# 安天周观察

主办：安天　2016 年 10 月 10 日（总第 59 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

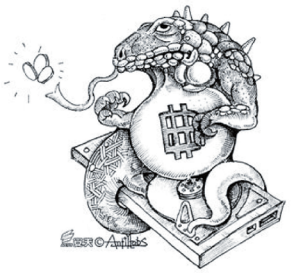

## 安天技术文章汇编——
# 《“敲诈者”分析专题分册》发布

安天从 2014 年开始研究跟踪勒索软件，深入分析其机理，积极改善安天产品对其的检测与防御能力，并发布多篇分析报告。今年 9 月，安天重新修订校对部分报告，并补充了一次安天内部相关讨论的内容，推出：安天技术文章汇编·热点事件卷——《“敲诈者”专题分册》，供安天内部学习和业界同行交流参考。

安天智甲终端防御系统产品负责人徐翰隆为《“敲诈者”专题分册》撰写了序言。下为序言内容节选（全文可见安天微信公众号 antiylab）：

勒索软件对国内政企网络安全也带来了新的挑战，在较长时间内，国内部分政企机构把安全的重心放在类似网站是否被篡改或 DDoS 等比较容易被感知和发现的安全事件上，但对网络内部的窃密威胁和资产侵害则往往不够重视。因为这些攻击更难被发现，但“敲诈者”以端点为侵害目标，其威胁后果则粗暴可见。同时，对于类似威胁，仅仅依靠网络拦截是不够的，必须强化端点的最后一道防线，必须强调终端防御的有效回归。

安天智甲终端防御系统研发团队依托团队对“敲诈者”的分析和预判，依托安天反病毒引擎和主动防御内



核，完善了多点布防：包括文档访问的进程白名单、批量文件篡改行为监控、诱饵文件和快速文件锁定等。经过这些功能的强化，安天不仅能够有效检测防御目前“敲诈者”的样本和破坏机理，还对后续“敲诈者”可能使用的技巧进行了布防。除了 PC 端的防护产品，安天 AVL TEAM 对 Android 平台的反勒索技术做了很多前瞻性的研究工作，并应用于安天移动反病毒引擎中。

一直以来，安天都乐于进行技术分享，积极活跃在安全会议上分享自身最新的研究进展，并始终坚持原创、沉淀、共享的原则。从 2006 年至今，安天技术文章汇编印发了如《热点事件分析》、《移动安全分册》、《工控安全分册》、《专题报告分册》、《APT 专题分册》、《文献翻译分册》等 15 卷中文版及部分英文版分册，印刷 70 余次，总印量超过 40000 多

册，全部免费在业界发放，与同行共享。此外，安天有关技术负责人还参与翻译了《Reverse Deception》等书目。安天的公益翻译小组也持续面向业界推出“安天每周一译”。安天还曾赞助 GPG 等开源软件开发工作。

在本次发布的《“敲诈者”专题分册》中，除其中一份关于“敲诈者”病毒的相关讨论之外，其他内容都已在网上公开，更多关于勒索软件专题报告内容详情可参见安天微信公众号自定义菜单“技术分享——勒索软件专题报告”，该系列分析报告内容如表 1 所列。

表 1　敲诈者（勒索软件）安天系列分析报告

| 发布时间 | 报告 |
|---|---|
| 20150430 | 《“攻击 WPS”样本实为敲诈者》 |
| 20150803 | 《揭开勒索软件的真面目》 |
| 20151204 | 《邮件发送 JS 脚本传播敲诈者木马的分析报告》 |
| 20160209 | 《发现使首例具有中文提示的比特币勒索软件“LOCKY”》 |
| 20160408 | 《勒索软件家族 TESLACRYPT 最新变种分析》 |

## ◆ Spamhaus 警告：IPv4 网络劫持已经越来越严重

近日，根据国际非盈利组织跟踪垃圾邮件团伙的 Spamhaus 调查报告显示，网络挟持事件的数量正在激增。Spamhaus 昨日的博客中描述了一家知名的垃圾邮件运营商通过模仿已去世几年的站长，成功地接管了合法公司的 IPv4 空间。通过使用他的姓名和域名极为相像的电子邮件地址，垃圾邮件发送者成功地接管了 IPv4 地址，然后将其连接到垃圾邮件僵尸网络中。Spamhaus 还表示，建议执法机构开始起诉这些犯罪劫持团伙和互相勾结的垃圾邮件发送者。(http://www.cnnvd.org.cn/news/show/id/7705)

