

[20160801]

- 1、[Locky](#) 勒索软件变种 [Zepto](#) 超越 [CryptXXX](#) 成主流
- 2、[Conficker](#) 病毒旧 C&C 地址被用于劫持网站流量
- 3、[XEN](#) 虚拟机监控器致命漏洞，仅影响 [X86](#) 硬件
- 4、[俄安全部门](#)发现针对其政府军事组织间谍软件
- 5、[美官员](#)称美国将不遗余力对网络攻击做出回应
- 6、[美军](#)或利用潜水艇作为水下网络攻击作业平台

【安天 CERT】搜集整理（来源：[softpedia](#)、[itsecuritynews](#)、[freebuf](#)、[securityaffairs](#)、[sputniknews](#)、[washingtonpost](#)）

[20160802]

- 1、研究人员发现针对银行账户恶意攻击 [SupporBuddy](#)
- 2、安全厂商报告揭露谷歌商店口袋妖怪相关恶意 APP
- 3、[Pokemon Go](#) 作者 [Twitter](#) 遭 [OurMine](#) 黑客组织入侵
- 4、[迪士尼](#) [Playdom](#) 论坛被黑，造成 35 万用户信息泄露
- 5、继印度 AP 警察招聘网站被黑后又一大学官网被攻击
- 6、信息泄露传闻后，微软禁用 [SwiftKey](#) 单词预测功能

【安天 CERT】搜集整理（来源：[wncn](#)、[trendmicro](#)、[fin24](#)、[softpedia](#)、[newindianexpress](#)、[softpedia](#)）

[20160803]

- 1、谷歌商店百款 App 感染木马，下载达 280 万次
- 2、安全团队解读匿名者组织 [OpAfrica](#)“非洲行动”
- 3、黑帽大会 App 漏洞，可冒充用户进行间谍活动
- 4、黑客 [Peace](#) 在暗网出售 2 亿多雅虎用户帐户信息
- 5、[Windows](#) 漏洞可泄露用户密码和 VPN 登录凭证
- 6、谷歌推出帐户安全新特性：新设备登录有通知

【安天 CERT】搜集整理（来源：[softpedia](#)、[qq](#)、[securityweek](#)、[softpedia](#)、[softpedia](#)、[thehackernews](#)）

[20160804]

- 1、安全团队曝光基于 [Office](#) 宏的恶意代码传播新手段
- 2、安全厂商详解用户可自定义插件的远控木马 [ORCUS](#)
- 3、研究人员发现微软网络共享 Bug，可致帐户凭据泄露
- 4、世界最大比特币交易所 [Bitfinex](#) 12 万枚比特币被盗
- 5、[Telegram](#) 服务被入侵，1500 万伊朗用户电话号码泄露
- 6、为追踪网络罪犯匿名访问暗网 [FBI](#) 开展 [Pacifier](#) 行动

【安天 CERT】搜集整理（来源：[softpedia](#)、[paloaltonetworks](#)、[securityweek](#)、[securityweek](#)、[venturebeat](#)、[securityaffairs](#)）

[20160805]

- 1、[银行木马 Gozi 新版本活跃在日本、西班牙等国家](#)
- 2、[巴西短信钓鱼和手机银行钓鱼攻击数量呈上升趋势](#)
- 3、[安全厂商发布报告阐述 15 年来工控系统漏洞情况](#)
- 4、[HTTP/2 协议发现漏洞，可被黑客用于扰乱服务器](#)
- 5、[安全团队曝光针对叙利亚的 APT 组织 Group 5](#)
- 6、[安全团队发布 APT 报告分析“摩诃草”组织四次攻击](#)

【安天 CERT】搜集整理（来源：[softpedia](#)、[securelist](#)、[fireeye](#)、[thehackernews](#)、[softpedia](#)、[360](#)）

[20160806]

- 1、[研究人员利用 Adobe AEM 漏洞进入微软服务器](#)
- 2、[Kasidet 家族 C2 服务器藏身于 Namecoin 区块链](#)
- 3、[开发商称：Pokemon Go 已成为黑客攻击目标](#)
- 4、[研究人员展示利用 EMV 卡窃取 ATM 现金新手段](#)
- 5、[美国非营利性医疗系统班纳健康 370 万数据泄露](#)
- 6、[FossHub 下载站两款流程序被替换为恶意软件](#)

