安天周观察

主办：安天　2016 年 4 月 11 日（总第 35 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天每日安全简讯 引领安全早新闻“微传播”

由安天安全研究与应急中心（安天 CERT）每日清晨在微信群发出的“每日安全简讯”已经在安全圈的十几个主要微信群传播转发 4 月有余，被业内称为安全新闻的“微传播”。

安天每日安全简讯源起于通过邮件分发的“安天每日安全事件简报”，2014 年 12 月 3 日安天应客户需求，建立了这一信息通报机制。天长日久，一些客户提出，邮件阅读起来不是很方便，能否改为微信发送。于是，安天 CERT 想到能否采取一种方式，让更多业内友人和用户更快捷地阅览安全信息，小伙伴们先后提出了分享网页链接、分享文件、分享图片等不同风格的发布形式，其中一位同事提出，不如干脆做成一段文本短消息，只包括 24 小时内的安全热点事件名称，这样既简洁又清晰。在信息爆炸的时代，用户更多需要的是感兴趣的安全线索，如果有读者对其中哪条内容感兴趣，自然会检索查询或询问安天的工程师。而文本消息也更便于拷贝粘贴，编辑查询。这个建议被安天 CERT 立即采纳，并命名为“每日安全简讯”。

从 2016 年 1 月 1 日起，安天主管分析与响应的副总工李柏松，每早 6 点整，准时在威胁情报、网安技术等几个微信群发出“每日安全简讯”，几个月来从无间断，也从未出现一次延迟，包括柏松出国访问友商期间都一切照旧。同时，这个每天准时而来的“新闻叫早服务”也得到了很多网友的即时转发。

目前，这一行动得到了友商的响应，多个友商陆续加入进来，以自己熟悉的领域和视野，整理每日发生的安全事件，进行新闻早报，可以说这股微传播之风，已然成为了安全业界各微信群和朋友圈的靓丽小风景。

安天四项产品荣获北京市新技术新产品（服务）证书

近日，经北京市科委、市发展改革委、市经济信息化委、市住房城乡建设委、市质监局、中关村管委会共同组成的新技术新产品（服务）认定小组联合审定，安天研发的四项产品：追影安全平台 V3.0、主机安全检查系统 V2.0、私有云安全系统 V3.0、PTD 威胁检测系统 V6.0，荣获了北京市新技术新产品（服务）证书，自认定之日起有效期 3 年。

据了解，北京市新技术新产品（服务）认定管理办法中明确指出，获选项目应具有技术先进性和创新性，并拥有自主知识产权；技术成熟、质量可靠；具有潜在的经济效益和较大的市场前景等属性。安天多项产品通过该审核，获得证书，体现了安天在信息安全领域的专业实力。

【安天 CERT】发布

《勒索软件家族 TeslaCrypt 最新变种分析》

近日，安天 CERT 发现了勒索软件 TeslaCrypt 的最新变种 TeslaCrypt 4.0，并开始进行跟踪分析。TeslaCrypt 是在 Cryptolocker 的基础上修改而成的，在其第一个版本中，TeslaCrypt 声称使用非对称 RSA-2048 加密算法，但实际上使用的是对称的 AES 加密算法，由此 Cisco（思科）发布了一款解密工具，在找到可恢复主密钥的 key.dat 文件时，可以解密被 TeslaCrypt 勒索加密的文件；但在之后的多个版本中，勒索软件 TeslaCrypt 开始使用非对称的 RSA 加密算法，被加密的文件在无密钥的情况下已经无法成功被解密。

TeslaCrypt 4.0 在 2016 年 3 月份开始出现，使用的是 RSA-4096 加密算法。经安天 CERT 分析，它具有多种特性，例如：加密文件后不修改原文件名、对抗安全工具、具有 PDB 路径、利用 CMD 自启动、使用非常规的函数调用、同一域名可以下载多个勒索软件等。

勒索软件的泛滥对企业和个人用户都具有极大的威胁，被加密后的文件无法恢复，将给用户造成巨大的损失。解决勒索软件威胁问题除了安装安全产品、防护产品、备份产品外，更需要用户在接收邮件时谨慎小心，慎重打开邮件附件或点击邮件内的链接，尤其是陌生人的邮件。

目前，安天智甲终端防护系统（IEP）可以在用户失误点击运行勒索软件时阻止其对用户文件进行加密，安天追影高级威胁鉴定系统（PTD）则具有自动识别未知勒索软件的能力。（报告完整版可登录安天官网或公众号查看）

