安天周观察

主办：安天　2017 年 1 月 23 日（总第 74 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布方程式系列报告之四——《方程式组织 Equation Drug 平台解析（提纲）》

2017 年 1 月 17 日，安天发布《方程式组织 Equation Drug 平台解析（提纲）》，这是安天发布的针对方程式组织的第四篇分析报告。

在过去的两年中，安天已经连续发布了三篇针对方程式组织的分析报告，分别为：《修改硬盘固件的木马——探索方程式 (EQUATION) 组织的攻击组件》、《方程式 (EQUATION) 部分组件中的加密技巧分析》、《从“方程式”到“方程组”——EQUATION 攻击组织高级恶意代码的全平台能力解析》。在这三篇报告中，安天对多个模块进行了分析，并对其写入硬盘固件的机理进行了分析验证；对攻击组件中使用的加密方式实现了破解；独家提供了方程式 Linux 和 Solaris 系统的样本分析，这也是业内首次正式证实这些“恶灵”真实存在的公开分析。

此次安天再度发布针对“方程式”组织的分析，旨在能抛砖引玉，邀请更多兄弟团队共同加入分析工作，以便进一步呈现出其全貌。

本篇报告是围绕 2017 年 1 月 12 日，“影子经纪人”放出 Equation Group 组件中的 61 个文件展开的。报告由三部分组成，详细分析了方程式线索曝光和分析成果时间链梳理、DanderSpritz 攻击平台、部分组件与插件分析等。安天本次发布的报告还在不断的更新中。关于“方程式”系列报告和内容更新可以登录安天官网或微信公众号查看。

安天召开 2016 年度工作总结大会

金猴辞旧岁，瑞鸡送春来。

2017 年 1 月 19 日，安天召开 2016 年度工作总结大会。

首先，安天新任总裁胡忠华通过视频致新年贺词。他梳理了 2016 年度公司的经营情况，对当前的工作进行了总结，并对今后的工作做出了布置和安排。2017 年，安天要在战略上聚焦，不论是市场拓展，还是产品开发，都需要安天人把功课做扎实。

安天创始人、首席技术架构师肖新光做了总结报告。他总结了过去一年里安天所取得的成绩以及所面临的主要问题，提出了企业的使命与愿景，希望安天能做“中国网络安全的国家企业，做全球网络安全市场格局下的终局赢家”。他向全体员工再次解读了“智者 . 安天下”的概念，“智者”不是指安天人自己，安天只是扮演能力输出和服务的角色，安天的客户才是直面威胁、创造价值的真正智者。

对新一年的工作，他提出了新的目标任务和要求，安天将建立以“威胁响应”为驱动的快速能力型研发组织，将业务高度聚焦。同时，把安天“探海”、“智甲”、“镇关”、“追影”、“态势感知”、“威胁情报”等产品做好，发挥综合系统、多点布局的优势，化散点为基石。

2017 年，安天还将建立适配历史使命的新组织文化，形成一支“革命化、正规化”的组织，为安天的“第三次创业”狂飙突进，为“服务客户，解决问题。应对威胁，保障价值”不懈努力。

北京安天乔迁新址

2017 年 1 月 16 日，随着安天人员规模的扩大和业务发展的需要，安天迁入位于北京市海淀区闵庄路 3 号清华科技园玉泉慧谷一期 1 号楼的新址。

北京安天承载着安天业务总部和政企安全产品研发的职能。目前安天已经形成了由流量检测产品“探海”、终端防护产品“智甲”、威胁阻断产品“镇关”、深度分析产品“追影”等组成的威胁检测防御产品线；并基于可靠的基础检测感知能力和威胁情报能力，为关键基础设施管理机构、行业客户等提供态势感知与监控预警解决方案。北京安天迁址后，将会继续增加产品和服务的投入，增强、扩建安天应急响应体系和感知分析能力，提升服务用户的整体能力。

