1. 护网基础知识

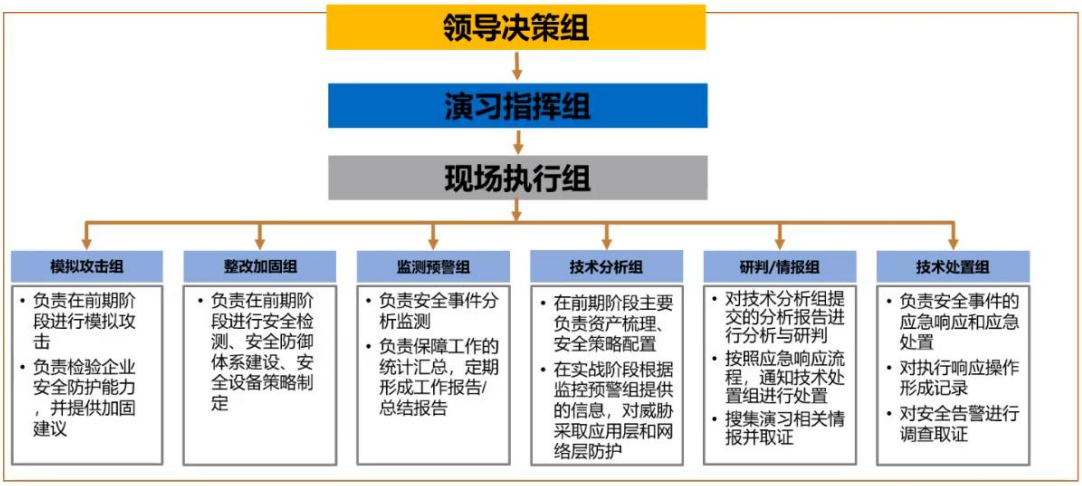
1.1 护网定义:护网行动是由公安机关组织的“网络实战攻防演习”

1.2 HW 目的:

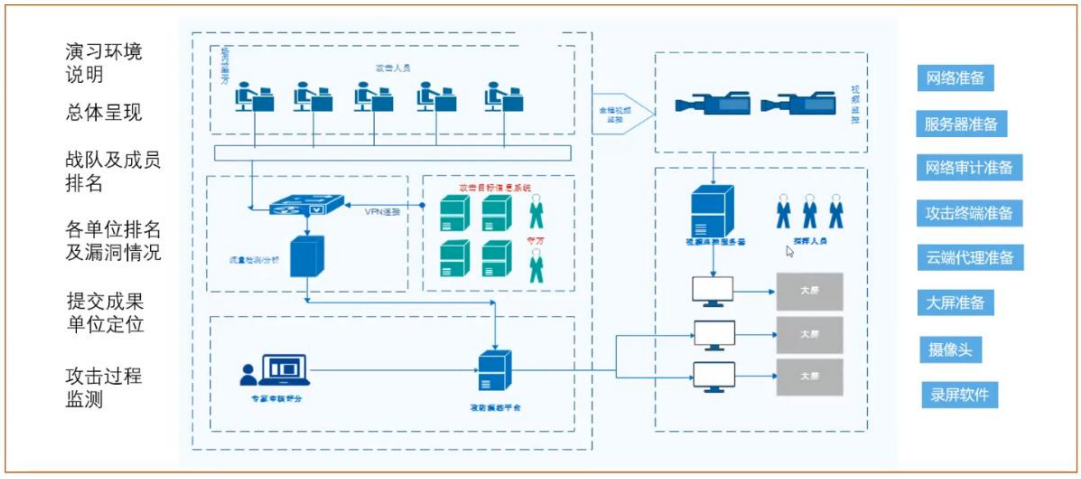
(1)及时发现并整改网络安全深层次问题隐患，检验并提升国家关键信息基础设施安全防护能力和应急处置能力

(2)进一步加强重点单位、社会力量与公安机关的协同配合和联合作战能力;“(3)通过攻防实战，提高攻防双方技术对抗、决策指挥及应急处置能力

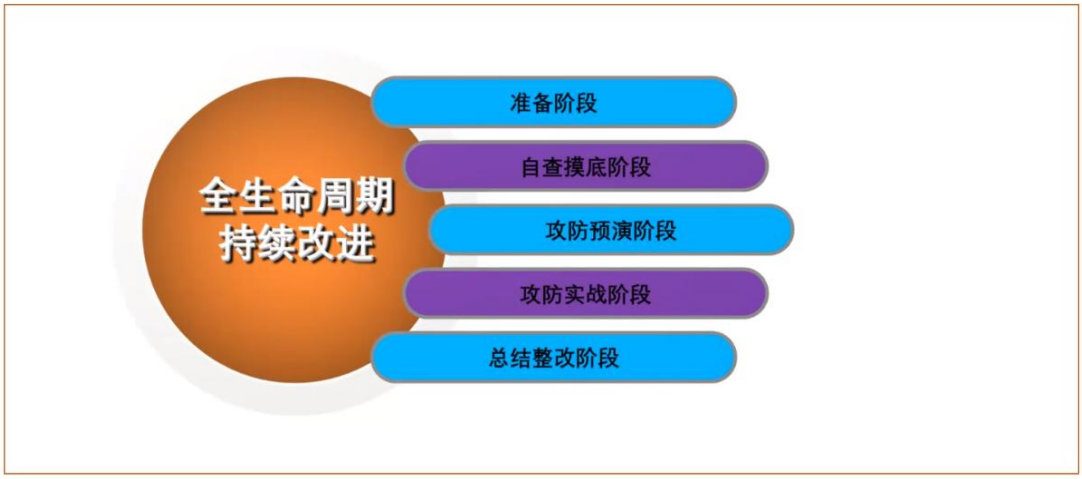
组织架构



HW组织方与平台



攻防演习及防护过程总览



1.3 攻防演习防护过程

(1)准备阶段

1、防守方案编制
2、防守工作启动会
3、人员结构组织
4、目标系统梳理
5、网络架构检查
6、安全防护设备、厂商梳理了解
7、APT 检测、流量分析、态势感知等安全监测设备梳理了解

