安天 CERT 发布《Rovnix 攻击平台分析》研究报告

近期，安天安全研究与应急处理中心(安天 CERT)的安全研究人员在跟踪分析 HaveX 家族样本的过程中，意外地发现了 Rovnix 家族 (Trojan/Win32.Rovnix) 在建立其恶意代码下载服务器时，也开始使用类似 HaveX 的方式，即：使用 WordPress 搭建的网站，或入侵第三方由 WordPress 搭建的正常网站 (HaveX 的 C&C 服务器地址都是通过入侵由 WrdPress 搭建的网站得到的)。因此，安天 CERT 的研究人员对 Rovnix 家族展开分析。

Rovnix 家族于 2011 年首次被发现，至今依然十分活跃。该家族恶意代码插件众多，具有反调试、反虚拟机、反沙箱、安装 VBR-BootKit(VBR 全称 Volume Boot Record，卷引导记录)等技术手段，同时具有收集用户信息、盗取比特币、盗取银行密码、远程控制等功能。

该家族主要通过电子邮件传播，通过诱使用户点击邮件正文中的链接地址下载 Rovnix 主程序(安天 CERT 迄今共发现了 300 多个恶意代码下载地址)。主程序在执行后会搜集、回传用户系统信息，其中，信息回传地址以硬编码形式加密保存在主程序内部。随后，主程序根据 GDA(Domain Generation Algorithm) 计算出配置文件的下载地址。配置文件使用 RC2 算法加密，每个配置文件功能各不相同。例如：配置文件 Host.dat 存放插件下载服务器地址。主程序根据当前系统版本下载对应的插件列表，再下载该插件列表中的恶意插件，这些插件即是上述具有安装洋葱 (Tor) 客户端、盗取比特币、盗取银行密码、远程控制等功能的插件。

安天 CERT 联想到了 2014 年出现的 APT 事件 HaveX，HaveX 的 C&C 服务器都是通过入侵由 WordPress 搭建的正常网站得到的。Rovnix 中也有一部分的 URL 下载地址是入侵由 WordPress 搭建的正常网站得到的。Rovnix 在后期回传数据时用使用了其它的 C&C 服务地址。

Rovnix 是一个喜欢使用冷门技术的恶意代码家族，具有如下特性：它喜欢使用 VEH 异常处理机制，BootKit 使用的是 VBR-BootKit；支持众多的 Windows 版本，根据环境投放 32 位或 64 位的插件；定制化的插件支持多种恶意功能。这些特性让安天 CERT 的研究人员将其归类为专业化的攻击平台，是有可能被用来进行定向攻击的武器之一。

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，依据行为即可对 Rovnix 攻击平台进行有效检测，下为其自动形成的分析报告

文件被内部组件发现，经由 BD 静态分析鉴定器、美国软件交叉索引 (NSRL) 鉴定器、数字证书鉴定器、可交换信息 (EXIF) 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。依据 BD 静态分析鉴定器、静态分析鉴定器、动态行为鉴定器最终将文件判定为木马程序。

该文件具有以下行为：删除自身；其他进程写入可疑数据；读取自身文件；释放 PE 文件；创建互斥体 (mutex)；关机；增加 run 自启动项；获取系统版本；创建挂起的进程；访问其他进程内存；遍历进程；获取计算机名称；篡改系统文件创建时间；复制自身文件；创建特定窗体；获取驱动器类型；独占打开文件；打开自身进程文件；获取主机用户名称；请求加载驱动的权限。

文件名	rovnix-main
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	607 KB
MD5	6EB761EA46A40AD72018D3CEE915C4CD
首次发现时间	2015-07-30 19:41
末次发现时间	2015-07-30 19:41
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan.GenericKD.2397482
判定依据	静态分析
下次鉴定时间	约 2 周

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
删除自身	★★★★	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	★★	释放 PE 文件	★★
创建互斥体 (mutex)	★	关机	★
增加 run 自启动项	★	释放 PE 文件	★
获取系统版本	★★	创建挂起的进程	★★
访问其他进程内存	★	遍历进程	★
获取计算机名称	★	复制自身文件	★★
篡改系统文件创建时间	★★	创建特定窗体	★
获取驱动器类型	★	独占打开文件	★
打开自身进程文件	★	获取主机用户名称	★
请求加载驱动的权限	★		

◆ 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

完整报告地址：http://cloud.antiyfx.com/_lk/details.html?hash=6EB761EA46A40AD72018D3CEE915C4CD

