安天周观察

主办：安天　2017 年 3 月 27 日（总第 81 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天再次荣获 CNVD “漏洞信息报送突出贡献单位”荣誉称号

近日，国家信息安全漏洞共享平台 (CNVD)2017 年工作会议在京召开。安天荣获 CNVD “漏洞信息报送突出贡献单位”荣誉称号，这也是安天第三次荣获该荣誉称号。

作为 CNVD 技术组成单位之一，安天多年来一直为 CNVD 持续报送漏洞信息，2016 年安天为 CNVD 报送公开漏洞 7417 条，报送数量位居前列。安天还曾获 CNVD “共建工作 2009 年度突出贡献”奖，也是中国国家信息安全漏洞库 (CNNVD) 技术支撑一级单位、微软 MAPP 计划成员。

安天始终专注威胁检测领域，提供先进的威胁检测能力，在漏洞检测响应领域中，安天重点监测可以被用于恶意代码传播、木马植入等相关漏洞的分布和被利用情况；对可以用于 APT 攻击的格式文档等漏洞类型，进行深度分析，完善针对未知漏洞的静态格式分析和动态沙箱检测能力。安天曾对震网、火焰、毒曲、沙虫、方程式、白象等 APT 攻击进行深度分析，分析成果获得了业内好评。持续的关键威胁分析和漏洞跟踪报送，也推动了安天反病毒引擎和安天 PTD 探海威胁检测系统、PTA 追影威胁分析系统等产品的能力进步。

日后，安天会继续与行业主管部门和国家互联网应急中心保持密切协作和配合，积极应对新发现的漏洞，充分发挥自身技术优势，为网络与信息安全保驾护航。

埃塞俄比亚信息网络安全局、中兴公司一行参观安天

3 月 23 日，埃塞俄比亚信息网络安全局、中兴公司一行人参观了安天公司，并进行了企业安全服务与产品方面的技术交流与探讨。

在产品展示中心内，安天负责人介绍了安天发展历程、安天参与重大活动的网络安保支撑、安天在专利技术方面所取得的部分成果；并介绍了安天在重大恶意代码和 APT 攻击事件的应急响应、追踪溯源方面所做出的努力。同时，针对“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。

埃塞俄比亚信息网络安全局一行人详细了解了安天由探海、追影、智甲等态势感知产品协同组成的态势感知系统，以及全球首个移动威胁情报平台 AVL Insight。并表示，希望未来能够进行产品和安全服务的合作。

安天获得国家信息安全服务（安全工程类一级）资质

近日，安天通过中国信息安全测评中心的信息安全服务资质（安全工程类一级）审核并获得证书。国家信息安全服务资质是对信息安全工程服务提供者的资格状况、技术实力和安全工程实施等综合实力所做出的专业评估和权威认定，该资质的获得是安天安全服务全过程能力的体现。

中国信息安全测评中心组织专家组对安天进行了全面、严格的静态评估和现场审核。通过对安天在信息安全服务资质的基本资格和能力、信息安全工程能力、项目和组织管理能力三个方面共 22 大类的核查，最终认定安天有信息安全风险评估、安全规划设计、安全集成、安全运维和应急响应等信息安全服务能力。符合《信息安全服务资质评估准则》(一级）要求。

该资质的获得，标志着安天的信息安全服务理念和保障能力得到了国家级的权威认证，也推动安天信息安全服务业务开拓迈入新的里程碑。

商务部中国服务外包研究中心副主任邢厚媛一行参观安天总部

3 月 23 日，商务部中国服务外包研究中心副主任邢厚媛等领导参观了安天哈尔滨总部，并听取了关于我司发展近况、技术产品、商务合作等情况的汇报。

在展示厅里，安天负责人介绍了安天的历史、发展现状及在技术创新和知识产权方面所取得的成果，安天参与重大活动的网络安保支撑等；并介绍了安天持续与网络安全威胁对抗的情况，汇报了安天对高级威胁发现、捕获、分析方面所做的工作。

