安天周观察

主办：安天　2016 年 2 月 29 日（总第 29 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

《乌克兰电力系统遭受攻击事件综合分析报告》【联合分析小组】发布

在乌克兰电力部门遭受恶意代码攻击事件后，安天、四方继保与复旦大学建立了联合分析小组，开始对此次事件进行跟踪分析。2 月 24 日，安天将联合分析组的研究成果集结成册，印发《乌克兰电力系统遭受攻击事件综合分析报告》单行本。

报告共分为五个部分，联合分析组分别从电力系统原理及断电原因分析、攻击组织及 BLACKENERGY 分析、相关样本分析等方面对该事件进行了研究。联合分析组认为这是一起以电力基础设施为目标；以 BlackEnergy 等相关恶意代码为主要攻击工具，通过 BOTNET 体系进行前期的资料采集和环境预置；以邮件发送恶意代码载荷为最终攻击的直接突破入口，通过远程控制 SCADA 节点下达指令为断电手段；以摧毁破坏 SCADA 系统实现迟滞恢复和状态致盲；以 DDoS 服务电话作为干扰，最后达成长时间停电并制造整个社会混乱的具有信息战水准的网络攻击事件。特别值得注意的是，本次攻击的攻击点并不在电力基础设施的纵深位置，同时亦未使用 0Day 漏洞，而是完全通过恶意代码针对 PC 环节的投放和植入达成的。其攻击成本相对震网、方程式等攻击，显著降低，但同样直接有效。（完整报告请登录安天官网 http://www.antiy.com/index.html 阅览）

安天成为中国互联网网络安全威胁治理联盟首批成员单位

2 月 26 日，国家互联网应急中心（CNCERT）联合中国互联网协会网络与信息安全工作委员会在北京召开互联网网络安全威胁治理行动总结大会。

大会对行动所取得的积极成果予以总结，并对行动过程中表现突出的单位进行了表彰。受表彰的包括安天、中国电信、腾讯、知道创宇、阿里、绿盟等在内的 31 家行动单位。为巩固行动取得的成果，建立互联网网络安全威胁治理长效机制，大会宣布成立“中国互联网网络安全威胁治理联盟”，加强互联网网络安全威胁情报共享、相互协作，对与互联网黑产密切相关的各类威胁进行整治，有效净化网络安全环境，维护用户网络安全和利益。安天与其他共 90 家企业成为该联盟首批成员单位。

俄罗斯安全企业大蜘蛛 Dr.Web 参观访问安天北京分公司

2 月 24 日，俄罗斯安全企业大蜘蛛（Dr.Web）CEO Boris Sharov、中国区总经理张原一行人参观访问了安天北京分公司，并同安天哈尔滨总部进行了一场远程视频会议。


大蜘蛛（Dr.Web）代表与安天哈尔滨总部进行远程视频会议

会议期间双方介绍了各自的整体概况，包括团队能力储备、公司目标及定位、主要产品等。同时就威胁检测方面的成果与问题进行了分享与探讨，大蜘蛛主要介绍了其发现中国某品牌手机存在恶意代码追踪和中国某网上银行的银行卡存在可能被恶意盗用的情况，并提出希望可以在这些问题上寻求安天协助的意愿。安天则针对某 DDoS 攻击软件（在俄罗斯发现）在国内的流行情况，同大蜘蛛代表进行了技术交流与探讨。

会议结束后安天负责人陪同大蜘蛛代表参观了北京分公司，他们对安天的预警平台非常感兴趣，并提出希望今后能够加强同安天的沟通与合作。

安天即将参展 RSA 2016

RSA 2016 即将于 2 月 29 日至 3 月 4 日，在美国旧金山启幕，本届大会的主题为“联接安全”（Connect to Protect）。作为全球规模最大、最具影响力的安全产业年度盛会，今年 RSA 将迎来其 25 周年。届时，来自全球的顶级安全专家将围绕物联网安全、工控系统安全等热门话题展开技术分享与探讨。

