

[20160601]

- 1、[USCERT: ESC 电厂数据控制器漏洞难修补，或被远程利用](#)
 - 2、[研究人员发现加州天然气电力公司数据库敏感数据发生泄露](#)
 - 3、[Tumblr 6500 万用户信息泄露，黑客在暗网廉价出售泄露信息](#)
 - 4、[FrameworkPos 恶意代码变种使美国中小企业 POS 设备受感染](#)
 - 5、[间谍组织 Stealth Falcon 利用恶意代码监控阿联酋记者被曝光](#)
 - 6、[伊朗政府要求所有即时通讯应用需将公民数据在其国内存储](#)
- 安天 CERT 搜集整理（来源：theregister、securityweek、thehackernews、news-press、networkworld）

[20160602]

- 1、[研究人员发现三星 KNOX 平台漏洞，影响 BYOD 企业网络安全](#)
- 2、[Windows 被发现本地提权 0-Day 漏洞，覆盖 Win2K 以上各版本](#)
- 3、[勒索软件 Zcrypt 表现出蠕虫特性，利用 U 盘和网络驱动器传播](#)
- 4、[我国安全研究人员公开全球 24 款反病毒软件存在的安全漏洞](#)
- 5、[朝鲜山寨版 Facebook 内测时因管理员弱口令遭黑客攻击下线](#)
- 6、[敏捷开发培训认证网站 Scrum.org 遭到入侵，帐户信息泄露](#)

安天 CERT 搜集整理（来源：softpedia、ibtimes、theregister、四叶草安全、sohu、securityweek）

[20160603]

- 1、[安全厂商发现概念验证型工业控制系统恶意代码家族 IRONGATE](#)
- 2、[安卓间谍软件伪装聊天应用，窃取沙特阿拉伯政府安全求职者信息](#)
- 3、[Lilence 行动：“幽灵小队”对福克斯和 CNN 新闻网站发动 DDoS 攻击](#)
- 4、[SWIFT 攻击第三波：黑客转账 1 千 2 百万美元到香港、迪拜和美国](#)
- 5、[安全厂商发布报告，解读黑客攻击银行 SWIFT 系统所使用的技术](#)
- 6、[用户反映攻击者利用 TeamViewer 盗取用户信息，TeamViewer 否认](#)

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

[20160604]

- 1、[Dridex 勒索软件卷土重来，伪装成证书逃避杀软检测](#)
- 2、[WP 手机插件漏洞，使全球上万 WordPress 网站受影响](#)
- 3、[安全厂商曝光巴基斯坦 APT 组织对印度政府攻击行动](#)
- 4、[篡改主机 DNS 指向恶意服务器的 DNS Unlocker 被发现](#)
- 5、[安全厂商发布勒索软件 CryptXXX 变种新特性分析报告](#)
- 6、[手机银行木马 Marcher 新变种，英国银行加入攻击列表](#)

【安天 CERT】搜集整理（来源：softpedia、securityaffairs、fireeye、welivesecurity、proofpoint、securityintelligence）

[20160605]

- 1、[研究人员破解勒索软件 BadBlock，免费提供解密工具](#)
- 2、[勒索软件 CERBER 逃避检测新手段，每 15 秒变形一次](#)

- 3、[安全厂商披露恶意软件绕过安卓最新安全机制技术细节](#)
- 4、[安全厂商预警：Struts2 最新高危漏洞官方修复方案无效](#)
- 5、[安全厂商揭示 POS 机恶意代码新变种快速窃取信息手段](#)
- 6、[罗马尼亚黑客 GhostShell 公开 MongoDB 泄露数据超 5GB](#)

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

[20160606]

- 1、[美国高校研究人员开发出芯片内部硬件级别后门](#)
- 2、[以色列研究者演示利用 PC 噪音盗取 RSA 密钥方法](#)
- 3、[匿名者组织泄露南非铂金矿业公司百人帐户信息](#)
- 4、[SS7 协议弱点令 IM 应用程序端到端加密形同虚设](#)
- 5、[FBI 所谓“网络调查技术”：恶意代码明文回传证据](#)
- 6、[微软近期报告显示：九成恶意网页利用 Flash 漏洞](#)

