高级威胁

此报告为针对近期出名的 cve-2014-1761 免杀工具的样本，追影无需升级即可检测。

文件被页面手工提交发现，经由安全云鉴定器、智能学习鉴定器、动态行为 (默认环境) 鉴定器等鉴定分析。

依据动态行为鉴定器最终将文件判定为高级威胁。

该文件具有以下行为：仿冒 SVCHOST；利用漏洞释放 PE 文件；格式溢出；隐藏文件；填充导入表 (疑似壳)；释放 PE 文件；获取系统内存；获取系统版本；创建挂起的进程；访问其他进程内存；创建特定窗体；获取驱动器类型；独占打开文件；获取计算机名称；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	4ba4594cf5074b8239f5c6ac95c18ad1d76b22a571a0aebf7a254bad582e3bc1
文件类型	Document/Microsoft.RTF[：Rich Text Format]
大小	493 KB
MD5	311CEE2FEDD8EA96A4569DE35FB6D12A
首次发现时间	2015-07-19 11：56
末次发现时间	2015-07-19 11：56
病毒类型	高级威胁
恶意判定 / 病毒名称	Exploit.CVE-2014-1761
判定依据	动态行为
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
仿冒 SVCHOST	★★★★	格式溢出	★★★★
利用漏洞释放 PE 文件	★★★★		

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
隐藏文件	★★	填充导入表 (疑似壳)	★★
释放 PE 文件	★	获取系统内存	★★
获取系统版本	★★	创建挂起的进程	★★
访问其他进程内存	★	创建特定窗体	★
获取驱动器类型	★	独占打开文件	★
获取计算机名称	★	获取主机用户名称	★
查找特定窗体	★	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，ffice 2003，flash，wps，FoxitReader，adobe reader

完整报告可点击 http://antiy.pta.center/_lk/details.html?hash=311CEE2FEDD8EA96A4569DE35FB6D12A 下载。

不忘初心 大圣归来

——哈尔滨举行集体观影活动

7 月 17 日，哈尔滨总部举行集体包场观影活动，全体员工观看影片《大圣归来》。从放映厅出来，，每个人的心里都装着一个齐天大圣。但愿每个人都领会到大圣诠释的自我救赎，不忘初心，还原内心英雄！

一句话消息

◆ 游戏公司 Epic Games 的论坛遭黑客攻击，用户账户、密码及年龄等信息遭泄露。

◆ 7 月 12 日，美国国民警卫队警告可能的数据泄露，但这次数据泄露事件与联邦人事局的黑客攻击无关

◆ 7 月 13 日，流行即时通讯软件 Telegram 过去几天遭遇了 DDoS 攻击，导致亚洲以及全球用户出现登录和收发信息问题。

◆ 7 月 13 日，马来西亚警方的推特和 facebook 账户遭到疑似黑客入侵。自称是“AnonGHost”的黑客，在侵入警方的账户后，更向首相纳吉放话“我们冲着你来”。

◆ 黑客入侵比特币云挖掘平台 Cloudminr.io，涂鸦了网站首页并在网络上以 1 比特币的低价“甩卖”近 8 万用户数据。

(以上内容来自互联网搜索)

安天周观察

主办：安天 2015 年 7 月 (总第 2 期) 试行 本期 4 版 微信搜索：antiylab

安天潘宣辰接受央视采访 揭秘网络黑色产业

7 月 19 日，CCTV-13(央视新闻频道)《新闻直播间》播出了“打击网络黑色产业”的专题节目。安天移动安全团队潘宣辰和其他业内网络安全工程师、研究员做相关分析，并给广大网民提出避免网络安全风险的基本常识和方法。

有报告显示：2011 年至 2014 年底，中国公民个人信息多达 11.27 亿条隐私被泄露，其中包括电话号码、电子邮件、身份证号码、账号、密码等信息被窃取。而短信拦截马作为一个功能简单开发成本低，但获利颇高的黑色行业，在短时间内便形成了一条完整的黑色产业链。从 2013 年 5 月开始，到 2014 年短信拦截马集中爆发，此类木马开始升级，在通过其他手段获取用户的信息后，无论是精度还是时效性都可以做到更有针对性和欺骗性的攻击。

