安天周观察

主办：安天　2016 年 8 月 15 日（总第 52 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天获得《商用密码产品生产定点单位证书》

根据《商用密码管理条例》和《商用密码产品生产管理规定》的相关规定，国家密码管理局对安天的研发力量、研发环境、生产安全保密措施、综合管理能力等进行全面考察后，安天于近日获得由国家密码管理局颁发的《商用密码产品生产定点单位证书》。

商用密码是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。随着我国社会、经济活动信息化的飞速发展，信息的安全问题日益突出。采用密码技术对信息进行加密保护和安全认证，是保护信息安全的有效技术手段。

安天获得《商用密码产品生产定点单位证书》，是国家密码管理局对安天在网络安全产品研发技术的肯定，也进一步完善了安天的资质体系。

该证书的获得，标志着安天成为国家指定的，具备保密资格认证的网络安全产品生产企业之一。

安天北京分公司举办“网络安全基础知识培训”

近日，安天北京分公司为员工举办了一场网络安全基础知识培训，安天副总工程师杨祖明担任本次讲师，他以“互联网与网络威胁的演进”为主题，对互联网以及应用的演进、网络安全威胁的演进、网络攻击的演进等内容进行了培训。为小伙伴们普及网络安全知识，扩大知识面，大家都认真听讲并做记录，纷纷表示对此次培训受益匪浅。

安天哈尔滨总部为员工送来夏日里的一份“清凉”

连日来，哈尔滨气温不断升高。为了减少因持续高温造成的不适，安天总部后勤小伙伴们为大家熬制了健康解暑的绿豆汤，并贴心地分发到大家的工位上。小伙伴们在紧张的工作中喝着及时配送的绿豆汤，调节了身心疲劳，也为自己的工作心情带来了一份清凉，此举受到了大家的一致好评。

◆ 爱尔兰警方 IT 系统受到恶意软件攻击

近日，“The Register”网站发布消息称，爱尔兰警署的 IT 系统遭到外部黑客入侵，警方暂时关闭了部分计算机系统。关于攻击的细节还未公布，但据报道此次攻击涉及到一种新型恶意软件。爱尔兰警方发表声明表示：其系统使用了加强版安全程序和标准协议，以保护系统免受任何恶意攻击。目前安全专家已进行了威胁识别，正在采用恰当的方法解决问题，并且没有敏感数据泄露。此前曾有过少数恶意软件引起警察系统崩溃。例如，2010 年 Conficker 蠕虫病毒爆发，导致曼彻斯特警方暂时停止访问国家系统。（来源：http://www.theregister.co.uk/2016/08/08/irish_police_malware_attack/）

◆ 甲骨文 MICROS 系统出现数据泄露

近日，甲骨文 (Oracle) 公司的 MICROS 系统出现了大规模数据泄露事件，由于该系统是基于云的 POS 管理解决方案，这或将影响全球使用该系统 POS 终端的商家。

据统计，使用 MICROS 系统 POS 终端的商家店面遍布全球 180 个国家，总数超过 33 万个。该数据泄露事件起初仅在小范围内影响，但据匿名消息源称一台连接甲骨文网络的终端系统被感染，并迅速扩散到其余联网终端。甲骨文公司表示正在深入调查此次事件。同时，还有消息发现 MICROS 客服支持站点与金融黑客组织 Carbanak Gang 的服务器建立了连线，后者或直接参与了攻击。（来源：http://www.cnbeta.com/articles/527743.htm）

