[20161001]
1、勒索软件 Bitter 服务器关闭，主密钥被删
2、巴西黑客组织开发勒索软件变种在当地传播
3、僵尸网络 Tofsee 活跃，借垃圾邮件活动传播
4、研究人员在 D-Link 移动热点发现漏洞及后门
5、印度海关部门因黑客入侵造成 5 亿卢比损失
6、MH17 调查记者收到俄方威胁组织钓鱼邮件

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

[20161002]
1、恶意脚本新手段：借用户交互对抗自动分析
2、美国楼宇自控产品存漏洞，易受远程攻击
3、思科安全设备内部测试接口引入关键漏洞
4、美国食品药物管理局系统面临网络攻击风险
5、Office 365 管理员账户被黑客在暗网出售
6、苹果向美国执法部门共享 iMessage 元数据

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

[20161003]
1、Android 恶意软件 DressCode 可渗透企业内网
2、海马助手为牟取广告利益增加更多恶意行为
3、Cobalt Strike team 服务被曝远程代码执行漏洞
4、研究人员发布利比亚天蝎网络间谍活动报告
5、安全团队解析美国政府主导"爱因斯坦"计划
6、莫斯科决定以本国软件替换掉全部微软软件

【安天 CERT】搜集整理（来源：trendmicro、trendmicro、360、freebuf、freebuf、malwarebenchmark）

[20161004]
1、僵尸网络 Mirai 程序代码被作者公开
2、攻击者使用被黑 Steam 帐户传播木马
3、Rotten Tomato APT 组织仍在行动
4、韩国军方网络指挥部被植入恶意代码
5、OpenJPEG 被发现任意代码执行漏洞
6、利用 DNS 流量数据可以辨识 Tor 用户

【安天 CERT】搜集整理（来源：krebsonsecurity、securityaffairs、freebuf、yonhapnews、securityaffairs、securityweek）

[20161005]
1、安全厂商发布勒索软件 Marsjoke 解密工具
2、安全厂商发布 Mirai 僵尸网络调查分析报告
3、研究人员发现针对巴西实时网络钓鱼攻击
4、EMC 发布 VMAX 命令执行等关键漏洞补丁
5、黑客论坛 w0rm.ws 被黑，EK 和数据库泄漏
6、影子经纪人抱怨 NSA 泄露武器库乏人问津

【安天 CERT】搜集整理（来源：softpedia、malwaretech、magazine、securityweek、hackread、sophos）

[20161006]
1、BadKernel 漏洞影响 1/16 安卓设备，涵盖主流品牌
2、研究者发现胰岛素泵存在远程恶意指令控制漏洞
3、苹果 iMessage 新版存泄露 IP 地址和设备信息漏洞
4、研究人员发现三星移动安全方案 KNOX 绕过方法
5、Dropbox 6800 万账号信息被安全研究人员泄漏
6、Yahoo 被指允许美国政府暗中扫描用户邮件

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

[20161007]
1、勒索软件 Cerber 变种关闭数据库进程
2、FastPos 木马借进程通信机制窃取数据
3、伊朗 OilRig 组织升级工具扩大攻击范围
4、NSA 承包商雇员涉嫌窃取国家机密被捕
5、谷歌修复 Android 可被远程利用 DoS 漏洞
6、电信诈骗新伎俩：伪造二维码交通罚单

【安天 CERT】搜集整理（来源：securityaffairs、softpedia、paloaltonetworks、huanqiu、securityweek、sina）

[20161008]
1、勒索软件 WildFire 出现变种 Hades Locker
2、Mac 间谍软件可借助合法视频程序后台监控
3、安全厂商发布世界僵尸网络分布城市调查表

4、X.Org 开发者修复本地远程 DoS 和提权等漏洞
5、研究者称苹果削弱 Safari 隐私浏览模式安全性
6、Yahoo 或因数据泄露事件损失收购价 10 亿美元

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

[20161009]
1、安全厂商发布勒索软件 Cerber3 分析报告
2、WMI 查询被滥用于检测环境和沙箱逃逸
3、调查表明 RIG 仍为最流行漏洞利用工具包
4、VMware 修复 Horizon View 目录遍历漏洞
5、GE 监控系统发现远程非法访问提权漏洞
6、美国指控俄政府为网络袭击"幕后黑手"

【安天 CERT】搜集整理（来源：freebuf、fireeye、symantec、securityweek、securityweek、secwk）

[20161010]
1、勒索软件又添新家族：Mamba 加密硬盘 MBR
2、安全团队发布物联网恶意代码 mirai 分析报告
3、DDoS 僵尸网络利用国产摄像头默认密码传播
4、音乐服务平台 Spotify 向用户投放恶意广告
5、思科修复 Nexus7000 系列交换机 RCE 关键漏洞
6、美政府让 Yahoo 安装的扫描程序疑为黑客工具

