# Win 应急响应

1,系统安全

当企业发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，急需第一时间进行处理，使企业的网络信息系统在最短时间内恢复正常工作，进一步查找入侵来源，还原入侵事故过程，同时给出解决方案与防范措施，为企业挽回或减少经济损失。

web 安全

恶意软件

日志

其他应用

应急响应步骤：

前期交互-主机排查

前期交互：主要是先找客户了解主机的基本情况。如：

主机是否存在弱口令

主机是否对外网接通

什么时候发现电脑被入侵，网络攻击的事件类型。

主机日常是否有人进行维护

主机是作为客户机还是服务器

客户机：最近有没有点一些恶意链接，或收到钓鱼邮件

服务器：主机开放了什么服务，日常扮演的角色。

当我们对这台主机了解的越多，我们就越能有一个明确的排查思路，工作就会比较流畅。

主机排查

2.Windows 应急响应

1)操作系统信息

查看这台主机的操作系统信息。

1、开始-》运行-》cmd-》systeminfo

2、开始-》运行-》appwiz.cpl-》已安装更新 查看已安装的补丁信息或者 cmd-wmic qfe list brief

3、查看开放端口：开始-》运行-》cmd-》netstat -ano（注意开放的可疑端口，如果主机未进行断网，则可能还在进行外连，这时需要重点注意 ESTABLISHED。如果有些开放的端口你不太清楚干什么用的，可以在 C:\Windows\System32\drivers\etc\service 查看）

| | |
|---|---|
| LISTENING | 侦听状态 |
| ESTABLISHED | 建立连接 |
| CLOSE_WAIT | 对方主动关闭连接或网络异常导致连接中断 |

