



# TAC产品使用分析培训

绿盟科技版权所有

2019护网专项培训



# CONTENTS 目录 >>>

- 01 产品简介
- 02 部署方式
- 03 TAC的使用和配置
- 04 FAQ
- 05 日志分析



01

# 产品简介

绿盟科技版权所有

## ▶▶ **TAC**是什么？

- ◆ TAC: Threat Analysis Center
- ◆ 威胁分析系统
- ◆ 针对高级威胁，具备多种检测能力的分析系统
- ◆ 针对APT、勒索软件、特种木马等高级威胁的，具备信誉、病毒检测、静态、动态检测技术的威胁分析系统
- ◆ TAC可以作为传统安全设备检测能力的扩展组件：与IPS/FW/SEG联动，组成NGTP解决方案，通过联动，建立针对高级威胁的检测与防御能力

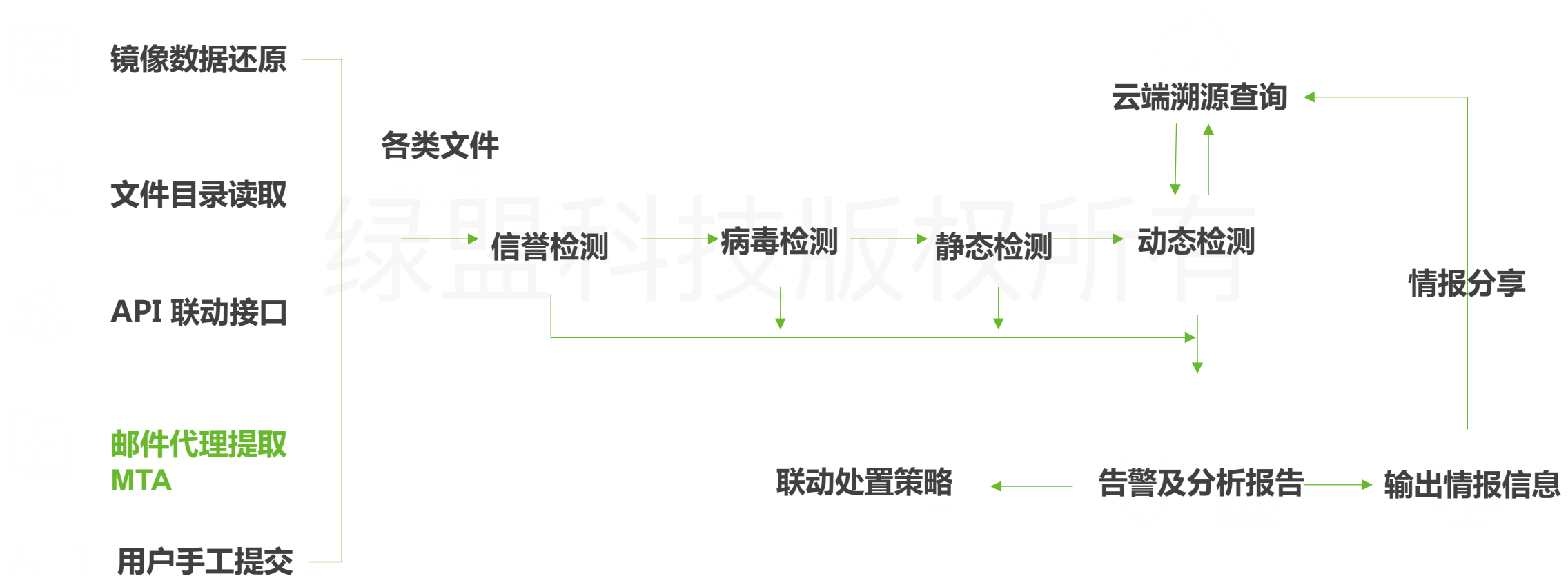
## ▶▶ 三种系列

- ◆ D系列：绿盟威胁分析系统D系列（NSFOCUS Threat Analysis Center D-series），网络高级威胁检测系统
- ◆ E系列：绿盟威胁分析系统E系列（NSFOCUS Threat Analysis Center E-series），邮件高级威胁防御系统
- ◆ V系列：绿盟威胁分析系统V系列（NSFOCUS Threat Analysis Center V-series），虚拟化部署

## ▶▶ TAC检测

- ◆ 信誉检测：基于黑白IP/URL/域名/MD5等情报信息检测可疑链接与文件
- ◆ 病毒检测：基于专业的Bitdefender与火绒引擎检测已知病毒
- ◆ 静态检测：基于静态特征检测隐藏在文件中的可疑SHELLCODE与可执行脚本
- ◆ 动态检测：俗称沙箱，利用虚拟化技术，模拟用户操作环境运行可疑文件，通过文件行为检测威胁