安天周观察
主办：安天 2015年8月3日(总第3期)试行 本期4版 微信搜索：antiylab

报评

警惕商业自动化攻击平台

安天小编 / 文

7月21日，安天发布了《Rovnix 攻击平台分析》研究报告，2011 年就被发现的 Rovnix 家族，至今依然十分活跃。该家族恶意代码插件众多，具有收集用户信息、盗取比特币、盗取银行密码、远程控制等功能。同时，Rovnix 攻击平台的一些特性让小编想到了安天在 2015 年 05 月 28 日发布的《一例针对中国官方机构的准 APT 攻击分析》的报告，两者虽然一个被定性为木马，一个被定义为 APT 攻击，却具有一些共同的特性，比如具有反调试、反虚拟机、反沙箱等技术手段，隐蔽性较强。更重要的是：两者并非更多依赖攻击团队自身的能力，而是依托商业的自动化攻击测试平台来达成。

我们不禁要再次引用信息安全前辈 Bruce Schiner 的观点“我认为目前正在发生而且真正重要的趋势是：越来越多战争中的战术行为扩散到更广泛的网络空间环境中。这一点非常重要。通过技术可以实现能力的传播，特别是计算机技术可以使攻击行为和攻击能力变得自动化。”显然，高度自动化的商业攻击平台使这种能力扩散速度已经超出我们的预测。

安天认为同样存在另外一种倾向，就是商业化的工具和样本会更多的出现在国家与政经集团的相互的 APT 攻击当中。一种有趣的现象是，被先进者淘汰的滑膛枪，同样可以用于屠杀使用弓箭的原始部落(或平民)，而这种“穷国原子弹”可能因为门槛较低对安全形成巨大的杀伤力。

我们需要提醒各方关注的是，商业渗透攻击测试平台的出现，一方面成为高效检验系统安全的有利工具，但对于缺少足够的安全预算、难以承担更多安全成本的国家、行业和机构来说，会成为一场噩梦。在这个问题上，一方面需要各方面建立更多的沟通和共识；而另一方面毫无疑问的是当前在攻防两端均拥有全球最顶级能力的超级大国，对于有效控制这种武器级攻击手段的扩散，应该负起更多的责任。而有效地防范这些具有武器级水准的攻击是安全厂商的安全和服务将面临的挑战。

安天 CERT 发布《Rovnix 攻击平台分析》研究报告
第四版

安天参与互联网网络安全威胁治理行动

7月31日，由国家互联网应急中心(CNCERT)和中国互联网协会网络与信息安全工作委员会牵头组织的互联网网络安全威胁治理行动启动会在京召开。首批有24家单位签署《互联网网络安全威胁治理行动承诺书》，共同配合此行动的开展。

威胁互联网网络安全的行为涉及多个环节，互联网网络安全威胁的治理需要多方的共同参与，发挥各自的技术和资源优势，规范各自的行为并承担相应的社会责任。所以在首批 24 家企业中，包括了中国电信、移动、联通三家运营商、阿里、百度等互联网厂商和安天、绿盟、启明等安全厂商以及域名注册服务商、数据中心(IDC)、搜索引擎和互联网企业等构成。本次行动将以行业自律的方式，动员行业内相关单位，从加强监测入手，通过密切配合、积极处置、曝光攻击者黑名单等措施，有效防范和治理威胁互联网网络安全的行为。

专家发现：黑客可以通过彩信远程控制 Andorid 设备

攻击者仅仅需要得到你的手机号码，然后通过这个手机号码，攻击者就可以使用彩信将一个经过精心设计的多媒体文件发送给目标设备。通过这个媒体文件，攻击者就可以在目标设备上远程地执行任意代码了。在一次完全成功的攻击中，黑客会在你看到这条彩信之前就将其删除，你仅仅只能看到一条手机的通知信息。这些漏洞的危险系数非常的高，因为黑客在利用这些漏洞的时候并不需要目标设备进行任何的操作。不同于网络钓鱼攻击，这种漏洞甚至可以允许攻击者在你睡觉的时候对你发动攻击。在你醒来之前，攻击者将会从设备中删除所有的入侵记录，然后你又会和往常一样继续你的工作和生活，与之前不同的是你使用的手机变成了一个带有木马病毒的手机。(http://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/)

