每日安全简讯

[20160301]

1、美国国土安全部 CERT 证实 乌克兰断电事件为网络攻击导致
2、菲律宾新闻署网站被黑并发布多条假新闻 当地媒体险被误导
3、报告显示 2015 年移动恶意软件数量翻三倍 勒索软件首当其冲
4、"阅后即焚"应用厂商 Snapchat 被钓鱼 新老雇员敏感信息泄露
5、安全厂商报告称 Angler EK 和勒索软件仍活跃于各大热门网站
6、研究者称 "系统升级"功能是多数软件内置的"万能钥匙"级后门

安天 CERT 搜集整理（来源：Securityaffairs、中国网、firstpost、techcrunch、Informationsecuritybuzz、arstechnica）

[20160302]
1、安全厂商曝光首个以色列银行木马 ATMZombie
2、厂商发现窃密木马 Rover 针对印度驻阿富汗大使
3、人气约会网站 Mate1 被黑 2700 万用户密码将出售
4、Outlook 2016 最新版本被发现误删除用户邮件 bug
5、Mac 样本使用新版 RCS Hacking Team 或重出江湖
6、Uber 验证不严格 被盗号用户将成黑客的"提款机"

安天 CERT 搜集整理（来源：Securelist、Paloaltonetworks、cnBeta、Solidot、Engadget、凤凰网）
[20160303]
1、OpenSSL 出现新漏洞 三成 HTTPS 网站受严重影响
2、BIFROSE 木马跨平台新变种 可感染类 UNIX 系统
3、Web 版勒索软件 CTB-Locker PHP 源码现身 GitHub
4、研究发现 Netgear 及 D-Link 设备存在多个高危漏洞
5、19 岁黑客入侵航空公司官网 窃取旅客信息 167 万条
6、骗走全球 5 千万美元的土耳其 ATM 黑客在美国认罪

安天 CERT 搜集整理（来源：Softpedia、Trendlabs、Freebuf、Computerworld、sohu、nydailynews）
[20160304]
1、勒索软件借信用卡钓鱼邮件传播 受害者以英、美国家为主
2、研究者发现 Win10 默认 PDF 阅读器风险 或用于 drive-by 攻击
3、幽灵电子书(ChmGhost)木马 专偷网络安全人员文档、帐号
4、研究者发现 RSA 大会徽章扫描程序存安全隐患 可恶意利用
5、Foxmail 最新版客户端或有漏洞 打开邮件即可执行远程命令
6、美国国防部新举措：五角大楼请黑客找出技术缺陷和漏洞

安天 CERT 搜集整理（来源：Helpnetsecurity、Softpedia、freebuf、Securityweek、乌云、thestreet）

[20160305]

1、勒索软件 Cerber 具语音能力 "勒索即服务"时代到来
2、移动威胁新伎俩 Triada 木马可感染 Zygote 核心进程
3、巴西跨平台银行木马初露端倪 三大系统无一幸免
4、研究者发现最新广告件木马家族 专门针对 Mac 系统
5、研究发现低成本侧信道取证设备 窃取安卓苹果密钥
6、统计表明银行帐户弱密码仍占三成 或泄露 3.5 亿帐号

安天 CERT 搜集整理（来源：Softpedia、Securelist、Drweb、Arstechnica、Threatpost）

[20160306]

1、WordPress 插件有后门 可记录窃取用户登录密码
2、Android"辅助功能"可用于窃密 超 5 亿设备存隐患
3、警用无人机有漏洞 黑客称可在一英里外将其劫持
4、库尔德反 ISIS 黑客攻击斐济共和国军事部队网站
5、匿名者黑客组织发布蒙哥马利警局人员个人资料
6、报复马航 MH17 坠机 年轻黑客计划攻击俄文网站

安天 CERT 搜集整理（来源：Softpedia、Minternets、wired、asiapacificreport、montgomeryadvertiser、vice）

[20160307]

