每日安全简讯

[20170101]
1、攻击者伪造 ICANN 邮件传播勒索软件 Cerber
2、美国电力公司内部系统检测到俄方恶意代码
3、Sundown EK 新变种使用图片隐藏恶意代码
4、彼尔德伯格集团网站遭受匿名黑客组织攻击
5、美国军方着手研究未来核武器系统安全问题
6、土耳其宣布建立网军保障国家基础设施安全

【安天】搜集整理（来源：techdirt、theguardian、securityaffairs、softpedia、easyaq、bleepingcomputer）

[20170102]
1、安全厂商发布 Darkleech 组织行动报告
2、美国公布灰色草原网络攻击报告摘要
3、学者称黑客是美俄非军事化战争起点
4、研究者称去年网页加密流量显著增加
5、Firefox 借鉴 Tor 引入防指纹跟踪功能
6、媒体回顾 2016 年最严重黑客入侵事件

【安天】搜集整理（来源：paloaltonetworks、easyaq、youth、slashdot、solidot、wired）

[20170103]
1、美国称"俄制"恶意软件曝光要求多州自查
2、华盛顿邮报称俄入侵美国电厂报告说法有误
3、部分 DNS 查询服务因今年闰秒出现报错现象
4、行李标签代码可泄漏旅客航班和身份信息
5、研究者公开 iMessage 字符崩溃 Bug 测试方法
6、比特币硬件钱包 KeepKey 被黑客攻击和勒索

【安天】搜集整理（来源：cnbeta、ibtimes、easyaq、cnbeta、freebuf、securityweek）
[20170104]
1、猎豹移动发布"微信支付大盗"样本分析报告
2、黑客 Gh0s7 入侵泰国政府网站回应逮捕行动
3、美国特种作战司令部 11G 明文员工数据泄露
4、研究者将建立网站连接白帽子和潜在受害者
5、研究人员盘点 2016 年五大致命银行恶意软件
6、研究人员称 Android 产品 2016 年发现漏洞最多

【安天】搜集整理（来源：freebuf、securityaffairs、easyaq、darkreading、ibsintelligence、bleepingcomputer）

[20170105]
1、DeriaLock 等三勒索软件家族解密程序发布
2、感染 LG 智能电视的勒索软件为 Flocker 变种
3、研究人员盘点以 Fsociety 主题命名恶意软件
4、印度发现针对 WhatsApp 用户的移动恶意软件
5、开源 PHP 库 RCE 高危漏洞影响数百万 Web 服务器
6、美国纽约州加强针对金融行业网络安全法规

【安天】搜集整理（来源：securityweek、securityaffairs、bleepingcomputer、scmagazine、freebuf、securityweek）
[20170106]
1、恶意软件自动创建电邮草稿可致 Mac 系统崩溃
2、勒索软件活动针对 HR 部门企业威胁持续上升
3、黑客攻击 MongoDB 数据库窃取内容并索要赎金
4、Oracle 酒店管理平台 RCE 漏洞致持卡人数据泄漏
5、FBI 网站遭黑客 CyberZeist 入侵造成数据泄露
6、研究人员称智能电表漏洞可造成网络攻击风险

【安天】搜集整理（来源：softpedia、securityweek、securityaffairs、freebuf、securityaffairs、securityweek）
[20170107]
1、新型勒索软件 FireCrypt 集成 DDoS 攻击能力
2、具备加密勒索能力 KillDisk 瞄准 Linux 系统
3、安全厂商发现针对中东木马 MM Core 新版本
4、Ghost Host 技术可绕过恶意域名过滤机制
5、D-Link 因路由器等安全问题被美国 FTC 起诉
6、超声跟踪技术可能被用于辨识 Tor 用户身份

【安天】搜集整理（来源：securityaffairs、securityweek、securityweek、darkreading、securityweek、solidot）
[20170108]
1、山寨超级马里奥跑酷安装银行木马 Marcher
2、研究人员发布恶意软件 GM Bot 变种分析报告
3、卡巴斯基反病毒产品存在 SSL 证书验证缺陷
4、伊朗 APT 组织 OilRig 仿冒 Juniper 和牛津网站
5、研究人员警告黑客通过网络摄像头监视用户
6、维基解密声称将公开部分推特用户私人信息