(2)自查阶段

1、互联网资产扫描探测
2、漏洞扫描
3、渗透测试
4、安全风险检查(集权类系统、网络划分应用系统、网络攻击风险等检查
5、安全基线/配置核查
6、安全设备策略有效性检查
7、日志审计情况检查
8、重大活动或之前进行的安全评估结果复查
9、安全监测、防护设备补充完善
10、安全整改加固

安全设备:

边界隔离：网闸、下一代防火墙/UTM

旁路检测：IDS/CS，网络审计、数据库审计、APT、全流量分析系统

数据传输加密：VPN、加密机

WEB 服务器重点防护：服务器区前端部署 WAF，部署网页防篡改系统

终端管控：EDR

平台监控：安全管理平台

其他设备：漏洞扫描、基线核查、威胁情报系统、蜜罐、攻防演练平台

(3) 演练阶段

1、授权与备案
2、预演习攻击
3、预演习防护
4、问题分析总结
5、安全整改与加固

(4)实战阶段

1、安全事件实时监测

2、安全事件分析

3、应急响应和决策处置

(5)总结阶段

在演习过程中还存在的脆弱点，开展整改工作，进一步提高目标系统的安全防护能力

防守事件分类：木马后门、异常登陆、钓鱼邮件、漏洞攻击、暴力破解、数据窃取、拒绝服务。

事件分级:

一级：演习目标被控制

二级：黄重要系统或设备被控制

三级：内网一般设备被控制

四级：DMZ 区一般设备被控制

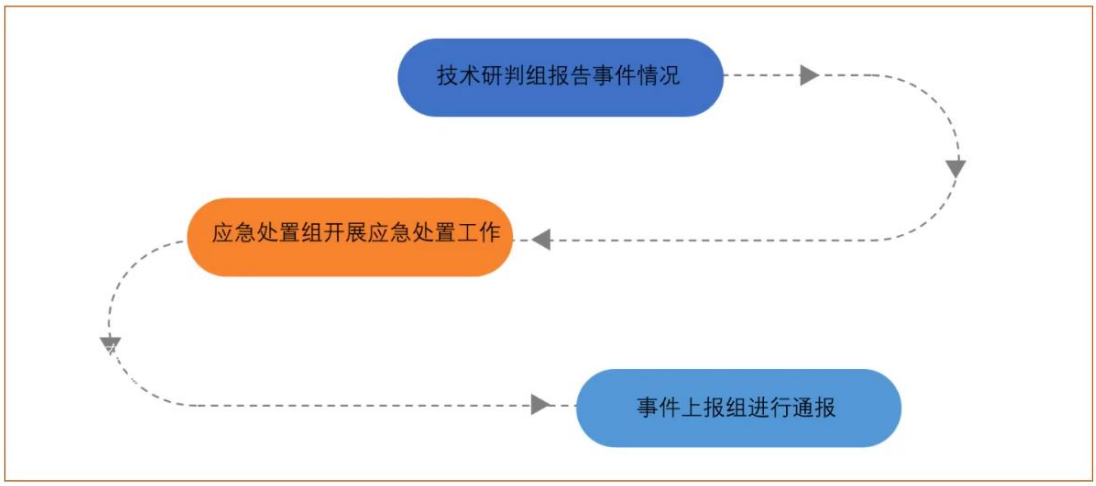
五级：DMZ 区设备遭到攻击或内网终端遭到攻击

事件流转

按照扁平化指挥原则，通过建立护网行动即时通讯群组，统一进行调度：

1. 总部在群组中及时发布预警信息指令，
2. 子分公司及时通过群组向总部进行事件汇报。
3. 随后详细情况材料按照处置流程通过OA系统、事件上报平台上报。

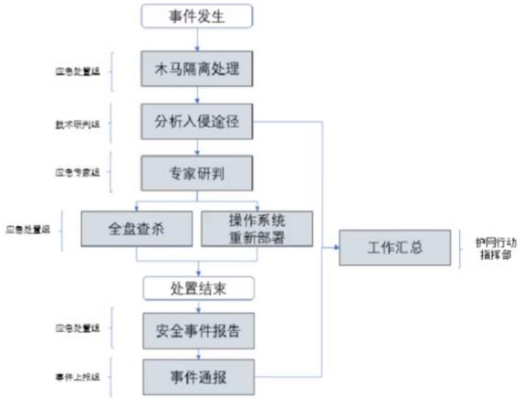
事件处置方式



木马后门事件

处置方法:

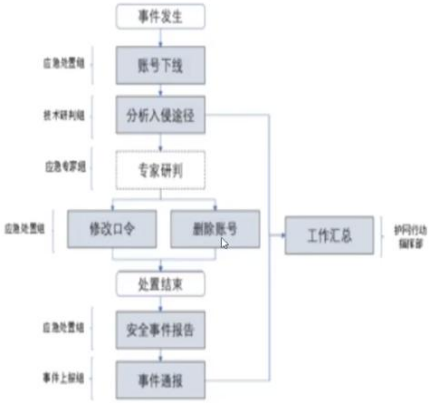
1. 先针对出现木马后门设备进行断网隔离处理，
2. 同时将该设备日志进行备份留存分析入侵途径，
3. 随后对操作系统进行重新部署或病毒软件进行全盘查杀



异常登录事件

处置方法:

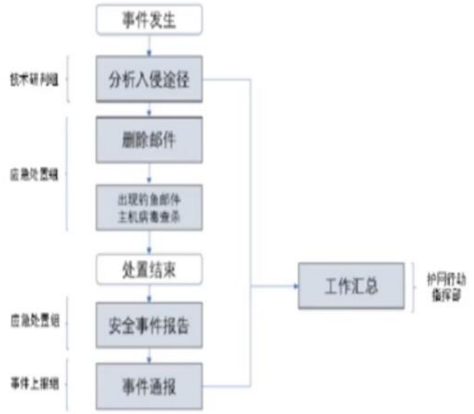
1. 先将相关账号下线并留存账号相关日志
2. 随后针对问题账号采取修改口令或删除账号等方式进行处理。



钓鱼邮件事件处置

处置方法:

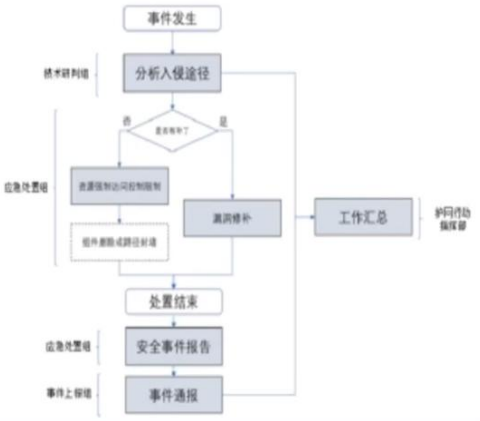
1. 对邮件内链接仔细核查溯源，
2. 删除相关邮件
3. 对收到钓鱼邮件的主机进行病毒查杀。



漏洞攻击事件处置

处置方法:

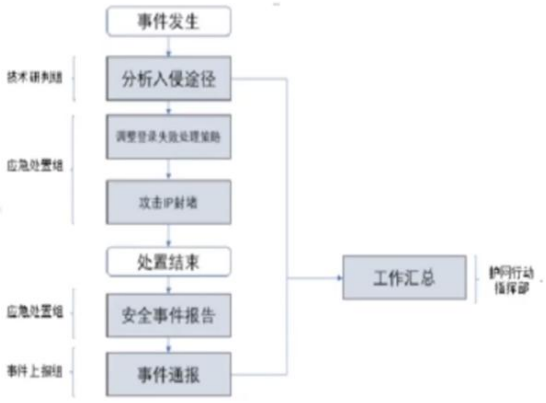
1. 无补丁情况，采取“白名单”策略，对正常服务的路径进行加白，
2. 在主机配置强制访问控制策略，对进程、驱动等资源进行强制管理;
3. 有补丁情况，加强信息系统漏洞巡检和补丁修复，采取相应技术手段，检查漏洞修复情况，并督促整改。



暴力破解事件处置

处置方法:

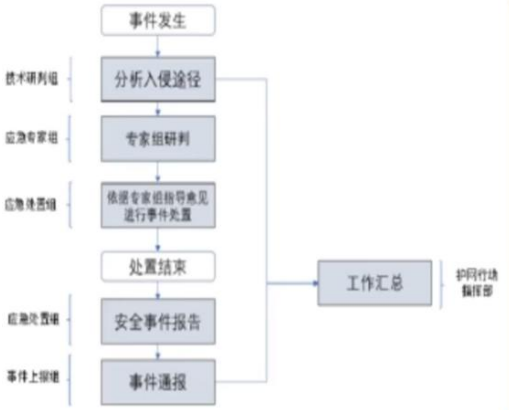
1. 针对产生暴力破解事件的相关攻击IP 进行有效封锁
2. 并关注出现被暴力破解事件系统运行状态。



事件流转

处置方法:

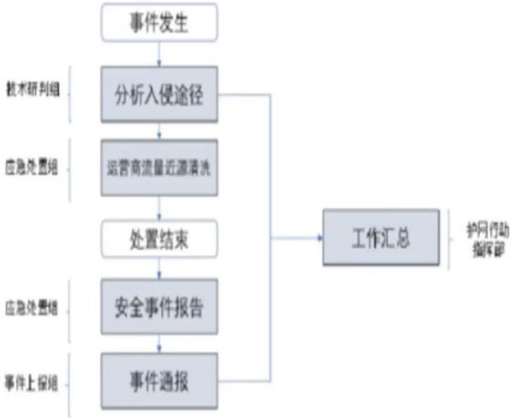
1. 组织技术研判组对失窃数据内容及范围进行研判，根据研判结果向相关业务主管部门进行通报，
2. 相关业务主管部门在收到通报后，应在第一时间根据技术研判组研判建议采取相关处置措施，防止事件升级。



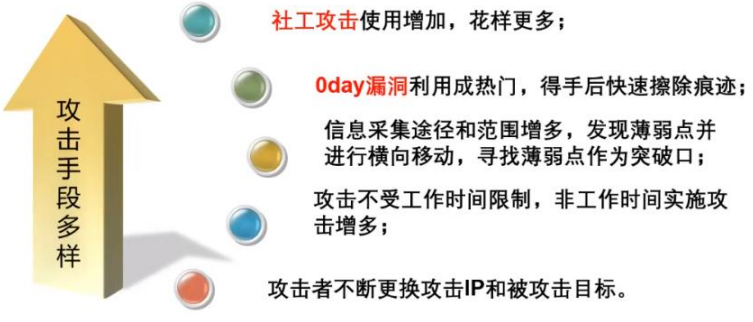
事件流转

处置方法:

1. 借助互联网出口运营商防护资源实现拒绝服务流量近源清洗
2. 关注出现拒绝服务攻击事件系统的运行状态。



HW新变化



社工攻击使用增加，花样更多；

0day漏洞利用成热门，得手后快速擦除痕迹；

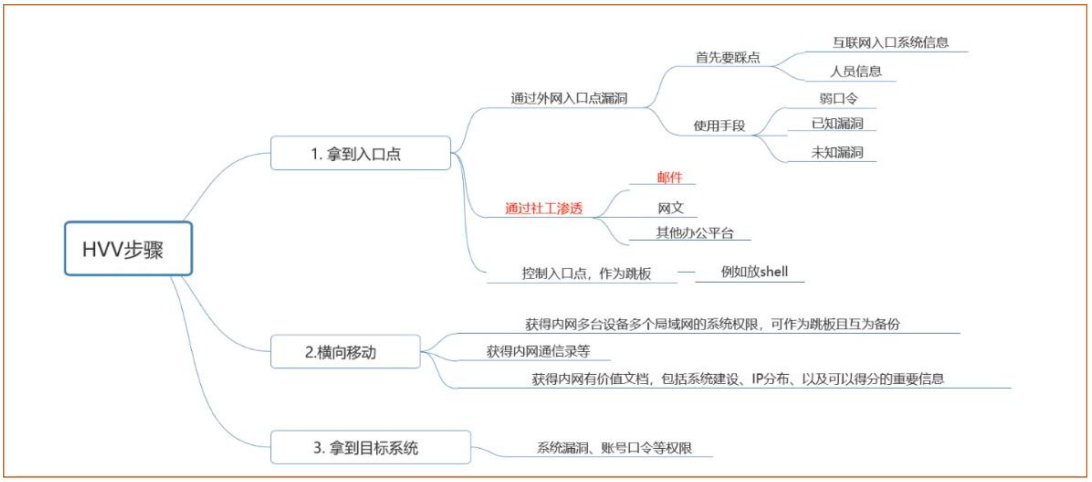
信息采集途径和范围增多，发现薄弱点并进行横向移动，寻找薄弱点作为突破口；

攻击不受工作时间限制，非工作时间实施攻击增多；

攻击者不断更换攻击IP和被攻击目标。

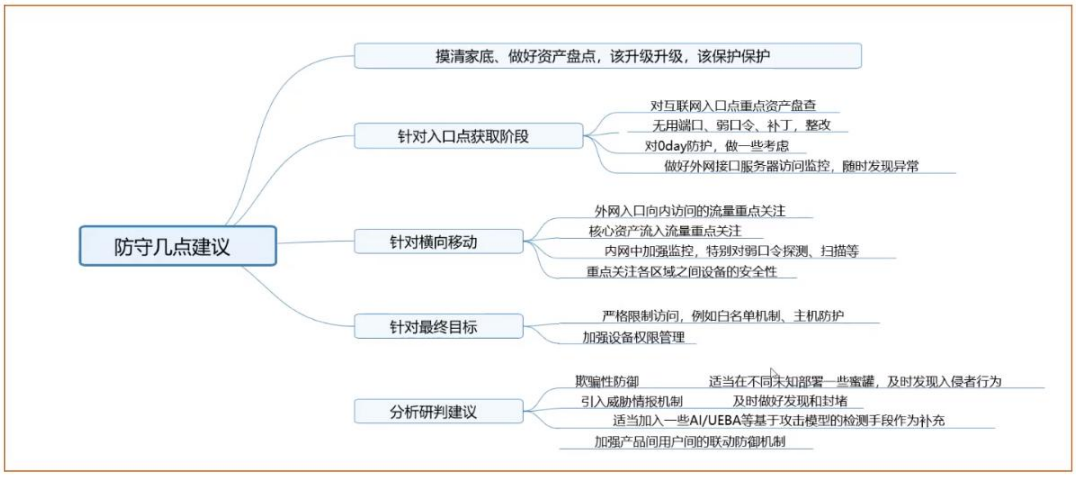
攻击手段

攻击方式



全面防护，与时俱进

基于攻击的防守应对措施



经验总结

1. **攻击方不会守规矩**：名义上攻击时间段为工作日的 9:00-17:00；实际上攻击方不会遵守时间规则，晚上和周末均会发起攻击。
2. **攻击方式多样：**主要以远程网络入侵为主、还会存在社工等方式。
3. **谨慎上报目标系统：**目标系统被攻破意味着该单位此次护网失败。
4. **充分备战最为关键：**深入研究得分规则和总结往年攻防经验，在演习前做好充分的防护准备和应急预案等。
5. **全面检测、分析、展示机制不可缺失：**被动安全防护机制不能实现全面感知、智能协同的主动防御目的，难以满足HW过程中的多点、多样化攻击。
6. **建立威胁情报系统：**建立适合自身需要的威胁情报系统，及时更新威胁情报库。
7. **证据妥善保管：**保留好相关攻击数据、截图及样本证据，为溯源提供材料。

经验总结

准备阶段：

资产梳理，对资产进行漏洞扫描，补丁修复。根据业务通过流量监控设备建立黑白名单，有利于发现0day。
明确防守边界，对边界防火墙进行访问控制策略收紧，关闭不必要的（高危）端口

攻击阶段：

保证7*24小时安全监控，多为夜间攻击。
加强弱口令防护，发现弱口令及时上报修改。
防范钓鱼邮件。
及时应急响应处置，将危险范围降为最小，并及时溯源上报。
威胁情报：因为攻击方使用的都是运营商提供的新的IP和域名，可以进行随时更换，
所以需要建立自己的威胁情报系统。通过兄弟单位、协作单位进行威胁情报收集；及时更新威胁情报库。

溯源阶段：

保留好相关攻击数据、截图及样本证据，为溯源提供材料。

经验总结

高效联动	• **明确**保障目标、多部门确保高效协作
实战练兵	• **实战**是检验安全防护能力的最快方法
体系建设	• 安全保障是一个**体系**，不只是**攻**与**防**
应急机动	• **体系建设**重在坚持、**应急处置**贵在争分夺秒

3.Windows 问题排查

3.1 文件排查,

3.1.1 文件分析

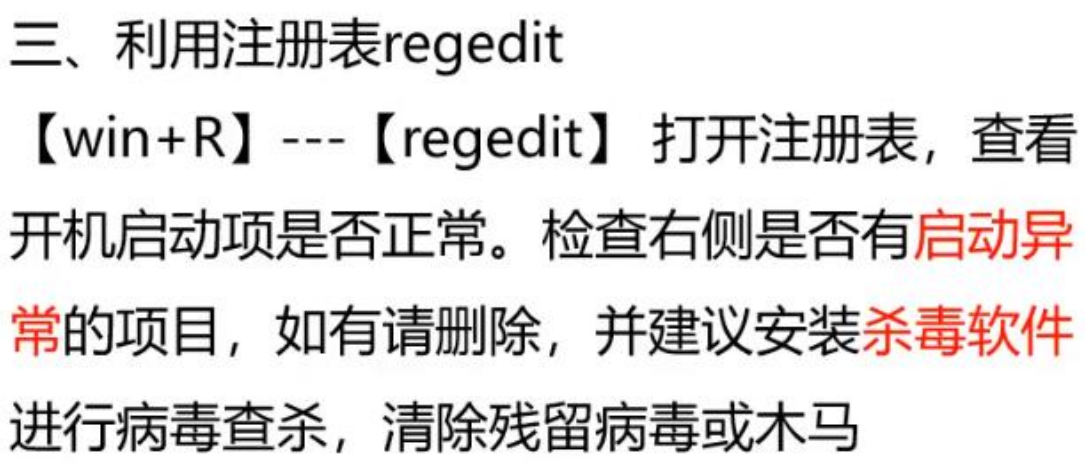
windows 系统中可以通过以下三种方式查看开机启动项

1. 利用操作系统中的启动菜单

2. 利用系统配置 msconfig 查看

二、利用系统配置msconfig （ms代表微软，config代表配置）【win+R】---【msconfig】，查看是否存在可疑启动项

3.利用注册表 regedit 查看



3.1.2 临时文件

文件分析-- temp临时文件

Temp是指系统临时文件夹。在Windows中，temp文件夹主要分布在下面三个位置。

1. C:\Windows\Temp 系统公用;
2. C:\Users\Administra tor\Local Settings\Temp;
3. C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\（默认为隐藏目录）