1、石油天然气企业关键设备存漏洞 或成黑客攻击目标
2、黑客入侵美国总统候选人特朗普语音邮件 并予泄露
3、海盗懂技术：入侵航运公司网站 找高价值目标船只
4、黑客利用 Facebook 测验骗取用户信息 传播恶意代码
5、黑名人帐户的罗马尼亚黑客 最终将引渡到美国受审
6、亚马逊计划停用加密技术 设备或成黑客"瓮中之鳖"

安天 CERT 搜集整理（来源：Hackread、Betanews、Securityaffairs、msnewsnow、Softpedia、腾讯）

[20160308]

1、OS X 平台首个全功能勒索软件被发现 借 BT 下载软件传播
2、"透明部落"行动曝光：针对印度外交、军事实体间谍行动
3、ATM 劫匪越狱 使用恶意代码 Tyupkin 盗窃 ATM 机细节曝光
4、知错能改：亚马逊称将恢复设备全盘加密及数据保护功能
5、鹰眼攻击：揭示黑客利用特制 Office 文档窃巨款最新伎俩
6、黑客组织 Onion Dog 曝光 攻击目标为朝鲜语国家基础行业

安天 CERT 搜集整理（来源：paloaltonetworks、Security Affairs、Softpedia、securityweek、komando、360bobao）

[20160309]

1、韩称朝入侵其政要智能手机 系四次核试后系列行动
2、首个 Mac 勒索软件已被清剿 Transmission 业已下架
3、研究者曝光 iOS 9 多种密码绕过漏洞 建议暂关闭 Siri
4、研究发现密码重置漏洞 Facebook 帐号可被暴力破解
5、Netskope 报告称攻击者利用云同步和共享传播威胁
6、希捷员工被钓鱼 近万雇员社会安全号隐私信息泄露

安天 CERT 搜集整理（来源：securityweek、usatoday、Security Affairs、InformationSecurityBuzz、Softpedia）
[20160310]
1、"帮你拍的小视屏"手机木马肆虐 传播途径已被及时切断
2、基于 JAR 跨平台恶意代码制造和传播 巴西名列世界第一
3、美国罗森连锁酒店被安装恶意代码 窃取客人信用卡信息
4、研究人员发现手机新木马 可仿冒银行应用绕过短信验证
5、逾百万搭载高通处理器智能设备存漏洞 轻易获 root 权限
6、微软将发布多项安全更新 含锁屏状态 USB 代码执行漏洞

安天 CERT 搜集整理（来源：anva、SecurityAffairs、theregister、pymnts、trendmicro、securityweek）
[20160311]
1、libotr 有漏洞 多款 IM 软件可被攻击者执行远程代码
2、ICIT 报告称勒索软件即将肆虐于美国关键基础设施
3、勒索软件或将取代僵尸网络成为企业主要安全威胁
4、研究者称垃圾邮件中勒索软件占两成 多数为 Locky
5、商家确认海底捞系统服务配置不当可控万余台 ipad
6、苹果勒索软件 KeRanger 原系改造后 Linux.Encoder

安天 CERT 搜集整理（来源：helpnetsecurity、scmagazine、siliconangle、pcworld、wooyun、mackungfu）
[20160312]
1、恐怖组织 ISIS 数据 U 盘泄露 2.2 万成员个人信息曝光
2、Dridex 僵尸网络借 JS 邮件附件传播勒索软件 Locky
3、黑客转帐时拼错一个词 孟加拉国央行少丢 10 亿美元
4、厂商确认：海尔某系统漏洞涉及全国上亿工单数据
5、阿里发布 2015 物联网安全年报：威胁攻击日益凸显
6、多个 ISC BIND 拒绝服务高危漏洞已修复需及时更新

安天 CERT 搜集整理（来源：Freebuf、securityweek、nbcnews、补天、securityweek）
[20160313]
1、安全厂商称找到 Mac 勒索软件 KeRanger 加密文件的解密方法
2、移动恶意代码 GM Bot 源码泄露后续 原作者提价发布新版本
3、安全厂商发布智能手表版本 android 安全软件 可控手机安全
4、研究人员发布报告宣称大多数云服务仍未修补 DROWN 漏洞
5、苏格兰皇家银行遭黑客攻击 攻击者采用 SMS 短信息钓鱼手法