安天 AVL Team 移动安全团队持续关注并监测到此类威胁，并于 2015 年 5 月发布了《短信拦截马 " 相册 " 综合分析报告》。可关注安天网站查阅完整报告。http://www.antiy.com/response/emial.html，同时用户可以下载并使用AVL Pro对该类木马进行检测和查杀。

安天成为移动应用指定安全检测机构

7 月 21-23 日，第十四届中国互联网大会召开。

为保障网民权益，治理恶意手机应用软件，12321 举报中心发起手机软件“安全百店”行动，在“2015 中国网民权益保护论坛”上，宣布安天成为该行动的移动应用指定安全检测机构。

德国通过严格的“关键基础设施”保护法

关键词：德国 “关键基础设施”保护法

随着网络安全威胁愈演愈烈，德国刚刚通过了一项法案，对 2000 余家关键服务提供商推行最低安全标准，如果提供商在两年内无法达到新规要求，就将被处罚。该法案在 6 月通过了众议院，并于上周五通过了德国联邦参议院投票。这项法案将会影响被认为是“关键基础设施”的机构，如交通、医疗、水电、电信、金融、保险公司。(http://www.aqniu.com/news/8718.htmll)

社保系统三年曝出近 200 条漏洞，黑客可获取多种敏感信息

关键词：社保系统 漏洞 信息泄露

7 月 16 日消息，因为个人信息泄露导致的电信诈骗时有发生，骗子们知道受害者的单位、名字、身份证号、收入水平。社保系统漏洞导致的个人信息泄露，可能是其中的来源之一。

2013 年至今，国内漏洞平台上提交的各种社保、医保漏洞高达 200 余条，存在问题的不乏省部级官网。(http://www.2cto.com/News/201507/419624.html)

《大圣归来》

安天小编 / 文

7 月 17 日下午三点半，安天哈尔滨总部集体提前收工，被几辆大客车，运到某影院，包场观看大圣归来。

画面流转，时而一起爆笑，时而一起沉默。

当画面中那条精致的龙飞扬天际的时候，我心底突然煽动了一下。因为那不是我们在一切魔幻电影中看到的，带有翅膀并喷火的西方龙，而是真正威武修长的中国龙。尽管情节和编剧还不够完美，但这真的是我们久违的国产动画精品。

多年来，国人期待国产动漫再现“大闹天宫”的辉煌。但我们却看惯了“孙悟空”大战“奥特曼”式的无厘头滥造，看到“高铁侠”对“铁道侠”的赤裸裸抄袭。但如果把这种审视的目光放到我们自己，放到网安产业身上，我不禁亦感到惭愧，我们是否很长时间同样也因种种原因，钝化了应对威胁的敏锐，失落了保障用户价值的勇气，冷却了打造精品的热血。

若干年前，安天决定回购全部渠道中的盒装“安天防线”，退出零售市场。一位软件连锁的副总连夜到哈尔滨劝说安天负责人。他语重心长的说，安天退出桌面的不利影响，三年后你们自己才会看到。而当时，我们对自己说，我们要的不止是市场的“存在感”，我们需要真正能达成用户价值的场景。

