安天周观察

主办：安天　2016 年 11 月 7 日（总第 63 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

【安天 CERT】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

方程式攻击组织是一个与美国 NSA 相关的一个超级网络攻击组织。安天曾在去年陆续公布了两篇针对方程式攻击组织的分析报告，分析了其针对 Windows 平台的恶意代码组件构成、对硬盘的持久化能力和对加密算法的使用。

安天的本篇报告首次公布了对该组织针对 Solaris 平台和 Linux 平台的部分样本分析，这是业内首次正式证实这些攻击武器真实存在的公开分析。这些载荷不是常见脚本木马，是组件化、具备 Rootkit 能力、具有超强加密抗分析能力、严格进行加密通讯的二进制组件。

通过安天、卡巴斯基的分析报告，以及代号“影子经纪人”的爆料，相互印证，一个关于这个超级攻击组织的几乎无死角的、全平台化攻击能力已经日趋清晰。这份分析报告（包括安天此前两篇分析报告）主体均形成于数年前，一直在等待发表时机，在过去数年，安天进行了艰苦的分析工作。安天这样比喻分析工作的难度：我们需要破解的已经并不只是一个“方程式”，而是更为复杂的多元多次的“方程组”。

1. 报告主体内容

方程式组织采用了工业水准的制式化攻击武器库，安天在此前报告中已经对其 6 件恶意代码组件“装备”进行了分析，目前已经发现并证实其中 2 个组件

具有多平台特性，其中一个组件可以推测存在多平台特性。通过相关信息汇总可以肯定方程式的攻击组件至少覆盖 Windows、Linux、Solaris、Oracle-owned Unix、FreeBSD 和 Mac OS 平台。

安天捕获分析了其 Linux 下的一个侦查探测的前导组件，该组件通过参数执行不同的功能流程。样本可以采集系统相关信息。样本动态加载调用函数和数据，使用了一种自定义的加密算法，安天破解了其加密秘钥，该秘钥与安天对其 Windows 组件破解出的秘钥一致。安天分析获得了其分支指令。

安天捕获分析了方程式组织在 Sun SPARC 架构下的一个 Rootkit，并认为这是第一个 SPARC 架构下的具有 Rootkit 属性的恶意代码，用于为其他部件的 Solaris 版本来提供掩护。SPARC 架构下 Solaris 恶意代码非常罕见，因为 SPARC 架构的计算机一般用于工业、航天等领域，很少出现在民用领域。

方程式制造的 Rootkit 主要负责隐藏主功能样本文件、以及相关衍生的文件和其自身，包括进程、文件、和服务信息。其自身文件名使用了一定的伪装技巧命名。安天破解这个 Rootkit 使用的加密算法。

安天同时曝光分析了另一个攻击组件的 Sparc 模块，该模块可以窃取用户和密码信息。该样本使用了一种自定义加密算法，安天破解了其秘钥和通讯子秘钥，并还原了其网络指令体系。

2. 结论部分

这些攻击武器在过去十余年中，陆续出现在针对中国互联网节点的攻击当中。“暴露在互联网上的节点，乃至能够访问互联网的内网中，并不存放高价值的信息”，这并非是这个信息大量产生、高速流动时代的真实情况。在大数据时代，高价值信息的定义和范围也在不断变化着。更多的信息资产已经不可避免地分布在公共网络体系中。而对这些资产的窥视和攻击也在持续增加着。而超级攻击组织则是类似攻击的始作俑者和长期实践者。

针对 DNS 服务器的入侵，可以辅助对其他网络目标实现恶意代码注入和信息劫持；针对邮件服务器的植入可以将用户所有的邮件通联一网打尽，针对运营商骨干节点的持久化，可以用来获取全方位的信息。“物理隔离”的安全神话也已经到了应该破灭的时候，习近平总书记在 4.19 讲话中已经提醒国内用户和网络安全工作者：“‘物理隔离’防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患。”

相关超级攻击组织拥有“成建制的网络攻击团队、庞大的支撑工程体系与制式化的攻击装备库、强大的漏洞采集和分析挖掘能力和关联资源储备以及系统化的作业规程和手册，具有装备体系覆盖全场景、漏洞利用工具和恶意代码载荷覆盖全平台、持久化能力覆盖全环节的特点。面对这种体系化、既具备工业级水准又具有高度定向性的攻击，永动机注定停摆，银弹注定哑火。想要达成防御效果，实现追踪溯源，唯有以清晰的战略、充分的成本投入，以体系化的防守对决体系化的攻击，通过长期艰苦、扎实的工作和能力建设，才能逐渐取得主动。