2016 年，安天在北美市场将以移动安全作为主要市场发力点，因此，安天今年在 RSA 将重点展示安天全域检测引擎能力、深度分析能力、纵深支持能力和高价值情报分享能力。同时，安天还会在展台发放富有特色的原创威胁通缉令扑克牌，展示移动威胁演进。安天的展台位于南馆 744 号，届时期待您的莅临！

每周安全事件

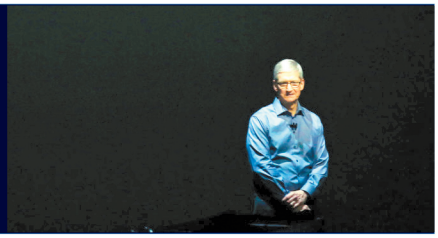
类 型	内 容
中文标题	GM Bot(安卓恶意软件) 源代码被公开
英文标题	GM Bot (Android Malware) Source Code Leaked Online
作者及单位	Swati Khandelwal，The Hacker News
内容概述	近日，安卓木马 GM Bot(又称 Mazar BOT) 的源代码被泄露在网上，该木马能够获得访问智能手机的管理员访问权限，完全清除手机的存储。同时，GM Bot 的最新版本能够在移动端银行应用程序上显示一个钓鱼页面，借此诱骗安卓用户输入个人金融账户及凭证。除此之外，这款银行木马还具有转接电话、拦截短信等功能，以此绕过银行安全机制的附加层，锁定设备屏幕。GM Bot 是安卓生态系统中最危险的银行木马之一，在其源代码泄露之后，用户在登录网上银行时要保持高度警惕。
链接地址	http://thehackernews.com/2016/02/android-malware-source-code.html