# ▶▶ TAC工作原理



# ▶▶ TAC的检测对象



## 常见文件载体

例如office文档、pdf、exe、zip、rar等可在windows 平台执行的文件



## 企业自建邮件系统：

包括邮件正文中的域名、url地址、邮件附件



## 安卓移动应用：

apk安装文件

绿盟科技版权所有





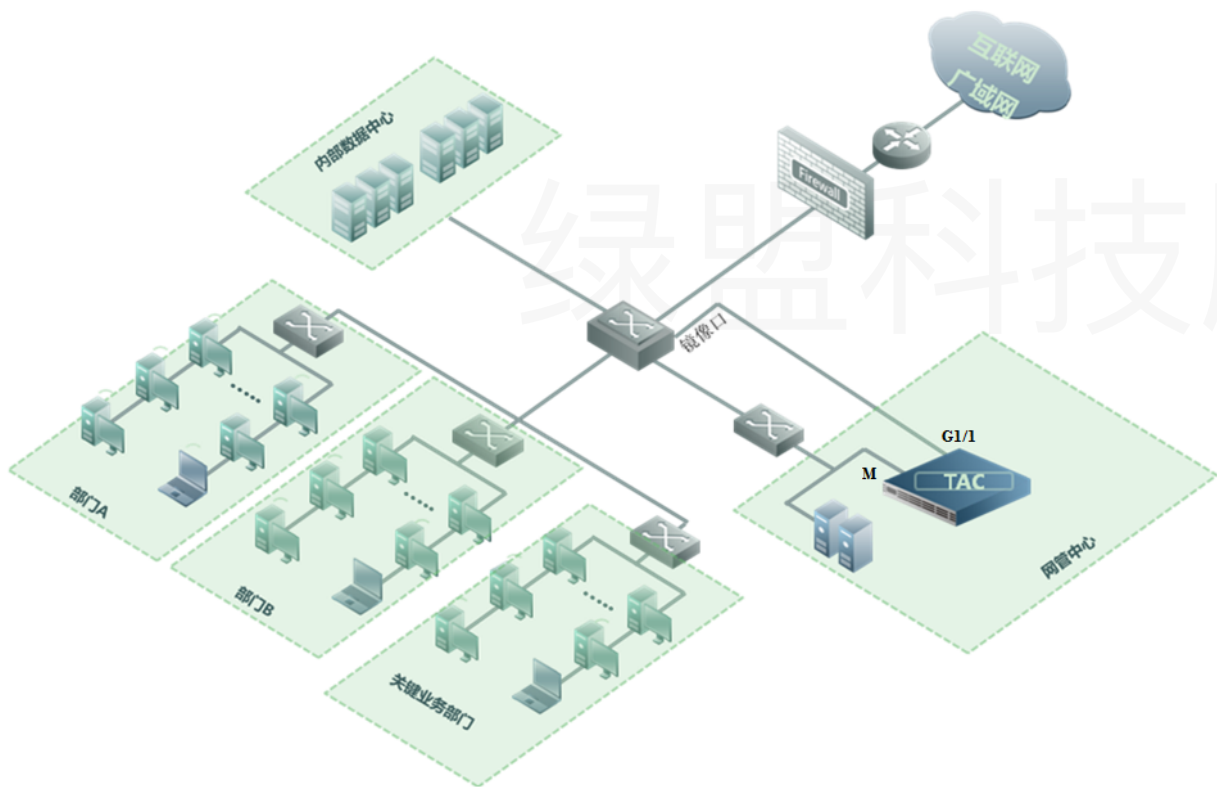
02

# 部署方式

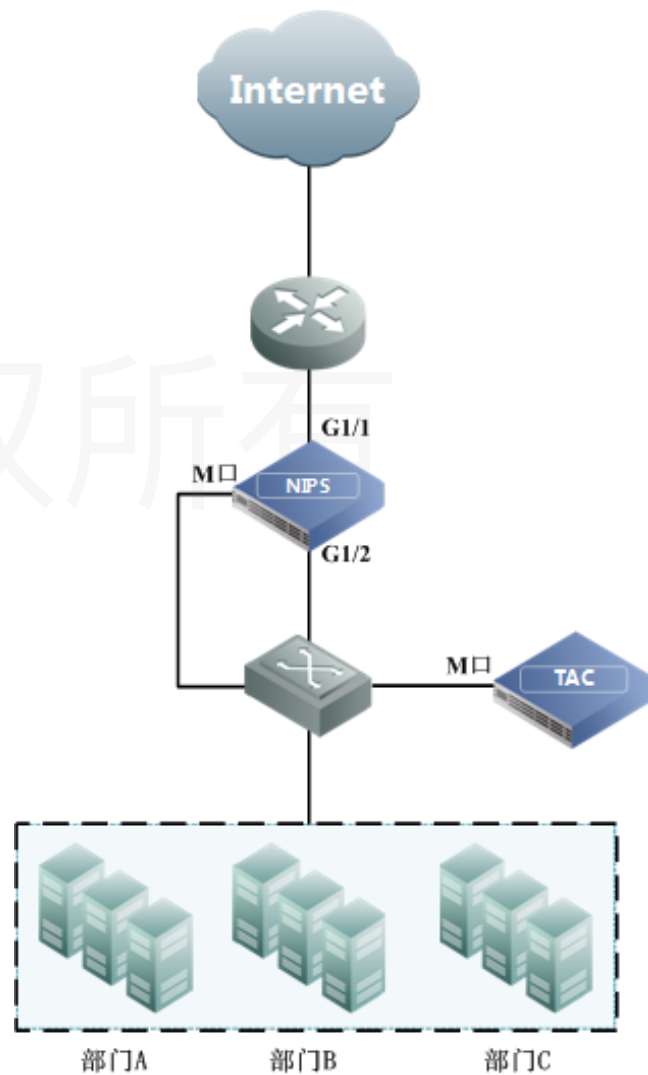
绿盟和网安版权所有

# ▶▶ TAC-D部署方式

监听部署：

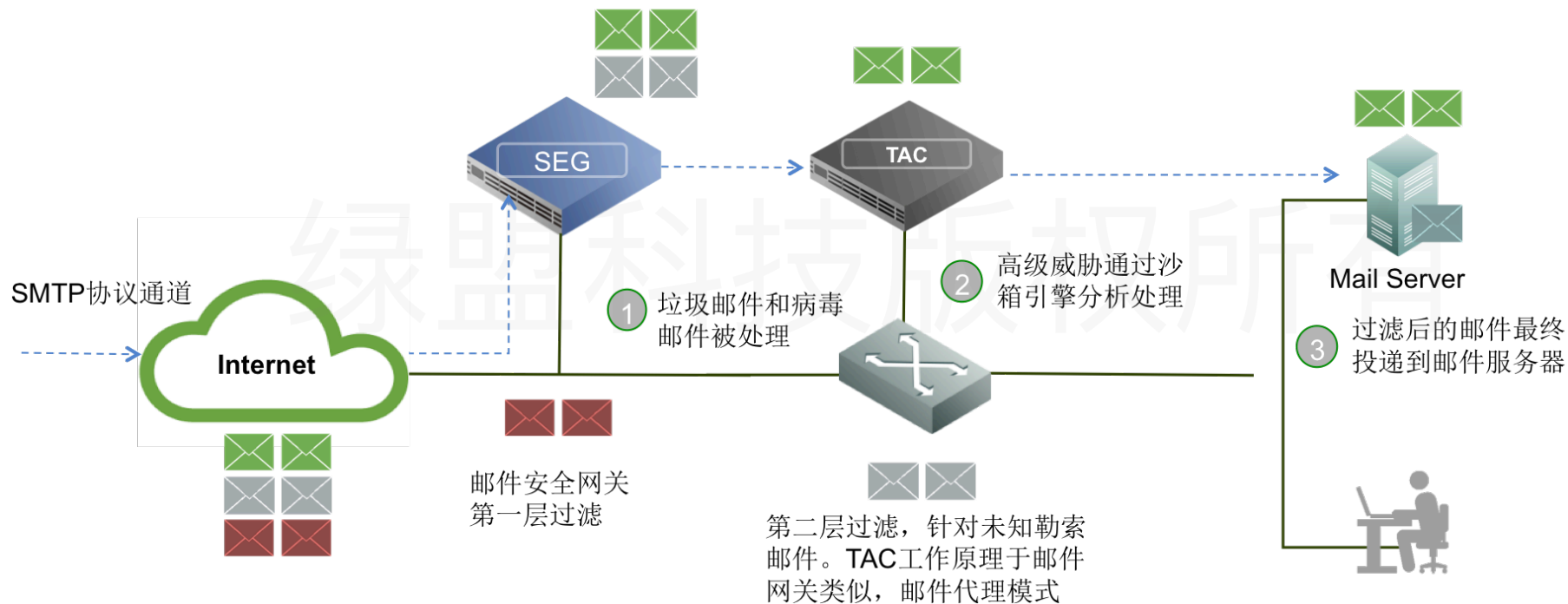


联动部署：



# ▶▶ TAC-E部署方式

邮件网关部署：





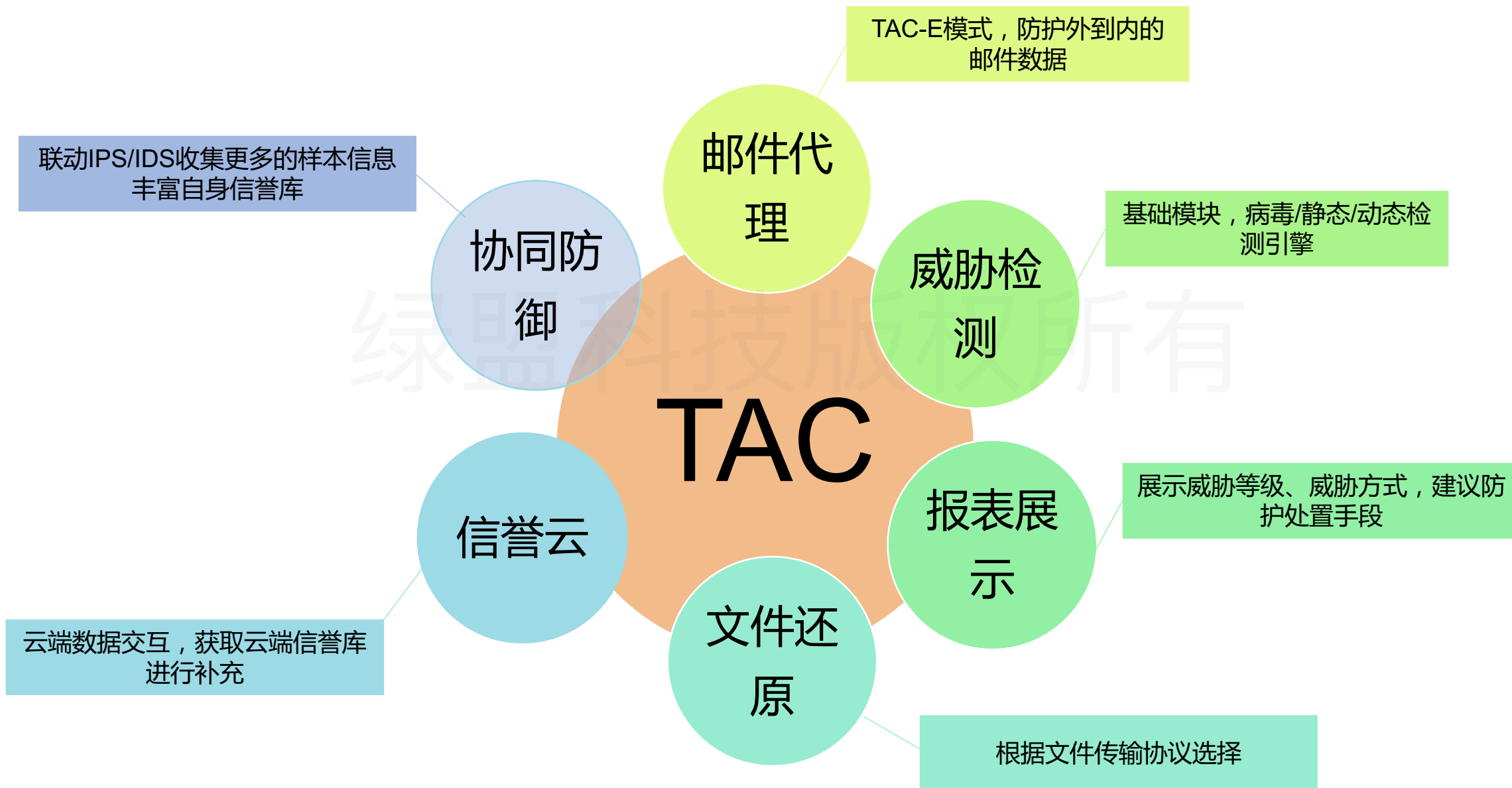
03

# TAC的使用和配置

## ▶▶ 初始web账户

	Web操作员	Web审计员	Console口管理员
