

# 先发性滥发者通信行为解析 精准拦截全球各地不速之客



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，急速扩张资源，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. 附件型態：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	窃取情报	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	85-95%
先发性恶意威胁程序行为解析	
动态沙盒鉴识	10-30%
实时静态特征码	

# 全球最悍 APT 恶意狙击手 先发性威胁行为动态沙箱解析



## 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 交接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



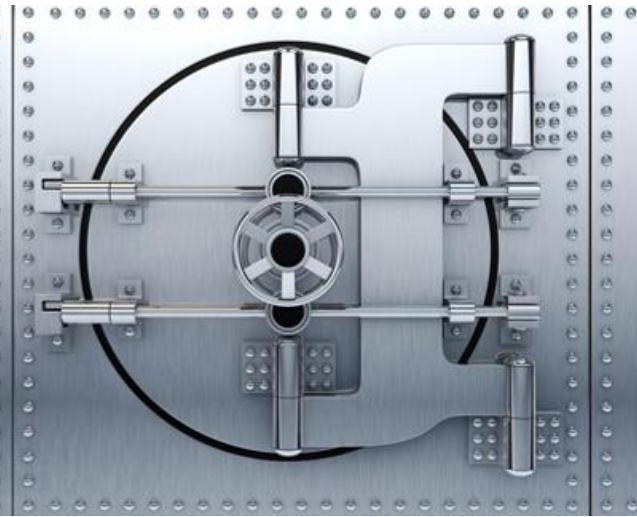
# DLP 营业密文与个人数据 滴漏外泄防御与数据加密保护

电子邮件为现代企业商务往来重要沟通工具，基于营业秘密保护与法规遵循，例如各国个人资料保护法、欧盟 GDPR、ISO27001、BS10012 等，企业必须善尽电子邮件归档与审计责任。

企业审计分为事前审计与事后审计。事前审计主要目的为 DLP 数据外泄防御，分为单封超量与累计超量(意即滴漏外泄防御)，着重风险指数与行为分析。事后审计主要任务为常态后稽管理与个案调阅申请。BestFiler 支持在线放行申请、在线调阅申请、各式审计报表，为企业效率落实无纸化严密审计管理。

## BestFiler 系统运作示意图

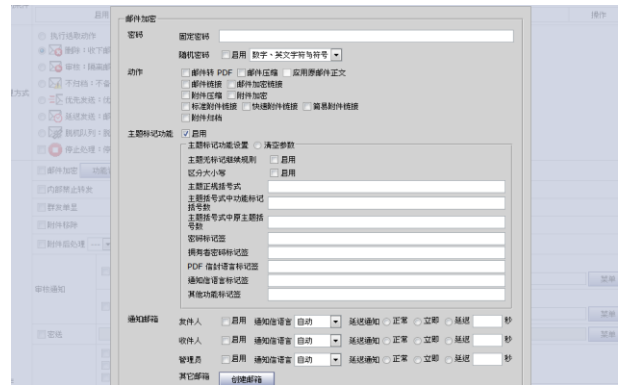




事前审计：绝佳风险管理工具

- 合法性：预设 PII 标准个资与 PII II 行为个资
- 精确度：支持正规表示式与程序检验、自定义排除
- 完整性：32/64 位各种应用程序、大型与多空白附件
- 防御力：支援单封超量与区间累计超量(意即滴漏外泄防御)
- 数据保护：支持邮件/附件加密、不允许加密附件(规避检查)
- 寄件信件：群发单显(优于密件)、主旨/内容置换(省时个别化)
- 执行弹性：在线例行/个案白名单、主管立即通知与审核放行
- 管理报表：依据审计与管理需求，产制各类统计与分析报表

PDF/ZIP/HTTPS 邮件加密



事后审计：UBA 大数据行为分析

- 常态后稽管理：设定查询条件、查询权限、有效期间
- 个案调阅申请：调阅者向审核者(可要求多人双签)提出申请
- 滴漏报表：超过上限，立即通报最大值与总量，并显示明细
- 管理报表：排程发送各类用户与群组报表给主管与审计者
- 邮件日志：显示认证账号与来源国码/城市，支持转寄与重送
- 系统日志：包含核心日志、认证日志、扫描日志、负载日志
- 安全日志：记录管理者动作，包含查询、转寄与变更设定等
- 队列管理：设定队列重送与延迟、队列通知、定期队列报告

