安天周观察

主办：安天　2016 年 8 月 8 日（总第 51 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

国家信息安全测评中心主任朱胜涛一行莅临安天总部参观指导

8 月 5 日，国家信息安全测评中心朱胜涛主任一行七人莅临安天哈尔滨总部参观指导，并听取了安天发展近况汇报。

在安天一楼展示厅里，安天负责人介绍了安天近期发展情况，包括公司的发展目标、定位、团队能力储备及主要产品方案体系等。展示了安天反病毒等领域的核心技术积累和高级威胁检测和态势感知产品线。介绍了国内网络威胁疫情趋势和遭受网络攻击威胁情况的分布。

目前安天已经形成了由网络侧“探海”威胁检测系统、主机侧“智甲”终端防御系统、“镇关”威胁阻断系统和追影威胁分析系统组成的体系化的威胁检测防护解决方案。并通过态势感知与监控预警平台对感知、分析产品的统一管理与业务分析形成服务行业、地区级用户的整体能力。

在安天安全研究与应急处理中心，安天负责人结合安天捕获分析的 APT-TOCS、白象等境外组织对境内进行 APT 攻击事件汇报了安天在高级威胁分析、溯源方面的相关工作。

朱胜涛主任对安天所取得的技术成果给与了肯定，并积极评价了安天长期在非常艰苦的条件下，脚踏实地、坚持专注自主创新核心安全技术研发的的工作精神。希望安天抓住历史机遇，快速对接用户需求，加速自身发展。测评中心外联处、在线评估处、科技处、创新中心等处室负责同志和安天主要研发、研究部门负责人进行了深入的沟通交流。

安天移动安全公司 (AVL Team) 携“移动威胁情报平台”亮相 2016 黑帽大会

美国时间 2016 年 8 月 3 日，著名的美国黑帽大会 (Black Hat USA 2016) 在拉斯维加斯拉开帷幕，来自世界各地的信息安全专家、黑客、政府人员、安全厂商齐聚一堂，共同分享最新的网络安全技术资讯、攻防手法以及网络安全产品与方案。

位于走廊中人气爆棚的 Arsenal 展区，可谓是一个安全工具的小型盛会。一个展台，一个屏幕，一腔热情，在 Arsenal 展区，安天移动安全公司 (AVL Team) 主要展示了安天移动威胁情报平台 AVL Insight，它主要用于呈现移动威胁的高价值情报信息，通过对移动威胁的全面感知能力和快速分析响应能力，提供应对移动威胁的预警和处置策略。该平台

旨在提高银行、政府等大型机构对威胁事件的感知、预警、预防、取证、响应和处置能力，以达到降低 IT 安全成本，提高资产和信息安全保障的最终目的。

安天荣获『2015-2016 年度国家网络安全信息通报工作优秀技术支持单位』称号

近日，由公安部第十一局、国家网络与信息安全信息通报中心主办的“2016 年国家信息通报机制技术支持工作会议”在北京召开。

国家计算机网络应急技术处理中心、公安部第一研究所、公安部第三研究所、国家计算机病毒应急处理中心、中国科学院软件研究所、国家计算机网络入侵防范中心、安天等 12 家机构或单位获得“2015 年度优秀技术支持单位”称号。这也是安天继 2015 年获得“国家网络与信息安全信息通报机制技术支持先进单位”称号后，于今年再次获“国家网络安全信息通报工作优秀技术支持单位”的殊荣。

大会分析总结了上一年度信息通报技术支持工作并通报网络安全形势，部署下阶段重要网络安全支持工作，并宣布了入围第四批信息通报机制技术支持单位的企业名单。

迄今为止，国家网络与信息安全信息通报中心信息通报机制技术支持单位已达到 71 家。各技术支持单位利用各自的技术专长，对重要信息系统和重点网站开展安全监测，并将发现的问题及时上报，为网络安全的态势感知和通报预警工作提供支持。