截止目前为止，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，

安天的反病毒引擎得以为全球近十万台网络设备和网络安全设备、超过六亿部手机提供安全防护。安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

邢厚媛副主任对安天 17 年来取得的成绩和坚持给予了肯定，并表示安天拥有一支年轻的研发团队，应该坚守理想，以全球化的视野开拓国际市场，输出网络安全技术。

每周安全事件

类 型	内 容
中文标题	苹果公司遭遇黑客组织勒索：不付赎金就曝光或抹除 3 亿 iCloud 账户信息
英文标题	Hackers Threaten to Remotely Wipe 300 Million iPhones Unless Apple Pays Ransom
作者及单位	Mohit Kumar；The Hacker News
内容概述	近日，据 Motherboard 报道，自称为“Turkish Crime Family”的黑客团伙声称掌握 3 亿 iCloud 账户，意图对苹果公司进行勒索，要求赎金必须以比特币或 Ethereum 的形式支付。 某自称能代表该组织的黑客，把据称是该组织与苹果安全团队之间的邮件截图发给了 Motherboard。 根据黑客提供的截图，苹果公司的安全团队要求这个黑客阻止提供被黑账户样本，以证实他们的说法。但是这个组织仅在 YouTube 上传了一段视频，展示他们能够访问一个被黑的账户，并远程抹除了该账户设备上的所有内容。 苹果警告该组织称，不会奖励违法犯罪行为，还要求该组织撤下 YouTube 视频，认为该组织是在“寻求不必要的关注”。 黑客组织给苹果的期限是到 4 月 7 日，如果苹果没有满足他们的要求，他们就要远程抹除受害苹果设备数据，并重置 iCloud 账户。
链接地址	http://thehackernews.com/2017/03/hacking-apple-icloud-account.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 5 个 PC 平台的恶意代码值得关注

