TT Talk

December 2013. Issue 182 in the series

TT Talk 第182期

1. 运输中的网络风险正逐渐扩大

网络技术的进步毫无疑问地加快了业务效率，同时也为承运人和物流运营商提供了机会，来降低偷盗和欺诈风险。但遗憾的是，有组织的犯罪团伙也同样受益。随着微创数码技术的日益普及，TT Club 认为最近几个月所发生的事故，可能对于合法贸易而言是一个新兴的风险，将对运输链中的运营商造成经济上和商业上的损害。

机关算尽的小偷和骗子，总是能令不明真相的受害者感到震惊。赌注虽高，但很明显对于国际运输，其跨境运输的性质决定了回报也高，特别是针对人口和毒品买卖，以及其他非法贸易，诸如非法倾倒废弃物，和拦截贵重货物。

间谍软件的渗透

之前我们已经着重提示了有关清算网站和诸如此类的风险，但最近的新闻报道已经确定了关于 IT 偷盗的另一种方法。该方法超越了单纯通过假网站，误导运营商认为是与一个合法公司在交易。新的方法是网络犯罪分子可以访问并控制运营商的 IT 系统。

在过去的几周内，报道了若干起金额小但却值得注意的事件，乍看之下似乎是一些小型的非法渗透办公 IT 系统的事件。损失很小——甚至没有财物丢失。但经过彻

底的事故调查发现，“小偷”实际是在运营商的 IT 网络系统内安装了间谍软件。有趣的是，这需要实质性的软件安装。典型的情况是，犯罪分子确定了某些网络安全保障不充分、但拥有高级访问权限的个人为作案目标。因此，需要大量出差的运营商的高管们，特别容易被利用。

“犯罪分子确定了其网络安全保障不充分、但拥有高级访问权限的个人为作案目标。”

被找寻和提取的信息类型可能是要求从港口和堆场释放集装箱的指令。同时，间谍软件可以记录操作步骤、所用按键、甚至下载和打印文档、截屏，再传输到外部源。根据迄今为止发现的案件，网络罪犯的目标显然在于特定的个别集装箱，然后采取步骤，通过运营商的系统追踪集装箱至目的卸货港。一旦集装箱到达，犯罪分子就会介入，从尚不知情的运营商 IT 系统中收集所需的放箱数据，最终促使集装箱纳入他们的监管和控制。截至目前，这些事故已被认定与贩毒有关，通过运输链上被忽视的环节来进口非法货物。

犯罪分子关注利用新兴技术

“运输链上重要信息的潜在作用是不可低估的。”

这样的新兴技术很容易被复制，然而可以被利用并渗透到运输链上的其他领域，包括从货运代理到仓库经营商。运输链上重要信息的潜在作用是不可低估的。除了关注至今已发生的事故外，还会发现其涉及范围的选择性很强，并以货物偷盗、贩卖人口和瓦解全球运输链为目标。通常情况下，网络安保工作的重点是对抗干扰和减少“业务中断”的潜在风险；近期的间谍软件更凸显出以刑事犯罪去获得高额非法利益的手段。所以，实施有效的计算机日志和“仪表板 Dashboards”的检查（如详细的操作和绩效管理信息），可能比更新和检测适当的应急计划更为迫切。

迫于成本压力和必须更具高效，现今许多本地的和全球性的物流运营商大量地依赖于 IT 系统，来管理其自身的业务包括仓储、车辆调度工具，以及会计、安保甚至是通信系统。这些增值的信息也吸引了网络罪犯的眼光。

“网络不法分子已经具备了侵入电子邮件账户和联络渠道的能力，物流经营商对此风险不可忽视。”

有组织的犯罪集团实力雄厚且专注于利用新兴技术，不仅能实施犯罪，也会反侦察。网络不法分子已经具备了侵入电子邮件账户和联络渠道的能力，物流经营商对此风险不可忽视。举例来说，如果一个司机收到指示要求偏离原定计划的交货目的地，转而送往一个附近的仓库，这看似从他们自己公司且可信赖的渠道获得的指