每周安全事件

类 型	内 容
中文标题	XEN 虚拟机监控器出现“致命”漏洞
英文标题	Xen hypervisor has“fatal”security vulnerability
作者及单位	Sead Fadilpašić；betanews
内容概述	内容概述 近日，Xen 平台 PV 模式下运行的虚拟机被披露存在权限提升漏洞。当满足一定条件时，用于控制验证页表的代码可被绕过，导致 PV 模式下的普通用户（如 Guest）可使用超级页表映射权限重新定义可写入的映射。由于漏洞产生原因为页表关联权限绕过，即使在 Xen 系统配置“allowsuperpage”命令行选项为“否”的情况下也会受到漏洞的影响。综合利用漏洞，可提升普通用户权限，进而控制整个虚拟机系统，构成用户主机数据泄漏风险。目前，该漏洞版本已确定为 CVE-2016-6258。
链接地址	http://betanews.com/2016/07/28/major-security-vulnerability-xen-hypervisor/#comments

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.odpis.a[exp，rog]2016-08-1	该应用程序运行后会隐藏图标，私自访问指定网站，拦截指定内容短信和多种广告，建议卸载。（威胁等级中）
		Trojan/Android.Instealy.a[prv]2016-08-1	该应用程序在用户登录 instagram 时，会获取用户账号和密码并上传，向用户推送垃圾广告。用户会有信息泄露的风险，造成隐私泄露。（威胁等级高）
		Trojan/Android.korovk.a[prv，fra]2016-08-2	该应用程序运行后会隐藏图标，诱导激活设备管理器，会弹出虚假银行界面，窃取用户填写的账号密码信息，并发送指定短信，造成用户隐私泄露，建议及时卸载。（威胁等级高）
		Trojan/Android.Fake System Service.b[exp，prv]2016-08-3	该应用程序伪装成系统应用，安装后无图标，后台会私自提权，联网后会获取相关配置信息，推送广告，下载安装未知文件，同时会上传设备安装列表及下载安装的日志信息，建议立即卸载，避免造成资费损耗和隐私泄露。（威胁等级高）
	较为活跃的样本	G-Ware/Android.Dropper.b[exp，rog]	该应用程序运行后会私自下载色情程序，弹出虚假提示诱导用户安装，会在桌面创建大量快捷方式，影响用户正常体验，会造成用户资费消耗，建议及时卸载。（威胁等级低）
		Trojan/Android.AppBotSMS.e[prv，rmt]	该应用程序伪装成 google 应用，运行后会弹出虚假界面诱导用户点击，执行隐藏桌面图标操作，联网后会上传手机固件信息，获取指令后执行发送指定短息、拨打指定号码操作，上传来信内容，造成用户隐私泄露和资费消耗，建议及时卸载。（威胁等级高）
		Trojan/Android.Mobilespy.t[prv，spy]	该应用程序是一款间谍应用，安装后无图标，会执行录像、拍照、录音操作，会获取用户地理位置信息并上传，造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.Rootnik.f[rog，exp]	该应用程序安装后无图标，后台会联网下载 ROOT 文件私自提权，静默下载指定文件并诱导安装，建议立即卸载，避免造成资费损耗。（威胁等级高）
		G-Ware/Android.FakeApp.bh[prv，exp]	该应用为 Google Play 上的一些虚假应用，并无实际功能，会收集用户填写的信息，诱导用户下载 apk 应用，有推送广告等行为，会造成用户隐私泄露和资费消耗。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	微软 Office CVE-2015-6172 远程代码执行漏洞	Microsoft Outlook 分析经特殊设计的电子邮件时，存在远程执行代码漏洞。成功利用此漏洞的攻击者可以登录用户身份运行任意代码，并完全控制受影响的系统。攻击者可随后安装程序，查看、更改或删除数据，或者创建拥有全部用户权限的新帐户。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Reloadves	此威胁是一类可以连接网络后会下载恶意代码的木马家族。该家族样本运行后可以下载恶意代码到本机并运行，窃取用户信息并回传。（威胁等级中）
		Trojan[Downloader]/JS.ObfuJS	此威胁是一类可以下载恶意代码的木马家族。该家族样本通过 JS 脚本编写，运行后会连接网络下载恶意代码到本机并运行。（威胁等级中）
		Trojan[Backdoor]/Win32.Dridex	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后会连接远程服务器接受攻击者的恶意操作，会删除文件、回传敏感信息等。（威胁等级中）
		Trojan/Win32.Waldek	此威胁是一类可以释放恶意代码的木马家族。该家族样本运行后会释放恶意 DLL 文件并使用 rundll32.exe 加载，连接远程服务器，上传用户敏感信息。（威胁等级高）