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

[20160607]

- 1、[安全厂商发现 Angler EK 已经具备绕过微软 EMET 的能力](#)
- 2、[研究人员发现针对 Magento 用户的信用卡信息窃取木马](#)
- 3、[俄罗斯最大社交网站 VK.com 被黑，1.71 亿用户账号出售](#)
- 4、[沙特阿拉伯黑客组织接管扎克伯格 Twitter、Pinterest 帐号](#)
- 5、[号称最安全比特币交易服务商 BitGo 遭大规模 DDoS 攻击](#)
- 6、[厂商确认：饿了么某处设计不当，泄露大量用户手机号](#)

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

[20160608]

- 1、[攻击者假冒 Skype 帐户针对美国签证申请者传播恶意代码 QRAT](#)
- 2、[安全厂商发现攻击者在 Shellcode 中滥用 COM 技术躲避杀软检测](#)
- 3、[安全厂商揭露仿冒苹果域名的 Zycode 钓鱼攻击，针对中国用户](#)
- 4、[研究人员发现使用 Zeus 和 Carbeep 技术的银行木马，针对俄罗斯](#)
- 5、[Icarus 行动：匿名者组织对伦敦证券交易所网站发动了 DDoS 攻击](#)
- 6、[研究者发现恶意软件利用微软 BITS 服务在清除后重新感染计算机](#)

【安天 CERT】搜集整理（来源：secure、mcafee、fireeye、techweekeurope、sputniknews、softpedia）

[20160609]

- 1、[加拿大大学遭勒索软件感染，被迫支付 2 万加元赎回被加密文件](#)
- 2、[勒索软件全球范围扩散，部分企业开始储备比特币应对勒索威胁](#)
- 3、[研究人员发现 Facebook 消息应用漏洞，攻击者可以替换聊天内容](#)
- 4、[LinkedIn 泄露的个人资料被用于在荷兰发起针对性钓鱼邮件攻击](#)

- 5、[Akamai 发布 2016 年第一季度互联网安全报告：DDoS 攻击量激增](#)
- 6、[研究人员发现 D-Link Wi-Fi 摄像头漏洞，黑客可远程获取监控内容](#)

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

[20160610]

- 1、勒索软件 [SNSLocker](#) 代码中未发现 C&C 服务器登录凭证
- 2、安全厂商发现跨平台恶意软件 [Crysis](#) 已具有勒索软件特性
- 3、[3200 万 Twitter 用户帐户密码在暗网出售，官方否认泄露](#)
- 4、研究人员在欧洲议会与欧盟委员会网站发现 [SQL 注入漏洞](#)
- 5、研究者发现 [Office](#) 恶意宏代码使用新的反虚拟机/沙盒手段
- 6、[uTorrent 论坛被黑，攻击者通过论坛软件供应商入侵窃取信息](#)

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

[20160611]

- 1、谷歌修复 [Chrome](#) 图片解析漏洞：攻击者可用恶意代码控制主机
- 2、安全厂商发现勒索软件 [JIGSAW](#) 采用网页聊天方式进行勒索尝试
- 3、安全厂商统计：[RansomWeb](#) 勒索攻击今年发生频率为去年五倍
- 4、研究人员发现黑帽 [SEO](#) 活动，通过 [SQL 注入](#) 感染至少 700 台主机
- 5、[Icarus](#) 行动：匿名者黑客组织计划对全球证券交易所发动 [DDoS](#)
- 6、[VMware](#) 更新严重漏洞：攻击者可利用漏洞远程访问敏感信息

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

[20160612]

- 1、[世界最大僵尸网络 Necurs](#) 或已被瓦解
- 2、勒索软件感染美国俄亥俄州地方政府
- 3、[CryptXXX](#) 活动转移至 [Neutrino EK](#)
- 4、[Carberp](#) 继承者银行木马 [Bolek](#) 正崛起
- 5、安全厂商警告联网智能汽车或遭勒索
- 6、安全厂商：云应用恶意软件呈上升趋势

