



快速应急响应技术

绿盟科技版权所有 2019护网专题培训



CONTENTS 目录 >>>

- 护网行动应急响应概述
- 快速识别安全事件
- 快速分析与侦察
- 快速取证与隔离



01

护网行动应急响应概述

1. 什么是护网行动
2. 护网行动应急响应的必要性

▶▶ 护网行动应急响应概述

- 护网行动是公安部门为检验国家关键信息基础设施安全防护和应急处置能力，而开展的网络安全攻防演练，会邀请国内安全企业和部分甲方企业作为攻击方：
 - 采取 **“单盲式”**，即**攻击时间不固定、攻击源不明确、攻击目标不明确、攻击手段不明确**
 - 以获得目标**系统权限、数据**为得分点开展模拟攻击
 - 企业作为防守方以**发现**入侵事件、**处置**事件、配合执法机关**取证**为目标获取得分。
- 由于攻击面广、攻击路径不定，在护网行动期间用户系统被攻击丢分在所难免：
 - 如何**快速定位、快速分析**安全入侵、攻击事件，**快速取证并及时上报**得分就显得尤为重要。



02

快速识别安全事件

1. 常见安全事件
2. 如何发现安全事件
3. 如何判断影响范围

2.1

常见安全事件

- a. 常见安全事件
- b. 常见安全攻击思路

护网常见安全事件

□ 入侵事件

- 主机、服务器被入侵
- WEB站点入侵

□ 信息泄露事件

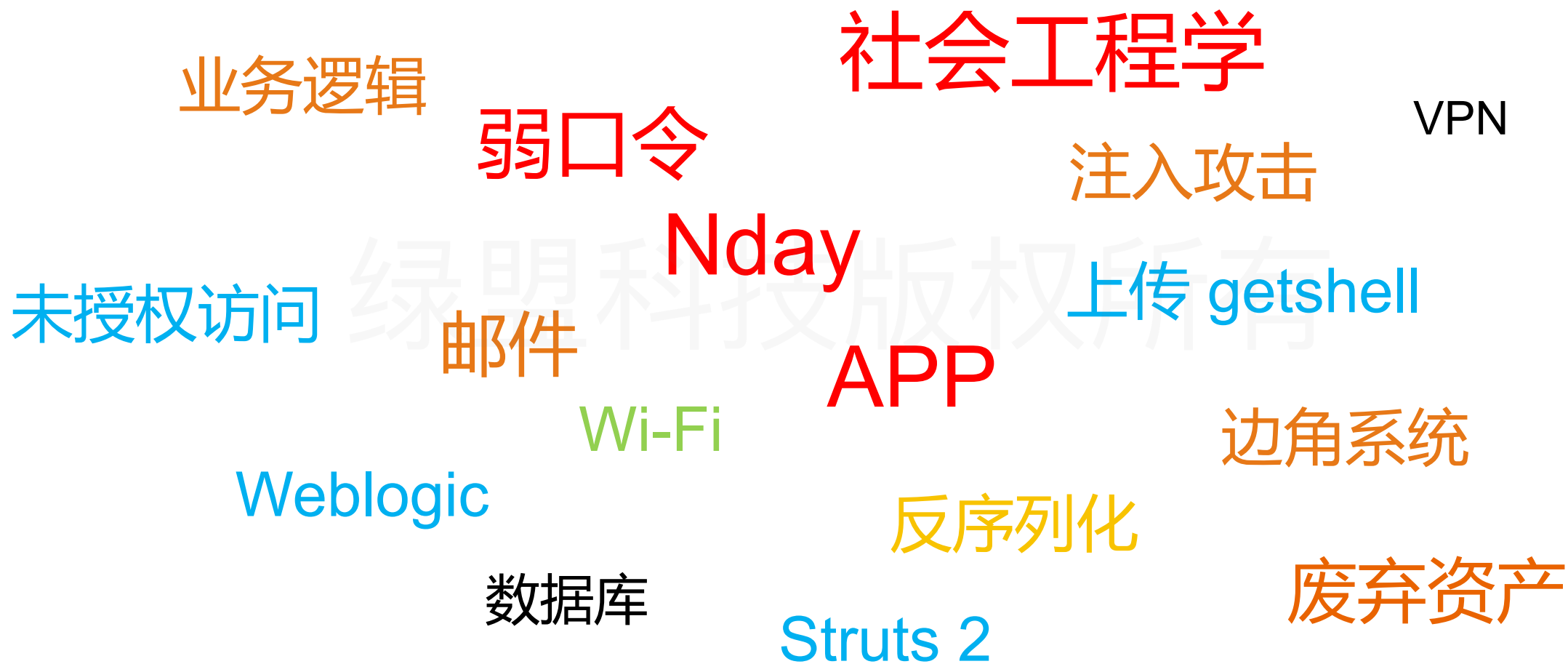
- 敏感信息泄露
- 用户弱口令
- 源代码泄露

□ Web应用安全事件

- SQL注入
- XSS
- XXE
- 短信炸弹
- ...



▶▶ 不知攻焉知防——护网行动常见攻击思路



2.2

如何发现安全事件

- a. 常用主动发现技术
- b. 常见被动发现场景

▶▶ 常见主动发现技术

- 日志分析
 - 安全设备日志
 - 主机日志
 - 中间件日志
 - 应用程序日志
- 恶意文件监控
 - 木马
 - Webshell
 - 其他可疑文件
- 安全威胁情报



