安天周观察

主办：安天　2016 年 5 月 9 日（总第 38 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

黑龙江省委书记王宪魁莅临安天总部考察指导

5 月 8 日，黑龙江省委书记王宪魁在哈尔滨市委书记陈海波、哈尔滨市长宋希斌、黑龙江省委网信办主任李耀东、黑龙江省科技厅厅长杨廷双、黑龙江省工信委主任聂云凌等领导陪同下莅临安天哈尔滨总部考察指导，并听取了关于我司发展近况的汇报。

在展示厅里，安天负责人向王宪魁书记介绍了安天近期的发展情况以及在产品创新和知识产权等方面取得的成果。并陪同各位领导观看了安天威胁态势感知捕获系统，介绍了全国网络威胁疫情趋势和黑龙江遭受网络攻击威胁情况分布。

针对王宪魁书记关心的关键基础设施安全问题，安天负责人详细结合“伊朗核设施和基础工业厂商遭受‘震网病毒’攻击事件”和近期发生的“乌克兰电力系统遭受攻击事件”，进行了汇报。并对“乌克兰电力系统遭受攻击事件”进行了可视化靶场模拟演示。

王宪魁书记还观看了安天伙伴墙，了解了国际国内厂商使用安天反病毒引擎的情况。

在听完讲解后，王宪魁书记表示，在网络安全领域，黑龙江省是有手段、有措施、有人才的，安天就是在龙江创新创业的典型代表，希望安天在保持技术领先的基础上，要进一步加快核心技术向产业成果的转化。

同时，王宪魁书记还指出，在信息技术和网络快速发展的当下，网络安全对于黑龙江和全国来说都是一件大事，安天作为在网络安领域具有竞争力的企业，要充分发挥技术和能力优势，为黑龙江的网络安全防护，为国家网信大战略做出贡献。

安天移动安全团队发布

《针对移动银行和金融支付的持续黑产行动披露——DarkMobileBank 跟踪分析报告》

近日，安天移动安全团队 (AVL Team) 发布了《针对移动银行和金融支付的持续黑产行动披露——DarkMobileBank 跟踪分析报告》。报告所涉及的研究历时近 3 年，早在 2013 年 5 月，AVL Team 就已经开始关注到这种攻击形态，并将整个黑产和威胁用代号名称 DarkMobileBank 命名。

作为一类典型的黑产犯罪，DarkMobileBank 具有极大的危害性，它会瞄准智能终端的安全弱点和用户心理特点，凭借高度程序化进行团伙作业，随着犯罪经验、工具、平台交叉共享，作案成本会不断下降，作案手法会不断更新，同时，随着团伙分化与家族化的培训，作案群体人数会逐步膨胀。另外，这种攻击并非只来自境内，也存在境外黑产团伙攻击的可能，从而使整个局面更为复杂。

在这样的背景之下，AVL Team 希望以威胁情报的视角和手法，通过本篇报告披露该持续性地下黑产攻击行动的细节，以此提高广大用户的网络安全意识和基本安全技能。（完整报告地址 http://blog.avlsec.com/）

安天携『监控预警平台及可视化展示系统』亮相 4·29 网络安全日展会

4 月 28 日，第三届“4·29 首都网络安全日”网络与信息安全博览会在北京展览馆拉开帷幕。安天携“监控预警平台及可视化展示系统”亮相本次展会，以独特的可视化展示效果和监控预警平台为展台背景，运用直观的动态效果向公众展现监控预警平台的部署和全球恶意代码的安全态势，使观众对全球恶意威胁的态势有了更加直观的了解和认识。同时，安天沿袭传统，免费发放了原创的技术文章汇编等资料，受到众多安全爱好者的好评。

安天监控预警和可视化展示方案，是基于安天产品：“追影”威胁分析系统 (PTA)、“探海”威胁检测系统 (PTD)、“镇关”威胁阻断系统 (PTF)、“智甲”终端威胁防护系统 (IEP) 等建立的适应性强且技术能力国内领先的网络犯罪感知发现、深度分析、追踪溯源的恶意代码和高级威胁检测能力部署，通过安天安全可视化管理平台进行统一管理，通过该平台，观众可以对网络侧、终端侧的威胁事件进行密切监控，实时跟踪可疑文件信息并进行多维度的数据挖掘，从而达到掌握安全态势，发现高级威胁的目的。

