2022北京网络安全大会

2022 BEIJING CYBER SECURITY CONFERENCE

全球网络安全 倾听北京声音

攻防实战下的深度威胁监测

安芯网盾 李正

攻击方手法变化 2019~2021

信息收集更为多元

信息收集粒度更细范围更广，不仅收集单位组织架构、信息资产、技术架构、防护措施等信息，也收集单位个人电话、邮箱、社交网络、社会关系等信息。

攻击方式越发隐蔽

大量采用更为先进的攻击手段，逃避安全检测，如采用流量加密、代码混淆、无文件攻击、内存马攻击等方式来隐藏自身，以提升攻击成功率。

落脚位置趋向角落

优先选择防护力度相对薄弱甚至是被忽视的边缘资产设备作为攻击落脚点，或是直接攻击安全设备，以规避核心资产在蓝队严防死守下难以直接被攻破的难题。

社工攻击广泛应用

充分利用人性弱点，精心构造社工场景，以实现载荷投放，如采用钓鱼邮件、伪装造访、伪装设备检修、投放恶意存储介质诱饵或开放恶意网络等。

红队重要手段

1

钓鱼

邮件钓鱼

即时通讯

社交网站

WIFI

客服钓鱼

……

2

弱口令

操作系统

中间件

数据库

WEB管理后台

安全设备

……

3

内存破坏攻击

缓冲区溢出

堆喷射

ROP攻击

栈翻转

执行shellcode

……

4

无文件攻击

脚本攻击

漏洞利用攻击

凭据盗用

系统工具利用

注册表驻留

……

5

内存马

Servlet-api型注入

字节码增强型注入

远程执行漏洞利用

文件上传

流量加密

……

红队所用手段主要技术特点

绕过性好

利用混淆、加密、加壳、无文件等方式执行恶意命令，有效逃避常规安全手段检测。

成功率高

红方队伍往往利用预先准备的0day漏洞来发起攻击，使攻击所用的手段隐蔽性特点更加突出，因此更加容易突破用户安全防线。

溯源难度大

很多攻击往往采用无文件形式，利用内存漏洞，直接远程加载恶意代码，一旦机器重启，则证据直接消亡，给溯源带来很大困难。

隐蔽性强

通过修改开机启动项、创建新账户、创建自启动服务后门、创建系统计划任务后门、动态库劫持等方式植入持久化后门。

防守方变化 2019~2021

