每日安全简讯

[20161201]
1、安天联合电信云堤分析 Mirai 传播新手段
2、远控木马 NetWire 回归，窃取支付卡数据
3、安全厂商称劫持无人机或成网络新威胁
4、火狐浏览器 0Day 漏洞被用于攻击 Tor 用户
5、Win10 系统更新时会关闭 BitLocker 功能
6、斯诺登最新泄露：AT&T 大厦或为 NSA 基地

【安天】搜集整理（来源：qq、threatpost、securityweek、securityweek、freebuf、freebuf）

[20161202]
1、勒索软件 Cerber 通过谷歌链接和 Tor2web 传播
2、安卓木马 PluginPhantom 利用插件框架逃避检测
3、Gooligan 恶意软件活动导致百万谷歌账号泄露
4、微软将为 Windows 10 加入反侦察工具 SAMRi10
5、微软修复被用于绕过 Chrome 沙箱机制内核漏洞
6、Sailfish 成俄罗斯"替代安卓"计划首选系统

【安天】搜集整理（来源：securityweek、paloaltonetworks、checkpoint、securityweek、threatpost、cnbeta）

[20161203]
1、安天移动安全发布企业移动威胁检查工具
2、SmsSecurity 变种可由 TeamViewer 远程访问
3、Shamoon 组织使用恶意代码擦除目标主机
4、僵尸程序 Proteus 具备挖矿和键盘记录功能
5、两巨头预测威胁新趋势：勒索软件成重点
6、俄称外国间谍将对其金融体系发动网络攻击

【安天】搜集整理（来源：avlsec、trendmicro、paloaltonetworks、securityweek、aqniu、securityweek）

[20161204]
1、加拿大 Carleton 大学感染比特币勒索软件
2、AirDroid 存在中间人攻击和信息拦截漏洞
3、委内瑞拉军方网站被黑，3 千用户信息泄露
4、俄罗斯央行遭到黑客入侵，20 亿卢布被盗
5、NPort 串行设备被发现远程代码执行等漏洞
6、研究者发现绕过苹果激活锁定机制 iOS 漏洞

【安天】搜集整理（来源：softpedia、softpedia、softpedia、sina、securityweek、securityweek）

[20161205]
1、恶意代码托管网站 Avalanche 被执法机构撤销
2、安全专家建议特朗普培训 10 万黑客保护美国
3、朝鲜 Red-Star 操作系统被发现远程攻击漏洞
4、Google 修复 Chrome 浏览器多个高危安全漏洞
5、分布式猜测攻击方法破解 VISA 卡只需六秒钟
6、售价 50 美元 USB Killer 设备开始大规模生产

【安天】搜集整理（来源：itp、easyaq、vice、threatpost、securityaffairs、arstechnica）
[20161206]
1、安全厂商发布勒索软件 Cerber5 新变种分析
2、安全厂商发布 Shamoon 2 恶意代码分析报告
3、研究人员发现比 Mirai 更危险的新僵尸网络
4、Titathink 修复 IoT 摄像机缓冲区溢出漏洞
5、Kapustkiy 利用 SQLi 入侵厄瓜多尔国民议会
6、奥巴马总统委员会发布网络安全建议报告

【安天】搜集整理（来源：fortinet、codeandsec、securityaffairs、theregister、securityaffairs、easyaq）
[20161207]
1、安天联合猎豹分析 Camouflage 木马攻击手段
2、研究人员警告植入式医疗设备可被黑客攻击
3、索尼 SNC 系列安防 IP 摄像机被发现后门帐户
4、研究人员发现 Uber 应用在后台跟踪用户位置
5、视频分享网站 Dailymotion 数百万账号被盗
6、日本化妆品牌资生堂确认 42 万用户数据泄露

【安天】搜集整理（来源：avlsec、softpedia、securityweek、securityaffairs、csoonline、freebuf）
[20161208]
1、勒索软件 Locky 新变种借助 Excel 文档传播
2、勒索软件感染医疗系统影响 2800 患者预约
3、安全厂商发现广告横幅用于隐藏恶意代码
4、苏格兰足球协会被黑向球迷发送恶意软件
5、研究者揭示 Linux 内核提权漏洞技术细节
6、新的脏牛漏洞可将恶意代码直接写入进程

