安天周观察

主办：安天　2016 年 10 月 24 日（总第 61 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加“新时代云安全创新策略高层研讨会”并发表演讲

10 月 21 日，由信息安全与通信保密杂志主办、山石网科承办、中国计算协会计算机安全专委会协办的以“云起苏州，共话安全”为主题的新时代云安全创新策略高层研讨会在苏州举行。来自全国网络安全领域的主管、专家学者、行业精英等齐聚一堂，就云计算时代下的网络安全策略展开深入交流和探讨。

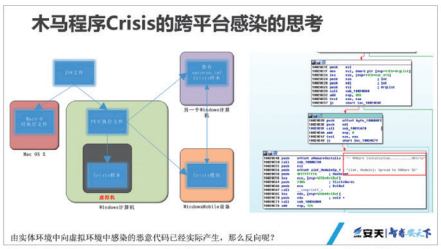
本次会议由中国计算机学会安全专委会严明主任主持。倪光南院士和来自人民银行、全国信安标委、公安部等各机构的专家分别就云安全政策解读、理论、标准、等级保护、技术创新等方面的的问题进行了解读。

安天首席技术架构师肖新光做了题为《虚拟化场景下的恶意代码威胁与防御》的大会报告，报告指出恶意代码在针对关键基础设施攻击中发挥着致命的作用，APT 攻击中的恶意代码工程规模不断膨胀，商用攻击平台 + 恶意代码为核心的军火扩散也已开始影响整个地区平衡。云计算作为重要的信息基础设施，云中的世界很不安宁，安天在云中部署的蜜罐，相比传统蜜罐，感知到的攻击更为频繁。在安天部署的蜜罐中可以发现，来自境内的 IP 地址针对云中主机的扫描攻击中，一半以上来自云内部。报告介绍了恶意代码在各种 Server 平台的现状，分析了不同攻击者的攻击意图与路径和使用不同类型恶意代码的情况。

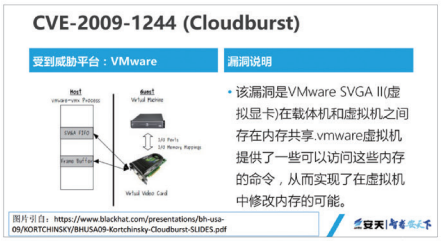
报告摘录：对云中服务节点攻击的目的、路径和可能出现的恶意代码

报告还介绍了被称为云服务梦魇的虚拟化逃逸威胁，并解读了其中两个例子。

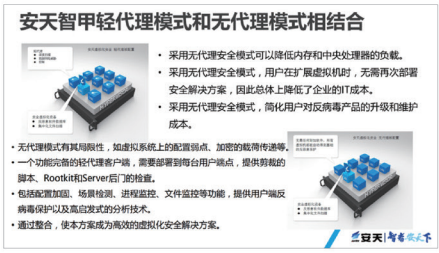
肖新光介绍了安天在虚拟化安全方面的工作。安天智甲终端防御系统在去年年底已经发布了虚拟化版本，针对云中的主机改善了配置加固、场景检测、进程监控、文件监控等功能，通过轻代理模式和无代理模式相结合，有效解决了应对传统主机防护软件在云中部署所存在的内存消耗、扫描风暴、带宽占用等问题。安天以全域融合防御为思路，为客户定制态势感知与监控预警平台，从而实现对云中的与传统 IT 网络中的资产与威胁的统一管理。



报告摘录：对木马程序 Crisis 的跨平台感染的思考



报告摘录：对 Cloudburst 虚拟机逃逸漏洞的介绍



报告摘录：安天智甲的无代理模式和轻代理模式结合

一周简讯

- 安全厂商溯源 PHP 勒索软件 JapanLocker 作者
- 研究人员发现 Skype 通话期间击键可被窃听
- 物联网新威胁：Hajime 蠕虫比 Mirai 更复杂
- 研究人员发现利用硬件漏洞绕过 ASLR 方法
- Ollydbg 插件 StrongOD 存在中间人攻击漏洞
- 安全专家称亚太地区在线金融威胁增加
- 黑客仿冒 Gmail 安全更新入侵 DNC 邮件系统
- 最新木马 Acecard 分分钟窃取用户信息
- D-Link DWR-932B LTE 路由器中发现多个后门