当年之憾，不再评说。今天，当安天剑指 APT 的时候，我们能否把自己的解决方案打造成金甲倚天的孙大圣。

我相信，大圣终将归来。

每周 APT(高级持续性威胁) 新闻

类 型	内 容
中文标题	俄罗斯对五角大楼发动钓鱼攻击
报道时间	2015 年 7 月 22 日
关联对象	俄罗斯黑客、美国五角大楼
内容概述	来自俄罗斯的顶尖 APT (高级持续性威胁) 攻击小组曾攻击过美国白宫和国务院，最近又开始对五角大楼发动了钓鱼攻击。 《每日野兽》透露，“曾经入侵白宫和国务院的俄罗斯黑客将视线转向了五角大楼。这次，黑客使用了更为高明的方法隐蔽自己，隐藏自己的行踪。”《每日野兽》获取到了国防部发布的邮件通知，通知中警告称，“至少 5 台”国防部电脑已经被黑客攻陷，通知中确认了此次事件的黑客与针对白宫、国防部攻击的黑客存在关联，但没有提及黑客窃取了哪些信息。 国防部的通知中提到，黑客会进行多阶段的攻击，一旦第一个组件感染了目标，它就会从 C&C 服务器下载其他的 payload，这些连接都经过了加密，以防止检测。 《每日野兽》获取到的另一份通知中警告称，黑客正将目标瞄准五角大楼、美国政府部门和私人企业，他们使用了 Hacking Team 泄露事件中的其中一个 Adobe Flash 漏洞。
链接地址	http://www.freebuf.com/news/72757.html

每周新恶意代码信息

本周有 1 个移动恶意代码和 12 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
移动恶意代码	Trojan/AndroidOS.Gupno 发现日期：2015 年 7 月 22 日	此威胁是针对 Android 设备的 Trojan 木马，伪装成合法的 app，试图收取用户费用，也能够在所攻击的设备上显示广告。
PC 恶意代码	Trojan/Win32.Fareit.AE 发现日期：2015 年 7 月 20 日	此威胁能够窃取用户个人信息，如：用户名和密码，发送给恶意黑客。
	Trojan[Downloader]/Win32.Kolilks.F 发现日期：2015 年 7 月 20 日	此威胁未经用户允许，下载、安装其他程序到用户电脑，包括恶意程序。
	Trojan[RiskWare]/Win32.Aneatop.A 发现日期：2015 年 7 月 20 日	此威胁能够收集用户敏感信息，发送给恶意黑客。
	Trojan[Dropper]/MSIL.Golbla.C 发现日期：2015 年 7 月 20 日	此威胁能够安装其他恶意的或多余的软件到用户电脑。
	Trojan[Backdoor]/Win32.Darksun.A 发现日期：2015 年 7 月 21 日	此威胁能够打开所入侵电脑的后门。(威胁等级较低)
	Trojan[Backdoor]/Win32.Chaapt.A 发现日期：2015 年 7 月 22 日	此威胁给予恶意黑客未授权的访问权限，控制用户电脑。
	Trojan[Proxy]/Win32.Mediana 发现日期：2015 年 7 月 22 日	恶意黑客能够利用此威胁隐藏其身份，采取行动，包括发送垃圾邮件。
	Trojan/Win32.Zbot.VM 发现日期：2015 年 7 月 22 日	此威胁能够监控用户按键信息，发送给恶意黑客，包括类似用户浏览银行网站等网上活动信息。
	Trojan[Backdoor]/Win32.PcClient.CQ 发现日期：2015 年 7 月 23 日	此威胁能够给予恶意黑客未授权的访问权限，控制用户电脑。
	Trojan[RiskWare]/Win32.Bholog.B 发现日期：2015 年 7 月 23 日	此威胁能够收集用户敏感信息，发送给恶意黑客。
	Trojan[Downloader]/Win32.Banload.BCL 发现日期：2015 年 7 月 23 日	此威胁是 Win32/Banload 家族的一部分，能够下载其他恶意代码到用户电脑，包括 Win32/Banker and Win32/Bancos。同时也能够窃取银行用户名称和密码，发送给远程攻击者。
	Trojan[RiskWare]/MSIL.Tese.A 发现日期：2015 年 7 月 24 日	此威胁能够收集用户敏感信息，发送给恶意黑客。

美国决定不就 OPM 黑客事件公开指责中国

Ellen Nakashima / 文 安天公益翻译小组 / 译

美国政府雇员记录大规模泄露事件的几个月之后，奥巴马政府决定不公开指责中国的黑客活动或者使用网络措施破坏 OPM(人事管理局) 被盗的敏感数据。美国官员表示，部分原因是不愿透露美国调查人员已经获得的证据。

