每日安全简讯

[20160501]

1、研究人员发现攻击者利用仿冒谷歌 Chrome 更新包传播移动恶意软件
2、木马 BPlug 隐藏于 Chrome 拓展程序，诱引点击虚假 Facebook 恶意链接
3、研究人员发现勒索软件 TrueCrypter 支付环节可绕过 一个按钮即可解密
4、包含 Slack 访问令牌的代码在 GitHub 公开，可导致开发者敏感数据泄露
5、研究人员发现，恶意软件 Dridex 卷土重来，攻击目标转向美国
6、受钓鱼邮件攻击 美国兰顿技术学院近 800 员工私人数据遭泄露

安天 CERT 搜集整理（来源：softpedia、securityweek、seattletimes）

[20160502]

1、最流行网络黑市 Alphabay 存在安全漏洞，可泄露用户隐私数据
2、因员工打开钓鱼邮件附件 勒索软件破坏公司电力以及供水系统
3、研究人员发现勒索软件 Lokey 借 Flash 和 Windows 内核漏洞传播
4、美国牙医协会因包含恶意代码 USB 驱动致数千牙科诊所受感染
5、研究人员称每年约有 6000 万网络攻击针对沙特阿拉伯公共机构
6、研究人员发现 Google Play 多款应用通过网络钓鱼盗取用户钱财

安天 CERT 搜集整理（来源：securityaffairs、freebuf、trendmicro、magazine、saudigazette、digitaltrends）

[20160503]

1、澳洲企业家克雷格·赖特公开承认自己为比特币发明人中本聪
2、密歇根州参议员提出法律草案：给予破解汽车黑客终身监禁
3、研究人员破解勒索软件家族 Alpha 加密算法，可为受害者解密
4、菲律宾警方宣称成功逮捕第二名参与选民信息泄漏事件黑客
5、"幽灵小队"黑客组织因种族主义攻击黑人生命物质运动网站
6、攻击卡塔尔银行黑客将放出另一银行数据 或被勒索软件使用

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

[20160504]

1、安全厂商发布恶意代码 Infy 十年来针对性攻击行动报告
2、勒索软件攻击新途径：通过暴力破解的 RDP 服务器部署
3、三星智能家居系统存在漏洞，攻击者可获取门锁控制权
4、研究人员逆向巴厘岛 ATM 盗刷装置，发现存储密码视频
5、Pwnedlist 网站电子邮件服务曝漏洞 8.66 亿用户信息泄露
6、研究人员发现：电子病历经常成为勒索软件攻击目标

安天 CERT 搜集整理（来源：paloaltonetworks、fox-it、arstechnica、theregister、claimsjournal）

[20160505]
1、开源图像处理库 ImageMagick 曝远程代码执行 0day 漏洞
2、研究人员发现 Lost Door 远控木马在社交网站广泛传播
3、Icarus 行动：匿名者组织对希腊央行网站发动 DoS 攻击
4、Icarus 行动：匿名者组织威胁对全球金融机构发动攻击
5、WordPress 插件 bbPress 存跨站脚本漏洞，影响 30 万网站
6、OpenSSL 修补严重漏洞：可执行任意代码及发动 DoS 攻击

安天 CERT 搜集整理（来源：theregister、trendmicro、thepeninsulaqatar、ibtimes、softpedia、securityweek）
[20160506]
1、ImageMagick 漏洞影响扩大，CNNVD 发布分析情况通报
2、App Store 疑似被黑，微信、搜狗输入法等国民级应用躺枪
3、数亿谷歌雅虎微软电邮账号被盗，在俄罗斯黑市低价交易
4、勒索软件新家族 CrpytMix 声称将部分赎金捐给慈善组织
5、Google Play 商店再度出现恶意 App 或只针对俄罗斯用户
6、研究人员发现 Jaku 僵尸网络实施针对性攻击 疑为朝鲜发动