每周值得关注的恶意代码信息

经安天检测分析，本周 9 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	Trojan/Android.mazar.a[prv，exp，rmt]2016-02-21	该应用运行会请求激活设备管理器，隐藏图标，启动后台服务，联网获取远程指令，执行相应操作，包括发送短信、拨打 / 挂断电话、锁 / 解屏等等一系列操作，另外还有监听短信，拦截包含指定字符的短信、将短信内容转发到指定的远控号码，造成用户隐私泄露和资费消耗。(威胁等级高)
		Trojan/Android.antivol.a[exp] 2016-01-22	该应用程序伪装成正常程序，无实际功能，诱导用户点击按钮后会隐藏图标，后台执行联网上传联系人、短信箱、通讯录、地理位置等隐私信息，还含有拍照、通话录音功能，会给用户造成隐私泄露，建议及时卸载该程序。(威胁等级中)
		Trojan/Android.rtpkg.a[pay，sys]2016-01-23	该应用程序伪成装系统程序，安装无图标运行释放恶意子包，检测杀软，后台联网获取配置信息，安装卸载指定程序，还会发送付费短信，还含有风险赋权代码段，会给用户造成资费消耗，建议及时卸载该程序。(威胁等级中)
	较为活跃的样本	Trojan/Android.emial.cq[prv，rmt，exp]	该应用伪装成“校园通”，程序运行会请求激活设备管理器，提示与手机不兼容自动卸载，实则隐藏图标后台运行，监听短信获取短信指令，拦截短信，向远控号码发送短信，获取用户短信信息和通讯录信息上传到指定邮箱，监听用户通话获取通话录音上传到指定邮箱，造成用户隐私泄露。(威胁等级中)
		Trojan/Android.emial.cp[fra，exp]	该程序伪装成系统更新，安装运行后向手机联系人发送带有恶意软件的网址链接造成恶意传播，建议立即卸载该软件。(威胁等级中)
		Trojan/Android.Downloader.bh[rog，exp]	该应用伪装成系统应用，安装无图标，程序运行后会请求激活设备管理器，私自联网上传设备相关信息，联网下载未知应用，造成用户资费消耗。(威胁等级中)
		RiskWare/Android.FakeApp.az[fra，exp]	该程序本身无实际功能，运行会诱导激活设备管理器，后台无提示发送注册，联网上传固件信息及该程序版本信息，下载具备实际功能的同名应用，同时创建桌面快捷方式广告，具有一定的欺诈性，可能会造成一定的资费损耗，建议谨慎使用。(威胁等级低)
		Trojan/Android.FakeInst.dy[prv，exp，rmt]	该应用运行会请求激活设备管理器，隐藏图标，监听短信，拦截短信，获取短信信息，通讯录信息上传到远程服务器，联网获取远程指令发送短信，拨打电话，造成用户隐私泄露和资费消耗。(威胁等级中)
		Trojan/Android.SmsThief.aa[prv，fra]	该应用伪装成视频应用，程序运行会请求激活设备管理器，隐藏图标，私自发送短信，拦截短信并转发到指定号码，根据短信指令拨打指定号码设置呼叫转移，获取用户通讯录信息和短信信息发送到指定邮箱，造成用户隐私泄露和资费消耗。(威胁等级中)
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Word 远程代码执行漏洞 (CVE-2015-0097)(MS15-022)	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。 Office 解析构造的 Office 文件时存在 Local Zone 相关错误，通过构造 Office 文件，攻击者利用此漏洞可执行任意代码，破坏内存。(威胁等级高)
	较为活跃的样本	Trojan[Dropper]/Win32.StartPage	此威胁是一种修改浏览器首页的木马类程序。该家族将浏览器首页地址修改为指定地址，这些地址通常以广告目的为主。部分变种会修改的地址为挂马网站或钓鱼网站。部分变种会修改系统 hosts 文件，使用户不能正常访问某些网站，如安全网站。(威胁等级中)
		GrayWare[AdWare]/Win32.Verti	此威胁是一种广告行为的灰色软件类程序。该家族样本运行后在主机显示广告页面，同时具有发送电子邮件的功能，部分变种可以被黑客远程访问，是一类较危险的风险软件家族。(威胁等级中)
		GrayWare[AdWare]/Win32.SideTab	此威胁是一种广告行为的灰色软件类程序。它可以通过安装免费软件捆绑安装到浏览器，造成浏览器劫持。将修改浏览器的默认或自定义设置，包括主页，搜索设置。弹出广告和网页链接链接广告。(威胁等级中)

解密苹果与 FBI 之争



Kim Zetter / 文　安天公益翻译小组 / 译

近日，一名法官命令苹果帮助 FBI 解锁圣贝纳迪诺枪击案一名嫌疑人使用的 iPhone。这并不是解锁一部手机的问题，而是命令苹果公司创建一个新的软件工具，绕过苹果内置到手机软件中来保护客户数据的特定安全保护措施。

该案例事关重大，因为它涉及苹果等硅谷公司在过去两年中与美国国会的“加密 / 后门”争论。如果 FBI 成功迫使苹果公司就范，这也将成为其他国家当局效仿的先例，他们也会要求苹果公司提供同样的软件工具。为了澄清事实，纠正一些误解，我们对该问题的来龙去脉进行一下汇总。

问题是什么

涉事手机是 iPhone 5C，其上运行 iOS 9 软件版本。由于手机软件的内置安全功能，FBI 无法暴力破解 (即输入不同的密码，直至找到正确的密码) 手机的密码和访问其中的数据，因为尝试密码可能会导致手机中的数据被永久性销毁。

苹果如何做到这一点

为了防止有人暴力破解密码，苹果用户可以启动一个功能，限制输入密码的次数，超过次数之后密码就会被擦除。虽然数据还保存在手机上，但是它再也无法被解密，因此，就会永远不可访问。

除了自动擦除功能，还有另一个针对暴力破解的保护措施：时间延迟。即每一次在手机上输入密码时，系统需要大约 80 毫秒的时间来处理密码并判断它是否正确。这有助于防止人们快速尝试一个新密码，因为每 80 毫秒才能尝试一个密码。这个时间看起来并不长，但是根据密码的不同长度，这种延迟可能导致破解过程非常漫长。

