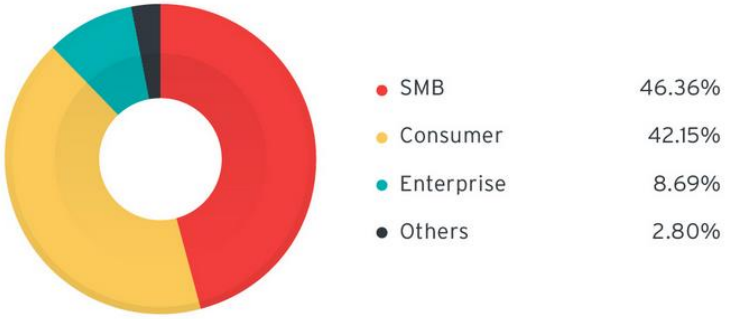
亚信安全 新闻稿
[即时发布]

亚信安全发布警示：锁定中小企业的勒索软件正在改变战术

【亚信安全】-【2015 年 11 月 13 日】勒索软件 Ransomware 已经成为一个突出的网络安全威胁，他们往往会以加密文件的方式勒索高额的赎金。亚信安全在近日发布警示：勒索软件攻击的发起者已经将攻击延伸到中小企业（SMB），因为中小企业往往不会像大型企业那样部署复杂的安全解决方案，且与消费者相比，中小企业也更有能力支付赎金。对此，亚信安全建议：中小企业员工不仅要提高安全意识，按照 3-2-1 法则备份文件，而且企业应部署周密的网络安全解决方案，通过侦测恶意文件和垃圾邮件并封锁相关网址等技术，在各层面防御勒索软件带来的威胁。

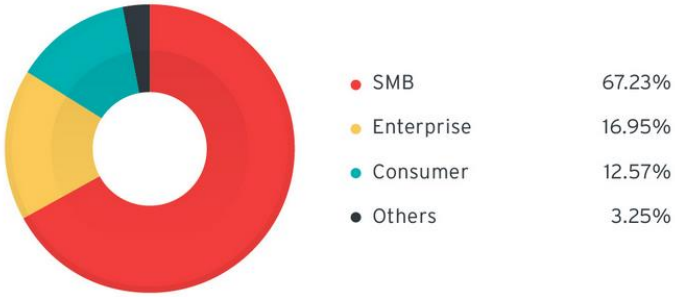
想像一家拥有少于 50 名员工的公司，某天公司主管收到了一封内嵌看似正常网址的电子帐单邮件，他们点击链接而导致感染勒索软件。不幸的是该公司并没有备份信息，因此他们更倾向选择支付赎金以解密文件，但这样很可能会导致网络犯罪分子在未来进行更多轮攻击。

在近期发现的勒索软件中，亚信安全发现最大的威胁来自 TorrentLocker 和 CryptoWall，他们都属于 Ransomware 的变种。亚信安全通过统计点击 TorrentLocker 和 CryptoWall 相关电子邮件内恶意链接（2015 年 6 月-7 月）的用户类型，发现中小企业在受害者中的比例最高。其中，点击 CryptoWall 相关电子邮件内恶意链接的用户大多数属于中小企业用户。