安天 CERT 搜集整理（来源：CNNVD、toutiao、163、softpedia、theregister）
[20160507]
1、 Icarus 行动：匿名者组织对塞浦路斯央行发动大规模 DDoS 攻击
2、WordPress 再曝漏洞 攻击者可将请求重定向至恶意 url
3、SpeedCharge 锁屏 app 恶意广告 可绕过 PIN 和指纹验证访问链接
4、安全厂商发现高通设备漏洞 5 年内多数安卓设备受该漏洞影响
5、安全厂商发布一季度威胁报告 勒索软件及网银木马感染量增加
6、研究者发现黑客攻击勒索软件传播渠道 替换 Locky 为无害程序

安天 CERT 搜集整理（来源：softpedia、fireeye、securelist、securityweek）
[20160508]
1、安全厂商发现勒索软件家族 Bucbi 新变种
2、阿联酋投资银行遭入侵，信用卡信息泄露
3、联想修复其预装软件的本地提权安全漏洞
4、邮件服务商称 2.72 亿泄露邮件信息多数无效
5、印度电信部长称印度已研发 iPhone 破解工具
6、黑客公开出售成人网站 4000 万泄露账户信息

安天 CERT 搜集整理（来源：paloaltonetworks、ibtimes、securityaffairs、cnet、feng、softpedia）
[20160509]
1、攻击者利用 Skype 垃圾邮件发送伪装成图片的木马
2、VirusTotal 政策调整：不再向新一代安全公司开放
3、印度铁路订票网站遭到攻击 1000 万乘客信息泄露
4、美国将研究一新技术用来识别和跟踪全球的黑客
5、12321 举报中心披露十大钓鱼网站：假冒建行居首

6、安全厂商策划恶意代码博物馆展示古老病毒界面

安天 CERT 搜集整理（来源：malwarebytes、cnbeta、digitalmunition、freebuf、techweb、dailydot）

[20160510]

1、Google Play 商店发现 190 种应用受恶意软件感染
2、安全厂商发现利用 Qzone API 针对韩国银行木马
3、Icarus 行动：全球已有超八家银行遭受 DDoS 攻击
4、关键医疗设备在心脏手术期间因杀软扫描崩溃
5、PHP zip 组件存整型溢出漏洞，可远程命令执行
6、安全厂商发布勒索软件 Locky 最新传播载体分析

安天 CERT 搜集整理（来源：softpedia、paloaltonetworks、freebuf）

[20160511]

1、CNCERT 发布 S2-032 漏洞威胁监测、处置情况公告
2、AVL 移动安全团队曝光利用极光推送 SDK 的恶意程序
3、Google Play 商店应用被发现高危木马 Viking Horde 家族
4、研究人员发现 SS7 漏洞可被黑客用于冒充受害人身份
5、韩国调查结果显示朝鲜对韩海军造船厂发动网络攻击
6、FBI 怀疑孟加拉中央银行窃案可能是内部人员所为

安天 CERT 搜集整理（来源：cnvd、avlsec、softpedia、theregister、sputniknews、marketwatch）

[20160512]

1、安全厂商曝光利用 IE 0day 漏洞的对韩国网络攻击事件
2、研究人员发现勒索软件新家族 Enigma，仅针对俄罗斯
3、黑客试图使用钓鱼邮件渗透美国国会计算机实施勒索
4、研究人员验证：可在 PLC 之间传播工业控制系统蠕虫
5、安天 CERT：警惕利用 UNICODE 反转字符串技术后门
6、研究人员发现 Android 系统的 WI-FI 漏洞，可实现提权

安天 CERT 搜集整理（来源：symantec、bleepingcomputer、theintercept、微信、securityweek）

[20160513]

1、外媒称中国 ARM 系统芯片制造商在产品预置内核后门
2、安全厂商曝光黑客利用微软 0day 漏洞攻击支付卡数据
3、APT 组织兵风暴自 4 月起攻击德国基督教民主联盟网络
4、勒索软件 CryptXXX 出现新变种，现有解密工具已失效
5、SAP 商务应用 5 年前旧漏洞，影响全球 36 家大规模企业
6、安全厂商发现首例具有简体中文提示的比特币勒索软件