每周 APT(高级持续性威胁) 新闻

类 型	内 容
中文标题	社交媒体变武器：俄黑客用 Twitter 无痕访问政府电脑
报道时间	2015 年 7 月 30 日
关联对象	俄国黑客、Twitter
内容概述	据《财富》网络版报道，俄国黑客找到了使用 Twitter 与目标电脑里已感染的恶意软件沟通的方法，这可以使他们侵入机密政府电脑系统的同时掩盖自身行 踪。《金融时报》指出，这些黑客们在社交媒体 Twitter 上传特殊图像，该图像可暗地里导向事先安装好的恶意软件，这些恶意软件便可以进行窃取文件或者其他行为。这个方法的优势在于目标电脑系统并不会注册这类入侵，而仅仅将其当作一个在 Twitter 上发布微博的行为。 著名的网络安全公司 FireEye 发布了一篇关于上述方式的报告，并将该方式命名为“Hammertoss”。FireEye 写道：“这类攻击方式的设计使防御者既难以发现此类活动，也无法将其定性。该公司称“Hammertoss”的幕后黑手极有可能是俄国黑客。 “社交媒体的武器化是一个不断增长的威胁。”商务智能公司 KCS 的高管斯图尔特·普勒－罗布 (Stuart Poole-Robb) 提到：“这种方式可轻易将信息传递给隐蔽的恶意软件。”
链接地址	http://www.cnbeta.com/articles/415823.htm

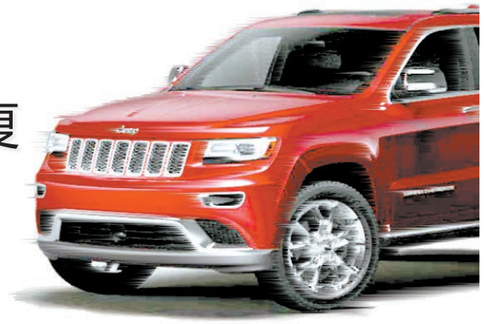
本周值得关注的恶意代码信息

本周有 13 个 PC 恶意代码值得关注 (表中的恶意代码名称使用安天规范命名)

病毒分类	病毒名称	病毒特点
PC 恶意代码	Trojan/Win32.Rikamanu 发现日期：2015 年 7 月 25 日	此威胁能够窃取所入侵的计算机信息。(威胁等级较低)
	Trojan[Backdoor]/MSIL.Spedear 发现日期：2015 年 7 月 26 日	此威胁能够打开被入侵计算机的后门。(威胁等级较低)
	Trojan[Downloader]/Win32.Codumwis.A 发现日期：2015 年 7 月 27 日	此威胁未经用户允许，下载、安装其他程序到用户电脑，包括其他恶意程序。
	Trojan[Backdoor]/MSIL.Povbop.A 发现日期：2015 年 7 月 27 日	此威胁给予恶意黑客未授权的访问权限，控制用户电脑。
	Worm/Win32.Gamarue.AU 发现日期：2015 年 7 月 27 日	此威胁能够使恶意黑客控制用户电脑，窃取用户敏感信息，更改电脑安全设置。其安装由漏洞利用包或其他恶意代码执行，也可以通过垃圾邮件附件传播，或通过被感染的可移动驱动器安装。
	Trojan/Win32.Blakamba.gen 发现日期：2015 年 7 月 28 日	此威胁能够下载恶意代码到用户电脑。
	Trojan[Backdoor]/Win32.Cobrike 发现日期：2015 年 7 月 28 日	此威胁能够打开所入侵电脑的后门，也能够进行其他恶意行为。(威胁等级较低)
	Trojan[Dropper]/Win32.Zbot.D 发现日期：2015 年 7 月 28 日	此威胁能够窃取用户个人信息和财务信息，给予恶意黑客未授权的访问权限，从而控制用户电脑。也可以降低用户互联网浏览器安全性，关闭防护墙。
	Trojan[Clicker]/Win32.Frosparf.F 发现日期：2015 年 7 月 28 日	在未经用户允许或用户不知情的情况下，此威胁利用用户点击网上广告，通过制作网站或应用为恶意黑客赚取金钱利益。
	Trojan/Win32.Cryptolocker.W 发现日期：2015 年 7 月 28 日	此威胁能够对被入侵电脑的文件加密，勒索用户付款解密。(威胁等级较低)
	Worm/Win32.Xtrat.C 发现日期：2015 年 7 月 29 日	此威胁通过多种方式进行传播，包括通过自行复制到可移动驱动器，网络文件夹或通过电子邮件传播。
	Trojan[GrayWare]/MSIL.Irstil.A 发现日期：2015 年 7 月 29 日	此威胁能够收集用户敏感信息，发送给恶意黑客。
	Trojan[Backdoor]/Win32.Netduke 发现日期：2015 年 7 月 30 日	此威胁能够打开所入侵电脑的后门，进行其他恶意活动。

