# 绿盟 TAC-E 邮件高级威胁防护系统

# 产品白皮书

**【绿盟科技】**

| | | | |
|---|---|---|---|
| ■ **文档编号** | NSF-PROD-TAC-产品白皮书 | ■ **密级** | 完全公开 |
| ■ **版本编号** | V1.0 | ■ **日期** | 2019-08-02 |
| ■ **撰 写 人** | | ■ **批准人** | |

**© 2019 绿盟科技**

■ **版权声明**

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**绿盟科技**所有，受到有关产权及版权法保护。任何个人、机构未经**绿盟科技**的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ **版本变更记录**

| 时间 | 版本 | 说明 | 修改人 |
| --- | --- | --- | --- |
| 2019-08-02 | V1.0 | 新建 | 林俊 |
| | | | |
| | | | |
| | | | |
| | | | |

# 目录

一. 现状概述 1

二. 系统简介 2

三. 检测能力 4

四. 系统部署 8

# 一. 现状概述

*“Email is the preferred channel to launch advanced targeted attacks”*

*.Gartner: Magic Quadrant for Secure Email Gateways*

## 1.1 高级持续性威胁成为主流攻击方式

如今，政府和企业同时面临着一个不断演变的网络威胁环境。早期的黑客攻击是为了获得影响力及自我满足去发起攻击，而现在已演变成为了经济、政治等目的的攻击。

攻击者能够通过窃取知识产权来直接获取利益，也可以入侵、窃取客户的个人金融信息，甚至直接加密文档后进行赤裸裸的勒索，更有甚者破坏对方的服务以至国家的基础设施。动机的变化，同时也带来了攻击方式的变化。

## 1.2 邮件是发起高级定向攻击的首选渠道

电子邮件系统在各个行业应用广泛，因其使用便捷且相对开放，已成为攻击者发起攻击的首选渠道。

从早年得“Operation Aurora”（极光）事件、到近年来的“APT28”” Darkhotel”，大量的 APT 事件中，攻击者都采用鱼叉邮件的方式展开攻击。

## 1.3 传统邮件网关难以应对复杂邮件威胁

邮件安全网关是常见的邮件安全防御方案，主要依赖特征及信用发现威胁邮件/垃圾邮件。目前典型的攻击邮融合了社交工程，身份欺骗，网络钓鱼站点，恶意软件、无威胁软件等攻击手段，电子邮件威胁已成为多种威胁技术的组合。

新型邮件威胁往往可以逃避传统邮件安全网关的检测，特别是那些只具备特征检测能力的解决方案。

# 二. 系统简介

## 2.1 产品概述

绿盟 TAC-E 邮件高级威胁防护系统是针对邮件投递过程中的勒索病毒，特种木马等高级威胁进行检测与处置的邮件安全产品。系统内置信誉检测、病毒检测、静态检测、动态检测引擎，可有效发现并拦截各类已知与未知威胁，保护用户免受邮件高级威胁攻击。

针对外发邮件内容，提供基于正则的文本内容检测能力，及时发现可能的敏感信息外泄行为。

## 2.2 应用场景

系统适用于本地自建邮件系统安全防护：

**入站：**

已知病毒邮件检测

高级威胁邮件检测

无恶意代码威胁邮件检测

钓鱼邮件检测

**出站：**

敏感信息外发检测

## 2.3 系统特性

**互补传统邮件安全网关：**

TAC-E 邮件高级威胁防护系统可与传统的邮件安全网关互补，构建完整覆盖反垃圾、反病毒、反高级威胁的安全防护体系。系统可与传统邮件安全网关协同部署，在不影响原有部署拓扑的情况下，实现高级威胁防御能力的上线和融合。

**具备未知威胁检测能力：**

高级可持续性威胁，多采用定制化的攻击工具（木马、后门等恶意软件），甚至还会使用零日漏洞，这样的攻击方式传统的安全检测体系很难有效发现，针对这种情况，TAC-E 提供了检测零日漏洞、未知木马等未知威胁的能力。

