安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 10 月 29 日 (总第 157 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

喜报：安天斩获国家应急中心网络安全引擎大赛双料冠军

在今年 7 月 26 日至 8 月 16 日国家互联网应急中心（CNCERT/CC）举办的“恶意代码分析引擎大赛”（14 家企业参赛）与“网络流量分析引擎大赛”（13 家企业参赛）中，安天以嵌入安天下一代威胁检测引擎的追影威胁分析系统、探海威胁检测系统两项产品分别参赛，经过 16 天的对比评测，安天最终包揽两项赛事第一名。

国家互联网应急中心举办的这次活动，是面向国内网络安全企业的专业赛事，比赛基于真实的网络安全业务场景和数据进行评测，旨在全方面考察参赛产品核心检测分析引擎的技术能力与业务实战能力。安天产品展示出了在恶意代码动静态分析与流量侧检测能力方面的底蕴积累，并在材料审查、现场专家评审答辩等环节表现良好，依托对比测试结果的较大优势，结合安全领域专家对引擎的技术路线、创新性、监测成果、应用场景等方面的全面评判，最终包揽两项赛事冠军。

安天追影获奖证书

安天在恶意代码分析和流量引擎分析领域具有长期、专业的能力与数据积累，能够快速、精准地应对赛场各项测试和评比。在本次实战型比赛中，安天探海威胁检测系统展示了零拷贝流量高速捕获技术、高速协议栈带来的高速流量分析能力，特别是单边流量解析能力；产品单包检测、流监测、载荷异步还原检测、上下文关联检测的多层次检测优势相对于检测层次较为单一的竞品展示出明显的检测深度优势。安天追影威胁分析系统展现出了强大的静态解析能力和模拟环境分析能力。

安天探海获奖证书

安天 AVL SDK 威胁检测引擎曾先后获得科技部创新基金、国家 863 和发改委信息安全专项支持，AVL SDK 检测引擎的移动版本曾获得中国厂商首个 AV-TEST 年度奖项。安天引擎为自身探海、追影、智甲等全线产品和全球数十家合作伙伴赋能威胁检测能力。在传统以文件载荷为主要对象的第一代检测引擎基础上，安天研发了针对载荷、信标、流量、场景等不同对象进行检测，识别，标记，向量化的下一代威胁检测引擎。其不仅进行有害识别，同时实现对检测对象的信誉判定和向量拆解，为后续检测分析环节提供更细粒度的数据。以威胁检测能力为基础，结合其他功能模块，安天研发了探海、追影、智甲、拓痕等安全产品。

作为国家级网络安全应急支撑单位，安天长期在国家应急中心指导下，积极承担国家网络安全应急工作，成长为中国网络安全应急体系最重要的企业节点之一。安天在恶意代码检测、恶意代码自动化分析等方面承担了工程项目建设的主力角色，并在应急分析与处置、高级威胁深度分析中为国家中心提供服务支撑。国家应急中心对实际业务场景和真实流量的实战化检测分析能力的诉求亦不断促使安天对自身能力与产品进行提升与优化，安天对流量检测引擎支持 SNORT 格式规则扩展，对文件检测引擎支持 YARA 规则的扩展，都是在应急中心的实战需求中产生。

通过本次比赛，我们看到自身产品的检测和分析能力距离国家应急中心的实战化期望还有很大的可提升空间，比如，产品自动化生成的分析报告还不能完全达到用户的业务要求。今后，安天将在应急中心指导下，发挥技术能力优势，并将分析工程师的经验逐步固化为产品能力。

安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，以网络安全能力叠加演进为导向，协助用户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能用户筑起可对抗高级威胁的网络安全防线。安天人深知，基础检测分析能力是这一工作目标的支撑能力，但仅靠基础检测分析能力，远不足以达成这一目标。任重道远，我们会继续努力。

