安天周观察

主办：安天　2017 年 7 月 10 日（总第 94 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加第三届军民融合展并发表演讲

7 月 3 日至 5 日，第三届中国北京军民融合技术装备博览会在北京国家会议中心举行，主题为“聚焦自主创新技术装备，促进军民融合深度发展”。

展会上，安天以“赛博超脑 – 网络靶场”作为参展核心，同时展示了安天网络靶场、态势感知与监控预警系统以及安天智甲终端防御系统、探海威胁检测系统、追影威胁分析系统、移动引擎等产品和解决方案。

安天为军工、公安、海关、水利、交通等部委行业提供安全服务与解决方案。特别是为我国重大的国防、军工科研成果提供了网络安全保障，包括载人航天、空间站对接等，安天的产品与服务不但为我国航天发射任务保驾护航，也为我国商用大飞机首飞的网络安全提供了网络安保支持。

在 7 月 5 日上午的网络空间安全论坛上，安天技术负责人发表了题为《网络安全领域军民融合能力流动方向与路径思考》的演讲。

2016 年 5 月 25 日，习近平主席在黑龙江考察期间视察了安天总部，在听取了安天的汇报后，对安天人说“你们也是国家队，虽然你们是民营企业。”军民融合是当前的大势所趋，安天作为网络安全的“国家队”，定会不负重托，军民团结如一人，试看天下谁能敌！

安天获大数据协同安全技术国家工程实验室授牌

7 月 4 日，安天获授“大数据协同安全技术国家工程实验室”牌匾，将与 360 公司、国家计算机应急中心、国家信息中心等多家机构共同建设国内首个专注于保障大数据安全和提升大数据安全分析能力的国家实验室，联合致力于建立大数据安全技术标准和产业规范等大数据安全顶层设计。

伴随着互联网的普及和应用的深入，大数据正在成为网络攻击的目标，5.12“魔窟”(WannaCry) 勒索蠕虫全球攻击事件，正是通过加密锁定机构的重要数据，直接影响到了全球多个国家的医疗、交通、政务等业务的正常运行。因此，大数据安全国家工程实验室将重点建设大数据协同安全技术应用研究平台，以解决我国大数据环境下所暴露出的数据安全和系统安全监测、预警和控制处置能力不足等问题。

安天在网络安全行业拥有十七年深厚积淀，综合应用大数据分析、安全可视化等方面经验，不断推出可抵御各类已知和未知威胁的多样化解决方案。作为实验室共建者，安天将继续致力于大数据安全协同开发、验证和应用平台的建立，为推进大数据协同安全技术的发展和应用，推动国家大数据时代的整体网络安全能力和水平的提高贡献自己的力量。

安天参与 2017 年中央企业网络安全交流研讨大会

7 月 5 日，以“国之重器 网安筑梦”为主题的 2017 中央企业网络安全交流研讨大会在北京国际饭店会议中心成功举办。来自能源、电力、石油、海运、航空、运营商、建筑、铁路、建设、航天、核工业、电子信息、机械制造、银行、证券、保险等 200 余家中央企业和中管金融企业的 400 余位嘉宾参加会议。安天作为企业代表参加了会议，并在展览区对安天综合安全解决方案、产品部署方案、网络安全等级保护解决方案等进行了集中展示。

本次大会旨在贯彻《网络安全法》，加强关键信息基础设施等级保护安全防护能力，落实国家网络与信息安全信息通报工作规范要求等。安天时刻不忘总书记在网信座谈会上对网络安全企业提出的要求，依托深厚的技术沉淀，在关键信息基础设施安全防护等方面贡献自己的力量。不断提高对网络安全的保障能力，助推网络强国建设前进。

安天赴约 2017 民航大数据、信息安全峰会

2017 民航大数据、信息安全峰会于 7 月 6–8 日在成都双流国际机场召开，安天参与峰会并由技术负责人发表题为《由高级持续性威胁 (APT) 引发的防御思考》的主题演讲。

本届峰会以互联网 + 智慧民航、安全民航为研讨主题，意在推动中国民航信息安全建设，打造快捷智慧交通，全面服务区域经济，为建设具有中国特色的国际智慧民航、安全民航提供充分的理论及技术支持。

近年来安天针对重要行业推出的产品和解决方案能够有效地保护关键基础设施和重要 IT 资产的安全，具备威胁持续采集、快速发现，深度分析和及时响应的能力。民航业作为国家交通的基础工具，承担了人们的日常外出和国内的物流运输的重要责任，民航业的网络安全直接影响国家经济的发展和人们的日常生活。

