每日安全简讯

[20160401]

1、恶意软件 Remaiten 借路由器、IoT 设备建立僵尸网络
2、研究人员发现 PayPal 服务漏洞 可被利用发送钓鱼邮件
3、美国国土安全部称其海港攻击事件涉打印机预置后门
4、为防御网络攻击 美英两国计划升级三叉戟导弹程序
5、研究人员在美国自动药材供应系统发现上千远程漏洞
6、伪造 jQuery 攻击 WordPress 和 Joomal 网站攻击被曝光

安天 CERT 搜集整理（来源：securityweek、softpedia、publicintelligence、computerworld、avast）

[20160402]
1、勒索软件 Rokku 为受害者提供二维码支付赎金
2、HID 门控制器被曝严重漏洞 可供黑客远程开门
3、iOS 存 SideStepper 漏洞 可借 MDM 传播恶意代码
4、Android 勒索软件来向亚洲袭来 日本首当其冲
5、开源解压库 Lhasa 被曝存任意代码执行严重漏洞
6、俄巴两国攻击者交易工具和技术 攻击各自国家

安天 CERT 搜集整理（来源：softpedia、securityweek、computerworld、symantec、theregister、zdnet）
[20160403]
1、研究人员公开绕过 OS X、iOS 系统完整性保护 PoC
2、安全厂商曝光最新的电话社工+恶意代码攻击手段
3、勒索软件感染数量激增 美加两国政府联合发布预警
4、黑客入侵美国成人网站 黑市出售 237,000 用户信息
5、匿名者黑客组织出于政治目的入侵 20 家安哥拉政府
6、FBI 改变官方立场：不再支持向勒索软件支付赎金

安天 CERT 搜集整理（来源：thehackernews、paloaltonetworks、zdnet、softpedia）
[20160404]
1、匈牙利政府网站因遭受境外网络攻击暂时关闭
2、安全厂商发布勒索软件家族 Petya 详细分析报告
3、亲美黑客 Jester 对以色列情报部门网站发动攻击
4、国外黑客找到 iOS 9.3 越狱漏洞 可能已卖往中国
5、媒体曝光链家"信息门"事件 涉及百万人隐私信息
6、记者揭露 170、171 号段诈骗号码未能实名制问题

安天 CERT 搜集整理（来源：securityaffairs、f-secure、ibtimes、cnbeta、qq、cntv）
[20160405]
1、安全厂商发布勒索软件 Locky 家族感染过程分析报告
2、6.6GB 土耳其公民信息库泄露 包含近 6 千万国民信息
3、研究人员发现 Firefox 扩展被用于隐藏静默恶意软件
4、史上最大数据泄露事件：ICIJ 曝光 2.6TB"巴拿马档案"
5、美英两国计划在核安全峰会期间演习核电站网络攻击
6、美国签证和护照数据库被发现漏洞 数据可能遭到篡改

安天 CERT 搜集整理（来源：welivesecurity、网路冷眼、theregister、thehackernews、securityaffairs、helpnetsecurity）
[20160406]
1、安天曝光木马反弹连接 C2 新手法:利用 QQ 昵称
2、研究人员发现 AndroidAPI 提权漏洞:可泄漏私钥
3、FBI 称有神秘黑客组织长年访问美国政府文档
4、Google 取缔 Better History 等流量劫持扩展程序
5、微软关闭相关服务 48 小时：修补账号劫持漏洞
6、安全厂商发现 Google 商店 104 款 App 感染广告件

安天 CERT 搜集整理（来源：freebuf、threatpost、vice、softpedia、theregister、deccanchronicle）
[20160407]
1、安全厂商跟踪发现 Locky 勒索软件变种通信特征发生变化
2、安全厂商发现勒索软件变种 Samsam 已具针对性攻击能力
3、安全厂商发布勒索软件 Locky 分析报告:席卷世界的加密者
4、安全厂商曝光经济动机的恶意参与者 TA530 典型攻击手法
5、全球最大手机聊天工具 WhatsApp 将启用消息端到端加密
6、iPhone6s/Plus 曝锁屏绕过漏洞：由 Siri+3D Touch 访问照片

安天 CERT 搜集整理（来源：securityweek、symantec、securelist、proofpoint、qq、thehackernews）
[20160408]
1、菲律宾选委会网站被黑：约 5500 万投票人身份数据泄露
2、Hacking Team 执照被吊销 不得售间谍软件给欧盟外国家
3、Ubuntu 修补四个内核漏洞 可执行任意代码和拒绝服务攻击
4、安全团队发布黑产调查报告：业务明码标价 服务一应俱全
5、因缺乏业界支持 开源漏洞数据库(OSVDB)项目将永久关闭
6、以色列安全机构称：已对匿名者黑客组织攻击做好防范准备