防止勒索软件攻击的 6 条建议

Marc Laliberte / 文　安天公益翻译小组 / 译

2016 年似乎是勒索软件之年，无论你是世界 500 强企业的雇员还是个体经营者，你都有可能沦为勒索软件的受害者，它可以发生在任何人身上。为了避免成为勒索软件的下一个受害者，你可以参考以下 6 条建议：

1. 从数据备份开始，但不止于此

预防勒索软件最常见的措施就是妥善备份所有重要数据。这是非常好的建议，可以使你在被感染时无需支付赎金就有办法恢复自己的数据。但是，仅仅连接一个外部硬盘驱动器或备份到网络共享是不够的。

类似 Locky 和 CryptoFortress 这些现代勒索软件的进化产物，将会在你有权限的地方寻找和加密存储位置，即使那些位置没在你的系统上标明。为了解决这一问题，你必须保持离线数据备份，以避免威胁。

2. 阻止勒索软件穿越你的网络边界

一个常见的勒索软件交付方法是通过浏览器挂马，其会在用户不知情的情况下利用未打补丁的浏览器插件安装勒索软件。流行网站的跨站脚本漏洞也可以在用户不知情的情况下迫使浏览器加载一个恶意网站。

防御可预见攻击，需要把第一道防线移动得越远越好。在造成伤害之前，网络边界会是阻止即将到来的攻击的绝佳之地。基于网络的杀毒软件及 APT 扫描解决方案可以在其到达内置客户端之前识别并阻止恶意负载。当客户端甚至还不知道它们正加载勒索软件或其他有害下载时，这是相当有用的。

3. 阻止类似网络钓鱼式的选择交付方法

在 CryptoLocker 被 Operation Tovar 利用之前，该勒索软件一般作为冒充 Fedex 及 UPS 货运跟踪通知的网络钓鱼邮件的恶意附件来感染客户端。Locky 的变种则会通过在伪装成账单的恶意 Word 文档中的宏命令安装自身来持续其影响。

实施反垃圾邮件解决方案可以帮助阻止旨在传递勒索软件的网络钓鱼欺诈。大多数钓鱼邮件来自感染僵尸网络的客户端，包含的相似之处可以被反垃圾邮件服务提供商识别出。通过使用反垃圾邮件服务，可以在收件箱中限制钓鱼邮件的数量，同时会限制伪装良好的恶意软件攻击成功的机会。

4. 不要忘记你的客户端

终端保护在信息安全领域已不是新鲜事。基于签名的杀毒扫描仪可以发现明显的勒索软件样本，但是基于启发式的端点防护已经导致客户端防御出现了缺口。举例来说，名为 VIRLOCK 的勒索软件变种使用多态代码来规避基于签名的检测。当相同的勒索软件，其样本却不相同时，只是进行基于签名的扫描是不够安全的。

相反，对勒索软件的检测不应停留在代码层面上，启发式扫描关注的是该勒索软件实际执行了什么操作。如果下载行为足够可疑，启发式保护就可以在造成任何伤害之前将其锁定。

5. 早打补丁，经常打补丁

挂马可以从恶意网站加载跨站脚本攻击或破坏合法网站的广告活动等方式发起。这些攻击的成功往往依赖于应用补丁的浏览器插件。所以安装更新是对抗勒索软件攻击者的最简单方法。攻击者喜欢利用未打补丁的 Flash 和 Java 运行恶意代码。你应该调查 Flash 和 Java 对于你的客户端来说是否是必要的。今年甲骨文宣布将在下一代 Java Development Kit 的主版本中取消其 Java 浏览器插件，Flash 也会被替换为 HTML5。