构建主动防御体系

完善安全技术体系建设，细化访问控制粒度，开展脆弱性检查和修复；

采用蜜罐系统，结合人工布设诱饵等方式，形成攻击溯源和反制能力。

提升安全管理水平

提升安全运维人员攻防对抗能力，提升网络安全事件应急处置水平；

组织开展安全宣贯教育，树立全员网络安全意识，重点形成社工防范能力。

优化资产盘点管理

全面梳理单位信息资产，确保全部资产落实到具体责任人；

重点检查高价值数据管理情况，确保高价值数据可管可控，降低数据泄露风险。

红队武器top之无文件攻击

无文件 非恶意软件 潜伏周期长 传播快 零足迹 危害大

❶ 目标攻击

选取攻击目标
找准上传点

❷ 绕过检测

符合上传文件要求
AV、HIDS记录未报警

❸ 内存执行

Powershell/WMI
内存加载执行

❹ 远程控制

修改执行权限
尝试外联

❺ 重启销毁

检测重启生成文件
服务加载自动销毁

❻ 反取证

难以获取执行文件
网络层取证大海捞针

无文件勒索

- ProLock
- WannaRen 勒索软件
- FTCode 勒索软件
- Sorebrect

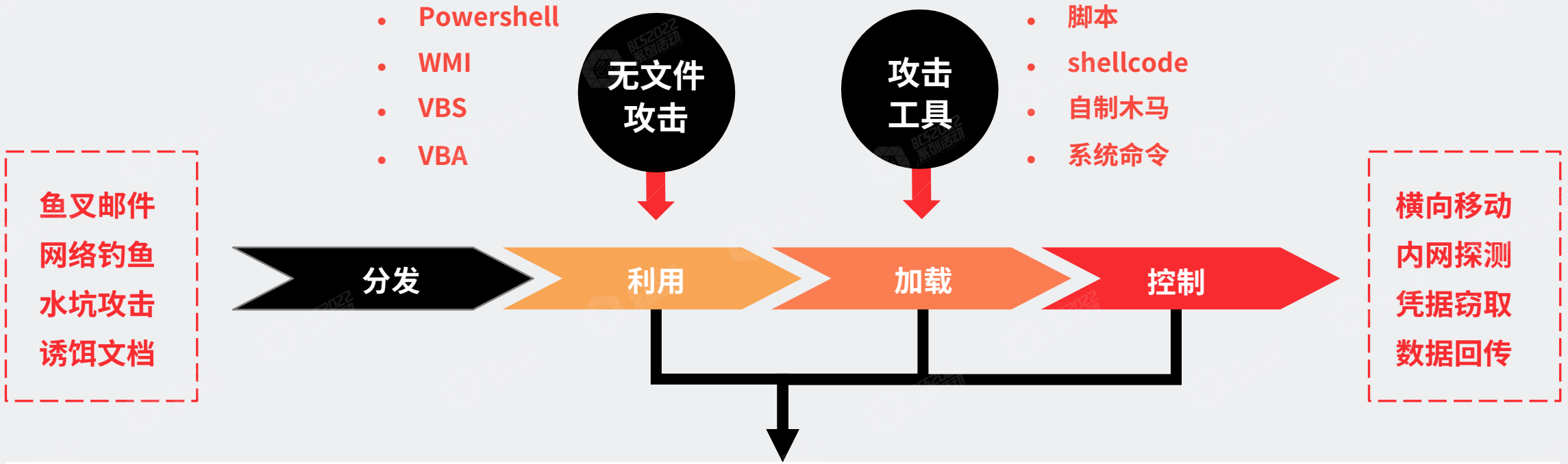
无文件挖矿

- PowerGhost 最新样本
- 永恒之黑木马
- Coinminer
- PowershellMiner

无文件窃取

美国大选无文件攻击

安芯网盾无文件攻击防护



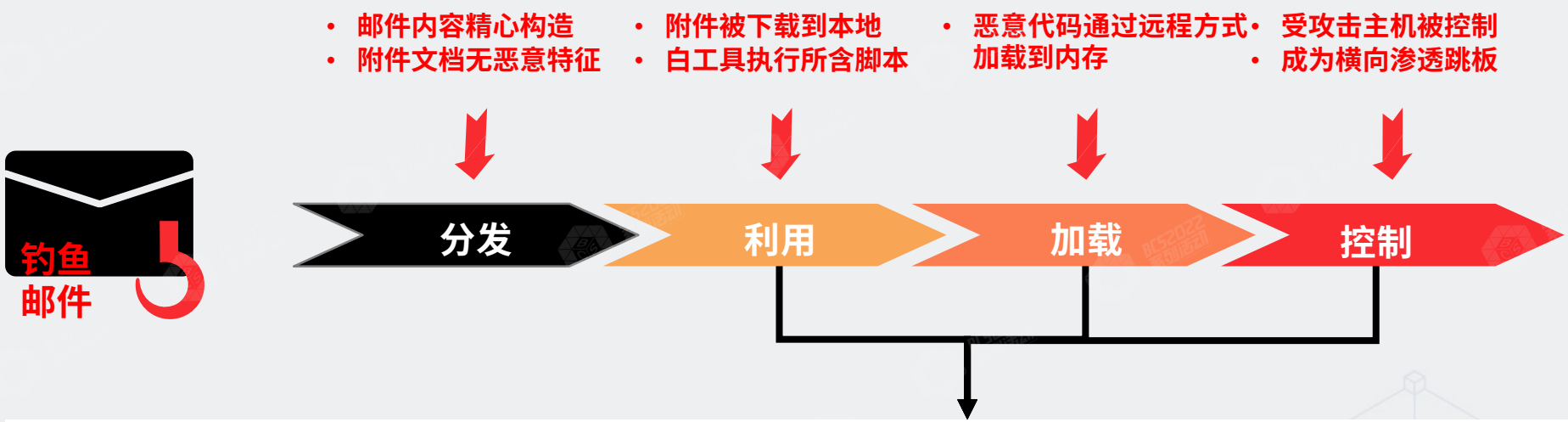
行为分析引擎
关联分析引擎

- 加载敏感子进程
- 启用灰色工具执行敏感行为

- 敏感OS API调用
- 内存异常行为

攻防演练案例一：无文件钓鱼

用户收到钓鱼邮件，邮件名称为：xxxx 公司内部xxx决定初稿.docx.；打开邮件附件后利用系统工具远程下载含有恶意载荷的.jpg，该图片的恶意载荷被释放到内存中，执行远控。
脚本执行HTTP（GET）请求：c:\windows\system32\windowspowershell\v1.0\powershell.exe,url:http://xxx/i.php?i=1.jpg