超级攻击组织的能力强大到了只能猜测和想象的程度时，不可能不引发恐慌，从而导致对超级大国产生“滥用供应链和信息流优势”的严重质疑。而近期的方程式攻击代码泄露事件以及此前“ANT”装备体系的曝光，则又使我们看到了相关的 Exploit 储备和攻击思路流入到网络犯罪组织、甚至恐怖主义组织的可能性。鉴于网络攻击技术存在极低的复制成本的特点，当前已经存在严峻的网络军备扩散风险。（全文：http://www.antiy.com/response/EQUATIONS/EQUATIONS.html）

每周安全事件

类 型	内 容
中文标题	黑客使用硬件攻击 GSM A5 加密算法
英文标题	Hacking GSM A5 crypto algorithm by using commodity hardware
作者及单位	Pierluigi Paganini；Securityaffairs
内容概述	近日，安全研究专家表示，在普通 GPU 处理器的帮助下，便可以在几秒钟之内破解 GSM 移动数据所采用的加密算法。 GSM 只会对访问网络的用户身份进行验证。因此，通信的加密安全层只能够提供数据保密和身份验证功能。但需要注意的是，这是一种功能有限的身份验证，因为它并不具备不可否认性这种特征。为了实现通信的安全，GSM 采用了多种加密算法。比如说，GSM 使用了 A5/1 和 A5/2 这两种流密码来确保用户语音通话数据的安全。但是，这两种加密算法中却存在严重的安全问题。
链接地址	http://securityaffairs.co/wordpress/52666/hacking/gsm-crypto-hacking.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	新出现的样本家族	Trojan/Android.Agcr.a[rog, exp]2016-10-31	该应用安装后无图标显示，运行后会私自联网上传设备固件信息，释放子包文件并下载文件提权，会造成用户资费消耗。（威胁等级高）
		Trojan/Android.timobox.b[exp] 2016-11-02	该应用程序安装后，后台会监听设备联网状态的变化情况，联网时会检查当前版本并下载更新自身安装包，并下载诸多不同类型的文件。另外其资源目录下的更新包包含广告推送行为，会造成用户流量资费损失，同时存在恶意应用和文件下载风险，建议谨慎使用。（威胁等级中）
		G-Ware/Android.FakeSIMupdate.a[rog，exp，rmt]2016-11-02	该程序会伪装成常用程序，运行后会诱导激活设备管理器并隐藏图标。执行短信指令发送短信、拨打电话、修改手机设置等操作，同时会窃取用户短信和安装列表信息，避免造成资费损耗和隐私泄露，建议立即卸载。（威胁等级低）
		Trojan/Android.Triada.p[exp，rog]2016-11-04	该应用包含色情敏感内容，运行后会释放恶意子包并提权安装，会上传手机固件信息和手机号码信息，并在后台加载广告，造成用户资费损耗和隐私泄露，建议不要安装。（威胁等级高）
	较为活跃的样本	Trojan/Android.emial.dk[prv]	该程序会伪装安全控件，运行后会诱导用户激活设备管理器，收集用户设备固件和短信并上传到远程服务器，同时会私自删除短信，避免造成资费损耗，建议立即卸载。（威胁等级中）
		Trojan/Android.SmsSend.kq[exp]	该程序运行后会隐藏图标，后台会联网下载未知文件，造成用户资费损耗。（威胁等级高）
		Trojan/Android.Downloader.cl[rog，exp]	该应用会伪装成正常应用，运行后隐藏图标，后台会私自下载恶意应用和提权工具，并在后台静默安装，会造成用户资费损耗，建议不要安装。（威胁等级高）
		Trojan/Android.FakeUpdate.d[exp，fra]	该程序会伪装正常软件，安装后无图标显示，后台会静默下载并安装软件，存在隐私泄露，流量消耗等安全隐患。建议用户卸载。（威胁等级高）
		G-Ware/Android.Fakegupdt.cb[exp，rog]	该应用运行后会私自下载子包，上传手机固件信息，加载广告，并跳转到谷歌市场，会私自下载并提权安装，造成用户资费损耗，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	Microsoft Office 无效索引远程执行代码漏洞 (CVE-2014-6334)	Microsoft Word 在分析经特殊设计的 Office 文件时未正确处理内存中的对象，会导致当前用户的上下文中存在远程执行代码漏洞。这会允许攻击者执行任意代码，从而会损坏系统内存。以下产品受到影响：Microsoft Word 2007 SP3，Word Viewer，Office Compatibility Pack SP3。（威胁等级高）
	较为活跃的样本	Trojan[Ransom]/Win32.Crysis	此威胁是一种可以加密用户文件并勒索金钱的敲诈者木马，加密时不会影响系统运行的所有文件。目前，俄罗斯、乌克兰、日本受到攻击。（威胁等级中）
		Trojan[DDoS]/Linux.Znaich	此威胁是一种可以发动分布式拒绝服务攻击的木马家族。该家族样本基于 Linux 系统，运行后会向指定目标发起 DDoS 攻击。（威胁等级中）
		Trojan[Downloader]/Win32.Bedobot	此威胁是一种木马类程序。该家族样本运行后连会接远程服务器下载恶意代码，不过目前 URL 已经失效。它还可以遍历系统目录，分析下列后缀后的文件：.dbx、.wab、.mbx、.mai、.eml、.tbb、.mbox，收集系统中的邮件地址，回传至远程服务器。如果用户系统中包含重要人士的邮箱地址，危害会非常之大。（威胁等级中）

