安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 11 月 05 日 (总第 158 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天召开“CNCERT 网络安全引擎大赛双冠获奖总结会”

2018 年 7 月 26 日至 8 月 16 日，国家互联网应急中心（CNCERT/CC）举办了“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），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。

11 月 2 日，安天召开了对于此次大赛的工作总结会。一方面为表彰在比赛中做出突出贡献的集体和个人；更重要的是，对其中反映出的问题和不足进行总结与反思，以帮助未来进一步推动相关问题的改善和解决。

在总结会上，几位负责人分别从参赛前期准备、比赛期间各相关部门的协调运行及比赛现场情况进行了详细总结，对产品表现及能力不足方面进行了反思，同时对辛苦一线的同事们表示了感谢。随后，对于为比赛获奖做出突出贡献的集体与个人给予了表彰。

对贡献突出的集体和个人进行表彰

最后，安天创始人、首席架构师进行了总结。他表示，虽然安天的产品和队伍在本次比赛中取得了一定的成绩，但更难能可贵的是，我们的参赛团队以及后台支撑团队，敢于直面和正视自身问题，主动总结自身产品、能力的许多不足，如产品易用性、界面友好性以及其他待提升的功能等。

他指出，此次参赛我们实际上并未真正将产品能力转化为客户侧价值，如何将能力向客户价值转化，形成综合性体系，依旧是我们非常大的挑战。网络安全领域的威胁已经由过去应对单点威胁，转入应对复杂的高级网空威胁行为体组合式的网络攻击。对安天来说，也需要进行相应调整，由自我能力闭环，转为安全厂商与客户、与攻击对手之间的能力闭环；由单点防护能力转为动态防护能力；由监测型态势感知转为战术型态势感知。

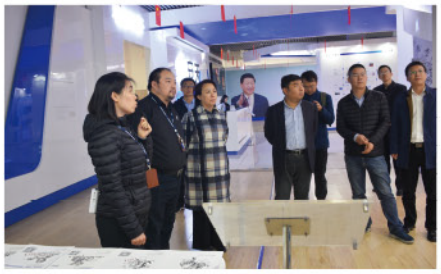
安天将继续夯实基础能力，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，以网络安全能力叠加演进为导向，协助用户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能用户筑起可对抗高级威胁的网络安全防线。

安天调研考察

中央网信办杨春艳副局长一行莅临

近日，中央网信办副局长杨春艳一行莅临安天进行调研考察，黑龙江省委网信办孙主任陪同参观。安天相关负责人为来宾介绍了安天的发展历程及现状，并展示了安天取得的各项资质荣誉。在安天持续与网络安全威胁对抗方面，特别汇报了对高级威胁的发现、捕获、分析等方面所做的工作。重点介绍了安天针对 APT-TOCs、白象、方程式、绿斑等攻击组织的攻击情况、所使用的攻击装备等的分析进展。

各位领导在参观后对安天的技术能力及取得的成果表示肯定，并对安天的产品、发展等各方面与安天负责人进行了深入交流。



新 WiFi 密码破解技术被公开，能轻松破解大多数现代路由器的 WiFi 密码

在 2018 年 7 月，US-CERT 对 Emotet 银行木马提出警告与减少恶意软件影响的措施之后，该木马的开发者采用了新技术以绕过这些措施。Emotet 木马出现于 2014 年，现已发展具有多种功能，可以进行信息窃取，传播垃圾邮件和充当释放程序，并具有规避技术和保持持久性等功能。其中一项为使用基于域的消息身份验证，报告和一致性（DMARC），来评估电子邮件的真实性，DMARC 依赖于“发件人政策框架”（SPF）和“域名密钥识别邮件”（DKIM）。而攻击者使用一种称为域劫持技术来规避 DMARC 控制的机制。

（原文链接：https://www.bleepingcomputer.com/news/security/malware-distributors-adopt-dkim-to-bypass-mail-filters/）

