[20161101]
1、Mirai 源码存在缓冲区溢出，可阻止部分 DDoS 攻击
2、研究者发现 IoT 设备 DDoS 僵尸网络恶意代码 Aidra
3、W3C Web 蓝牙 API 被发现漏洞，可影响物联网设备
4、谷歌研究人员发现 OS X 和 iOS 系统的内核提权漏洞
5、Joomla 已修复的严重漏洞被黑客用于入侵众多网站
6、研究者发现英国苹果用户面临新一轮短信钓鱼活动

【安天】搜集整理（来源：itsecuritynews、malwaremustdie、softpedia、feng、securityweek、ibtimes）

[20161102]
1、中国高校与企业曾为 NSA 主要攻击目标
2、研究人员调查中国最大 Webshell 后门箱子
3、恶意代码 Nymaim 以 PS 脚本下载攻击载荷
4、CNVD 发布 Memcached 存在高危漏洞预警
5、微软内核整数溢出漏洞可导致本地提权
6、安全厂商发布 Q3 期间 DDoS 攻击统计报告

【安天】搜集整理（来源：easyaq、freebuf、securityweek、CNVD、fortinet、securelist）

[20161103]
1、微软称谷歌发现漏洞被俄方 APT 组织利用
2、微软 IE 0day 曾被用于 AdGholas 攻击活动
3、谷歌 AdWords 可向 Mac 用户传播恶意代码
4、安全团队发布九头虫病毒技术分析报告
5、SAP 已修复漏洞仍会影响全球 941 个系统
6、研究人员发现施耐德工控套件严重漏洞

【安天】搜集整理（来源：threatpost、trendmicro、theregister、freebuf、securityweek、securityaffairs）

[20161104]
1、安全厂商发布 Linux 恶意代码 Moose 分析报告
2、针对欧美银行的安卓木马伪装 Flash 应用传播
3、Belkin WeMo 物联网设备被发现代码执行漏洞
4、MySQL 等多数据库被发现代码执行高危漏洞
5、Wix 云主机平台存在 XSS 漏洞，影响百万网站
6、安全团队发布瑞典 OMX 30 企业信息泄露调查

【安天】搜集整理（来源：welivesecurity、ibtimes、securityweek、easyaq、threatpost、anomali）

[20161105]
1、安天发布方程式组织多平台样本深度分析报告
2、安天 AVL 团队发布勒索拦截马"Trick"分析报告
3、英国 NHS 网络因恶意代码感染取消手术和预约
4、GitLab 未授权访问漏洞可导致远程命令执行
5、Mirai 僵尸网络欲搞垮利比亚国家网络基础设施
6、以色列研究人员展示利用智能灯泡传播蠕虫

【安天】搜集整理（来源：antiy、leiphone、securityaffairs、freebuf、securityweek、timesofisrael）

[20161106]
1、研究人员发现商用安卓间谍软件 Exaspy
2、日内瓦伊朗核问题谈判地发现间谍软件
3、Sophos 安全产品发现远程代码执行漏洞
4、OWA 设计缺陷可导致双因子验证被绕过
5、加拿大长达十年"ODAC"监控计划曝光
6、利用 DRAM 攻击可窃取断网虚拟机数据

【安天】搜集整理（来源：threatpost、securityaffairs、packetstormsecurity、threatpost、easyaq、securityweek）

[20161107]
1、美国总统大选在即，政府称其网军严阵以待
2、安全研究员发现 Gmail 严重漏洞，可轻易破解
3、新型 DDos 攻击：利用 LDAP 服务器放大攻击
4、MalwareTech 绘制 Mirai 等僵尸网络地图
5、银行行长泄露密码导致 257 万个人信息被盗
6、统计表明 Chrome 访问 https 加密网页占半数

