安天周观察

主办：安天　2016 年 3 月 21 日（总第 32 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加『网络与信息安全信息通报席位协同工作部署会』

3 月 18 日，由北京市公安局网安总队主办的“网络与信息安全信息通报席位协同工作部署会”顺利召开，安天、绿盟、知道创宇、启明星辰、奇虎 360 等 11 家单位参加了会议。在国家网络与信息安全信息通报中心的支持下，“国家网络与信息安全信息通报中心——北京分中心”宣告成立，在会上，主办方表示希望各单位发挥各自技术特长与其他相关单位通力合作，在分中心的统一指挥和协调下完成具体通报预警工作。

安天在今年全国“两会”期间的安保工作得到了分中心领导的充分肯定。安天凭借在历年重大活动安保工作中的优异表现，获得了参与2016年“两会”期间安保工作的机会，在主管部门的指导下，紧紧围绕全国“两会”安保工作的部署需求，保障了会议期间的网络安全。

安天历经十五年持续积累，综合应用已经形成了海量安全威胁知识库、网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面的经验，推出了应对持续、高级威胁 (APT) 的先进产品和解决方案，在公安部测试中被认定为增强级产品。凭借感知捕获和自动化分析能力，参与国内多个综合安全监控预警平台建设。今后，安天将继续发挥自身技术优势，在各主管部门的统一指挥和协调下，切实做好网络安全相关工作，积极完成北京分中心的具体通报预警任务。

安天参加“工业控制系统安全研讨会”

乌克兰电力系统遭受攻击事件发生后，工业控制系统的安全问题持续受到关注。3 月 17 日，由《中国信息安全》杂志主办的“工业控制系统安全研讨会”在中国信息安全测评中心召开，来自相关管理部门、能源、电力、船舶等重要行业的管理人员、业内专家等 20 多人参与了相关讨论。

会上，安天技术负责人分享了事件发生后由安天、四方继保、复旦大学联合分析小组发布的《乌克兰电力系统遭受攻击事件综合分析报告》。主要分析了本次事件的攻击原理、所使用的 BlackEnergy 等相关恶意代码攻击工具，通过 BOTNET 体系进行前期的资料采集和环境预置；利用邮件发送恶意代码载荷为最终攻击的直接突破入口等手段；以及通过远程控制 SCADA 节点下达指令，摧毁破坏 SCADA 系统以实现攻击目标的攻击原理，并对此事件给工控系统网络安全带来的思考等进行了分享。

来自各管理部门和一线行业的管理人员在会上也汇报和分享了工控系统网络安全在各个行业的现状和思考。

一周简讯

- 研究发现滥用 API 造成漏洞更加普遍 尤其是移动应用
- 抗 DDoS 厂商 Staminus 被入侵 客户信息和敏感数据泄露
- Word 文档宏 +PS 脚本钓鱼邮件是近几月主流攻击方法
- 勒索软件家族 TeslaCrypt 借 Neutrino 漏洞套件传播
- 300 流行网站钓鱼域名曝光 重定向安装 OS X 恶意代码
- “奥运愿景”行动针对中东、亚太地区企业邮箱发动攻击
- 安天 AVL 联合猎豹安全首曝“多米诺”恶意应用市场 APP

（安天 CERT 搜集整理，完整内容可登录创意安天论坛 http://bbs.antiy.cn/forum.php）

配备骁龙芯片的安卓手机可被攻击，受影响设备数量达十亿

近日，安全人员表示，高通的骁龙处理芯片中存在一个严重的设计漏洞，使攻击者能够通过各种方法来获取到目标设备的 root 访问权限。据不完全统计，目前大约有超过十亿台安卓设备正在使用这款可能被恶意软件所攻击的处理器芯片。

获取安卓手机的 root 权限是一个非常值得关注的问题。因为当用户对手机进行 root 操作之后，虽然方便了自己的使用，却也给攻击者提供了可乘之机。攻击者可以利用这一点来获取到目标设备的管理权限，这样一来，他们就可以截取手机屏幕的信息，并且窃取你手机中的个人资料，包括账户密码、电子邮件、手机短信和照片等等。

(http://news.hitb.org/content/more-billion-snapdragon-based-android-phones-vulnerable-hacking)

