安天周观察

主办：安天　2016 年 3 月 28 日（总第 33 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

中国网络空间安全协会在京成立 安天当选首批常务理事单位

2016 年 3 月 25 日，由中央网络安全和信息化领导小组办公室领导创建，并由国务院批准同意成立的中国网络空间安全协会（CSAC），在北京举行成立大会暨第一届会员代表大会。网信办、工信部、公安部、民政部和互联网协会的领导及安天、奇虎 360、百度、阿里等企业代表出席了会议。

国家互联网信息办公室副主任王秀军出席大会并致辞，她对中国网络空间安全协会提出了 4 点希望，同时指出协会成立顺应了我国互联网行业和社会各界共同参与维护网络安全的愿望，对加强行业自律、促进行业健康发展、维护我国网络安全、加强网络安全国际交流合作将发挥积极作用。

大会现场审议通过协会章程、选举办法、会费缴纳管理办法，并选举产生了协会第一届理事会，安天当选为常务理事单位，安天技术负责人肖新光当选为协会副理事长，并作为企业代表在会上做了发言。

▲ 大会现场

通道的勒索软件当心以邮件为传播

安天再次提醒用户：

近期，在安天的每日安全资讯中，与勒索软件相关的新闻频繁出现，安天研究和跟踪多年的此类恶意代码也逐渐被更多的安全厂商和用户注意到，业界对于勒索软件的关注正在迅速升温。

安天最早从 2014 年开始全面跟踪此类恶意程序，并于 2015 年 8 月 3 日发布专题分析报告《揭开勒索软件的真面目》，详细地揭露了勒索软件的传播方式、勒索形式、历史演进以及相应的防御策略。而在 2015 年 12 月 4 日，我们又根据敲诈软件依托 JS 脚本进行邮件传播的新特点，跟进发布了《邮件发送 JS 脚本传播敲诈者木马的分析报告》，至今已经进行详细分析的报告为 4 篇，包括率先发现使用中文提示信息的 Locky 软件变种等等。安天 CERT 再次提醒用户，近期勒索软件越发猖獗，用户务必警惕这类恶意程序，特别是对其传播的重要入口——电子邮件，予以警惕，尽量选用可靠的安全软件进行防范，安天引擎和全线企业级安全产品已经支持勒索软件的检出，并已经针对用户进行了升级服务，安天更针对邮件服务商推出 SDK 级别解决方案。

（相关分析报告请详见安天微信公众号“勒索软件”专题，防范方式请见三版）

报评

承担责任，保护网络空间安全

网络安全企业是网络安全产品和技术的研发服务载体，网络安全产业是网络安全技术发展和创新的迭代动力。而从网络安全到网络空间安全，这是一个安全境界上的巨大飞跃。安天人的学习感受与理解总结起来有以下三点。

一、完善网络空间风险认知、建立总体安全观

当前包括中国在内的全球主要国家，都面临着网络空间安全领域的内外部挑战。“网络地下经济”、“网络恐怖主义”等带来的社会治理压力空前。网络空间更是激烈的短兵相接，从“方程式”、“APT-TOCS”、“Hangover”等事件中，我们看到中国面临着来自不同方向，不同能力层次的网络攻击。这些安全威胁的表现不再是传统的“网站涂鸦”、“盗号侵财”，而是信息战的战场预置、是情报获取的持续通道，呈现出高度隐蔽、难以感知、后果严重的特点。

在“互联网 +”全面拉动盘活我国基础产业潜力的同时，也在加剧网络安全风险与传统安全风险的合流趋势。高级攻击、复合化攻击将成为常态，重要信息系统和关键基础设施都会遭遇到更为严峻的挑战。“乌克兰遭遇攻击大面积停电”、“孟加拉央行被盗”等事件，都成为我们的前车之鉴。