安天 CERT 搜集整理（来源：thehackernews、fireeye、trendmicro、digitaltrends、securityweek）

[20160514]

1、第二家银行受到恶意代码攻击，类似孟加拉央行窃案
2、据称孟加拉央行窃案中恶意代码或与索尼攻击案有关
3、安全厂商揭示 Dridex 家族协助传播勒索软件 Cerber
4、德特勤局称：俄罗斯是对德国网络袭击事件幕后黑手
5、研究人员确认松下 PLC 编程软件存在漏洞，现已修补
6、开源压缩工具 7-zip 被发现安全漏洞，可执行任意代码

安天 CERT 搜集整理（来源：thehackernews、scmp、fireeye、securityweek）

[20160515]
1、安全人员发现勒索软件 Petya 和 Mischa 的二合一版本
2、SAP 旧漏洞危害范围扩大，受害企业已升至 500 余家
3、微软删除 Windows 10 具有争议的 Wi-Fi 密码共享功能
4、匿名者黑客组织攻击名单出现香港金管局和人民银行
5、安全厂商揭露黑客利用 Flash 漏洞 2016-4117 攻击过程
6、健身应用 Runkeeper 因秘密收集用户信息受挪威控诉

安天 CERT 搜集整理（来源：thehackernews、scmp、fireeye、softpedia）

[20160516]
1、知名黑客论坛 Nulled.io 遭入侵，泄露 9.45 GB 数据
2、孟加拉央行窃案恶意代码为巴基斯坦或朝鲜制作
3、土耳其黑客组织 Bozkurtlar 泄露六家国际银行数据
4、黑客声称能够读取 WhatsApp 和 SnapChat 加密消息
5、研究人员发现勒索软件 CryptoHitman 联合 Jigsaw
6、安全厂商发布 DarkHotel 定向攻击样本分析报告

安天 CERT 搜集整理（来源：softpedia、straitstimes、ifeng、tomsguide、freebuf）

[20160517]
1、CryptXXX 2.0 加密算法被破解，已提供解密工具
2、谷歌 Chrome 浏览器计划年底用 HTML5 取代 Flash
3、安全专家预警：ATM skimming 攻击全球大幅增长
4、研究人员揭示恶意软件和 EK 使用新域名生成算法
5、"光明黑客"行动：罗马尼亚黑客 GhostShell 复出
6、非洲行动：NWH 黑客组织泄露南非大学考试题

安天 CERT 搜集整理（来源：kaspersky、sina、securityaffairs、securityweek、softpedia）

[20160518]
1、境外安全厂商杀毒引擎存在漏洞，发送邮件即可触发
2、研究人员发现百万规模僵尸网络，劫持搜索引擎流量
3、大批知名论坛被挂马，系 Discuz!论坛标签权限设置不当

4、比特币交易所服务器遭黑客入侵，损失多达 200 万美金
5、Docker 远程管理默认配置漏洞，可远程获取系统权限
6、安全厂商发布海莲花黑客组织新近攻击活动分析报告

安天 CERT 搜集整理（来源：theregister、securityaffairs、360、softpedia、freebuf、wooyun）

[20160519]
1、安全厂商发现 Suckfly 间谍组织使用 APT 战术攻击印度政府
2、印第安纳州医疗机构遭勒索软件感染，系统被迫中断运行
3、勒索软件 Locky 分销网络再受打击，勒索软件被正常文件替换
4、VMware 发布关键漏洞更新，漏洞可被用于远程执行任意命令
5、研究人员发现印度手机银行应用严重漏洞，可窃取 250 亿美金
6、安全厂商发现 ATM 恶意代码家族 Skimer 时隔七年再度活跃