示，那么他们会否关心该指示的真假呢？同样地，通过访问仓库经营人的管理系统，犯罪团伙可以对仓库内真实的库存数据进行修改而达到其目的。

对抗网络风险

随之而来的损失可能引发巨大的财产风险，更不用说商业和声誉俱损。当然，这种不断增加且复杂的“网络攻击”，对于物流经营商如何建立行之有效的防御手段是一种挑战。有风险意识是第一步，紧接着应进行彻底的风险评估。董事会和管理人员需要清楚阐明该风险状况，谨慎地建立相关程序并予以跟进。在许多情况下，人为因素是“风险防御”中最强也可能是最薄弱的环节。通过全面的培训和建立有效的规章（如职责分明和“内部举报”），个人的泄密行为或承包商的渎职均可能被机敏的其他人所察举而减少损失。

日常操作中保持警惕性和尽职尽责——尽可能多的予以实践——显然是至关重要的，包括安装普通的IT防护软件。然而，对于经营商来说，开发一个更为强大的防护技术，侦查骇客和间谍软件的活动也不失为一种明智的做法。在您评估自身的IT系统时，由Kroll公司发布的 2013/2014全球反欺诈报告确定了两个关键问题需要被考虑：

- 如果您发现您的系统已经被入侵，那么您的系统是否有功能可以追踪并确定哪些信息被浏览、修改或被盗取？

- 如果您的客户知道相关资料是通过您的 IT 系统被外部获取，将会对您的业务产生什么潜在影响？

同样地，需要消除对单一系统的依赖性，如通过不同的设备实现双信息传递功能，并控制由 GPS 映射定位的信息，这都被证明能有效阻止系统被渗透。

在运输链上的安保措施已不再是“简单地”使用挂锁、报警器和追踪系统。有组织的犯罪团伙已经催生了新的风险。对于那些需要进一步思考这个议题的工作者，Kroll报告提供了一个完整的全球概述，内含许多评论可供与运输和物流有关的人员参考。此外，TT Club的防损手册“运输链安全——管理、举措和技术”也是一个有用的参考。这是对会员公司及其保险经纪人免费赠与的出版物，其他人士可购买打印版或PDF电子版，价格为 36 英镑。

2．网络身份——你所看到的未必是真实的

欧盟委员会估计，每年在运输途中被盗取的货物价值高达 82 亿欧元。TT Club 也从中发现，通过欺诈所造成的损失正在不断扩大。一个显著的趋势是，有组织犯罪团伙冒充合法的经营人或使用货物清算网站，更容易盗取高价值的货物。也许最令人担心的是，这是一个全球性的问题。

与清算网站有关的诈骗

货运代理、以及类似的货运或陆路运输经纪人，需要注意到窃取商业身份的案件，正在增加。其中窃贼伪装成合法的承包商，盗走数百万美元的货物。专家指出，此类案件增长如此之快，将成为盗取货物的最常见方法。互联网——我们都已对其严重依赖——更有利于这种诈骗手段，可以使窃贼更容易地接触到大量的资料。在线数据库和货物清算网站可帮助犯罪分子们，确定采取哪个既有身份或貌似合理的分包商身份，来寻找他们想要盗取的特定货物。

“据报道，之后假冒的中国货代会要求支付赎金，来换取递送这些必要文件。”

在最近几周，有关多起“虚假”中国货运代理人的案件报道，频繁出现。其首先与英国的货代通过网络建立业务合作关系，在实际发运集装箱后但不主动提供正本提单，导致集装箱到达英国港口后无法安排放箱。据报道，之后假冒的中国货代会要求支付赎金，来换取递送这些必要文件。如果不这样做，英国的货代需要支付大量的滞期费和仓储费用，以及试图使自己走出困境而产生的高额法律费用。

货物清算网站被冒用的可能性也在不断增长。当运营商在其不熟悉的地区需要援助，特别是在时间紧迫的情况下，运营商可能会冒险使用这些网站所提供的不熟悉的分包商。

“现有记录表明犯罪组织购买了一些频临倒闭的货代公司，并继续用他们的合法身份来从事运输业务。”

现有记录表明犯罪组织购买了一些频临倒闭的货代公司，并继续用他们的合法身份来从事运输业务，主要通过互联网进行活动。这些公司实质上处于破产的状态，犯罪团伙等待机会接收一票高价的货物，然后消失。在其他情况下则更简单，假冒的陆路承运人不断的进行广告宣传，能接受临时性的运输任务委托，希望某些不知情的货代公司，由于急于完成手上的运输工作而无暇进行仔细的检查，而将高价的货物委托这种公司来运输。