（安天 CERT 搜集整理，详见：http://bbs.antiy.cn）

MongoDB 再出安全事故，5800 万商业用户信息泄露

近日，知名数据库及数据存储服务提供商 MBS，遭到黑客攻击。其 MongoDB 数据库由于缺乏有效的安全保护措施，5800 万商业用户的重要信息泄露，包括名称、IP 地址、邮件账号、职业、车辆数据、出生日期等信息。黑客通过物联网搜索引擎 Shodan 找到的这些未受保护的数据库，但却没有选择通知相关企业，而是把这些信息公布了出来。

经网络安全公司检测，数据库中的数据表的前缀是“hw_”，而 Hardweel 是 MBS 实施数据管理服务的主要程序。

目前尚未发现 Hardweel 的用户信息遭泄露。

（文章来源：http://www.cnnvd.org.cn/news/show/id/7772）

每周安全事件

类 型	内 容
中文标题	恶意代码利用隐写方式盗取信用卡信息
英文标题	Magento Malware Uses Steganography to Steal Payment Card Data
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，黑客入侵使用 Magento(一套专业开源的电子商务系统) 的电商以收集银行卡数据，他们将窃取的数据隐藏在 JPG 图片中，以便神不知鬼不觉的从被感染的电商下载图片。在过去的一年中，攻击者已经将其攻击目标转向了在线电子商务平台。他们发现这是一个收集信用卡数据的沃土，多数情况下，他们会将所获取的数据在地下黑客论坛中出售。 据外媒报道，目前超过 5700 家网站感染了恶意软件，其中超 100 家网站感染的是近日被发现的 MageCart 恶意软件。近几个月来，入侵电子商务网站已经成为了黑客入侵的常见手法。
链接地址	http://news.softpedia.com/news/magento-malware-uses-steganography-to-steal-payment-card-data-509388.shtml

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

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.Vnapstore.a[rog, exp]2016-10-17	该应用开机后自动启动，会诱导激活设备管理器，私自下载虚假应用，并诱导用户安装，实际是用于推送广告，建议立即卸载，避免造成资费损耗。(威胁等级高)
		Trojan/Android.vada.a[exp] 2016-10-19	该应用运行后会私自发送注册短信，联网下载更新，会监听短信并获取短信内容，若短信内容包含指定网址则访问该网址下载 apk 文件，造成用户资费消耗。(威胁等级中)
		Trojan/Android.Meuspy.a[prv, rmt]2016-10-20	该应用是间谍程序，运行后会请求设备管理器，获取 root 权限，隐藏图标，并请求指定网站获取远程指令，根据指令监听联系人信息，通话记录，短信，录音，WhatsApp 数据，建议立即卸载。(威胁等级中)
		Trojan/Android.FakeFlashPlayer.q[prv, rog]2016-10-20	该应用会伪装成 FlashPlayer，程序运行后会请求激活设备管理器，联网上传用户手机号码，并弹窗显示虚假界面，诱骗用户输入姓名和身份证号信息进行联网上传，监听短信拦截短信并联网上传短信信息，造成用户隐私泄露。(威胁等级高)
	较为活跃的样本	Trojan/Android.E4AQQspy.j[prv]	该应用会伪装 QQ 刷钻工具，诱导用户输入 QQ 账号密码，并通过短信转发，建议立即卸载，避免隐私泄露。(威胁等级中)
		Trojan/Android.emial.dj[prv，exp]	该应用程序运行后会请求激活设备管理器，隐藏图标，获取用户设备固件信息和短信信息发送到指定号码、联网上传并发送到指定邮箱，监听短信拦截短信，获取短信信息转发到指定号码、联网上传和发送到指定邮箱。(威胁等级高)
		Trojan/Android.emial.di[prv，rmt，rog，exp]	该应用会伪装成中国移动，程序运行后会请求激活设备管理器，隐藏图标，获取用户短信信息上传到指定邮箱。会监听短信获取短信信息发送到远控号码并上传到指定邮箱，会执行锁机、短信群发、向指定号码发送指定内容短信等行为，造成用户资费消耗，建议卸载。(威胁等级高)
		Trojan/Android.Downloader.ck[rog，exp]	该应用运行后会私自下载非恶意应用，频繁推送广告，安装桌面快捷方式图标，造成用户资费消耗。(威胁等级高)
		G-Ware/Android.jianmo.as[rog，sys]	该应用会伪装成黑客工具，置顶界面勒索用户添加指定 QQ 进行付费解锁，造成用户金钱损失，建议不要安装。(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 Office CVE-2015-2545 Remote Code Execution Vulnerability	Microsoft Office 容易出现远程代码执行漏洞。攻击者可以利用此问题在受影响的应用程序的上下文中执行任意代码。尝试漏洞失败可能会导致拒绝服务攻击。(威胁等级高)
	较为活跃的样本	RiskWare[Downloader]/Win32.AdLoad	此威胁是一种具有下载广告软件的风险软件类程序。该家族可以入侵用户系统；窃取重要数据，同时在被感染的电脑中安装恶意软件，使用户的电脑性能变慢。(威胁等级中)
		Trojan[Dropper]/Win32.VB	此威胁是一种使用 VB 编写的捆绑类木马程序。该家族通过与正常软件捆绑在一起，或由捆绑生成器生成捆绑文件等方式进行传播。(威胁等级中)
		Trojan/Win32.Bublik	此威胁是一种以窃取用户敏感信息为目的木马类程序。该家族样本运行后，会安装恶意浏览器工具栏和扩展工具，引起搜索结果重定向等问题。该家族通过电子邮件或捆绑安装等方式进行传播。(威胁等级中)