二、科学评价产业力量、坚决承担产业责任

在中国网络空间安全的产业层次中，既有国家队、也有大量民营企业；既有已经上市的规模企业代表、也不乏个性企业

（下转第四版）

每周安全事件

类 型	内 容
中文标题	赛门铁克 SEP 系统存在的一系列安全漏洞
英文标题	Symantec warns of serious security holes – in Symantec security kit
作者及单位	Shaun Nichols；The Register
内容概述	赛门铁克 SEP 是一款基于 WEB 门户的管理系统，你可以通过网络或本机的 SEP 管理服务系统登录到控制台，然而该系统却存在两个漏洞，跨脚本漏洞 (XSS) 和 SQL 注入漏洞。由于程序系统设计的问题，有两处均可被已登录用户利用来提升用户控制权限。另外一个系统 bug 存在于 SEP 的驱动文件 SysPlant.sys 中，该 bug 可被利用来绕过 SEP 的安全控制防护，该防护功能本来是用于防止用户电脑上恶意代码的运行，因为驱动文件不能感知到恶意代码的存在，恶意代码便可在机器上快速运行，一击致命。
链接地址	http://www.theregister.co.uk/2016/03/18/serious_security_holes_in_symantec_security/

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 5 个 PC 平台恶意代码值得关注

平台分类	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.Vhist.a[prv,exp] 2016-03-21	该程序开机自启、监听收件箱，拦截指定短信，并将信箱信息上传到远程服务器，建议立即卸载避免造成隐私泄露。（威胁等级高）
		Trojan/Android.viptrack.a[prv,exp,rmt] 2016-03-21	该程序为国外一款定位跟踪的监控软件，程序运行会请求激活设备管理器，隐藏图标，监听短信，拦截包含指定指令的短信，根据短信指令内容执行开启或关闭监控等行为，获取用户的位置信息上传到远程服务器并发送到指定号码，造成用户隐私泄露和资费消耗。（威胁等级高）
		Tool/Android.shadowtracker.a[prv,rmt,fra] 2016-03-23	该程序为一款工具类软件，主要功能为监听短信指令，开启 GPS，更新地理位置，以邮件方式上传地理位信息，若非本人安装请及时卸载。（威胁等级低）
		Trojan/Android.Fakeqhmkiller.a[prv,fra] 2016-03-23	该应用伪装成 360 手机急救箱，运行会隐藏图标；后台私自下载未知文件；上传手机信息；拦截屏蔽并删除短信；上传指定短信；检索安全软件；后台发送短信；静默安装 apk。造成用户隐私泄露，资费消耗。（威胁等级中）
	较为活跃的样本	Trojan/Android.chksms.c[prv,rmt]	该程序伪装成系统服务，运行后隐藏图标并后台上传信箱信息，接收短信指令上传位置信息，建议立即卸载，避免造成隐私泄露。（威胁等级高）
		Trojan/Android.ilfsmsgpspy.b[prv]	该程序伪装系统应用，安装运行后台私自上传用户输入的 user_key，窃取并上传用户接收到的短信到远程服务器，造成用户隐私泄露。（威胁等级高）
		Trojan/Android.emial.cy[prv,exp]	该程序伪装成正常应用，安装后运行隐藏桌面图标，后台发送短信，拦截并转发短信，造成用户隐私泄露，资费消耗，建议卸载该应用。（威胁等级中）
		Trojan/Android.kaka.g[prv,rmt]	该程序会伪装 Google 应用，开机自启动，后台私自上传设备信息及本机号码，拦截屏蔽短信并上传，诱导激活设备管理器并阻止取消激活，致使无法正常卸载，诱导用户输入银行账户信息并上传输入的信用卡卡号及 cvv，具有网络远程控制行为，造成用户隐私泄露，资费消耗，建议卸载该应用。（威胁等级中）
		G-Ware/Android.jianmo.x[rog,sys]	该程序伪装成刷会员的应用，强制置顶界面，勒索用户并指定 QQ 解锁，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	WebDAV 本地提权漏洞（CVE-2016-0051）	该漏洞存在于 Microsoft Web 分布式创作和版本管理 (WebDAV) 中，如果 Microsoft Web 分布式创作和版本管理 (WebDAV) 客户端验证输入不当，其中就会存在特权提升漏洞。成功利用此漏洞的攻击者可以使用提升的特权执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/JS.JScript	此威胁是一种具有下载行为的木马类程序，运行该脚本后会执行里面的代码，链接网络下载恶意文件，通常以网页挂马和邮件进行传播。（威胁等级中）
		Trojan[Downloader]/Win32.Delf	此威胁是一种使用 delphi 语言编写具有下载行为的木马类程序，运行后会连接网络并下载其他恶意程序执行，通过以邮件、挂马、捆绑正常软件来进行传播。（威胁等级中）
		GrayWare[AdWare]/Win32.BrainInst	此威胁是一种广告行为的广告软件类程序，会在未经同意的情况下下载并安装多个程序，如 IE 搜索条，推广的软件等程序。（威胁等级低）
		Trojan[Downloader]/Win32.VB	此威胁是一种以 VB 语言开发的，具有下载功能的木马类程序。该家族程序会在系统启动时自动运行，通常是从网页中下载或是捆绑正常程序，这种类型的恶意代码通常会在用户访问具有漏洞的网站时感染计算机。（威胁等级中）