▶▶ 常见被动发现场景

□ 系统运维报告异常

- 网络丢包
- 系统频繁重启
- 系统蓝屏
- 系统资源占用率过高

□ 业务用户投诉或抱怨

- 用户收到异常短信
- 用户异常退出登陆

□ 被通报



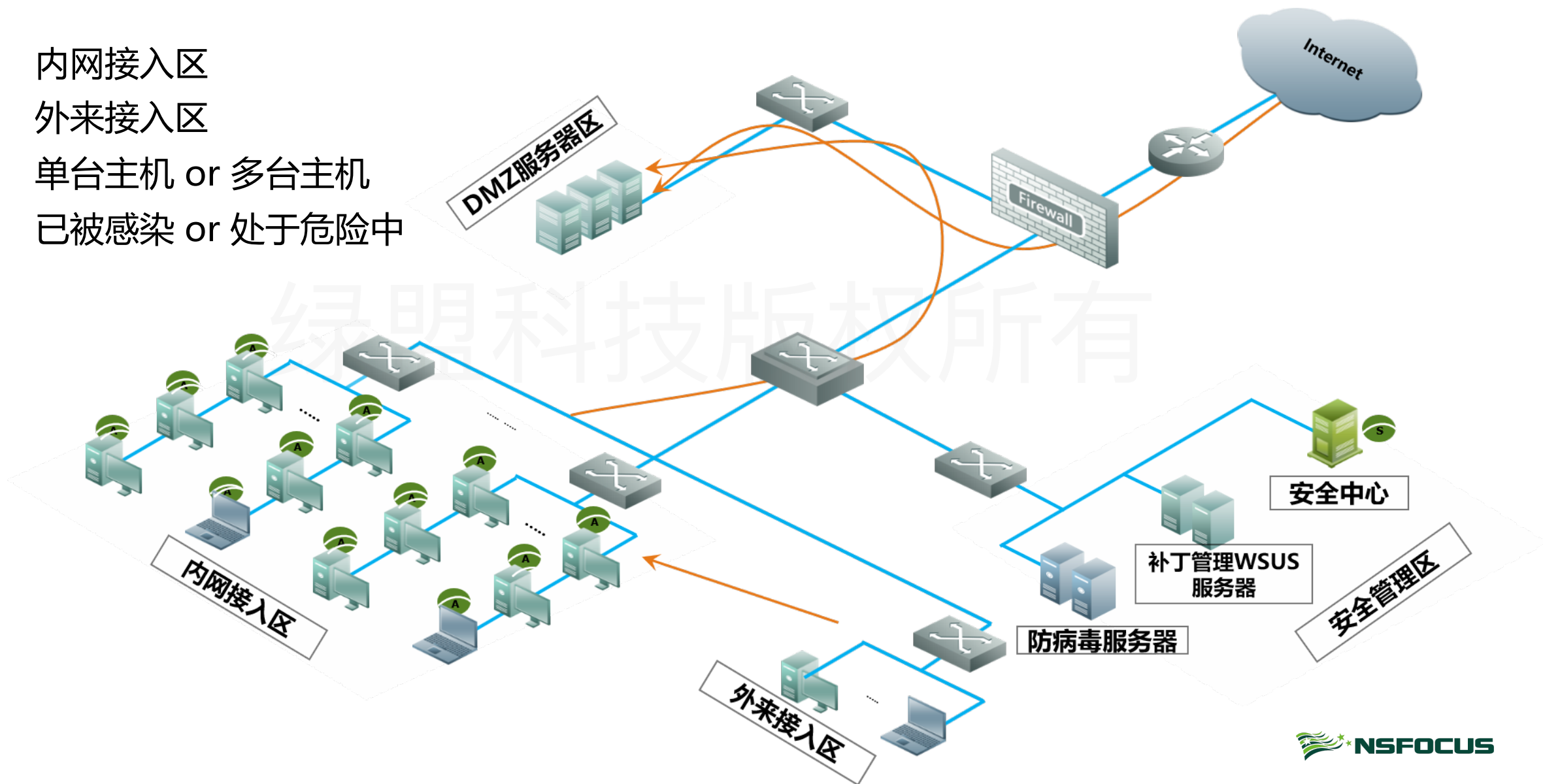
2.3

如何判断影响范围

- a. 异常主机所处网络环境
- b. 异常主机用途

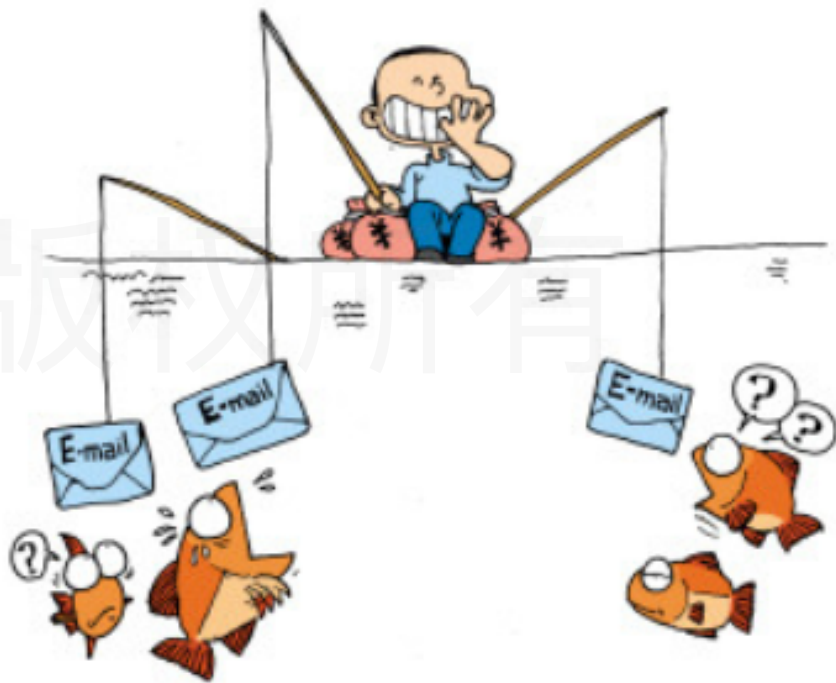
异常主机所处网络环境

- 内网接入区
- 外来接入区
- 单台主机 or 多台主机
- 已被感染 or 处于危险中



▶▶ 异常主机用途

- 个人办公主机
- 特殊权限主机
- 工控主机
- 应用服务器
- 数据库服务器
- 域控服务器





03

快速分析与侦查

1. 三要素法
2. 回溯攻击法
3. 经验法

3.1

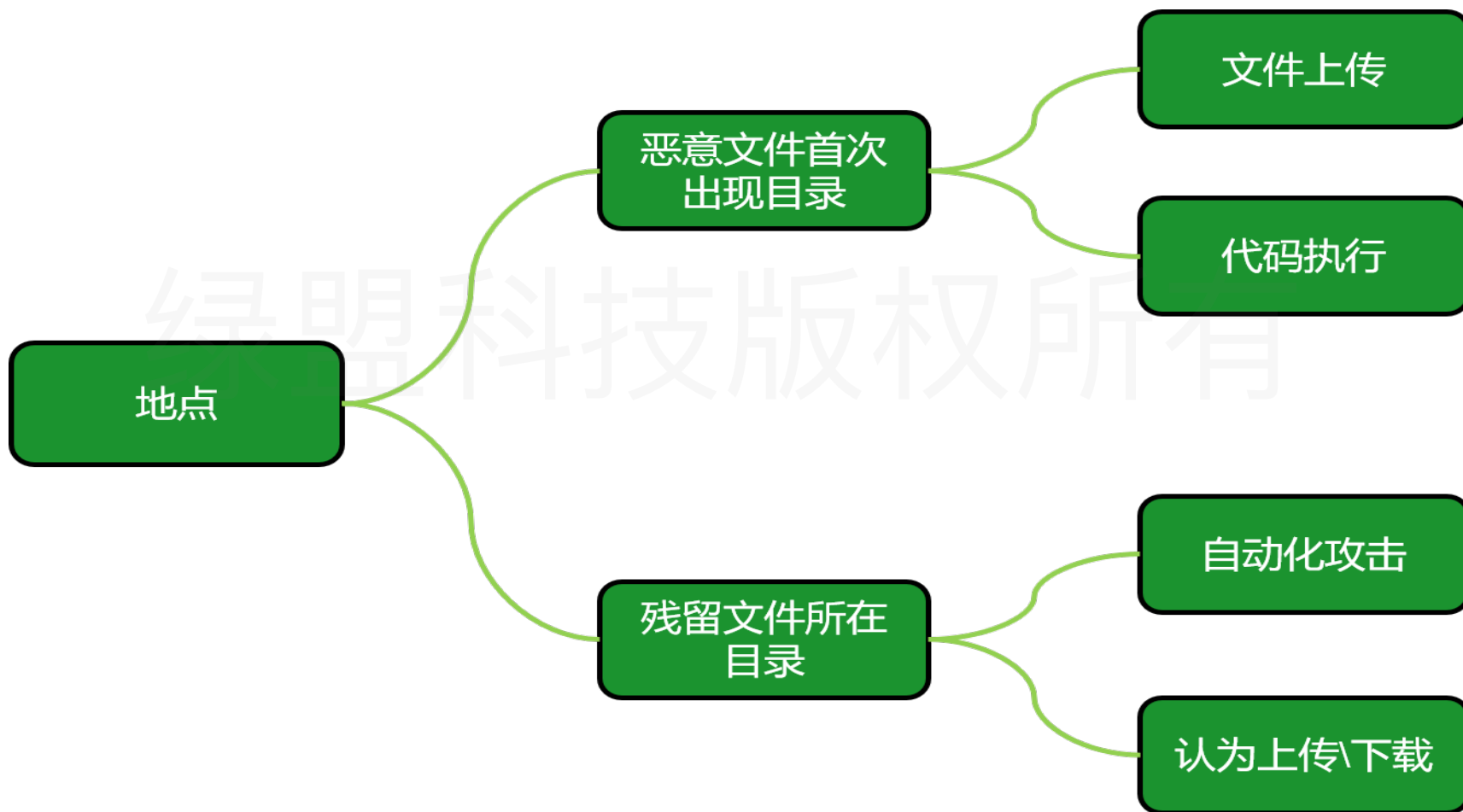
三要素法

- a. 时间
- b. 地点
- c. 事件

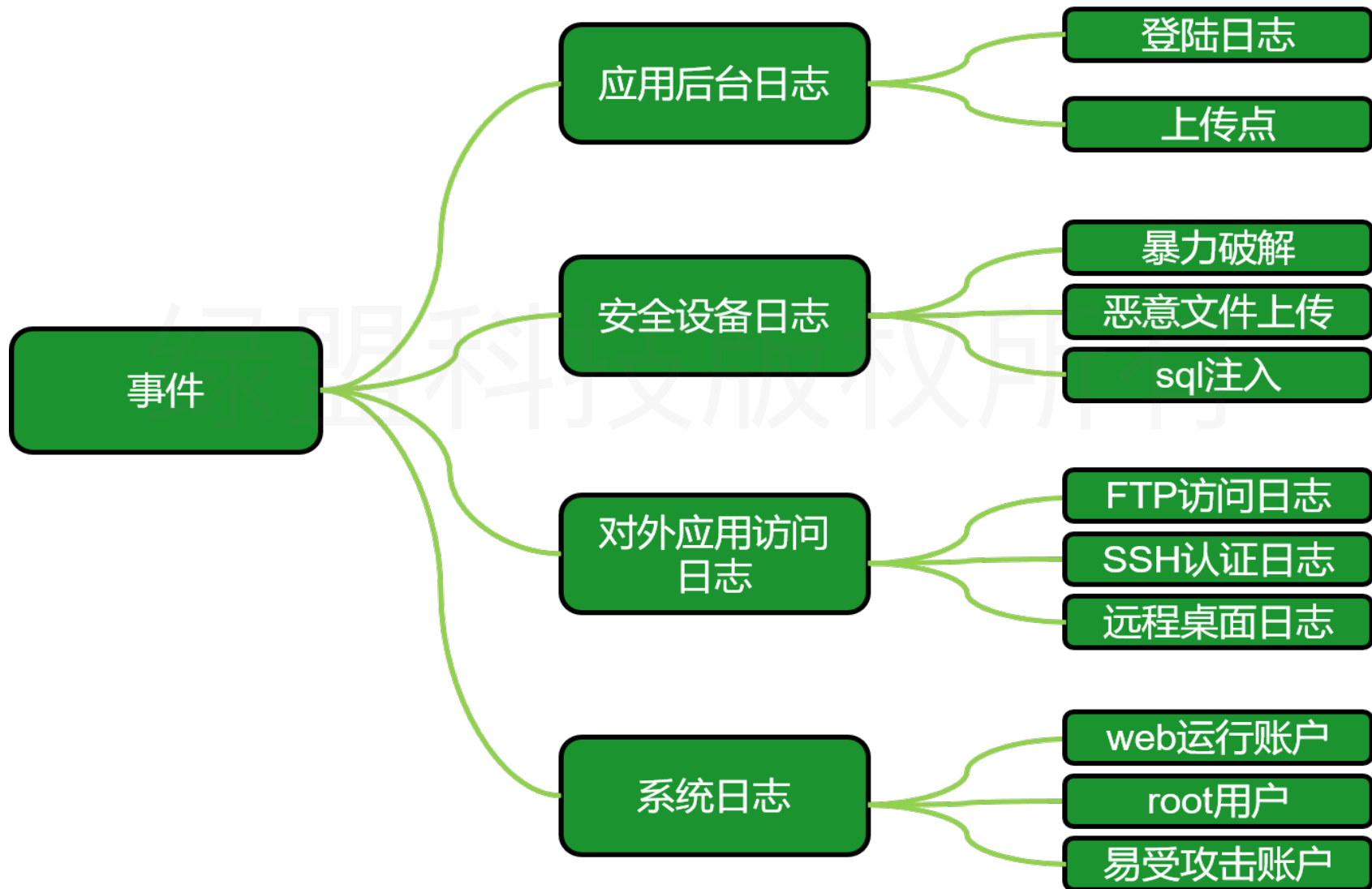
▶▶ 三要素法 —— 时间



▶▶ 三要素法 —— 地点



▶▶ 三要素法 —— 事件



3.2

回溯攻击法

a. 回溯攻击法

▶▶ 回溯攻击法

□ 护网行动中常见的安全风险

主机监听端口整理

- 异常被监听端口
- 异常会话链接

代码/命令执行

- Weblogic
- Struts2
- JBoss
- ThinkPHP
- MS17-010
- Fastjson

弱口令

- Web应用弱口令
- 中间件弱口令
- 数据库
- ssh、ftp、ssh、rdp

