Softnext

新型态邮件攻击防御方案

Email X Malicious Analyzation X Threat Defense

90% 的渗透攻击以恶意威胁邮件的形式进入企业

71% 的恶意软件是被创新出，并只使用一次

76% 的企业曾发生非预期的危险联机

新型态邮件攻击防御方案

Email X Malicious Analyzation X Threat Defense

> **企业只分为两种：已经被入侵的 与 即将被入侵的**
> **甚至正融合为一个类别-已经被入侵的并将再度被入侵的**
>
> There are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.
>
> Robert Muller, Former FBI Director
> 前美国联邦调查局局长

企业不论规模大小，都面临黑客威胁攻击的严峻考验

网络安全话题已从垃圾邮件、破坏为目的病毒邮件转变为追求利益的攻击，例如自 2013 年开始广泛出现至今仍难以扼止的勒索病毒、企业汇款诈骗、以及 APT 攻击。为了能够得到更好的收益，黑客攻击的对象也不再局限于政府单位或大型企业，人人都是勒索病毒的攻击目标；只要有贸易行为，就是黑客眼中诈骗汇款的肥羊；信息安全防护较弱的中小企业也成为 APT 攻击目标，因为只要能够入侵中小企业，要渗透攻击合作的上下游大型企业就不是什么难事了。

锁定从事跨国贸易的企业集团　攻击转向防护相对不完善的企业集团　人人都是黑客目标

上述威胁大多利用电子邮件搭配社交工程发起攻击，再通过恶意软件、恶意网页、中继站等多种工具的运行达成入侵的目的。

为何防病毒软件无法拦阻进阶式邮件攻击？

既然邮件威胁大多通过电子邮件发送恶意软件发起攻击，为何杀毒软件无法拦阻进阶式邮件攻击？

关键在于病毒与 APT 有着不同的攻击目的：无差别病毒攻击与客制化针对型攻击。无差别病毒攻击不分对象，目的在短时间内造成大规模的破坏与感染，快速为攻击者带来利益。客制化针对型攻击，则是黑客锁定明确目标而量身打造，这类攻击手法复杂且隐匿性高不易被诱捕，因此一般的防毒机制无法在短时间内拦截，受攻击者难以肉眼察觉分辨。

> **单一防御技术已无法抵御现今攻击渠道复合、多变、不易归纳出固定模式的攻击，面对不同的攻击手法，应采取不同的防御技术来对应**

Softnext 以先进理念开发防御技术，提供企业威胁防御对策

Softnext 守内安长期观察邮件网络安全趋势，以先进理念开发防御技术，提供企业威胁防御对策，除了可防护来自电子邮件与网页等恶意攻击，留存相关攻击记录外，当渗透攻击事件发生时，亦提供信息安全事件处理咨询与专家顾问服务。