每周安全事件

类 型	内 容
中文标题	Systemd 套件漏洞可以导致运行 Linux 的计算机崩溃
英文标题	Systemd flaw could cause the crash or hijack of vulnerable Linux machines
作者及单位	Pierluigi Paganini
内容概述	谷歌安全团队的 Felix Wilhelm 披露开源 Systemd 管理套件的 DHCPv6 客户端中存在漏洞，攻击者可以使用恶意制作的 DHCPv6 数据包触发漏洞并修改易受攻击系统的部分内存，从而可能导致远程执行代码。该漏洞被追踪为 CVE-2018-15688。Wilhelm 称函数 dhcp6_option_append_ia 用于将服务器接收到的身份关联编码到传出 DHCPv6 包的选项缓冲区中，攻击者可以使用服务器 id 大于等于 493 个字符的 DHCPv6 服务器触发溢出。Systemd 套件存在多个 Linux 发行版，专家指出通过网络或 ISP 中恶意 DHCPv6 服务器发送特制路由器通告消息，启用 DHCPv6 客户端可劫持或基于 Systemd 的 Linux 计算机崩溃。Systemd 开发者及时发布了安全修复程序。
链接地址	https://securityaffairs.co/wordpress/77470/hacking/systemd-security-flaw.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 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	Trojan/Android.SpamSms.a[exp,rog] 2018-10-26	该应用程序伪装正常应用，运行就会获取参数私自发送指定短信，监听、拦截短信，造成用户资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.SpyApp.s[prv,mat,spy] 2018-10-27	该应用程序伪装成系统应用，运行后激活设备管理器，接收远程指令，可获取手机位置、短信记录、通话记录、联系人信息及 Gtalk、Skype、Facebook、Yahoo、WhatApp 等社交应用消息记录上传远程服务器，造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.Spyoo.g[prv,spy] 2018-10-28	该应用程序是一款间谍软件，运行后私自提权，窃取用户短信、联系人、通话记录、地理位置、浏览器历史记录、社交软件信息、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，建议立即卸载。（威胁等级中）
	较为活跃样本	G-Ware/Android.jiasuo.da[rog,sys,lck]	该应用程序伪装正常应用，诱骗用户激活设备管理器，篡改界面欺骗用户付费解锁，造成用户设备无法正常使用，建议不要使用。（威胁等级中）
		RiskWare/Android.E4Acili.a[exp]	该应用程序是一个磁力播放器，诱导用户加 QQ 群，部分功能需要购买卡密付费使用，存在一定的风险，请谨慎使用。（威胁等级低）
		Trojan/Android.Locker.bd[rog,sys,lck]	该应用程序伪装游戏外挂辅助类工具，诱导用户获得 root 权限，而后篡改锁屏界面，要求用户付费解锁，影响用户手机的正常使用，建议不要使用。（威胁等级中）
		G-Ware/Android.Dropper.br[exp,rog]	该应用程序经过重打包处理，运行后会激活设备管理器，释放恶意子包，静默子包私自下载其他应用，加载广告，造成用户流量消耗，建议不要使用。（威胁等级低）
		Trojan/Android.adups.b[exp,bkd,tmt]	该应用程序安装无图标，包含风险代码，存在执行控制命令的行为，后台私自加载广告，静默安装、私自启动未知文件，造成用户手机流量消耗，存在安全隐患，建议删除。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 权限提升漏洞（CVE-2018-15967）	该漏洞影响 30.0.0.154 及更早版本的 Adobe Flash Player，成功利用该漏洞可能导致信息泄露。（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可能并推送广告。（威胁等级低）
		RiskWare[Downloader]/Win32.Kasinr	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）
		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，持有最基础特定性的恶意代码样本。（威胁等级中）
		GrayWare[AdWare]/Win32.IBryte	此威胁是一种广告类程序，该家族样本运行后连接远程服务器下载推广应用并安装，占用系统资源，影响用户使用。（威胁等级低）
		Trojan[Rootkit]/Boot.Cidox	此威胁是一种可以修改 MBR 并在系统与核之前加载的木马家族，该家族通常以正常的应用程序伪装，会监控网络流量和击键组合，在电脑中留下隐蔽的后门，并试图攻击局域网内的其他机器。（威胁等级高）

如何控制供应商风险：六步走

Jeff Rowley, Sara Laverick/ 文 安天技术公益翻译组 / 译

要想掌控公司面临的风险，你需要了解第三方供应商所带来的风险。

这听起来可能很简单，但是，除非你能够持续追踪第三方供应商，否则你就无法了解他们带来的网络安全和技术风险。

追踪供应商风险是一项艰巨的任务，需要付出大量的时间和资金，可能会超出公司的承受能力。但是，考虑到众多的网络安全威胁，以及各类关于网络风险和数据隐私的法规，密切关注供应商风险十分必要。