【安天 CERT】搜集整理（来源：[securityaffairs](#)、[dispatch](#)、[securityweek](#)、[fireeye](#)、[crn](#)）

[20160613]

- 1、邮件服务故障导致 7618 个 [Let's Encrypt](#) 用户邮件地址信息泄露
- 2、匿名者组织黑入 [ISIS](#) 支持者 [twitter](#) 账号，并替换为成人主题背景
- 3、安全团队改进解密工具支持 [Teslacrypt](#) 新变种所加密文件的恢复
- 4、安全厂商发现 [TeleScope](#) 实时解密技术 可实现 [TLS](#) 协议通信窃听
- 5、报告称去年台湾平均每天有 72000 台移动设备受到恶意软件感染
- 6、[社工手段](#)达到新水平，攻击者冒用谷歌身份绕过谷歌双因素验证

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

[20160614]

- 1、[已停用的 iMesh 文件共享服务泄露 5100 万条用户记录，并在黑市出售](#)
- 2、[匿名黑客针对南非广播公司 SABC 主要电视和电台频道发起 DDoS 攻击](#)
- 3、[新型银行木马 Bolek，结合 Zeus 和 Carberp 木马源代码攻击俄罗斯银行](#)
- 4、[韩国称朝鲜向其 14 万台电脑植入恶意代码，计划发动大规模网络攻击](#)
- 5、[三菱公司承认其欧蓝德 PHEV 车型存在安全漏洞，可被黑客远程控制](#)
- 6、[研究者揭露短信拦截马工作机理：黑产如何强刷用户银行卡 8.1 万元？](#)

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

[20160615]

- 1、[勒索软件 Flocker 感染 Android OS 智能电视，锁屏勒索 iTunes 礼品卡](#)
- 2、[研究人员发现银行木马 Vawtrack v2 活跃 目标范围扩大至更多国家](#)
- 3、[PhotoMiner 蠕虫通过不安全 FTP 服务器感染托管网站并持久化驻留](#)
- 4、[美国 NSA 及情报机构：不排除通过入侵物联网医疗设备收集情报](#)
- 5、[路透社称朝鲜黑客从韩国窃取美国战斗机蓝图，但并非机密文档](#)
- 6、[黑客在暗网出售 29 万美国公民驾照记录，包括公民详细个人信息](#)

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

[20160616]

- 1、[因设计问题 Windows 存 BadTunnel 漏洞 20 年，Win95 以上均受影响](#)
- 2、[勒索软件新家族 RAA，完全使用 JavaScript 代码实现感染目标系统](#)
- 3、[安全厂商发现俄罗斯 APT28 组织对美国政府机构发起钓鱼攻击](#)
- 4、[Verizon 邮件漏洞，允许攻击者针对性劫持用户邮件到任意地址](#)
- 5、[全新的移动应用合谋攻击：不同应用程序协作来进行恶意操作](#)
- 6、[安全厂商发现 IOS 版移动广告 SDK 包含允许攻击者远程窃密代码](#)

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

[20160617]

- 1、[微软 OLE 技术被滥用，将恶意代码嵌入 Office 文档，类似宏病毒](#)
- 2、[黑客 Guccifer 2.0 承认为 DNC 攻击事件负责，并披露部分泄露文件](#)
- 3、[安全厂商披露 APT 组织 ScarCruff 利用 Flash 0day 漏洞攻击高价值目标](#)
- 4、[US CERT 警告：西门子 SIMATIC flexible 工控软件漏洞，可远程利用](#)
- 5、[思科公司无线套件关键漏洞被曝光，可绕过身份验证执行任意代码](#)
- 6、[加拿大公司 VerticalScope 被黑客入侵，超过千家网站 4500 万密码泄露](#)

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

[20160618]