AAR 主动式审计报表

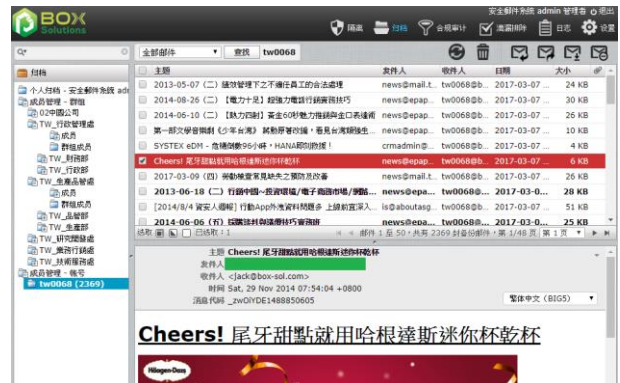
稽核报表 稽核报表  
期间 2018/02/13 - 2018/02/13

序	日期	部门	寄件者名称	寄件者	收件者	主旨	附件	大小 (KB)	最大值	比例	规则名称	稽核结果
1	2018-02-13 15:32:58		kan kan@box194.com	kan@box194.com	kanivan@box194.com	Re: test99	2,476	1	3			
2	2018-02-13 15:32:31		kanikan kanikan@box194.com	kanikan@box194.com	kanivan@box194.com	test99	1,551	1	3			
3	2018-02-13 15:59:25	test	megan megan@box194.com	megan@box194.com	ds@box194.com, ew@box194.com, kanivan@box194.com, kanivan@box194.com	捷捷 科技	5,655	3	6			
4	2018-02-13 16:05:36		kanikan kanikan@box194.com	kanikan@box194.com	kanivan@box194.com	Re: test99	2,839	1	3			
5	2018-02-13 16:05:50		kanivan kanivan@box194.com	kanivan@box194.com	kanivan@box194.com	Re: test99	3,109	1	3			
6	2018-02-13 16:06:58		kan kan@box194.com	kan@box194.com	kanivan@box194.com	Re: test99	4,331	1	3			
7	2018-02-13 16:05:59		kanikan kanikan@box194.com	kanikan@box194.com	kanivan@box194.com	Re: test99	3,422	1	3			
8	2018-02-13 16:06:09		kan kan@box194.com	kan@box194.com	kanivan@box194.com	Re: test99	3,720	1	3			
9	2018-02-13 16:06:44		kanikan kanikan@box194.com	kanikan@box194.com	kanivan@box194.com	Re: test99	4,033	1	3			
10	2018-02-13 16:52:20		kanikan kanikan@box194.com	kanikan@box194.com	kanivan@box194.com	Re: test99	4,644	1	3			

ELM 巨量数据高效管理

- 支持本地与网芳 Cluster 丛集管理。
- 支援 Journal SMTP/POP 去重复化归档。
- 支援 .eml 格式(加密)储存与多种还原方式。
- 支持全方位归档机制，包含本地、网芳、光盘、磁带。
- 超过 50 种以上附件格式与千万封电子邮件 5 秒搜寻。
- 支持不可否认性、高效全文检索、简繁互换与进阶搜寻。
- OEA 支持阶层式组织展开、邮件预览、附件内文快速搜寻。
- OEA 取代邮件封存，利于删除管理收信匣，提升工作效率。

OEA 邮件预览与快速搜寻



# 独家 SMTP 串流处理与 MTA 传输控制

## 双认证 · 数据不落地 · 读信地域 | 下载控制

### 绝佳安全

- 核心安全** 最重要的安全所在，严格把关硬件驱动与软件程序行为
- 作业安全** 中介程序正向表列检查、关闭无用指令、零时差弱点防护
- 静态加密** 国家安全等级，数据外泄防御最高规格 DLE 动态长度加密
- 动态加密** 第三方或自发凭证加密、迄今无破解纪录的 SSH 加密联机
- 身分安全** Root PKI/ACL 控管、(自然人)凭证数字签名、OTP 安全认证
- 应用安全** 高可用性、丛集管理、自我修复、DLP 滴漏防御与数据加密保护
- 威胁安全** 瘫痪、字典、垃圾、病毒、跳板攻击、APT 组合式进阶渗透攻击

### 创新强大

#### 邮件传输

支持进阶 SMTP TLS、SMTP 认证伪造防御、SMTP 成功与失败认证控管、SMTP 代转、SMTP 代转表、进阶 SMTP 代转、网域认证密钥、签章加密代理、快速备份、邮件路由、寄信网卡 IP 绑定(搭配 IP 化名对应多个外部 IP，利于大量寄信)、邮件置换、错误讯息置换(避免封网掉信)、编码置换(避免乱码)、变量置换(LDAP 兰位置换于主旨/内文)、外寄通讯簿、假冒 Postmaster 退信攻击防护、还原 winmail.dat 邮件格式、特别标题(记录所有收件者信箱与信封发件人信箱)、队列管理(重送次数/延迟传送/查询/重送/通知/报告)。