钓鱼邮件

- 恶意word
- 恶意PPT
- 恶意链接
- 信息收集

常见web漏洞

SQL注入

XSS

XXE

越权操作

任意文件读取

文件上传风险

头像

附件

图标

3.3

经验法

a. 经验法

经验法

攻击者常用目录

- 中间件根目录
- 文件上传目录
- /var/tmp
- 默认下载路径 : C:\Users\Account\Downloads
- apache-tomcat-*/conf/tomcat-users.xml
- servers/AdminServer/tmp/_WL_internal/bea_wls_internal/9j4dqk/war
- servers/AdminServer/tmp/_WL_internal/bea_wls9_async_response/8tpkys/war/
- servers/AdminServer/tmp/_WL_internal/wls-wsat/54p17w/war/
- servers/AdminServer/tmp/_WL_internal/wls-wsat/

经验法

□ 常见服务端口

- 21 : FTP (未授权访问、弱口令)
- 22 : SSH (弱口令)
- 23 : Telnet (未授权访问、弱口令)
- 445 : SMB (远程命令执行)
- 1433 : MSSQL (弱口令、提权)
- 3306 : MySQL (弱口令、提权)
- 3389 : RDP (弱口令、远程代码执行)
- 7001 : weblogic (弱口令、SSRF、反序列化)
- 8080 : Tomcat (启用PUT方法、弱口令)
- 27017 : MongoDB (未授权访问)