用户名	admin	auditor	conadmin
密码		无	

# 主要功能



# TAC-D威胁检测

## TAC

实时监控

策略

- 威胁检测
- 文件还原
- 用户管理
- 协同防御
- 文件扫描
- 信誉云
- 自定义规则
- 白名单管理

日志报表

系统

### 威胁检测

#### 病毒检测

BitDefender引擎  开启  关闭

火绒引擎  开启  关闭

#### 静态检测

启用  是  否

#### 动态检测

启用  是  否

自定义规则  是  否

文件类型识别  后缀优先  内容优先

行为白名单  开启  关闭

网络访问控制  ?

沙箱逃逸检测  是  否

虚拟环境 \*

- WinXP SP3(o2k7,IE8,r1010,f102152) V2.3.0
- WinXP SP3(o2k3,IE6,r90,f10r1236) V2.3.0
- WinXP SP3(o2k7,IE8,r1010,f102152,w2013) V2.3.0
- Win7 SP1(o2010,IE9,r1100,f115502) V2.3.0
- Win7 SP1(o2013,IE11,r11r10,f16r287) V2.3.0
- Win10 1709(o2016,r151536,IE11,f1800160) V2.3.0
- Android 4.4.4 V2.3.0

保存

CPU- 20% , 内存- 8% , 系统空间- 86% , 数据空间- 1% 系统信息

## 威胁检测

静态检测：静态检测引擎新增复合格式检测、JS样本检测、office宏检测，新增内置yara规则。复合格式检测即针对PE类修改后后缀为图片格式的样本检测告警，告警摘要如下：

### 分析概述

文件名称	md5.exe.jpg
文件类型	Win32 EXE
文件大小	80.0KB (81920 bytes)
会话信息	10.14.80.1:51265 → 127.0.0.1:0
文件来源	admin[10.14.80.1],2017-03-01 15:55:48,手动上传

威胁等级

高

威胁行为	1)可疑文件
危害	1)含有可疑特征的文件

### 威胁详情

高威胁 !