## ◆恶意程序通过计算 Word 文档数躲避检测

近日，卡巴斯基实验室的安全研究人员发现了一种 Word 宏恶意程序能通过计算运行环境的 Word 文档数量去躲避检测。安全研究人员通常利用虚拟机测试可疑程序，虚拟机环境一般缺乏多个 Word 文档和其它类型的文件，这意味着如果恶意程序在系统中没有找到 2 个以上的 Word 文档，那么它可以假设自己正在被研究。研究人员发现了该恶意程序如果在本地磁盘内没有发现 2 个以上的文档就会拒绝执行。如果发现两个以上的 Word 文档，它会执行 PowerShell 脚本，并从 silkflowersdecordesign.com 这个网站下载按键记录程序。(http://www.solidot.org/story?sid=49804)

# 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | 微软日记本功能格式漏洞过多，微软补丁彻底删除该应用 |
| 英文标题 | Microsoft Removes Windows Journal Due to Security Flaws |
| 作者及单位 | Eduard Kovacs；Securityweek |
| 内容概述 | 近日，据 Softpedia 报道，是最新的由安全专家 Honggang Ren 报告的内存堆溢出 (Heap overflow).JNT 文件特有漏洞令微软痛下杀手，由于存在太多漏洞，微软认为不值得投入过多精力更新，索性直接彻底删除日记本应用。<br>安全专家 Honggang Ren 报告的内存堆溢出 (Heap overflow) 漏洞，能够通过恶意 JTP 文件传播，感染后攻击者能够在 PC 内存其它堆栈写入可执行代码，进行攻击和破坏行为，用户在打开 JNT 文件格式后就会运行恶意代码。<br>微软还建议，有便签功能需求的用户，可以使用 OneNote。如果你还是更喜欢古老的 Windows 日记本，微软也单独提供了一个可下载版本，但注意其中同样存在安全漏洞。 |
| 链接地址 | http://www.securityweek.com/microsoft-removes-windows-journal-due-security-flaws |

# 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.CheckPhone.a[prv，rmt]2016-09-29 | 该应用运行后会隐藏图标，后台会接收远程指令，获取用户手机号码和接收短信并上传到服务器，会造成用户隐私泄露，建议立即卸载。( 威胁等级高 ) |
| | | G-Ware/Android.PlaySound.a[rog]2016-09-29 | 该应用程序会伪装成系统应用，运行后创建后台服务并设置最大音量播放自带音频，建议卸载。( 威胁等级低 ) |
| | | RiskWare/Android.Vzlomvk.a[exp]2016-09-30 | 该应用程序无实际功能，会跳转 Google 指定页面，诱导用户下载指定应用，避免造成资费损耗，建议谨慎使用。( 威胁等级低 ) |
| | | Trojan/Android.Litecoins.a[exp]2016-09-30 | 该应用软件嵌入了恶意代码，会在用户不知情的情况下，私自联网进行电子货币的开采，赚取非法所得，造成用户手机设备损耗。( 威胁等级高 ) |
| | 较为活跃的样本 | Trojan/Android.raccoon.b[prv，rmt，spy] | 该程序运行后会释放恶意子包，通过子包联网下载恶意 APK，进行动态加载。接收远程指令控制，收集用户设备固件、安装列表、信箱、通话记录、通讯录等隐私信息，设置呼叫转移、短信拦截、电话拦截，制作虚假短信、加解密文件、删除文件、置顶界面、发送短信、下载更新恶意 APK，避免造成隐私泄露和资费损耗，建议立即卸载。( 威胁等级高 ) |
| | | G-Ware/Android.FakeApp.bn[rog，exp] | 该应用程序会伪装成 Pokemon GO 的相关应用，无实际功能。运行后会诱导用户激活设备管理器，访问指定网页，推送广告或诱导用户下载未知应用，会造成用户资费损耗，建议卸载。(威胁等级低) |
| | | Trojan/Android.moproot.b[prv，exp] | 该程序安装后无图标，启动后会监听用户手机启动程序及用户短信信息，会造成一定的资费损失，建议卸载该软件。( 威胁等级高 ) |
| | | Trojan/Android.SmsSend.kl[exp] | 该应用为一款色情图片应用，运行后会私自发送短信到指定 SP 号，并拦截用户短信，造成资费消耗，请谨慎使用。( 威胁等级高 ) |
| | | G-Ware/Android.Fakesysui.j[rog，exp，prv] | 该程序会伪装系统应用，安装后无图标，会诱导激活设备管理器。后台联网获取推送配置信息并推送广告，静默下载并安装推广 APP，同时还存在恶意刷单行为，私自反复安装卸载指定列表应用，影响手机性能，建议立即卸载，避免造成资费损耗。( 威胁等级低 ) |
| | | Trojan/Android.Rootnik.g[rog，exp] | 该应用包含色情敏感内容，运行后会获取 root 权限，私自下载并静默安装恶意应用，会弹出虚假广告界面诱导用户下载，请用户及时卸载以免造成资费损耗。( 威胁等级中 ) |
| PC 平台恶意代码 | 活跃的格式文档漏洞、0day 漏洞 | 多款 Cisco 产品信息泄露漏洞 (CVE-2016-6415) | 多款 Cisco 产品中的服务器 IKEv1 实现过程中存在信息泄露漏洞。远程攻击者可通过发送 Security Association 协商请求，利用该漏洞获取来自设备内存的敏感信息。( 威胁等级高 ) |
| | 较为活跃的样本 | Trojan[Dropper]/Win32.Renum | 此威胁是一种具有捆绑行为的木马类程序。该家族样本运行后会释放捆绑的恶意代码，会连接网络下载其他恶意代码和窃取用户信息等。( 威胁等级中 ) |
| | | Trojan[Spy]/Win32.Goldun | 此威胁是一种窃取在线交易网站的用户密码及账户余额的木马类程序。该家族类程序会修改注册表，使用浏览器加载恶意代码运行，并监控浏览器窗口。当发现在线交易网站登陆时会记录键盘操作，窃取某在线交易网站用户密码及其帐户余额等机密信息，并将机密信息发送到黑客指定站点。( 威胁等级中 ) |
| | | Trojan[Dropper]/Win32.Scheduler | 此威胁是一种可以释放恶意代码的木马家族。该家族样本运行后会释放“CutePDF Writer”并安装，会连接网络并执行其他的恶意操作。( 威胁等级中 ) |
| | | Trojan[Downloader]/Win32.Oxes | 此威胁是一种可以下载其他恶意代码的木马家族。该家族样本运行后可以连接网络下载其他恶意代码并安装，会窃取用户信息并回传。( 威胁等级中 ) |