6. 有些教育任重道远

勒索软件攻击会通过大量钓鱼邮件或挂马等方式来感染系统，一旦用户打开受感染的附件或访问一条被破坏的链接，就有可能成为勒索软件的受害者，从而导致重要数据遭到破坏，使企业受到损失。所以企业不仅需要有恢复被加密文件的能力，还需要对员工进行网络安全培训。网络使用者需要了解如何发现和应对网络钓鱼邮件，需要意识到点击特定链接的潜在后果，需要知道那些讨厌的应用程序更新通知的关键本质，否则他们会一直成为勒索软件攻击极易击破的点。

原文名称	6 Tips to Prevent Ransomware Attacks
作者简介	Marc Laliberte，Information Security Threat Analyst at WatchGuard Technologies。
原文信息	2016 年 6 月 27 日 Help Net Security 发布，原文地址 https://www.helpnetsecurity.com/2016/06/27/prevent-ransomware-attacks/

安天发布《Pony Loader 样本分析报告》

近日，安天追影小组在梳理网络安全事件时注意到，Pony Loader 样本被黑客用于多起攻击。经分析，黑客通过社会工程学方法使受害者下载并执行 Pony Loader 木马程序，从而窃取受害者的敏感信息并上传至 C&C 服务器，进而利用获取的信息对受害者造成财产和物理破坏，如获取受害者的财务账号、车辆信息、物流数据等。

Pony Loader 恶意软件在几年前已经开始传播，近期该恶意软件的升级版本开始在网络上被售卖，包括 2.0 版本和 2.2 版本。同时，其 1.9 版本的源码已经被泄漏，这使得其他黑客可以根据自身需要修改源码，变相促进了该木马的传播。

该恶意软件的主要功能是窃取受害者电脑中不同服务、应用的数据信息，包括 System Info、RDP、HTTP、FTP、SFTP、SMTP、POP、IMAP、MySQL、比特币信息等。为了破解所需要密码的账号信息，该恶意木马病毒还包含一个密码表，该密码表存储的密码均为出现频率较高的密码，从而提高了密码破解效率。值得一提的是，该恶意软件不仅窃取用户信息，还具有免杀功能，可以通过识别受害者电脑上运行的杀毒软来逃避检测，目前其逃避的杀毒软件包括卡巴斯基、AVG、BitDefender 等。

经过安天追影小组分析发现，大部分该类恶意代码都是通过名为“PonyBuilder”的生成器生成的，且有些利用 DarkEyE Protector 的加密工具加密过。

通过分析总结大量的攻击事件，我们可以发现，越来越多的攻击者会通过社会工程学获取目标组织的信任，引诱受害者打开非法链接或带有病毒的文件，进而实施病毒投放和资料窃取。安天追影小组提醒网络使用者，不要轻易下载邮件中不明来源的附件，不要随意点击不明来源的邮件或社交网站中的链接，养成及时更新操作系统和软件应用的好习惯。目前，安天追影产品已经实现了对 Pony Loader 样本的检出。

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：

文件被网络威胁感知类设备发现，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、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、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、静态分析鉴定器、安全云鉴定器将文件判定为木马程序。

该文件具有以下行为：

创建特定窗体、查找指定内核模块。

文件名	143C9261B19118863882A2E9793D0840
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	173 KB
MD5	143C9261B19118863882A2E9793D0840
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Yakes
判定依据	安全云

◆ 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
创建特定窗体	★	查找指定内核模块	★

◆ 网络监控

HTTP 信息		
方法	URI	端口
GET	http://www.msftncsi.com/ncsi.txt	80

TCP 信息			
源 IP	源端口	目的 IP	目的端口
192.168.122.243	49163	61.213.149.11	8080
61.213.149.11	80	192.168.122.243	49163

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=143C9261B19118863882A2E9793D0840