每周安全事件

类 型	内 容
中文标题	安卓恶意软件 GMBot 2.0 版本出现，售价比 v1 版本贵三倍
英文标题	GM Bot v2 Emerges on the Underground Markets，Three Times the Price of v1
作者及单位	Catalin Cimpanu；Softpedia
内容概述	近日，安全团队检测到了第二个版本的 GM Bot 银行木马病毒。GM Bot 可以在移动端银行软件上层显示一个钓鱼页面，借此诱骗安卓用户输入个人金融账户及凭证。GM Bot v1 版本出现的时间是 2014 年，售价最高可达到 5000 美元。目前，其制造者 GanjaMan 已经发布了 GM Bot v2 版本，比 v1 版本贵三倍，而且他表示未来 v2 版本将可以通过 Tor 网络使用木马程序。但从另一面来看，GM Bot v2 的出现正是因为 GM Bot v1 已经可以被安全公司检测和查杀。
链接地址	http://news.softpedia.com/news/gm-bot-v2-emerges-on-the-underground-markets-three-times-the-price-of-v1-501637.shtml

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	Trojan/Android.SmsCall.a[exp，sys] 2016-03-14	该程序安装无图标，通过 so 文件及资源文件的配合使用完成提权及下载安装的操作，建议立即卸载，避免造成资费损耗及用机体验。（威胁等级高）
		G-Ware/Android.Golem.a[rog，exp，rmt]2016-03-15	该程序运行后隐藏图标，后台下载恶意文件在用户不知情的情况下远程控制手机，启动并运行应用，这些恶意行为会消耗大量的网络数据、电池电量和本地设备资源，造成用户资费损耗的同时还会影响用户的用机体验，建议立即卸载。（威胁等级低）
		Trojan/Android.ViaDial.a[prv，fra] 2016-03-15	该程序伪装 Google 服务，运行隐藏图标诱导用户激活设备管理器，后台联网上传手机号、imei 等固件信息，获取网址执行私自下载操作，后续会执行上传联系人，对通讯录插入指定号码等敏感操作，还含有关闭指定进程等风险代码段，会给用户造成资费消耗和隐私泄露，建议及时卸载该程序。（威胁等级高）
		RiskWare/Android.xsxux.a[sys] 2016-03-16	该应用是个恶意插件，联网下载提权相关文件私自提权，屏蔽运营商订阅类的短信，存在隐私泄露的风险，建议谨慎使用。（威胁等级低）
		Trojan/Android.Triada.d[sys，prv，exp] 2016-03-17	该应用程序运行监听短信，后台联网上传短信信息，具有发送短信的能力，建议立即卸载避免造成隐私泄露和资费损耗。（威胁等级中）
	较为活跃的样本	G-Ware/Android.FakeApp.ba[rog，exp]	该程序伪装成系统应用，运行后隐藏图标，后台推送大量广告，会造成用户资费损耗，建议立即卸载。（威胁等级低）
		Trojan/Android.emial.cw[prv，exp，fra]	该应用运行会隐藏图标，私自发送指定短信，获取用户联系人信息和短信信息，上传到指定邮箱，监听短信拦截短信，获取短信信息转发到指定号码和上传到指定邮箱，造成用户隐私泄露和资费消耗。（威胁等级高）
		Trojan/Android.Zmnspy.b[prv，fra]	该程序伪装成系统程序，安装无图标，运行获取用户收件箱、通话记录、位置信息、通话录音等隐私信息，并执行邮箱上传操作，会造成用户隐私泄露和资费消耗，建议立即卸载该程序。（威胁等级中）
		Trojan/Android.Stealer.o[prv，rmt，exp]	该程序伪装成其他应用，运行后会激活设备管理器，隐藏图标，联网上传用户短信信息，获取远程指令执行相应操作，包括发送指定短信、拨打电话、安装和卸载应用、清除数据恢复出厂设置等行为，还有监听短信拦截短信，更新删除短信的行为，造成用户隐私泄露和资费消耗。（威胁等级中）
		Trojan/Android.SmsThief.ae[prv]	该程序伪装成图片应用，后台上传用户信箱信息到远程服务器，建议立即卸载，避免造成用户隐私泄露。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	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[Downloader]/Win32.Adload	此威胁是一种木马类程序，运行后会释放可执行文件，并访问远程服务器，会下载其他恶意可执行程序，添加注册表信息，并添加计划任务，用来执行恶意程序。（威胁等级中）
		Trojan/Win32.StartPage	此威胁是一种木马类程序，会将浏览器首页地址修改为指定地址，通常以广告为主，部分变种会修改为挂马网站或钓鱼网站地址。还有部分变种会修改系统 host 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.Lollipop	此威胁是一种广告行为的广告软件类程序。在用户浏览网页时弹出广告，还可以重定向搜索引擎搜索结果，监测用户行为，下载其他应该程序，可能会发送用户信息给攻击者。（威胁等级低）