勒索者病毒借助邮件疯狂传播，安天提出面向邮件服务商的反病毒引擎

电子邮件是具有高度定向性的信息攻击入口。而最近几年，又一种重要的恶意代码安全威胁随同邮件疯狂传播，那就是勒索软件。此类恶意代码以邮件附件传播，被用户执行后，加密用户数据文件，必须通过难以追踪的匿名网络缴纳比特币才能解密，一旦用户不能交纳费用，就会造成不可逆的严重损失。

为此安天依托 AVL SDK 反病毒引擎，提供面向公共邮件服务商和邮件建站工具开发商的有效解决方案。

方案

安天 AVL SDK 反病毒引擎邮件服务解决方案，通过邮件服务的开发者调度引擎接口进行工作，无需采购任何安全设备，对用户提交的对象进行本地化检测，用户只需有应用开发经验，无需对安全有任何了解，即可实现引擎嵌入，而检测能力的升级、病毒库的维护完全由安天进行。

安天 AVL SDK 反病毒引擎邮件服务解决方案，对用户提交的邮件对象提供是否安全、威胁名称、威胁等级等信息，安天辅助用户根据自身需求，根据相关信息对相关邮件进行删除、隔离、更名、通知等处理。

AVL SDK for Network 引擎说明

安天邮件服务恶意代码解决方案是对安天反病毒引擎 AVL SDK for Network 的邮件场景封装，安天依托长期传统恶意代码检测研究底蕴开发，具有全平台能力的本地化检测引擎，全球有 30 家以上的安全厂商、通讯厂商和手机厂商选择安天作为病毒检测合作伙伴，安天反病毒引擎为接近 10 万台防火墙和超过 1 亿部手机提供病毒检测服务。

该引擎提供了文件级别（包括对文件对象、扇区对象、内存对象）、流级别和包级别的病毒检测能力，AVL SDK 采用纯 C/C++ 编写，具有极好的移植性，目前已经有 Linux、Windows 等多个平台版本，并支持 X86、ARM、MIPS（含 Cavium）等体系架构，可以与防火墙、UTM、IPS 以及各种主机和应用环境结合，进行基于网络和主机的病毒检测。

（请邮件联系我们获取更多技术和产品支持：avlnetwork@antiy.com）

AVL SDK 引擎技术特点	
全规则高速引擎	可使用海量的本地病毒库，具有百万条高质量病毒特征，检测数千万个病毒样本； 检测速度极快，约为其他引擎产品的 2–5 倍。
全方位病毒检测	可检测蠕虫、病毒、木马、黑客工具、流氓软件、风险程序等各种类型恶意代码；
跨平台可移植性	支持 POSIX 标准； 适用于各类系统平台（如 Windows、Linux）； 可用于硬件平台（如 Intel、Arm、X86、MIPS、嵌入式）中。
版本灵活可定制	根据应用场景、硬件平台、操作系统、内存存储及计算能力的不同需求可定制不同的引擎版本。
操作简单易集成	简单调用接口即可使产品具有反病毒能力； 将待测对象传给 AVL 引擎即可得到详细检测结论。