【安天】搜集整理（来源：securityaffairs、cnbeta、freebuf、malwarebenchmark、sohu、threatpost）

[20161108]
1、网络安全法获通过，明年六月起施行
2、安全厂商分析仿冒流行应用移动木马
3、新型邮件钓鱼活动针对 LinkedIn 用户
4、俄外交部要求美方澄清入侵俄方消息
5、印度驻六国大使馆员工数据被泄露

6、特易购银行 2 万帐户被黑客窃取资金

【安天】搜集整理（来源：people、securelist、securityaffairs、securityweek、securityaffairs、irishexaminer）

[20161109]
1、猎豹移动揭露席卷全球的"霸屏"手机勒索软件
2、安全厂商警告勒索软件 Cerber 开始加密数据库
3、Bopup 商用通讯服务器存在远程代码执行漏洞
4、台湾 Moxa 科技公司工业以太网产品发现漏洞
5、思科招聘网站移动版漏洞导致求职者信息泄露
6、FBI 越权使用恶意代码调查暗网 TorMail 使用者

【安天】搜集整理（来源：freebuf、itproportal、securityweek、securityweek、securityaffairs、rt）

[20161110]
1、研究者分析针对白俄罗斯军事部门 APT 样本
2、安卓银行木马 Svpeng 可通过 Chrome bug 传播
3、研究人员警告：D-Link 路由器存在 RCE 漏洞
4、研究人员发现 OAuth2.0 漏洞可致账户被接管
5、黑客可以滥用 LTE 协议关闭手机网络连接
6、德总理称俄方或通过网络攻击影响德国大选

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

[20161111]
1、研究人员发现首个利用电报协议的恶意软件
2、恶意软件 Mirai 被曝曾攻击美国候选人网站
3、雅虎对其受大规模攻击事件透露更多细节
4、研究者用无人机远程控制飞利浦智能灯泡
5、安全厂商发布 Q3 垃圾邮件和网络钓鱼报告
6、研究人员发现可通过 iOS WebView 拨打电话

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

[20161112]
1、谷歌和亚马逊云服务平台发现隐藏恶意软件
2、Tesco 银行仅为恶意软件 Retefe 攻击名单之一

3、APT29 在特朗普当选后发动鱼叉式钓鱼攻击
4、美国麦迪逊县计算机系统遭受勒索软件攻击
5、低带宽 BlackNurse DDoS 攻击可致防火墙中断
6、加拿大赌场系统遭黑客入侵，顾客资料被盗

【安天】搜集整理（来源：easyaq、welivesecurity、techtimes、securityweek、securityweek、securityweek）

[20161113]
1、知名博客 MMD 关闭，抗议 NSA 实施网络攻击
2、恶意软件变种和垃圾邮件在 10 月增长迅速
3、研究者称 IoT 恶意软件即将扩大感染范围
4、俄罗斯五家主流大型银行受僵尸网络攻击
5、美国国标研究院发布小微企业网络安全指南
6、研究者称超声波将成黑客窃取隐私新途径

【安天】搜集整理（来源：securityaffairs、scmagazine、securityweek、easyaq、nist、indiatimes）

[20161114]
1、安全专家担心俄黑客影响英国脱欧投票
2、美指控 Florida 黑客与攻击摩根大通有关
3、俄罗斯调查 Windows 10 防毒软件垄断问题
4、Facebook 错误使全部用户显示"纪念账户"
5、特朗普当选导致加密邮件服务申请翻倍
6、D-Link 被发现可获 root 权限的 HNAP 漏洞

【安天】搜集整理（来源：mirror、reuters、arstechnica、securityaffairs、easyaq、computerworld）

[20161115]
1、勒索软件 Locky 借 OPM 泄露事件邮件传播
2、发布 Mirai 源代码的黑客论坛关闭相应版块
3、VMware 修复拖拽触发任意代码执行漏洞
4、成人交友网站被黑，4.12 亿用户数据泄露
5、德国设立网络和信息空间参谋部
6、研究人员发现通过 WiFi 信号监听密码方法