04

快速取证与隔离

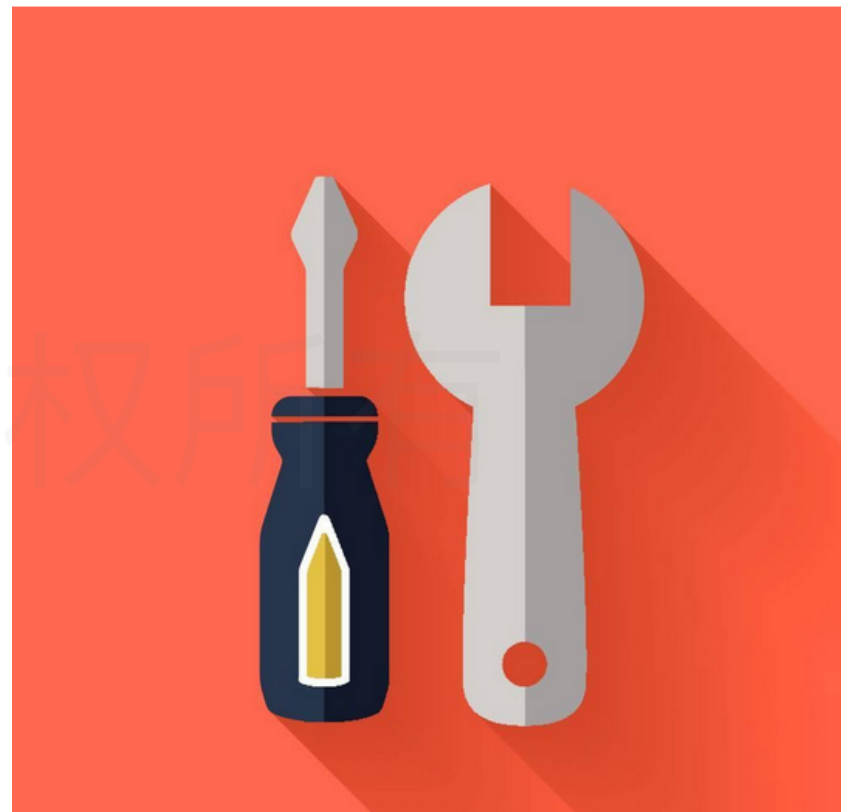
1. 常用工具及脚本
2. 取证对象及流程
3. 远控木马应急响应分析

4.1

常用工具及脚本

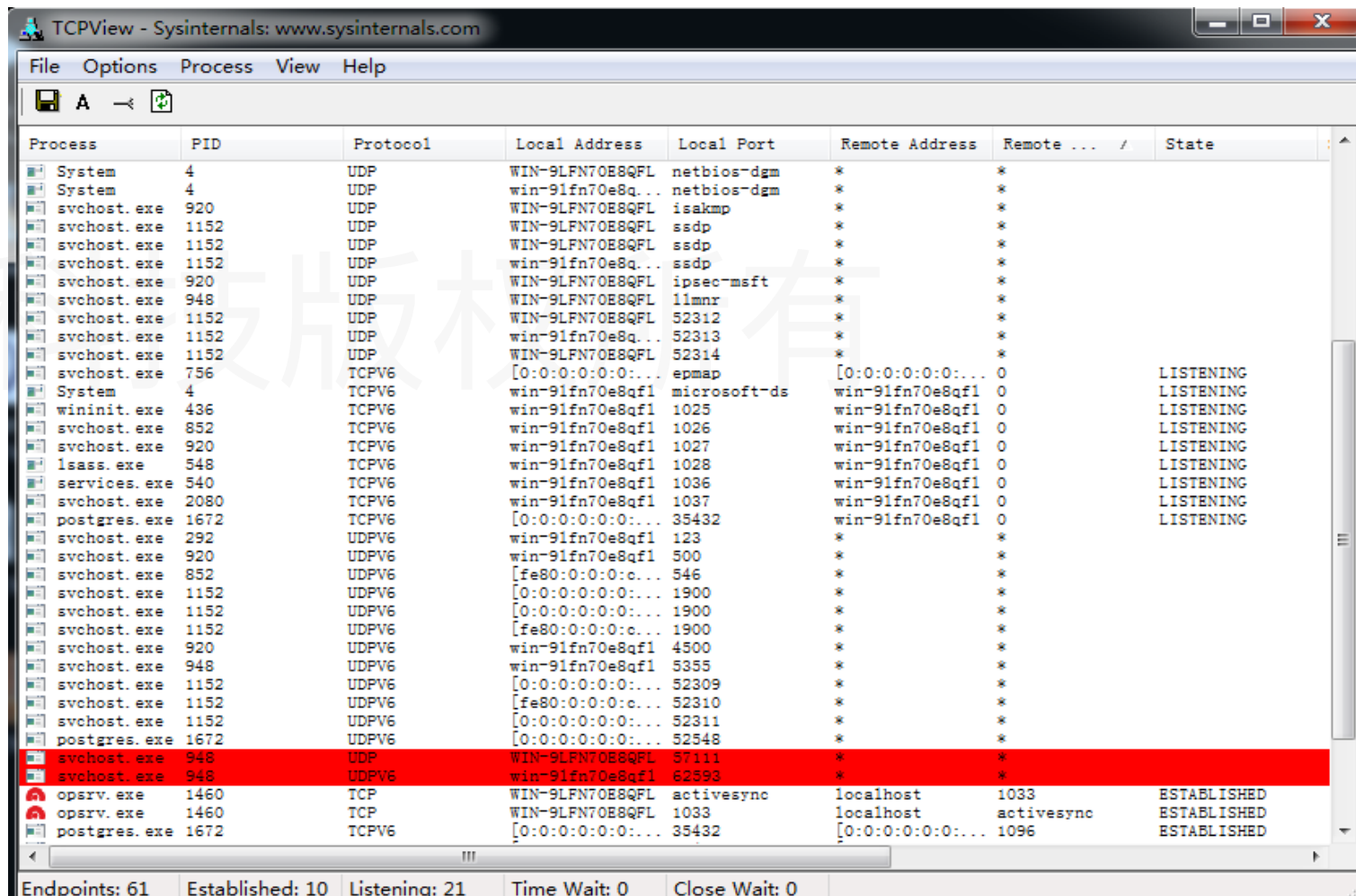
▶▶ 常用工具及脚本

- Tcpview
- AutoRuns
- WebShell查杀工具
- 日志工具



▶▶ Tcpview

- TCPView是一个用来显示系统中所有的TCP和UDP端点(列表的程序,包括本地和远程的网络地址,以及TCP连接的状态。

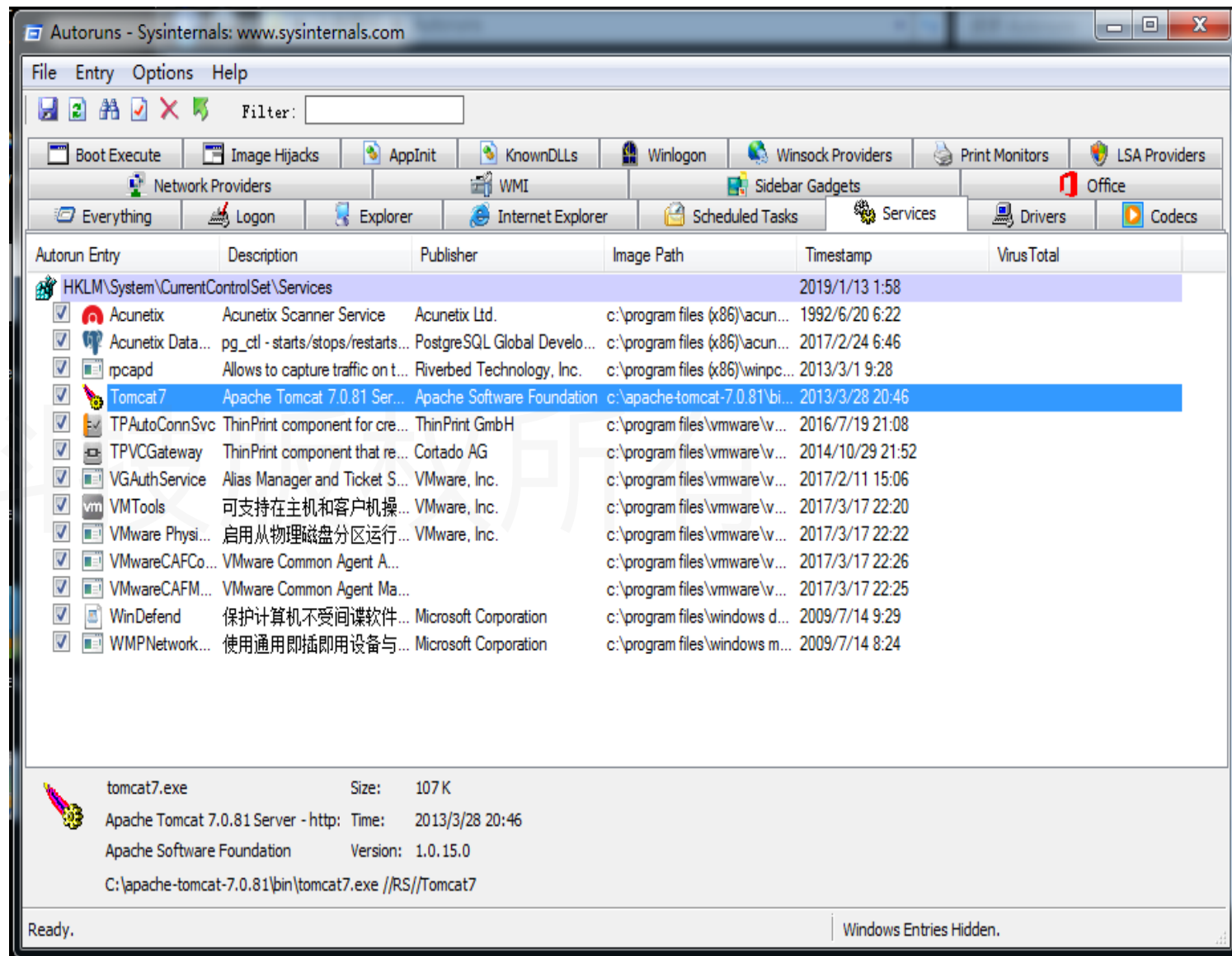


The screenshot shows the TCPView application window with a menu bar (File, Options, Process, View, Help) and a toolbar. The main area displays a table of network endpoints and connections. The table has columns for Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State. The status bar at the bottom shows summary statistics: Endpoints: 61, Established: 10, Listening: 21, Time Wait: 0, Close Wait: 0.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote ...	State
System	4	UDP	WIN-9LFN70E8QFL	netbios-dgm	*	*	
System	4	UDP	win-91fn70e8q...	netbios-dgm	*	*	
svchost.exe	920	UDP	WIN-9LFN70E8QFL	isakmp	*	*	
svchost.exe	1152	UDP	WIN-9LFN70E8QFL	ssdp	*	*	
svchost.exe	1152	UDP	WIN-9LFN70E8QFL	ssdp	*	*	
svchost.exe	920	UDP	win-91fn70e8q...	ssdp	*	*	
svchost.exe	920	UDP	WIN-9LFN70E8QFL	ipsec-msft	*	*	
svchost.exe	948	UDP	WIN-9LFN70E8QFL	llmnr	*	*	
svchost.exe	1152	UDP	WIN-9LFN70E8QFL	52312	*	*	
svchost.exe	1152	UDP	win-91fn70e8q...	52313	*	*	
svchost.exe	1152	UDP	WIN-9LFN70E8QFL	52314	*	*	
svchost.exe	756	TCPV6	[0:0:0:0:0:0:...	epmap	[0:0:0:0:0:0:...	0	LISTENING
System	4	TCPV6	win-91fn70e8qf1	microsoft-ds	win-91fn70e8qf1	0	LISTENING
wininit.exe	436	TCPV6	win-91fn70e8qf1	1025	win-91fn70e8qf1	0	LISTENING
svchost.exe	852	TCPV6	win-91fn70e8qf1	1026	win-91fn70e8qf1	0	LISTENING
svchost.exe	920	TCPV6	win-91fn70e8qf1	1027	win-91fn70e8qf1	0	LISTENING
lsass.exe	548	TCPV6	win-91fn70e8qf1	1028	win-91fn70e8qf1	0	LISTENING
services.exe	540	TCPV6	win-91fn70e8qf1	1036	win-91fn70e8qf1	0	LISTENING
svchost.exe	2080	TCPV6	win-91fn70e8qf1	1037	win-91fn70e8qf1	0	LISTENING
postgres.exe	1672	TCPV6	[0:0:0:0:0:0:...	35432	win-91fn70e8qf1	0	LISTENING
svchost.exe	292	UDPV6	win-91fn70e8qf1	123	*	*	
svchost.exe	920	UDPV6	win-91fn70e8qf1	500	*	*	
svchost.exe	852	UDPV6	[fe80:0:0:0:c...]	546	*	*	
svchost.exe	1152	UDPV6	[0:0:0:0:0:0:...	1900	*	*	
svchost.exe	1152	UDPV6	[0:0:0:0:0:0:...	1900	*	*	
svchost.exe	1152	UDPV6	[fe80:0:0:0:c...]	1900	*	*	
svchost.exe	920	UDPV6	win-91fn70e8qf1	4500	*	*	
svchost.exe	948	UDPV6	win-91fn70e8qf1	5355	*	*	
svchost.exe	1152	UDPV6	[0:0:0:0:0:0:...	52309	*	*	
svchost.exe	1152	UDPV6	[fe80:0:0:0:c...]	52310	*	*	
svchost.exe	1152	UDPV6	[0:0:0:0:0:0:...	52311	*	*	
postgres.exe	1672	UDPV6	[0:0:0:0:0:0:...	52548	*	*	
svchost.exe	948	UDP	WIN-9LFN70E8QFL	57111	*	*	
svchost.exe	948	UDPV6	win-91fn70e8qf1	62893	*	*	
opssrv.exe	1460	TCP	WIN-9LFN70E8QFL	activesync	localhost	1033	ESTABLISHED
opssrv.exe	1460	TCP	WIN-9LFN70E8QFL	1033	localhost	activesync	ESTABLISHED
postgres.exe	1672	TCPV6	[0:0:0:0:0:0:...	35432	[0:0:0:0:0:0:...	1096	ESTABLISHED