“我们选择不做出任何关于责任方的官方声明”，一位政府高级官员说，尽管普遍认为中国是幕后的始作俑者。该官员提到了一些担忧因素，包括公开指责中国可能需要公开美国自己的间谍活动和网络空间能力。

因此，中国不须承担 OPM 黑客活动 (被美国官员描述为美国历史上最具破坏性的网络黑客活动之一) 的追责后果，这似乎也反映出美国对商业和传统间谍活动的区别对待。在做出这样的区别时，美国可能会遵守被其他国家无视的不成文的规定。美国政府的冒险行为实际上发出了一个信号：与保护联邦雇员的数据相比，它更愿意捍卫美国产业的秘密。

在过去的一年半中，美国一直“积极”指控外国政府窃取美国各大公司的企业机密。最值得关注的是，去年，美国司法部就 5 名中国军官涉嫌美国钢铁、西屋等公司的黑客活动提出了刑事指控。

美国对政府持有数据的渗透活动的响应一直较为克制，部分原因是美国官员认为这属于传统的间谍活动。对美国间谍机构来说，经济间谍是一个单独的类别，可以给别国有力的回击，比如新的制裁措施等。

在计算机屏幕上用放大镜观察到的中国地图
Edgar Su / 路透社

OPM 事件泄露了超过 2200 万人的个人数据，包括社会保障号码、绩效评估、申请安全许可的数百万雇员的家人和朋友 (作为参考人) 的姓名。攻击发生后，美国一直寻求支撑整个联邦政府的 OPM 系统和计算机的安全性。官员们减少了特权用户帐户的数量，增加了登录的安全步骤，并修复了关键的软件漏洞。

美国官员私下表示，取证证据毫无疑问地将该事件指向中国。但是官员说，白宫不愿透露如何做出的判断，这可能不仅涉及追踪入侵源，还会涉及美国利用其能力拦截外国政府官员的通信。

“在这一点上，公开责任国的利益不足以抵消情报收集能力曝光导致的损失”，美国官员说。

前白宫网络官员罗伯特·K·斯内克指出，不愿报复可能会鼓励对手继续攻击美国政府的网络。他指出，在整个冷战时期，逮捕和驱逐涉嫌间谍被视为一种重要的威慑手段。

“我们可以明确地说，与冷战时期相比，现在人们可以在网络空间执行更多的间谍活动，而且导致的后果更少”，外交关系委员会高级研究员斯内克说。“没有人会因为网络入侵被关进监狱。中国或俄罗斯的操作者也不会以任何方式把自己置于危险之中。”

前美国情报官员说，鉴于冷战期间形成的不成文的间谍规范，在某些方面来说，OPM 黑客活动是一场公平的游戏。

即使在 OPM 事件之前，美国对网络入侵的响应也有所不同，主要取决于攻击目标和性质。

去年，美国官员发现了针对白宫和国务院机密计算机网络的攻击企图。官员私下承认，调查人员发现入侵黑客与俄罗斯政府有关，但是并没有指控俄罗斯。该案件也被视为传统的间谍活动。

相反地，去年秋天，索尼影视娱乐遭到黑客攻击，旨在阻止其讽刺朝鲜的电影 (《刺杀金正恩》) 的放映。自后，奥巴马立刻指责朝鲜，并实施了制裁制度。美国官员说，该攻击具备严重的破坏性和胁迫性，因此美国做出了激烈的响应。

今年 4 月，奥巴马签署了一项行政命令——针对恶意网络行为创建针对性的制裁方案，如破坏重要的基础设施、扰乱网络，或窃取美国公司的商业秘密或美国人的个人数据进行牟利。

原文名称	U.S. decides against publicly blaming China for data hack
作者简介	Ellen Nakashima，《华盛顿邮报》国家安全领域的记者，主要关注情报、科技和公民自由问题。
原文信息	2015 年 7 月 21 日发布于《华盛顿邮报》，地址：https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/ 2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html
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。