使用大数据实现智能企业安全

Dale Kim / 文　安天公益翻译小组 / 译

近年来，几乎所有行业都受大数据的影响，网络安全行业当然也不例外。最近的一项 MarketsandMarkets 研究预测，网络安全分析市场将从 2016 年的 28.3 亿美元增长到 2021 年的 93.8 亿美元，复合年增长率为 27.1%。这种巨大的增长是比较好理解的。随着攻击环境变得越来越复杂，资金越来越丰富，许多最危险和潜在危险的威胁需要深入了解企业的数据、网络和检测方法。

多年来，我们听到很多安全研究人员哀叹传统的网络安全方法，这些方法无法有效应对复杂的、无所不在的网络威胁。虽然一些企业可能具有警告异常事件的系统，但是许多黑客现在领先他们一步。

传统解决方案数据过载

例如，一些传统解决方案能够识别出对同一账户和来自相同 IP 地址的多次失败登录尝试，并生成潜在“可疑活动”的警报。或者，如果它在正常工作时间之外发现了某个账户的过度数据访问，它也可能发送警报。但是黑客意识到这些解决方案使用该模式，他们正在调整方法来规避这些方法。

此外，传统的安全解决方案往往无法处理庞大的数据量，这是企业不断增长的网络和网络边界的关键点。非结构化数据不适合预定义的数据模型，并且不以预定义的方式组织，是迄今为止被访问和使用的增长最快的数据类型，并且一次性摄入太多也会阻塞系统。

采用安全分析方法

大数据解决方案现在可用于安全分析，每秒捕获、过滤和分析数百万的网络事件。这些解决方案处理各种来源的数据，如审计和日志文件，以及非结构化数据 (包括电子邮件，社交媒体，图像，视频，新闻源等)。

国际数据分析研究所 (International Institute of Analytics) 预测，安全分析将与文本挖掘、机器学习和本体建模一起成为“第一道防线”，嗅探安全威胁。毫无疑问，未来几年综合安全性方法对这一点的需求将会增加。事实上，大数据分析市场在 2015 年达到 1250 亿美元，这并不奇怪。

但是为了成功部署安全分析以满足当今威胁形势的要求，企业必须保留大规模分析所需的大量数据。对整个基础设施和网络的所有活动实现最佳可视性至关重要，这使得企业能够通过自动化、可操作的情报来发现潜在的恶意异常行为。

开始行动

对于长期依赖现成的传统安全解决方案的企业来说，毫无疑问，将大数据安全分析融入防御系统是很复杂的。

以下是几个建议：

1. 确保部署的数据平台非常注重授权、身份验证和数据保护功能，以保护收集的所有数据。对于跟踪数据访问和追溯数据泄露来说，审查也至关重要。

2. 传统数据平台不能以干净和高效的方式处理非结构化数据，因此，希望部署大数据安全分析的企业选择一个平台，使他们能够以可扩展的方式在该平台上应用各种各样的分析工具。企业应该考虑部署最新的大数据工具的解决方案，以帮助他们更全面地了解环境中的潜在威胁。

