0day漏洞防护

伪装 、异构、阻断、拦截、诱捕、排查 6步法

1、伪装关键应用指纹 伪装常用中间件、更改http协议header头的server字段。可将linux改为IIS6.0。修改中间件配置文件，将移动通讯app的web服务页面配置成“错误”页面返回信息。修改网关系统配置指纹，将邮件系统指纹改为“Moresec HoneyPot”，转移攻击者注意力。

2、异构边界防护设备 （增加入侵难度和成本） vpn和防火墙采用异构方式部署，同时在内外层vpn系统网络区域间部署大量蜜罐。

3、严控出网访问 （有来无回） 攻击者需要受害主机出网访问的权限，采用配置防火墙双向白名单，阻断协议包括tcp 、udp、 icmp 、dns等，达到攻击无法完成的效果。

4、强化主机安全防护 部分0day利用成功后需要主机读写文件权限，部署终端防护系统，一是监控非白名单地址的运维操作和敏感操作命令，及时发现异常命令执行行为，包括攻击者常用的whoami 、id等。二是监控服务器敏感配置文件的读取，例如passwd、shadow、*.conf 文件。三是进制web目录写入脚本文件，防止webshell后门落地执行。

5、布置内网诱捕陷阱 一是边界区域部署办公系统蜜罐。二是在核心计算区域布置核心系统和集权系统蜜罐。三是将真实系统的非业务端口访问流量转发至蜜罐，第一时间发现内网扫描行为。

6、紧盯零日漏洞利用痕迹 一是加强敏感文件和目录监控。主机层面，流量层面、加强敏感目录读取排查，和返回包的监控。二是加强敏感命令执行监控。主机层面通过入侵检测系统替换操作者系统bash程序，形成命令执行钩子，监控敏感命令执行操作。流量层面，利用流量监测设备匹配敏感命令执行结果。

总结实战经验发现，不管什么0day漏洞，最终都需要在内网主机执行命令，主机是防护零日漏洞攻击最后也是最关键的一道关卡。

制定了以主机异常命令执行为核心，以识别网络及应用层异常行为、收敛攻击面、制定快速攻击定位及处置流程为辅助的0day漏洞防护战术。

在全网生产主机部署入侵检测系统hids，检测反弹shell等关键攻击行为。由于运维人员也会执行bash、nc等指令，为避免误报，递归分析shell日志每条命令的父进程，如果发现是web类进程调用shell则出发告警（如父进程是java、httpd 子进程是sh、python）。告警配置短信实时提醒。

部署高交互、高仿真蜜罐，将vpn、oa系统做蜜罐备份，攻防期间替换掉真实业务域名，混淆攻击者，捕获零日漏洞。同时将下载页面中vpn、oa客户端替换为cs免杀木马，在云服务器部署通过cna脚本进行上线微信提醒，一旦上线即可第一时间反制溯源。

出网管控。最小化授权，梳理资产，绘制攻击路径。

0day攻击应急处置流程

0信任网络：

默认不信任办公网、生产网所有网络流量，基于身份属性、设备属性、设备状态、权限关系并结合密码技术实现细粒度可信网络访问度量及管控。解决了it无边界化趋势下带来的安全问题，相对传统边界模型信任但验证不同，零信任始终保持从不信任，始终验证。零信任关注的主体是数据及应用。零信任网络解决网络边界被突破后对数据及应用的过度访问带来的数据窃取，服务器沦陷等安全问题。

防护对象，改变传统安全架构中以网络为中心的防护，改为以数据为中心的安全防护，关注应用和资源。防护基础，改变传统基于”边界“的防护，改为“无边界”防护，默认不信任，做到最小权限防护。防护理念，改变传统一次认真的静态策略，改为持续评估，动态访问控制。

连环陷阱的apt攻击捕获战法

基于主动防御理念，利用 动态伪装和反向水坑，对抗0day高级攻击者。该技战法以守为攻，出奇制胜，不仅捕获攻击行为，利用浏览器漏洞成功实施反制，获得了攻击者真实身份信息。