【安天】搜集整理（来源：zdnet、easyaq、securityweek、securityaffairs、easyaq、theregister）

[20161116]

1、追日团队曝光蔓灵花 APT 攻击行动
2、Windows 10 加入勒索软件防护机制
3、勒索软件 CrySis 被破解公开主密钥
4、黑客 Kapustkiy 复出，瞄准使馆高校
5、苹果应用 SHAZAM 后台监听麦克风
6、Linux LUKS 漏洞可被本地远程攻击

【安天】搜集整理（来源：360、windows、threatpost、securityaffairs、com、zdnet）

[20161117]

1、第三届世界互联网大会在乌镇召开
2、PoisonTap 技术可向锁定 PC 安装后门
3、Lynxspring 公司 SCADA 产品存严重缺陷
4、赛门铁克安全产品修复 DLL 劫持漏洞
5、17 岁英国少年承认参与 TalkTalk 攻击
6、Carbanak 犯罪团伙瞄准酒店餐饮行业

【安天】搜集整理（来源：chinadaily、wired、securityweek、securityweek、welivesecurity、threatpost）

[20161118]
1、研究者发现勒索软件新变种 CryptoLuck
2、危险 Android 木马指向 Hacking Team 组织
3、CNVD 发布 Nginx 远程本地提权漏洞公告
4、iOS 漏洞允许未授权问 iPhone 照片和消息
5、美军方欲使用"网络迷雾"存储重要数据
6、安全厂商发布 2017 年安全威胁预测报告

【安天】搜集整理（来源：securityweek、helpnetsecurity、cnvd、cnbeta、easyaq、securelist）

[20161119]
1、美国国土安全部发布保障物联网安全战略原则
2、安全团队发布 DDoS 攻击地下产业链调研报告
3、调查发现 iCloud 启用后手机将会上传通话数据
4、招聘网站 GeekedIn 泄漏 800 万 GitHub 用户信息
5、英国运营商 Three 数据泄漏影响数百万个人数据
6、文件共享站 Mega.nz 被黑，源码及机密文件泄漏

【安天】搜集整理（来源：easyaq、ArkTeam、techdirt、oschina、securityaffairs、360）

[20161120]
1、安全团队发布勒索软件 HadesLocker 分析报告
2、勒索软件 Ransoc 借社交网络威胁受害人声誉
3、研究者发布 Geinimi 木马家族相似性分析报告
4、调查表明 300 万安卓手机 OTA 升级机制有隐患
5、Moxa 和 Vanderbilt 监控设备发现远程接管漏洞
6、意大利政府网站被黑，4.5 万用户信息泄露

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

[20161121]
1、安全团队发布魔波广告恶意病毒分析报告
2、研究人员提供 Crypto88 勒索软件处理方法
3、俄罗斯起重机制造商发现窃密木马 Crane
4、安全团队公开 Edge 浏览器 RCE 漏洞技术细节
5、Drupal 修复 CMS 引擎可引起社工和 DoS 漏洞
6、PlayStation 和 Xbox 等多个 Twitter 账号被黑

【安天】搜集整理（来源：freebuf、virusguides、securityweek、tencent、threatpost、easyaq）

[20161122]
1、勒索软件 Locky 以 SVG 图像在 Facebook 传播
2、安卓银行木马利用社会工程绕过 Doze 机制
3、安全团队发布利用漏洞传播的萝莉蠕虫分析
4、意大利研究人员发布自动化网络钓鱼工具
5、Ubuntu 存在声音文件触发的代码执行漏洞
6、谷歌研究员发现 PAN-OS 任意代码执行漏洞

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

[20161123]
1、安全厂商发现 Gatak 木马将攻击目标瞄准医疗机构
2、Cobalt 组织利用恶意代码远程攻击欧洲多国 ATM
3、美国国防部漏洞披露政策：黑客可访问政府系统
4、CNVD 通报广升 FOTA 服务存在权限提升漏洞