每周安全事件

类 型	内 容
中文标题	包含 5000 万条土耳其公民记录的数据库被曝光
英文标题	50 million exposed in Turkish data breach
作者及单位	Doug Olenick；SC Magazine
内容概述	近日，一套包含 5000 万条土耳其公民信息记录的数据库被泄露至网上，数据包括了土耳其公民的名和姓、身份证号码、性别、其父母的名字、出生城市、生日、完整的住址及 ID 注册城市和地区，值得注意的是，土耳其现任总统兼前总理雷杰普·塔伊普·埃尔多安的个人信息也在其中。目前这批数据已经能够通过种子及 Magnet URL 被下载，专家推测，其很可能是窃取自某个管理土耳其公民数据的政府机构。同时，通过黑客留下的消息显示，这似乎是一起政治性质的安全事件。
链接地址	http://www.scmagazine.com/50-million-exposed-in-turkish-data-breach/article/487474/

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 4 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	G-Ware/Android.xuplant.a[rog，exp] 2016-04-04	该程序开机自启动，后台拦截屏蔽并删除指定短信，向指定号码发送短信，通过网络上传设备信息，私自下载未知文件，私自下载安装未知应用，造成用户隐私泄露，资费消耗，建议及时卸载该应用。（威胁等级低）
		Trojan/Android.Zitmo.a[prv，rmt，fra] 2016-04-04	该程序伪装成系统应用，运行隐藏图标，发送反馈短信，后台联网上传手机通讯录信息，通过极光推送服务获取网络指令，执行向手机联系人群发推广信息、设置短信屏蔽、上传等操作，包含诱导界面，窃取用户输入的基本信息，造成用户隐私泄露和一定的资费消耗，建议及时卸载该程序。（威胁等级高）
		Trojan/Android.sostation.a[exp] 2016-04-05	该应用运行会后台私自下载多个 apk 文件，监听联网变化私自下载推送应用，通知栏推送消息，包含判断是否 root、静默安装和卸载相关代码 ，造成用户资费消耗。（威胁等级高）
		G-Ware/Android.AnonyPlayer.a[rog] 2016-04-05	该应用运行会诱导用户安装恶意子包，子包会植入广告插件在一些指定的应用打开时会弹出广告，建议用户谨慎使用。（威胁等级低）
		Trojan/Android.matrixdj.a[prv，fra] 2016-04-05	该程序伪装成系统程序，安装无图标，运行后联网上传用户手机通讯录、短信箱、地理位置信息等隐私信息，还会上传环境录音和手机截屏文件，造成用户隐私泄露，建议及时卸载该程序。（威胁等级中）
		Trojan/Android.robust.a[prv，rmt，spy] 2016-04-06	该应用运行后激活设备管理器，接收邮箱指令，窃取用户短信和短信记录，通话录音，地理位置信息并通过邮箱上传，同时修改用户系统设置，造成用户隐私泄露，建议立即卸载。（威胁等级中）
	较为活跃的样本	G-Ware/Android.deltaBro.a[exp，rog]	该应用伪装成色情播放器，运行后私自下载恶意应用并静默安装，后台推送广告，造成用户资费损耗，建议及时卸载。（威胁等级中）
		Trojan/Android.lifering.a[prv，rmt]	该程序运行获取短信指令，窃取用户地理位置信息，发送反馈短信，加载启动指定组件，存在一定的安全风险，会造成用户隐私泄露，建议及时卸载。（威胁等级中）
		Trojan/Android.Downloader.bq[exp]	该程序运行后私自下载大量未知应用，建议及时卸载，避免造成资费损耗。（威胁等级中）
		Trojan/Android.emial.cz[prv，fra]	该程序伪装成正常程序，无实际功能，运行后私发短信，后台拦截用户来信执行转发操作，造成用户隐私泄露，建议及时卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 双删除远程代码执行漏洞 (CVE-2014-6333)(MS14-069)	Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。Microsoft Word 2007 SP3，Word Viewer，Office Compatibility Pack SP3 版本在解析构造的 Office 文件时，没有正确处理内存对象，远程攻击者通过构造的 Office 文档，利用此漏洞可执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Delf	此威胁是一种使用 delphi 语言编写，具有下载行为的木马类程序，运行后会连接网络并下载其他恶意程序执行，以邮件、挂马、捆绑正常软件等方式来进行传播。（威胁等级中）
		GrayWare[AdWare]/Win32.Gamevance	此威胁是一种广告类木马程序，用户为了换取免费游戏服务，同意通过软件的文本链接，以横幅和弹出窗口的形式接收广告，无论是在浏览器前端还是后台。弹出的广告一般根据用户的浏览历史和访问最频繁的网站而决定的。（威胁等级低）
		RiskWare[Downloader]/Win32.AdLoad	此威胁是一种可传播、下载广告软件的木马类程序，可以在未经用户许可的条件下侵入用户系统，并窃取重要数据，安装其他恶意软件后可以使用户的电脑性能变慢。（威胁等级中）