安天作为国内网络安全领域专注于威胁检测防御技术的领导厂商，将依靠自身优势为国家民航业的发展献策献力。

每周安全事件

类 型	内 容
中文标题	30 万 WordPress 站点所使用的插件被发现 SQL 注入漏洞
英文标题	SQL Injection flaw in WordPress Plugin WP Statistics potentially exposed 300,000+ Sites
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，Sucuri 的安全专家在一款 WordPress 插件中发现了漏洞，插件影响的网站超过 30 万。 漏洞出现在一款安装量很大的插件 WP Statistics 插件中。这款插件让网站管理员们获得网站在线用户数量、访问次数和访问者数量以及页面统计等详细信息。漏洞的原因在于对用户输入的数据没有做过滤，黑客可以泄露敏感信息甚至入侵 WordPress 网站。漏洞影响到的函数包括 wp_statistics_searchengine_query()。研究人员已经把漏洞汇报给了插件厂商，WP Statistics 团队已经更新了 12.0.8 版本。
链接地址	http://securityaffairs.co/wordpress/60596/hacking/wordpress-wp-statistics-flaw.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 个移动平台恶意代码和 4 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	新出现的样本家族	Tool/Android.ExtremeSpy.a[prv，exp] 2017-06-25	该应用程序是一款监控工具，根据需求可以监控的业务：短信、通话记录、联系人、地理位置等，谨慎使用。（威胁等级低）
		Trojan/Android.woSpy.a[prv，exp] 2017-06-27	该应用程序无实际功能，运行后远程控制操作：私自发送短信、上传短信、手机频繁振动等，造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.Terbod.a[prv，rmt，fra] 2017-06-27	该应用程伪装成正常应用，运行后隐藏图标，利用 Telegram 提供的通讯接口，接收远程指令，窃取用户短信和通讯录并上传，造成用户隐私泄露和流量消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.MeihuaK.a[prv，rmt] 2017-06-28	该应用程安装无图标，运行后接收短信指令，收集并上传用户短信、通话记录、QQ 聊天记录等隐私信息，按指令发送指定短信、拨打指定电话，还能弹窗锁定手机进行勒索，同时发送邮件报告服务端软件运行情况。造成用户隐私泄露、资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.DroidMiner.a[prv，exp] 2017-06-29	该应用运行后隐藏图标，窃取用户短信、联系人、谷歌账号、通话记录、手机基本信息等隐私信息，使用前置摄像头进行人脸拍照，并发送到指定邮箱。造成用户隐私泄露和资费消耗。（威胁等级高）
	较为活跃样本	Trojan/Android.QQspy.cg[prv，exp]	该应用程序伪装成 QQ 刷赞类应用，运行后诱导用户输入 QQ 账号密码，通过邮箱转发，造成隐私泄露和资费损耗，建议立即卸载。（威胁等级中）
		Trojan/Android.SmsFilter.h[sys，rmt]	该应用程序监听收件箱，拦截指定短信，接收短信指令拨打电话，影响用户正常使用，建议卸载。（威胁等级中）
		Trojan/Android.Triada.ap[exp，rog]	该应用程序运行后加载恶意网址，上传用户的手机 imei 号、imsi 号、mac 等信息，下载其他软件，造成用户流量消耗和隐私泄露。（威胁等级高）
		Trojan/Android.Guerrilla.e[fra，exp]	该应用程序伪装成系统应用，启动后隐藏图标并加载广告，造成用户资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.FakeInst.eu[prv，exp]	该应用程序运行后隐藏图标，后台联网收集用户短信、通讯录隐私上传，遍历通讯录联系人群发指定短信，建议立即卸载，避免造成隐私泄露和资费损耗。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	FFmpeg 本地文件任意读取漏洞	由于 FFmpeg 可处理 HLS 播放列表，而播放列表中已知可包含外部文件的援引。恶意攻击者可以利用精心构造的 avi 文件中的 GAB2 字幕块，上传构造的 avi 视频到使用 FFmpeg 的目标站点，可以通过 XBIN codec 获取到视频转换网站的本地文件（例如：查看 /etc/passwd 文件内容），从而导致敏感数据信息泄露。（威胁等级高）
	较为活跃的样本	Trojan[Ransom]/Win32.Petya	此威胁是一类可以加密用户数据索取赎金的勒索软件家族。该样本遍历磁盘加密文件并修改 MBR，重起后提示勒索信息。（威胁等级中）
		Trojan[Banker]/Win32.Tuhkit	此威胁是一类可以窃取用户银行信息的木马家族。该家族样本运行后连接远程服务器，收集用户系统中网络银行信息并回传。（威胁等级中）
		Trojan[Dropper]/Win32.Brpd	此威胁是一种具有捆绑行为的木马类程序。该家族会携带各种恶意软件，在用户电脑中安装并运行。（威胁等级高）