5、研究人员发现 HDF5 库存在任意代码执行漏洞
6、人权基金会网站被黑，超过 2 万账户信息泄露

【安天】搜集整理（来源：symantec、softpedia、easyaq、cnvd、securityweek、softpedia）

[20161124]
1、安全厂商勒索软件解密工具加入 Crysis 支持
2、勒索软件 Locky 以假冒 ISP 投诉钓鱼邮件传播
3、安卓银行木马具备阻止反病毒程序启动功能
4、OneDrive 商用账户被发现用于传播恶意软件
5、攻击者试图利用 ask.com 工具栏传播恶意软件
6、美国政府修订规则，允许入侵全球嫌疑用户

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

[20161125]
1、滥用 Telegram API 勒索软件 TeleCrypt 被破解
2、麦迪逊广场花园公司支付数据被恶意软件窃取
3、InPage 软件 0day 漏洞被用于攻击亚洲金融机构
4、FBI 史上最大规模网络行动，入侵 120 个国家
5、美国海军遭黑客入侵，13.4 万士兵信息泄露
6、访问恶意视频链接可导致任何 iOS 设备死机

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

[20161126]
1、安卓银行木马 Gugi 以社工技巧获取权限
2、移动应用漏洞可供黑客解锁和盗取汽车
3、两黑客宣称出租 40 万节点 Mirai 僵尸网络
4、研究者对俄罗斯银行 DDoS 事件展开分析
5、黑客对欧盟委员会发动大规模网络攻击
6、以色列公司演示在数秒内窃取手机数据

【安天】搜集整理（来源：comodo、softpedia、ibtimes、securelist、express、solidot）

[20161127]
1、勒索软件 Cerber5.0 变种使用新 IP 地址范围
2、360 安全团队发布勒索软件 XTBL 分析报告

3、黑客利用 MailChimp 邮件服务传播恶意软件
4、攻击者滥用 YouTube 推广包含后门钓鱼模板
5、Fancy Bears 组织入侵反兴奋剂官员机密邮件
6、黑客组织 PGA 攻破印度多个高级委员会网站

【安天】搜集整理（来源：securityweek、freebuf、vice、securityweek、theguardian、easyaq）

[20161128]
1、研究人员剖析 10 种常见勒索软件加密算法
2、爱尔兰数万宽带猫存在可被远程控制漏洞
3、黑色星期五邮件被用于向亚马逊客户钓鱼
4、Akamai 发布 2016 年第三季度攻击分析报告
5、UberCENTRAL 工具漏洞可致用户数据泄露
6、黑客组织 Hazaristan 攻击阿富汗国家安委会

【安天】搜集整理（来源：freebuf、freebuf、reporter、easyaq、securityweek、sputniknews）

[20161129]
1、旧金山市政铁路系统被入侵、数据遭加密勒索
2、恶意代码 Speake(a)r 可利用耳机实现窃听功能
3、cURL 工具及库中被发现远程代码执行严重漏洞
4、微软 Azure 云平台存在漏洞，可破坏 RHEL 实例
5、黑客攻击导致德国电信近百万家用路由器中断
6、安全厂商发现 1/4WiFi 热点缺乏密码保护和加密

【安天】搜集整理（来源：securityaffairs、freebuf、securityweek、theregister、securityweek、silicon）

[20161130]
1、研究人员 2017 年预测：勒索软件模式转向新平台
2、勒索软件 Kangaroo 由开发者经远程桌面手动安装
3、PayPal 修复导致应用程序 OAuth 令牌被劫持漏洞
4、德国电信攻击事件元凶为新发现路由器高危漏洞
5、列支敦士登银行遭入侵，攻击者向储户勒索赎金
6、xHamster 色情网站数据泄露，数十万账号被售卖

【安天】搜集整理（来源：paloaltonetworks、virusguides、threatpost、arstechnica、theregister、vice）

==========

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）