每周安全事件

类 型	内 容
中文标题	新的 NFCdrip 攻击可从物理隔离系统中窃取数据
英文标题	New NFCdrip attack could be used to exfiltrate data from air-gapped systems
作者及单位	Sophia Brown
内容概述	新研究表明，被称为 NFCdrip 攻击的技术可以利用近场通信（NFC）协议从通信设备中窃取有价值的数据，包括窃取密码和加密密钥，这些数据的范围可达 10 米。应用安全公司 Checkmarx 的高级研究员 Pedro Umbelino 使用几个物理隔离系统进行了实际操作，使用最简单的幅度调制方法开关键控（OOK）来调整 NFC 操作模式的数据，使攻击者可以轻松访问恶意应用程序，最终可能通过 NFC 频率窃取数据。 尽管随着距离的增加，误差的数量增加，但 LeClair 表示可以通过使用 AM 天线或软件无线电（SDR）加密器来扩展数据传输范围。研究人员发现，这种攻击在具有 Wi-Fi，蓝牙和 GSM 禁用等通信系统的设备上非常高效。
链接地址	https://cyware.com/news/new-nfcdrip-attack-could-be-used-to-exfiltrate-data-from-air-gapped-systems-7148b98c

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 6 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	Tool/Android.ANDRAX.a[sys,exp] 2018-10-22	该应用程序为 Android 手机的渗透测试平台，运行点击下载工具包，可用于信息收集、网络扫描、网络数据包制作，并集成了大量开发工具和黑客工具，可能存在风险，建议用户谨慎使用。（威胁等级中）
		Trojan/Android.advhot.a[prv,exp,rmt,spy] 2018-10-23	该应用程序伪装其他应用，运行会弹窗虚假信息诱骗用户开启辅助功能。会监听电话状态并自动挂断电话，监听短信，私自联网上传用户短信信息和通讯录信息，获取远程指令执行发送指定短信、向用户通讯录群发指定短信、拨打电话等，造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.Onespy.b[prv,rmt,spy] 2018-10-24	该应用程序是一款间谍软件，运行后私自提权，获取远程控制指令，窃取用户短信、联系人、通话记录、地理位置、社交软件信息、电子邮件信息，私自录音、录像，并将用户隐私上传至服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃样本	G-Ware/Android.CoinMiner.c[exp,rog]	该应用程序伪装正常应用，运行隐藏图标，后台私自挖矿，影响用户正常使用，建议不要使用。（威胁等级低）
		Trojan/Android.movi.a[prv,spy]	该应用程序伪装为正常应用，诱导激活设备管理器，运行隐藏图标，获取用户位置信息，对通话私自录音并上传，私自截屏并上传，会造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Tool/Android.FindMe.b[prv]	该应用程序是一款定位工具，联网获取位置信息，可通过短信和邮件的方式发送，建议谨慎使用。（威胁等级低）
		RiskWare/Android.Thief.c[prv,exp]	该应用程序安装后通过设置，可以监听用户手机来电号码，拨出号码，接收收件箱，转发用户手机信息到指定手机号码，执行拍照并将照片发送到指定邮箱，建议谨慎使用。（威胁等级中）
		Trojan/Android.Sandeep.a[prv]	该应用程序运行获取用户短信、通话记录、联系人信息，上传至服务器，造成用户隐私泄露，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	LIVE NETWORKS LIVE555 streaming media RTSP 服务器远程代码执行漏洞（CVE-2018-4013）	该漏洞源于 LIVE555 RTSP 服务器库的 HTTP 数据包解析功能，攻击者可以通过发送一个特制的数据包造成堆栈的缓冲区溢出，从而导致代码执行。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/Win32.Winner	此威胁是一种有广告行为的灰色软件类程序。该家族通常与正常软件捆绑到一起进行传播，它会在电脑上收集用户信息，并根据这些信息获取用户习惯并推送广告。（威胁等级低）
		RiskWare[Downloader]/Win32.Kasinst	此威胁是一种下载广告软件的风险软件类程序。该家族会自动下载并运行用户不知情或不允许安装的软件，同时它也可以不断地检查更新文件本身。（威胁等级低）
		GrayWare[AdWare]/Win32.ConvertAd	此威胁是一种有广告行为的灰色软件类程序。该家族通常与正常软件捆绑到一起进行传播，它会在电脑上收集用户信息，并根据这些信息获取用户习惯并推送广告。（威胁等级低）
		Worm[Net]/Win32.Kido	此威胁是一种可以复制自身并通过网络传播自身的蠕虫家族。该家族样本运行后复制自身，通过网络共享及垃圾邮件进行传播，可能会窃取用户信息。（威胁等级中）
		Trojan[Exploit]/JS.Agent	此威胁是一种使用 JS 脚本语言编写的、可以利用漏洞下载恶意代码的木马家族。该家族并没有统一的行为、统一的功能，而是像一个木马集合一样，将大量基因片段定性的恶意代码归类。（威胁等级中）