# 大数据安全九大挑战

Aleksandr Panchenko / 文　安天公益翻译小组 / 译

近年来，隐私和机密信息的保护获得越来越多的关注。根据全球唯一的应用程序质量报告《2015-2016 世界质量报告》，安全性在 IT 战略中具有最高的优先级。

在此之前，公司的应用程序主要是内部使用的，安全风险较低。然而，随着公司越来越多地采用网络、移动和基于云的应用程序，敏感数据能够从不同的平台进行访问。因此，这些平台非常容易被黑客攻击，特别当它们是低成本或免费的。

如今，企业收集和处理大量的信息。存储的数据越多，保护数据安全性就越重要。缺乏数据安全性会导致巨大的经济损失和声誉损失。就大数据而言，IT 安全性差导致的损失甚至会超过最坏的预期。

## 大数据安全的主要挑战

几乎所有的数据安全问题都是由缺乏有效的反病毒软件和防火墙导致的。这些系统旨在保护存储在硬盘上的某些信息，但是大数据超出了硬盘和隔离系统的范围。

## 九个大数据安全挑战

1. 大多数分布式系统的计算只有一个保护级别，不推荐使用。

2. 非关系数据库 (NoSQL) 正在积极发展，因此安全解决方案很难跟上需求。

3. 自动化的数据传输需要额外的安全

措施，而这种措施往往未被设置。

4. 当系统接收大量的信息时，应当进行验证，以确保可信性和准确性。然而，企业并不总是进行验证。

5. 不道德的 IT 专家能够进行信息挖掘，不需用户许可或通知用户就能够收集其个人数据。

6. 访问控制加密和连接的安全性会变得过时，依赖于此的 IT 专家就无法进行访问了。

7. 有些企业不能 ( 或不会 ) 在内部建立访问控制来划分保密级别。

8. 由于大数据涉及大量的信息，因此无法定期进行推荐的详细审核。

9. 由于大数据的规模太大，其来源不会一直被监控和追踪。

## 如何改善大数据安全?

云计算专家认为，提高大数据安全性的最合理的方式是不断扩大的反病毒行业。很多反病毒厂商提供了多种解决方案，能够更好地防御大数据安全威胁。

令人耳目一新的是，反病毒行业往往具有开放性。反病毒软件厂商自由地交换大数据安全威胁的信息，行业领导者经常一起应对新的恶意软件攻击，提供最大限度地提高大数据安全性。以下是加强大数据安全性的一些建议：

- 专注于应用程序而非设备的安全性；
- 隔离包含关键数据的设备和服务器；
- 引入实时安全信息和事件管理；
- 提供被动和主动的保护。

## 大数据安全的前景

使用大数据的公司首先关心的是基于云的系统的安全性。英特尔安全公司最近发布了《迈克菲实验室威胁预测报告》，该报告预测了未来短期的数据安全情况。本报告指出，托管服务 ( 如：Dropbox、Box、Stream Nation) 的合法云文件会在即将到来的网络间谍活动中被用作控制服务器。一旦受到攻击，这些流行的云服务会在不引起怀疑的情况下使恶意软件传输命令。