▶▶ AutoRuns

AutoRuns是一款出色的启动项目管理工具，他的的作用就是检查开机自动加载的所有程序，例如硬件驱动程序，windows核心启动程序和应用程序。它比windows自带的msconfig.exe还要强大，通过它我们还可以看到一些在msconfig里面无法查看到的病毒和木马以及恶意插件程序，还能够详细的把启动项目加载的所有程序列出来。



Webshell查杀工具

- D盾
- findwebshell

绿盟科技 版权所有

webshell后门报告

路径	类型	修改时间
/Users/juzheng/apps/mini-scripts/wst/one.php	evalassert后门	2017-11-10 19:42:18
/Users/juzheng/apps/mini-scripts/wst/pic.gif	evalassert后门	2011-08-23 11:15:06
/Users/juzheng/apps/mini-scripts/wst/wp-login.php	includelrequire(_once)非法引用后门	2017-10-13 10:10:48
/Users/juzheng/apps/mini-scripts/wst/wp-admin/media-upload.php	includelrequire(_once)非法引用后门	2016-08-23 02:25:31
/Users/juzheng/apps/mini-scripts/wst/wp-admin/includes/class-wp-list-table.php	includelrequire(_once)非法引用后门	2017-07-27 08:40:43
/Users/juzheng/apps/mini-scripts/wst/wp-admin/includes/class-wp-plugin-install-list-table.php	includelrequire(_once)非法引用后门	2017-10-19 02:01:49
/Users/juzheng/apps/mini-scripts/wst/wp-admin/includes/class-wp-plugins-list-table.php	includelrequire(_once)非法引用后门	2017-10-05 07:43:46
/Users/juzheng/apps/mini-scripts/wst/wp-admin/includes/class-wp-upgrader-skin.php	includelrequire(_once)非法引用后门	2017-07-27 08:40:43
/Users/juzheng/apps/mini-scripts/wst/wp-admin/includes/deprecated.php	includelrequire(_once)非法引用后门	2017-09-26 16:24:46
/Users/juzheng/apps/mini-scripts/wst/wp-admin/includes/file.php	includelrequire(_once)非法引用后门	2017-11-27 11:29:25
/Users/juzheng/apps/mini-scripts/wst/wp-admin/includes/media.php	includelrequire(_once)非法引用后门	2017-10-21 21:27:48
/Users/juzheng/apps/mini-scripts/wst/wp-admin/includes/meta-boxes.php	includelrequire(_once)非法引用后门	2017-11-24 02:03:43
/Users/juzheng/apps/mini-scripts/wst/wp-admin/includes/template.php	includelrequire(_once)非法引用后门	2017-11-11 06:32:47



▶▶ 日志工具

□ windows

- Sublime/UE
- LogParser/LogParser Lizard
- Event log Explorer

□ web应用

- WebLog Expert

□ linux

- Goaccess
- grep、cat、more、less、awk

绿盟科技版权所有

▶▶ 日志工具

□ Sublime

- 批量操作

□ 快速文本编辑

```
20 (Thu Nov 09 00:12:23 2017.7246468) : C:\Windows\System32\drivers\zh-CN\bthpan.sys.mui[N
21 (Thu Nov 09 00:12:23 2017.7246468) : *****
22 (Thu Nov 09 00:12:23 2017.7247000) : WDM call returned error: 4200
23 (Thu Nov 09 00:12:23 2017.7247031) : WDM call returned error: 4200
24 (Thu Nov 09 00:12:23 2017.7247031) : WDM call returned error: 4200
25 (Thu Nov 09 00:12:23 2017.7247093) : WDM call returned error: 4200
26 (Thu Nov 09 00:12:23 2017.7247093) : WDM call returned error: 4200
27 (Thu Nov 09 00:12:23 2017.7247093) : WDM call returned error: 4200
28 (Thu Nov 09 00:12:24 2017.7247140) : WDM call returned error: 4200
29 (Thu Nov 09 00:12:24 2017.7247140) : WDM call returned error: 4200
30 (Thu Nov 09 00:12:24 2017.7247140) : WDM call returned error: 4200
31 (Fri Nov 10 11:17:23 2017.46343) : WDM call returned error: 4200
32 (Fri Nov 10 11:17:23 2017.46359) : *****
33 (Fri Nov 10 11:17:23 2017.46359) : Could not get pointer to binary resource for file:
34 (Fri Nov 10 11:17:23 2017.46359) : C:\Windows\system32\drivers\ndis.sys [MofResourceName
35 (Fri Nov 10 11:17:23 2017.46375) : *****
36 (Fri Nov 10 11:17:23 2017.46375) : *****
37 (Fri Nov 10 11:17:23 2017.46375) : Could not get pointer to binary resource for file:
38 (Fri Nov 10 11:17:23 2017.46375) : C:\Windows\system32\drivers\zh-CN\ndis.sys.mui[MofRe
39 (Fri Nov 10 11:17:23 2017.46375) : *****
40 (Fri Nov 10 11:17:23 2017.46390) : *****
41 (Fri Nov 10 11:17:23 2017.46390) : Could not get pointer to binary resource for file:
42 (Fri Nov 10 11:17:23 2017.46390) : C:\Windows\System32\drivers\bthpan.sys [NdisMofResour
43 (Fri Nov 10 11:17:23 2017.46390) : *****
44 (Fri Nov 10 11:17:23 2017.46390) : *****
45 (Fri Nov 10 11:17:23 2017.46390) : Could not get pointer to binary resource for file:
46 (Fri Nov 10 11:17:23 2017.46390) : C:\Windows\System32\drivers\zh-CN\bthpan.sys.mui[Ndi
47 (Fri Nov 10 11:17:23 2017.46406) : *****
48 (Fri Nov 10 11:17:23 2017.46406) : *****
49 (Fri Nov 10 11:17:23 2017.46406) : info Could not get pointer to binary resource for fi
50 (Fri Nov 10 11:17:23 2017.46406) : C:\Windows\System32\drivers\monitor.sys [MonitorWMI] (
51 (Fri Nov 10 11:17:23 2017.46406) : *****
52 (Fri Nov 10 11:17:23 2017.46484) : info WDM call returned error: 4200
53 (Fri Nov 10 11:17:23 2017.46500) : info warning WDM call returned error: 4200
54 (Fri Nov 10 11:17:23 2017.46500) : WDM call returned error: 4200
55 (Fri Nov 10 11:17:23 2017.46500) : WDM call returned error: 4200
56 (Fri Nov 10 11:17:23 2017.46500) : WDM call returned error: 4200
57 (Fri Nov 10 11:17:23 2017.46500) : WDM call returned error: 4200
58 (Fri Nov 10 11:17:23 2017.46500) : WDM call returned error: 4200
59 (Fri Nov 10 11:17:23 2017.46500) : WDM call returned error: 4200
60 (Fri Nov 10 11:17:23 2017.46515) : WDM call returned error: 4200
61 (Fri Nov 10 11:19:28 2017.171843) : WDM call returned error: 4200
62 (Fri Nov 10 11:19:28 2017.171859) : WDM call returned error: 4200
```