【安天 CERT】搜集整理（来源：anonhq、qq、secjia、ubergizmo、securityaffairs、techtimes）

[20161011]
1、安全厂商曝光针对意大利等国 APT 组织 StrongPity
2、研究者发现对抗关闭进程行为的新型 JS 恶意软件
3、攻击者利用 Windows 疑难解答平台安装恶意软件
4、攻击者利用"飓风马修"主题邮件进行攻击活动
5、Facebook 大规模垃圾邮件活动瞄准法国用户
6、蜥蜴小队和 PoodleCorp 成员因涉嫌 DDoS 被逮捕

【安天 CERT】搜集整理（来源：securelist、easyaq、softpedia、securityaffairs、softpedia、softpedia）

[20161012]

1、勒索软件 DXXD 以微软法律声明界面显示勒索信息
2、研究人员发现微软 JEA 技术被攻击者用于提升权限
3、国际原子能机构确认德国核电站遭破坏性网络攻击
4、微软故障排除平台被攻击者用于传播后门 LatentBot
5、英国内阁会议禁止佩戴苹果手表以防被黑客窃听
6、土耳其屏蔽 Dropbox 等网盘和 GitHub 以防邮件泄露

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

[20161013]
1、攻击者仿冒安全厂商网页传播勒索软件 Petya
2、证据表明银行木马 Odinaff 与 Carbanak 组织有关
3、OffensiveWare 黑客工具在地下黑客论坛出售
4、泄漏数据披露网站 Leakedsource 发生数据泄漏
5、数据存储服务提供商 5800 万用户记录被窃
6、攻击者利用在线游戏币融资进行网络犯罪活动

【安天 CERT】搜集整理（来源：securelist、softpedia、softpedia、360、softpedia、trendmicro）

[20161014]
1、安天 AVL 团队发布手机蠕虫 Curiosity 报告
2、勒索软件 Cerber 再度升级，4.0 版在线销售
3、第一个用 Go 语言编写的勒索软件已被解密
4、零售商店 Vera Bradley 遭 PoS 恶意软件感染
5、微软 0day 漏洞被攻击者用于广告攻击活动
6、恶意软件 Mirai 几乎感染了全球物联网设备

【安天 CERT】搜集整理（来源：avlsec、softpedia、softpedia、softpedia、securityweek、easyaq）

[20161015]
1、安全厂商发现 Python 编写的勒索软件 CryPy
2、新 Linux 木马 NyaDrop 出现，威胁物联网领域
3、包含富士康固件的安卓设备可能存在秘密后门
4、广告软件 Youndoo 使用隐藏任务计划卷土重来
5、BIND 存在漏洞可被攻击者利用发起 DoS 攻击
6、Evony 游戏公司被黑，3300 万玩家记录泄露

【安天 CERT】搜集整理（来源：securelist、softpedia、softpedia、softpedia、trendmicro、securityaffairs）

[20161016]

1、研究人员发布勒索软件 Locky 配置提取工具
2、Ascesso 木马被用于学生贷款主题诈骗邮件
3、研究人员发现 Zeus 木马通过 MSG 附件传播
4、安卓应用泄露微软 Exchange 服务用户凭据
5、安卓木马要求用户提交手持身份证自拍照
6、Mirai IoT DDoS 木马已瞄准蜂窝网络设备

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

[20161017]

1、猎豹移动发布 GhostPush 木马家族分析报告
2、美中情局将对俄发动"前所未有"网络攻击
3、安全专家称亚太地区在线金融威胁增加
4、思科会议服务器漏洞允许假冒合法用户
5、澳大利亚活动策划公司 Pont3 遭数据泄露
6、黑客仿冒 Gmail 安全更新入侵 DNC 邮件系统

【安天】搜集整理（来源：cmcm、hackernews、bizhub、securityaffairs、softpedia、buzzfeed）

[20161018]
1、勒索软件 Exotic 对桌面文件二次加密
2、银行木马 TrickBot 与旧版本 Dyre 有关
3、安全厂商发布第三季度威胁态势报告
4、百度网盘遭到撞库攻击影响 50 万账户
5、国外黑客发现国产摄像机存在 XXE 漏洞
6、影子经济人放弃 NSA 武器库拍卖模式

【安天】搜集整理（来源：bleepingcomputer、softpedia、proofpoint、sina、freebuf、softpedia）

[20161019]
1、安全厂商发布勒索软件 Cerber4 分析报告
2、恶意代码利用隐写方式盗取信用卡信息
3、日本氢同位素实验室人员遭到钓鱼攻击
4、安全团队发布技术支持诈骗分析报告
5、研究人员发现 VeraCrypt 多处关键漏洞
6、安全团队揭露仿冒公检法手机诈骗过程