针对 IT 系统的恶意攻击正变得越来越复杂，而且新的恶意软件正在不断被开发出来。不幸的是，使用大数据的公司每天都面临这些问题。然而，每一个问题都有解决方法，为自己的企业找到有效和合适的解决办法是完全可能的。

| 原文名称 | Nine Main Challenges in Big Data Security |
|---|---|
| 作者简介 | 数据知识中心 (Data Center Knowledge，DCK)，数据中心行业每日新闻和分析的主要来源。 |
| 原文信息 | 2016 年 1 月 19 日发布于数据知识中心 (Data Center Knowledge，DCK)<br>原文地址 http://www.datacenterknowledge.com/archives/2016/01/19/nine-main-challenges-big-data-security/ |
| 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。<br>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《Ursnif 木马沙箱绕过技术分析报告》

近日，安天追影小组在一次名为“Ursnif Banking”的攻击事件中，发现了一款利用宏病毒技术来进行感染传播的Ursnif木马。“Ursnif Banking”的攻击事件，通过 microsoft office word 文档的宏方式来释放 Ursnif 木马，同时针对沙箱分析和恶意代码分析工程师的分析手段使用了新型绕过技术。

经安天追影小组分析，Ursnif 木马样本为 word 文档，文档中含有利用 Office word 宏语言编写的恶意代码，攻击者通过发送含有公司名称、个人姓名、职位等敏感信息的电子邮件，诱导被攻击者查看并下载文档。文档被打开时，会自动运行其中隐藏的木马文件，进而感染被攻击者的电脑。该恶意代码通过多种方式来绕过沙箱检测，主要为以下几种：文件名 Hash 检测绕过方式、进程数量检测绕过方式、应用程序黑名单检测绕过方式、Maxmind 设备检测绕过方式。

常规的沙箱分析恶意样本，均采用 SHA256 或 MD5 等 16 进制 Hash 字符串作为文件名。因此，文件名 Hash 检测绕过方式，在样本检测到自身的文件名被修改为 16 进制字符串时，会停止释放木马。进程数量检测绕过方式，主要针对样本运行系统的进程数进行检测，从而达到绕过沙箱的目的。当恶意代码检测到当前感染环境进程数量少于 50 个，且没有运行图形界面时，则判定当前为沙箱分析环境从而停止感染行为。应用程序黑名单检测绕过方式，在为发现当前运行环境中存在 Wireshark、Vbox 等常用的恶意代码分析工具则停止感染。Maxmind 设备检测绕过方式，运行恶意代码时通过访问 Maxmind 第三方服务，来获取恶意代码运行环境的 IP 所在地理位置，进行判断是否为其设定的感染区域，若不是则不进行感染。

通过对本次事件的分析，可见信息安全技术的对抗是持续存在的，攻击者不仅对攻击技术进行研究，而且对防御分析技术也进行了研究。

安天建议网络使用者，针对邮箱匿名邮件应谨慎对待，切勿随意点击下载，防范于未然。对于已经受到感染的机器设备，及时寻求专业人士取证分析、恢复系统。

目前，安天追影产品已经实现了对该样本的检出。

## 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、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 | AB89AD40755D6A762BC6EDC98F49C434 |
| 文件类型 | Document/Microsoft.DOCX[:Word 2007-2012] |
| 大小 | 31 KB |
| MD5 | AB89AD40755D6A762BC6EDC98F49C434 |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan[Downloader]/Win32.Ursnif |
| 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 |

该文件具有以下行为：

获取系统版本、打开自身进程文件、查找指定内核模块、隐藏文件、请求加载驱动的权限、创建特定窗体、获取驱动器类型、获取系统内存、查找特定窗体、独占打开文件、获取计算机名称、获取主机用户名称。

◆ 其他行为

| 行为描述 | 危险等级 | 行为描述 | 危险等级 |
|---|---|---|---|
| 获取系统版本 | ★★ | 打开自身进程文件 | ★ |
| 查找指定内核模块 | ★ | 隐藏文件 | ★ |
| 请求加载驱动的权限 | ★ | 创建特定窗体 | ★ |
| 获取驱动器类型 | ★ | 获取系统内存 | ★★ |
| 独占打开文件 | ★ | 查找特定窗体 | ★ |
| 获取计算机名称 | ★ | 获取主机用户名称 | ★ |

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=AB89AD40755D6A762BC6EDC98F49C434