【安天】搜集整理（来源：zscaler、securityaffairs、techtarget、securityweek、dailystar、slashdot）

[20170109]
1、英国警方警告针对教育系统的勒索软件攻击
2、研究人员认为攻击台湾和欧洲 ATM 系同一团伙
3、安全团队详解拒绝服务攻击影响美国 911 原理
4、域名注册及网站托管商 123-Reg 遭 DDoS 攻击
5、安全媒体盘点 2016 年最活跃的五个黑客组织
6、FBI 披露去年破解恐怖分子 iPhone 5c 的细节

【安天】搜集整理（来源：news、darkreading、easyaq、theregister、freebuf、cnbeta）
[20170110]
1、安全团队借助蜜罐揭秘真实 Mirai 僵尸网络
2、安全团队揭示流氓软件对抗安全软件的手段
3、特朗普首次承认俄罗斯黑客曾干扰美国大选
4、法国国防部长担忧黑客行动将影响法国大选
5、电子竞技娱乐协会被黑 150 万玩家资料泄漏
6、研究者发现借浏览器自动填充功能钓鱼风险

【安天】搜集整理（来源：freebuf、freebuf、cnbeta、securityaffairs、csoonline、bleepingcomputer）

[20170111]
1、勒索软件"圣诞快乐"通过恶意代码窃取信息
2、勒索软件 Kraken 感染 2.8 万台 MongoDB 服务器
3、安全厂商发现 Shamoon2 变种针对虚拟化产品
4、土耳其能源部长称停电事故与网络攻击有关
5、Hello Kitty 母公司被黑 330 万用户数据泄露
6、专家警告：剪刀手拍照可能被黑客盗取指纹

【安天】搜集整理（来源：bleepingcomputer、bleepingcomputer、securityweek、securityaffairs、threatpost、cnbeta）
[20170112]
1、勒索软件新家族 Spora 拥有复杂支付赎金网站
2、研究者发现释放挖矿机的新漏洞利用包 Terror
3、安全厂商发布乌克兰变电站被黑事件分析报告
4、安全厂商发布僵尸网络 Death 黑雀攻击分析报告
5、安全厂商发现针对 Netflix 用户网络钓鱼活动
6、微软发布今年首个补丁包修复两个关键漏洞

【安天】搜集整理（来源：bleepingcomputer、securityweek、secjia、venustech、fireeye、threatpost）
[20170113]
1、意大利当局逮捕 EyePyramid 间谍行动嫌疑人
2、安全厂商称袭击美国黑客组织真面目难识破
3、以色列国防军智能手机发现哈马斯间谍软件

4、GoDaddy 域名验证机制漏洞导致 6 千证书撤销
5、CNNVD 发布关于微信"藏蛟"漏洞情况的通报
6、GCHQ 网络加速器计划：与创业公司密切合作

【安天】搜集整理（来源：bleepingcomputer、easyaq、grahamcluley、threatpost、cnnvd、darkreading）

[20170114]
1、勒索软件 Marlboro 因加密算法简单当日被破解
2、ATM 恶意代码 Ploutus 变种在拉丁美洲大肆传播
3、"跨浏览器指纹"技术可跟踪不同浏览器用户
4、影子经纪人再次释放部分方程式组织泄漏文件
5、安全厂商发布 APT28 报告剖析俄罗斯网络行动
6、手机破解公司 Cellebrite 被黑，900GB 数据泄露

【安天】搜集整理（来源：bleepingcomputer、fireeye、bleepingcomputer、threatpost、easyaq、freebuf）

[20170115]
1、研究人员成功接管勒索软件 Cerber 临时服务器
2、丹麦防长警告：俄罗斯黑客准备攻击丹麦电网
3、部分 Intel CPU 存在通过 USB 接口入侵主机漏洞
4、研究人员发现 WhatsApp 加密会话可被拦截缺陷
5、英国劳埃德银行因 DDoS 攻击导致在线业务瘫痪
6、2016 年常用密码排行榜：使用 123456 接近两成