转账出现错别字 10 亿美元终落空

路透社 / 文　安天公益翻译小组 / 译

近日，网上银行转账指令中的拼写错误防止了一起近 10 亿美元的盗窃，涉事银行是孟加拉国中央银行和纽约联邦储备银行。但未知黑客仍设法卷走了 8000 万美元，这是历史上已知的最大的银行盗窃案件之一。

两名高级银行官员说，黑客攻破了孟加拉国银行的系统，窃取了转账凭证。然后，他们向纽约联邦储备银行发送了近 30 个请求，要求把孟加拉国银行账户中的资金转移到菲律宾和斯里兰卡实体的账户中。

前 4 个请求要求转账到菲律宾实体的账户中，总计约 8100 万美元，进展颇为顺利。但是第 5 个请求 (转账 2000 万美元到斯里兰卡一家非营利组织的账户中) 被阻止了，因为黑客拼错了该非政府组织 Shalika Foundation 的名字。

黑客将该非政府组织名称中的“Foundation”拼写为“fandation”，这促使汇款银行 (德意志银行) 向孟加拉国中央银行寻求验证，此后这一交易被终止。

斯里兰卡注册的非盈利组织名单中并没有名为 Shalika Foundation 的非政府组织。路透社未能立即查到该组织的联系信息。另一方面，德意志银行拒绝对此发表评论。

与此同时，与其他银行相比，美联储向私营实体的支付指令和转账请求的数量异常得高，这也引起了孟加拉国的怀疑。

黑客活动是如何被发现的，又是如何在造成更多损害之前被阻止的，这些还未

被报道过。孟加拉国银行的美联储账户中有数十亿美元的资金，用于国际结算。其中一名官员指出，被阻止的交易总额达到 8.5 到 8.7 亿美元。

孟加拉国银行表示，他们已经追回了一部分被盗的资金，并正在与菲律宾反洗钱机构合作，希望追回其他资金。追回的资金是被阻止的斯里兰卡转账。

一个泛亚银行官员说，最初，斯里兰卡交易已经到达了泛亚银行，因为转账金额异常巨大，泛亚银行再次与德意志银行进行确认。

这位官员说：“对于我们这样的国家来说，这个交易额实在是太大了。然后，德意志银行回复称这是一个可疑的交易。”

泛亚银行发言人没有立即对此事发表评论。

全球黑客抢劫事件层出不穷，这说明网络犯罪威胁越来越严重，而黑客们总是能够从最安全的计算机网络中找到薄弱环节。2015 年，俄罗斯计算机安全公司卡巴斯基实验室指出：跨国网络犯罪分子团伙在两年内从世界各地多达 100 个金融机构窃取的资金高达 10 亿美元。

攻击发生后一个多月，孟加拉国的官员争先恐后地追查资金去向，完善其安全措施，并确定其系统漏洞。他们说，逮捕黑客的希望不大，即使真得能够追回这笔钱，可能也需要几个月的时间。

安全专家称，涉事黑客非常了解孟加拉国银行机构的内部运作，可能是通过监控银行职员获得了信息。

同时，孟加拉国政府指责美联储没有更早地终止交易。周二，财政部长阿布·马尔·阿布杜尔·穆希特告诉记者，孟加拉国可能会起诉美联储来收回这笔钱。

他说：“美联储必须承担责任”。

纽约联邦储备银行曾表示，它的系统没有被攻击，事件发生后，一直与孟加拉国中央银行协作。

孟加拉国银行的黑客攻击发生在 2 月 4-5 日之间，是一个周五，正是孟加拉国的周末，银行并不上班。

最初，中央银行不确定它的系统是否已被攻击，但是网络安全专家调查之后发现了黑客的“足迹”，这说明系统已遭到了攻击。并且这些专家也能够确定攻击来自孟加拉国境外，银行正在调查攻击者是如何进入其系统的，目前内部调查正在进行中。