行为分析引擎
关联分析引擎

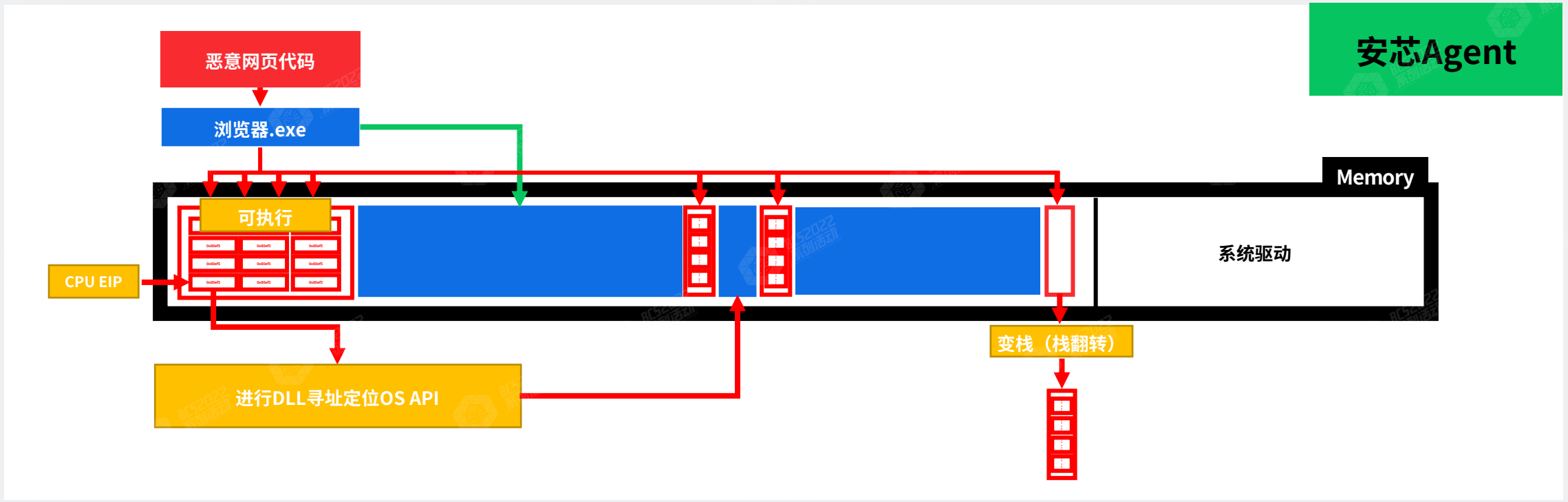
加载敏感子进程	启用灰色工具执行敏感行为	敏感OS API调用	内存异常行为

红队武器top之内存破坏攻击

内存破坏型漏洞产生于非预期的内存越界访问，攻击者利用零日漏洞或未修复漏洞进行内存篡改以避开传统安全解决方案，并在受害主机上执行恶意代码。

- ROP攻击
- 堆喷射
- 反射式注入
- 缓冲区溢出
- 栈缓冲区溢出
- 格式串问题
- 远线程注入
- 引擎攻击
- 释放后重利用
- 内存代码注入
- 布局Shellcode
- 堆缓冲区溢出
- 远程加载模块
- 二次释放
- ……

安芯网盾内存破坏攻击防护



内存写入监控