冒牌安卓 Flash Player 安装银行恶意软件

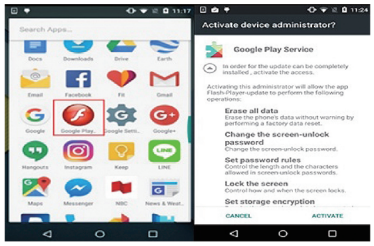
Tom Spring / 文　安天公益翻译小组 / 译

近日，安全研究人员警告说，针对安卓移动设备的假冒 Flash Player 应用程序已经浮出水面，它诱导受害者下载和安装银行恶意软件，并窃取用户的信用卡信息，能够击败双因素认证方案。

美国富国银行 (Wells Fargo)，发现金融服务公司 (Discovery Financial)，美国大通银行 (Chase)，Skype，Snapchat 和 Facebook 等服务的客户都是攻击目标。Fortinet 研究人员在近期表示，这个冒牌 Flash Player 应用程序是在 10 月 21 日发现的。它不是通过 Google Play 应用商店传播的，目前尚不清楚其传播途径。

Fortinet 的安全分析师说：“该银行恶意软件可以窃取 94 个不同的手机银行应用程序的登录凭证。由于能够拦截短信通信，该恶意软件还能够绕过基于短信的双因素身份验证。”Fortinet 称，该恶意软件正在美国、德国、法国、澳大利亚、土耳其、波兰和奥地利传播。一旦安装，它会在安卓设备的应用启动屏幕上创建一个图标。

相关安全专家介绍说，当用户启动假冒 Flash Player 时，“会被欺骗通过假的 Google Play 服务向应用程序授予设备管理员权限”。攻击者可以通过，安装在用户设备上的假冒 Google Play 服务屏幕 (实际上是屏幕覆盖) 激活恶意软件。

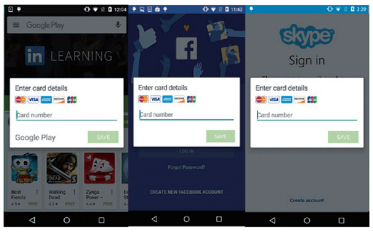


如果用户决定取消下载，则窗口关闭，但是之后会再次出现。从菜单选项中选择“激活”，可以取消该覆盖屏幕的。这样一来，就会向恶意软件授予完全的设备管理员权限。Fortinet 说，在这之后，Flash Player 图标会隐藏，该恶意软件会在后台保持活跃。

Lu 写道，一旦获得管理员权限，该应用程序就无法轻易从设备中卸载。更糟的是，恶意软件已被授予发送和接收短信的权限。Lu 指出，这种权限能够使攻击者绕过双因素身份验证系统。

Lu 写道：“在恶意软件安装之后，它会收集设备的信息，将其发送到其 C & C 服务器，并等待服务器发出新的命令。”授予恶意软件的权限包括向任何号码撰写、编辑、读取、发送和接收文本消息。其他权限包括修改手机上的内容、更改 Wi-Fi 连接设置、防止手机进入睡眠模式、将设备重置为出厂设置。

当用户启动目标银行、通信或社交媒体应用程序时，恶意软件就会在应用程序上方显示覆盖屏幕。此操作会强制受害者与恶意软件交互，因为用户在输入信用卡数据之前无法使用所需的应用程序。