文件分析-- temp临时文件

【win+E】
【C:\Users\Administrator\AppData\Local\Temp】

查看temp文件夹下的PE文件(exe , dll , sys)，查看是否有特别大的tmp文件

文件分析-- temp临时

【win+R】---【%temp%】

查看temp文件夹下的PE文件(exe , dll sys) , 查看是否有特别大的tmp文件

发现可疑文件，检测是否为恶意软件

将可疑文件上传到在线网站 https://www.virustotal.com 或微步云沙箱https://s.threatbook.cn/ 进行查看， 检查是否为恶意文件。

文件分析--时间属性分析

黑客拿下服务器后，极有可能会使用浏览器进行网站访问。我们可查看浏览器记录，进一步分析：

- 查看浏览器下载记录，看是否被使用下载恶意代码及文件
- 查看浏览记录是否有浏览恶意网站等

文件分析--时间属性分析

在Windows系统下，文件属性的时间属性具有：

- 创建时间
- 修改时间
- 访问时间

如果修改时间要早于创建时间那么这个文件存在很大可疑。（中国菜刀等工具可修改）

选中文件【右键】---【属性】

文件分析--最近打开文件分析

Windows系统会记录系统中最近打开使用文件的快捷方式，通过以下方法可查看最近打开的文件：

- 【win+E】---【C:\Documents and Settings\Administrator\Recent】
- 【win+E】---【C:\Users\Administrator\Recent】
- 【win+R】---【%UserProfile%\Recent】

进程排查

本地计算机与外部网络通信是建立在TCP或UDP协议上通过端口（0-65535)进行通信，通常计算机被中木马后，一定会与外部网络通信，此时可通过网络连接状态，找到对应的进程ID，关闭进程ID（关闭进程ID即意味着关闭连接状态）

状态	含义
listening	表示监听 表示这个端口正在开放 可以提供服务
closing	表示关闭的 表示端口人为或者防火墙使其关闭(也许服务被卸载)
time wait	表示正在等待连接 就是你正在向该端口发送请求连接状态
established	表示是对方与你已经连接 正在通信交换数据

查看所有的端口占用情况命令 netstat-ano

参数说明:

-a 显示所有网络连接、路由表和网络接口信息

-n 以数字形式显示地址和端口号

-0 显示与每个连接相关的所属进程 ID

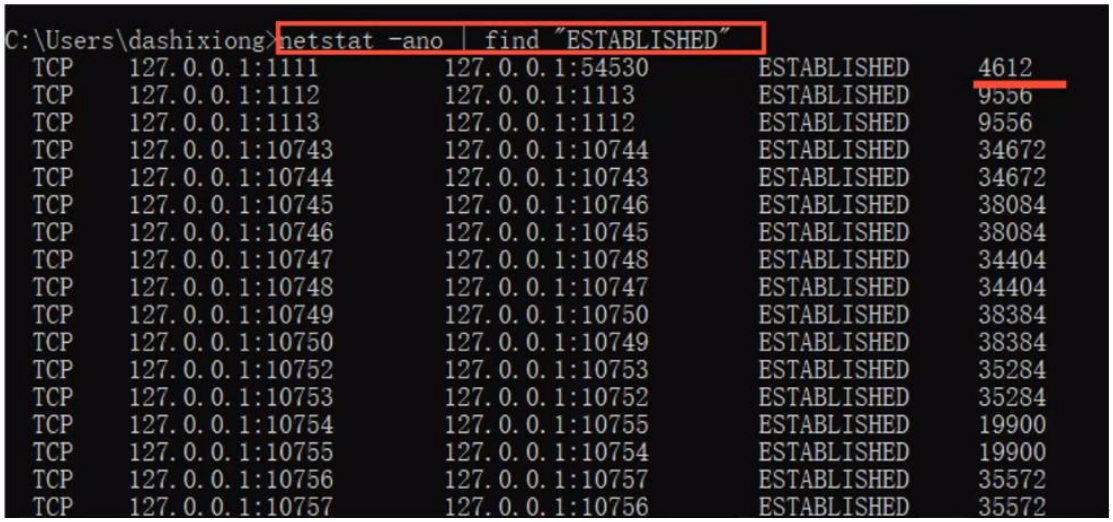
-r 显示路由表

-s 显示按协议统计信息、默认地、显示 IP

记录一次进程排查:

1. 查看所有 的端口占用情况命令 netstat -ano

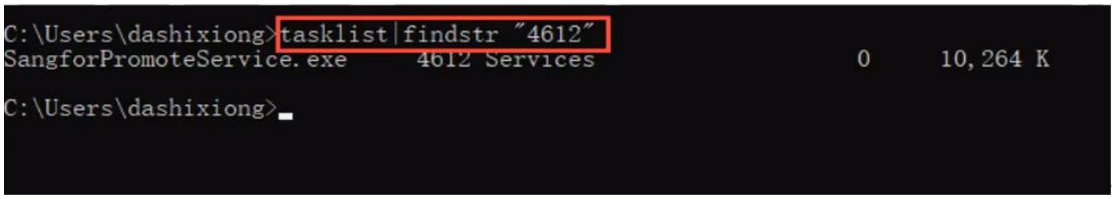
2. 查看端口 中状态为 established 的所有进程 netstat -ano | find "ESTABLISHED"



发现"可疑进程”定位 PID 值为 4612

查看指定 PID 的占用情况: netstat -aon | findstr "XXX"(XXX 代表的是具体进程的 PID 值)

查看 PID 对应的进程命令: tasklist | findstr "XXX"



杀死(结束)该“可疑进程“: taskkill /f /t /im SangforPromoteService.exe

进程排查

也可以采用以下方法:

1. 先根据netstat定位出pid
2. 再通过tasklist命令进行进程定位,
3. 根据wmic process 获取进程的全路径任务管理器定位到进程路径