#### 安全控管

支持条件式转寄备份、多域免责宣言、外寄速度控制(避免上灰黑名单)、进阶 SMTP 控管(单封/累计控管寄信次数/收件者数/大小/总量)、发件人网域限制、附件备份、附件移除、收件者互斥、安全等级(设定账号与邮件安全等级)、(PDF/ZIP/HTTPS)邮件加密、病毒扫描。

#### 信箱服务

支持 POP(S)/IMAP(S)/HTTP(S) ActiveSync 读信服务、信箱容量、信箱容量届满管制、信箱总览、信箱清理、信箱参数、内部邮件回收、内部已读追踪、整合寄信备份、新闻组、读信控管(账号/内外/地域、下载标题/本文/附件)、认证控管(POP/IMAP 猜密码防御)。

### 弹性扩充

#### 丛集架构

- HA Heartbeat 自动备援与回复
- AA SAN 丛集管理
- Rsync 参数同步
- DRBD 本地与 Cyrus 异地信箱同步

#### 高效率丛集 LDAP

- 多域管理与进阶路由
- 密码政策与在线申请
- 个别权限共享通讯簿
- AD/LDAP 多台整合
- SQL 休假代理整合

#### 各种 SOAP (XML) API 接口

### 完善报表

#### 邮件日志

- 支持 SMTP 认证账号与来源国码、回收与转寄、读信日志与排程报表。

#### 系统日志

- 提供完整日志，包含 SMTP(S)/POP(S)/IMAP(S)、LDAP、Anti-Virus、Kernel 等。

#### 安全日志

- 详细记录管理者动作，包含新增账号、修改密码、查询关键词、转寄或重送、变更设定等。

#### 统计报表

- 包含日报表、排行榜、图形报表等。

LisoMail 电子邮件协同作业

地表最强 内外都安

Web Mail 通行全球，速度最快  
行动商务与协同作业全面启动



## 新一代云数据中心与行动商务端 · 解决企业三大难题

巨量数据管理 PST 5~20GB 就需要封存，更换设备时数据搬移费时或不兼容；

行动装置支持 无法读取或搜寻所有信件、通讯簿输入不易、行事历无法同步；

出差在外存取 传统工具带宽使用率 40%，网络服务可能仅提供 HTTP(S)。

超大容量！一封信一个档、虚拟信箱、不需封存

超省空间！最新邮件索引技术、重复信件单一存放

极致快速！最新互动网页技术、带宽使用率近 100%

## 超高效率 人性化电子邮件

### 读信

邮件预览(上下/左右)、键盘 Shift 多选与 Ctrl 单选、鼠标右键选单(已读未读/黑白名单/邮件规则)、IMAP Thread 邮件串、树状收信匣、个别收信匣代理人、最新最多编码、强化裸码与混码辨识、简繁体转换

### 写信

多个身份信息与电子签名文件(繁中/简中/英文...)、收件者随打即找、群发单显、主旨/内容置换、简繁体转换、内部禁止转寄、预约寄信、内部邮件回收、内部已读追踪、寄信备份整合

### 管理

人性化与高效率邮件规则、条件式拦截远程图片、自动回复(不重复发送天数)、邮件标签(依照发件人或主旨，标记关键词与颜色)、个别权限 POP 与 IMAP 外部信箱、个别收信匣清理(保留天数)、邮件日志、队列管理

### 安全

登入日志：支持来源国码，利于发现可疑

虚拟键盘与图形验证：防御机器人猜账号与密码

APP OTP 安全密钥：需要两组密码正确才可登入

PKI 个人凭证：支持(自然人)凭证数字签名与加密

外部禁止：支持附件下载、邮件下载、转寄与回复附件

## 通讯簿共享 行动商务好帮手

个人通讯簿 群组、汇入、汇出

### 系统通讯簿

组织通讯簿：树状与多个网域整合

共享通讯簿：客户或供货商，多本与个别权限控管

外寄通讯簿：可以查询，作为邮件威胁防御白名单

支持 ActiveSync、CardDAV、LDAP 搜寻

## 会议与沟通 万事在握行事历

个人行事历

系统行事历 强制订阅

新增活动 重复行事历、资源(冲突)行事历、提醒

支援 ActiveSync、CalDAV

支持 iCalendar(ics) 与 Outlook 等沟通

## 轻松文件分享 安全网络硬盘

对外 WebDAV HTTPS 网页连结分享

树状文件夹、加密

下载通知发件人、期限、次数、限制来源 IP

系统有完整记录

对内 公用文件夹



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

# EP 电子报 · 使命必达

## 成就优越的寄达、开信、点击率

有效的电子邮件营销，不仅要确保客户能收到讯息，更要知道客户喜爱怎样的讯息，以利营销人员持续精进营销作品与提高营销绩效。利用这套系统独特的编辑信件机制，可以将一般信件内容转换为各种收集条件，并将各类反应设定成不同积分，以利分析与提升电子邮件营销绩效。