3. 组织内部资源可以方便大数据安全分析。公司应确保他们的 IT 安全分析师和数据科学家定期会谈，以确保他们同步最佳方法，发展应对新威胁的安全平台。

在当今的威胁环境中，预测攻击和识别系统中的漏洞是至关重要的。事实上，认为一个现成的解决方案可以提供企业需要的全面保护未免太过天真，可能会造成灾难性的后果。

各个行业的企业使用大数据生成了价值，他们还应考虑使用此技术保护其当前客户和资产，以应对日益增长的网络威胁。

努力保护网络的企业必须超越传统的安全解决方案，在融合的数据平台上部署大规模的、高级分析方法，结合异常检测和机器学习，在打击网络犯罪的斗争中提供先机。

原文名称	Using Big Data for intelligent enterprise security
作者简介	Dale Kim，MapR Technologies 公司行业解决方案高级总监。
原文信息	2016 年 10 月 4 日发布于 Help Net Security, 原文地址 https://www.helpnetsecurity.com/2016/10/04/big-data-intelligent-enterprise-security/
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《Hangover 利用合法空间进行通信样本分析报告》

近日，安天追影小组在整理网络安全事件时，发现了“Hangover”家族的木马变种，并对其进行了简要的分析。以下简称发现的变种为“Hangover 变种 1”和“Hangover 变种 2”，其均采用合法的 web 服务，以代替 DNS 查找检索 C&C 地址，该方法使得攻击者的通信在众多合法的服务流量中，难以被发现。

安天追影小组，针对“Hangover 变种 1”和“Hangover 变种 2”的两个样本进行分析。

当攻击目标被感染后，不会像传统僵尸网络中的僵尸主机一样直接连接 C&C 服务器，而是请求一个合法的地址间接获取 C&C，较为常见的是 Yahoo 和 Quora 的问答页面。

“Hangover 变种 1”样本在请求的页面中，查找检索 C&C 地址。经过分析，发现在样本的源代码中，包含一个简单查找表。查找表的起始为开始和结束标记的词组，之后为 255 个单词，每一个都对应一个编号。通过这个查找表，可将开始标记和结束标记之间的关键字转化为 C&C 地址。而“Hangover 变种 2”样本，通常打包在一个可自解压的文件中，并伪装成一个 PPT 文件。“Hangover 变种 2”与 Hangover 变种 1”的区别，最主要在于，“Hangover 变种 2”中存在一个自定义的混淆方案，并且在请求的页面中，无法找到任何明显的标记词组。“Hangover 变种 2”样本将页面中的一些关键字，匹配存在于源代码中的查找表，将匹配到的字符串转化为数字，从而得到一个 C&C 地址。使得合法页面上的内容，可以重复被攻击者利用。因此，通过分析可以发现两个变种的行为非常类似，使用相似的技术获取 C&C 地址，通过请求合法 web 服务逃避传统阻止机制。

经以上分析，安天追影小组认为，攻击者逃避传统检测机制的技术在不断变化，受害者对此防不胜防。为了避免此类的攻击，安天追影小组提醒广大网络用户，加强网络安全意识，不要随意点击不明的链接，面对来源不明的邮件时，不要轻易去下载其中的附件，并及时更新所使用的软件等。

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、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 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 BD 静态分析鉴定器、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：获取系统版本、获取主机用户名称、访问文件尾部、篡改系统文件创建时间、连接特殊 URL、自启动、获取 socket 本地名称、连接网络、增加 run 自启动项、独占打开文件、获取系统内存、获取计算机名称。

文件名	5FC8AF63B2A1872B2E250CEF1649CDB3
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	296 KB
MD5	5FC8AF63B2A1872B2E250CEF1649CDB3
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Hangover.a
判定依据	BD 静态分析

◆ 运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认，IE6，Office 2007，Flash，WPS，FoxitReader，Adobe Reader

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取系统版本	★★	获取主机用户名称	★
访问文件尾部	★	篡改系统文件创建时间	★★
连接特殊 URL	★	自启动	★
连接网络	★	获取 socket 本地名称	★
独占打开文件	★	增加 run 自启动项	★
获取系统内存	★★	获取计算机名称	★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=5FC8AF63B2A1872B2E250CEF1649CDB3