保护云环境免遭勒索攻击的九个措施

Kelly Sheridan / 文　安天公益翻译小组 / 译

技术推动了更快的协作和数据传输，也使网络犯罪分子能够迅速地传播勒索软件。

1. 保护云计算层

Evident.io 创始人兼首席执行官提姆·普伦德加斯特 (Tim Prendergast) 表示：“最重要的事情就是保护云计算机层。自动化很容易实现，创业公司和大企业都能轻松实现。”

保护计算层将确保系统和数据的可用性，并防止威胁源利用你的计算能力在整个组织中传播恶意软件。普伦德加斯特说，组织首先要做的是，向个人分配 SSH 密钥来启用安全登录。

2. 分离数据存储

Shpantzer 建议了解正式和非正式资产所在的位置，这是规划勒索攻击应对方案时非常重要的一步，但是经常被忽视。他解释说，例如，许多开发人员正在云端的服务器上进行快速测试，但是并不完全了解这样做的安全性和合规性。有时他们会暴露生产数据库的完整副本，这种错误会在勒索软件和可用性问题之外增加保密性问题。至于存储，Shpantzer 建议使用廉价的云存储来存储截图、文件、文件夹以及重建操作所需的任何东西。将它们冷存储在一个单独的 MFA(多因素身份验证) 保护的账户中。

雷维斯 (Reavis) 还建议分离数据存储，特别是脱机备份，以便在发生攻击时保护备份。

3. 网络分段

皮伦蒂 (Pironti) 表示，既然现在的架构已经合适，企业应该利用这个机会对网络进行分段。这样可以限制和遏制勒索攻击的传播。

在云中，皮伦蒂继续说，安全团队可以使用架构在关键活动之间设置“门”。如果发生攻击事件，组件周围的墙壁和隔离区可以保护它们。

4. 身份管理

普伦德加斯特认为身份管理是继保护云计算层之后第二大重要措施。

他说：“一旦你设置了核心安全层，就能了解人们的特性和正常的行为模式，这可以帮助你做出更明智的业务决策。”

5. 数据访问管理

除了采用复杂、安全的密码和多因素身份验证外，企业还应限制员工对敏感信息的访问。这会限制攻击者访问账户时能够执行的攻击规模。

身份和访问管理 (IAM) 策略和访问控制列表可以帮助企业组织和控制云存储的权限。桶策略可以帮助企业根据账户、用户或条件 (如 IP 地址或日期) 设置或拒绝权限。

6. 使用跳转主机

跳转主机位于不同的安全区域，提供了访问系统中其他服务器或主机的唯一方法。普伦德加斯特表示，“从管理的角度来看，这是一种一站式入站访问方法”。

该主机是单一的管理入口点。它配置了标准的 DNS 名和 IP 地址，并且只允许企业 IP 登录，然后才会授予更广泛的访问权限。

因为跳转主机是单一入口点，所以它简化了保护服务器和维护严格访问控制的流程。如果这个服务器被跳过，我们很容易创建一个新的服务器。

普伦德加斯特 (Prendergast) 说：“跳转主机也不能免疫攻击，但是能够将攻击面减小到一个非常小的接入点。”保护一台服务器的安全比保护数千台更容易，特别是在新兴的攻击中。

7. 基于云的安全即服务

雷维斯建议企业实施基于云的安全即服务解决方案，该方案共享一个共同的威胁情报库，可以阻止勒索软件下载。虽然他没有具体介绍该解决方案，但是指出需要安全 Web 网关和 CASB 类型的功能。

8. 设置 (系统) 管理程序防火墙规则

许多专家在设置出站规则方面颇为犹豫，但这是很重要的，因为勒索软件会导致知识产权的暴露。如果可以在防火墙上编写实时监控和执行操作，就能够更好地在整个环境中保持一致性。”普伦德加斯特说。