1、投递污染信息 对数据库配置、缓存配置、交互服务器配置以及令牌加密因子，写入污染信息，指向蜜罐或诱捕探针。在linux系统中主要针对history、shadow、config、ssh等核心配置文件进行伪造。尤其重视history、结合运维习惯、对其周期性的写入污染信息，能够极大几率迷惑攻击者。

2、配置虚拟进程 完成本机的诱捕陷阱后，需要对虚拟机周围形成联动的诱捕体系，以防止攻击者绕过本机陷阱，直接对网络可达的其他主机进行渗透。可通过配置虚拟进程，模仿真实的高危服务，与真实业务共同对外发布。选定具有为授权访问漏洞的数据库服务作为陷阱模板。为保证拟真性，需详细分析每个应用系统真实业务模式，针对性的部署redis、zookeeper、es、mongodb等虚拟进程。

Rinetd端口转发工具进行端口转发。对于高并发的网站类应用，mysql数据库中部署redis虚拟进程，对于消息类应用，在kafka消息队列所在虚拟机中部署zookeeper虚拟进程，

3、构造反向水坑 当捕获攻击者上传的webshell后，防守方可在其中插入js代码（探针），攻击者再次访问后会返回其操作系统和浏览器资产信息。若出现两个不同版本资产信息，则说明攻击者使用虚拟机进行攻击，继续在之前的js代码基础上插入Canvas代码（探针），获取攻击者计算机硬件信息。如cpu、显卡、电池、屏幕尺寸等。通过返回数据明确攻击者所使用的的操作系统和浏览器后，充填相关资产的漏洞验证数据，探测是否存在可利用漏洞。再确认漏洞存在后，通过该漏洞投递免杀cs木马并进行释放。溯源攻击者身份。

WebShell 跟踪技术较多本次是通过 js 脚本远程获取黑客（攻击者）基本信息，在定位到 WebShell 后，打开 WebShell 源代码加入写好的 js 脚本，为确保脚本是否有效需要是自己先测试一下，看看是否可以获取浏览者信息，确认无误根据之前记录的 WebShell 文件属性，恢复文件修改时间为写入时间！注：具体 js 脚本可根据自己的需求编写，或者根据网上的开源脚本自行扩展，开源工具如 BeeF 、或其他开源工具等！

零信任架构

可实现几个关键目标：1、vpn始终在线 2、安全防御足够，有效切断攻击方的攻击链条 3、运行过程灵活自动，避免运维人力大量投入。

1.践行零信任架构体系，建立员工身份安全基准 所有员工安装安全app，绑定设备指纹和手机号，开启扫码、动态口令等强因素认证功能，系统登录都必须使用该app完成认证。

2.让攻击者看不见 第一层防御 边界防火墙设置策略，使vpn地址不对互联网开放，攻击者不能直接探测发现，无法正常攻击。员工需在app上提交合法pc的ip地址，改地址经过acl策略管理系统的自动处理，将会加入到边界防火墙的白名单列表，然后可正常发起访问。同时，在网上搭建一套高仿的vpn蜜罐，迷惑攻击者。

3.让攻击者进不去 第二层防御 对vpn加固，启用vpn客户端的专线功能，使用户电脑在建立vpn隧道的同时自动断开与其他互联网地址的通信。

4.让攻击者摸不到 第三层防御 限制从vpn设备到内网方向的网络访问权限，默认只能访问零信任安全网关。在零信任安全网关上设置策略，使所有流量进行持续认证和权限校验，

5.使用高密度异构蜜罐 蜜网：由一个蜜网管理中心进行统一调度，下设互联网、dmz、内网数据中心、海外网络汇接点和信息系统内部共五道蜜罐防线组成的蜜网。管理中心通过syslog统一收集蜜罐告警，基于ssh实现控制指令下达，综合实现蜜罐资源调度、访问控制、日志分析、态势展示等功能。

ip归属地筛选方案

将已知的安全ip进行去除，利用开源ip地址库对剩余ip进行归属地标注，筛选其中各公有云厂商ip，公有云ip由于其易获取，方便假设攻击工具等特点，通常被攻击者使用。