安天 CERT 搜集整理（来源：networkworld、theregister、secureworks、securityweek）
[20160409]
1、安天发布勒索软件家族 TeslaCrypt 最新变种技术特点分析报告
2、安全厂商联合执法机构打击 Mumblehard 家族 Linux 僵尸网络

3、Adobe 紧急修复被用于传播勒索软件 Cerber 的 Flash 关键漏洞
4、孟加拉央行窃案新进展：相关恶意代码或已将信息传往埃及
5、研究者称近 3 千万装有医疗 App 的移动设备感染高危恶意软件
6、美国儿童支持执行办公室笔记本被盗 百万儿童社保信息泄露

安天 CERT 搜集整理（来源：antiy、securityweek、nbcnews、straitstimes、itproportal、informationsecuritybuzz）
[20160410]
1、安全厂商发现 Dridex 木马用于窃取银行卡数据及传播勒索软件
2、研究人员称有组织犯罪集团日渐贪婪 银行家成为 APT 攻击目标
3、研究者发现恶意软件工具包 Su-A-Cyder：可监控未越狱 iPhone
4、境外安全厂商揭示黑客借助第三方将恶意代码加入白名单伎俩
5、研究人员发现谷歌和 Facebook 验证码系统漏洞 可绕过保护限制
6、安全厂商曝光 Locky 等多个勒索软件家族开始设法逃避杀软检测

安天 CERT 搜集整理（来源：darkreading、securityintelligence、hackread、checkpoint、securityweek、paloaltonetworks）
[20160411]
1、勒索软件 CryptoHost 家族使用 RAR 的密码保护机制加密文件
2、德克萨斯地区 20 所院校遭受勒索软件攻击 2.5TB 数据被加密
3、黑客组织"网络正义小队"入侵叙利亚政府网站曝光 43GB 数据
4、研究人员警告美国再现针对移动设备的 iScam 式仿冒弹窗勒索
5、研究人员称 1.35 亿路由设备存在漏洞 可被利用发动 DoS 攻击
6、抗议新劳动法 黑客组织泄漏意大利公司高管和雇员私人信息

安天 CERT 搜集整理（来源：securitynewspaper、softpedia、163、oaoa、slashdot、hackread）
[20160412]
1、研究人员发现亚马逊在售某型号室外摄像机包含恶意软件
2、安全厂商曝光俄罗斯移动端勒索软件：仿冒色情视频传播
3、研究人员发布破解工具：勒索软件 Petya 加密文件可被解密
4、研究者警告:蠕虫式勒索软件（cryptoworm）时代即将到来
5、比特币交易商 ShapeShift 因网络攻击而彻底重建其基础设施
6、瑞典军方发现服务器被黑 曾在 2013 年被用于攻击美国银行

安天 CERT 搜集整理（来源：securityaffairs、trendmicro、softpedia、phys、securityweek）
[20160413]
1、安全团队联合分析恶意软件 Ramdo 躲避检测新手段
2、OS X 短信应用存漏洞 攻击者可窃取历史聊天数据
3、研究人员发现针对家用路由器、修改 DNS 恶意软件
4、勒索软件"拼图"每次重启删除一千文件 有解密方法
5、勒索软件 Locky 放弃垃圾邮件 开始采用新方式传播
6、"勒索软件 ID"网站问世 可识别 50 余种勒索软件格式

安天 CERT 搜集整理（来源：paloaltonetworks、softpedia、trendmicro、securityweek、malwarehunterteam）

[20160414]

1、安全厂商发布 2015 年网络安全威胁报告 强调纵深防御
2、银行木马变种 Atmos 活跃 曾被勒索软件 Teslacrypt 使用
3、僵尸网络 Gamarue 利用被黑 WordPress 站点发钓鱼邮件
4、调查发现美国彩票销售人员使用恶意 DLL 影响彩票号码
5、研究人员发现新版僵尸网络 Qbot 针对美国公共机构等
6、安全厂商发现 Magnitude 和 Nuclear 利用 Adobe 最新漏洞

安天 CERT 搜集整理（来源：symantec、securityaffairs、softpedia）

[20160415]

1、研究者发现 Linux 木马新家族 Xudp 具有后门功能
2、瑞典指责俄罗斯政府攻击其航空航天基础设施
3、美国前核能源管理委员会人员因黑客企图被判刑
4、iOS 再现 1970 变砖漏洞 由假 WIFI 和 NTP 服务器触发
5、中东黑客利用 LinkedIn 仿冒他人账户传播恶意软件
6、安全厂商与执法部门证明 ATM 恶意软件数量增多

安天 CERT 搜集整理（来源：softpedia、securityweek、securityaffairs、wpsdlocal6、trendmicro）

[20160416]