6、韩国方面称：过去一月朝对韩铁路和金融网络攻击规模加倍

安天 CERT 搜集整理（来源：softpedia、securityintelligence、techrepublic、securityweek、GrahamCluley、thehill）

[20160314]

1、调查者称孟加拉国央行窃案发现 0day 利用 为 APT 攻击
2、美肿瘤医院遭受黑客攻击 220 万员工和患者信息泄露
3、研究发现 Oracle 两年前发布 Java 沙箱逃逸补丁可绕过
4、研究发现滥用 API 造成漏洞更加普遍 尤其是移动应用
5、手机木马 Marcher 变种 借 Flash 安装包和成人网站传播
6、朝鲜否认韩国对其发动网络攻击指责 称之为政治宣传

安天 CERT 搜集整理（来源：fortune、Dark Reading、Security Week、networksasia、eweek、ibtimes）

[20160315]

1、巴基斯坦黑客入侵印医学网站 称将黑遍印度政府网站
2、官方警告:勒索软件借澳大利亚邮政名义发送社工邮件
3、不止是苹果 美国政府已经盯上了下一个目标 WhatsApp
4、罗马尼亚知名黑客 GhostShell 为求职自行透露真实身份
5、新世界黑客组对盐湖城警察局、机场和银行发动 DDoS
6、抗 DDoS 厂商 Staminus 被入侵 客户信息和敏感数据泄露

安天 CERT 搜集整理（来源：indiatimes、choice、techweb、softpedia、hackread）

[20160316]

1、匿名者组织扬言 4 月 1 日对美国总统竞选发动网络攻击
2、安全厂商称 AE Kit 感染流行网站 24 小时影响数万用户
3、安全厂商发现盗号木马瞄准 Steam 游戏平台帐号资产
4、Word 文档宏+PS 脚本钓鱼邮件是近几月主流攻击方法
5、300 主流网站存在钓鱼域名 重定向安装 OS X 恶意代码
6、安全厂商发现多起针对外蒙政府鱼叉式钓鱼邮件攻击

安天 CERT 搜集整理（来源：softpedia、trendmicro、securelist、pcworld、gizmodo、paloaltonetworks）

[20160317]

1、安全厂商曝光首个可感染未越狱苹果系统的木马
2、Yahoo 修复电子邮件服务漏洞 可用于伪造发件人
3、勒索软件家族 TeslaCrypt 借 Neutrino 漏洞套件传播
4、研究人员发现 Carbanak 组织行动 针对中东、美国
5、安全厂商发布 2015 年 Exploit Kits 规模与分布报告
6、代码签名证书大揭密：安全厂商曝光 Suckfly 团伙

安天 CERT 搜集整理（来源：paloaltonetworks、zdnet、mcafee、securityweek、trendmicro、symantec）

[20160318]

1、安天 AVL 联合猎豹安全首曝"多米诺"恶意应用市场 APP
2、研究人员发现已弃用 iOS App 数据库泄露 20 万用户隐私
3、百万部安卓手机易受 Stagefright 漏洞影响绕过安全防御
4、安全厂商借勒索软件 Radamant 后台漏洞 获取解密密钥
5、勒索软件 EDA2 新变种问世 已被安全研究人员轻松化解
6、奥运愿景行动针对为中东、亚太地区企业邮箱发动攻击

安天 CERT 搜集整理（来源：freebuf、softpedia、theregister、softpedia、securityaffairs、trendmicro）

[20160319]

1、安天 CERT 曝近日多起利用 PowerShell 脚本传播恶意代码事件
2、短信拦截马借视频播放器传播：三阶段安装逃避反病毒检测
3、研究人员发现利用僵尸网络 ZeroAccess 发动 DDoS 攻击新途径
4、Locky 勒索软件潮来袭 借垃圾邮件传播 短期内中招超过万人
5、勒索软件 TeslaCrypt 升级存储加密密钥方式 旧破解工具失效
6、Buhtrap 组织用钓鱼邮件攻击俄罗斯银行 半年盗取数亿卢布