疯狂的克莱斯勒安全漏洞：

140 万辆车将采用 U 盘修复



Iain Thomson / 文 安天公益翻译小组 / 译

在菲亚特克莱斯勒存在的安全漏洞被发现几天之后，NHTSA(美国国家公路交通安全管理局) 召回了 140 万辆汽车。

周二，著名黑客查理·米勒和克里斯·瓦拉塞克警告说：内置到菲亚特克莱斯勒汽车的计算机系统存在漏洞，攻击者能够利用该漏洞远程控制引擎、刹车和娱乐系统。

汽车通过菲亚特克莱斯勒的 UConnect 蜂窝网络连接到互联网，因此，只要知道汽车的公共 IP 地址，任何人都能够无需验证地远程访问和篡改汽车设置。NHTSA 一直在验证菲亚特克莱斯勒的漏洞修复措施是否完全有效。该汽车巨头已经针对漏洞的根本原因开发了更新，不幸的是，该更新要通过插入 U 盘进行安装。

“为了解决该安全漏洞，克莱斯勒要求无线服务提供商断开了能够未经授权地访问汽车网络的开放的蜂窝连接。”NHTSA 召回通知这样说。

“该措施可能还没有付诸所有车辆，而且无法解决其他能够通过软件更新补救的访问方法。制造商尚未提供通知日程。”

此次召回影响到菲亚特克莱斯勒的 5 款车型：2013-2015 公羊；2014-2015 吉普大切诺基、切诺基和道奇杜兰戈；2015 道奇战马和道奇挑战者；过去两年中出售的道奇蝰蛇。

受影响车辆的车主将得到一个包含更新的 U 盘，或者他们可以自行下载补丁、将其复制到备用 U 盘。另外，克莱斯勒经销商将免费更新汽车软件。

“黑进车辆的能力并不容易。安全研究人员查理·米勒和克里斯·瓦拉塞克耗用了数月的时间来窃听并控制米勒 SUV。他们可都是专家。”克莱斯勒在一份博客中表示。

“7 月 23 日的安全措施之后，此次召回将解决软件更新问题，这需要独特和广泛的技术知识、涉事车辆的长时间物理访问、较长的代码编写时间。”

一个通信端口被无意开放，这使得它能够监听并接收来自未经验证的来源的命令。此外，默认情况下，无线电防火墙规则是广泛开放的，这使得外部设备能够与无线电通信。迄今为止，除了在研究环境下，还没有报道或发现与此相关的漏洞实例。

在去年的黑帽安全大会上，米勒和瓦拉塞克指出，保护汽车的计算机系统实际上是很容易的。他们开发了一个能够阻止大多数黑客活动的简单入侵保护系统。

“对计算机来说，IDS(入侵保护系统) 很逊；但事实证明，它们对汽车很有效，因为汽车是比较简单的。”米勒说。

大约 7 个月前，克莱斯勒被告知了该无线漏洞。开发了修复补丁后，制造商本月早些时候发布了补丁服务包，但是未大肆宣扬。直到米勒和瓦拉塞克崩溃在公路上破坏了一辆汽车之后，该漏洞才被公众所知。

克莱斯勒汽车公司的最大客户之一是美国警察，而他们将会特别恼怒。狡猾的犯罪分子能够破坏追赶警员的汽车引擎，并对此津津乐道。所以这些警车最好赶快进行修复。

受影响车辆的车主应该都知道了车辆存在漏洞的问题，但是对于很多车主来说，手动更新软件可能是一个问题。考虑到很多人不会更新个人电脑的软件，所以让他们自己动手更新车辆软件也会有问题。

原文名称	Crazy Chrysler security hole - USB stick fix incoming for 1.4 million cars
作者简介	Iain Thomson，The Register 的记者，专注 IT 领域。
原文信息	2015 年 7 月 24 日发布于 The Register，原文地址 http://www.theregister.co.uk/2015/07/24/chrysler_recall_for_wireless_hacking_hole/
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。