【安天】搜集整理（来源：freebuf、sucuri、softpedia、malwarebytes、theregister、freebuf）

[20161020]
1、利用 Mirai 发动 DDoS 攻击在源码公开增加
2、物联网新威胁：Hajime 蠕虫比 Mirai 更复杂
3、APT 组织开发漏洞利用平台 DealersChoice
4、央视揭露针对苹果手机远程锁定勒索手段
5、研究者利用 WhatsApp 和 Gmail 解锁 iPhone6s
6、研究人员发现利用硬件漏洞绕过 ASLR 方法

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

[20161021]
1、安全厂商溯源 PHP 勒索软件 JapanLocker 作者
2、安卓恶意应用采用"双实例"盗取 Twitter 密码
3、僵尸网络程序利用黑名单机制提高传播效率
4、开源 CMS Joomla 组件被发现 SQL 注入漏洞
5、Ollydbg 插件 StrongOD 存在中间人攻击漏洞
6、研究人员发现 Skype 通话期间击键可被窃听

【安天】搜集整理（来源：fortinet、avast、paloaltonetworks、securityaffairs、theregister、securityweek）

[20161022]
1、研究人员发现 VoIP 服务器被用于传播木马
2、APT 组织 FruityArmor 用微软 0day 发动攻击
3、研究人员称 TheMoon 僵尸网络仍然存活
4、针对中国苹果用户的钓鱼行动再次启动
5、Linux 内核被发现本地提权漏洞 Dirty Cow
6、网站托管服务 Weebly 4300 万用户数据泄露

【安天】搜集整理（来源：symantec、securelist、softpedia、fireeye、softpedia、thehackernews）

[20161023]
1、DNS 服务提供商遭 DDoS 攻击影响美国大量站点
2、安全厂商发现无需 root 权限 Linux 木马后门 FakeFile
3、研究人员称巴基斯坦政府成为网络间谍活动目标
4、研究人员披露 Slack 漏洞，攻击者可接管用户账户

5、土耳其政府多名高级官员遭针对性恶意代码攻击
6、Lexmark 修复其打印机管理产品的 RCE 关键漏洞

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

[20161024]
1、安天发布美国 DDoS 攻击事件分析报告
2、黑客组织承认发动美国大规模 DDoS 攻击
3、美国黑客为报复入侵俄罗斯外交部网站
4、犯罪组织以默认密码攻击巴西家用路由
5、NSA 前承包商被指控窃取政府 50TB 文件
6、研究人员称 SHA3-256 算法可防量子攻击

【安天】搜集整理（来源：antiy、360、securityaffairs、welivesecurity、zdnet、aqniu）

[20161025]
1、勒索软件首次进入最危险恶意软件 TOP3
2、研究人员破解银行木马 Sphinx DGA 算法
3、恶意软件 Hicurdismos 假冒微软蓝屏诈骗
4、网上购物系统 Prestashop 被植入恶意代码
5、已修补 BIND DNS 远程 DoS 漏洞仍有影响
6、统计表明 iOS 应用比安卓应用更易泄露隐私

【安天】搜集整理（来源：softpedia、softpedia、com[应为 itnews]、softpedia、securityweek、softpedia）

[20161026]
1、研究人员发现利用安卓硬件漏洞的 Drammer 攻击
2、勒索软件 Locky 新变种使用新的加密文件扩展名
3、移动恶意软件 GM Bot 变种可绕过系统安全机制
4、研究人员发现 OpenSSL 存在"红色警戒"DoS 漏洞
5、研究人员发现绕过 PayPal 双因子验证的简单方法
6、研究人员发现利用语音邮件漏洞窃取激活码方法

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

[20161027]
1、CNNVD 发布 IoT 漏洞引发网络攻击事件通报
2、安全厂商发现巴西葡萄牙语提示的勒索软件
3、Mac 版 VMware 漏洞，可用于绕过安全机制
4、旧金山博物馆遭钓鱼邮件攻击泄露登录凭据
5、叙利亚网络军对比利时媒体网站发起 DDoS
6、新西兰公司 Endace 产品帮助 GCHQ 监视全球

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

[20161028]
1、APT 组织 Moonlight 瞄准中东和非洲国家
2、日本成为 BLACKGEAR 间谍行动新目标
3、攻击者滥用 LDAP 服务器放大 DDoS 攻击
4、新加坡也被 IoT 设备僵尸网络 DDoS 攻击
5、美国互联网瘫痪背后为 10 万物联网设备
6、以色列手机司法取证公司所用固件泄露

