

[20160701]

- 1、[安全厂商揭示弱口令 RDP 服务器传播勒索软件细节](#)
- 2、[安全厂商曝光通过 Facebook 消息传播的恶意软件](#)
- 3、[思科安全产品发现严重缺陷，可被攻击者远程控制](#)
- 4、[研究发现过百僵尸网络受 Lizard Stresser DDoS 控制](#)
- 5、[VR 厂商 Oculus CEO 推特账号被偷，发布虚假消息](#)
- 6、[调查表明安装最新安全补丁 Android 设备不足两成](#)

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

[20160702]

- 1、[流行 Linux 办公软件 LibreOffice 被发现任意代码执行漏洞](#)
- 2、[ICS-CERT 公告：西门子电力自动化系统存在安全漏洞](#)
- 3、[Foxit Reader 及 PhantomPDF 任意代码执行漏洞被修补](#)
- 4、[研究人员称恶意软件 Hummer 已感染全球数百万智能手机](#)
- 5、[研究人员称安卓全盘加密可被暴力破解 并公开技术细节](#)
- 6、[调查表明加拿大网民近期频繁收到含网银木马钓鱼邮件](#)

【安天 CERT】搜集整理（来源：[helpnetsecurity](#)、[securityweek](#)、[securityweek](#)、[securityweek](#)、[theregister](#)、[securityaffairs](#)）

[20160703]

- 1、[恶意软件 SBDH 被用于针对中东地区网络间谍活动](#)
- 2、[安全厂商揭露中东地区的定向攻击活动人面狮行动](#)
- 3、[俄罗斯社交网站被植入 RIG EK 传播 Dofoil 后门程序](#)
- 4、[勒索软件新家族 satana，加密用户文件和主引导记录](#)
- 5、[勒索软件 Unlock92 已破解，研究人员发布解密工具](#)
- 6、[Istanbul 行动：匿名者组织重启对恐怖组织攻击行动](#)

【安天 CERT】搜集整理（来源：[welivesecurity](#)、[360](#)、[securityweek](#)、[pcworld](#)、[softpedia](#)、[softpedia](#)）

[20160704]

- 1、[研究人员怀疑勒索软件 Zepto 为 Locky 变种](#)
- 2、[勒索软件 CryptXXX 变种可破坏备份数据](#)
- 3、[交易将可追踪，比特币勒索软件有望终结](#)
- 4、[Thinkpad UEFI Oday 漏洞代码细节被公开](#)
- 5、[安全厂商发布针对欧亚国家 APT 事件报告](#)
- 6、[调查显示针对交通部门网络攻击趋势增长](#)

【安天 CERT】搜集整理（来源：[threatpost](#)、[freebuf](#)、[newsbtc](#)、[github](#)、[bitdefender](#)、[theregister](#)）

[20160705]

- 1、[研究人员发现 SQLite 安全隐患，或可导致泄漏敏感数据](#)
- 2、[安全厂商发布 HummingBad Android 恶意软件分析报告](#)
- 3、[ICS-CERT: Sierra Wireless 即将淘汰工业网关发现漏洞](#)
- 4、[日本大型旅行社服务器被黑，近 800 万人身份信息泄露](#)
- 5、[安全厂商发现加拿大近期频繁遭受六大银行木马攻击](#)
- 6、[5000 万安装量安卓键盘应用，被曝后台收集用户信息](#)

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

[20160706]

- 1、[攻击者利用英国脱欧主题实施电子邮件钓鱼攻击](#)
- 2、[利用 Adwind RAT 木马攻击丹麦企业的行动被曝光](#)
- 3、[勒索软件 MIRCOP 已破解，研究者发布解密工具](#)
- 4、[StartEncrypt 漏洞允许攻击者获得其他域 SSL 证书](#)
- 5、[蜥蜴队 DDoS 攻击升级：转向网上银行和政府网站](#)
- 6、[谷歌修复可利用 Google Docs 实施 XSS 攻击的漏洞](#)