【安天】搜集整理（来源：securityweek、softpedia、arstechnica、softpedia、360、trendmicro）

[20161209]
1、统计表明美国感染勒索软件全球居首
2、勒索软件 Petya 新变种更名"黄金眼"
3、无文件实体窃密木马 August 近期活跃
4、开源 Web 邮件 RoundCube 发现严重漏洞
5、漏洞预警：ImageMagick 远程代码执行
6、阿根廷工业部网站被黑导致数据泄露

【安天】搜集整理（来源：darkreading、securityweek、proofpoint、securityweek、darkzome、softpedia）
[20161210]
1、德国重工业巨头发现东南亚黑客窃密迹象
2、黑客控制以色列新闻频道播放穆斯林宣礼
3、安全厂商称外来的 PS 脚本是企业主要威胁
4、斯诺登文档显示 NSA 监视飞机上的 GSM 服务
5、研究者发现雅虎邮件服务任意读邮件漏洞
6、印度 UAN 网站发现严重漏洞，影响百万用户

【安天】搜集整理（来源：securityweek、securityaffairs、symantec、securityaffairs、securityaffairs、securityaffairs）

[20161211]
1、安全厂商发布 2016 年勒索软件变革情况
2、安全团队发布敲诈者木马免疫技巧分析
3、研究人员发布 Floki Bot 僵尸网络分析
4、垃圾广告借 Facebook 群组传播恶意代码
5、安全厂商发布 2017 年网络安全八个预测
6、研究表明互联网用户常用密码发生改变

【安天】搜集整理（来源：securelist、freebuf、talosintel、neowin、trendmicro、easyaq）
[20161212]
1、勒索软件爆米花鼓励受害人协助传播
2、Locky 和 Cerber 已成主要勒索软件家族
3、安全厂商剖析移动平台勒索软件机理
4、勒索软件即服务(RaaS)呈爆炸式发展
5、研究者发现恶意脚本检测沙箱新手段
6、麦当劳得来速点餐系统遭到黑客入侵

【安天】搜集整理（来源：bleepingcomputer、digitaltrends、trendmicro、aqniu、sans、easyaq）
[20161213]
1、安天揭露一例跨期两年电信诈骗进化史
2、安全团队分析恶意代码 Depriz 工作机理

3、研究人员发现一例多合一木马攻击场景
4、黑客可利用新工具窃取无钥匙启动汽车
5、普华永道 SAP 安全工具被发现致命缺陷
6、NSA 前局长称负面形象导致 NSA 人才流失

【安天】搜集整理（来源：avlsec、microsoft、badcyber、cnbeta、securityaffairs、solidot）

[20161214]
1、JS 脚本后门 Ostap 用于传播银行木马
2、安全厂商称 Zcash 将使挖矿程序回归
3、McAfee 企业版反病毒被发现 RCE 漏洞
4、安全专家警告停止使用 Netgear 路由
5、国家电网 App 造成海量用户数据泄露
6、法国成立网络战部队以应对外国黑客

【安天】搜集整理（来源：securityweek、securelist、zdnet、solidot、cnbeta、securityweek）

[20161215]
1、安卓木马 Loki 变种具 Root 设备能力
2、多款低端手机固件被植入恶意代码
3、IoT 僵尸网络 Mirai 变种加入 DGA 特性
4、KFC 上校俱乐部部分会员帐户被入侵
5、俄罗斯领事馆网站被黑影响 3 万用户
6、安全厂商发布前三季度网络安全报告

【安天】搜集整理（来源：bleepingcomputer、drweb、securityweek、cnbeta、softpedia、mcafee）

[20161216]
1、调查显示勒索软件受害企业七成付钱
2、影子经济人向买家直销 NSA 泄露工具
3、研究人员发现 MacOS 版 Skype 内置后门
4、Adobe 修复 Flash 可用于监听用户漏洞
5、雅虎官方证实 10 亿用户帐户信息失窃
6、Joomla CMS 发现可致网站被接管漏洞