【安天】搜集整理（来源：bleepingcomputer、cphpost、hothardware、hackbusters、weibo、easyaq）

[20170116]
1、安全厂商发现 ATM 恶意软件新变种 Ploutus-D
2、攻击 MongoDB 黑客团伙瞄准 Elasticsearch 集群
3、研究者发现 Office OLE 被用于传播 Keylogger
4、美国学生因编写 Keylogger 面临十年牢狱之灾
5、Aerospike 早期版本存在 RCE 和信息泄露漏洞
6、中国联通被诉流量劫持透视背后黑色产业链

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

[20170117]
1、RIG EK 被利用向流行应用传播勒索软件 Cerber
2、四家不同英国医院遭到大规模恶意软件攻击
3、钓鱼攻击活动伪装用户联系人欺骗 Gmail 用户
4、三星智能摄像头存在远程命令执行安全漏洞

5、黑客入侵韩国总统案件的调查人员个人电脑
6、特朗普网络安全顾问网站被发现安全性极差

【安天】搜集整理（来源：securityweek、newsbtc、mentalfloss、softpedia、sputniknews、cnbeta）

[20170118]
1、安天发布方程式组织 Drug 攻击平台分析报告
2、山寨超级马里奥跑酷安装远控木马 DroidJack
3、研究者发现麦当劳网站搜索功能存在 XSS 漏洞
4、Carlo Gavazzi 能源监控产品存在高危漏洞
5、雅虎帐号泄露事件影响 3 千澳大利亚政府官员
6、俄罗斯国家电视台谴责黑客提前泄露夏洛克

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

[20170119]
1、勒索软件 Spora 为受害者提供独特支付选择
2、勒索软件攻击全文索引引擎 Elasticsearch
3、新恶意软件 GhostAdmin 可窃取和过滤数据
4、谷歌商店有多款 App 可以窃取 INS 用户密码
5、Carbanak 组织回归，以谷歌服务器作为 C2
6、US-CERT 警告：影子经纪人售 SMB 0Day 漏洞

【安天】搜集整理（来源：threatpost、aqniu、bleepingcomputer、softpedia、darkreading、securityweek）

[20170120]
1、勒索软件 Locky 和银行木马 Dridex 活动出现停滞
2、勒索软件活动盯上美国非营利性癌症服务组织
3、研究人员发现今年首个 Mac 恶意软件 Quimitchin
4、研究人员发现针对谷歌 Chrome 用户恶意软件活动
5、研究人员发现特殊表情符号可导致 iOS 设备重启
6、安全媒体揭秘美国总统奥巴马在任期间通信设备

【安天】搜集整理（来源：thehill、securityaffairs、slashdot、wccftech、securityaffairs、easyaq）

[20170121]
1、勒索软件交易服务平台 Satan 现身暗网
2、CouchDB 和 Hadoop 数据库遭比特币勒索

3、Apache Struts 多个版本被发现 RCE 漏洞
4、乌克兰确认 2016 年停电事故是黑客所为
5、著名游戏公司 Supercell 社区账户泄露
6、美国空军实验室投资建设网络欺骗系统

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

[20170122]
1、安全团队称勒索软件垃圾邮件活动重启
2、安全厂商发布 Carbanak 组织攻击活动报告
3、研究人员找到 Mirai 僵尸网络可能作者
4、俄罗斯恶意代码作者被西班牙警方拘留
5、绿盟发布 2016 年软件定义安全 SDS 白皮书
6、安全厂商研究伪 VM 对抗恶意代码新技术

【安天】搜集整理（来源：securityaffairs、trustwave、easyaq、novinite、secjia、mcafee）

[20170123]
1、安全厂商发现安卓木马 BankBot 源代码泄露
2、黑客攻击印度国家艾滋病研究所 NARI 数据库
3、BBC 推特账户被黑，发布特朗普遭枪杀消息
4、圣丹斯电影节票房等多个系统遭遇网络攻击
5、美国陆军公布"Hack the Army"众测结果
6、白宫称将优先考虑发展防御和进攻网络能力