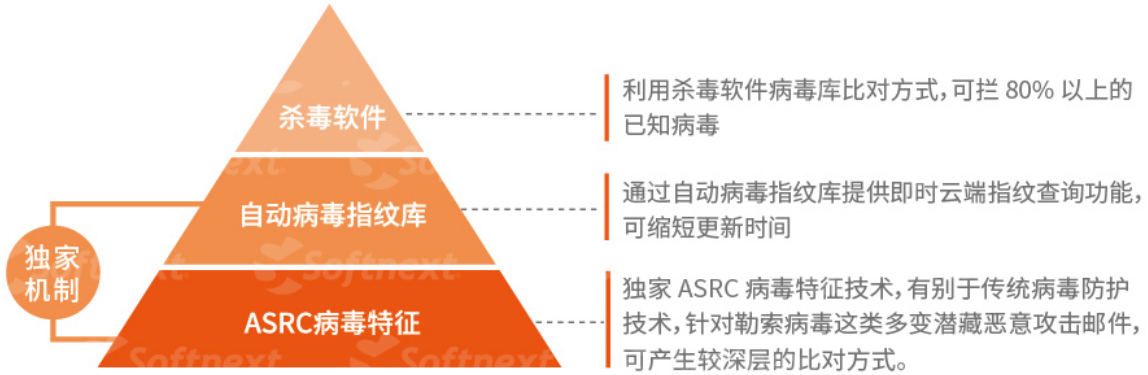
面对不同的攻击手法，采取不同的防御技术对应

攻击手法	无差别病毒攻击 一般病毒、Rootkit、蠕虫、间谍软件、后门程序及勒索病毒	客制化 / 针对型攻击 诈骗、针对型鱼叉攻击、APT 攻击
静态特征	SPAM SQR 标准防毒功能 | 双重防毒模块	SPAM SQR ADM高级防御模块
动态沙箱	内建多重分析引擎	

SPAM SQR病毒防御机制，防范无差别病毒攻击

SPAM SQR 可同时挂载多防毒引擎，并结合自动指纹辨识与 ASRC 病毒特征防护，达到较好的拦截效果。

SPAM SQR 病毒防御机制



静态特征联合动态沙箱分析，防御更全面

进阶持续性攻击的目的在于以各种方法击溃企业的安全防线，然而这些方法为成功达成目的尽其所能地避开现有的防御机制。SPAM SQR 通过多层次过滤技术，可先行分类垃圾邮件及可疑威胁邮件，再将特定格式附件拆离传送至沙箱进行比对，于虚拟平台进行程序运作状态分析。通过分析软件的仿真，再将监测程序运作过程所产生的行为回传至 SPAM SQR，将动态沙箱分析结果统一整合于 SPAM SQR，揭露风险一目了然且更易于管理。

SPAM SQR ADM & 动态沙箱联防特色

良好的分析速度
分类扫瞄 节省资源消耗

动静态交叉分析
增加入侵的困难

单一系统整合报表
风险揭露 易于追踪

SPAM SQR ADM 静态特征防御，先期抵御新型态攻击

ADM (Advanced Defense Module) 高级防御模块，通过长时间的追踪并模拟黑客攻击行为，利用云端差分技术更新静态特征。程序会自动解封装档案进行扫描，可发掘潜在代码、隐藏的逻辑路径及反组译程序代码，以利进行进阶恶意软件比对。可拦截附件及档案夹带零时差 (Zero-day) 恶意软件、使用APT 攻击工具及含有文件漏洞的攻击附件等攻击手法的威胁邮件。

ADM 机制特色

特征分析

有别于一般防毒商以被动式蜜罐捕获，采主动追踪攻击族群并产出特征

风险揭露

同时揭露漏洞编码、攻击工具及攻击族群等信息

快速反应

线上回报机制缩短反应时间

SPAM SQR 搭配动态沙箱分析侦测仿真复杂多变的攻击

通过创新的分层方法，结合了防毒特征码、信用评估、实时模拟防御、深层程序代码及动态分析 (沙箱作业)。一方面使用特征码和实时仿真这类分析强度较低的方法找出已知的恶意软件，进而确保高效能分析；另一方面也为沙箱作业新增深层程序代码分析功能，针对高度伪装、擅于规避的威胁提供更完善的检查。

动态沙箱特色

强大的分析能力

结合深层程序代码分析与动态分析，提供更精准的侦测功能

平衡的处理效能

动静态交叉比对，提升分析速度

客制化环境部署

最广的操作系统支持，以满足企业服务器环境

SPAM SQR 层层过滤邮件威胁，降低企业风险

防毒引擎

直接隔离已知病毒，防止不当转发降低中毒的风险

恶意档案分析引擎

逐层解封装档案进行扫描，可发掘潜在恶意软件及漏洞编码

威胁感知引擎

侦测邮件行为及频率，阻绝恶意瘫痪邮件系统等行为

智能诈骗侦测

检查邮件伪造痕迹并分析来源，当邮件放行至用户端时加强警示，藉以提高使用者警觉

动态沙箱

执行档案并检测程序造成的影响以及相关的行为，提供详细的历程和分析报告

Softnext 守内安信息科技

TEL : +86-21-51036007 FAX:+86-21-62741030
Email : service@softnext.com.cn
www.softnext.com.cn

产品最新资讯以官网内容为主

P0320E0320