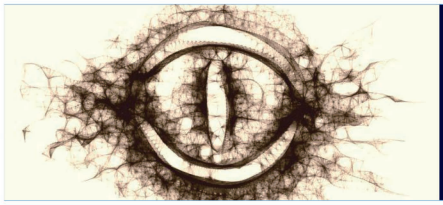
每周安全事件

类 型	内 容
中文标题	Linux 子系统为 Windows 10 带来了新的安全隐患
英文标题	Linux Subsystem Creates New Security Risks on Windows 10
作者及单位	Bogdan Popa；Softpedia
内容概述	近日，安全专家表示 Linux 子系统为 Windows 10 带来了新的安全风险。Windows 10 周年更新的一个大变化，就是引入了 Linux 子系统，以便用于在 Windows 10 上运行 Linux 应用程序。对于开发人员来说，这项功能可谓是大大的方便。为试图提升 Windows 10 中 Linux 子系统的性能，微软提供了对于原始硬件的直接访问，所以 Linux 应用程序并不是在 Hyper-V 容器中运行的。专家解释称，Hyper-V 容器有助于隔离进程和任何潜在相关的威胁。正因如此，Linux 拥有了完整的系统访问权限，这显然是一把很容易适得其反的双刃剑——黑客能够很容易地在 Linux 应用程序中注入恶意代码。此外，Linux 应用能够访问 Windows 上相同的文件和文件夹，相关攻击得手的可能性非常高。
链接地址	http://news.softpedia.com/news/linux-subsystem-creates-new-security-risks-on-windows-10-507060.shtml

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 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.Lostil.a[prv，exp]2016-08-08	该应用程序首次运行后会隐藏图标，窃取用户短信、通讯录、通话记录、通话录音、GPS 定位信息、浏览器书签记录、安装应用及进程相关信息等，会造成用户个人敏感隐私数据泄露。同时会向指定群体发送诈骗短信，扩大恶意影响范围，造成用户资费损失。建议立即卸载或查杀该应用。（威胁等级高）
		Trojan/Android.Dmrcla.a[prv，rog，spy]2016-08-09	该应用程序安装后无图标，会伪装成系统应用，运行后会诱导激活设备管理器，设置环境录音，通话录音、手机截屏、记录键盘输入信息并执行上传操作，会释放加载子包恶意程序，执行私自提权、关闭杀软等操作，会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.zospy.a[prv，fra]2016-08-09	该应用为一款间谍程序，会伪装成系统应用，程序运行后会申请获取 root 权限，监控来电号码、地理位置、WhatsApp 消息、Facebook 消息、短信内容、浏览器历史记录、相册、Viber 语音信息，执行上传操作，会造成用户泄露，建议及时卸载。（威胁等级高）
		Trojan/Android.Fraud.a[prv] 2016-08-09	该应用程序运行后，会上传手机收件箱信息、获取指令，执行发送指定短信和删除指定收件箱内容的操作，会造成用户隐私泄露，建议及时卸载。（威胁等级高）
		Trojan/Android.plirismobile.a[prv，rmt，spy] 2016-08-10	该应用是间谍程序，运行后会激活设备管理器，会隐藏图标，获取用户通话记录和地理位置信息，通过短信转发并联网上传。会接收短信指令，清除用户手机数据和锁屏密码，造成用户隐私泄露和资费损耗，建议及时卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.SmsThief.al[prv]	该应用会伪装成其他应用，程序运行后会获取用户短信信息、通讯录、通话记录、GPS 位置等隐私信息上传到指定服务器，造成用户隐私泄露。（威胁等级中）
		Trojan/Android.kichhoat.f[pay，prv，rmt]	该应用运行后会隐藏图标，会上传手机固件信息获取返回值，控制显示图标和发送短信，短信转发手机固件信息，造成用户资费损耗和隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.Dendroid.d[prv，spy]	该应用伪装成输入法应用，记录用户输入信息，从远端下载 ROOT 工具私自提权，将自身置为系统应用，并接收远端控制指令，上传用户短信、联系人、通话记录、位置、书签等敏感信息，并录音、拍摄照片上传到服务器，会造成用户隐私泄露。建议卸载。（威胁等级高）
		Trojan/Android.SpyPhone.e[prv，spy]	该应用是一款间谍程序，安装后会隐藏图标，可获取用户短信信息，通话记录，地理位置信息，网页浏览历史记录，录像拍照记录及 WhatsApp 消息并上传远程服务器，造成隐私泄露。（威胁等级高）
		G-Ware/Android.Jzkapp.a[exp，rog]	该应用程序捆绑了恶意广告插件，运行后会推送通知栏广告、会私自下载推广应用，诱导用户执行安装，会加载指定网页，造成流量损耗，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	Adobe Reader 双重释放远程代码执行漏洞 (CVE-2016-0935)	Adobe Reader 在处理 PDF 文档内畸形的 ExtGState 字典时存在安全漏洞，会导致双重释放。攻击者利用此漏洞可在当前进程上下文中执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Nurjax	此威胁是一类可以下载恶意代码的木马家族。该家族样本运行后会劫持浏览器，在用户浏览特定网页时重定向到恶意页面，会下载恶意代码并运行。（威胁等级中）
		Trojan[Ransom]/Win32.Zerber	此威胁是一类可以加密用户数据的木马家族。该家族样本是勒索软件，运行后会加密用户文件，会播放声音提示用户文件已被加密，需支付比特币解密。该家族目前已经作为商业军火在俄罗斯地下黑市出售。（威胁等级中）
		Trojan[Ransom]/Win32.Petr	此威胁是一类可以修改用户 MBR（主引导记录），运行后会导致系统蓝屏崩溃，自动重启后显示骷髅头图形和警告声明，会提示用户访问特定的地址交付比特币解密。（威胁等级中）
		Trojan/Win32.Shifu	此威胁是一类可以窃取银行相关信息的木马家族，它可以注入系统进程，记录用户击键信息，并通过网络回传给控制者。（威胁等级高）