安天智甲终端防御系统可查检勒索软件

安天智甲终端防御系统是专为企业、政府、机构等业务网络研发的终端威胁安全防护产品。该产品采用安天独立自主研发的反病毒引擎，在智甲产品中形成了一套独有的针对勒索软件及变种家族的检测、防御和阻断方法，可帮助企业用户免受勒索软件骚扰。

安天智甲产品特点

独立基线

用户网络千差万别，每个网络中都存在特定的业务和办公系统，其组成文件一般很少会存在安全厂商的白名单中，其他产品的黑名单也只能引用外部通用积累，难以针对企业用户自身使用场景变化。安天智甲支持设置全网安全基线，通过基线保障网内设备安全运行。支持多级基线设置，管理粒度可达单主机独立安全基线，坚固安全性与终端使用的灵活性。

四级策略

安天智甲提供用户终端的分级管理机制，可根据终端的使用范围、管理要求和承载的信息价值不同，设定不同的运行监控策略。典型应用是设置开放、审计、重要和受限终端或区域，执行不同的策略，搭配基线管理，使每个终端都在业务流畅性 & 安全性上达成最佳效果。

全方位阻止勒索软件

比特币的不可追踪使勒索软件在全球范围快速的传播，由于一般采用超长加密技术破解成本远超赎金，中招者只能支付赎金或者忍痛丢弃电脑中所有重要文件。智甲拥有专门针对勒索软件的从检测、预警到阻断的整套保护机制。安天智甲的检测和防护既关注了勒索软件的入口（邮件、网页访问、即时通讯软件等），也能够预警勒索软件的启动和运行，保护用户终端不被加密。

全网追溯，定点清除

智甲通过反病毒引擎和内置高级威胁库，可在全网追溯病毒和高级威胁。智甲内置已知高级威胁特征库，当有新的高级威胁事件爆发时，用户可全网追溯检查自身网内是否存在事件相关威胁，在 10+ 分钟完成数千台主机的威胁追查，并可通过管理端进行定点清除，管理员可以对这些病毒进行远程“定点清除”，无需进行既占资源又耗时的全盘扫描。

可疑文件动态行为分析

智甲在传统反病毒引擎检测的基础上，能够提供针对文件的多维静态分析能力，采用硬件虚拟技术模拟真实环境对文件行为进行动态分析，发现文档攻击、0day 漏洞、免杀木马、最新勒索病毒等未知威胁。

国产操作系统安全防护

智甲不仅支持传统的 Windows、Linux 等系统防护，同样提供对多种国产操作系统（麒麟、方德等）场景下的病毒扫描和实时监控功能，并支持国产龙芯等 CPU。

产品部署

智甲部署灵活，适用于多种网络环境。为满足大型网络部署需求，智甲支持分布式部署和集群扩展。

安天发布《首起利用网络蠕虫的 APT 攻击——BuhtrapWorm》

近日，安天追影小组发现了一起利用网络蠕虫针对银行的 APT 攻击，从 2015 年 8 月到 2016 年 2 月为止，黑客组织 Buhtrap 针对俄罗斯银行成功发起了 13 次攻击，共计窃取资金 18 亿卢布（约合 2740 美元），最多的一次窃取了 6 亿卢布（约合 880 万美元），最少的一次也高达 2560 万卢布（约合 37 万美元），这还并未包括对乌克兰的攻击造成的损失。

据调查，Buhtrap 早期与大多数黑客组织一样，使用邮件钓鱼、检查系统环境、创建远程连接的方式来实现攻击。但近期，新型的 Buhtrap 被曝光，它通过网络蠕虫的方式来感染整个内部网络，这种方法有效地增加了从网络终端删除恶意程序的难度。

在感染一台新的计算机之后，恶意软件会用相同的方式进行传播。如果公司内部网络中出现了一台被 BuhtrapWorm 感染的机器，其他所有计算机都会被反复感染。因此，仅仅只需要几分钟，它就可以在企业内部创建一个僵尸网络。