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

[20170124]
1、安天 AVL 联合小米 MIUI 捕获 O2O 病毒 EvilPea
2、研究人员发布 JavaScript 勒索软件分析报告
3、赛门铁克再一次错发证书，错误证书已撤销
4、被黑纽约时报推特发布俄欲导弹袭美假消息
5、安全媒体盘点 2016 年十大较为知名安全漏洞
6、统计表明仍有 20 万服务器未补心脏出血漏洞

【安天】搜集整理（来源：avlsec、cert、theregister、grahamcluley、freebuf、theregister）

[20170125]
1、勒索软件感染美国圣路易斯城市图书馆计算机
2、研究人员称勒索软件 Sage 2.0 将扩大传播范围
3、研究人员发现大规模休眠的 Twitter 僵尸网络

4、神州网云发布 Linux 下 DDoS 攻击木马分析报告
5、思科修补 WebEx Chrome 插件远程代码执行漏洞
6、Facebook 发现允许攻击者远程删除视频的漏洞

【安天】搜集整理（来源：theguardian、bleepingcomputer、threatpost、4hou、threatpost、softpedia）

[20170126]
1、安天更新方程式 EQUATION DRUG 平台分析报告
2、安全厂商在谷歌市场发现勒索软件 Charger
3、安卓远控木马 Spynote 伪装 Netflix 应用程序
4、Shamoon 所用被盗证书疑由 GreenBug 组织提供
5、暗网市场 AlphaBay 因漏洞泄露 21 万私人消息
6、研究人员发现 Linux systemd 本地提权漏洞

【安天】搜集整理（来源：antiy、checkpoint、threatpost、securityweek、bleepingcomputer、bleepingcomputer）

[20170127]
1、为防勒索软件 Gmail 下月起阻止使用 JS 类型附件
2、研究人员剖析金融类恶意代码隐蔽 VNC 通讯模块
3、研究发现众多 Android VPN 应用含恶意间谍软件
4、安全厂商发现数千 Linux 设备感染木马 Proxy.10
5、施耐德工业实时数据库产品发现默认口令问题
6、西数云产品存在远程命令注入和登录绕过漏洞

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

[20170128]
1、安全厂商发布安卓木马 rootnik 深度分析报告
2、恶意软件 Nuke HTTP bot 被发现在暗网出售
3、社工库网站 LeakedSource 受到攻击停止服务
4、亚马逊谷歌苹果 epub 服务被发现 XXE 漏洞
5、Facebook 将采用物理安全密钥保护用户账号
6、统计报告表明 2016 年数据泄露数量超 42 亿条

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

[20170129]
1、安全厂商解析 Shamoon 攻击组织完整作业过程
2、Dridex 银行木马回归，新变种可绕过 UAC 机制
3、恶意代码伪造银行邮件传播盗取密码和比特币
4、安全厂商发现 IBM 大数据存储分析平台 XSS 漏洞
5、美国杨百翰大学语料库网站部分用户身份泄露

6、Google 计划脱离中介成为独立根证书颁发机构

【安天】搜集整理（来源：mcafee、threatpost、cyren、fortinet、byu、bleepingcomputer）

[20170130]
1、勒索软件 OSIRIS 感染美国警方电子证据服务器
2、研究人员提供勒索软件 VirLocker 简易解密方法
3、三星 Galaxy 短信存在漏洞，可被勒索软件利用
4、微软警告用户防范利用 PDF 文档的社工钓鱼手段
5、思科部分型号视频会议 MCU 产品被发现 RCE 漏洞
6、英国网安专家称：俄黑客可侵入该国军用电脑

【安天】搜集整理（来源：scribd、malwarebytes、boingboing、eweek、hackbusters、dailymail）

[20170131]
1、安全厂商发现冒充 Netflix 登录器的勒索软件
2、360 团队发布 MBR 勒索木马 GoldenEye 分析报告
3、奥地利酒店感染勒索软件 客人无法自由出入
4、香港证监会称部分证券公司网站曾受 DDoS 攻击
5、OurMine 黑客组织入侵 CNN 等多个社交媒体帐户
6、专家担心特朗普三星 Galaxy 手机遭到黑客攻击

【安天】搜集整理（来源：trendmicro、freebuf、securityaffairs、securityaffairs、ibtimes、securityaffairs）

==========

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）