进程排查

- ✓ 查询进程
- wmic process（带有cmdline）
- wmic process list brief
- wmic process where name= “xxxx” get executablepath
- ✓ 删除进程
- wmic process where processid="2345" delete

进程排查

- ✓ 查询服务
- wmic SERVICE（涵盖服务关联所有信息）
- wmic SERVICE where caption(name)=” XXX” call stopservice
- wmic SERVICE where caption(name)= “XXX" call delete

进程排查

- ✓ 启动项枚举
  - wmic startup list full
- ✓ 计划任务枚举
  - schtasks /query /fo table /v（执行前先执行chcp 437）

系统信息排查

系统信息排查

- ✓ 查看环境变量的设置【我的电脑】---【属性】---【高级系统设置】---【高级】---【环境变量】
- ✓ Windows 计划任务【程序】---【附件】---【系统工具】---【任务计划程序】

系统信息排查

- ✓ Windows帐号信息，如隐藏帐号等【开始】---【运行】---【compmgmt.msc】---【本地用户和组】---【用户】(用户名以$结尾的为隐藏用户)
- ✓ 命令行方式：net user，可直接收集用户信息，若需查看某个用户的详细信息，可使用命令---net user username;

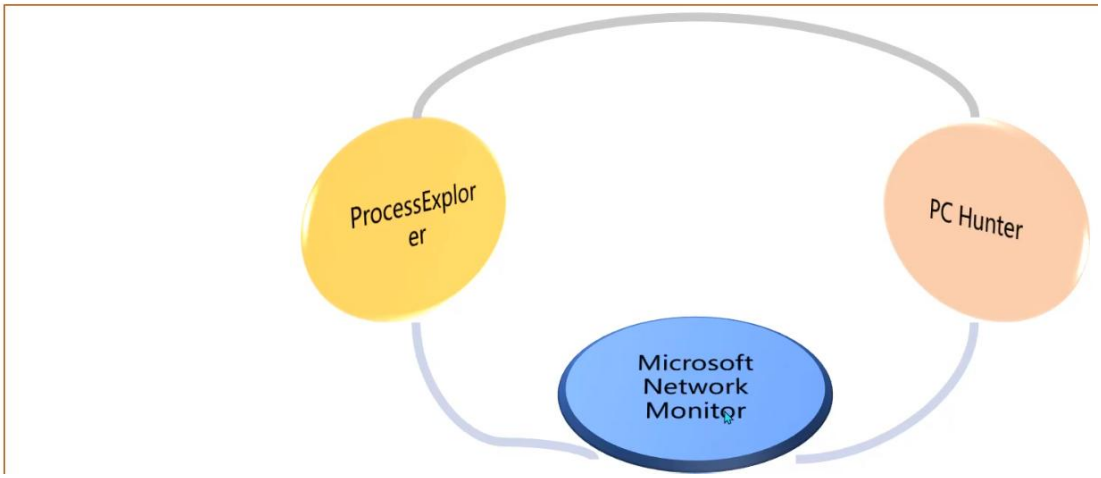
系统信息排查

- ✓ 查看当前系统用户的会话使用➜ query user 查看当前系统的会话，比如查看是否有人使用远程终端登录服务器
- ✓ logoff 踢出该用户

系统信息排查

- ✓ 查看systeminfo信息， 系统版本以及补丁信息
- ✓ Github源码： https://github.com/neargle/win-powerup-exp-index

工具排查



工具排查

Procexp是常用的进程查看工具：

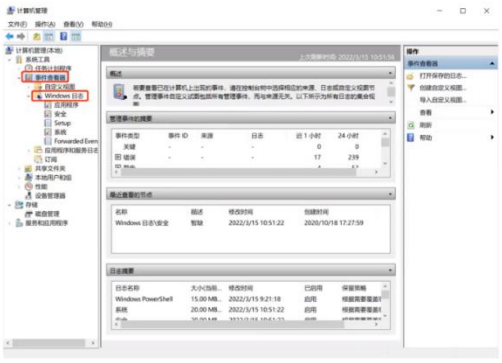
- ➢ 打开procexp，进程标识颜色不同是用于区分进程状态和进程类型， 进程开始启动时为绿色， 结束时为红色
- ➢ 可对某个进程进行操作， 右键单击即可

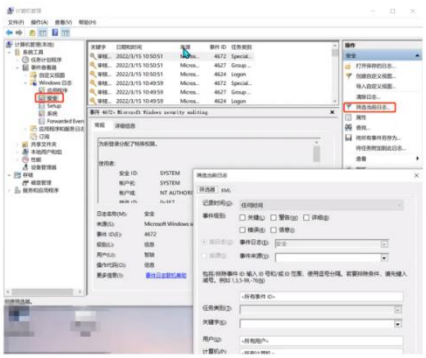
日志排查

Windows 日志包括:登录日志、安全日志、中间件日志

日志排查

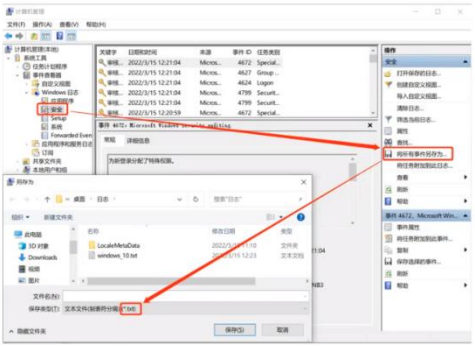
- ✓ Windows登录日志排查
- ✓ 主要分析安全日志， 可以借助自带的筛选功能