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

[20160520]
1、勒索软件 TeslaCrypt 金盆洗手，向用户提供免费解密工具
2、全球最大职场社交网站领英(LindedIn)1.17 亿条数据泄露
3、Icarus 行动：匿名者组织对纽交所、美联储发动 DDoS 攻击
4、黑客从银行窃取钱财，捐赠给反 ISIS 的叙利亚某区
5、Moxa 工业安全路由器发现严重漏洞，可执行恶意代码
6、安全厂商发布 2016 年勒索软件统计报告，3 月份为其顶峰

安天 CERT 搜集整理（来源：softpedia、easyaq、ibtimes、youxia、securityweek、fireeye）

[20160521]
1、AVL-Team：Macbeth 病毒植入流行社交应用，上亿用户或受影响
2、匿名者组织声称成功入侵 33 家土耳其医院，百万人医疗信息泄露
3、西门子 SIPROTEC 保护继电器中发现漏洞，更新固件已经发布
4、黑客利用孟加拉政府网站对多知名机构发动银行网络钓鱼攻击
5、蠕虫利用旧漏洞感染 Ubiquiti 路由器设备，影响巴西等多国 ISP
6、雄鹿球员信息因假冒球队主席的钓鱼邮件遭窃，FBI 涉入调查

安天 CERT 搜集整理（来源：avlsec、ibtimes、securityweek、theregister、securityweek、hupu）
[20160522]
1、勒索软件作者开辟新业务：向攻击载荷加入 DDoS 功能模块
2、SWIFT 系统攻击第三例：厄瓜多尔银行被窃 1200 万美元
3、研究者找到入侵任意 Instagram 帐户方法：移动端 API+暴力破解
4、斯诺登批评谷歌 Allo 聊天 app 未采用端对端加密，通信不安全
5、NSA 研究表明电话日志元数据可导致个人信息泄露给监管机构

6、北加州用户就 facebook 扫描个人隐私信息向 facebook 提起集体诉讼

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

[20160523]
1、勒索软件威胁愈演愈烈，引起美国立法人员关注
2、马来西亚研究者称勒索软件攻击转向商用计算机
3、黑客入侵 Drupal CMS 上传无加密能力假勒索软件
4、以色列公司开发廉价解决方案，对抗黑客 GPS 干扰
5、美国高校研究新兴网络追溯技术：音频指纹追踪
6、Google Play 手电筒 App 存在恶意广告，可传播恶意代码

安天 CERT 搜集整理（来源：eweek、thestar、softpedia、timesofisrael、securityaffairs）

[20160524]
1、瑞士 CERT：RUAG 网络间谍事件所用恶意代码为 Turla 家族
2、Ke3chang 组织最近再活跃，开发新的恶意软件家族 TidePool
3、安全厂商发布报告曝光针对中东地区部分银行网络攻击事件
4、南非银行数据泄露，导致日本 1400 台 ATM 遭盗提 14.4 亿日元
5、安全厂商发现恶意 JS 脚本被用于下载合法程序 Notepad++
6、凯悦酒店支付系统感染恶意代码，信用卡关键信息或已泄露

安天 CERT 搜集整理（来源：govcert、paloaltonetworks、fireeye、easyaq、mcafee、pcadvisor）
[20160525]
1、勒索软件家族 Cerber 使用双重 ZIP 包裹手段绕过反病毒检测机制
2、谷歌发布新版安全浏览 API 为移动和桌面用户提供最大限度保护
3、研究人员警告电子商务系统 OpenCart osCommerce 小心信用卡盗窃
4、研究人员发现 EITest 恶意软件活动已从 Angler EK 移至 Neutrino EK
5、研究人员称高通安全执行环境关键提权漏洞影响全球 60%移动设备
6、SWIFT 称将推出新安全计划，为恢复因孟加拉央行窃案受损的声誉