可疑文件

Suspicious File : PE file with fabricate extension



## ▶▶ 威胁检测

### □ 压缩包检测：

新增压缩包检测引擎，处理压缩包样本，进行解压和检测恶意压缩包样本，压缩包检测引擎在web界面没有展示。

### □ 动态检测：

动态引擎新增自定义规则、网络访问控制、沙箱逃逸检测，另外告警日志的展示相对201也有很大的改变，增加了威胁行为、危害和处理建议，整个页面的展示风格也跟以前有所不同。

## ▶▶ 威胁检测

- 自定义规则可以支持用户自定义动态规则，可以通过备份恢复中的恢复功能导入用户自定义的规则，规则导入后重启引擎生效。
- 网络访问控制分为三种，默认配置为限制部分访问，即限制虚拟机访问私有网络地址；限制网络访问即限制虚拟机网络访问，不能访问任何地址；开放网络访问即不做任何限制。
- 沙箱逃逸检测默认支持，web上不能配置，TAC检测到沙箱逃逸的样本后再文件分析报告中会有具体展示。下面是导出的一份动态检测样本的分析报告：



Adobe Acrobat  
Document

# ▶▶ TAC-E

□ 邮件代理配置步骤：

□ 1、选择菜单 **策略 > 邮件代理 > 邮件代理**，进入邮件代理配置页面

TAC

实时监控

策略

威胁检测

**邮件代理**

信誉云

自定义规则

白名单管理

日志报表

系统

邮件代理 收信域 投递路由 个性化配置

系统主域设置

主域

声明主机名设置

主机名

模式设置

模式选择 监控

延迟发送

时间(分) 2

可信网络

网络对象

保存

主域：内部邮件系统的主域名称  
主机名：TAC对外发送smtp  
helo/echo 的名称

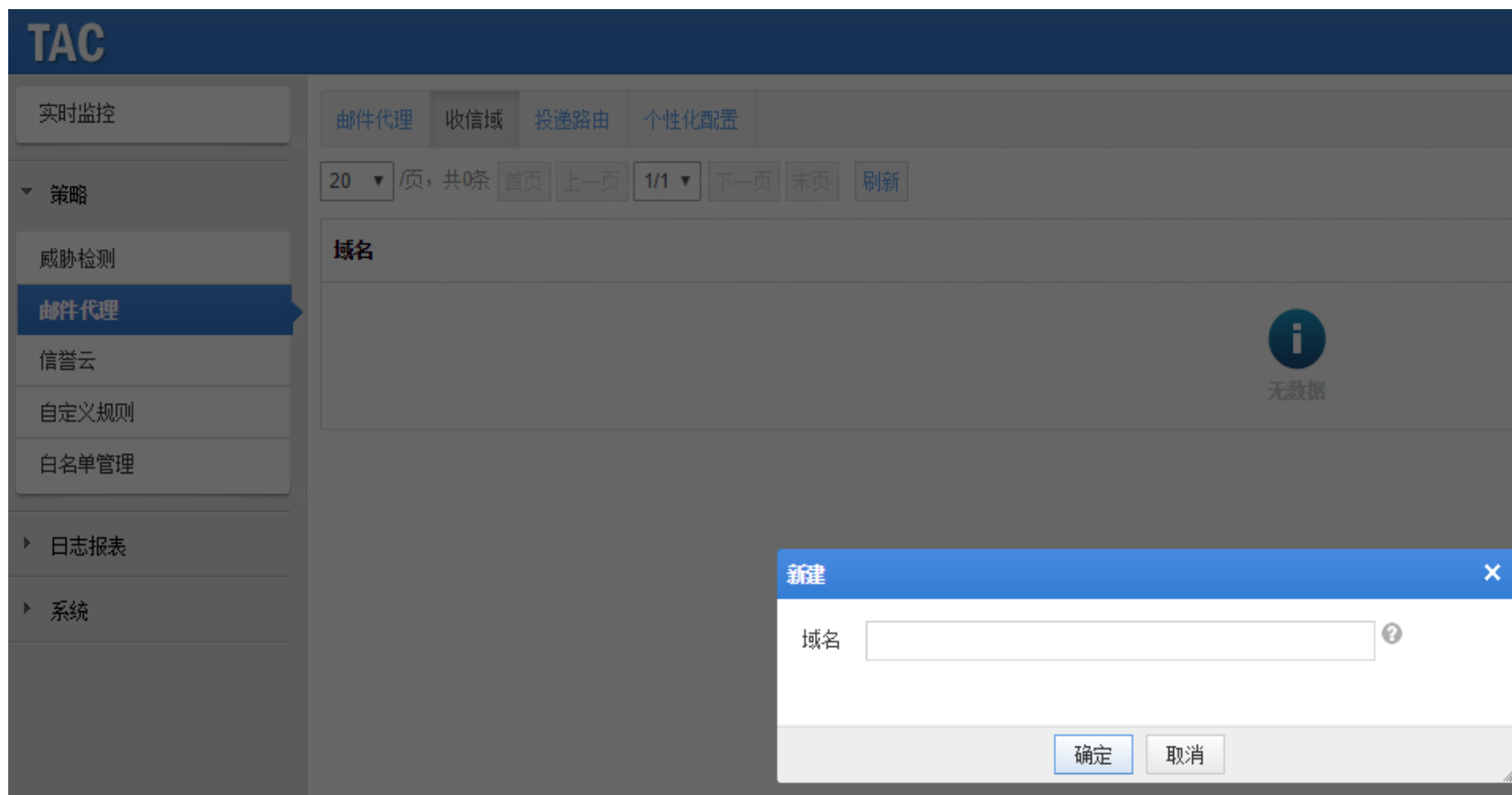
**隔离**：检测到异常邮件进行隔离。  
**监控**：检测到异常邮件进行告警。