何为供应商风险

许多公司与第三方供应商合作，以实现关键业务功能并提高运营效率。然而，这些供应商可能是网络安全和技术风险的重要源头。

最近的报告表明，第三方数据泄露是最常见、代价最高的网络事件类型。对大型企业而言，发生事件后的平均恢复成本接近 123 万美元，而且这一数字正在以每年高达 35% 的比例增长。能够访问企业敏感数据的供应商（如金融服务公司、“软件即服务”[SaaS] 提供商和数据存储公司）可能会给企业带来严重的风险。

但是，在追踪和处理第三方供应商风险方面，许多公司仍然挣扎在分配必要的时间或资源上。因此，这些公司无法完全了解他们有多少供应商，或者他们暴露的数据量。Ponemon Institute 最近的一份报告显示，只有 33% 的公司会整理第三方供应商清单，并统计这些供应商可以访问的公司数据。

如何追踪供应商风险

控制供应商风险的关键是：保持完整的供应商风险追踪清单；其挑战在于：如何利用有限的时间和资源实现最好的效果。各公司可以通过以下六个措施来掌握供应商的情况，充分了解并控制他们带来的网络和技术风险。

1. 考虑到每个供应商

你可能拥有完整供应商的清单，或者部分供应商的清单。重要的是，要及时更新供应商清单，保持其完整性和全面性。与公司的会计部门以及负责采购的人员核实供应商信息——在清单中删除重复项或不再合作的供应商。要求所有部门主管列出他们使用的供应商，并确保他们给出的信息与清单中的信息是一致的。此外，在对供应商进行确认以及后续跟踪过程中，应该限制其直接在公司的系统中更新其信息的权限（这些信息包括但不限于其 logo、地址、产品、服务以及分支机构等）。

2. 集中管理供应商清单

公司应该集中管理供应商清单，并确保这些清单能够轻松访问。各公司可以指定专人来维护清单，由高层管理人员对其授权并在整个公司公示。此外，公司还可以根据需要使用专用的供应商管理技术解决方案。

3. 对供应商进行尽职调查

公司应对每个供应商的网络安全实践进行评估，确定这些安全实践是否与自己的一致。优先评估能够访问公司敏感数据或可能导致运营风险的供应商，包括其保护措施、事件响应计划、业务连续性计划等等。

4. 评估供应商风险

评估第三方供应商对公司的重要性或者其风险水平，可以用数值或者其他排名办法。让相关业务部门对供应商的重要性进行排名（例如，关键、重要、有用或多余）。让公司的网络安全团队（或者至少是 IT 团队）分析供应商的响应计划和尽职调查结果——注意不要让供应商自我审查。公正客观地对供应商进行排名，并及时更新。

5. 定期，持续地追踪和处理供应商风险

通过控制供应商风险来保护公司需要持续不断的努力，不可以“三天打鱼两天晒网”——例如，今天记录了供应商风险，以后就不再维护和更新了。控制供应商风险的关键是持续追踪和责任追溯。为了降低风险，请将供应商风险追踪作为一项常规工作。如果他们为公司提供关键服务，则增加追踪的频率。

6. 获取专业公司的帮助

就像你与供应商签订合同来处理专业任务一样，请考虑采用相同的策略来追踪供应商风险——可以将供应商管理外包给专门监控供应商、跟进其尽职调查的公司。这些公司拥有丰富的经验和专业知识，能够高效和有效地执行此类工作，从而节省你的时间、资金和精力。获取专业公司的帮助，是大幅降低网络安全和技术风险的好办法。

追踪供应商风险，保护公司安全

各公司都致力于降低其网络安全和技术风险，上述措施能够帮助他们牵制网络犯罪分子和其他不良行为者，避免由于违规而受到监管机构的处罚。

要想控制供应商风险，你首先需要了解第三方供应商所带来的风险。为此，请保持公司供应商的完整清单，不断更新和完善清单，并对其进行集中管理。此外，还需要对供应商风险进行排名，并跟进其尽职调查。各公司应该将追踪供应商风险作为一项常规性和持续性工作，或者将此类工作外包给专业公司。通过这些措施，公司可以控制供应商风险，保护自己的数据安全。