在进一步检查恶意软件时，攻击者提示受害者输入他们的信用卡号，并且能够通过与 C&C 服务器通信来验证有效的信用卡。

可以通过禁用假冒 Flash Player 的管理员权限来删除恶意软件，步骤如下：设置 -> 安全 -> 设备管理员 ->Google Play 服务 -> 停用和卸载“Flash Player”。

根据 IBM X-Force 安全研究人员 4 月的一份报告，今年初，覆盖恶意软件急剧增加。X-Force 指出，今年 2 月，GM Bot 恶意软件代码在线泄露，此后，攻击者对覆盖恶意软件的兴趣开始上升。从那时起，黑客重新编写了泄露的代码，并重新推出了一个新的 GM Bot 变种，它的价格为 15,000 美元，远高于 6 个月前的 5,000 美元。

原文名称	Phony Android Flash Player Installs Banking Malware
作者简介	Tom Spring，卡巴斯基《安全周报》的的副主编。
原文信息	2016 年 11 月 1 日发布于《安全周报》(Threatpost)，原文地址 https://threatpost.com/phony-android-flash-player-installs-banking-malware/121696/
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《Sarvdap 样本分析报告》

近日，安天追影小组在进行安全事件梳理时，注意到了 Sarvdap 家族木马利用 RBL(Realtime Blackhole List) 过滤技术来进行选择性感染，安天追影小组对该家族的样本行为做简要的介绍。

Sarvdap 家族木马主要采用网络钓鱼的方式来进行传播， RBL 为实时黑名单列表的英文缩写，该列表中的 IP 地址均对外发送过垃圾邮件，一般被邮件过滤器用于过滤垃圾邮件。正是利用了 RBL 这一特性，Sarvdap 家族恶意代码能够避免感染 RBL 黑名单中的主机，来提高感染的有效性。

安天追影小组针对 Sarvdap 家族样本进行分析，通过分析可知该样本编译环境为 Microsoft C++ 8.0 的可执行文件。

Sarvdap 样本将功能函数和字符串地址进行硬编码，依赖于内存基地址为 0x2001000 的功能模块，当无法获取到功能函数及字符串时将无法运行，从而来增加静态调试的难度。

在程序执行时，该样本将进行自我复制，将自身复制到 %windir% 目录的文件夹里，并执行一个名为 svchost.exe 的进程，将主要代码写入该进程内存中，设置注册表自启动。

成功写入代码后，恶意进程会尝试访问 http://www.microsoft.com 来测试网络连接状态，若网络处于连通状态，则将被感染主机的 IP 在 RBL 列表中进行检索，判断是否进行感染，若被感染主机不在 RBL 黑名单中，则将继续进行感染，进而获取主机控制权，否则将终止执行恶意代码。

Sarvdap 样本的 RBL 检查模块进行深入分析可以发现，样本的 RBL 黑名单为硬编码，且列表中包含的服务器 IP 范围遍布全世界，可见该恶意代码攻击的范围之广。

通过本次事件的技术分析，可以发现网络钓鱼传播木马仍然是企业、政府和家庭用户一个非常普遍的威胁，攻击者也不断更新技术来躲避查杀，安全技术必然需要与时俱进。安天建议网络使用者，针对邮箱匿名邮件应谨慎对待，切勿随意下载启动，防范于未然。对于已经受到感染的机器设备，及时寻求专业人事行分析处理。目前，该样本已经被追影产品检出。

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。最终依据动态行为鉴定器将文件判定为木马程序。

文件名	41481C0A3180B63BBFF7CA4E754CD5F7
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	211 KB
MD5	41481C0A3180B63BBFF7CA4E754CD5F7
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[RAT]/Win32.Sarvdap.a
判定依据	动态行为

◆ 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

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=41481C0A3180B63BBFF7CA4E754CD5F7

该文件具有以下行为：注入其他进程、其他进程写入可疑数据、创建挂起的进程、填充导入表（疑似壳）、查找指定内核模块、读取自身文件、创建服务、访问其他进程内存、自启动、释放 PE 文件、获取驱动器类型、增加 run 自启动项、打开自身进程文件、启动服务、疑似桌面控制。

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
注入其他进程	★★★★	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
创建挂起的进程	★★	填充导入表（疑似壳）	★★
查找指定内核模块	★	读取自身文件	★★
创建服务	★	访问其他进程内存	★
自启动	★	释放 PE 文件	★
获取驱动器类型	★	增加 run 自启动项	★
打开自身进程文件	★	启动服务	★
疑似桌面控制	★		