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

[20161029]
1、安卓勒索软件使用新手段实现开机启动
2、匈牙利出现勒索软件 Locky 山寨版 Hucky
3、研究者发现 AtomBombing 代码注入手段
4、网银木马 CloudFanta 通过云存储应用传播
5、乌克兰黑客组织泄露普京助手 2337 封邮件
6、海豚捕杀季引发匿名者新一轮 DDoS 攻击

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

[20161030]
1、Mirai 僵尸网络感染设备涉及 164 个国家
2、实验型僵尸网络 Rex 开始引入 Mirai 组件
3、安全厂商发布银行木马 Gootkit C2 分析
4、通过搜索引擎访问恶意链接的数量上升
5、iOS 漏洞被用于向 911 系统发动 DDoS 攻击
6、澳大利亚红十字会 120 万捐血记录泄露

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

[20161031]

1、意大利开发支持 IPv6 的新型 IoT 僵尸网络
2、对美国 DNS 服务提供商 Dyn 攻击或为误伤
3、安全团队发布商业木马盗神分析溯源报告
4、新型勒索软件强迫用户填写在线调查表
5、欧盟勒令 Facebook 停止使用 WhatsApp 数据
6、前员工爆料：NSA 安全防范技术滞后 10 年

【安天】搜集整理（来源：securityaffairs、freebuf、freebuf、vice、36kr、easyaq）

附录：

Mirai 未来、物联网、DDOS 相关主题[序号 发布日期 标题 URL]：

01 20161024 安天发布美国 DDoS 攻击事件分析报告
http://www.antiy.com/response/Mirai/Mirai.html

02 20161027 CNNVD 发布 IoT 漏洞引发网络攻击事件通报
http://www.cnnvd.org.cn/notice/show/id/7802

03 20161004 僵尸网络 Mirai 程序代码被作者公开
https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

04 20161005 安全厂商发布 Mirai 僵尸网络调查分析报告
https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

05 20161010 安全团队发布物联网恶意代码 mirai 分析报告
http://mp.weixin.qq.com/s?__biz=MzI4ODA4MTcxMA==&mid=2649549863&idx=1&sn=f8ccfb1f0c197cf8d357a3db62

06 20161010 DDoS 僵尸网络利用国产摄像头默认密码传播
http://toutiao.secjia.com/xiongmai-technologies-dvr-root-password

07 20161014 恶意软件 Mirai 几乎感染了全球物联网设备
https://www.easyaq.com/newsdetail/id/1162661789.shtml

08 20161016 Mirai IoT DDoS 木马已瞄准蜂窝网络设备
http://news.softpedia.com/news/mirai-iot-ddos-trojan-now-targets-cellular-network-equipment-509310.shtml

09 20161020 利用 Mirai 发动 DDoS 攻击在源码公开增加

http://www.securityweek.com/mirai-increasingly-used-ddos-attacks-after-source-leak

10 20161020 物联网新威胁：Hajime 蠕虫比 Mirai 更复杂
https://www.easyaq.com/newsdetail/id/364671781.shtml

11 20161023 DNS 服务提供商遭 DDoS 攻击影响美国大量站点
http://www.freebuf.com/news/117403.html

12 20161024 黑客组织承认发动美国大规模 DDoS 攻击
http://bobao.360.cn/news/detail/3679.html

13 20161028 新加坡也被 IoT 设备僵尸网络 DDoS 攻击
http://news.softpedia.com/news/singapore-telco-blames-recent-ddos-attacks-on-compromised-iot-devices-509673.shtml

14 20161028 美国互联网瘫痪背后为 10 万物联网设备
http://news.softpedia.com/news/botnet-of-100-000-iot-devices-behind-dyn-ddos-attack-509687.shtml

15 20161030 Mirai 僵尸网络感染设备涉及 164 个国家
http://www.securityweek.com/mirai-botnet-infects-devices-164-countries

16 20161030 实验型僵尸网络 Rex 开始引入 Mirai 组件
http://news.softpedia.com/news/the-super-dangerous-rex-botnet-has-only-around-150-bots-509768.shtml

17 20161031 意大利开发支持 IPv6 的新型 IoT 僵尸网络
http://securityaffairs.co/wordpress/52845/malware/linuxirctelnet-malware.html

18 20161031 对美国 DNS 服务提供商 Dyn 攻击或为误伤
http://www.freebuf.com/news/117830.html

19 20161015 新 Linux 木马 NyaDrop 出现，威胁物联网领域
http://news.softpedia.com/news/a-new-linux-trojan-called-nyadrop-threatens-the-iot-landscape-509278.shtml

20 20161018 国外黑客发现国产摄像机存在 XXE 漏洞

http://www.freebuf.com/vuls/116613.html

21 20161024 犯罪组织以默认密码攻击巴西家用路由
http://www.welivesecurity.com/2016/10/21/cybercriminals-target-brazilian-routers-default-credentials/

==========

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）