目前，安天正在进行面向政企安全市场领域的“第三次创业”，新地址，新起点，新征程，安天将在新的平台上继续努力，做出成绩。

尊敬的读者：

2017 年春节即将来临，《安天周观察》于春节期间休刊二期，恢复出版时间为 2017 年 2 月 13 日。

感谢所有读者对《安天周观察》一直以来的支持与关注！

祝大家新春快乐！

2017 年 1 月 23 日

每周安全事件

类 型	内 容
中文标题	“自动填充”功能可能泄露个人信息
英文标题	Browser AutoFill Feature Can Leak Your Personal Information to Hackers
作者及单位	Swati Khandelwal；The Hacker News
内容概述	近日，芬兰的 Web 开发者和白帽黑客 Viljami Kuosmanen 一同展示了攻击者操纵并利用拥有自动填充功能的浏览器、插件和密码管理器等工具的过程。大多数用户在填写网页表单时，都曾为重复填写信息而苦恼。为满足用户需求，Google Chrome 等主流浏览器均提供了“自动填充”功能。它能记录下用户曾填写过的信息，例如姓名、身份证号码、银行卡卡号和密码等，以后遇见相同的问题，它将自动填充答案。然而，事实证明，攻击者可以利用这项功能收集用户的隐私信息或将用户隐私信息泄露给恶意的第三方。 尽管这个问题在 2013 年已经被 ElevenPaths 的安全分析师 Ricardo Martin Rodriguez 发现，但是至今 Google 尚未采取任何行动处理“自动填充”这一弱点。
链接地址	http://thehackernews.com/2017/01/browser-autofill-phishing.html

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

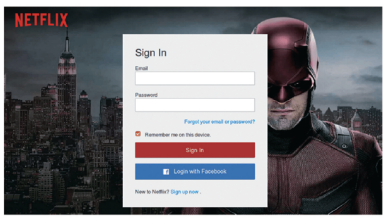
平台分类	关注方面	名称与发现时间	相关描述
移动恶意代码	较为活跃的样本	RiskWare/Android.FakeSystem.f[exp]	该应用程序会伪装成系统升级服务，安装后无图标显示，除广告外无实际功能，后台会消耗用户流量。造成用户资费损失，建议立即卸载。（威胁等级低）
		G-Ware/Android.HiddenAds.bb[exp]	该应用运行后会隐藏图标，后台频繁访问广告，造成用户资费消耗，建议卸载。（威胁等级低）
		Trojan/Android.FakeApp.cx[exp，rog]	该应用会伪装成安全软件，无实际功能。运行后会隐藏图标，获取电话号码、IMEI 等固件信息，损害用户隐私。会将带有广告的信息插入用户短信收件箱，进行广告推送，具有一定流氓性，影响用户体验，建议谨慎使用。（威胁等级高）
		Trojan/Android.FakeSystem.g[exp，rog]	该应用安装运行后会隐藏图标，私自与指定 URL 建立网络连接，上传用户的设备固件信息等隐私数据，下载未知数据，静默安装未知应用，此外还会推送广告，影响用户体验，造成用户流量资费损失，建议立即卸载。（威胁等级高）
		Trojan/Android.oxti.r[exp]	该应用会隐藏图标，后台频繁访问色情网站，造成用户流量耗费，建议立即卸载。
		Trojan/Android.Joyreach.e[exp]	该应用运行后会加载广告，私自提权，静默安装未知应用，建议立即卸载。（威胁等级中）
		Trojan/Android.Triada.aa[exp，sys]	该应用程序运行后，会在后台释放文件提权，自身包含风险代码，私自下载安装未知应用，建议卸载，避免造成资费损耗。（威胁等级中）
		Trojan/Android.Rootnik.t[exp，sys]	该应用程序包含危险代码，会私自联网下载恶意子包，私自提权推送广告，下载安装推广应用，造成用户资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.FakeFlashPlayer.x[exp，rog]	该应用会伪装成 Flash Player，运行后会隐藏图标，私自申请激活设备管理，自身包含风险代码。用户需警惕后台下载造成不必要的资费消耗。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 中存在安全漏洞 (CVE-2015-0311)	Adobe Flash Player 中存在安全漏洞，远程攻击者可利用该漏洞执行任意代码。以下产品和版本受到影响：基于 Windows 和 OS X 平台的 Adobe Flash Player 16.0.0.257 及之前版本和 Adobe Flash Player 13.0.0.260 及之前版本，基于 Linux 平台的 Adobe Flash Player 11.2.202.429 及之前版本。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Zeagle	此威胁是一种具有下载行为的木马类程序。该家族样本运行后，会添加注册表启动项达到随机启动的目的。会与远程服务器连接，下载其它的恶意程序到本地运行。（威胁等级中）
		Trojan[Dropper]/Win32.Nail	此威胁是一种具有捆绑行为的木马类程序。该家族会携带各种恶意软件，运行后会将捆绑的恶意软件安装在计算机上，窃取用户信息，占用系统资源，影响用户使用。（威胁等级中）
		Trojan/Win32.Carberp	此威胁是一木马类程序。该家族专门用于盗取用户银行信息。运行后能够感染硬盘的主引导记录，对包括使用 EV-SSL 的 HTTPS 在内所有类型的网络流量进行控制，会在被窃取的信息被发送到金融网站之前将信息发送到远程服务器上。（威胁等级高）