4、查看开机启动：

a) 任务管理器-》启动

b) 设置-》应用-》启动

c) 开始-》运行-》msinfo32-》软件环境-》启动程序

d) 检查注册表

HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce

2)环境变量

查看环境变量：cmd-wmic environment list 或者我的电脑-右键属性-高级系统设置-高级-环境变量

排查内容：

1)temp 变量的所在位置的内容；

2)后缀映射 PATHEXT 是否包含有非 windows 的后缀；

3)有没有增加其他的路径到 PATH 变量中(对用户变量和系统变量都要进行排查)；

3)账户和组

1、开始-》运行-》cmd-》net user

3、去 C:\Users 查看是否有多出的家目录

4、开始-》运行-》cmd-》query user。查看现在在线的用户

5、开始-》运行-》cmd-》net user 用户名 查看用户名上次登录时间

排查项：注意是否存在异常用户，或者隐藏用户，克隆用户， 打开 lusrmgr.msc 用户，用户名后面如果有$则是隐藏用户。可以结合日志，查看用户的异常登录时间

6、wmic useraccount list 查看用户，如果只想查看其中的某一项：wmic useraccount get name

7、Wmic group list 查看组，或 wmic group get name 查看某一项

8、开始-运行-compmgmt.msc-本地用户和组-用户

4)网卡

1、wmic nic list

2、网络和共享中心查看有无可疑网络

5)进程

1、netstat -ano

2、tasklist:显示运行在本地或远程计算机上的所有进程；

3、wmic process 获取进程的全路径 get 某一项,第二项

4、终止进程：手动任务管理器或 wmic process where processid=4016 call terminate

主要观察：

- 没有签名验证信息的进程
- 没有描述信息的进程
- 进程的属主
- 进程的路径是否合法
- CPU 或内存资源占用长时间过高的进程

6)计划任务

1、开始-》运行-〉taskschd.msc

2、开始-》运行-〉cmd-》at 或者 schtasks.exe。

7)日志

1、开始-》运行-》eventvwr

可以把日志导出为文本格式，然后使用 notepad++ 打开，使用正则模式去匹配远程登录过的 IP 地址，在界定事件日期范围的基础。

或者通过事件 id，类型，时间等痕迹联动判断是否为攻击行为，以及攻击特点等

这样就可以把界定事件日期事件快速检索出来进行下一步分析；

重要的事件 ID（安全日志，Security.evtx）

4624：账户成功登录

4648：使用明文凭证尝试登录

4778：重新连接到一台 Windows 主机的会话

4779：断开到一台 Windows 主机的会话

2、wmic nteventlog

8)文件

1、开机启动有无异常文件-开机自启动

2、各个盘下的 temp(tmp)相关目录下查看有无异常文件 ：windwos 产生的临时文件 windows/temp

3、浏览器浏览痕迹、浏览器下载文件、浏览器 cookie 信息，根据不同浏览器进行排查；例如：IE 浏览

4、Recent 是系统文件夹，里面存放着你最近使用的文档的快捷方式，查看用户 recent 相关文件，通过分析最近打开分析可疑文件：开始-运行

-%UserProfile%\Recent

5、根据文件夹内文件列表时间进行排序，查找可疑文件。当然也可以搜索指定日期范围的文件及文件

6、查看文件时间，创建时间、修改时间、访问时间，黑客通过菜刀类工具改变的是修改时间。所以如果修改时间在创建时间之前明显是可疑文件

7、获取可执行文件列表

wmic process where "NOT ExecutablePath Like '%windows%'" Get Executabl

ePath ExecutablePath

9)其他

1、如果存在 445 端口查看文件共享

开始-》运行-》cmd-》net share

2、查看服务开始-》运行-》services.msc

3、敏感目录排查

%WINDIR%

%TEMP%

%UserProfile%\Recen 最近打开的文件

%LOCALAPPDATA%

%APPDATA%

Appdata 下有三个子文件夹 local，locallow,roaming,当你解压缩包时如果不指定路径，系统就把压缩包解到 local\temp 文件夹下，存放了一些解压文件，安装软件时就从这里调取数据特别是一些制图软件，体积非常大，占用很多空间。locallow 是用来存放共享数据，这两个文件夹下的文件就用优化大师清理，一般都可以清理无用的文件。roaming 文件夹也是存放一些使用程序后产生的数据文件，如空间听音乐，登入的号码等而缓存的一些数据，这些数据优化大师是清理不掉的，可以打开 roaming 文件夹里的文件全选定点击删除，删除不掉的就选择跳过，不过当你再使用程序时，这个文件夹又开始膨胀，又会缓存数据.

4、组策略排查开始-》运行-》gpedit.msc

5、可以把 wmic 的命令写下来

Wmic 1>1.txt

Wmic 2>2.txt

保存成 bat 文件

病毒分析

PCHunter：http://www.xuetr.com

火绒剑：https://www.huorong.cn

Process Explorer：
https://docs.microsoft.com/zh-cn/sysinternals/downloads/process-explorer

processhacker：https://processhacker.sourceforge.io/downloads.php

autoruns：https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

OTL：https://www.bleepingcomputer.com/download/otl/

SysInspector：http://download.eset.com.cn/download/detail/?product=sysinspector

病毒查杀

卡巴斯基：http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe

大蜘蛛：http://free.drweb.ru/download+cureit+free

火绒安全软件：https://www.huorong.cn

360 杀毒：http://sd.360.cn/download_center.html

病毒动态

CVERC-国家计算机病毒应急处理中心：http://www.cverc.org.cn

微步在线威胁情报社区：https://x.threatbook.cn

火绒安全论坛：http://bbs.huorong.cn/forum-59-1.html

在线病毒扫描网站

多引擎在线病毒扫描网：http://www.virscan.org

腾讯哈勃分析系统：https://habo.qq.com

Jotti 恶意软件扫描系统：https://virusscan.jotti.org

针对计算机病毒、手机病毒、可疑文件等进行检测分析：http://www.scanvir.com

webshell 查杀

D 盾_Web 查杀：http://www.d99net.net/index.asp

河马 webshell 查杀：http://www.shellpub.com

深信服 Webshell 网站后门检测工具：
http://edr.sangfor.com.cn/backdoor_detection.html

在线沙箱分析

360 安全大脑沙箱云：https://ata.360.net/dashboard

微步云沙箱：https://s.threatbook.cn/

魔盾安全分析：https://www.maldun.com/submit/submit_file/

3.如何查找克隆账号

查找办法为打开注册表，其中 users 字段为用户权限有密码; names 字段为用户名。在 Users 这个注册表中，F 为权限值，V 为密码值。我们判断是否存在提权用户或克隆用户，是将用户的权限键值与管理员的权限键值作对比分析。其中权限项中的键值并不是全部为权限值，而是后面四行为权限键值，我们的分析办法就是把这些用户的权限键值全部取出来，然后和管理员的权限键值作比较。和管理员的权限键值一样的，我们就判断为提取用户。

可以看到 admin$和 administrator 注册表 F 值的权限值(最后 4 行)一样，说明

admin$是 个克隆账号。另外，如果一个账号属于 administraotrs 管理员组，它的 F 值和 administrator 的 F 值中的权限值是不一样的。查找克隆账号必须通过注册表中 sam 中用户 F 值的最后四行来区分;管理员组只需要通过 net localgroup administrators 就可以查找到，但是通过 net localgroup administrators 无法找到克隆账号。

查找隐藏账户：

1、wmic useraccount get name,SID

2、注册表　HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names

3、控制面板-用户账户-管理账户

日志分析工具：

链接：https://pan.baidu.com/s/1M1pmAPc1gAAxXjw4ouprUQ

提取码：24z5

用法：evtxLogparse.exe -r success security.evtx