ProjectSauron APT 强势来袭

Michael Mimoso / 文　安天公益翻译小组 / 译

近日，卡巴斯基实验室和赛门铁克公司发布了运行有五年之久的 APT 攻击行动，分别命名为 ProjectSauron 和 Strider。卡巴斯基实验室指出，ProjectSauron 针对多个国家的政府机构、电信公司、金融机构、军事和研究中心发动了大规模攻击。该平台具有高级攻击的所有特征，采用隐蔽手段，利用零日漏洞和精炼的编码技术来窃取敏感数据。自 2011 年以来，ProjectSauron 一直被用来窥探政府机构和其他关键行业。研究人员表示，时至今年，这些攻击活动仍然活跃。

虽然目前尚不明确攻击者的入侵手段，但他们执行的大部分活动已经暴露。例如，其攻击平台被称为 Remsec 的模块化框架，一旦成功部署，攻击者就能够横向运动，窃取数据并注入更多的攻击代码。卡巴斯基实验室指出，该平台能够根据不同的攻击目标来制定专门的攻击方案，并最大程度地绕过被攻击主机安装的杀毒产品的检测。ProjectSauron 使用了自定义的 LUA 脚本引擎来实现平台的核心功能和部分插件，其至少有五十余种不同类型的

插件可供选择。研究人员在一个 LUA 模块中发现了名为“SAURON”的变量。ProjectSauron 的一个关键特性是其采用强加密算法，例如 RC6、RC5 和 Salsa20 等。

卡巴斯基实验室的报告中指出：“ProjectSauron 背后的攻击者对政府机构广泛使用的通信加密软件很感兴趣。他们窃取与加密软件有关的加密密钥、配置文件和关键基础设施服务器的 IP 地址。”

在持续性方面，攻击者在域控制器上注册了一个后门模块，作为 Windows 本地安全权限密码过滤器，它通常用来执行密码策略。只要有网络或本地用户 (包括管理员) 登录或更改密码，ProjectSauron 被动后门模块就能够启动并以明文形式收集密码。”

攻击者植入的大部分程序作为后门使用，它们或者安装新的模块，或者运行命令。卡巴斯基实验室报告称，每个植入程序都是唯一的，具有独特的文件名、大小和任务，如窃取文件、记录击键，或从本地和连接的硬盘上窃取加密密钥。

卡巴斯基实验室发现了 28 个 C&C 域，分别指向美国和一些欧洲国家的 11 个 IP 地址。该公司已经将这一发现纰漏给当地计算机安全应急响应中心 (CERT) 和执法机构。

此外，卡巴斯基的报告还指出：“从操作安全方面来看，ProjectSauron 的操作者准备非常充分。运营昂贵的网络间谍活动需要庞大的域和服务器基础设施。ProjectSauron 平台选择了多个互联网服务提供商 (ISP) 的做法，足以说明他们尽一切可能避免创建固定的攻击模式。”