### 电子报类型

可以设定名称、是否做为订阅页面选项、订阅页面显示名称(正体中文、简体中文、英文)、权限(使用者、群组)、附注；是否需要审核、审核者(主管、类型主管、自定义)、通知信箱、通知信语言；使用者是否可以多选、多选上限、取消订阅名单套用模式(符合任一、符合全部)。

### 营销范本

来源包含档案、网址。文件格式支持自动判断、RFC/822 格式(.eml)、MHTML 格式(.mht、.mhtml)、HTML 格式(.htm、.html)、ZIP 格式(.zip，包含 HTML 与图片文件)。网址仅限静态网页；JavaScript 或复杂 CSS 网页内容可能失真。

### 营销名单

包含营销名单、拒收名单、测试名单；用户可删除来自系统的营销名单；新增名单字段包含名称联络人、权限、附注；联络人提供新增、编辑、删除、汇入，汇入格式支持 .csv 格式、.txt 格式，资料分栏符支持逗号、分号、Tab，字段包含信箱、显示名称、公司名称、职称等等。

### 邮件发送

支持内嵌图转连结、群发单显、内容变量置换、在线预览、取消订阅、预约寄信、审核、网页版电子报显示社群网站分享链接等。

支持队列模式寄信、重送次数、队列重送时间、DKIM/DomainKeys/SPF 网域认证密钥、外寄速度、IP 化名、网卡 IP 绑定等。

### 计划任务

查询字段包含期间(最近 N 日/周/月、自年月日至年月日)、使用者、主旨、审核账号、审核结果(全部、待审核、允许、不允许)；支持比对方式(部分比对、完全比对、靠左比对、靠右比对)、是否显示已删除。列表字段包含寄信时间、发件人、主旨、使用者、审核账号、审核结果、审核意见、审核时间、发送状态；发送状态包含。动作包含审核(是否同意、审核意见)、删除。

### 统计报表

查询字段包含期间(最近 N 日/周/月、期间)、使用者(用户、群组)、电子报类型。列表字段包含使用者、发送数、信箱数、成功数、失败数、开信数、点击数、成功率、失败率。

### 营销日志

查询字段包含期间(最近 N 日/周/月、期间)、发件人、主旨；支持比对方式(部分比对、完全比对、靠左比对、靠右比对)。列表字段包含营销活动、主旨、信箱数、取消订阅、失败率、成功率、开信率、点击率、订阅异动率；营销活动信息包含营销活动、电子报类型、账号、活动时间、主旨、发件人、系统名单、拒收名单、其他收件者、取消订阅、总收件者数、预约寄信、讯息代号。发送日志显示字段：收件者、寄件日期、DSN 代码、寄送结果。查询条件：支持名单筛选、收件者、过滤寄送结果(全部、成功、失败、队列)、开信(全部、已开信、未开信)、点击(全部、已点击、未点击)。

### 系统特点

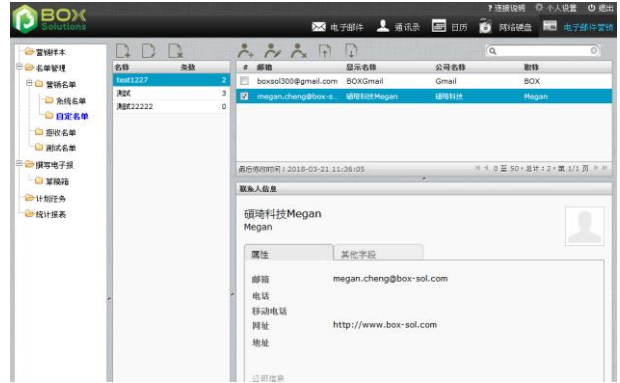
取消订阅支持自定义文字、图形化 RWD 可以针对查询结果执行二次营销 定义收件者行为积分，以利分析与第三方系统整合 API 与 CRM 同步名单 与 CRM 同步日志

# EP 电子报操作接口

## 邮件版型



## 邮件名单



## 邮件发送



## 计划任务



## 寄送报告



## 二次营销



## 邮件类型



## 图形化 RWD 取消订阅



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 上海市市长宁区定西路 1277 号长峰大厦 3006 室 T 021-5238-3756