Shellcode布局

内存执行监控

变更读写执行权限

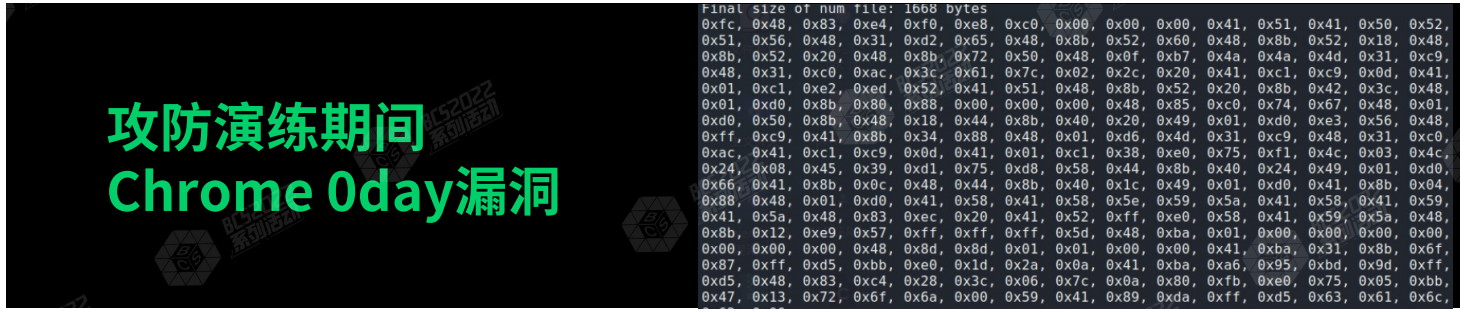
内存读取监控

OS API异常遍历

OS API调用监控

易被利用的API监测

攻防演练案例二：
内存攻击-chrome 0day漏洞利用



2021年4月11日12点57分

发现一台终端执行shellcode攻击，进一步发现由PC端微信执行的操作

分析:

受到影响的版本，Google Chrome <= 90.0.4430.72

进一步分析:

基于Chromium内核的Microsoft Edge <= 89.0.774.77

防护结果:

安芯支持实时检测及拦截

防护结果:

客户第一时间找到“CVE-2021-21220”和“CVE-2021-21224”漏洞进行测试，发现安芯网盾“内存保护系统”可准确识别并拦截

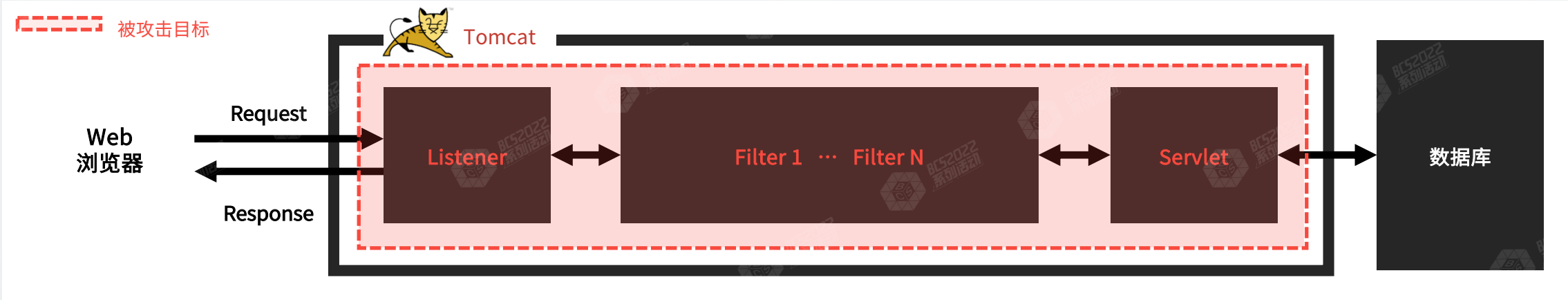
检测原理

- CVE2021-21220和CVE2021-21224漏洞
- 微信浏览器关闭sand-box
- 利用内存下溢执行ShellCode
- 针对内存破坏型漏洞，安芯对内存读写等操作进行行为监测，发现攻击

实现效果

- 在未升级安芯神甲的情况下通过攻击样本复现能够100%检测
- 可针对该Shellcode进行拦截
- 提供Shellcode溯源

红队武器top之内存马攻击



Tomcat对于这三种组件的加载顺序依次为Listener、Filter、Servlet。

Listener攻击手段

Listener是Web服务器中监听事件的组件,可以通过截获组件间的消息进行攻击。

选取ServletRequestListener进而拿到ServletRequestEvent，通过其中的getServletRequest()函数就可以拿到本次请求的request对象，从而加入恶意代码 。

Filter攻击手段

Filter是Web应用的过滤器，它管理Web访问内部资源的权限。

伪造恶意Filter并通过FilterMaping与特定URL绑定，将创建的Filter移到过滤链的第一个，此后只要访问该URL就会触发Filter中的代码，可灵活向其中添加想要执行的代码。

Servlet攻击手段

Servlet是解析特定URL的组件。

同Filter类似，Servlet也可通过ServletMapping与特定的URL绑定，首先伪造Servlet并用Wrapper对其进行封装添加到StandardContext的children中。

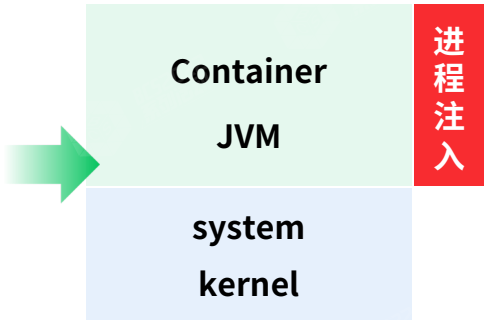
其他Web容器也有类似Listener、Filter、Servlet的解析机制，攻击手段大体相同。