【安天】搜集整理（来源：solidot、vice、freebuf、bleepingcomputer、solidot、bleepingcomputer）

[20161217]
1、勒索软件 BandarChor 变种以恶意广告传播
2、360 发布 2016 敲诈者病毒威胁形势分析报告
3、NoMoreRansom 计划为受害者免费解密文件

4、Ubuntu 又发现音频文件触发代码执行漏洞
5、Ubuntu 崩溃记录器存在远程执行代码漏洞
6、苹果磁盘加密程序密码可被廉价硬件获取

【安天】搜集整理（来源：bleepingcomputer、360、zdnet、arstechnica、softpedia、slashdot）

[20161218]
1、安卓银行木马 Tordow 具备 root 设备能力
2、BlackEnergy 黑客组织攻击乌克兰银行
3、研究者发现 Facebook 聊天记录窃取漏洞
4、Nagios 监控程序核心代码被发现 RCE 漏洞
5、分析表明 WordPress 官方插件两成有缺陷
6、Cryptolulz 欲向政府网站发动 DDoS 攻击

【安天】搜集整理（来源：softpedia、easyaq、360、threatpost、securityaffairs、securityaffairs）

[20161219]
1、Odinaff 木马是土耳其金融攻击幕后黑手
2、Trickbot 木马主要针对东南亚部分国家
3、大规模僵尸网络 Mirai 控制服务器藏身 Tor
4、雅虎 10 亿泄露数据已在暗网找到购买者
5、体育门户网站 Bleacher Report 数据泄露
6、英国政府发布国家安全战略年度报告

【安天】搜集整理（来源：securityaffairs、securityweek、slashdot、securityaffairs、bleepingcomputer、freebuf）

[20161220]
1、DNSChanger 被用于入侵家用路由
2、调查发现多数人从不更新 IoT 设备
3、FBI 逮捕 DDoS 僵尸网络服务出租商
4、DDoS 攻击或成为全球战争新形式
5、领英学习平台被黑影响 5.5 万密码
6、印度理工学院数据库 1.2 万用户泄露

【安天】搜集整理（来源：securityaffairs、solidot、bleepingcomputer、easyaq、securityweek、securityaffairs）

[20161221]

1、乌克兰再次因黑客攻击电力中断
2、影子经纪人泄露代码来自 NSA 内部
3、多家工厂遭鱼叉式钓鱼邮件攻击
4、安卓银行木马加入勒索软件特性
5、仿冒超级玛丽近七成有恶意行为
6、娱乐系统安全漏洞可使飞机受控

【安天】搜集整理（来源：softpedia、threatpost、kaspersky、bleepingcomputer、trendmicro、softpedia）

[20161222]
1、勒索软件 CryptXXX 已被破解
2、安全厂商发现新型 ATM 恶意代码
3、恶意代码 Ticno 伪装系统对话框
4、恶意代码 Rakos 可感染 IoT 设备
5、OpenSSH 7.4 修复多个安全漏洞
6、公检法出台意见打击电信诈骗

【安天】搜集整理（来源：bleepingcomputer、trendmicro、bleepingcomputer、bleepingcomputer、phperz、xinhuanet）

[20161223]
1、俄黑客组织利用安卓木马入侵乌克兰炮兵部队
2、黑客组织 OurMine 接管 Netfix 官方 Twitter 账户
3、安全厂商警告新型垃圾邮件活动 hailstorm 威胁
4、西门子 Desigo PX 和 SIMATIC 产品发现安全漏洞
5、欧盟报告声称植入加密后门或使情况更加糟糕
6、Facebook 推出无需短信二步身份认证功能组件

【安天】搜集整理（来源：cnbeta、softpedia、securityweek、securityweek、techdirt、grahamcluley）

[20161224]
1、立陶宛指控俄罗斯向其政府电脑植入间谍软件
2、研究人员警告"非恶意软件"威胁呈上升趋势
3、安全团队深度分析"净广大师"流量劫持手段
4、研究人员发现 NETGEAR WNR2000 路由器 RCE 漏洞
5、黑客 Kapustkiy 入侵哥斯达黎加驻华大使馆网站
6、OurMine 组织接管漫威、NFL 等更多 Twitter 账户