【安天 CERT】搜集整理（来源：[softpedia](#)、[softpedia](#)、[femalefirst](#)、[securityweek](#)、[securityweek](#)、[pcworld](#)）

[20160807]

- 1、[VMware Tools 漏洞：可通过 DLL 劫持执行代码](#)
- 2、[一款专门针对中国用户安卓木马或来自意大利](#)
- 3、[报告披露俄罗斯 APT 组织青睐 IE 和 Office 漏洞](#)
- 4、[意大利开发者在黑客论坛出售 Remcos 远控木马](#)
- 5、[研究者发现不破坏数字签名添加恶意代码方法](#)
- 6、[开发者论坛数据泄露，涉及谷歌、苹果员工](#)

【安天 CERT】搜集整理（来源：[securityweek](#)、[softpedia](#)、[securityweek](#)、[softpedia](#)、[computerworld](#)、[ibtimes](#)）

[20160808]

- 1、[勒索软件 Cerber 出现新变种，原解密工具失效](#)
- 2、[新型勒索软件模仿系统弹窗诱骗用户拨打电话](#)
- 3、[研究者发现微软系统 Evil Butler 远程攻击漏洞](#)
- 4、[研究人员展示针对显示器固件的恶意攻击方法](#)
- 5、[银行木马 Panda 在里约奥运期间攻击巴西银行](#)
- 6、[匿名者组织借里约奥运会对巴西政府发起攻击](#)

【安天 CERT】搜集整理（来源：[softpedia](#)、[softpedia](#)、[softpedia](#)、[pcworld](#)、[softpedia](#)、[softpedia](#)）

[20160809]

- 1、[安全团队发布分析报告曝光南亚 APT 组织“丰收行动”](#)
- 2、[安全厂商发现针对中国和欧洲国家攻击组织 Strider](#)
- 3、[高通芯片存高危漏洞 Quadrooter，影响 9 亿安卓设备](#)
- 4、[研究人员披露四个安卓上帝模式漏洞，可用于提权](#)
- 5、[Samsung Pay 令牌存在漏洞，可以导致欺诈交易](#)
- 6、[美国警方发现两窃贼利用汽车漏洞盗窃百余辆汽车](#)

【安天 CERT】搜集整理（来源：aptno1、symantec、checkpoint、theregister、securityaffairs、lasvegasherald）

[20160810]

- 1、[勒索软件 Hitler 新变种，支付赎金倒计时设为一小时](#)
- 2、[Oracle PoS 系统数据泄露，疑遭受 Carbanak 组织入侵](#)
- 3、[研究人员证明物联网设备存在感染勒索软件可能性](#)
- 4、[AppStore 出现假冒比特币钱包应用，用户资金被窃](#)
- 5、[Fortinet 几款安全产品发现远程注入代码执行漏洞](#)
- 6、[安全厂商发现使用 GO 语言开发的 Linux 挖矿木马](#)

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

[20160811]

- 1、[安全厂商发布网络间谍平台 ProjectSauron 研究报告](#)
- 2、[微软 PDF 库存在远程代码执行漏洞，设备可被接管](#)
- 3、[安全厂商发现具有窃密行为的移动勒索软件 EIGato](#)
- 4、[研究人员发现勒索软件 CryptFile2 借助恶意邮件传播](#)
- 5、[调查发现暗网平均每月新增 16 个 0day 漏洞利用工具](#)
- 6、[网络游戏 Dota2 论坛遭到入侵，200 万账户信息泄露](#)

【安天 CERT】搜集整理（来源：securelist、slashdot、softpedia、proofpoint、softpedia、zdnet）

[20160812]

- 1、[安全厂商发布 Monsoon APT 事件分析报告](#)
- 2、[追日团队披露索伦之眼针对中国的攻击](#)
- 3、[Linux 内核 TCP 漏洞，可劫持流量注入代码](#)
- 4、[研究人员发现微软安全启动机制可被绕过](#)
- 5、[劫持浏览器恶意代码变种利用合法应用程序](#)
- 6、[Instagram 泄露账号被用于传播成人内容牟利](#)

【安天 CERT】搜集整理（来源：forcepoint、qq、thehackernews、securityweek、mcafee、scmagazine）

[20160813]