每周安全事件

类 型	内 容
中文标题	黑客组织匿名者再作祟 DDoS 攻击希腊银行网站
英文标题	Anonymous Target Bank of Greece Website with Massive DDoS Attack
作者及单位	Agan Uzunovic；HACKREAD
内容概述	近日，匿名者黑客组织 (Anonymous) 再次推出针对美国和欧洲银行系统的“OpIcarus” 运动，第一个不幸中标的就是希腊银行网站。Anonymous 对其进行了一系列大规模的分布式拒绝服务攻击 (DDoS 攻击)，迫使希腊银行网站服务器离线时间超过 6 小时。参与此次运动的黑客坚信银行和金融巨头都参与了金融腐败，他们不得不采取新一轮的战斗，来对抗银行金融腐败。早在今年 3 月，“匿名者”就曾发布过 YouTube 视频公布该行动的攻击列表，其中包含巴西、孟加拉国、中国、美国、英国、巴基斯坦、伊朗和其他国家银行等金融机构。
链接地址	https://www.hackread.com/anonymous-ddos-attack-bank-greece-website-down/

每周值得关注的恶意代码信息

经安天检测分析，本周 10 个移动平台和 5 个 PC 平台的恶意代码家族值得关注

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.installAPK.a[rog] 2016-05-02	该应用程序安装后无图标，私自在后台静默安装设备指定路径下的 APK 文件。（威胁等级低）
		Trojan/Android.Iop.a[rog，exp] 2016-05-03	该程序运行后，可在后台私自联网下载恶意应用，判断是否 root，选择静默安装或正常弹框安装，可造成用户资费消耗。（威胁等级中）
		Trojan/Android.Loki.a[prv，exp，rmt] 2016-05-04	该程序是个插件，可被恶意利用配合正常程序窃取用户隐私或下载未知文件，造成隐私泄露或资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.zscreen.a[rog] 2016-05-04	该程序安装后会杀掉任何新创建的置顶进程以劫持屏幕，给用户造成恶意影响，建议立即卸载。（威胁等级中）
		Trojan/Android.mepage.a[prv] 2016-05-05	该程序运行后会获取用户 WhatsApp 聊天记录并上传到指定服务器，造成用户隐私泄露，建议不要安装。（威胁等级中）
	较为活跃的样本	RiskWare/Android.e4aspr.c[exp]	该程序伪装成微信抢红包，实际为诱导用户下载推广 APK，可对用户造成一定资费损耗，且推广的 APK 均非官方正版，存在安全隐患，建议立即卸载。（威胁等级低）
		G-Ware/Android.Fakesysui.i[rog，exp]	该程序伪装成其他工具类应用，后台联网推广广告，下载并静默安装推广 APP，建议卸载，避免造成资费损耗。（威胁等级低）
		Trojan/Android.FakeBank.m[prv]	该程序伪装成美国 Regions 登陆界面，获取用户银行账户密码及密码提示问题答案，上传到远程服务器，造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.BqSpy.t[prv，spy]	该程序伪装成系统应用，窃取用户通话录音，建议立即卸载避免造成隐私泄露。（威胁等级中）
		Trojan/Android.crittercismSpy.b[prv，spy]	该程序运行后在后台窃取用户隐私如：短信、通讯录、通讯录记录、位置等信息上传到远程服务器，建议立即卸载，避免造成隐私泄露。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Apache Struts 2 任意代码执行漏洞 (CVE-2016-3081，S02-32)	Struts2 官方发布两个 CVE，其中 CVE-2016-3081 官方评级为高。主要原因为在用户开启动态方法调用的情况下，会被攻击者实现远程代码执行攻击。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.VB	此威胁是木马类程序，使用 VB 开发，运行后会连接网络下载其他恶意程，还会获取系统信息，用户信息等，发送数据到远程服务器。（威胁等级中）
		Trojan[Backdoor]/Linux.Gafgyt	此威胁是一种木马类后门程序，运行在 linux 平台，主要功能为 DDOS 攻击、更新和下载等，通过扫描 SSH 弱口令进行传播。（威胁等级中）
		Trojan[Downloader]/Win32.Tintin	此威胁是一种木马类程序，运行后会添加注册表启动项实现自身随机启动；与指定的远程服务器连接，下载其他的恶意软件到本地运行。（威胁等级中）
		Trojan[Downloader]/Win32.CcKrizCry	此威胁是一种木马类程序，通过网站下载进行传播，多为 IE 安装程序，但在安装过程中会下载其他恶意程序，一般会下多种文件大多为游戏、播放器等。（威胁等级中）