Netflix 网络钓鱼活动窃取用户凭证和信用卡数据

Chris Brook / 文　安天公益翻译小组 / 译

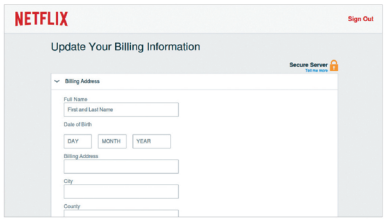
近日，研究人员发现了一项网络钓鱼活动，该活动旨在诱使不知情的 Netflix 用户提供凭证和信用卡数据。

该活动 (目前已经终止) 首先会向用户发送电子邮件，通知他们更新 Netflix 账户信息。一旦受害者点击邮件中的链接，就会被引向一个貌似合法的 Netflix 登录页面，并被要求输入电子邮件地址和 Netflix 密码。但攻击者并不满足于只获取用户的登录凭证信息，他们还会诱导用户填写一个表格，要求他们更新支付信息 (输入姓名、出生日期、地址和信用卡信息)。



攻击者甚至会要求用户提供他们的社保号 (Netfli 从未有过这种要求) 和 VBV 3D 安全代码 (这是 Visa 在欧洲和印度使用的一个相当新的服务，尚未在美国部署)。

钓鱼页面模仿真实的 Netflix 页面，甚至设置了一个黄色的“安全服务器”锁。该活动会通过 PHP 邮件实用程序将所有信息发送给攻击者，这将允许他们在多个网站上部署网络钓鱼工具。



发现该钓鱼活动的是火眼公司威胁研究团队的研究员穆罕默德・莫辛・达拉 (Mohamed Mohsin Dalla)。他指出，攻击者擅长绕过网络钓鱼过滤器，他们使用 AES 加密方法进行编码，其提供的内容能够更容易地规避检测。

达拉在报告中写到：“攻击者通过模糊网页来欺骗文本分类器，防止它们检查网页内容。该技术使用两个具有加密和解密功能的文件 (一个 PHP 文件和一个 JavaScript 文件)，用以加密和解密输入的字符串。PHP 文件在服务器端加密网页，JavaScript 文件则在客户端解密被加密的内容。”

此次针对 Netflix 客户的网络钓鱼活动并没有多么了不起，但是其规避检测和提供钓鱼页面的方式却有特殊之处。这些钓鱼页面托管在合法但被感染的服务器上，如果用户的 DNS 链接到 Google 或 PhishTank(一个反网络钓鱼服务)，则不会向用户显示这些页面。

火眼公司指出，如果 Google、Phishtank 或其他网站 (例如 Calyx Institute 或 Netflix) 的用户访问了该伪造的网站，则会显示“404 Not Founderror”，以此来降低该活动被发现的可能性。

近期，Netflix 网络钓鱼活动的覆盖范围越来越大。2016 年夏天，英国出现了一些假账单电子邮件，诱骗用户以为自己订阅了 Netflix 服务，要求他们提供信用卡信息。7 月发生的另一个骗局则通知 Netflix 用户他们需要更新信用卡数据。在受害者输入信息后，就会被告知其账户已停用，需要下载“Netflix 支持软件”。商业改进局 (Better Business Bureau) 指出，该软件实则是一款“远程登录软件”，会将受害者计算机的密钥发送给攻击者。

原文名称	Netflix Phishing Campaign Targeted User Information，Credit Card Data
作者简介	Chris Brook，卡巴斯基实验室《安全周报》(Threatpost) 的副编辑。
原文信息	2017 年 1 月 10 日发布于《Threatpost》 原文地址 https://threatpost.com/netflix-phishing-campaign-targeted-user-information-credit-card-data/122988/
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《勒索木马 Shade 新变种》分析报告