日志工具

LogParser

- 基本格式：LogParser -i:输入文件的格式 -o:输出格式 “SQL语句”
- Logparser.exe -i:EVT -o:DATAGRID “select * from C:\path\xx.evtx where EventID=5080”

```
C:\Soft\LogParse>LogParser.exe -i:EVT -o:DATAGRID "select * from C:\Users\AAA\Desktop\security.evtx where EventID=5080"
-resolveSIDs ON

Statistics:
-----
Elements processed: 23420
Elements output: 22
Execution time: 346.09 seconds (00:05:46.09)
```

Log Parser

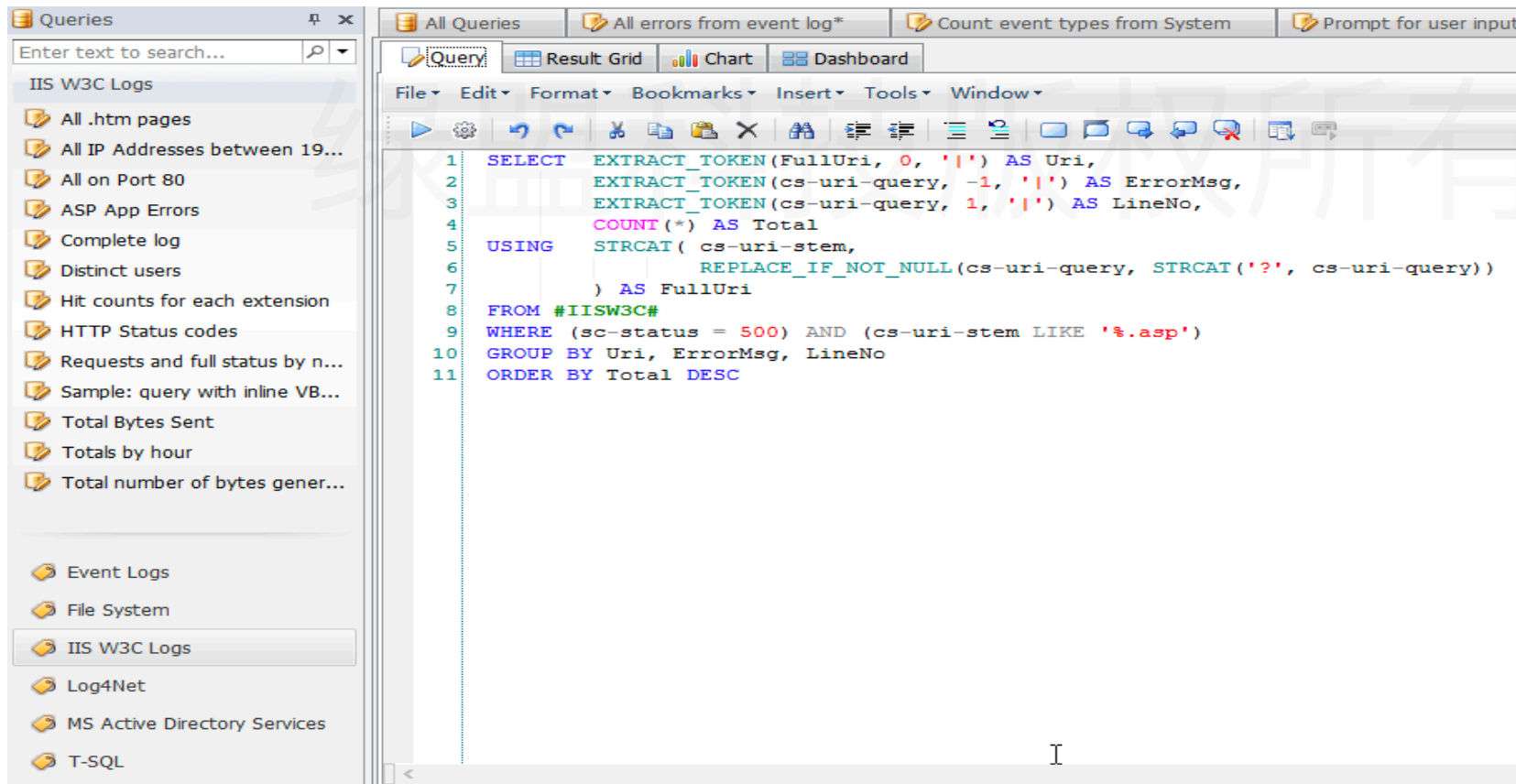
Edit View Format

EventLog	RecordNum...	TimeGenerated	TimeWritten	Event...	EventTy...	Event TypeName	EventCateg...	EventCategoryName	SourceName
C:\Users\AAA\Desktop\Security.evtx	744	2017-11-08 22:07:...	2017-11-08 22:07:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	746	2017-11-08 22:07:...	2017-11-08 22:07:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	748	2017-11-08 22:07:...	2017-11-08 22:07:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	750	2017-11-08 22:07:...	2017-11-08 22:07:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	752	2017-11-08 22:07:...	2017-11-08 22:07:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	842	2017-11-08 22:13:...	2017-11-08 22:13:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	14263	2017-11-10 11:19:...	2017-11-10 11:19:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	14462	2017-11-11 16:15:...	2017-11-11 16:15:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	14545	2017-11-17 16:15:...	2017-11-17 16:15:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	14767	2017-11-27 10:05:...	2017-11-27 10:05:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	14846	2017-11-27 14:49:...	2017-11-27 14:49:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	14852	2017-11-27 14:51:...	2017-11-27 14:51:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	19361	2017-11-27 22:45:...	2017-11-27 22:45:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	19363	2017-11-27 22:45:...	2017-11-27 22:45:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au
C:\Users\AAA\Desktop\Security.evtx	22521	2017-11-28 16:21:...	2017-11-28 16:21:...	5058	8	Success Audit ev...	12292	The name for category 12292 in Source "Microsoft-Windows-Security-Auditi...	Microsoft-Windows-Security-Au

日志工具

LogParser Lizard

- 封装了logParser命令，带图形界面，大大降低了LogParser的使用难度。
- 使查询结果可以方便的以图表或EXCEL格式展示
- 集成了几个开源工具，如log4net等。可以对IIS logs、EventLogs、log4net等进行方便的查询。



▶▶ 日志工具

□ Event Log Explorer

- 自动读取本地所有系统日志
- 可读取远程主机日志
- 可看到内核级日志

The screenshot displays the Event Log Explorer interface. On the left, the 'Computers Tree' shows the hierarchy of event logs for 'DESKTOP-LCAELT8 (local)'. The 'Security' log is expanded, showing a list of 23018 events. The main pane shows a table of events with columns for Type, Date, Time, Event, Source, Category, User, and Computer. A specific event is selected, and its details are shown in the 'Description' pane below.

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2017/12/7	16:28:40	4798	Microsoft-Windows-Se	用户帐户管理	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	13:16:32	4616	Microsoft-Windows-Se	安全状态更改	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	12:28:40	4616	Microsoft-Windows-Se	安全状态更改	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	11:31:36	4672	Microsoft-Windows-Se	特殊登录	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	11:31:36	4624	Microsoft-Windows-Se	登录	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:50:02	4799	Microsoft-Windows-Se	安全组管理	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:50:02	4799	Microsoft-Windows-Se	安全组管理	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:49:27	4672	Microsoft-Windows-Se	特殊登录	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:49:27	4624	Microsoft-Windows-Se	登录	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:44:38	4798	Microsoft-Windows-Se	用户帐户管理	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:40:32	4798	Microsoft-Windows-Se	用户帐户管理	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:40:04	4672	Microsoft-Windows-Se	特殊登录	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:40:04	4624	Microsoft-Windows-Se	登录	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:30:35	4798	Microsoft-Windows-Se	用户帐户管理	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:30:16	4672	Microsoft-Windows-Se	特殊登录	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:30:16	4624	Microsoft-Windows-Se	登录	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:30:15	4672	Microsoft-Windows-Se	特殊登录	N/A	DESKTOP-LCAELT8
Audit Success	2017/12/7	10:30:15	4624	Microsoft-Windows-Se	登录	N/A	DESKTOP-LCAELT8

Description

A user's local group membership was enumerated.