- 1、[研究人员曝光 Intel x86 处理器存在无法审计的独立隐藏芯片](#)
- 2、[安天发布远程控制木马预警：假借知名应用植入恶意模块](#)
- 3、[研究者发现 Nemucod 恶意代码采用多重混淆逃避杀软检测](#)
- 4、[调查统计表明：免费体育直播网站中五成广告为恶意广告](#)
- 5、[Adobe 公司紧急修复被 APT 组织 ScarCruft 所利用的 0day 漏洞](#)
- 6、[代码库网站 GitHub 警告：部分帐户已被攻击者通过撞库获取](#)

【安天 CERT】搜集整理（来源：slashdot、avlsecc、softpedia、memeburn、securityweek、thehackernews）

[20160619]

- 1、[勒索软件新家族 Crypt38 使用简单加密算法，已被成功破解](#)
- 2、[研究表明美国超过 6 千台摄像头无访问密码，存在安全隐患](#)
- 3、[黑客利用编程漏洞获取价值 5000 万美元网络虚拟货币以太币](#)
- 4、[北约正式声明网络空间为第五空间，网络攻击将被视为战争](#)
- 5、[宏基声称其电子商务网站数据泄漏，影响信用卡号码等信息](#)
- 6、[TeamView 余波危机，英国运营商 TalkTalk 用户深陷水火](#)

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

[20160620]

- 1、[加拿大政党视频会议系统因弱口令遭黑客入侵，视频内容被泄露](#)
- 2、[美国民主党全委会入侵后续：黑客披露捐助人信息和党内财务记录](#)
- 3、[德国安全专家称 ISIS 黑客组织 Cyber Caliphate 或为俄罗斯幕后支持](#)
- 4、[审计表明：FBI 面部识别数据库 4 亿图片不够精确且缺少隐私保护](#)
- 5、[印度称其警方已具备破解黑莓和中国手机能力，正着手破解 iPhone](#)
- 6、[安全厂商报告显示，83%受测企业网络的 DNS 存在恶意活动迹象](#)

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

[20160621]

- 1、[比特币采矿恶意代码活动借助社会工程手段死灰复燃](#)
- 2、[钓鱼攻击新伎俩：从网址托管公司租用临时 URL 地址](#)
- 3、[ISIS 黑客组织威胁美驻韩空军基地：利用 IM 获取 GPS](#)
- 4、[T-Mobile 捷克公司 150 万客户信息泄露，面临钓鱼威胁](#)
- 5、[2 月份有攻击者尝试用僵尸网络攻击 2 亿金融机构邮箱](#)
- 6、[安全厂商发现被黑 RDP 服务器在黑市贩卖，来源成谜](#)

【安天 CERT】搜集整理(来源: fireeye、softpedia、chosun、theregister、slashdot、securelist)

[20160622]

- 1、[安全厂商发现 RAA 勒索软件新特性: 可窃取用户密码和比特币钱包](#)
- 2、[安全厂商发现巴西地下黑客兜售 Mangit 银行木马, 已成为产品服务](#)
- 3、[美国民主党全委会入侵后续: 美国厂商称攻击者受俄罗斯政府支持](#)
- 4、[Pawost 安卓木马利用 Google Talk 呼叫未登记号码, 目标为中国用户](#)
- 5、[苹果修复 Airport 设备 DNS 解析漏洞, 可被攻击者用于执行任意代码](#)
- 6、[安全厂商揭示去年 DUBNIUM 攻击行动中的 Adobe 漏洞利用技术细节](#)

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

[20160623]

- 1、[工信部将建国家级网络安全信息共享数据库](#)
- 2、[安全团队曝光定向攻击的 JavaScript 远控木马](#)
- 3、[三百万 Twitter 帐户僵尸网络, 或被用于 C&C](#)
- 4、[Conficker 蠕虫仍在活跃, 占已知攻击的 14%](#)
- 5、[世界最大僵尸网络 Necurs 的 C&C 再度活跃](#)
- 6、[恶意代码 Godless 具备多种 root 安卓设备能力](#)

【安天 CERT】搜集整理(来源: cankaoxiaoxi、freebuf、slashdot、securityaffairs、softpedia、trendmicro)

[20160624]