延迟发送：邮件最大延迟发送时间

# ▶▶ TAC-E

□ 邮件代理配置步骤：

□ 2、选择菜单 **策略 > 邮件代理 > 收信域**，进入收信域防护配置页面



收信域是指TAC作为邮件网关，TAC只对收信域列表中的邮件进行检测。

# ▶▶ TAC-E

□ 邮件代理配置步骤：

□ 3、选择菜单 **策略 > 邮件代理 > 投递路由**，进入投递路由配置页面

The screenshot displays the TAC-E management interface. On the left, a sidebar menu shows '策略' (Strategy) expanded to '邮件代理' (Mail Proxy). The main area has tabs for '邮件代理', '收信域', '投递路由', and '个性化配置'. Below the tabs, there's a pagination bar showing '20 / 页, 共0条' and navigation buttons. A table with columns '域名' and '转发至' is visible, but it's empty. A modal dialog titled '新建' (New) is open, containing two input fields: '域名' (Domain) and '转发至' (Forward to), with '确定' (Confirm) and '取消' (Cancel) buttons at the bottom.

投递路由为收信域指明了邮件的转发路径。当邮件到达TAC并经安全检测后，按照投递路由的设置，将检测后未发现异常的邮件转发至目的地。

# ▶▶ 信誉云

□如果设备能够正常上网，且证书中包含信誉云模块，则设备每天早上七点从云端拉取信誉（文件信誉和url信誉），一天更新一次，初始状态这两个信誉文件都是空的。若证书中不包含信誉云模块，TAC虽然可以连上云，但是无法拉取信誉。

证书状态	正常
证书类型	试用证书
产品型号	TAC
序列号	031D-5B60-76BA-53FB
功能模块	邮件网关 信誉云
颁发对象	试用证书
本期服务起始日期	2019-05-08
本期服务终止日期	2020-06-09

设备上的开关控制信誉检测的时候过不过云信誉文件，若选择启用信誉检测，则设备在信誉检测的时候会过从云端更新到的两个信誉文件；若选择否，则设备在信誉检测的时候不过从云端更新到的信誉文件。

## 协同防御

- 原有的API管理模块现在放在协同防御标签页下，新增了提交记录和企业信誉两个功能。
- 提交记录中记录了第三方如IPS、NF或其他使用API账号通过API接口提交文件进行检测的提交信息，包括提交IP、提交文件总数、和最近提交时间。

The screenshot displays the TAC interface with the '协同防御' (Collaborative Defense) section selected. The main content area shows a table of submission records under the '提交记录' (Submission Records) tab. The table has columns for '提交IP' (Submission IP), '提交文件总数' (Total Files Submitted), and '最近提交时间' (Last Submission Time). The user 'admin' is logged in.

提交IP	提交文件总数	最近提交时间
10.67.4.10	2571	2017-03-01 14:03:25
10.14.53.33	10038	2017-02-10 14:04:17
10.14.43.94	91	2017-01-13 17:22:16
10.66.250.120	115	2017-01-12 16:07:05
10.8.202.101	1344	2017-01-12 14:22:53
10.14.19.120	612	2017-01-09 15:05:13
10.8.15.31	176	2017-01-03 16:08:29

## 协同防御

企业信誉中记录了TAC自身产生的信誉信息，包括文件信誉、URL信誉和CC信誉，以及这些信誉的最后更新时间（TAC需开启专业参数中generate\_credit参数才能产生信誉）。

**TAC**

实时监控

策略

威胁检测

文件还原

用户管理

**协同防御**

文件扫描

信誉云

自定义规则

白名单管理

日志报表

系统

API帐号管理 提交记录 企业信誉

信誉信息:文件信誉:0(未更新),URL信誉:0(未更新),CC信誉:0(未更新) [清空全部信誉](#)