1、勒索软件 CTB-Locker 使用比特币区块链技术交付解密密钥
2、高危漏洞 美国政府建议 Windows PC 用户卸载 QuickTime
3、研究人员发现混合型木马家族 GozNym 针对北美金融机构
4、黑客组织 Lizard Squad 对视频游戏服务网站发动 DDoS 攻击
5、黑莓向加拿大警方提供解密密钥 可解其所有设备加密内容
6、研究人员发布报告：短网址可为云服务带来严重安全风险

安天 CERT 搜集整理（来源：computerworld、businessinsider、securityintelligence、softpedia、vice、arxiv）

[20160417]

1、全球约 320 万台服务器有 Jboss 平台后门 或被勒索软件利用
2、西部数据公司出现 DNS 配置问题 可使攻击者获得用户数据
3、Fappening 论坛 18 万用户数据泄露 恶意广告指向勒索软件
4、泄露 Hacking Team 400G 数据人员揭秘入侵行动技术细节
5、研究人员发现三星 Galaxy 手机电话短信功能绕过锁屏漏洞
6、安全团队警告 WordPress 站点受到新型 C99 Webshell 攻击

安天 CERT 搜集整理（来源：softpedia、securityweek、scmagazine、vice、freebuf、securityintelligence）

[20160418]
1、勒索软件 Locky 山寨版 AutoLocky 解密程序已公开
2、Facebook 恶意视频 针对 Chrome 用户传播恶意软件
3、研究人员发现窃取敏感信息广告件 Faster Internet
4、商业邮件诈骗在全球增长 美国公司损失近亿美元
5、研究人员在 Microsoft Edge 发现 XSS Filter 绕过漏洞
6、ShapeShift 攻击事件系内部员工向攻击者提供帮助

安天 CERT 搜集整理（来源：softpedia、hackread、securityaffairs）

[20160419]
1、北美和中国能源部门某型号电力仪表被发现高危漏洞
2、USB-C 接口新标准规范公布 有利于防范 USB 恶意软件
3、统计表明 Power Shell 已经成为最受欢迎针对性攻击手段
4、 安天移动安全团队联合猎豹共同截获手机病毒"僵尸之手"
5、点击欺诈类恶意软件 Kovter 家族正演变为勒索软件变种
6、研究人员测试发现 Avactis PHP 购物车平台漏洞数量惊人

安天 CERT 搜集整理（来源：us-cert、softpedia、AVL Yun、securityaffairs）
[20160420]
1、孟加拉央行资金失窃案日前告破 20 名参与者身陷法网
2、比特币支付机构提醒用户警惕剪贴板木马 Coinbitclip
3、厂商发现高度针对性 POS 机木马新变种 MULTIGRAIN
4、研究人员发现跨平台 BOT 新家族 PWOBot 由 Python 编写
5、研究者称 Hacking Team 泄漏事件中涉及部分漏洞仍未补
6、为独占受害主机 Thanatos 木马家族竟装备病毒清除模块

安天 CERT 搜集整理（来源：cnbeta、softpedia、fireeye、paloaltonetworks、theregister、informationsecuritybuzz）

[20160421]
1、研究人员发布 OSX 平台能用勒索软件检测工具
2、美国某成人网站被入侵 约 380 万帐户信息泄露
3、Exploit kit 作者放弃 Java 漏洞 转向 Flash 漏洞
4、研究者由暗网发现黑客感染 IPS 社区套件图谋
5、安全厂商曝光勒索软件家族新变种 JIGSAW
6、记者卧底揭露河南 7 万银行卡信息被泄露事件

安天 CERT 搜集整理（来源：hackersonlineclub、softpedia、theregister、trendmicro、weibo）
[20160422]

1、CNCERT 权威发布《2015 年我国互联网网络安全态势综述》
2、勒索软件再添新家族 CryptoBit 因为漏洞或可被解密
3、安全厂商发现勒索软件 CryptXXX 借木马 Bedep 传播
4、勒索软件 TeslaCrypt 新变种 更加复杂也更具适应性
5、安全厂商揭露黑客组织 FIN6 盗卖百万 PoS 机支付卡
6、研究发现欺诈网站新伎俩 Exploit Kit 藏身社交按钮

安天 CERT 搜集整理（来源：51cto、pandasecurity、bravenewcoin、endgame、fireeye、malwarebytes）

[20160423]
1、微软 AppLocker 机制可被 regsvr32 隐藏特性绕过
2、攻击者借 Google 文档漏洞传播木马 Laziok 被曝光
3、研究人员预言：智能汽车或成勒索软件未来目标
4、泄露 5500 万选民数据黑客之一被菲律宾警方逮捕
5、研究者发现 Facebook 服务器留有 2015 年 WebShell
6、统计称逾 4 亿未及时更新安卓设备易受黑客攻击