平台分类	关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.UpdateSpy.a[prv，rmt，exp]2017-03-20	该程序为间谍应用，运行后隐藏图标，后台窃取用户通讯录、通话记录、通话录音、收件箱短信、SD 卡中的指定格式文件 (PDF、DOC 和 XLS 等) 等隐私信息上传，拦截短信，会根据指令执行录音、上传等一些列恶意行为，建议立即卸载避免隐私泄露。(威胁等级高)
	较为活跃的样本	Trojan/Android.FakeApp.dt[prv，rmt]	该程序伪装知名应用，运行后会隐藏图标，后台接受远程指令，会执行拍照、录音、等高危行为，同时窃取用户位置、通讯录、通话录音、通话记录、短信等隐私信息，造成用户隐私泄露。(威胁等级高)
		Trojan/Android.QQspy.an[prv，exp]	该程序会伪装 QQ 相关应用，诱导用户输入账户和密码，并通过邮件转发，造成用户隐私泄露和资费损耗，建议卸载。(威胁等级高)
		G-Ware/Android.jianmo.cb[rog，sys]	该应用会伪装成色情、游戏辅助等应用，激活设备管理器，锁定用户手机，勒索用户添加指定 QQ 进行付费解锁，造成用户经济损失，建议不要安装。(威胁等级中)
		Trojan/Android.oxti.z[exp]	该程序伪装系统更新，运行后会隐藏图标，后台频繁访问指定网址，造成用户流量资费损耗，建议卸载。(威胁等级中)
		Trojan/Android.Rootnik.x[exp，sys]	该应用私自提权，加载广告，诱导下载恶意 APK 文件并且安装。造成用户资费消耗，建议卸载。(威胁等级中)
		Trojan/Android.FakeFB.g[prv，fra]	该应用会伪装成 Facebook，诱导用户输入账号密码并通过短信转发，造成用户隐私泄露和资费损耗，建议卸载。(威胁等级中)
		G-Ware/Android.LockScreen.r[rog]	该应用利用 Xposed 框架劫持设备管理器，破解设备 PIN 码并将其重置。要求加指定 QQ 以解锁恢复。具有流氓性，会对用户正常使用造成影响，并引发可能的经济损失。建议立即卸载。(威胁等级底)
		Trojan/Android.E4Aspy.ae[prv]	该应用会伪装成 POS 终端管理，程序运行后会获取固件信息、短信信息和通话记录等隐私信息连网上传，造成用户隐私泄露。(威胁等级中)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 内存破坏漏洞 (CVE-2017-2930)	Adobe Flash Player 是美国 Adobe 公司开发的一款，被广泛使用的、专有的多媒体程序播放器。 Adobe Flash Player 中存在内存破坏漏洞，攻击者可利用漏洞控制受影响的系统，导致任意代码执行。(威胁等级高)
	较为活跃的样本	Trojan[Ransom]/Win32.Bart	此威胁是一类可以加密用户数据索取赎金的勒索软件家族。该样本遍历磁盘加密文件并添加 .bart 后缀，加密后在桌面留下 TXT 和 BMP 格式的勒索信并改变桌面，要求用户支付赎金解密。(威胁等级中)
		Trojan[Ransom]/Win32.CryptoBit	此威胁是一种勒索者家族程序。这种家族的样本伪造为播放器图标，对文档进行加密，连接 C&C 服务器 (laoismacau.com/58.64.142.89，未使用 DGA)，并在多个文件夹下留下勒索信 "HITLERHASYOURFILES"，在『我的文档』留下被加密过的文件的列表。CPU 占用较低，不易察觉。(威胁等级中)
		Trojan[Backdoor]/Win32.FinFish	此威胁是一类可以窃取用户信息并回传的木马家族。该家族样本运行后会连接远程服务器，收集系统信息并回传，运行后会自删除。(威胁等级中)
		Trojan[Downloader]/Win32.Pfoenic	此威胁是木马类家族程序。这种程序的样本执行后会进行文件下载并静默安装，同时在任务栏和桌面上创建游戏“超霸传奇”的快捷方式。(威胁等级中)

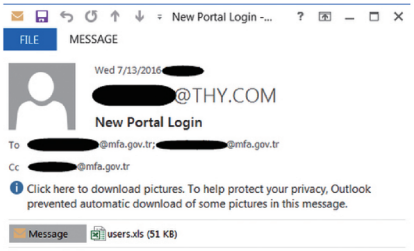
OilRig 攻击扩展到更多的行业和地区

James Carder / 文　安天公益翻译小组 / 译

近日，中东航空公司、政府、金融行业和关键基础设施遭到了恶意软件的攻击。攻击者首先向目标发送钓鱼邮件，该邮件包含的恶意 Excel 文件能够创建一个简单而强大的后门。在最新发布的报告中，LogRhythm Labs 详细分析了这个被称为“OilRig”的恶意软件活动，包括用于感染中东政府，金融，航空和关键基础设施实体的安全操作中心的工具、技术和程序。与之前发布的威胁情报报告不同的是，这份新报告确定了完整的前端基础设施，包括与初始感染相关的恶意软件以及大量尚未公布的感染信标。

OilRig 网络攻击首次出现在 2015 年年底。自那以后，威胁情报界确定了它的两个高度活跃的时期：2016 年 5 月和 10 月。

所有已知样本都利用附加到钓鱼邮件中的恶意 Excel 文件来感染受害者，我们以下面的钓鱼邮件为例分析具体过程，可以看出该邮件貌似是发送给一个土耳其政府机构的。一旦实现感染，攻击者就能控制受害者的机器，执行基本的远程访问木马类任务，包括命令执行、文件上传和下载。