“犯罪分子登陆网站，并提供了虚假的保险单。”

最近在美国发生的一个案子，使问题更加突出。某陆路运输经纪人在清算网站上公布了一票货物，该清算网站通常是由货运代理人来选择适合的汽车公司，完成货物运输的。之后有一家汽车运输公司来电询问货物的情况，但被要求提供一份已投保的保险证明。当保险单被接收后，陆路运输经纪人和该汽车运输公司商定价格，并确定了提取和送达货物的地址。该运输公司派的卡车接收了两票货，总价值175,000美元，但最终货物并未到达既定的运输目的地！实际是犯罪分子侵入了网站，并提供了虚假的保险单。运输经纪人最终致电给该真正的汽车运输公司，发现货物是在加利福尼亚州被提走的，而该公司只从事佛罗里达州境内的运输。

风险防范的建议

TT Club建议，此类网络风险可以通过以下方法来成功减损：

1. 在公司内部设定一个强有力的分包商选择策略。在实施此类选择策略后，即使是在时间紧迫的情况下，也可以从根本上减少使用清算网站时的风险。TT Club发布的防损信息中曾登出“常见被盗货物”（Theft Attractive Cargoes）一文，里面包含了一系列问题，以备货运代理或经纪人在选择分包商时提问。还有一个威胁是有组织的犯罪预先接管了与您之前有正常业务往来的合法公司；您应该特别留意，如果一些经常联系的人员突然发生了变动。

2. 清算网站通常包含一个免责声明，即对该网站上发生的欺诈活动不负责任。然而，此类网站的运营方对用户仍然需要承担谨慎义务。他们会经常提供安全使用网站的建议、最佳做法列表和防损建议，来减少用户可能面临的风险。TT Club认为，您可以完全接受和遵从这些建议。

3. 当分包商使用诸如Hotmail, Gmail和Yahoo等免费电子邮件账户时，应引起警觉。同样也应当避免使用Skype或其他免费的视频交流软件。犯罪分子会使用和真实的承运人完全不同的电话、传真和电子邮件。使用已建立的途径（如美国的Carrier411）来对承包商的名字做一个快速的网络搜查；反复确认联系方式和其他已知的细节。特别注意接近下班时间或晚上打入的电话，因为此时所有的承运人信息是难以核实的。

4. 当要求提供保险证明时，应确保邮寄正本文件。对以电子格式提供的保险证明加以留意。虽然电子格式节约了时间，但犯罪分子使用先进的图形软件更易于制造假的文件。尝试与保险人联系以验证保单的合法性。如果未能联络到保险人和/或该保险人不提供包含详细联系方式的网址，这可能是一个关于该承包商是否合法的暗示。

5. 事先获得卡车和拖架的标识和牌照信息，并提供给托运人，以便在提货时确认该信息。应要求在托运人的仓库或放货时复印承运人委托的卡车司机的执照，并单独与汽车运输公司核实情况（当司机在他的车内等候时）。鼓励使用闭路电视，拍下清晰画面来核实司机身份，重复检验汽车标志、号码牌等。如果与来自货运代理的信息有任何差异，应要求给予明确的解释来澄清。

最终，犯罪分子会在任何已知的运输链中寻找并识别最薄弱的环节，互联网则提供了很多机会。谨慎尽责的程序包括对给予的信息进行充分调研、合理怀疑、仔细分析、重复检验，并且细心评估。在您委托一个新的分包商处理您客户的货物时，这也代表着您的声誉，所以采用一个严格的审核程序，是明显合理的。

结束语

我们真诚地希望上述内容对您的风险管理有所帮助。如果您想了解更多信息，或有任何意见，请给我们发电子邮件。我们期待着您的回音。

百富勤·斯托斯-福克斯(Peregrine Storrs-Fox)
风险管理总监
TT Club

TT Talk是TT Club不定期出版的免费电子通讯文件，原稿由TT Club伦敦发放，其地址是英国伦敦芬彻奇街90号，邮编EC3M 4ST。(90 Fenchurch Street, London, EC3M 4ST, United Kingdom)

您也可以登录我们的网站阅读本通讯和过去所有的通讯文件，网址是：
http://www.ttclub.com/publications/tt-talk/

如果您想要了解本公司的登记注册信息，请点击以下网址：
http://www.thomasmiller.com/terms-and-conditions/company-information/