppData\Roaming" 目录下复制自身，文件名为 WindowsSidebarT.exe。还存在添加注册表实现开机自启动；通过服务及注册表设置情况查询 Windows Defender 反间谍软件的配置情况；设置关闭 Windows Defender 服务，获取系统盘信息、用户登录信息等危险操作。在木马与 C&C 服务器建立连接之后，采用 Http 协议与控制端进行通信，用于隐藏通信流量，传回敏感信息并接受控制端的控制。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，在日常工作中应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木马软件样本的检出。

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：

文件被页面手工提交发现，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。

文件名	94ba894594d3af4ec5d6e342ea7435bc706011ae064f3750e1e835b822b14b15
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	208 KB
MD5	69401F8C1B4EF17AA8183EFF6CB3F531
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Kasidet
判定依据	静态分析

完整报告地址：https://10.255.16.99/_lk/details.html?hash=69401F8C1B4EF17AA8183EFF6CB3F531

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	行为描述	危险等级
删除自身	★★★★	延时	★★★

根据动态行为（默认环境）得出该文件具有以下行为：获取主机用户名称、查找指定内核模块、获取驱动器类型、创建挂起的进程、获取计算机名称、遍历进程、读取自身文件、创建特定窗体、释放 PE 文件、增加 run 自启动项、查询 windows product key、独占打开文件、连接网络自启动。

常见行为

行为描述	危险等级	行为描述	危险等级
获取主机用户名称	★	获取驱动器类型	★
查找指定内核模块	★	创建挂起的进程	★★
获取计算机名称	★	遍历进程	★
读取自身文件	★★	创建特定窗体	★
释放 PE 文件	★	增加 run 自启动项	★
查询 windows product key	★★	独占打开文件	★
连接网络	★	自启动	★

进程监控

PID	创建	命令行
1264	msiexec.exe	msiexec.exe