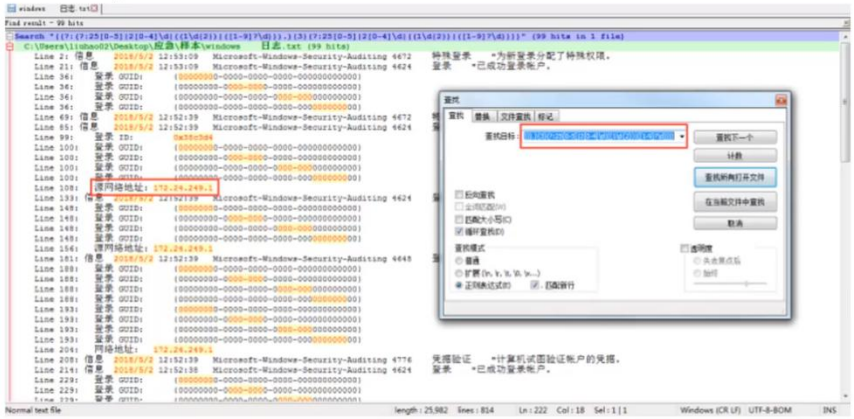
日志排查

- ✓ 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使用正则表达式匹配



日志排查

- ✓ 中间件日志(Web日志access_log)nginx、 apache、 iis、 tomcat、 jboss、 weblogic、 websphere



4.2 SQL 注入

4.2.1 原理

SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令

4.2.2 危害

(1)未经授权可以访问数据库中的数据，盗取用户的隐私以及个人信息，造成用户的信息泄露。

(2)对数据库的数据进行增加或删除操作(私自添加或删除管理员账号)

(3)篡改网页且发布违法信息(网站目录存在写入权限，写入网页木马)

(4)获取服务器最高权限(提权)，远程控制服务器，安装后门，修改或控制操作系统

4.2.3 修复建议

1、代码中的数据库操作采用 sql 语句预编译和绑定变量,避免直接使用参数值拼接字符串。可从根本上杜绝 SQL 注入

2、在代码中对用户输入的数据进行严格过滤。对涉及到数据库的操作的所有参数，过滤危险字符串，如 select union sleep '(from where concat char 等敏感字符

3、对所有传入 SQL 语句的变量进行处理，比如字符串变量单引号包裹并转义、数字类型变量进行强制类型转换等

4、在网络层面，部署 Web 应用防火墙

5、在数据库层面，对数据库操作进行监控

6、做好数据库用户权限控制,比如对数据库配置使用最小权限原则，线上尽量不使用 root、sa 等高权限用户连接数据库

核心：防御 SQL 注入的核心思想是对用户输入的数据进行严格的检查，并且对数据库的使用采用最小权限分配原则

4.3 XML 注入

4.3.1 原理

XPath 注入攻击，是指利用 XPath 解析器的松散输入和容错特性，能够在 URL、表单或其它信息上附带恶意的 XPath 查询代码,以获得权限信息的访问权并更改这些信息。XPath 注入攻击允许攻击者在事先不知道 XPath 查询相关知识的情况下，通过 XPath 查询得到一-个 XML 文档的完整内容。

4.3.2 危害

1、在 URL 及表单中提交恶意 XPath 代码，可获取到权限限制数据的访问权，并可修改这些数据

2、可通过此类漏洞查询获取到系统内部完整的 XML 文档内容

3、逻辑以及认证被绕过，它不像数据库那样有各种权限，xml 没有各种权限的概念，正因为没有权限概念，因此利用 xpath 构造查询的时候整个数据库都会被用户读取。

4.3.3 修复建议

1、数据提交到服务器上,在服务端正式处理这批数据之前,对提交数据的合法性进行验证
2、检查提交的数据是否包含特殊字符，对特殊字符进行编码转换或替换、删除敏感字符或字符串，如过滤[] ‘“and or 等,像单双引号这类，可以对这类特殊字符进行编码转换或替换

4.4 XXE

4.4.1 原理

XXE 漏洞全称 XML External Entity Injection 即 xml 外部实体注入漏洞，XXE 漏洞发生在应用程序解析 XML 输入时，没有禁止外部实体的加载。

4.4.2 危害

当允许引用外部实体时，通过构造恶意内容，导致可加载恶意外部文件和代码,造成任意文件读取、命令执行、内网端口扫描、攻击内网网站、发起 Dos 攻击等危害。

4.4.3 修复建议

1、处理 XML 时禁止引用外部实体,比如 php，可调用 libxml. disable. entity. loader(true)、 java 可调用 factory.setProperty(XMLInputFactory.SUPPORT DID, false)等
2、如有用到 libxml2 库，检查其版本是否为 2.9.0 或以上版本，如版本较低建议升级
3、尽量不要让用户直接提交 XML 代码，如果业务需要得做好过滤等处理

4. 5 XSS

4.5.1 原理

XSS (Cross Site Scripting): 即跨站脚本攻击，在页面中注入恶意的脚本代码，当受害者访问该页面时，恶意代码会在其浏览器.上执行，XSS 不仅仅限于 JavaScript,还包括 flash 等其它脚本语言。

XSS 种类

恶意代码是否存储在服务器中，XSS 可以分为存储型的 XSS 与反射型的 XSS。
反射型(非持久):主要用于将恶意代码附加到 URL 地址的参数中,常用于窃取客户端 cookie 信息和钓鱼欺骗。
存储型(持久型):攻击者将恶意代码注入到 Web 服务器中并保存起来,只要客户端访问了相应的页面就会受到攻击。

4.5.2 危害

(1)窃取管理员帐号或 Cookie (恶意操纵后台 数据)
(2)窃取用户的个人信息(登录帐号、冒充用户身份进行各种操作)
(3)网站挂马
(4)发送广告或者垃圾信息(利用 XSS 漏洞植入广告、发送垃圾信息)
(5)劫持用户(浏览器)会话,从而执行任意操作(非法转账、强制发表日志、电子邮件)
(6)进行大量的客户端攻击，如 DDoS 等
(7)获取客户端信息，如用户的浏览历史、真实 ip、 开放端口等
(8)控制受害者机器向其他网站发起攻击

4.5.3 修复建议

(1)输入编码转义:对输入的数据进行 HTML 转义，使其不会识别为可执行脚本
(2)增加过滤器 XssFilter
(3)白名单过滤:根据白名单的标签和属性对数据进行过滤，以此来对可执行的脚本进行清除(如 script 标签，img 标签的 onerror 属性等)

4.6 CSRF

4.6.1 原理

CSRF(Cross- site request forgery):跨站请求伪造，是指利用受害者尚未失效的身份认证信息(cookie、会话等)，诱骗其点击恶意链接或者访问包含攻击代码的页面，在受害人不知情的情况下以受害者的身份向(身份认证信息所对应的)服务器发送请求，从而完成非法操作(如转账、改密等)。