具体的攻击步骤如下：

1. 初始入侵公司内部网络后，攻击者使用远程控制软件安装和启动主模块，该模块负责为木马提供生存能力和银行内部主机的多重感染。

2. 黑客采用改良版的 Mimiikatz 来收集域账户凭据。

3. 恶意软件搜索安装了 AWS CBC 软件的系统。

4. 一旦得以访问 AWS CBC ，该恶意软件就伪造付款单据发送给中央银行。

5. 感染导致银行的基础工作站瘫痪，无法从中搜索相关证据。

目前的杀毒软件只能检测 launcher 本身是没有威胁的，此外 Buhtrap 删除文件时并不会删除恶意文件，因此恶意软件会大量存储在受感染的主机中。

2016 年 2 月 5 日，Buhtrap 源码在地下论坛“exploit.in”被公布，作者声称自己是 Buhtrap 一员，但是没有得到开发报酬，因此决定公布恶意软件的所有源码。Buthtrap 的开源必定会导致更多相似恶意程序的诞生以及更多类似攻击事件的发生，安天提醒相关机构要注意防范，在发现异常的第一时间将情况交由专业安全人员处理。

木马程序

安天【追影高级持续威胁分析系统】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：

文件被网络威胁感知类设备发现，经由 BD 静态分析鉴定器、YARA 自定义规则鉴定器、可交换信息 (EXIF) 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。

暂时依据 BD 静态分析鉴定器、动态行为鉴定器、智能学习鉴定器将文件判定为高级威胁，正在等待美国软件交叉索引 (NSRL) 鉴定器进行分析。

该文件具有以下行为：利用漏洞释放 PE 文件；打开自身进程文件；创建互斥体 (mutex)；隐藏文件；获取计算机名称；创建特定窗体；释放 PE 文件；获取驱动器类型；获取系统内存；查找特定窗体；请求加载驱动的权限；获取主机用户名称。

同时，该文件利用了 CVE-2012-0158 漏洞。

文件名	2DD786157BC8A6618BAD11CB50E46EC4
文件类型	Document/Microsoft.RTF[:Rich Text Format]
大小	595 KB
MD5	2DD786157BC8A6618BAD11CB50E46EC4
病毒类型	高级威胁
恶意判定 / 病毒名称	Trojan[Exploit]/Win32.CVE-2012-0158.CJ
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=2DD786157BC8A6618BAD11CB50E46EC4

◆ 危险行为

行为描述	危险等级
利用漏洞释放 PE 文件	★★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
打开自身进程文件	★	获取主机用户名称	★
创建互斥体 (mutex)	★	获取系统内存	★★
隐藏文件	★★	查找特定窗体	★
获取计算机名称	★	请求加载驱动的权限	★
创建特定窗体	★	获取驱动器类型	★
释放 PE 文件	★		

（上接第一版）

和新锐创业团队，百花齐放，百家争鸣。在我国在基础信息技术相对落后的大背景下，更需要网络安全产业成为数字立国的盾甲、网络强国的保障。

三、直面压力和挑战、把握大时代的使命与机遇

中国网络安全产业在取得不断进步的同时，也面临着严峻的困难与挑战。但我们坚信发展的问题终究要靠发展解决，我国对网络空间安全日趋重视，随着网络安全技术在网络强国路径上发挥更大的屏障价值，网络安全市场将逐步呈现出“用户觉醒、需求激活”的气象；随着我国在“一带一路”等战略中的全球进取，安全防护需求也会不断外延，中国网络安全产业也必将在全球化道路上结出果实。

作为网安产业人，我们要许下这样的誓言：我们以用户需求为引导，以解决用户安全威胁为己任。我们有为用户创造安全新境界的勇气，我们有为大国网络空间铸盾的信心。在“没有网络空间安全就没有国家安全”的大时代，我们将承担责任，奏响强音。

（本文根据安天技术负责人在中国网络空间安全协会成立大会发言整理）