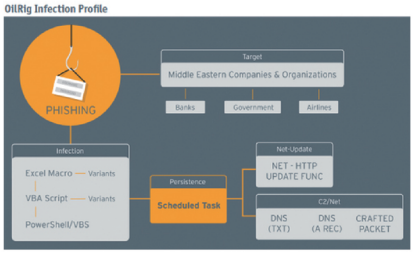


鱼叉式钓鱼邮件示例 (来源：LogRhythm Labs)

目标扩张

早期的攻击目标是中东银行，政府实体和关键基础设施实体。 然而，随着时间的推移，目标在地理和行业方面都有所扩张。例如，2016 年 10 月的攻击以美国公司，沙特阿拉伯、阿拉伯联合酋长国、卡塔尔、土耳其和以色列的政府机构、公司和政府所有公司为目标。 OilRig 还扩展了目标行业，包括一些中东航空公司。

历史数据表明，相比其他的恶意活动，攻击者对间谍活动最感兴趣。然而，攻击者也有可能继续扩张到其他行业。



恶意软件提交

通过分析威胁情报数据，可以了解哪些国家提交了相关的恶意软件，揭示了该活动的目标国家和可能对该攻击组织进行分析的国家。例如，沙特阿拉伯提交了 22 个样本，而这些样本来自该攻击组织的大多数目标。另外，英国和美国分别提交了 11 个和 9 个样本，说明他们在分析该攻击活动。

其他需要注意的国家包括阿拉伯联合酋长国、卡塔尔、以色列、土耳其和阿塞拜疆。虽然该报告没有充分证实该组织攻击了所有这些国家的目标，但是很多迹象能够证明这一点。诸如“TurkishAirline_Offers.xls”和“Israel Airlines.xls”的文件名说明这些组织是其攻击目标。

恶意软件分析

LogRhythm Labs 团队确定了 23 个武器化的 Microsoft Excel 文件 (包含 OilRig 恶意软件)。根据所使用的文件名、来源国、确定时间和 C&C 方法，我们能够确定几乎所有样本都属于这四个家族。该报告详细分析了每个家族的代表性样本。

当武器化文档被执行时，大多数恶意软件样本都会使用 VBA 载荷来感染具有 PowerShell(.ps1) 和 VisualBasic 脚本的系统。恶意软件利用 Microsoft 计划任务实现持续性，其功能包括非常基本的命令执行，文件上传和文件下载。

通信分析

分析得出该恶意软件存在针对 HTTP、更隐蔽的 DNS C2 和数据渗透机制的 C&C 机制。该恶意软件使用定制的 UDP 数据包，DNS 记录查询和响应模式进行 C&C 通信，具有基本的上传、下载和任意命令执行功能。LogRhythm Labs 的报告分析了该方法，并给出了检测和修复细节。

虽然 OilRig 攻击活动不是特别复杂，但却非常有效。攻击者使用被感染的 Excel 文件 (包含恶意 VBA，VBS 和 PowerShell 代码) 创建了一个简单强大的后门。到目前为止，攻击者主要使用钓鱼邮件中附加的 Excel 文件来传播恶意载荷。然而，这种攻击可以很容易地利用附加到钓鱼邮件中的许多不同文件格式。

尽管该活动目前只针对少数行业，但是其代码已经广为人知，这意味着其他威胁源会将这些代码纳入自己的攻击活动，从而攻击不同的国家或行业。因此，任何国家或行业的企业都应该及时防范类似的攻击。

原文名称	“OilRig” Attacks Expanding Across Industries，Geographies
作者简介	James Carder，LogRhythm 公司的首席信息安全官和副总裁，拥有超过 20 年的 IT 安全和顾问经验。
原文信息	2017 年 3 月 21 日发布于 Darkreading 原文地址 http://www.darkreading.com/threat-intelligence/report-oilrig-attacks-expanding-across-industries-geographies/a/d-id/1328443?
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《僵尸网络 Dnamic 家族分析报告》