安天 CERT 搜集整理（来源：antiy、softpedia、softpedia、360、yesky、theregister）

[20160320]

1、Anonymous 黑客组织网上泄露疑似特朗普手机及社保号码
2、安全厂商发现 Android 木马 Gmobi 感染 40 种固件及流行应用
3、SysMon 日志被找到 安全厂商给出孟加拉央行窃案更多细节
4、勒索软件新家族 Samas: 可内网传播主要感染中国印度欧美
5、勒索软件新变种 TeslaCrypt 4 出现 采用 RSA4096 高强度加密
6、安全厂商数据表明：下载者木马随勒索软件传播呈上升趋势

安天 CERT 搜集整理（来源：easyaq、softpedia、thedailystar、softpedia、securityaffairs、welivesecurity）

[20160321]

1、印度称巴基斯坦使用安卓应用 SmeshApp 监视其军事活动
2、研究者发现手机应用程序可利用麦克风秘密收集用户信息
3、瑞士人民党网站遭到黑客入侵 逾五万支持者个人数据曝光
4、瑞典主流报纸电子版网站因黑客 DDoS 攻击被迫关闭数小时
5、研究人员发现约一成工控设备 PLC 可远程恶意设置 CPU 模式
6、遭黑客网络攻击 比特币交易平台 BitQuick 宣布停用 2 至 4 周

安天 CERT 搜集整理（来源：softpedia、easyaq、securityaffairs、securityweek、plcscan、softpedia）

[20160322]

1、FBI 同意协助孟加拉国调查黑客巨额央行窃案
2、iOS 曝可解密短信照片 0Day 漏洞 FBI 垂涎欲滴

3、勒索软件新家族"Surprise"借 TeamViewer 传播
4、安全厂商预言 APT NG：未必高级，但却有效
5、安全厂商发现恶意代码 Dridex 采用新免杀机制
6、MITRE 推出新 CVE 编号方案 于昨日开始实施

安天 CERT 搜集整理（来源：securityweek、theregister、informationsecuritybuzz、co、fireeye、theregister）

[20160323]
1、孟加拉央行窃案后续：黑客曾窃取其接入 SWIFT 证书
2、iOS9.3 以下版本漏洞：iPhone 可被 PDF 格式文档感染
3、研究人员发现勒索软件 Locky 借 Nuclear Ek 感染和传播
4、研究人员发现勒索软件新家族 ItsMeFA 借 TOR 隐藏服务
5、Instagram 盗号木马再现：苹果商店谷歌市场均受影响
6、对网络威胁情报共享调查显示：仅 42%安全专家使用

安天 CERT 搜集整理（来源：wsj、grahamcluley、paloaltonetworks、cyphort、securelist、computerweekly）
[20160324]
1、Samba 严重漏洞 Badlock 影响多个系统 正在紧急修补
2、研究者发现中国广告平台 API 被滥用 可传播恶意代码
3、OSX 及 iOS 内核存安全漏洞 可内核权限执行任意代码
4、Adobe 再曝漏洞 攻击者可借不确定向量执行任意代码
5、安全厂商发现新 USB 窃密木马 具自保护躲避检测能力
6、Office2016 新安全特性 可通过设置组策略拦截宏病毒

安天 CERT 搜集整理（来源：securityweek、fireeye、blogspot、packetstormsecurity、welivesecurity、softpedia）
[20160325]
1、安全证书提供商 EC-COUNCIL 网站页面传播勒索软件
2、威胁情报组织发现勒索软件 Locky 随邮件大规模传播
3、苹果安全研究员推测:FBI 或用镜像存储破解罪犯手机
4、安全厂商发现使用首个使用双重数字签名的恶意代码
5、安全厂商发现恶意代码藏身于 PNG 图片 躲避杀软检测
6、勒索软件再出新招 借助恶意代码 SamSa 渗透内网传播