美国指控 7 名伊朗黑客攻击其银行和水坝

Ellen Nakashima , Matt Zapotosky/ 文　安天公益翻译小组 / 译

近日，美国司法部宣布，已经起诉了与伊朗政府有关的 7 名黑客，这是美国第一次指控政府支持的个人黑客攻击美国关键行业网络。

美国认为，所有被指控的黑客都来自伊朗。他们分别是：Ahmad Fathi，Hamid Firoozi，Amin Shokohi，Sadegh Ahmadzadegan，Omid Ghaffarinia，Sina Keissar 和 Nader Seidi。起诉书称，这 7 名黑客任职于两家伊朗计算机安全公司 ITSec Team 和 Mersad Co.，代表着伊朗革命卫队，属于伊朗军方的一个分支，旨在保卫该国的伊斯兰系统并宣传其思想。黑客的罪行包括：从 2011 年底到 2013 年 5 月攻击美国银行的公共网站；攻击纽约的一个小水坝的计算机系统，企图破坏其运作。

起诉书称，犯罪嫌疑人造成了网络混乱，包括执行分布式拒绝服务攻击 (或 DDoS 攻击)，他们雄踞世界各地的网络服务器，用它们传输大量的流量，导致 46 家美国金融机构的网站崩溃。这些攻击几乎每周都会发生，影响了几十家大型机构，使数十万客户无法访问其网上银行账户。受影响的机构和企业包括美国银行、纳斯达克综合指数、纽约证券交易所、Capital One 公司、AT & T 公司和 PNC 金融服务集团。

美国官员说，尽管伊朗不可能主动将被起诉黑客送到美国，但是起诉仍然是很重要的。

纽约大学法学院的法律与安全中心的院长扎卡里·戈德曼说：“这说明美国继续致力于提高网络犯罪的成本，美国政府能够发现网络犯罪分子的谍报技术，有信心追溯他们的活动。这也说明美国政府遵守使用一切可能的工具对付伊朗破坏核协议活动的承诺。”

情报官员表示，他们认为伊朗发动 DDoS 攻击是为了应对美国和欧洲迫使伊朗遏制其核计划而施加的越来越强烈的经济制裁。

战略与国际研究中心网络安全专家詹姆斯·刘易斯说，自 2009 年的绿色革命 (2009 年 6 月 12 日，伊朗举行总统大选。13 日，选举委员会宣布现任总统内贾德获胜；当天起，其竞争对手改革派候选人穆萨维的支持者走上德黑兰街头，抗议内贾德当局在选举中舞弊，引发自 1979 年伊斯兰革命以来的最大规模骚乱。) 伊朗开始积极发展网络空间能力。伊朗使用网络技术窥探抗议者并压制持不同政见者。尤其是伊朗革命卫队，喜欢在网络空间运作，利用前沿公司，规避西方法律，并给予他们一定程度的匿名性。伊朗不存在什么自由黑客，他们都与政府有关。

多年来，美国政府将外国政府实施的黑客攻击活动列为国家安全问题。出于外交或情报原因，官员们甚至不愿意承认遭到了外国政府的入侵。但是，随着入侵的范围和严重程度不断增加，这一点发生了改变。

总检察长助理约翰·卡林说，国家安全网络案件的起诉反映出从反恐借用的一个“新办法”。他的国家安全部于 2006 年创建，旨在防止恐怖袭击。2012 年，他表示，该部门开始训练检察官，与情报界和执法部门一起处理网络案件。

卡林说：“一旦任命了专用检察官，给予他们获取情报的权限，让他们作为一个团队协作，他们就会找出黑客和隶属关系，制定起诉书，列出证据，抓住应负责的国家黑客，并以儆效尤。”

一些政府官员说，对伊朗黑客的起诉有助于将要实施的经济制裁。奥巴马总统去年 4 月发布了一项行政命令，授权针对恶意网络活动进行制裁，这种授权还未被使用过。

原文名称	U.S. charges Iran-linked hackers with targeting banks , N.Y. dam
作者简介	Ellen Nakashima 是《华盛顿邮报》国家安全领域的记者，专注于情报、技术和公民自由问题。 Matt Zapotosky 是《华盛顿邮报》国家安全团队的成员，关注美国司法部的动向。
原文信息	2016 年 3 月 24 日《华盛顿邮报》发布 原文地址 https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html