公设辩护人：FBI 使用棱镜监控数据是违宪的

Ellen Nakashima/ 文　安天公益翻译小组 / 译

美国秘密监视法庭去年委任的一名公设辩护人指出，棱镜项目存在一个鲜为人知的条文，允许 FBI(美国联邦调查局) 查询外国情报信息，为国内犯罪调查取证。她认为该条文违反了宪法，但是法院不这样认为。

根据情报界发布的一份法院意见 (去年 11 月提出)，去年 8 月，外国情报监视法庭要求辩护人艾米・杰弗里斯 (Amy Jeffress) 评估该条文。该法庭衡量政府的监视申请，通常只在保密会议中听取政府的提议。一般来说，它的意见是保密的。

杰夫里斯曾是一名联邦检察官和司法部官员，现在是私人执业者。她是第一个根据《美国自由法案》(该法案于去年 6 月颁布，旨在限制政府的监控活动并增加其透明度) 任命的公设辩护人或“法庭之友”。

“棱镜”是一个情报收集项目。2013 年 6 月，前国家安全局承包商爱德华・斯诺登披露了一系列文档，由此，该项目的名称和范围被公之于众。

出于收集外国情报的目的，该项目从各大科技公司，包括谷歌，雅虎，微软，Facebook 和苹果，收集电子邮件、即时消息和视频。该项目的目标是外国人，但是他们可能与美国人进行通信。这些情报由 NSA(美国国家安全局) 收集，但是与其他机构共享，如 CIA(美国中央情报局) 和 FBI(美国联邦调查局)。

杰夫里斯提出了对该项目规则的担忧，这些规则允许 FBI 使用美国人的电子邮件地址和其他“信息”来查询这些数据，以便执行任何犯罪调查。也就是说，这并不是外国情报目的。

根据外国情报监视法庭法官托马斯・F・霍根 (Thomas F. Hogan) 的意见，杰夫里斯在简报中表示：“没有任何规定说，调查的事件必须是一个严重的问题，或者与国家安全有关。”

她写道：“这些做法不符合《第四修正案》，它们远远超出了棱镜项目数据收集的最初目的。”

杰夫里斯敦促法院加强规程，“向美籍人士给出书面理由，解释情报查询为何涉及外国情报，或者为何这种查询是合法的。”

但是，阿诺德 – 波特律师事务所的合伙人霍根 (他曾担任驻哥伦比亚特区美国律师事务所的国家安全科科长) 并不赞同杰夫里斯的意见。

法官指出，没有法规要求涉及棱镜数据的所有活动都只服务于“外国情报目的”。他说，《外国情报监视法案》涵盖了棱镜项目，该法案明确要求，政府能够保留作为犯罪证据的数据，不管它是否涉及外国情报或国家安全问题。

霍根写道，允许 FBI 保留美籍人士的犯罪证据，却禁止它查询此类证据的数据，是对该法规的“矛盾解读”。

根据设立了公设辩护人的《美国自由法案》，辩护人可能不会对法官的裁决提出上诉。该法律允许法官询问辩护人对重大事件的意见，特别是那些可能对隐私和公民自由产生影响的事件。

独立行政监督部门隐私和公民自由监督委员会在 2014 年 7 月发布了一份报告，指出 FBI 的做法存在问题。该委员会说，公众应该知道，不仅是 FBI 人员能够出于犯罪调查的目的查询数据，“还有很多人能够进行这样的查询”。报告还指出，应该更严格地限制这种查询。

两名成员，包括主席大卫・麦迪尼 (David Medine) 和帕翠西・沃德 (Patricia Wald)，建议监视法庭的法官批准各种涉及美国人士可能提供犯罪调查线索的查询。