为什么旧款 iPhone 不存在该问题

在 iOS 8 之前的旧版操作系统上，苹果公司能够绕过用户的密码，解锁手机，访问其中的数据。但从 iOS8 开始，苹果改变了这一情况，手机默认使用用户密码，对手机上的重要数据进行加密，包括照片、邮件、联系人和通话记录。就连苹果公司也无法绕过用户密码来获得数据。

政府想要什么

很多人都曲解了政府的要求，认为它要求法院命令苹果公司解锁涉事手机，就像苹果公司以前做过的那样。但如前所述，涉事手机上安装了特定的操作系统，苹果无法绕过密码和解密数据。因此，政府希望，在暴力破解密码时不会导致系统自动擦除解密密钥，而且在尝试密码时不会造成额外的时间延迟。

为了做到这一点，政府希望苹果公司创建一个特殊的操作系统版本，在固件中设置后门，消除暴力破解保护措施，并将该版本安装到涉事手机上。政府还希望苹果提供帮助，可以用电子方式输入猜测的密码，而不是通过触摸屏输入。这样，FBI 就可以运行一个密码破解脚本，自动输入猜测的密码。

政府正在利用的漏洞是什么

该漏洞是，苹果公司不需要用户获得同意，就可以更新固件，安装一个设置了后门的版本。

如何保护隐私

你可以设置由字母和数字组成的密码，这样，FBI 或其他任何人都不太可能暴力破解它。 如果密码由字母和数字组成，而且是 6 到 8 位，可能的密码组合非常多，没人能够破解。

苹果公司可以做什么

苹果可以并且应该修改其系统，使以后的机型无法做到 FBI 要求苹果公司做的事情，即使苹果公司愿意也无法做到。例如，在进行固件更新之前，他们可以要求某种类型的用户确认，要求用户输入 PIN 码。或者，他们可以将 secure enclave 烧录成芯片中的只读存储器，使其完全失去更新能力。这样，如果没有机主的同意，苹果就无法将有后门的固件上传到设备中。或者，根本就不能更新 secure enclave 的固件。

苹果应该预见到该漏洞吗

Trail of Bits 公司首席执行官丹・圭多表示 “直到最近，苹果公司才不得不考虑这一问题：如果我们攻击自己的客户，会是什么样？如果我们删除用来保护客户的安全措施，会是什么样？”

他补充说：“苹果竭尽全力地确保 iPhone 免受远程入侵或其他攻击。但是从现在开始，在保护用户方面，技术厂商需要考虑把自己也视为可能的威胁。这是一个相当大的转变。”

原文名称	Apple's FBI Battle Is Complicated. Here’ s What’ s Really Going On
作者简介	Kim Zetter，《连线杂志》一位屡获殊荣的资深记者，研究范围包括网络犯罪、隐私和安全。
原文信息	2016 年 2 月 18 日发布于《连线杂志》 原文地址 http://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/

安天发布《大灰狼远控变形 DNS 分析报告》

据调查，“大灰狼”远控长期以来一直处于不断更新、升级的状态。近日，安天追影小组通过威胁感知平台发现一类“大灰狼”远控样本，该样本的 C2 连接方式较为新颖，以第三方 ip 查询的方式来实现 DNS 的功能，以达到突破域名检测的目的，同时控制端使用的是免费二级域名 gnway.cc，为追踪黑客身份增加了难度。

安天追影小组在对其初步分析中发现，该样本会连接控制端下载文件“NetSyst81.dll”，该文件是“大灰狼”远控的典型文件。同时，该样本有自复制为常见系统进程名、自删除、修改注册表、设置自启动、通过 CMD 隐藏删除自身、创建可疑进程、设置调试器权限、检查摄像头、连接网络、查找杀软件相关进程等行为。