【安天】搜集整理（来源：cnbeta、securityweek、freebuf、securityaffairs、easyaq、softpedia）

[20161225]

1、攻击者在钓鱼活动中使用类似恶意软件分发策略
2、研究人员警告假日主题垃圾邮件活动呈上升趋势
3、黑客组织欲在圣诞节向 PSN XBOX 服务器发动 DDoS
4、瑞士破解 DGA 算法，关闭僵尸网络 Tofsee 五百域名
5、Signal 利用域名欺骗技术规避政府审查和限制措施
6、华盛顿健康计划组织被黑，成员个人信息遭泄露

【安天】搜集整理（来源：securityweek、securityweek、softpedia、securityweek、securityaffairs、softpedia）

[20161226]
1、勒索软件 Cerber 变种调整文件加密策略
2、美政府要求入境游客提供社交媒体账号
3、思科警告用户 CCO 系统存在严重提权漏洞
4、黑客 Kapustkiy 入侵俄罗斯驻美签证中心
5、黑客入侵香港英文报纸网站并泄露数据
6、工信部新规：手机预装软件必须可卸载

【安天】搜集整理（来源：virusguides、solidot、securityweek、securityaffairs、securityaffairs、163）

[20161227]
1、勒索软件 DeriaLock 既能锁屏又加密
2、勒索软件 Koolova 强迫受害者读文章
3、奥巴马敦促美国网络司令部脱离 NSA
4、研究人员称智能玩具可泄露儿童信息
5、谷歌内研可取代短信的二步认证设备
6、媒体总结 2016 年国内信息安全大事件

【安天】搜集整理（来源：bleepingcomputer、bleepingcomputer、securityaffairs、cbslocal、arstechnica、easyaq）

[20161228]
1、国家网信办发布《国家网络空间安全战略》
2、PHPMailer 发现 RCE 漏洞，影响众多开源项目
3、部分路由器厂商对研究者提交漏洞重视不足
4、黑客 Kapustkiy 入侵土耳其商会窃取个人信息
5、泰国警方逮捕 9 名参与攻击政府网站的嫌疑人
6、黑客盗用索尼音乐推特传播布兰妮死讯谣言

【安天】搜集整理（来源：chinanews、freebuf、bleepingcomputer、softpedia、hackread、cnbeta）

[20161229]
1、国务院印发"十三五"国家信息化规划
2、安天移动安全推出一站式情报管理服务

3、研究发现 2016 年无文件实体攻击模式激增
4、安全厂商发现感染 WiFi 路由安卓木马变种
5、WordPress 插件被发现任意文件删除漏洞
6、360 团队发布移动平台流量黑产调研报告

【安天】搜集整理（来源：xinhuanet、avlsec、darkreading、threatpost、packetstormsecurity、360）

[20161230]
1、KillDisk 变种或将勒索软件引入工控领域
2、安全厂商发现黑产的受害主机一站式商店
3、FDA 为联网医疗设备制定网络安全防护指南
4、ZyXEL 定制路由器被发现远程代码执行漏洞
5、安全团队揭示声波入侵物理隔离系统方法
6、IHG 假日酒店被 PoS 恶意代码窃信用卡数据

【安天】搜集整理（来源：securityweek、securityaffairs、cnbeta、securityaffairs、freebuf、softpedia）

[20161231]
1、勒索软件攻击智能电视，厂商协助用户修复
2、欧洲安全与合作组织上月遭受严重网络攻击
3、美国驱俄外交官，FBI 公布黑客攻击调查报告
4、研究人员发现监控工具 MONyog 存在提权漏洞
5、Topps 网站遭到黑客入侵，用户个人信息泄露
6、特殊短信可使主流 iOS 版本信息应用无法工作

【安天】搜集整理（来源：cnbeta、securityaffairs、solidot、securityaffairs、securityweek、cnbeta）

==========

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）