近日，安天追影小组发现一款勒索软件 Shade 木马家族的新变种，并对其进行了分析。Shade 于 2015 年初被发现，其利用恶意垃圾邮件或漏洞作为主要感染媒介。该勒索软件能够加密 150 余种格式的文件，文件内容和文件名均会被加密，同时，它会修改文件扩展名。在加密结束后，被感染主机的桌面会显示一封信，要求受害者支付赎金以解密文件。即使受害者支付了赎金，该木马依旧不会停止恶意行为，会继续下载其他恶意软件，持续感染受害者主机。

该勒索软件首先会在普通商务邮件的附件中存放一个经过压缩的脚本，通过具有欺骗性的邮件内容诱导接收者打开压缩包并运行该脚本。脚本运行后，会自动调用 Powershell 执行下载功能，从指定 URL 下载资源。脚本下载的木马程序会将自身的图标修改为 PDF 图标，目的是欺骗受害者主动运行该样本。

追影小组针对脚本下载的程序 Herty.exe 进行分析时，发现该程序会遍历进程，查找进程中是否存在“VboxService.exe”、“Vmtoolsd.exe”，以检测是否是在虚拟机环境下运行，若不是在虚拟机环境下运行则会继续执行。接着该样本程序会释放文件 Csrss.exe，创建子进程，并设置自启动。随后，该样本会生成公钥密码，遍历系统磁盘指定文件类型的文件，使用公钥密码对文件名和文件内容进行加密，并将文件类型修改为 DA_VINCI_CODE，创建隐藏文件 XFS，将加密文件的源文件信息写入 XFS。此外，该样本还会创建隐藏文件 State，将相关主机信息写入该文件，并向指定 IP 地址发送 TCP 请求，建立连接后发送 XFS、State 文件。最后，样本会修改感染主机的桌面背景，创建 README1.txt 和 README10.txt，在文本文档中留下联系信息和赎金需求，实现勒索功能。

针对该勒索软件，安天提醒各位网络用户，要及时备份重要的文件和数据，并确认备份的信息能够完整恢复。另外，要提升自身的网络安全意识，及时更新系统补丁，使用时采用较为可靠的安全软件，在接收邮件时要注意检查来源是否可靠，对于不明来源的附件不要轻易下载，以防止钓鱼软件中的恶意代码对系统进行感染。

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，依据行为即可实现对上述木马程序进行有效检测，以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：释放 PE 文件为常见系统进程名、其他进程写入可疑数据、读取自身文件、获取驱动器类型、通过设置为系统属性隐藏文件、填充导入表（疑似壳）、释放 PE 文件、获取系统内存、增加 run 自启动项、获取系统版本、创建挂起的进程、打开自身进程文件、设置自启动项、访问文件尾部、访问其他进程内存、获取计算机名称、获取 socket 本地名称、结束进程、连接网络、创建特定窗体、独占打开文件、遍历进程、获取主机用户名称、查找特定窗体、请求加载驱动的权限。

文件名	A6CD22776298A7B3E669FF2D879B10A5
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	904 KB
MD5	A6CD22776298A7B3E669FF2D879B10A5
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransomware]/Win32.Shade
判定依据	动态行为

◆ 危险行为

行为描述	危险等级
释放 PE 文件为常见系统进程名	★★★
其他进程写入可疑数据	★★★

◆ 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	★★	获取驱动器类型	★
通过设置为系统属性隐藏文件	★	释放 PE 文件	★
填充导入表（疑似壳）	★★	获取系统内存	★★
增加 run 自启动项	★	获取系统版本	★★
创建挂起的进程	★★	设置自启动项	★★
打开自身进程文件	★	访问文件尾部	★
访问其他进程内存	★	获取计算机名称	★
获取 socket 本地名称	★	结束进程	★★
连接网络	★	创建特定窗体	★
独占打开文件	★	遍历进程	★
获取主机用户名称	★	查找特定窗体	★
请求加载驱动的权限	★		

报告地址：https://antiy.pta.center/_lk/details.html?hash=A6CD22776298A7B3E669FF2D879B10A5