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

[20160707]

- 1、[安全厂商发现利用 Tor 网络的 Mac OS X 后门程序](#)
- 2、[安全厂商揭示针对 Mac OS X 广告软件 OSX.Pirrit](#)
- 3、[研究者发现攻击者在网络钓鱼服务器误留源代码](#)
- 4、[微软 Office 旧漏洞仍在流行，被用于传播恶意软件](#)
- 5、[银行木马 BEBLOH 随近期垃圾邮件攻击传播至日本](#)
- 6、[TP-LINK 路由配置的域名失效，用户面临钓鱼风险](#)

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

[20160708]

- 1、[公安部联合网信办启动网络诈骗举报联动机制](#)
- 2、[Android 将采用新机制遏制快速增长的锁屏勒索](#)
- 3、[安全厂商发现针对 Mac OS X 后门程序 Keydnep](#)
- 4、[Realstatistics 行动：CMS 平台 2000 余网站受感染](#)
- 5、[6338 台 Redis 服务器被攻击 存在被恶意利用风险](#)
- 6、[两种流行 EK 利用 Blackhat-TDS 有选择劫持流量](#)

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

[20160709]

- 1、[安全厂商曝光针对亚洲地区（包括中国）APT 攻击活动](#)
- 2、[安全厂商曝光针对罗马尼亚等国家 APT 攻击活动 Pacifier](#)
- 3、[安全厂商揭露由 Rig EK 传播的勒索软件 CryptoBit 新版本](#)
- 4、[点击欺诈软件 Kovter 不断演化，新版本伪装成火狐更新](#)
- 5、[研究者发现 Linux 发行版仍未修补 wget 远程代码执行漏洞](#)
- 6、[美国温迪快餐连锁集团透露逾千家餐馆感染 PoS 恶意代码](#)

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

[20160710]

- 1、[Angler EK 和 Nuclear EK 沉寂后 Sundown EK 崛起](#)
- 2、[勒索软件 CryptXXX 再更新，原解密工具已失效](#)
- 3、[勒索软件 BitStak 被破解，研究人员发布解密工具](#)
- 4、[Find My iPhone 勒索回归，针对美国和欧洲用户](#)
- 5、[安全厂商：英国网络犯罪已超过传统犯罪比例](#)
- 6、[研究者发现在手机播放视频可导致被黑客入侵](#)

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

[20160711]

- 1、[僵尸网络 Kelihos 通过荷兰语主题邮件传播勒索软件](#)
- 2、[山寨版 Pokemon GO 传播恶意软件 DroidJack RAT](#)
- 3、[黑客可利用 Oday 漏洞对宝马在线服务网站发起攻击](#)
- 4、[亚马逊服务器被黑，8 万 Kindle 用户登录凭证泄露](#)
- 5、[Penton 三家网站被黑，170 万用户数据在暗网出售](#)
- 6、[Facebook 向部分 Messenger 用户提供端到端加密选项](#)

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

[20160712]

- 1、[安天发布“白象”报告 披露针对我国多领域的 APT 攻击行动](#)
- 2、[研究人员发现新勒索软件 Alfa，开发者或为 CERBER 作者](#)
- 3、[Jigsaw 勒索软件再次被破解，研究人员已经提供解密工具](#)
- 4、[乌克兰黑客入侵波兰电信公司服务器 泄漏数据被地下出售](#)
- 5、[云平台监控服务商 Datadog 发生数据泄露 通知用户改密码](#)
- 6、[安全厂商发布工业控制网络安全威胁调查统计报告](#)

【安天 CERT】搜集整理（来源：[antiy](#)、[softpedia](#)、[checkpoint](#)、[securityaffairs](#)、[theregister](#)、[securelist](#)）

[20160713]