**可不依赖传统签名技术：**

基于先进的动态检测技术，即基于沙箱虚拟执行的方式，可以根据邮件附件在虚拟环境中的代码行为特征进行实时分析，来判断是否存在攻击特征，这种检测方式不需庞大的检测签名库，并且可以防止各种针对静态检测的逃避技术。是业界认可的高级威胁检测技术。

**集成已知威胁检测技术：**

攻击和监测的对抗是一个复杂的过程，应该考虑到有多种可能的攻击方式，TAC-E 集成了专业的反病毒引擎与文件静态检测引擎，以此提高系统对已知威胁的检测能力。已知威胁检测技术是邮件高级威胁防护系统的必要组成部分，它可弥补动态检测的在效率上的不足之处，构建更完备可靠的安全防御体系。

**提供威胁行为及处置建议：**

为了有效的进行安全响应，还需要监测系统能够提供详尽的报警信息，使响应的安全人员可以有的放矢的开展工作。具体的报警信息可以包括：是否修改了注册表，是否新建了进程，是否尝试对外连接命令与控制服务器，是否会直接感染其它机器等。系统可监测恶意软件是否有上述的活动，作为报警的一部分并在分析报告中提供处置建议输出给安全管理员。

# 三. 检测能力

## 3.1 信誉/情报检测

系统内置信誉检测引擎，通过 NTI（NSFOCUS Threat Intelligence center）获取最新威胁情报，支持在线与离线升级，实现对最新恶意 URL 和恶意文件的检测。

依托于绿盟科技多年的安全研究和安全沉淀，NTI 持续跟踪国内外网络安全研究动向，持续开展漏洞挖掘分析、逆向工程、入侵检测和防御、抗分布式拒绝服务、恶意软件、攻击行为分析和检测、蜜罐和蜜网等安全专项研究，在安全漏洞、入侵规则、恶意样本、安全事件等方面积累了大量的特色数据。

NTI 还集成了开源情报、商业购买情报、战略合作情报，通过不断丰富情报数据数量和情报类型，为客户提供更全面的威胁检测能力。

## 3.2 病毒检测

系统提供基于文件方式的病毒检测功能。内置第三方 av 检测引擎以及特征库，通过签名技术实现对恶意邮件附件的检测，同时集成绿盟自研 AVE 引擎作为检测能力补充。

1) 支持 AV 病毒库的在线与离线升级

2) 支持压缩文件的病毒检测（.rar、.zip、.7z、.tar、.gz、.bz2、.gzip、.tgz）

3) 支持 office 类文件的病毒检测（.ppt、.pptx、.rtf、.xls、.xlsx、.doc、.docx）

4) 其他类型文件的病毒检测

（.swf、.html、.xml、.js、.exe、.dll、.scr、.com、.pif、.bat、.pdf、.class、.jar）

5) 除以上提到的文件类型外，不管是正常文件还是恶意文件，有无扩展名都会进行病毒检测。

### 3.3 静态检测

系统提供基于虚拟执行的静态检测能力，主要针对邮件附件中常见的各类 OFFCIE 文档、PDF 文件、网络类文件。静态引擎会尝试分析传递进入的邮件附件文件类型，不同文件类型会进入不同的子引擎，子引擎主要包括 JS 引擎，AS 引擎和 shellcode 引擎。网页类的文件包括 HTML 文件、JS 文件、XML 文件进入 JS 引擎，SWF 类型的文件进入 AS 引擎，其它文件会进入 shellcode 检测引擎，最终输出是否在样本中发现了漏洞利用特征。