相反，成员瑞秋・布兰德 (Rachel Brand) 和伊丽莎白・柯林斯・库克 (Elisebeth Collins Cook) 建议，分析人员必须首先获得监管人的批准，才能查询美籍人士的信息。

原文名称	Public advocate-FBI's use of PRISM surveillance data is unconstitutional
作者简介	Ellen Nakashima，《华盛顿邮报》国家安全方面的记者，专注于情报、技术和公民自由问题。
原文信息	2016 年 4 月 20 日《华盛顿邮报》发布 原文地址 https://www.washingtonpost.com/world/national-security/public-advocate-fbis-use-of-prism-surveillance-data-is-unconstitutional/2016/04/20/0282ed52-0693-11e6-b283-e79d81c63c1b_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。

安天发布《修改 MBR 的敲诈者木马来袭》报告

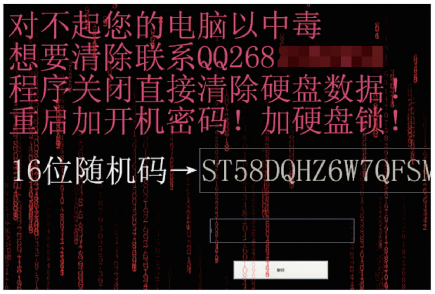
近期，敲诈勒索病毒的传播呈现出上升趋势，随着勒索得逞的案例越来越多，很多造马者开始使用不同的方法制作该类病毒。2016 年 3 月底，几家国外安全厂商先后发布了“修改 MBR、加密整个硬盘的勒索软件 Petya”的报告，值得关注的是，近期国内也出现了一款通过修改 MBR 来实现勒索的病毒软件，安天追影小组查询相关论坛后发现，该病毒的作者目前并没有进行敲诈，而且主动公开了密码，可能只是为了炫耀技术。以下为追影小组具体分析。

行为分析

该病毒运行后，屏幕如下图所示，文字不停的闪烁并伴有动画效果与音乐，重启后显示文字“mima lianxi qq 268****!!”提示输入密码。用户只有输入正确的密码，才可以正常启动系统。

样本行为如下：

1. 运行后直接获取 \\.\PhysicalDrive0



的句柄，从第 1 扇区 (偏移为 0x0) 读取大小为 200 字节的内容写入到第 3 扇区 (偏移为 0x400) 中。其目的应该在输入正确密码后，重新恢复原有第 1 扇区的信息。

2. 在第 1 扇区 (偏移为 0x0) 中写入大小为 200 字节的 MBR 敲诈信息 (即重启后的开机界面，需要输入正确的密码才能恢复第 1 扇区)。

3. 在创建输入密码界面的时候，则会不停的遍历进程比对来实现结束掉任务管理器进程 taskmgr.exe，主要是为了守护样本进程，防止其被任务管理器结束掉。

总结

近期国内出现的勒索软件很多都以中文为提示语言，QQ 为联系方式，以此可以推测，一些勒索软件是国内的造马者制作或修改他人代码形成的。安天追影小组提醒广大用户加强安全意识，通过官方网站下载正版软件，不要随意打开陌生链接运行不明的应用程序，同时，安天也会持续关注追踪勒索软件的发展态势。

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。

该文件具有以下行为：修改硬盘引导扇区，疑似感染引导区病毒、创建特定窗体、查找特定窗体、独占打开文件、遍历进程。

文件名	3254AE13661FAE33075349C3226FE940
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	9.30 MB
MD5	3254AE13661FAE33075349C3226FE940
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	动态行为

危险行为

行为描述	危险等级
修改硬盘引导扇区，疑似感染引导区病毒	★★★★

其他行为

行为描述	危险等级	行为描述	危险等级
创建特定窗体	★	查找特定窗体	★
独占打开文件	★	遍历进程	★

文件操作

操作	文件路径
新建	\\.\\physicaldrive0
新建	c:\windows\prefetch\copyfile.exe-3b1759c2.pf

静态启发式检测

检测类型	检测点	详细说明
PE 结构	非微软的版本信息	非受信厂商的版本信息，具有较低的受信级别。
PE 结构	PE 的子系统是 GUI	基于海量恶意代码和受信白名单文件名进行数据挖掘，恶意程序通常不包含 GUI。

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=3254AE13661FAE33075349C3226FE940