1、ip归属地过滤筛选 将第一周的来访ip进行提取，去重，排除白名单，将剩余ip进行归属地识别。提取到带有公网ip可以作为攻击机、跳板机以及远程控制服务器的云主机ip地址，将这些云主机ip进行单独提取。

2、基于时间维度分析 将演练前3个月至半年的访问数据进行提取，与演练开始后的数据进行对比，通过对比有效发现新增ip情况，新增部分往往包含演习攻击者ip。

3、基于地域维度分析 由于多地部署方式，不同数据中心所处网络位置不同，如果多个数据中心同时增加了新增访问ip，则该ip为对制定单位的攻击ip。

4、基于行为维度分析 借助威胁情报检查流量中包含的挖矿、DDOS脚本排除代理、爬虫、黑产攻击ip。

基于威胁情报构筑动态防御体系

日常威胁情报收集、处理与建模主要采取以下几方面策略：

1、将安全设备收集到的报警按照攻击行为分为端口扫描类、服务探测类、尝试攻击类、恶意代码类，4类。绝大部分攻击都是按照这四个步骤开展，再将监测到的攻击行为按攻击阶段进行分类。

2、基于对攻击行为事件序列的深入分析，为预测攻击和溯源提供依据，使用攻击行为的owasp分类和cve编号以及木马的执行顺序，为检测到的攻击行为进行编码，最终以字符串序列的形式，对每个攻击行为序列进行标识，将该序列在威胁情报库中应用威胁相似度计算模型，计算情报库中相似度高的攻击序列。

3、具体分析攻击行为的过程中，攻击者为了躲避检测，一般会采取低速、随机的扫描方式，结合数理统计等方法，反推出攻击者的攻击间隔分布，从而发现潜在攻击特性。

4、经汇总、筛选、清理，以攻击行为的响应时间、攻击间隔起止时间、顺序化的端口扫描列表、服务探测顺序、漏洞扫描顺序、恶意代码动作列表等维度，构建攻击特征数据库，形成威胁情报库，安全监测处置一体化目标。

专有情报生产

1、利用监测系统发现大量水利网内的攻击行为、漏洞情况、恶意文件、异常外联等告警数据，研判后发送至情报中心

2、情报中心将告警时间、告警原因、告警ip、资产ip等信息进行实时标准化和范式化，自动补充时间、来源等信息后，根据告警级别类型配置权重分数和生产情报的及格分数

3、完成情报制作后，通过restful api写入情报中心

4、对各单位提交统一格式的防守报告，情报中心利用基于深度学习的文本识别技术，自动提取出告警时间、告警原因、告警ip、资产ip等数据，之后进行同样处理完成制作。

黑客指纹收集

依托蜜罐系统生成黑客指纹库，指纹库融合了系统、设备、html5 webGL、HTML5 Canvas、第三方网站ID指纹等。

当攻击者访问蜜罐系统中的诱饵网页时，该页面会在黑客的机器上种植僵尸cookie。僵尸cookie遍布多处，难以删除，收集并形成独一无二的指纹信息，从而为黑客的捕获提供情报信息和溯源能力。

黑客在发起攻击时，若其已经登陆过百度、新浪、优酷等第三方网站，蜜罐系统能够捕获其登录id。二是通过分析黑客操作系统语言、时区、ip归属地等信息，判断是否为境外攻击者。

逐步发布仿真系统，结合最新的0day。推出一套全英文的业务仿真系统，在此站加载了反制诱饵。

暴力破解过程中使用的用户名、密码，补充至密码字典，用于日常内部弱密码检查，若用户名是企业名，需对该用户发出风险提醒。通过证书、代码标识等识别攻击者攻击工具，进行攻击者同源性分析。攻击成功后的外联地址，用于监测内部主机是否沦陷。下载的木马哈希，通过主机agent定时扫描服务器进程和启动项对应的文件哈希，判断是否有其他主机已经被控。