【点击 CryptoWall 设下钓鱼邮件的被害者，近七成为中小企业用户】

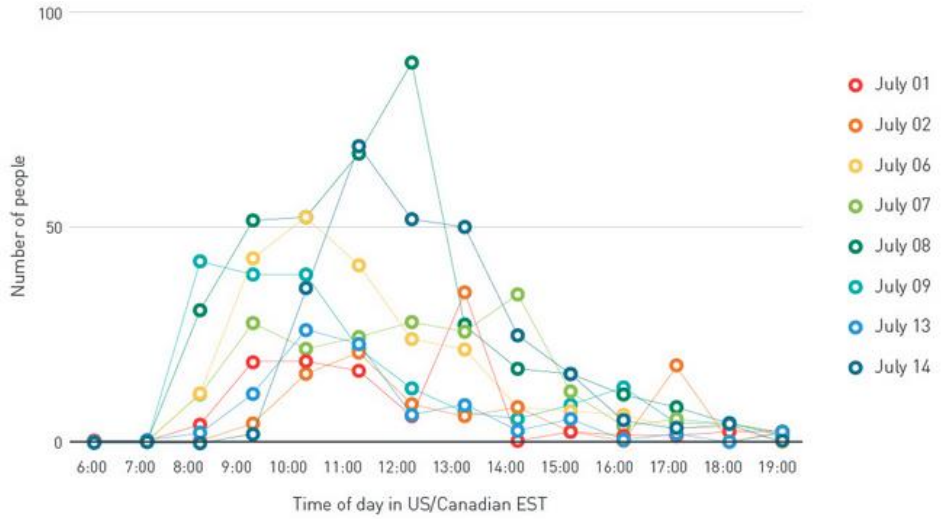
亚信安全还发现，大多数 TorrentLocker 相关恶意网址仍然是由中小企业(46.36%)点击，但消费者点击的比例（ 42.15% ）也居高不下。



【点击 TorrentLocker 相关网址的用户，中小企业仍然位居首位】

攻击往往在上班时间发动

由于勒索软件攻击主要以中小企业用户为主，因此不法分子更倾向在上班的时间来发动攻击。亚信安全将用户点击 CryptoWall 网址的时间数据（ 2015 年 7 月初）整理成下图，可以看到目标受害者一般在上午 9 点到下午 1 点之间点击这些链接，与员工的上班时间恰恰吻合。



【攻击爆发当天的每小时恶意网址点击量（ 2015 年 7 月）】

用来渗透企业用户的社交工程诱饵

今年大部分用于勒索软件的社交工程（ social engineering ）诱饵都和企业活动相关。例如，CryptoWall 会利用简历、订单和护照作为其垃圾邮件主旨。对此，亚信安全业务发展总监童宁指出：“虽然 CryptoWalll 所用诱饵不会根据区域而有所不同，但 TorrentLocker

却以针对区域定制化而知名，它们的社交工程诱饵会依受害国家设计，此类威胁通常会根据不同区域的特点，有针对性地假借邮递服务、电信、公共事业和政府机构通知的名义来制作诱饵。”

据亚信安全主动式云端截毒技术的反馈信息，澳大利亚（31.54%）、意大利（26.60%）和土耳其（20.40%）是 TorrentLocker 相关电子邮件攻击最流行的三个国家，并且在这三个国家中，勒索软件所使用的诱饵有很大的不同。

值得注意的绕过安全防御战术

勒索软件将焦点变换到企业目标的一个重要证据是其所使用的闪避技术，部分 TorrentLockerr 变种具备自毁功能，以防止 IT 人员采集样本建立安全措施。勒索软件网页还会要求用户使用验证码登录，这让自动抓取工具和沙箱技术更难识别恶意软件样本。同时，他们会选精心择攻击时间来攻击更多的企业用户。而另一个被用在 TorrentLocker 和 CryptoWall 的战术是利用沦陷网站来隐藏重新导向，进而避免在受感染系统上被侦测。

亚信安全建议：保护你的企业环境

在近几年的演化过程中，勒索软件已经从简单的恐吓软件演化成会加密文件、系统的加密勒索软件，最终达到让受害者支付赎金的目的。由于勒索软件攻击会给不法分子带来巨大的收益，因此有理由相信勒索软件会持续改善其战术，以感染更多的企业。

【从恐吓软件到加密勒索软件】

亚信安全业务发展总监童宁还建议：“勒索软件会给企业带来机密信息泄露的严重风险。然而，中小企业可以通过提高员工安全意识来保护自己的网络，例如，在打开电子邮件时先验

证发件人，在点击网站前先检查其信誉评比，不要启用巨集以避免 CryptoWall 执行。我们也再三强调过备份文件的重要性，最佳做法是按照 3-2-1 法则：针对每一份重要数据都备份三份数据副本，以两个不同的格式存储这些数据，并保持一份在异地。”

此外，亚信安全提醒中小企业主，必须部署周密的网络安全解决方案，通过侦测恶意文件和垃圾邮件并封锁相关网址等技术，在各层面防御勒索软件带来的威胁。

##

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