- 1、[漏洞预警：Struts2 devMode 导致远程代码执行漏洞](#)
- 2、[台湾第一银行 34 台 ATM 机被植入恶意软件，盗领 7 千万台币](#)
- 3、[研究人员发现数千网站被入侵，传播勒索软件 CryptXXX](#)
- 4、[研究人员开发出 Windows 版勒索软件检测、阻止工具软件](#)
- 5、[Omni 旗下酒店 POS 终端感染恶意代码，感染时间超 6 个月](#)
- 6、[Africa 行动：南非官方武器采购机构遭入侵，交易记录泄露](#)

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

[20160714]

- 1、[阿里安全峰会召开，集结最强阵容打造安全生态圈](#)
- 2、[微软打印机协议发现漏洞，影响 Windows 所有版本](#)
- 3、[Intel 核显驱动程序曝漏洞，攻击者可执行任意代码](#)
- 4、[WordPress 多个插件存有跨站脚本漏洞 现已被修复](#)
- 5、[研究人员称 Pokemon Go iOS 版可大量获取用户信息](#)
- 6、[暗网出现针对能源公司恶意软件，怀疑受政府支持](#)

【安天 CERT】搜集整理（来源：[china](#)、[softpedia](#)、[cisco](#)、[securityweek](#)、[magazine](#)、[securityaffairs](#)）

[20160715]

- 1、[研究人员发现勒索软件 Locky 新变种可离线加密](#)
- 2、[勒索软件新变种 Ranscam，收钱后删除用户文件](#)
- 3、[安全厂商发现暗网低价出售勒索软件变种及服务](#)
- 4、[Drupal 出现 RCE 漏洞，可被攻击者利用劫持网站](#)
- 5、[黑客入侵印度银行盗取 13 亿卢比，已经被抓获](#)
- 6、[美国 NSA 称将加大对 Tor 和 Linux 用户监听力度](#)

【安天 CERT】搜集整理（来源：[softpedia](#)、[cisco](#)、[magazine](#)、[theregister](#)、[manoramaonline](#)、[securityaffairs](#)）

[20160716]

- 1、[研究人员发现针对中国勒索软件 cuteRansomware](#)
- 2、[勒索软件 CryptXXX 部分版本解密密钥可免费获得](#)
- 3、[安卓木马变种 Fakebank 具有银行客服电话屏蔽功能](#)
- 4、[微软某漏洞源码公开后已快速被 Neutrino EK 采用](#)
- 5、[Juniper 存在高危漏洞，攻击者可使获得管理员权限](#)
- 6、[波兰国防部被入侵勒索，或与俄罗斯极端组织有关](#)

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

[20160717]

- 1、[文档转换应用藏有 Mac 后门，可远程控制摄像头](#)
- 2、[安全团队发现暗云 II BootKit 木马随游戏外挂传播](#)
- 3、[纽约大学研究发现，3D 打印面临网络安全威胁](#)
- 4、[Ubuntu 论坛被黑客攻击，逾 200 万用户信息泄露](#)
- 5、[研究者发现首个采用锁屏方式色情点击恶意程序](#)
- 6、[研究人员称在暗网发现了首个“圈内人威胁木马”](#)

【安天 CERT】搜集整理（来源：bitdefender、wooyun、educationdive、thehackernews、welivesecurity、securityweek）

[20160718]

- 1、[KeyBase 键盘记录器被用于窃取信息，作者宣布终止项目](#)
- 2、[微软最新调查报告显示东南亚国家为恶意代码感染重灾区](#)
- 3、[Pokemon Go 服务器遭 DDoS 攻击，PoodleCorp 宣布负责](#)
- 4、[Juniper 公司公钥应用漏洞，攻击者可以窃听路由设备流量](#)
- 5、[俄罗斯黑客入侵 4000 万 iCloud 账号，用户需付费解锁手机](#)
- 6、[研究人员发现飞利浦医疗产品大量高危漏洞，厂商已修复](#)

【安天 CERT】搜集整理（来源：softpedia、globe、gizmodo、threatpost、people、securityweek）

[20160719]

