近年已知 APT 受害金额：加密勒索 101 亿、交易诈骗 713 亿、操控窃取...、瘫痪勒索 more...。91% APT 攻击利用电子邮件，9% 利用网站水坑与网络诈骗；18% 从垃圾邮件转型 APT 邮件。APT 集团藉由所获取庞大利益，急遽扩张资源，包含带宽、IP 地址、域名、网络广告等。APT 攻击来源层级上至国家与军队，国际间打击网络犯罪的行动制裁与严刑峻法尚未可见。

台湾已成为 APT 受骇全球最严重与人均损失最高的国家，企业必须自行建立坚强防护罩。截至 2017 年底，已知恶意软件超过 8 千万笔，远远超过已知百万笔病毒与蠕虫；传统静态特征码无法侦测零时差恶意软件，整体拦截率也在 30% 以下；沙盒系统分析效能或涵盖软件版本亦无法实时与有效侦测。

先发性恶意威胁通讯行为解析

APT (Advanced Persistent Threat) 进阶持续威胁常见攻击手法为锁定目标后，搜集情资、设计诱饵与执行任务；其中设计诱饵常见手法为假冒客户、政府单位与知名服务提供商，例如 Apple、Google、国税局、健保局与国际快递等。此类社交工程信件由于邮件内容并无广告嫌疑，再加上利用传统电子邮件网关弱点，将往来单位的电子信箱设定为系统或个人白名单，使得这类商业假冒邮件诈骗横行无阻。本系统具备全球最前瞻假冒邮件辨识技术，提供独家双认证白名单机制，意即发件人信箱加上发件人主机同时符合才可放行；以及独家 SMTP 延迟反制，占据黑客系统资源不予回复，迫使转战他方。

先发性恶意威胁程序行为解析

可以定义各类型项目的评分，包含

1. 附件型态：附件加密、伪造扩展名、炸弹压缩(Zip Bomb)、解压缩次数
2. 特征数据库：完整(Md5)、多段(Ssdeep)、加载(Imphash)取样、原厂数据库
3. 程序行为：反侦测行为(Antidebug Antivm)、CVE 弱点漏洞侦测(CVE Vulnerability)、加密演算行为、嵌入漏洞检查套件(Exploit Kits)、隐藏包装(Packers Hidden)、文字命令程序(Webshells)、邮件识别、恶意文件、恶意软件、手机恶意软件、恶意网址
4. 沙盒分析(可选购独立动态沙盒仿真系统)：行为分析、网络分析

APT 攻击目的与手法

目的与手法	加密勒索	交易诈骗	操控系统	窃取情资	瘫痪勒索
搜集情资	●	●	●	●	●
设计诱饵	●	●	●	●	
建立中继站			●	●	
CALL Home			●	●	
植入程序			●	●	
执行任务	●	●	●	●	
网络综合攻击					●

设计诱饵 目的为找出组织弱点与寄送恶意超链接或附件；

Call Home 以取得更多恶意软件；

BEC 交易诈骗 渗透阶段目的为取得邮件系统用户的账号与密码，诈骗阶段目的为取得汇款。

APT 技术比较

方式	拦截成效
先发性恶意威胁通讯行为解析 先发性恶意威胁程序行为解析	85-95%
动态沙盒鉴识 实时静态特征码	10-30%

先发性滥发者通讯行为解析

运用全球独家专利技术「SMTP 实时回溯追踪」与「SMTP 黑客行为解析」，在 SMTP 交握阶段即可有效辨识滥发、非法、匿名、伪造等寄件行为，「有依据、决定性、高效率」拦截 90% 以上的垃圾邮件；搭配云端信誉黑名单、国际黑名单、DNSRBL、内容权重运算等，为企业带来极高与最佳防护成效。

完善功能与组织型报表

SpamTrap 提供自我学习、政策比照、黑名单检举、白名单反馈、个人与群组政策制定与黑白名单、逾期未读管理、代理人、隔离不发报告、重送报告、化名与群组合并处理等贴心机制。

SpamTrap 提供各种统计图表与排行榜，并可依照组织架构定时寄送统计报告给部门主管。

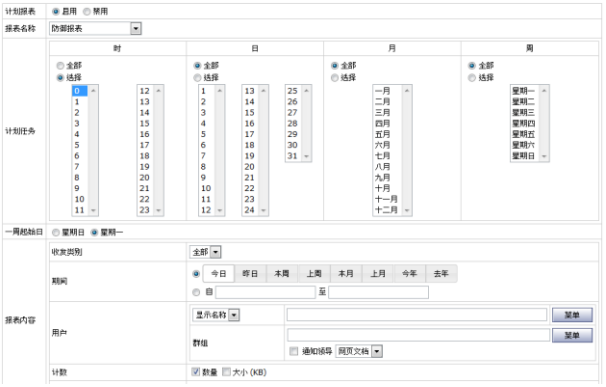
鉴识报表

排程可以立即发送或指定月、周、日、时；内容包含期间(起讫、今日、昨日、本周、上周、本月、上月、今年、去年)与风险等级，正规式比对输入发件人、收件者、主旨、来源路由、讯息代号；收件者可自行新增，自定义报表格式(支持网页、文字、PDF)。

隔离报告

隔离中心

计划报表



硕琦上海信息科技有限公司 北京 | 上海 | 苏州 | 深圳 | 海外
www.box-sol.com |业务信箱 sales@box-sol.com | 客服信箱 service@box-sol.com
200050 上海市长宁区定西路 1277 号长峰大厦 3006 室 T 021-5238-3756