### 3.4 Shellcode 检测

恶意攻击软件中具体的攻击功能实现是一段攻击者精心构造的可执行代码，即 ShellCode。一般是开启 Shell、下载并执行攻击程序、添加系统账户等。由于通常攻击程序中一定会包含 ShellCode，所以可以检测是否存在 ShellCode 作为监测恶意软件的依据。这种检测技术不依赖与特定的攻击样本或者漏洞利用方式，可以有效的检测已知、未知威胁。

需要注意的是由于传统的 ShellCode 检测已经被业界一些厂商使用，因此攻击者在构造 ShellCode 时，往往会使用一些变形技术来规避。主要手段就是对相应的功能字段进行编码，达到攻击客户端时，解码字段首先运行，对编码后的功能字段进行解码，然后跳到解码后的功能字段执行。这样的情况下，简单的匹配相关的攻击功能字段就无法发现相关威胁了。

系统在传统 ShellCode 检测基础上，增加了文件解码功能，通过对不同文件格式的解码，还原出攻击功能字段，从而在新的情势下，依然可以检测出已知、未知威胁。在系统中，此方式作为沙箱检测的有益补充，使系统具备更强的检测能力，提升攻击检测率。

### 3.5 动态检测

动态沙箱检测，也称虚拟执行检测，它通过虚拟机技术建立多个不同的应用环境，观察程序在其中的行为，来判断是否存在攻击。这种方式可以检测已知和未知威胁，并且因为分析的是真实应用环境下的真实行为，因此可以做到极低的误报率，而较高的检测率。

检测系统具备指令级的代码分析能力，可以跟踪分析指令特征以及行为特征。指令特征包括了堆、栈中的代码执行情况等，通过指令运行中的内存空间的异常变化，可以发现各种溢出攻击等漏洞利用行为，发现 0day 漏洞。 系统同时跟踪以下的行为特征，包括：

进程的创建中止，进程注入；

服务、驱动

注册表访问、改写

文件访问、改写、下载

程序端口监听

网络访问行为

其他行为检测…

系统根据以上行为特征，综合分析找到属于攻击威胁的行为特征，进而发现 0day 木马等恶意软件。

系统发现恶意软件后，会持续观察其进一步的行为，包括网络、文件、进程、注册表等等，作为报警内容的一部分输出给安全管理员，方便追查和审计。而其中恶意软件连接 C&C 服务器（命令与控制服务器）的网络特征也可以进一步被用来发现、跟踪 botnet 网络。

### 3.6 敏感信息检测

针对外发邮件，系统支持以关键字或正则表达式的方式对敏感信息检修检测。关键词即指定的文本词语，如秘密、机密、绝密等标记信息；正则表达式是对字符串操作的一种逻辑

公式，通过事先定义好的一些特定字符、及这些特定字符的组合，组成一个“规则字符串”，这个“规则字符串”用来表达对字符串的一种过滤逻辑。通过正则可灵活定义如身份证号、银行卡号、手机号等信息。系统同时支持识别外发文件中的附件类型，并根据预定规则产生告警；敏感信息匹配范围包括邮件标题、正文、附件；

# 四. 系统部署

## 4.1 MTA 部署

MTA(Mail Transfer Agent) 模式下，TAC-E 参与邮件转发，系统逻辑串接在反垃圾邮件网关与邮件服务器之间。如网络中没有反垃圾邮件网关，TAC-E 则逻辑串接在邮件服务器前，支持对威胁邮件的检测与处置。

## 4.2 BCC 部署

BCC（Blind Carbon Copy）模式下，TAC-E 类似于旁路设备，接收邮件服务器或其他邮件安全设备抄送给 TAC-E 的邮件进行检测。BCC 模式下支持检测威胁邮件，发现威胁只产生告警，无法进行拦截、隔离等处置动作。

## 4.3 多机部署

为避免单点故障，MTA/BCC 模式下，均可部署两台/多台 TAC-E 同时工作，通过 DNS 解析实现对两台/多台设备的负载均衡与故障切换。同时可通过 ESPC（绿盟企业安全中心）对多台设备的日志及运行状态进行统一管理。