- 1、[间谍软件利用远控工具 Ammyy Admin 官方网站下载传播](#)
- 2、[企业研发人员盛行使用开源代码 Java 组件安全漏洞蔓延](#)
- 3、[安全公司澄清：无证据表明恶意软件 SFG 针对工控系统](#)
- 4、[票务网站大麦网遭黑客“撞库”攻击，39 人被骗 147 万元](#)
- 5、[台湾第一银行 ATM 机现金遭盗领案进展：三嫌疑人被抓](#)
- 6、[黑客滥用语音验证，每年骗谷歌微软等公司数百万欧元](#)

【安天 CERT】搜集整理（来源：securelist、softpedia、theregister、cnr、toutiao、softpedia）

[20160720]

- 1、[安全厂商分析揭露勒索软件 Cerber 攻击方法](#)
- 2、[包含恶意宏的德语钓鱼邮件攻击行动被发现](#)
- 3、[僵尸网络仙女座对意大利发动垃圾邮件攻击](#)
- 4、[Mac 防火墙严重漏洞，可内核执行任意代码](#)
- 5、[Steem 社交网络遭入侵，用户帐户资金被窃](#)
- 6、[HTTPoxy 漏洞，可导致 Web 应用程序受攻击](#)

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

[20160721]

- 1、[研究者发现可通过 MMS 消息入侵 iPhone 手机](#)
- 2、[比萨连锁店顾客支付信息被 PoS 恶意代码窃取](#)
- 3、[英国铁路网络在去年遭到四次黑客网络攻击](#)
- 4、[ASN.1 编译器存漏洞，可致网络设备受攻击](#)
- 5、[Tor 核心人员退出项目，关闭多个重要 Tor 节点](#)
- 6、[勒索软件 Petya 升级，提高加密磁盘恢复难度](#)

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

[20160722]

- 1、[Python 编写的勒索软件 HolyCrypt 出现](#)
- 2、[勒索软件 CryptXXX 山寨版 CryMIC 出现](#)
- 3、[研究人员发布勒索软件 Bart 解密工具](#)
- 4、[Sofacy 组织被发现使用新的持久化方法](#)
- 5、[匿名者组织 DDoS 攻击里约法院网站](#)
- 6、[戴尔网络安全产品被发现严重漏洞](#)

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

[20160723]

- 1、[韩国超 16 万用户受到 BlackMoon 银行木马感染](#)
- 2、[大量商业网站被恶意软件 SoakSoak 攻击](#)
- 3、[勒索软件 PowerWare 变种模仿勒索软件 Locky](#)
- 4、[斯诺登设计 iPhone 无线监听检测阻断外壳](#)
- 5、[多家主要厂商产品受甲骨文 OIT 库漏洞影响](#)
- 6、[厂商继续揭秘 Facebook 恶意软件工作机理](#)

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

[20160724]

- 1、[研究人员发布勒索软件 ODCODC 解密工具](#)
- 2、[勒索软件团伙称曾受雇 500 强企业攻击对手](#)
- 3、[勒索软件 CTB-Locker 出现模仿者 CTB-Faker](#)
- 4、[香港卫生署信息系统被黑 10 万人或受影响](#)
- 5、[匿名者对土耳其煤气公司数据库发起攻击](#)
- 6、[两大游戏公司 230 万用户记录遭数据泄露](#)

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

[20160725]

- 1、[研究人员发布勒索软件 Bart 及 PowerWare 解密工具](#)
- 2、[研究人员怀疑 Carbanak 行动或与俄安全公司有关](#)
- 3、[黑客在暗网销售包含所有美国选民信息的数据库](#)
- 4、[入侵名人邮件账户的美国黑客被判有期徒刑半年](#)
- 5、[法国机构警告微软：停止采集 Win10 用户数据](#)
- 6、[谷歌将对 Android7.0 严格执行验证启动安全功能](#)

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

[20160726]