原文名称	Taking Control of Vendor Risk? A 6-Step Approach
作者简介	Jeff Rowley, Sara Lavenck。Jeff Rowley 和 Sara Laverick 是 ACA Aponix 公司的首席顾问。
原文信息	2018 年 10 月 24 日发布于 Information Week 原文地址 https://www.informationweek.com/strategic-cio/security-and-risk-strategy/taking-control-of-vendor-risk-a-6-step-approach/d/d-id/1333108

安天发布《Scarab 勒索病毒新变种分析报告》

安天捕风团队近期发现了 Scarab 的最新变种，其伪装成一个录屏软件，以此来绕过安全软件的检测。Scarab（圣甲虫）勒索病毒于 2017 年 6 月首次被发现，此后，有多个版本的变种陆续产生并被发现，其一般利用 Necurs 僵尸网络进行传播，但通过跟踪发现，近期的 Scarab 勒索病毒可以通过 RDP 爆破 + 人工、捆绑流氓软件的方式进行传播。

经分析发现，该变种从表面看是伪装成一个录屏软件，有详细的签名信息，可以截图快照，但是与多数病毒一样设置了自启动以及自删除功能，该功能给安全软件增加查杀难度，而且为保证数据不可恢复，该变种还进行了删除卷影的操作。它的危害性很大，一旦病毒感染某主机，便会杀掉多数的系统进程、应用进程，然后对文件夹进行遍历做加密动作，加密成功后弹出勒索信息。

样本运行后，首先会获取操作系统版本信息，启动子进程，进行持久化操作，复制自身到‘C:\Users\dell\AppData\Roaming’目录下并命名为 sevnz.exe，然后执行 sevnz.exe 对内存中相应字符串进行解密，之后通过执行 mshta.exe 来删除 sevnz.exe。然后主程序通过调用 mshta.exe 将相应的系统备份删除、磁盘卷影等操作命令行写入注册表项、遍历进程，如果发现相关进程则将相关进程结束，将内存解密出相应的加密字符串设置为注册表项，并在内存中解密生成相应的勒索信息和用户的加密 ID，然后遍历文件目录，加密相应的文件，并随机生成文件名，将加密之后的文件名后缀改为 .hitler。随后在加密文件的目录下会生成一个写有勒索信息的 txt 文档‘HOW TO RECOVER ENCRYPTED FILES’，之后屏幕上会弹出相应的勒索信息，包含用户 ID、联系邮箱以及货币购买地址。

勒索病毒给企业和个人的数据安全带来了严重的威胁，一旦主机被入侵，主机中的文件都有可能被锁，而且被锁文件将难以恢复，因此防护显得极为重要。在此，安天提醒广大互联网用户需安全、健康上网，安装杀毒、防毒软件（如：安天智甲工具）并及时升级系统和修补设备漏洞。

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。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

文件名	374F8ACCC92838939A6D3960AAB36AA0
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	844 KB
MD5	374F8ACCC92838939A6D3960AAB36AA0
病毒类型	木马程序
威胁名称	Trojan/Win32.Yakes
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=374F8ACCC92838939A6D3960AAB36AA0

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	附加信息	
延时	★★★	Sleeptime	0x0000EA60

常见行为

该文件具有以下行为：查找指定内核模块；创建特定窗体；获取计算机名；获取驱动器类型；获取驱动加载权限；读取自身；释放 PE 文件；复制自身；获得计算机用户名；打开自身进程文件；获取系统版本；查找窗口；独占模式打开，防止复制读取，防止杀毒软件扫描上报；获取指定套接字的一个本地 ip 地址；获取主机内存信息。

行为描述	危险等级
查找指定内核模块	★
创建特定窗体	★
获取计算机名	★
获取驱动器类型	★
获取驱动加载权限	★
读取自身	★★
释放 PE 文件	★★
复制自身	★★
获得计算机用户名	★
.....	.....

进程监控

PID	创建	命令行
1860	cmd.exe	"C:\WINDOWS\system32\cmd.exe" /c copy /y "C:\db2f09ef22a94ef3a34f5331a0649eab\share\target.exe" "C:\Documents and Settings\Administrator\Application Data\sevnz.exe"
2032	wuauclt.exe	"C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3dc]SUSDS902316e93b75a44e97e0a3a00fad9348