CSRF 和 XSS 区别

XSS:跨站脚本攻击，在用户的浏览器中执行攻击者的脚本，来获得其 cookie 等信息。
CSRF:借用用户的身份，向 web server 发送请求，因为该请求不是用户本意，所以称为“跨站请求伪造”。

4.6.2 危害

1.完成受害者所允许的任-状态改变的操作(邮件、 发消息、购买商品、更新账号、注销、登录等)
2.修改受害者的网络配置(修改路由器 DNS、重置路由器密码)
3.获取用，户的隐私数据、机密资料
4.用户财产安全
5.配合其他漏洞攻击

概括:盗用受害者身份，受害者能做什么，攻击者就能以受害者的身份做什么。

4.6.2 修复建议

1、验证 http referer 字段
2、在请求地址中添加 token 并验证
3 在 http 头中自定义属性并验证
4 其他防御方法
<1>关闭页面时要及时清除认证 cookie,对支持 tab 模式(新标签打开网页)的浏览器尤为重要。
<2> 尽量少用或不使用 request() 类变量，获取参数指定 request.form() 还是 request.querystring(),(增加了攻击难度)

5.蓝军防守技术

5.1 监控值守介绍

5.1.1 定义:

指借助安全设备(WAF、IDS、IPS 等)开展安全事件实时监测,对发现的攻击行为进行确认，详细记录攻击相关数据，为后续处置工作开展提供信息的一种工作。

工作内容:

负责安全事件分析监测，策略调整,状态巡检，协助封堵

负责保障事件的上报，统计汇总，定期形成工作报告/总结报告等

重要性:

整个防护体系的最前沿，安全事件的第一发现者

事件分析的前提，后续流程运转的基础

快速遏制攻击行为，可调整策略阻挡攻击

旁路部署:通过交换机等网络设备的“端口镜像"功能来实现监控质。

串联部署:指串联在链路中，可以控制流量。

5.2 蓝队工作职责与模式

5.2.1 岗位职责

设备监控岗:初步监控攻击事件，做简单分析并上报

分析研判岗:对攻击方式、路径、范围、结果等作分析研判，找到攻击者信息

应急响应岗:攻击事件影响分析，复现及溯源等

处置封禁岗:事件的处置，包括封禁 IP

安全事件的分析监测

1.从行内的背景流量 SQL 注入攻击中，甄别出真实攻击，第一时间向上报送，完成处置

2.演练刚开启前期，大量扫描探测行为，及时封禁可有效阻断攻击方对资产信息的收集

3. 从多条告警中形成对攻击者的画像

安全事件的策略调整

1.根据行内的业务和日常告警日志，优化整体策略

2.新出现的安全漏洞针对性增加规则

3.发现攻击者成功利用某种漏洞，针对漏洞优化规则

安全设备状态巡检

1.每日经过流量的变化情况

2. 特征库授权，探针授权等等

3. 设备磁盘，CPU 状态查看，长时间无新告警时的排查

安全事件的协助封堵:
1.防护类设备对攻击者 IP,进行加黑
2.通过策略对攻击行为进行阻断

5.2.2 事件上报一般性原则(重点)

1.上报事件查IP归属地
2.IP上报不重复
3.重点关注事件响应动作为PASS的
4.攻击频率高要上报
5.漏洞利用类要重点上报
6.低危事件大量扫描必上报（批量）
7.国外IP要上报处置
8.确定恶意攻击必上报
9.一个IP对多个资产进行攻击要上报
10.高危事件重点关注（敏感文件访问、文件上传、或者webshell连接等）
11.监控事件遵循原则：先看相应动作，再看详细报文分析，再看IP

事件上报:
事件上报时须包括:攻击 IP，归属地，目的 IP，时间，事件类型
封禁记录:
若担任有封禁 IP 任务的，在 IP 封禁后-般要填写封禁信息表

工作汇报
每日事件统计时，注意统计的时间、区间，设备和事件的对应。
每日工作报告需包括:总体告警数量，上报事件数量， 类型分布，重点关注事件等。

5.3 安全平台/设备

5.3.1 安全设备类别
安全监测类: IDS、IPS、APT4
安全防护类:防火墙、WAF、抗 DDOS
安全分析类:入侵分析、流量分析
安全管理/展示类:安全运营平台、态势感知

5.3.2WAF:

特点:
1.基于算法引擎和特征引擎双引擎检测方法
2．针对 Web 服务器进行 HTTP/HTTPS 流量检测和防御

防护场景:
恶意扫描防护
漏洞利用防护
暴力破解防护
SQL 注入防护
XSS 注入防护
敏感信息泄露防护
Web 网站应急保障

WAF 日志分析注意事项:
一键请求头信息提取
解码工具
安全事件日志导出
Web 应用漏洞事件分析:合理利用互联网资源，根据事件名称搜集漏洞相关信息，初步了解攻击原理;提取事件请求头信息和原始报文;根据用户环境分析是否真实攻击。

5.3.3 IPS
特点:
深层防御、精确阻断
可及时准确发现入侵攻击行为实时精确阻断
主动而高效
IPS 日志分析:
双击入侵防御日志，查看日志内容，特征性质判定，特征处理流程。
日志内容最大长度为 4k。
解码工具支持 URL 编解码，16 进制解码，BASE64 解码。
标红部分为命中特征部分
IPS 日志分析注意事项：
合理使用日志过滤功能，提高事件分析的效率，常用过滤动作: pass
点击事件右侧内容可以根据报文详细信息进一步分析攻击行为
针对攻击事件存在误报可能性，具体可通过安域 IP 列表查询

5.3.4 IDS
特点:
对攻击行为具有高精度的检测能力
对网络流量非常敏感
识别精度高
IDS 告警分析
通过页面告警信息和提取的原始报文，进行研判分析(查看请求方法，请求体，源目.IP)

5.3.5 产品联动

WAF 联动

TAR 联动

TAR 发现安全攻击通过 API 接口下发封堵策略至 WAF 设备进行源 IP 封堵

全流联动

联动 NFT 取证，还原攻击过程

蜜罐联动

WAF 将攻击流量引流至蜜罐产品进行攻击捕获及反制

威胁情报联动

挖掘攻击者信息

IPS 产品联动

场景：通过 restful 接收下发给 IPS 的阻断策略，可以与 SOC、TAR、IDS 联动实现自动阻断