安天发布《恶意样本移动后删除绕过防御识别的方法分析》

自删除行为是恶意样本的标志行为，一般的自删除行均采用直接的方式进行自删除，近期安天追影小组通过样本分析发现了一种间接自删除方式，即通过两次移动文件操作进行自删除。第一次 MoveFile 对源文件进行移动和重命名，第二次 MoveFileEx 将移动的目标指向 null，进行删除。虽然删除的是不同位置不同名的文件，但是也达到了自删除的目的，以下为原理分析。

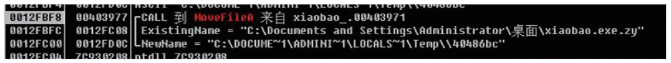
原理

底层功能函数 MoveFileWithProgress 具有将文件移动重命名的功能。

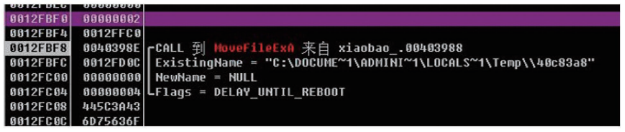
```
BOOL WINAPI MoveFileWithProgress(
    LPCTSTR          lpExistingFileName,
    LPCTSTR          lpNewFileName,
    LPPROGRESS_ROUTINE lpProgressRoutine,
    LPVOID           lpData,
    DWORD            dwFlags
    );
```

当 lpNewFileName = NULL 使用该函数会删除需要移动的文件，所以该函数在恶意代码中多用作自删除。

dwFlags 为执行该函数的方式。该样本中使用 MoveFile 进行移动和重命名。



通过设置 dwFlag = MOVEFILE_DELAY_UNTIL_REBOOT 执行完代码后，重启计算机将自删除。



实现

1) 获取当前文件路径：

```
char szPath[MAX_PATH];
GetModuleFileName(NULL,szPath,MAX_PATH);
```

2) 将自身重命名并且移动到其他指定目录下：

```
if (MoveFileWithProgress(szPath,NEWPATH,NULL,NULL,MOVEFILE_COPY_ALLOWED) == 0)
    return FALSE;
```

3) 将路径指向空，设置重启后删除方式，能完整执行完恶意代码：

```
if (MoveFileWithProgress(NEWPATH,NULL,NULL,NULL,MOVEFILE_DELAY_UNTIL_REBOOT) == 0)
    return FALSE;
```

运行该测试用例，将自身移动至指定目录下并且重命名为 7777.exe

NEWPATH=C:\\windows\\system32\\777.exe，运行后桌面的程序移动到指定目录下，重启后删除自身。

检测方法

由于该恶意行为不是直接通过删除自身而是命名后删除，混淆了主动防御对自删除的识别，因此需要通过组合规则来识别。首先获取初始样本的文件名，然后检测 MoveFile 中参数中 ExistingFileName1 是否与初始样本的文件名对应，并且记录 NewFileName1 的值。满足上述条件的情况下，获取记录 MoveFileEx 中的 ExistingFileName2 是否与 MoveFile 中的 NewFileName1 对应相等，如果相等则判断 MoveFileEx 中的 NewFileName2 是否为空，上述条件均满足就能识别出通过移动重命名自删除的这种方法。

恶意样本绕过主动防御的方法还在更新升级，越来越多的新行为会不断出现，目前，安天追影高级威胁鉴定系统 (PTD) 已经可以识别上述自删除行为。

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、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、动态行为鉴定器、智能学习鉴定器将文件判定为木马程序。该文件具有以下行为：自复制为常见系统进程名、通过 movefile 重命名，删除自身、获取系统版本、启动服务、自启动、复制自身文件、创建服务、获取计算机名称、获取 CPU 信息、访问 dns、释放 PE 文件、获取驱动器类型、独占打开文件、获取系统内存、打开自身进程文件、连接网络、疑似桌面控制。

文件名	57A9E94FABBAFF2C8DDAE39693F68393
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	28 KB
MD5	57A9E94FABBAFF2C8DDAE39693F68393
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[DDoS]/Win32.Nitol.G
判定依据	BD 静态分析

◆ 危险行为

行为描述	危险等级
自复制为常见系统进程名	★★★
通过 movefile 重命名，删除自身	★★★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=57A9E94FABBAFF2C8DDAE39693F68393