每日安全简讯

[20160222]

1、黑客入侵官网网站 向 Linux Mint ISO 植入后门
2、日本成为区域定制垃圾邮件攻击的新目标
3、厂商确认 搜狗浏览器存跨域、本地文件泄露漏洞
4、免费手机充电站被指窃取隐私
5、报告显示 社交媒体诈骗增长 鱼叉式钓鱼攻击下降
6、近日 Tor 节点数量突增 50% 具体原因不明

（来源：Linuxmint、Symantec、乌云、补天、FreeBuf、Solidot；安天 CERT 搜集整理）

[20160223]
1、德国联邦内政部批准德国警察使用定制木马监控可疑对象
2、匿名者组织攻陷多个沙特阿拉伯政府网站 抗议处决 47 人
3、俄罗斯六银行员工收钓鱼邮件 内含 Trojan.Ratopak 恶意软件
4、阿桑奇爆料 NSA 监控意大利首相贝卢斯科尼及其贴身顾问
5、最新研究发现 手机银行木马 Acecard 已感染 50 多款金融 app
6、美犹他州数据中心计算机系统每天遭到 30 万次攻击

安天 CERT 搜集整理（来源：Securityaffairs、Symantec、Sputniknews、Espresso、IBSintelligence）

[20160224]

1、VMware 产品受到 glibc 严重漏洞影响 包括 ESXi
2、德国内政部批准警方使用定制木马监控可疑对象
3、匿名者组织对沙特阿拉伯政府网站发动系列袭击
4、俄罗斯六银行遭鱼叉式钓鱼攻击（Ratopak 木马）
5、Acecard 木马绕过谷歌安全机制 感染多款金融 app
6、家庭影院商店 Lewis Audio Video 遭勒索软件破坏

安天 CERT 搜集整理（来源：securityweek、sputniknews、Securityaffairs、Symantec、IBSintelligence、kgw）

[20160225]

1、安全厂商公开 Dust Storm 行动 针对日本关键性基础设施
2、"匿名者"攻击法国国防部网站 CIMD 泄露军方敏感数据

3、Linux Mint ISO 后门系 Kaiten Bot 多用于发动 DDoS 攻击
4、勒索软件再出新招 在移动设备直接创建 Lockdroid.E 变种
5、报道称军火商 BAE 系统公司每年遭遇上百次 APT 攻击
6、研究人员发现 glibc DNS 漏洞可被用于传播恶意代码

安天 CERT 搜集整理（来源：securityweek、Securityaffairs、Phishlabs、Symantec、E 安全、hackread）

[20160226]

1、CTB-Locker 卷土重来 专门针对网站页面
https://threatpost.com/ctb-locke ... ng-websites/116457/
2、MouseJack 百米外劫持主流品牌无线外设
http://securityaffairs.co/wordpr ... usejack-attack.html
3、印私有银行遭钓鱼攻击 过万 ATM 受影响
http://www.zdnet.com/article/mal ... nk/#ftag=RSSbaffb68
4、尼桑聆风存安全隐患 可被黑客远程控制
http://www.securityweek.com/api- ... cars-remote-attacks
5、研究者发现微软 EMET 防护可被自身关闭
https://www.fireeye.com/blog/thr ... emet_to_disabl.html
6、SS7 惊天漏洞 精密系统监听全球手机网络
http://toutiao.com/i6255119463025213953/

安天 CERT 搜集整理（来源：Threatpost、Securityaffairs、ZDnet、securityweek、fireeye、安全牛）

[20160227]

1、安天发布乌克兰电力系统遭受攻击事件综合分析报告
2、KeyBase 攻击者自身中招 泄漏图片揭露攻击全过程
3、POS 机恶意代码出现新变种 Fighter 以蠕虫方式自传播
4、恶意网站利用 Silverlight 漏洞 Mac 和 Windows 均受影响
5、匿名者组织攻击意大利政府网站 抗议天然气管道工程
6、伊斯兰国黑客矛头指向 Facebook 和 Twitter 首席执行长

安天 CERT 搜集整理（来源：Antiy、Paloaltonetworks、Trendmicro、arstechnica、Softpedia、Huanqiu）

[20160228]

1、医疗机构屡遭勒索软件 又有三家德国医院中招
2、美国国税局 70 万纳税人资料被窃 近半面临威胁
3、Angler EK 借流行网站投放 TeslaCrypt 勒索软件
4、研究发现云应用程序同步功能成勒索软件帮凶

5、加州大学伯克利分校遭黑客入侵 8 万人信息泄漏
6、外媒指责我国 ISP 向流量中植入广告、恶意代码

安天 CERT 搜集整理（来源：Helpnetsecurity、联合早报、Threatpost、scmagazine、cnBeta、Softpedia）

[20160229]

1、勒索软件业已失控 医院、教堂、学校、法院接连中招
2、针对网站的 CTB-Locker 变种快速泛滥 已感染数千网站
3、据统计 XSS 和 SQL 注入在 Web 开源应用漏洞中最常见
4、摄像头 RTSP 服务缺乏认证 黑客可以获得实时拍摄内容
5、菲律宾 UST 医院遭黑客入侵 攻击者自称"全球安全黑客"
6、洛杉矶卫生局成最近勒索软件受害者 系邮件附件传播

安天 CERT 搜集整理（来源：thehackernews、Softpedia、Zol、philstar、gizmodo）

==========

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）