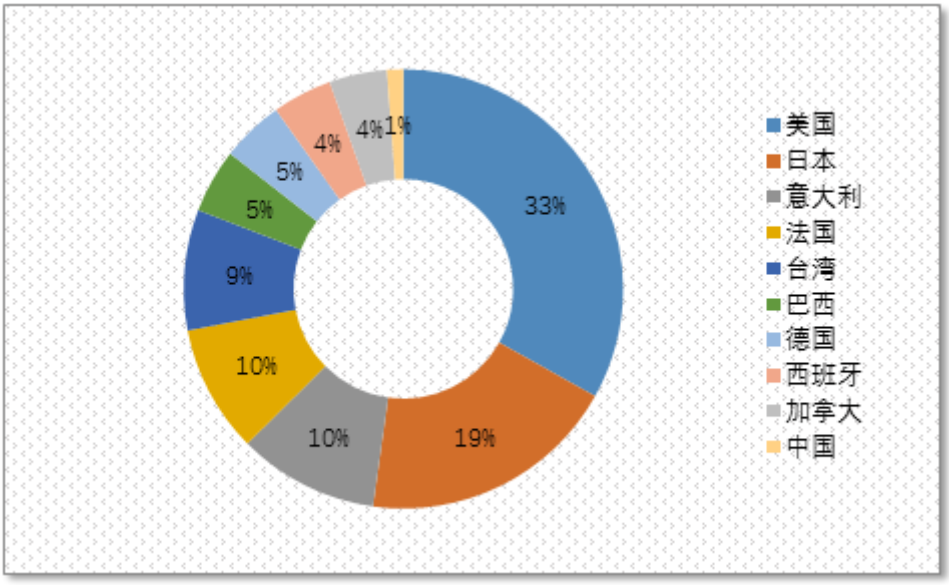
技术综述

[即时发布]

亚信安全发布 2016 年第一季度安全威胁报告：勒索软件成为威胁企业的头号病毒，安卓恶意程序比去年同期增长一倍以上

【亚信安全】-【2016 年 4 月 29 日】近日，云与大数据安全的领导者亚信安全发布了 2016 年第一季度安全威胁报告。报告显示，勒索软件病毒在本季度已经成为威胁企业安全的头号病毒，其不仅从代码结构方面发生变化，且感染方式更加多元化、本地化。此外，安卓恶意程序也从上个季度末的 1,770 万个增长到本季度末的 2,050 万个，与去年同期相比更是增长一倍以上。鉴于网络安全威胁数量仍在不断增多且技术更加精进，亚信安全建议企业用户应该建立纵深式的主动防御体系，提升网络安全能力。

勒索软件在全球肆虐　更加本地化、多元化



【勒索软件全球感染分布图】

勒索软件往往通过加密用户的文件来勒索高额赎金，而且其惯用的比特币交易方式让其很难被追踪，这让勒索软件成为备受网络不法分子欢迎的一种攻击方式。在本季度，勒索软件病毒已经在全球范围内呈现爆发态势，美国、日本、中国、欧洲都成为勒索软件肆虐的“重灾区”。网络不法分子还针对每个地区的语言及经济文化特点，对勒索软件进行了本地化，以提升索要赎金的成功率。

亚信安全网络安全监测实验室研究发现，本季度监测到的勒索软件在代码结构方面已经有深度进化，并产生了很多变种。本季度感染数量最多勒索软件变种是 LOCKY，其通过带有 JS 压缩包附件的邮件进行传播，病毒附件一旦被运行，用户计算机上的文档文件会被加密导致无法打开，同时会加密网络中可访问的网络共享文件。新型勒