对该样本进行网络分析后可发现，其网络行为中有连接某个 QQ 号空间的行为。通过对该 QQ 号的查找、分析发现，该 QQ 号的关联帐号，近期在一些黑客论坛上购买过“大灰狼”远控。所以该 QQ 号的所有者很有可能是该样本的制作者。

样本行为：

1. 样本运行后，会创建多个进程，自复制为常见的系统进程名 servise.exe 并自删除原样本。

2. 设置开机自启动，修改注册表路径 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run。

3. 网络连接通过 ip.cn 作为中转 DNS，查找控制端域名的 IP 地址，其中控制端域名为免费二级域名，本机与控制端通信下载文件“NetSyst81.dll”后访问某 QQ 空间两次，推测该行为是为了以 QQ 空间昵称为远控上线方式，经过对该 QQ 号的关联搜索发现，该 QQ 号 532**** 的所有者很有可能是该样本的作者（修改大灰狼源码的作者）。

4. 样本随后有设置调试器、检查摄像头、查找杀软等行为。

“大灰狼”远控有着较长久的历史，其软件更新换代较快，在搜索引擎中搜索该关键字，会出现大量的该远控的源码及生成器售卖，并且以免杀、破解来吸引用户，但大部被修改过的源码都会留有后门，所谓“螳螂捕蝉，黄雀在后”。为了预防该恶意样本，安天追影小组建议用户尽量在官网下载程序，不要随意打开不明链接。

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。

暂时依据 BD 静态分析鉴定器、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，正在等待美国软件交叉索引 (NSRL) 鉴定器进行分析。该文件具有以下行为：根据进程名称复制文件；删除自身；注册 tamper 服务；使用 cmd 删除自身；服务 DLL；可疑进程名称；请求调试权限；检查摄像头；读取自身文件；连接特殊 URL；查找反病毒程序；获取 CPU 信息；创建互斥体 (mutex)；隐藏文件；填充导入表（疑似壳）；释放 PE 文件；增加 run 自启动项；获取系统内存；访问 DNS；获取系统版本；打开自身进程文件；访问文件尾部；获取计算机名称；获取 socket 本地名称；在根目录创建可执行脚本；篡改系统文件创建时间；复制自身文件；创建服务；连接网络；创建特定窗体；获取驱动器类型；独占打开文件；遍历进程；启动服务；获取主机用户名称；查找指定内核模块；请求加载驱动的权限；更新服务配置信息。

文件名	A10E07BC570A329EE688EEA66D4BAC5A
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	544 KB
MD5	A10E07BC570A329EE688EEA66D4BAC5A
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[:HEUR]/Win32.AGeneric
判定依据	静态行为

危险行为

行为描述	危险等级	行为描述	危险等级
根据进程名称复制文件	★★★	删除自身	★★★★
注册 tamper 服务	★★★★	使用 cmd 删除自身	★★★★
服务 DLL	★★★	可疑进程名称	★★★★

其他行为

行为描述	危险等级	行为描述	危险等级
请求调试权限	★	检查摄像头	★★
读取自身文件	★★	连接特殊 URL	★
查找反病毒程序	★★	获取 CPU 信息	★★
创建互斥体 (mutex)	★	隐藏文件	★★
填充导入表（疑似壳）	★★	释放 PE 文件	★
获取系统内存	★★	增加 run 自启动项	★
获取系统版本	★★	访问 DNS	★
访问文件尾部	★	打开自身进程文件	★
获取 socket 本地名称	★	获取计算机名称	★
在根目录创建可执行脚本	★★	复制自身文件	★★
篡改系统文件创建时间	★★	创建服务	★
连接网络	★	创建特定窗体	★
独占打开文件	★	获取驱动器类型	★
获取主机用户名称	★	遍历进程	★
查找指定内核模块	★	启动服务	★
请求加载驱动的权限	★	更新服务配置信息	★★

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=A10E07BC570A329EE688EEA66D4BAC5A