研究人员还发现了有趣的模块，它通过使用特殊的 USB 存储驱动器从物理隔离网络 (air-gapped) 系统窃取数据。受害者一旦连接网络，系统被感染，攻击者就会等待 USB 驱动器连接到被感染的机器“并利用如 HTTP，TCP，SMTP 等通用协议从被感染机器窃取数据。研究人员还发现，一个插件使用域名系统 (DNS) 来传出窃取的数据。卡巴斯基实验室指出：“为了避免网络层面的 DNS 信道通用检测，攻击者在低带宽模式下使用它，所以它仅用于攫取目标系统的元数据 。利用 DNS 协议的 ProjectSauron 恶意软件的另一个有趣的特点是，其向远程服务器实时报告攻击进度。一旦到达某个阶段， ProjectSauron 就会向每个目标的独特子域发出一个 DNS 请求。”

卡巴斯基在报告中表示：“当渗透隔离系统时，在 USB 中创建加密存储区域并不能使攻击者控制物理隔离网络的机器。USB 的主分区必须具有另一个组件，如零日漏洞。到目前为止，我们还未发现任何嵌入恶意软件的零日漏洞利用代码。我们认为，这种代码很可能部署在难以捕获的攻击中。”

原文名称	ProjectSauron APT On Par With Equation , Flame , Duqu
作者简介	Michael Mimoso，卡巴斯基《安全周报》的编辑。
原文信息	2016 年 8 月 8 日 Threatpost 发布，原文地址 https://threatpost.com/projectsauron-apt-on-par-with-equation-flame-duqu/119725/
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《“ORCUS”远控木马样本分析报告》

近日，安天追影小组在梳理网络安全事件时，注意到名为“ORCUS”的远控木马样本并对其做了简要分析。经分析，“ORCUS”远控木马使用 C# 编写，其样本可以感染 windows 操作系统，感染该样本后攻击者可以完全控制受害者的电脑。在 2015 年 10 月左右，开发者先将样本以“Sorzus”命名并在黑客论坛上开源发布，之后将其命名为“ORCUS”并进行商业化出售，出售价格为 40 美元。

经安天追影小组分析，“ORCUS”远控木马具有以下恶意行为：远程执行代码、键盘记录、麦克风录音、远程管理、反向代理、拒绝服务、VM 检测、执行实时脚本、窃取密码、禁用网络摄像头指示灯、摄像头监控、截取屏幕、信息回传、插件系统等。与其它远控木马相比，“ORCUS”不仅有远控木马的共性，还有其它远控木马不具备的特点。例如“插件系统”功能，该插件系统功能允许“ORCUS”用户建立自己的插件或下载已经由开发者开发的插件，支持的开发语言为 C#、VB、.Net、C++，开发者提供了一个开发包来创建 IDE（集成开发环境）。

“ORCUS”远控木马会将窃取到的受害者信息，回传到其指定的服务器上。服务器上的信息可供该木马的众多使用者共享，以达到更好管理受害者网络的目的，并通过部署多个服务器来实现其可扩展性。该木马的使用者可以通过控制器工具，来访问存有窃取到信息的服务器以及受害者的电脑，其控制器不仅有 Windows 版本也有 Android 版本。

通过以上分析，可见远控木马的开发、部署、升级已经越来越规模化、商业化。安天追影小组提醒网络使用者，对攻击者来自暗处的攻击需时时提高警惕，不要随意点击不明来源的邮件或社交网站中的链接，不要轻易下载邮件中不明来源的附件，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“ORCUS”远控木马样本的检出。

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、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。

文件名	E887D9443E2022E27A57A944907D0503
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	658 KB
MD5	E887D9443E2022E27A57A944907D0503
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[:HEUR]/Win32.AGeneric
判定依据	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 2003，Flash，WPS，FoxitReader，Adobe Reader

最终依据静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。该文件具有以下行为：疑似键盘记录器、疑似键盘记录、读取自身文件、创建特定窗体、释放 PE 文件、获取驱动器类型、获取系统内存、独占打开文件、打开自身进程文件、获取 CPU 信息。

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
疑似键盘记录器	★★★	疑似键盘记录	★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
读取自身文件	★★	创建特定窗体	★
释放 PE 文件	★	获取驱动器类型	★
获取系统内存	★★	独占打开文件	★
打开自身进程文件	★	获取 CPU 信息	★★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=e887d9443e2022e27a57a944907d0503