- 1、[安天 AVLTeam 揭秘伪装 Pokemon Go 的恶意应用](#)
- 2、[安全厂商发现勒索软件 R980 滥用一次性邮箱服务](#)
- 3、[勒索软件 Shade 变种具 RAT 特性，监控高价值目标](#)
- 4、[研究者发现网络钓鱼行动利用 Jabber 服务外传数据](#)
- 5、[D-Link 修补 DIR 型号路由器远程任意代码执行漏洞](#)
- 6、[大众汽车遥控钥匙漏洞，上亿台汽车可被无线解锁](#)

【安天 CERT】搜集整理（来源：qq、trendmicro、softpedia、phishlabs、securityweek、thehackernews）

[20160814]

- 1、勒索软件 Smrss32 可加密六千种扩展名文件
- 2、[暗网黑客论坛出售金融木马开发包 Scylex](#)
- 3、[Twitter 出现冒充客服帐户的社工钓鱼骗术](#)
- 4、[世界反兴奋剂机构发现针对性攻击迹象](#)
- 5、[研究者公开 Bluetooth 4 中间人攻击方法](#)
- 6、[研究人员称可利用硬盘声音窃取数据](#)

【安天 CERT】搜集整理（来源：sensorstechforum、heimdalsecurity、metro、yahoo、softpedia、securityaffairs）

[20160815]

- 1、[研究人员发现窃取企业机密信息的新型木马程序](#)
- 2、[研究人员发布 RIG Exploit Kit 恶意活动分析报告](#)
- 3、[密码学专家发现苹果 iMessage 协议存在加密缺陷](#)
- 4、[比特币交易所悬赏 350 万征集恢复被盗比特币信息](#)
- 5、[研究人员称可通过入侵投票机控制选举投票结果](#)
- 6、[谷歌将为 Gmail 加入访问钓鱼网站链接时警告消息](#)

【安天 CERT】搜集整理（来源：bleepingcomputer、freebuf、softpedia、thehackernews、slashdot、onlinenewshearnow）

[20160816]

- 1、[勒索软件仿冒 Pokemon GO，在受感染设备装后门](#)
- 2、[巴西地下市场出现使用 WSF 的勒索软件 Locky 变种](#)
- 3、[Rowhammer 攻击新手法，可以劫持 Linux 虚拟机](#)
- 4、[利用 SSL 加密 C&C 通信的恶意软件呈显著增长趋势](#)
- 5、[攻击者劫持 WordPress 核心文件，嵌入 SEO 垃圾邮件](#)
- 6、[美国 20 家酒店支付系统感染恶意软件，危及客户资料](#)

【安天 CERT】搜集整理（来源：[softpedia](#)、[trendmicro](#)、[softpedia](#)、[softpedia](#)、[softpedia](#)、[reuters](#)）

[20160817]

- 1、[我国发射世界首颗量子科学实验卫星“墨子号”](#)
- 2、[黑客声称入侵 Equation 组织，部分武器库泄露](#)
- 3、[Linux 内核 TCP 漏洞，影响全球 14 亿安卓设备](#)
- 4、[多核 ARM CPU 缓存攻击，影响数亿安卓设备](#)
- 5、[HTTP 协议缺陷，微软、苹果等厂商均受影响](#)
- 6、[勒索软件 Shark 作者提供勒索服务，赚取提成](#)

【安天 CERT】搜集整理（来源：[cas](#)、[freebuf](#)、[softpedia](#)、[softpedia](#)、[softpedia](#)、[symantec](#)）

[20160818]

- 1、[安全厂商曝光针对工业和工程组织的 Ghoul 行动](#)
- 2、[TeamViewer 组件被用于在欧洲等地进行间谍活动](#)
- 3、[安全厂商证明 shadowbrokers 泄露恶意代码真实性](#)
- 4、[研究者称企业间谍软件 Shakti 或与印度黑客有关](#)
- 5、[银行木马 Panda 利用多国语言垃圾邮件大规模感染](#)
- 6、[巴西版银行木马 Sphinx 目标为银行及 Boleto 支付](#)

【安天 CERT】搜集整理（来源：[securelist](#)、[softpedia](#)、[softpedia](#)、[ibtimes](#)、[securityweek](#)、[softpedia](#)）

[20160819]

- 1、[勒索软件 Locky 近期借 DOCM 格式附件传播](#)
- 2、[勒索软件 CERBER 令犯罪组织年获利百万](#)
- 3、[勒索软件 CERBER 解密工具发布一天即失效](#)
- 4、[影响 Firefox 等浏览器 URL 欺骗新手段出现](#)
- 5、[思科修复 Shadow Brokers 泄露的 0day 漏洞](#)
- 6、[Social Blade 被黑，27 万用户数据遭泄露](#)