安天 CERT 搜集整理（来源：fox-it、cyveillance、arstechnica、softpedia、securelist、paloaltonetworks）
[20160326]
1、研究人员发现自保护 USB 木马或用于感染物理隔离主机
2、美国指控 7 名伊朗籍公民参与针对美国金融系统攻击行动
3、研究者曝光 OS X、iOS 严重漏洞 可用于突破最新 SIP 保护
4、勒索软件改变战术 新家族 Petya 加密整块磁盘 接管 MBR
5、增强产品易管理性和安全性 中国政府定制版 Win10 曝光

6、中国网络空间安全协会在京成立 发起成员单位 200 多家

安天 CERT 搜集整理（来源：arstechnica、securityweek、thehackernews、securityweek、pconline、xinhuanet）

[20160327]

1、勒索软件新家族 PowerWare 借 Word 宏和 PS 脚本感染
2、美国 Verizon 电信安全部门被黑 150 万客户信息泄露
3、日本一公司服务器发现 1800 万互联网用户账户密码
4、福克斯新闻及部分知名网站被攻击者投放恶意广告
5、欧盟反恐官员称：比利时核电厂面临网络攻击风险
6、为防社交网络诈骗 Facebook 加入仿冒身份提醒功能

安天 CERT 搜集整理（来源：softpedia、usatoday、securityweek、softpedia、securityweek、thehackernews）

[20160328]

1、匿名者黑客组织视频宣称将对 ISIS 展开网络攻击
2、黑客利用远程打印在美高校印发反犹太主义传单
3、苹果宣布计划将 iCloud 密钥管理责任完全转交用户
4、《汽车黑客手册》出版 将为汽车制造商敲响警钟
5、厂商确认：新浪账户体系高危漏洞 可改他人密码
6、Node.js 软件包管理器设计有缺欠 可传播恶意代码

安天 CERT 搜集整理（来源：chinabyte、databreaches、grahamcluley、digitaltrends、wooyun、softpedia）

[20160329]

1、恶意软件新骗术：利用真实 GPS 数据发送超速罚单诈骗邮件
2、威胁无处不在：加拿大公立大学图书馆惊现硬件键盘记录器
3、研究人员发现通话管理应用存在安全漏洞 波及百万安卓用户
4、匿名者黑客组织继续"金丝雀"行动 入侵加拿大矿业公司网站
5、安全厂商曝光 POS 机恶意代码定制工具"财宝猎人"最新变种
6、针对勒索软件肆虐现状 安全厂商发布安天智甲终端防御系统

安天 CERT 搜集整理（来源：theverge、softpedia、toutiao、fireeye、微信公众号）

[20160330]

1、StartSSL 用户邮件认证环节漏洞：可获取任意域名 SSL 证书
2、FBI 借助第三方技术获取圣贝纳迪诺枪击案凶手 iPhone 数据
3、安全厂商揭露勒索软件控制者利用 WMI 实现反取证新手段
4、攻击者利用 Angler EK 通过易趣旗下流行网站传播勒索软件
5、美国大型医护机构疑遭勒索软件 Samas 感染被迫关闭网络
6、安全厂商曝光针对台湾地区的木马新家族 Backdoor.Dripion

安天 CERT 搜集整理（来源：softpedia、aqniu、secureworks、malwarebytes、csoonline、symantec）

[20160331]

1、网易邮箱 52GB 数据被公开 涉及 163、126 邮箱用户
2、安天猎豹联合曝光手机扣费病毒 Client 感染超 7w 人
3、Web 勒索软件新家族 KimcilWare Magento 商店中招
4、vBulletin 德国服务器遭入侵 全部论坛用户密码重置
5、Angler EK 被用于攻击综合型社交网站 Live Journal
6、美国多个著名律师事务所被黑 内幕交易信息或被窃

安天 CERT 搜集整理（来源：mydrivers、avlyun、softpedia、theregister、wsj）

==========

微信公众号:Antiylab

网址：

- http://www.antiy.com （中文）
- http://www.antiy.net （英文）
- http://www.antiy.cn 安天企业安全公司
- http://www.avlsec.com 安天移动安全公司（AVL TEAM）