安天 CERT 搜集整理（来源：softpedia、fireeye、driving、ibtimes、tomsguide）
[20160424]
1、研究者发现 132GB 泄露数据：墨西哥 9300 万选民信息曝光
2、钓鱼诈骗新伎俩：骗子向苹果用户发送"Apple ID 过期"短信
3、勒索软件家族再添新变种：Nemucod 使用 7Zip 实现文件加密
4、安全厂商揭露远控木马新手段：使用 PNG 图片作为配置文件
5、英国防部承包商 Niteworks 被攻击 831 名高级成员身份被泄露
6、孟加拉央行八千万美元窃案反思：廉价路由器、未装防火墙

安天 CERT 搜集整理（来源：securityaffairs、hackread、myce、sentinelone、theregister、businessinsider）
[20160425]
1、厂商发现 BlackMoon 银行木马感染韩国 10 万用户主机
2、安全厂商揭露某阿联酋注册 VPS 被用于发动 APT 攻击
3、攻击者伪装太平洋保险发送钓鱼邮件传播 JS 恶意代码
4、DARPA 计划为美国军方建立超级安全信息应用程序
5、匿名者组织因种族问题向三 K 党网站发动 DDoS 攻击
6、MIT 称其新人工智能网络安全平台可预测 8 成网络威胁

安天 CERT 搜集整理（来源：fortinet、trendmicro、myonlinesecurity、thehackernews、hackread、bilbaoya）
[20160426]
1、黑客组织 NWH 因警察枪击案对美丹佛政府网站发动 DDoS 攻击
2、加密运营商 Ennetcom 受警方调查，因洗钱等违规操作被迫关停
3、孟加拉银行窃案黑客定制恶意代码攻击金融平台 SWIFT 过程曝光

4、消息应用 Viber 继 WhatsApp 后对其平台全部消息采用端到端加密
5、研究人员称预装恶意代码的廉价智能手机是网络犯罪的助推器
6、美国政府宣布将对恐怖组织 ISIS 展开黑客行动并使用网络武器

安天 CERT 搜集整理（来源：softpedia、securityaffairs、helpnetsecurity、devicemag、emirates247）

[20160427]
1、CNVD 公告：Apache Struts2 存在远程代码执行高危漏洞
2、研究者在德国巴伐利亚贡德雷明根核电站发现恶意代码
3、新勒索软件利用恶意广告安全漏洞非交互感染安卓设备
4、安全厂商揭示 ATM 易受黑客恶意代码攻击两个主要原因
5、交友网站 BeautifulPeople 百万用户数据泄露并被在线交易
6、ICIT 预测:工控系统、物联网设备等将遭到勒索软件攻击

安天 CERT 搜集整理（来源：cnvd、zerohedge、softpedia、kaspersky、icitech）
[20160428]
1、攻击者借 Flash0day 漏洞在海盗湾网站传播勒索软件 Cerber
2、卡塔尔国民银行 1.4G 数据泄露 受害者面临金融欺诈风险
3、黑客组织利用 Windows 热补丁技术向系统注入恶意代码
4、安全厂商升级勒索软件解密工具支持解密 CryptXXX 家族
5、研究人员发现勒索软件家族 7ev3n 新变种 降低赎金要求
6、安全厂商发布针对俄罗斯的短信拦截木马 RuMMS 报告

安天 CERT 搜集整理（来源：softpedia、arstechnica、kaspersky、grahamcluley、fireeye）

[20160429]
1、安天发布针对移动银行和金融支付的持续黑产行动跟踪分析报告
2、思科指责法国软件制造商 Tuto4PC 在其 1200 万用户电脑安装后门
3、调查发现 Tor 项目前雇员帮助 FBI 开发恶意软件监测 Tor 用户行踪
4、研究者发现利用 Windows PowerShell 注入恶意宏代码的 Fareit 变种
5、研究人员曝光非越狱 iOS 微信分身插件 ImgNaix 预留高危接口
6、域名注册处 ASNIC 存漏洞 数据泄露隐患自 90 年代中期开始存在

安天 CERT 搜集整理（来源：avlsec、softpedia、thehackernews、securityaffairs、wooyun）
[20160430]
1、勒索软件近期爆发 研究人员又发现三个新家族
2、安全团队揭露移动恶意代码黑市非法交易现状
3、攻击者借微软上帝模式彩蛋实现持久化被曝光
4、厂商曝光针对日本企业的攻击组织 Tick 的活动
5、加拿大黄金公司遭黑客攻击 14.8GB 数据被窃
6、匿名者黑客组织泄露肯尼亚外交部 1TB 文档数据

安天 CERT 搜集整理（来源：proofpoint、securityintelligence、mcafee、symantec、softpedia）

==========

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）