近日，安天追影小组在网络监控中发现一个未知的僵尸网络家族。通过本地多家杀毒引擎对其被控端样本进行检测，发现该家族为 DDoS 类型的样本，且具有免杀功能。该家族样本代码中多次出现标志性字符串“Dnamic”，因此将其命名为 Trojan[DDoS]/Linux.Dnamic。根据现有数据得出，Dnamic 家族的 BOT 被控端主要适用于 Linux x64 环境，且最早于 2017 年 2 月被发现；该家族功能比较单一，除实现 DDoS 攻击外，并不具有如自启动、横向感染等功能，进而可推测其功能还在开发完善中。

Dnamic 家族 BOT 被控端主要包括以下 2 个功能：

1) 连接 C2 与数据发送：Dnamic 家族和常见的 Win/linux x86/x64 家族一样，都需要获取受害系统的配置信息作为 BOT 被控端的首包和心跳包的数据包信息。

2) DDoS 攻击：在 BOT 被控端运行后，创建向 C2 发送数据的同时，其会创建一个线程来独立负责接收 C2 向 BOT 发送的相关指令，且只支持现有的 attack DDoS，Stop attack DDoS 两种类型执行指令，并没有像其它成熟的 DDoS 家族一样还支持 Update File、Shell comman 等类型执行指令。从目前的样本分析得知，Dnamic 家族 attack DDoS 仅是实现 syn flood、atk flood、tcp flood 3 种类型的 DDoS 攻击。

虽然 Dnamic 家族是新出现的 DDoS 家族，其一些 DDoS 木马基础功能上还未完善，但 BOT 被控端攻击类型在短短一天内就能实现从单一的“atk flood”攻击类型，增加了“syn flood”、“tcp flood”两种攻击类型，可以推测 Dnamic 家族的作者有较强的开发能力。

Dnamic 家族的发展在维护互联网安全的过程中增加了威胁的可能性，特别是其具有免杀，增快扩散蔓延的速度，继而伺机对互联网的某个目标进行 DDoS 攻击。

从目前的样本分析得知，若系统被植入该家族的 BOT 被控端，只需要删除 BOT 被控端文件后及时更新系统及软件，修复已知存在的漏洞即可；若该家族的被控端实现自启动功能，还需要将其及其备份的文件清除，并且清除关联到的自启动项。安天追影小组会持续监控该家族的动态，及时发现该家族进一步扩散的情况。

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，依据行为即可实现对上述木马程序进行有效检测，以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、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 BD 静态分析鉴定器、静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

文件名	malware.ViR
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	139 KB
MD5	D929EDA9C72BE88A8B311EB81C439C76
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Spy]/Win32.Agent
判定依据	静态分析

危险行为

行为描述	危险等级	行为描述	危险等级
删除自身	★★★★	延时	★★★
疑似查找游戏进程	★★★★		

报告地址：https://antiy.pta.center/_lk/details.html?hash=D929EDA9C72BE88A8B311EB81C439C76

根据动态行为（默认环境）得出该文件具有以下行为：删除自身、延时、疑似查找游戏进程、获取计算机名称、打开自身进程文件、释放 PE 文件、复制自身文件、增加 run 自启动项、获取驱动器类型、获取主机用户名称、查找浏览器进程、连接特殊 URL、遍历进程、查找指定内核模块、获取系统版本、独占打开文件、获取系统内存、创建特定窗体、获取 socket 本地名称、连接网络、自启动、疑似查找浏览器进程。

其他行为

行为描述	危险等级	行为描述	危险等级
获取计算机名称	★	打开自身进程文件	★
释放 PE 文件	★	复制自身文件	★★
增加 run 自启动项	★	获取驱动器类型	★
获取主机用户名称	★	查找浏览器进程	★★
连接特殊 URL	★	遍历进程	★
获取系统版本	★★	查找指定内核模块	★
获取系统内存	★★	独占打开文件	★
获取 socket 本地名称	★	创建特定窗体	★
自启动	★	连接网络	★
疑似查找浏览器进程	★★		