Subject:

Security ID: S-1-5-21-3777011902-4166502931-942617472-1000
Account Name: AAA
Account Domain: DESKTOP-LCAELT8
Logon ID: 0009185A

User:

Security ID: S-1-5-21-3777011902-4166502931-942617472-1000
Account Name: AAA
Account Domain: DESKTOP-LCAELT8

Process Information:

Process ID: 000011E4
Process Name: C:\Windows\explorer.exe

▶▶ 日志工具

□ WebLog Expert

- Web 日志分析
- 图表对比
- 统计请求数量

绿盟科技版权所有

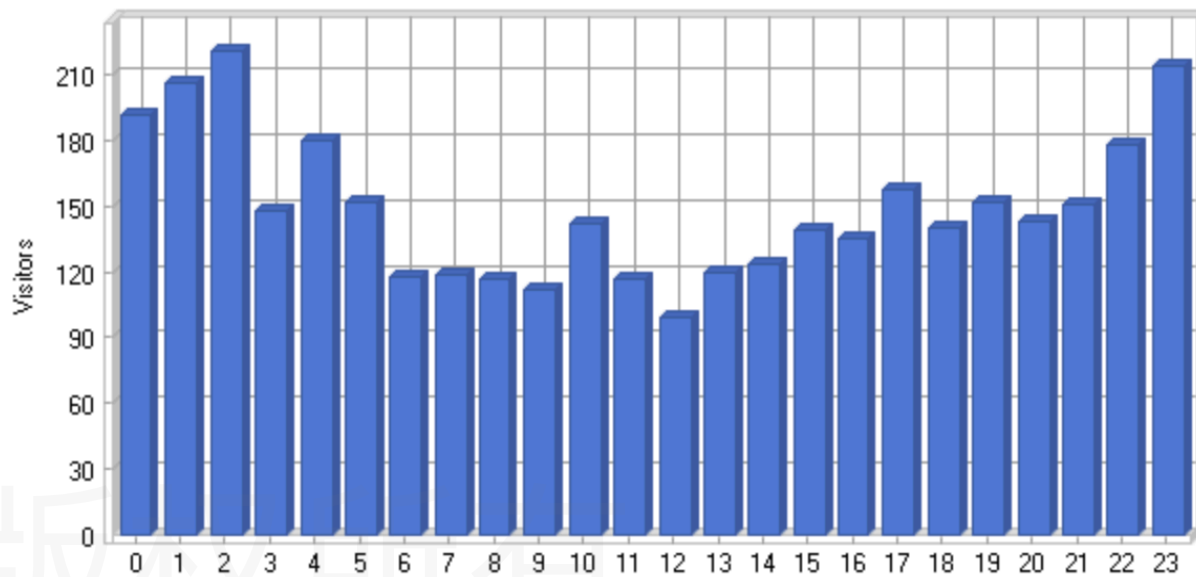
```
86.132.136.211 - - [08/Dec/2007:00:24:02 -0800] "GET /img/tm_home.gif HTTP/1.1" 200 554  
"http://www.smsync.com/order/?ref=001" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR  
2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506; InfoPath.1)" www.smsync.com
```

日志工具

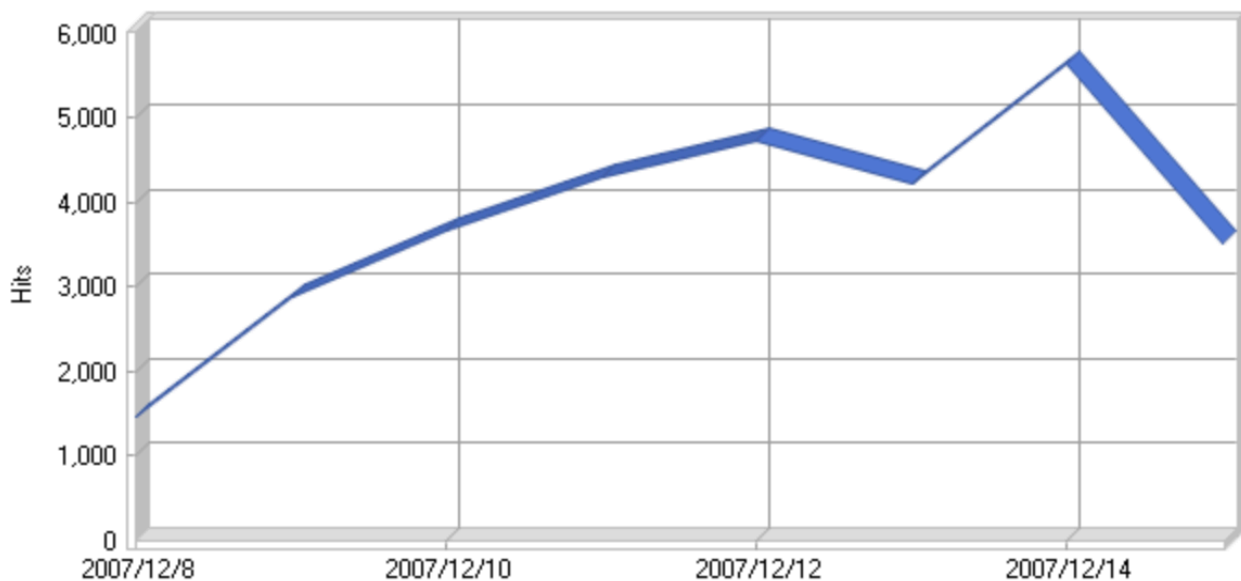
- 请求活跃时间
- 请求的分布
- 每天的访问量

绿盟科技版权所有

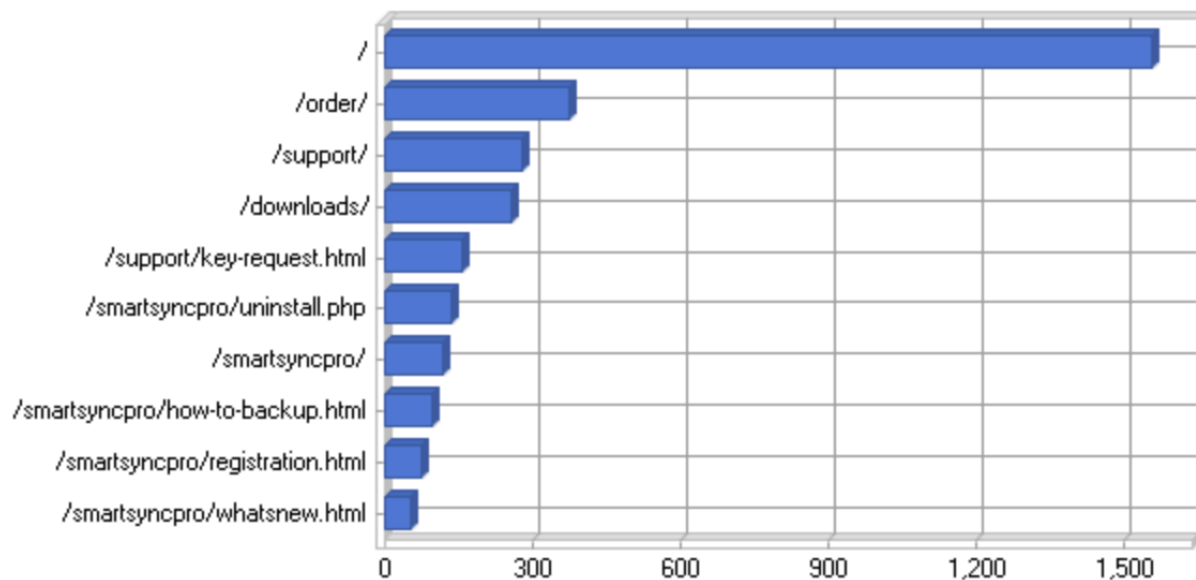
Activity by Hour of Day



Daily Hits



Most Popular Pages



▶▶ 日志工具

□ WebLog Expert

Most Popular Pages

	Page	Hits	Incomplete Requests	Visitors	Bandwidth (KB)
1	http://www.smsync.com/	1,973	0	1,554	10,401
2	http://www.smsync.com/order/	507	0	373	2,147
3	http://www.smsync.com/support/	395	0	280	2,106
4	http://www.smsync.com/downloads/	310	0	255	1,318
5	http://www.smsync.com/support/key-request.html	195	0	155	584
6	http://www.smsync.com/smartsyncpro/uninstall.php	150	0	134	564
7	http://www.smsync.com/smartsyncpro/	148	0	116	732
8	http://www.smsync.com/smartsyncpro/how-to-backup.html	98	0	94	102
9	http://www.smsync.com/smartsyncpro/registration.html	77	0	75	44
10	http://www.smsync.com/smartsyncpro/whatsnew.html	51	0	50	343