索软件 PETYA 不仅可以覆盖受影响系统的主引导记录（MBR）、锁定用户，还能够通过合法的云存储服务感染用户。

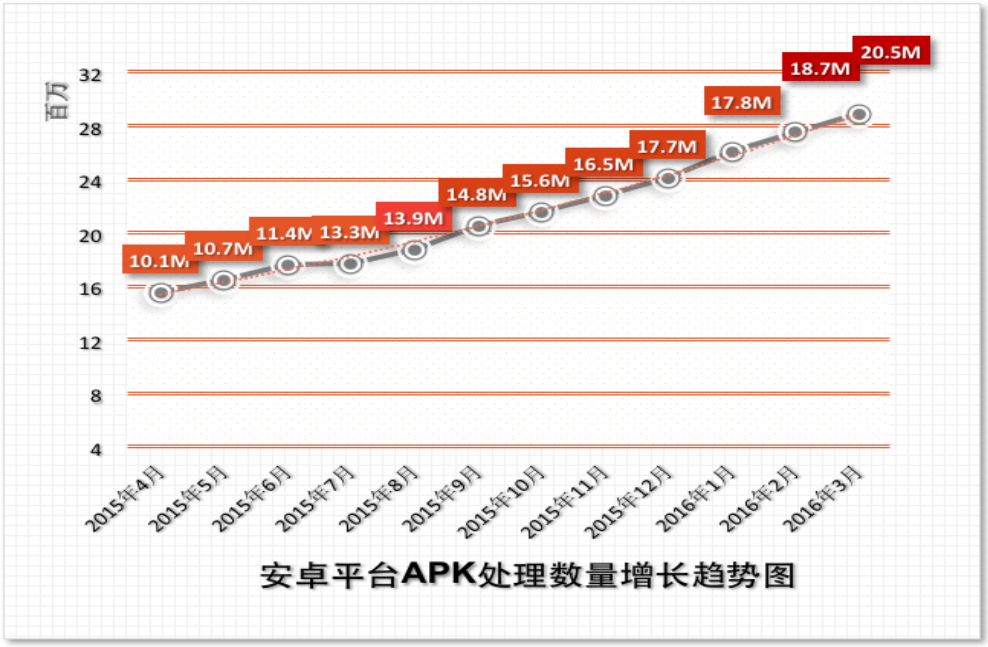
【勒索软件 PETYA 的加密界面】

此外，勒索软件的感染平台与方式也更加多元化，包括 Windows，OS X，Linux，IOS，android 在内的主流操作系统都有被感染的风险。而且，勒索软件的传播方式从最初的鱼叉式钓鱼邮件，到目前的漏洞利用传播、软件捆绑安装等，增加了用户预防感染勒索软件的难度。

亚信安全技术总经理蔡昇钦指出：“经济收益的提升是勒索软件肆掠的直接原因，要想有效防范勒索软件，一个重要策略便是采取 3-2-1 规则对重要文件进行备份，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。此外，由于勒索软件新变种不断产生，企业用户应该着重强化对未知威胁的防范能力，及时检测到文件中的未知样本。目前亚信安全的全线产品及解决方案均可以有效防御勒索软件。”

移动安全威胁数量稳步快速上升　比上年同期增长一倍以上

2016 年第一季度中，亚信安全对恶意 APK 文件（Android 安装包）的处理数量依旧呈快速上升趋势。在 2016 年 3 月份，亚信安全处理恶意 APK 文件数量达到 2,050 万个，比去年同期增长一倍以上。同时，亚信安全也发现了以苹果用户 Instagram 账号和密码为目标的病毒，这凸显了移动安全威胁的全平台性，任何平台的移动用户都不应该忽略移动安全。



【2016 年第 1 季度安卓平台 APK 处理数量走势图】

在本季度，移动安全威胁的一个重要特点便是恶意行为的不断拓展。除了用户熟知的恶意植入广告、恶意吸费、窃取个人信息等恶意行为之外，移动安全威胁正越来越多的被用于发动流量攻击甚至是作为侵入用户内部网络的跳板。亚信安全在本季度监测到一款针对安卓手机信息应用程序的病毒 ANDROIDOS_MSGCRACK.A，该病毒利用安卓漏洞对信息应用程序发起拒绝服务（DoS）攻击，以破坏目标网络。

亚信安全移动安全专家刘政平指出：“随着移动设备越来越多的深入到企业的工作流程之中，恶意移动程序给企业网络与数据带来的严重安全威胁需要被充分重视。企业需要将移动安全纳入到整体的安全防护体系之内，通过制定 BYOD 策略、企业数据与个人数据隔离等方式，来避免企业的信息资产受损。”

亚信安全 2016 年第一季度安全报告的主要发现还包括：

- 在病毒拦截排名中，Mal 及 PE 的感染类型病毒检测数量远高于其它检测名。其中，盗号木马 Mal_OLGM-6 在本季度被检测到的拦截次数约为 873 万多次，拦截次数位居榜首。
- WORM_DOWNAD 病毒依然是最为活跃的病毒。截止 2016 年第 1 季度，约有 6.49%的用户遭受到此病毒的攻击。
- 在通过 Web 传播的恶意程序中，.APK 类型的可执行文件占总数的 40%，所占比例比上一季度 42.5%的占比有所下降。
- 2016 年 1 月至 2016 年 3 月处理钓鱼网站共计 46,562 个。在所有钓鱼网站中，“支付交易类”和“金融证券类”钓鱼网站所占比例最多，占总数的 99%以上。

*报告全文下载 http://www.asiainfo-sec.com/report/375.html

##

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式 ,助力客户构建“立体化主动防御体系” ，为国家提供网络安全与云产业安全保障 ,推动实施自主可控战略。更多关于亚信安全公司及最新产品信息 ,请访问: http://www.asiainfo-sec.com