【安天 CERT】搜集整理（来源：[fireeye](#)、[softpedia](#)、[ibtimes](#)、[softpedia](#)、[softpedia](#)、[softpedia](#)）

[20160820]

- 1、[斯诺登文件证明 NSA 泄露真实性](#)
- 2、[研究者发现勒索软件新变种 Fsociety](#)
- 3、[智能插座漏洞可被用于远程攻击](#)
- 4、[Eddie Bauer 350 家店感染 PoS 恶意软件](#)
- 5、[巴西银行木马利用 PowerShell 脚本](#)
- 6、[Leet.cc 服务器 600 万玩家数据被盗](#)

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

[20160821]

- 1、[安卓木马 Marcher 可盗取 Facebook 等登录信息](#)
- 2、[银行木马 Dridex 卷土重来 主要目标为瑞士](#)
- 3、[Linux 木马 Rex 更新 可用于发动 DDoS 攻击](#)
- 4、[转储的维基解密电邮附件含 300 余恶意软件](#)
- 5、[BANKER 木马利用里约奥运会进行恶意活动](#)
- 6、[在线机器学习未来或许可检测安卓恶意软件](#)

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

[20160822]

- 1、[研究者深度分析美国国安局泄漏文件](#)
- 2、[勒索软件 DetoxCrypto 出现新变种](#)
- 3、[研究人员分析揭秘勒索软件 Chimera](#)
- 4、[安全厂商发布勒索软件屏幕解锁工具](#)
- 5、[匿名者组织为里约攻击开发 DDoS 工具](#)
- 6、[研究人员发现新的微软 UAC 绕过方法](#)

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

[20160823]

- 1、[安卓木马 DroidJack 借助短信钓鱼链接传播](#)
- 2、[阿尔法团队发现微信任意代码执行漏洞](#)
- 3、[GnuPG 修复存在 20 年的随机数生成器漏洞](#)
- 4、[安全公司披露 BHU WIFI 路由器多个漏洞](#)
- 5、[PayPal 修复双因子登录可绕过漏洞](#)
- 6、[维基百科联合创始人 Twitter 账号遭到入侵](#)

【安天 CERT】搜集整理(来源: itsecuritynews、360、gnu、ioactive、theregister、mashable)

[20160824]

- 1、[新型勒索软件 Alma Locker 通过 RIG EK 传播](#)
- 2、[新型勒索软件 DetoxCrypto 含截屏窃密功能](#)
- 3、[Juniper 证实 NSA 泄漏文件影响其防火墙产品](#)
- 4、[攻击者利用虚拟机在受害主机隐藏恶意活动](#)
- 5、[安全厂商发现创建 P2P 僵尸网络的 Linux 木马](#)

## 6、[Epic 游戏论坛再次被黑，80 万玩家信息泄露](#)

【安天 CERT】搜集整理（来源：[bleepingcomputer](#)、[securityweek](#)、[securityweek](#)、[secureworks](#)、[securityweek](#)、[zdnet](#)）

[20160825]

- 1、[安天 AVLTeam 发布移动银行应用仿冒攻击威胁分析报告](#)
- 2、[美国部分新闻媒体遭到攻击，或与俄罗斯情报机构有关](#)
- 3、[研究者认为开源 BTS 设备漏洞可用于劫持蜂窝数据基站](#)
- 4、[两厂商成功解密 WildFire 勒索软件，发布免费解密工具](#)
- 5、[研究人员发现 VR 技术可被用于绕过人脸识别验证](#)
- 6、[印度绝密潜艇数据泄露，官员称是黑客入侵所致](#)

【安天 CERT】搜集整理（来源：[avlsec](#)、[cnn](#)、[zimperium](#)、[softpedia](#)、[securityweek](#)、[manoramaonline](#)）

[20160826]

- 1、[研究人员发现首个由 Twitter 控制的安卓僵尸网络](#)
- 2、[追日团队发布银行 SWIFT 系统攻击事件综合报告](#)
- 3、[Linux 蠕虫 PNScan 暴力破解路由器并安装后门](#)
- 4、[工业网络厂商 Moxa 部分网络设备存身份验证漏洞](#)
- 5、[泰国 ATM 机骨干网络遭到入侵，1200 万泰铢被盗](#)
- 6、[Mail.ru 论坛遭黑客攻击，2500 万用户记录被窃](#)