Most Requested Directories

	Directory	Hits	Incomplete Requests	Visitors	Bandwidth (KB)
1	http://www.smsync.com/	3,845	0	2,324	18,710
2	http://www.smsync.com/img/	20,491	7	1,112	43,466
3	http://www.smsync.com/css/	1,032	4	865	6,236
4	http://www.smsync.com/downloads/	1,365	640	533	436,609
5	http://www.smsync.com/smartsyncpro/	806	0	532	50,187
6	http://www.smsync.com/support/	696	2	427	3,816
7	http://www.smsync.com/order/	568	0	380	2,425
8	http://www.smsync.com/images/	100	0	48	60
9	http://www.smsync.com/contacts/	57	0	44	157
10	http://www.smsync.com/smartsync/	38	0	38	22
11	http://www.smsync.com/partner-programs/	35	0	18	141
12	http://www.smsync.com/	14	0	14	58
13	http://www.smsync.com/partners/	3	0	3	1
14	http://www.smsync.com/images/uploads/thumbs/	1	0	1	0
	Total	29,051	653	N/A	561,896

	40	218
	37	125
	33	120
	31	97
	27	16
	22	62
	18	123
	18	65
	17	78
	15	81
	14	54
	12	49
	11	47
	9	11
	9	32
	8	60
	7	52
	6	26
	6	70
	6	27
	5	36
	5	3
	5	81

▶▶ 日志工具

□ Goaccess

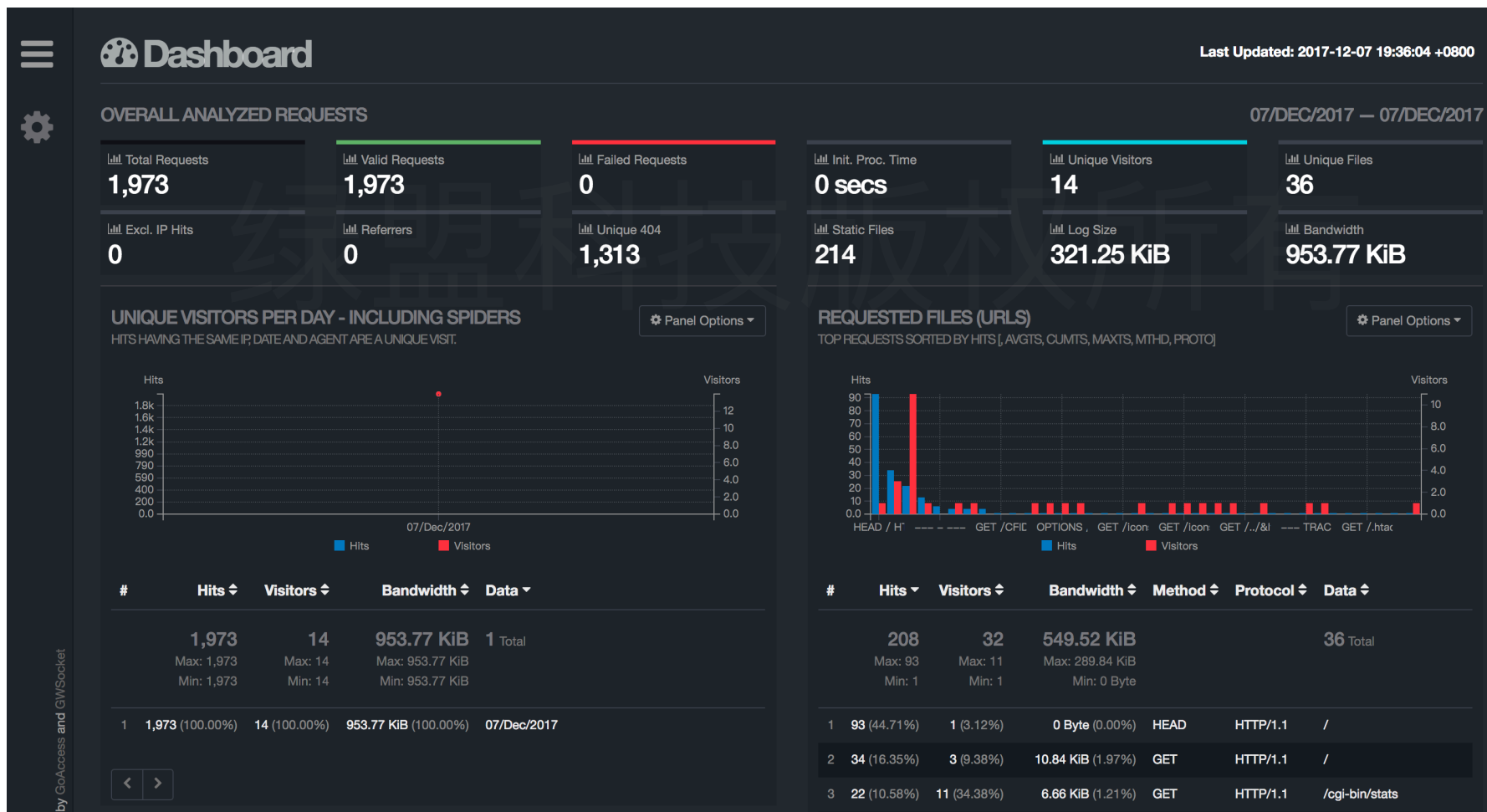
- `goaccess -f ./Desktop/access.log --real-os -i -m`

Hits	h% Vis.	v%	Bandwidth	Data
1367	69.29%	0	0.00%	0.0 B 4xx Client Error
1338	67.82%	0	0.00%	0.0 B —404 - Not Found: Requested resource could not be found
10	0.51%	0	0.00%	0.0 B —400 - Bad Request: The syntax of the request is invalid
9	0.46%	0	0.00%	0.0 B —403 - Forbidden: Server is refusing to respond to it
6	0.30%	0	0.00%	0.0 B —408 - Request Timeout: Server timed out waiting for the request
3	0.15%	0	0.00%	0.0 B —405 - Method Not Allowed: Request method not supported
1	0.05%	0	0.00%	0.0 B —417 - Expectation Failed
591	29.95%	2	40.00%	0.0 B 2xx Success
591	29.95%	2	40.00%	0.0 B —200 - OK: The request sent by the client was successful
10	0.51%	1	20.00%	0.0 B 3xx Redirection
10	0.51%	1	20.00%	0.0 B —304 - Not Modified: Resource has not been modified
5	0.25%	2	40.00%	0.0 B 5xx Server Error
4	0.20%	1	20.00%	0.0 B —500 - Internal Server Error
1	0.05%	1	20.00%	0.0 B —501 - Not Implemented

▶▶ 日志工具

□ 将日志分析结果以html格式呈现：

- `goaccess -f ./Desktop/access.log --real-os -i -m -a --log-form=COMBINED`
 > `~/Desktop/a.html`



▶▶ 日志思路

□ 应用被入侵

- Web/FTP 日志 – IP 地址
- 数据库日志/应用日志 – 访问操作、时间
- 系统日志 – 系统操作、用户

□ 怎么判断日志中异常请求

- 时间
- 频率
- 来源
- 恶意代码

绿盟科技版权所有

4.2

取证对象及流程

- a. 取证过程
- b. 常用快速隔离方法

▶▶ 取证过程

- 保护第一现场
 - 避免攻击痕迹被清除
- 按课程内容开展应急响应工作
 - 经验法
 - 回溯攻击法
 - 三要素法
- 不轻信一面之词
 - 与目击者交流相关细节
 - 亲自核实所述、转述情况



快速取证 —— 取证对象

- 病毒/木马文件
- 日志文件
 - 主机日志
 - 应用日志
 - 安全设备日志
- 攻击者残留文件
- 在主机上抓取的流量包



▶▶ 常用快速隔离方法

□ 已经发生安全事件的对象

- 采取例如断网、下线等可行措施进行隔离，避免影响其它主机
- 通过边界控制设备，防止网络区域间相互影响

□ 对于处在危险中的对象

- 采取及时的补救加固措施
- 相关漏洞的扫描修补与跟踪
- 进行黑盒/白盒安全测试





谢谢！

绿盟科技版权所有