澄清关于公有云安全的三个迷思

Laurence Pitt / 文　安天技术公益翻译组 / 译

随着越来越多的机构迁移到“云”，围绕云的安全性出现了一些不可避免的问题。具体而言，企业需要确认，如果他们选择基于云的模型（尤其是公有云），他们的数据将是安全的。关于公有云，我从客户那里最常听到的话是：“公有云是不安全的，因为它更容易受到攻击。一旦它受到攻击，任何人就都能访问我的数据了。”这种观点是不正确的。下面，我们把这个问题拆分开来，详细分析其中的每个部分。

迷思 1：“公有云不安全”

当公有云技术刚刚推出时，有人担心它无法提供必要的安全措施来保证数据的安全。当时，公有云技术尚未成熟，因此这些担忧是合理的。然而，这种情况早已发生了改变。现在，云提供商已经拥有多年的经验——最早可以追溯到现代云计算被首次引入的 20 世纪 90 年代初。几十年来，他们不断地对数据和应用程序访问进行微调，确保能够提供强大的监管、权限管理和系统监控功能。

虽然本地 IT 和基于云的 IT 有相同的目的——都是为了确保应用程序的可用性和安全性，但是云提供商能够在多个企业和地区进行扩展。这种规模和经验意味着，只要妥善管理，公有云解决方案会比本地解决方案更加安全可靠。

迷思 2：“公有云更容易受到攻击”

许多企业认为，使用公有云无异于将所有“鸡蛋”（即数据）放在一个篮子里。他们担心，一旦云提供商受到攻击，他们将会失去对云中数据的访问权限，导致无法开展业务。但是，在大多数情况下，即使攻击者成功地执行了攻击，他们也需要利用未打补丁的漏洞才能访问数据。而众所周知，如今对任何机构而言，最重要的任务之一就是及时打补丁。

公有云的一个重要优势是：云提供商不仅负责修复和监控网络，还能提供额外的安全层，以便将内部网络系统与外部可访问的应用程序和数据分离开来。通过添加第三方供应商（其职责是及时更新系统），公有云的安全性能够增强，便于更好地保护数据。相比于各机构自己存储数据，公有云更加安全。

迷思 3：“在公有云中，任何人都可以访问我的数据。”

人们对公有云最大的担忧之一是：如果将数据委托给云提供商，他们就会失去对这些数据的控制权。用公有云存储替代本地存储，我们可以了解公有云能够实现何种程度的安全。不过，“软件即服务”（SaaS）的一个主要优势就是数据隐私——实际上，相比于本地数据，攻击者更难访问公有云中的数据。

例如，公有云中的数据受到身份验证控制措施的保护，而且云提供商会持续监控这些措施。需要注意的是，云提供商不仅监控你存储在云中的数据，还监控其他客户存储在云中的数据。这样一来，如果有人试图访问你存储在云中的数据，云提供商可以近乎实时地更改安全措施，同时自动增强对其所有客户的云保护。此外，公有云是多租户的，云提供商会为各个企业提供数据保护，确保他们的数据不会被其他企业（例如竞争对手）访问。这意味着每个企业的数据实例都是唯一的，不会与其他企业的数据混杂——云提供商会使用安全密钥对数据加以混淆，防止泄漏。因此，心怀恶意的实体极难访问你的信息。

总结

公有云的最大特点是：它能够大规模地提供安全性。作为单一的机构，你所做的一切都是“个体”的。你可以从同行身上吸取经验教训、监控系统，为应用打补丁和更新应用，但是这种方法缺乏“互利性”。而且，由于网络安全专家的短缺，这些措施可能很难跟得上。