操作

时间范围 2017-04-17 06:00:00 - 2017-04-18 06:00:00

信誉类型 文件信誉

文件MD5

文件信誉

URL信誉

CC信誉

查询



# 文件还原

## TAC

- 实时监控
- 策略
  - 威胁检测
  - 文件还原**
  - 用户管理
  - 协同防御
  - 文件扫描
  - 信誉云
  - 自定义规则
  - 白名单管理
- 日志报表
- 系统

### 文件还原

应用协议  HTTP下载  HTTP上传  FTP  SMTP  POP3  IMAP

绿盟科技版权所有

# 文件扫描

□ 202版本中将之前的D、F、P系列三个系列合并，文件扫描的功能添加至策略目录下。文件扫描任务的具体功能与之前离线扫描系列一致。

The screenshot shows the TAC interface with the '文件扫描' (File Scanning) section active. The sidebar on the left lists various security features, with '文件扫描' highlighted. The main content area displays a table of scanning tasks. The table has the following columns: '任务号' (Task ID), '任务名称' (Task Name), '检测对象' (Detection Object), '检测类型' (Detection Type), '开始时间-结束时间' (Start Time-End Time), '威胁等级' (Threat Level), '进度' (Progress), and '操作' (Actions). Two tasks are visible, both with a progress of 100% and a threat level of '安全' (Safe).

任务号	任务名称	检测对象	检测类型	开始时间-结束时间	威胁等级	进度	操作
6	扫描文件样本_解压密码为nsf...	54dd5ec8d83814e dfb02...		2017-04-18 13:35:26 2017-04-18 14:54:52	安全	100%	
7	扫描文件样本_解压密码为nsf...			2017-04-18 13:35:26 2017-04-18 14:54:52	安全	100%	

# 文件扫描

包含文件上传和文件服务器扫描。

TAC

实时监控 文件扫描 新建

策略 25 页

任务类型  文件上传  文件服务器

新建

任务类型  文件上传  文件服务器

服务器路径 \*  支持SMB和FTP服务器。例: smb://192.168.1.10/pub, ftp://192.168.2.1/lib

帐号  例: intra/username

密码

任务名称 \*

白名单过滤  是  否

检测类型  病毒检测  静态检测  信誉检测  动态检测

执行方式

[高级选项>>](#)

备注

将文件拖拽至此区域, 不能超过10个



04

# FAQ

绿盟科技版权所有

## ▶▶ 注意事项

- 虚拟化TAC仅仅支持API上传文件检测，不支持镜像模式传输流量
- TAC各模块检测顺序：用户自定义白名单、用户自定义黑名单、文件白名单、信誉、防病毒、静态、动态
- Q：匹配了黑名单后，是否还会继续检测？
- A：匹配了白名单的不会再检测，匹配了黑名单和信誉的，会继续检测送到后面的检测引擎进行检测

## ▶▶ 注意事项

- ◆ 离线扫描时不能挂载根目录，只能挂载指定的文件夹；
- ◆ 推荐使用32G以上FAT32格式U盘对设备或虚拟机进行升级（不支持NTFS及其它格式），移动硬盘分区过多时可能出现加载失败的情况；
- ◆ av和静态检测引擎在检测之前都会过一次信誉检测，其中av的信誉检测只过白名单，静态的信誉检测黑白名单都过

## ▶▶ 注意事项

- ◆ 在界面上的文件分析报告处可以把样本加入白名单，在策略-白名单处也可以通过md5将样本加入白名单，这个白名单仅仅是将数据库file\_credit表该样本的level值置为0，只是该样本不生成告警了，但是样本进入TAC后依然会进行检测。
- ◆ 设备检测一个白样本3次，会自动把该样本加入白名单，此白名单放在/tmp/remote/db/file.db中，每次重启系统会清空。样本进入tac后会首先对比该白样本，如果匹配到该白名单则会直接放行，不再继续检测。