【安天 CERT】搜集整理（来源：[eset](#)、[360](#)、[securityweek](#)、[securityweek](#)、[freebuf](#)、[easyaq](#)）

[20160827]

- 1、[iOS 严重安全漏洞：iPhone 用户可被监听](#)
- 2、[勒索软件 Locky 新变种以 dll 文件格式传播](#)
- 3、[勒索软件 Alma Locker 免费解密工具发布](#)
- 4、[银行木马 Ursnif 变种利用 Tor 网络隐藏 C2](#)
- 5、[攻击者利用 PS 命令盗取网站证书和配置](#)
- 6、[VMware 修复 vRA 应用提权及 RCE 漏洞](#)

【安天 CERT】搜集整理（来源：[freebuf](#)、[softpedia](#)、[phishlabs](#)、[proofpoint](#)、[secureworks](#)、[securityweek](#)）

[20160828]

- 1、[针对叙利亚反对派的网络攻击组织 Group5 被曝光](#)
- 2、[银行木马 Ramnit 变种卷土重来，目标为英国银行](#)
- 3、[研究者发现可破解 HTTPS 流量的 Sweet32 攻击方法](#)
- 4、[研究者发现假冒 Windows 更新的勒索软件 Fantom](#)



- 5、[Dropbox 因 2012 年数据泄露而通知用户重置密码](#)
- 6、[Opera 自动同步服务器遭到入侵，部分数据泄漏](#)

【安天 CERT】搜集整理（来源：[freebuf](#)、[softpedia](#)、[arstechnica](#)、[bleepingcomputer](#)、[sina](#)、[techcrunch](#)）

[20160829]

- 1、[Kelihos 僵尸网络重心移至勒索软件和银行木马](#)
- 2、[研究人员发布分析报告揭示勒索软件 ZEPTO 机理](#)
- 3、[安全厂商:泰国 ATM 窃案或与恶意代码 Ripper 有关](#)
- 4、[研究者发现利用路由器 WIFI 信号可记录用户按键](#)
- 5、[美国特勤局通报两大连锁酒店可能发生数据泄露](#)
- 6、[黑客公开披露入侵多个 Facebook 账户的技术细节](#)

【安天 CERT】搜集整理（来源：[malwaretech](#)、[freebuf](#)、[fireeye](#)、[softpedia](#)、[softpedia](#)、[thehackernews](#)）

[20160830]

- 1、[伊朗石化厂系统发现恶意软件](#)
- 2、[揭秘 iPhone 间谍软件组织 NSO](#)
- 3、[iOS 间谍软件 Pegasus 技术分析](#)
- 4、[斯里兰卡总统网站被黑客攻击](#)
- 5、[澳大利亚政府网络遭黑客攻击](#)
- 6、[幽灵小队入侵以色列银行官网](#)

【安天 CERT】搜集整理（来源：[securityaffairs](#)、[bgr](#)、[freebuf](#)、[softpedia](#)、[sputniknews](#)、[softpedia](#)）

[20160831]

- 1、[新型勒索软件 FairWare 目标为 Linux 服务器](#)
- 2、[安全厂商证实 Angler EK 系由 Lurk 组织开发](#)
- 3、[垃圾邮件活动针对德语用户传播 Ozone 远控](#)
- 4、[谷歌登录页面 BUG 可导致自动下载恶意软件](#)
- 5、[研究人员曝光黑客劫持 Chrome 浏览器新伎俩](#)
- 6、[USBee:由电磁信号突破物理隔离的窃密软件](#)

【安天 CERT】搜集整理（来源：[softpedia](#)、[securityweek](#)、[softpedia](#)、[softpedia](#)、[softpedia](#)、[arstechnica](#)）





微信公众号:AntiyLab

网址:

- ② <http://www.antiy.com> (中文)
- ② <http://www.antiy.net> (英文)
- ② <http://www.antiy.cn> 安天企业安全公司
- ② <http://www.avlsec.com> 安天移动安全公司 (AVL TEAM)

特别申明: 每日安全简讯中的所有链接的文章均为公开渠道获得, 仅仅为安天的客户提供业内网络和信息安全的相关信息和参考使用, 这并不代表我们同意或者支持各自作者的观点和主张; 同时版权以及所有权归各自发表者所有。