我们经常谈论共享资源和信息的好处，特别是在网络安全领域。举例来说，安全厂商通过网络威胁联盟等组织共享威胁信息，能够实现客户互利。云提供商的客户也是如此。随着客户群的增长，云提供商会监控多个地区并处理全球范围内的攻击，这样一来，他们的所有客户都将从中受益。公有云提供商为了给某个客户提供更强大的安全性而做的任何更改，都将自动应用于其全球的所有客户——确保为他们提供更强大的安全性。

原文名称	3 Public Cloud Security Myths Debunked
作者简介	Laurence Pitt。Laurence Pitt 是 Juniper Networks 公司的全球安全战略总监。
原文信息	2018 年 10 月 18 日发布于 Security Week 原文地址 https://www.securityweek.com/3-public-cloud-security-myths-debunked
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《KeyPass 勒索软件分析报告》

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种名为 KeyPass 的勒索软件开始活跃。KeyPass 勒索软件通过虚假的软件安装程序进行传播，2018 年 8 月份在世界范围内大量出现。

KeyPass 程序用 C++ 编写，并在 MS Visual Studio 中编译，使用库 MFC、Boost 和 Crypto++ 进行开发。PE 报头包含的最近的编译日期为 8 月 7 日。当恶意代码在受害者的计算机上启动时，KeyPass 将自身复制到%AppData%并执行，然后删除自身。KeyPass 在加密时会将加密密钥和受害者 ID 作为命令行参数回传。KeyPass 从受感染计算机可枚举访问本地驱动器和网络共享并遍历所有文件，它会跳过系统目录中的文件维持系统正常运行，其路径被硬编码到样本中。KeyPass 开发人员在 CFB 模式下，使用带有 zero IV 和相同 32 字节密钥的对称算法 AES-256 的简单方案对所有文件进行加密，启动后，KeyPass 连接到 C & C 服务器，回传当前受害者的加密密钥和感染 ID，数据以 JSON 的形式通过纯 HTTP 传输。如果 C & C 无法访问，则使用硬编码密钥和 ID 进行离线加密。研究人员称 KeyPass 木马包含一个默认隐藏的表单，按下键盘后可以显示该表单，此功能表明该木马可以采用手动控制。

安天 CERT 提醒广大政企客户，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。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

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：

文件被页面手工提交发现，经由 YARA 自定义规则鉴定器、文件来源信息鉴定器、文件元数据鉴定器、BD 静态分析鉴定器、数字证书鉴定器、动态 (WinXP) 鉴定器、动态 (Win7 x86) 鉴定器、反病毒引擎鉴定器、聚类分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

文件名	ee74c63faa2eb9709b1d738762e28072aece2e7b9eeffc5913eb6a5fd1564752
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	2.82 MB
MD5	901D893F665C6F9741AA940E5F275952
病毒类型	木马程序
威胁名称	Trojan[Ransom]/Win32.Encoder
判定依据	动态行为

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=901D893F665C6F9741AA940E5F275952

运行环境

操作系统	内置软件
WinXP 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	附加信息	
删除自身	★★★★	FileName	C:\Documents and Settings\Administrator\Local Settings\Application Data\target.exe
		FileName	C:\ccb32a37e01a4e9581b04d929a47b089\share\target.exe

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器、动态行为鉴定器将文件判定为木马程序。

该文件具有以下行为：疑似桌面控制；独占模式打开，防止复制读取，防止杀毒软件扫描上报；获取当前光标位置；创建挂起进程；获取驱动器类型；访问文件尾部；获取系统信息。

常见行为

行为描述	危险等级
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
获取当前光标位置	★
创建挂起进程	★★
获取驱动器类型	★
访问文件尾部	★
疑似桌面控制	★

进程监控

PID	创建	命令行
1220	target.exe	"c:\ccb32a37e01a4e9581b04d929a47b089\share\target.exe"
1316	target.exe	"C:\Documents and Settings\Administrator\Local Settings\Application Data\target.exe"
1320	cmd.exe	cmd /c ""C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\delself.bat""