05

# 日志分析

绿盟科技版权所有



# 日志分析

## ■ 日志分析——威胁分析

TAC 您好, admin | 简体中文 | 关于 | 退出

实时监控 | 威胁分析

策略 | 日志报表 | 日志分析 | 统计报表 | 系统

威胁分析

Q 条件

20 /页, 共8条 | 首页 | 上一页 | 下一页 | 末页 | 1/1 页, 转到 | 操作

<input type="checkbox"/>	时间	告警摘要	客户端IP	服务端IP	文件名	应用摘要	样本来源	详情
<input type="checkbox"/>	2019-05-14 10:47:54	▲ Trojan.Downloader.JP...	10.102.1.49	127.0.0.1	注册机.rar	10.102.1.49	10.102.1.49	
<input type="checkbox"/>	2019-05-14 10:47:54	▲ Trojan.Downloader.JP...	10.102.1.49	127.0.0.1	注册机.exe	10.102.1.49	10.102.1.49	
<input type="checkbox"/>	2019-05-14 10:39:02	▲ Trojan.Downloader.JP...	10.14.166.60	123.58.178.212	注册机.rar	"123"<client660@16...		
<input type="checkbox"/>	2019-05-14 10:39:02	▲ Trojan.Downloader.JP...	10.14.166.60	123.58.178.212	注册机.exe	"123"<client660@16...		
<input type="checkbox"/>	2019-05-14 10:24:04	! Gen:Variant.Sirefef....	127.0.0.1	127.0.0.1	ZeroA...i.exe_			
<input type="checkbox"/>	2019-05-14 10:24:04	▲ Trojan.Inject.AKD	127.0.0.1	127.0.0.1	dumped.dll			
<input type="checkbox"/>	2019-05-14 10:24:04	▲ Trojan.Inject.AKD	127.0.0.1	127.0.0.1	cc-al...t.rar			
<input type="checkbox"/>	2019-05-14 10:19:13	! 可疑网络行为	10.14.53.47	10.34.55.91	cve-2...f.ppt	ftp://10.34.55.91/...		



# 日志分析

## 威胁分析——详情



### 文件分析报告

生成时间:2019-05-14 13:41:13



#### 分析概述

- 包含文件
- 威胁详情
- 静态信息

#### 分析概述

文件名称	注册机.rar
文件类型	RAR
文件大小	13.3KB (13589 bytes)
会话信息	10.102.1.49:3440 → 127.0.0.1:0
文件来源	nsfocus[10.102.1.49],2019-05-14 10:47:54,手动上传
威胁行为	1)下载器
危害	1)用来从远程服务器下载恶意程序, 安装并执行。
处理建议	1)使用杀软进行全盘查杀

威胁等级

高

#### 包含文件

子文件

子文件

文件摘要

文件上传



# 日志分析

## 威胁分析——详情



### 文件分析报告

生成时间:2019-05-14 13:41:13



#### 分析概述

- 包含文件
- 威胁详情
- 静态信息

#### 分析概述

文件名称	注册机.rar
文件类型	RAR
文件大小	13.3KB (13589 bytes)
会话信息	10.102.1.49:3440 → 127.0.0.1:0
文件来源	nsfocus[10.102.1.49],2019-05-14 10:47:54,手动上传
威胁行为	1)下载器
危害	1)用来从远程服务器下载恶意程序, 安装并执行。
处理建议	1)使用杀软进行全盘查杀

威胁等级

高

#### 包含文件

子文件

子文件

文件摘要

文件上传

# ▶▶ 首页展示

## ■ 自定义模块展示

The screenshot displays the TAC (Threat Analysis Center) interface. The top navigation bar includes the user name 'admin', language '简体中文', and links for '关于' and '退出'. The main content area is divided into several sections:

- 实时监控 (Real-time Monitoring):** A tabbed interface with '实时监控' and '接口状态' tabs.
- 策略 (Policies):** A sidebar menu with options for '策略', '日志报表', and '系统'.
- 自定义模块 (Custom Modules):** A row of filters for '受感染主机Top5', '服务端Top5', '可疑URL Top5', '流量监控', '接口信息', 'CC告警Top5', and '恶意邮件Top5'.
- 告警摘要 (Alert Summary):** A table listing various security alerts with columns for time, alert type, client IP, server IP, filename, and application summary.
- 可疑文件Top5 (Top 5 Suspicious Files):** A section at the bottom showing the top 5 most suspicious files.

时间	告警摘要	客户端IP	服务端IP	文件名	应用摘要	详情
2019-05-14 10:47:54	Trojan.Downloader.JP...	10.102.1.49	127.0.0.1	注册机.rar	10.102.1.49	
2019-05-14 10:39:02	Trojan.Downloader.JP...	10.14.166.60	123.58.178.212	注册机.rar	"123"<client660@16...	
2019-05-14 10:24:04	Trojan.Inject.AKD	127.0.0.1	127.0.0.1	cc-alert.rar		
2019-05-14 10:19:13	可疑网络行为	10.14.53.47	10.34.55.91	cve-2010-00...f.ppt	ftp://10.34.55.91/...	
2019-05-09 12:03:40	Gen:Heur.BZC.PZQ.Box...	127.0.0.1	127.0.0.1	恶意样本1.zip		
2019-05-08 12:02:46	Exploit.PDF-JS.JU	10.14.166.60	123.125.50.133	1557288166.eml	qiqudlmu@163.com	
2019-05-08 11:51:47	Generic.Ransom.SamSa...	192.168.16.167	127.0.0.1	0f2c5c39494...	192.168.16.167	
2019-05-05 16:26:09	W97M.Downloader.AFT	192.168.199.175	192.168.199.192	LM202.XLS	ftp://192.168.199....	
2019-05-05 16:26:09	Trojan.Inject.AKD	192.168.199.175	192.168.199.192	LM197.rar	ftp://192.168.199....	
2019-05-05 16:26:09	Gen:Variant.Kazy.146...	192.168.199.175	192.168.199.192	LM188.zip	ftp://192.168.199....	



# 谢谢！

绿盟科技版权所有