皮伦蒂补充说，领导者应该执行入口和出口过滤。“监控 C&C 活动，只允许符合规定的流量出站。”

9. 不要让服务与 SaaS 系统通信

普伦德加斯特警告说不要让服务与诸如 Github 这样的 SaaS 服务通信。一旦威胁源访问了您的 Git 库，当服务与 Github 通信时，他们就能感染和访问更多的公司系统。

他建议企业将 Git 或代码库存储在自己的云环境中，但是指出这种做法可能需要时间来适应。

“人们很难采用这一方法，”他承认，“随着服务越来越好，还有更多的自主托管选项，公司可以更好地控制离开其环境的数据。”

原文名称	9 Ways to Protect Your Cloud Environment from Ransomware
作者简介	Kelly Sheridan，Dark Reading 的副编辑。
原文信息	2017 年 6 月 27 日发布于 Dark Reading 原文地址 https://www.darkreading.com/cloud/9-ways-to-protect-your-cloud-environment-from-ransomware/d/d-id/1329221?image_number=1
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《CVE-2017-8225 漏洞分析报告》

近日，安天追影小组发现一个影响范围极广，危害性极高的漏洞，漏洞编号为 CVE-2017-8225（自定义 http 服务器中的预授权的身份信息 / 凭证泄漏）。

Shodan 列出了 185000 个易受攻击的摄像头。“云”协议通过仅使用目标摄像头的序列号，在攻击者和摄像头之间建立明文 UDP 隧道（以绕过 NAT 和防火墙）。最终，攻击者可以暴力破解摄像头的凭据。

漏洞原理

无线网络摄像头 (P2P)WIFICAM 是一款中文网络摄像头，可以远程流式传输。无线网络摄像头 (P2P)WIFICAM 是一款整体设计不佳的摄像头，具有很多漏洞，这款摄像头未正确检查对 .ini 文件（包含凭据）的访问。

在这款摄像头中，一般会使用自定义的 Http 服务提供 HTTP 接口。这个 HTTP 服务器实际上是基于 GoAhead 的，并由摄像头的 OEM 供应商修改（导致列出的漏洞）。

它允许两种认证：htdigest 认证或在 URI 中进行身份验证 (?loginuse=LOGIN & ?loginpas=PASS)。攻击者可以通过在 URI 中提供一个空的 loginuse 参数和一个空的 loginpas 参数来绕过身份验证。

漏洞利用

该漏洞通过在对 system.ini 文件的访问 URI 中提供一个空的 loginuse 和一个空的 loginpas 来绕过身份验证并获取用户名密码。攻击者通过获取的管理员身份进行认证，进而远程控制设备漏洞。

对于此漏洞，其命令注入位于 set_ftp.cgi 中，将需要执行的命令放于 pwd 参数后构造具有恶意命令的 URL，此命令就会在摄像头上执行。比如：通过 nc 命令，就可以建立攻击者和摄像头之间的一个反向连接，攻击者可以完全获取摄像头的 shell 权限，可以采取更多的恶意操作。

总结

首先，此漏洞利用起来并不复杂，只需要发送一条 URL 请求，在进行漏洞利用时可以绕过身份验证，这使得漏洞的利用难度大大降低。

此外，由于此漏洞对应的 HTTP 服务是基于 GoAhead（嵌入式 Web 服务器）的，而大部分的 IP 摄像头都包含 GoAhead，因此会被攻击者利用来构建僵尸网络，新型的 IoT 僵尸网络恶意软件 Persirai 就是利用了这个漏洞。

在此，安天提醒广大网络用户，使用网络摄像机时，应当尽快修改默认的密码，及时更新自己的设备，减少被漏洞利用的机会。

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：

文件被内部组件发现，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、静态分析鉴定器、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将文件判定为木马程序。

文件名	7e1c3834c38984c34b6fd4c741ae3a21.danger
文件类型	BinExecute/Linux.ELF
大小	161 KB
MD5	7E1C3834C38984C34B6FD4C741AE3A21
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Gafgyt.aw
判定依据	静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=7E1C3834C38984C34B6FD4C741AE3A21

◆ EXIF 信息

描述	值
File Size	161 kB
File Type	ELF executable
MIME Type	application/octet-stream
CPU Architecture	32 bit
CPU Byte Order	Big endian
Object File Type	Executable file
CPU Type	MIPS R3000