- 1、[黑客攻击美国公司 无意间泄露 1.54 亿具有价值选民个人信息](#)
- 2、[GozNym 银行木马利用重定向攻击技术对美国金融界发起攻击](#)
- 3、[印度最大的移动广告公司 InMobi 被曝秘密跟踪用户位置信息](#)
- 4、[开源压缩工具包 Libarchive 出现安全漏洞 几百个项目受影响](#)
- 5、[安全厂商称 Crypto 勒索软件攻击上升五倍 受害用户超过 70 万](#)
- 6、[Google 推出“谷歌提示”推送通知方式, 简化双因子验证方式](#)

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

[20160625]

- 1、[攻击者利用由 1C 语言编程的木马在俄罗斯企业传播勒索软件](#)
- 2、[研究人员发现 POS 机恶意软件 PunkeyPOS 感染美国 200 家企业](#)
- 3、[手机银行木马 Marcher, 发送 SMS 促使受害者启动钓鱼目标应用](#)
- 4、[安全厂商发布针对日本企业后门木马 Elirks 变种跟踪分析报告](#)
- 5、[即时用车软件 Uber 网站和服务器存在漏洞 可泄露乘客个人信息](#)
- 6、[研究发现通过 CPU、机箱风扇转速突破物理隔离泄露数据方法](#)

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

[20160626]

- 1、勒索软件 [Locky](#) 继续活跃 增加沙箱逃避技术
- 2、勒索软件新家族 [MIRCOP](#) 索高额比特币赎金
- 3、针对德语国家木马 [DEloader](#) 通过 [JS](#) 脚本传播
- 4、[Silence](#) 行动：幽灵小队泄露美军 3400 人数据
- 5、[PayPal](#) 漏洞：可在支付页面插远程恶意图片
- 6、[Facebook](#) 逻辑缺陷：黑客可删评论中视频

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

[20160627]

- 1、新型勒索软件 [Bart](#)，可离线完成加密过程
- 2、美国证券账户被黑，黑客以非法交易牟利
- 3、银行木马 [Dridex](#) 卷土重来，美国为重灾区
- 4、[Tor](#) 洋葱浏览器升级，追踪难度进一步增加
- 5、能源设备发现漏洞，可远程读取设备内存
- 6、[POS](#) 机木马 [Punkey](#)，窃取百万信用卡信息

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

[20160628]

- 1、银行木马 [Reteffe](#) 利用根证书攻击英国银行客户
- 2、美国机场将索取入境人员社交媒体活动记录
- 3、街拍网站 [Lookbook.nu](#) 的 110 万用户信息泄露
- 4、美国三家医疗机构数据库 65 万患者信息泄露
- 5、[Intel](#) 欲放弃网络安全市场，将出售 [McAfee](#) 业务
- 6、[Swagger](#) 框架曝 [RCE](#) 漏洞，影响众多开发语言

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

[20160629]

- 1、大量受感染的闭路电视摄像机卷入 [DDoS](#) 攻击
- 2、[Google](#) 商店 [LevelDropper](#) 暗藏静默 [root](#) 恶意代码
- 3、勒索软件 [CERBER](#) 大量感染 [Office](#) 企业版用户
- 4、针对欧洲的钓鱼短信传播手机木马活动被发现
- 5、黑客窃取 930 万条医疗保险信息，在暗网出售
- 6、黑客利用 [SWIFT](#) 漏洞窃取乌克兰银行千万美金

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

[20160630]

- 1、[俄 APT 组织对多个目标的谷歌邮箱展开钓鱼攻击](#)
- 2、[安全厂商产品出现严重漏洞，用户可被远程攻击](#)
- 3、[安全厂商挫败疑为伊朗组织发起的网络间谍活动](#)
- 4、[风险情报机构 World-Check 被黑，220 万数据泄露](#)
- 5、[美国 Hard Rock 酒店和赌场受 PoS 恶意代码攻击](#)
- 6、[AVLTeam 预警：丹麦“支付宝”MobilePay 被盯上了](#)

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



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。