安天 CERT 搜集整理（来源：softpedia、securityweek、threatpost、zdnet）
[20160526]
1、研究人员发现 WPAD 协议漏洞可用于企业网络发动中间人攻击
2、谷歌计划在 2017 年淘汰密码，用信任 API 技术"信任得分"取代
3、中国将发射首颗具备防御黑客拦截数据能力的量子通信卫星
4、FBI 警告：伪装 USB 充电器可能是无线键盘记录器 KeySweeper
5、TeslaCrypt 宣布退出后，新型勒索软件 DMA Locker 接替其位置
6、研究者发布窃取孟加拉央行 8100 万美元恶意代码样本分析报告

安天 CERT 搜集整理（来源：softpedia、securityaffairs、ibtimes、thehackernews、computerworld、malwarebenchmark）

[20160527]
1、安全厂商揭露新 APT 组织 Wekby，利用 DNS 请求作为命令控制手段
2、韩国空军网站因感染恶意代码自 12 日起已停用，疑为朝鲜黑客攻击
3、安全厂商发现俄罗斯的仿冒银行应用 Fanta SDK，可锁住用户设备
4、受 LinkedIn 泄漏过亿用户帐号影响，微软禁止其账户使用简单密码
5、安全厂商曝光针对印度政府机构发动网络间谍活动的 APT 组织 Danti
6、研究人员发现剪贴板"Pastejacking"攻击，用户需小心复制粘贴内容

安天 CERT 搜集整理（来源：paloaltonetworks、ibtimes、trendmicro、telegraph、securelist、grahamcluley）
[20160528]
1、安全厂商曝光攻击 SWIFT 平台恶意软件与多起金融攻击有关
2、勒索软件 TorrentLocker 发起新破坏活动，仅感染瑞典 IP 系统
3、又一波恶意代码侵袭欧洲，多数受害者感染勒索软件 Locky
4、研究人员发现安卓恶意软件 SpyLocker，针对欧洲银行等应用
5、研究者发现"SandJacking"攻击方式，可安装恶意的 iOS 应用
6、安全厂商发现利用 TeamViewer 作为攻击跳板的 Windows 后门

安天 CERT 搜集整理（来源：symantec、heimdalsecurity、eset、softpedia、securityweek、softpedia）

[20160529]
1、4.27 亿条 MySpace 数据泄露，或成 MySpace 历史上最大的数据泄露
2、研究人员证明，攻击者可利用廉价设备对 NTP 服务器远距离攻击
3、伊朗媒体称某匿名黑客组织持续攻击其文化部网站，或与 ISIS 有关
4、研究人员发现针对银行账户的恶意软件，怀疑其背景为东欧地区
5、国际物流公司 DHL 用户再遭钓鱼攻击，链接指向被黑南非政府网站
6、Jetpack 插件存储型 XSS 漏洞令超过百万 WordPress 网站面临攻击威胁

安天 CERT 搜集整理（来源：E 安全、securityweek、trend、cnbc、magazine、softpedia）
[20160530]
1、安全厂商曝光 APT 行动 IXESHE 升级版：针对美国的 IHEATE
2、勒索软件活动日益猖獗，开始为受害者提供技术支持服务
3、研究人员称，匿名者黑客组织在 2016 年黑客活动中最为活跃
4、新恐怖主义担忧：黑客使用 GPS jamming 技术影响开罗机场
5、研究人员发现新银行木马 Android.BankBot，藏于游戏作弊器
6、巴基斯坦知名房地产门户网站 Zameen 被入侵，用户数据泄露

安天 CERT 搜集整理（来源：trendmicro、finextra、softpedia、mirror、tribune）

[20160531]

1、LG 智能手机被发现严重漏洞，攻击者可获取设备控制权
2、以色列研究人员声称设计出"完美"的隐蔽数据泄露技术
3、USCERT 警告：医疗 APP 硬编码证书漏洞可入侵服务器
4、针对沙特阿拉伯银行和国防机构的攻击行动 OilRig 被曝光
5、安全厂商揭露境外 APT 组织美人鱼行动，或来自中东地区
6、研究人员发现 Bayrob 家族恶意代码蛰伏后九年再度出现

安天 CERT 搜集整理（来源：theregister、securityweek、softpedia、paloaltonetworks、360）

==========

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）