相关官员说，银行怀疑，转到菲律宾的资金被进一步挪用到了赌场。负责监管博彩业的菲律宾娱乐及博彩公司表示，他们已经就此展开了调查，同时，该国的反洗钱机构也正在调查此案。

原文名称	Spelling mistake prevented hackers taking $1bn in bank heist
作者简介	路透社，一家国际新闻机构，总部位于英国伦敦。
原文信息	2016 年 3 月 10 日发布于路透社 原文地址 http://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist
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《Hawkeye 键盘记录器网络犯罪分析报告》

安天追影小组近日在梳理恶意攻击事件时，发现了一起 Hawkeye 键盘记录器通过邮件发送 word 文档方式实施网络犯罪的安全事件，该事件的主要受害者是以邮件方式处理销售订单的公司。

黑客利用发送以 word 文档为附件的邮件，使受害者在未及时安装更新的环境下点击运行附件后触发漏洞，从而下载并安装 Hawkeye 的键盘记录器恶意程序，该程序通过电子邮件，FTP 或 web 的方式上传受害者的信息来达到获取键盘记录的目的，相关分析报告显示，该类键盘记录器已经感染过会计、金融、对外贸易、海关和物流、政府、科技等多个行业，受害者分布在许多国家。

黑客发送的电子邮件内容一般包含一个订单或者报价请求，邮件一般会被转发到公司处理财务的雇员处。恶意软件安装成功后，黑客等待受害者登录公司的邮件并窃取帐号和密码从而监视发件箱，当发现受害者给客户发送订单发票等有价值的邮件时，黑客则伺机而动，使用受害者邮箱发送其事先准备好的邮件给客户，通知其公司的收款帐号有改变，而改变后的帐号则为黑客的帐号，当客户没有电话确认的情况下，会汇款到黑客的帐号，使黑客完成其网路犯罪。经分析，在黑客发送的几千个邮件中只有极少数会成功，然而，有时一笔诈骗可达 100 万美元以上，这使得极少数的成功案例变得很“值得”。

网络安全事件防不胜防，一个看起来无害的 word 文档有时也会使客户造成巨大的损失，为了预防该类恶意程序，用户需要做到以下几点：及时下载安装正版的软件更新；不轻易下载不明发件人发来的邮件附件；对实际金钱交易的商业行为最好打电话或用其他方式进行二次确认后再实施。

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。

暂时依据动态行为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。

文件名	853F160A58FD2B8700E1B2F1ACB7B5D1
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	768 KB
MD5	853F160A58FD2B8700E1B2F1ACB7B5D1
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	动态行为

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
删除自身	★★★	BlackWorm	★★★★★
疑似键盘记录	★★★★★		

该文件具有以下行为：删除自身；BlackWorm；疑似键盘记录；请求调试权限；读取自身文件；获取驱动器类型；创建互斥体 (mutex)；填充导入表（疑似壳）；释放 PE 文件；获取系统内存；创建挂起的进程；关机；访问其他进程内存；获取计算机名称；获取 socket 本地名称；复制自身文件；创建特定窗体；独占打开文件；打开自身进程文件；获取主机用户名称；请求加载驱动的权限。

◆ 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	★	读取自身文件	★★
获取驱动器类型	★	创建互斥体 (mutex)	★
填充导入表（疑似壳）	★★	释放 PE 文件	★
获取系统内存	★★	创建挂起的进程	★★
关机	★	访问其他进程内存	★
获取计算机名称	★	获取 socket 本地名称	★
复制自身文件	★★	创建特定窗体	★
释放 PE 文件	★★	独占打开文件	★
获取主机用户名称	★	打开自身进程文件	★
请求加载驱动的权限	★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=853F160A58FD2B8700E1B2F1ACB7B5D1