- 1、[研究者发现 Hackhound 及其 C2 被用于工业间谍活动](#)
- 2、[勒索软件 Stampdado 被破解，解密工具已免费发布](#)
- 3、[攻击者利用 Twitter 公司 Docker 漏洞下载 Vine 源代码](#)
- 4、[PHP 0day 漏洞，允许攻击者以上帝模式访问网站](#)
- 5、[研究者利用洋葱蜜罐发现百余个暗网窥探节点](#)
- 6、[韩国网购网站疑因钓鱼邮件泄漏 10 万客户数据](#)

【安天 CERT】搜集整理（来源：mcafee、bleepingcomputer、softpedia、theregister、securityweek、koreaherald）

[20160727]

- 1、[安天 AVL 联合猎豹曝光仿冒知名游戏手机病毒](#)
- 2、[安全厂商发现 Patchwork 组织拓展攻击目标范围](#)
- 3、[研究人员怀疑一人与多个勒索软件家族有所关联](#)
- 4、[多家 IT 安全公司与执法部门联合对抗勒索软件](#)
- 5、[安全厂商发现无线键盘可被监听及注入恶意命令](#)
- 6、[Win10 磁盘清理工具可被恶意代码利用绕过 UAC](#)

【安天 CERT】搜集整理（来源：avlsec、symantec、cisco、kaspersky、softpedia、softpedia）

[20160728]

- 1、[研究者发现传播恶意远控 App 的推特账号，或用于监听 ISIS](#)
- 2、[Petya 和 Mischa 勒索软件作者披露勒索软件 Chimera 解密密钥](#)
- 3、[勒索软件 Locky 变种 Zepto 新版本由纯 JS 实现，利用邮件传播](#)
- 4、[研究人员发现网银木马 Chthonic 利用 PayPal 官方电子邮件传播](#)
- 5、[研究人员破解 Mad Max 僵尸网络混淆域名生成算法](#)
- 6、[美国总统奥巴马建立网络攻击指挥响应链](#)

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

[20160729]

- 1、[WPAD 协议和 PAC 文件可泄露用户访问网站 HTTP 流量](#)
- 2、[研究人员发现勒索软件 Petya 和 Mischa 以服务形式出现](#)
- 3、[LastPass 密码管理器出现严重漏洞，可泄露已存储密码](#)
- 4、[研究者曝光利用亚马逊隐藏订单功能的新型钓鱼骗术](#)
- 5、[调查表明俄罗斯网站 Deer.io 为网络犯罪提供一站式服务](#)
- 6、[欧盟数据保护官员建议采用端到端加密保护隐私通讯](#)

【安天 CERT】搜集整理（来源：softpedia、securityweek、magazine、qq、digitalshadows、techdirt）

[20160730]

- 1、[无需 Root 权限新型 Android 木马 SpyNote 在多个论坛泄露](#)
- 2、[韩国大型在线零售商数据泄露，媒体称遭 30 亿韩元勒索](#)
- 3、[安全厂商推出勒索软件检测工具，可检测未知勒索软件](#)
- 4、[研究者发现 AdGhlolas 恶意广告活动每天受害者达百万](#)
- 5、[Google 将在安卓核心代码中加入更多 Linux 内核防御机制](#)
- 6、[加密技术突破：研究人员使用双源提取器获得真正随机数](#)

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

[20160731]

- 1、[2015 年 DNC 服务器被黑客攻击或因心脏出血漏洞](#)
- 2、[研究者称二维码登录劫持技术成为新社工攻击手法](#)
- 3、[调查表明访问盗版电影网站感染病毒几率相对更高](#)
- 4、[研究表明代理服务器配置缺陷可泄露 HTTPS 访问 URL](#)
- 5、[SQLite 默认设置缺陷使 WhatsApp 无法删除聊天记录](#)
- 6、[统计显示超过三成 WEB 攻击和漏洞利用来源为美国](#)

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



微信公众号:AntiyLab 网址:www.antiy.com

特别申明：以上所有链接的文章的均为公开渠道获得，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。