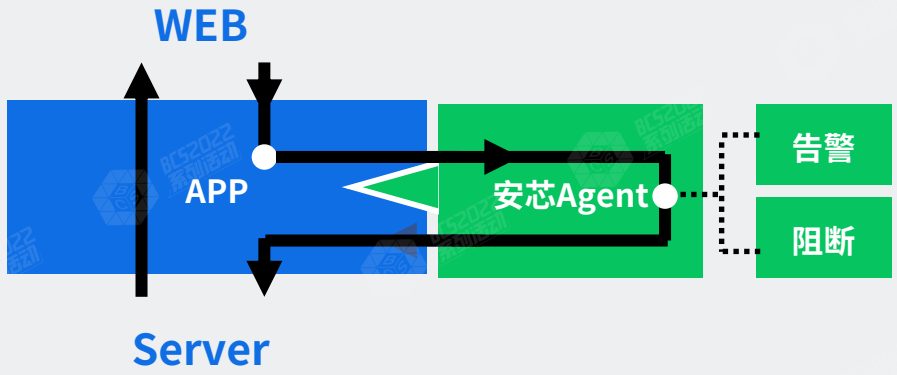
安芯网盾内存马防护

通过RASP运行时分析可检测变形攻击

通过API hook或JAVA Agent实现异常行为监控

通过AgentMain方式减少业务侵入度





类型	描述	防护原理	能力模块
Java内存马	Java内存马基于Java应用服务器的技术规范（例如：Servlet规范），利用服务器功能接口在JVM进程内驻留、运行，接收攻击者从外部发起的恶意请求，获取内部数据返回	通过JVM进程自省，对敏感Java应用服务器接口调用行为监控，收集潜在的内存马载体进程的操作，关联分析敏感行为识别此类攻击	行为分析 动态枚举
PHP内存马	PHP内存马利用脚本解析执行特性，调用PHP运行时文件访问接口动态加载恶意代码，之后调用PHP运行时外部命令执行接口执行恶意代码	通过对PHP进程执行行为进行监控，关联分析敏感行为以识别此类攻击	行为分析

安芯网盾内存马防护

轻侵入模式无需重启

和传统RASP技术相比，安芯采用轻侵入模式，业务无需重启，能够监测已加载的内存马。

行为分析引擎

安芯采用行为分析引擎，对jvm内运转的相关程序执行动作均会进行标记，能够有效应对未知威胁。

不占用业务进程空间

传统RASP技术占用业务应用的jvm内存，存在影响业务系统运行的风险，安芯只在jvm中对程序执行动作进行标记，分析进程是在jvm之外的单独进程中分析，不占用正常业务进程的jvm空间。

攻防演练案例三：内存马

4	内存Webshell	java	2021-04-22 02:26:40	高危	发现进程：[redacted]，仅上报
4	内存Webshell	java	2021-04-22 02:26:33	高危	发现进程：[redacted]，仅上报
3	内存Webshell	java	2021-04-22 02:26:24	高危	发现进程：[redacted]，仅上报
3	内存Webshell	java	2021-04-22 02:25:00	高危	发现进程：[redacted]，仅上报
3	内存Webshell	java	2021-04-22 02:23:15	高危	发现进程：[redacted]，仅上报
	内存Webshell	java	2021-04-22 02:22:54	高危	发现进程：[redacted]，仅上报
2	内存Webshell	java	2021-04-22 02:20:12	高危	发现进程：[redacted]，仅上报

检测原理

- 发现java加载异常filter
- 持续发现bin bash异常操作

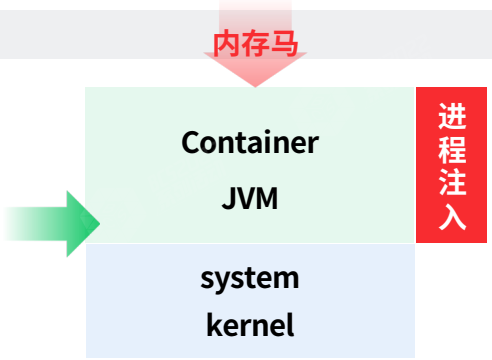
实现效果

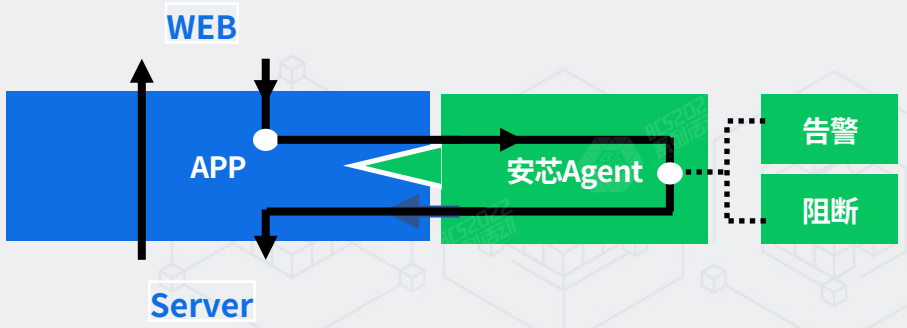
- EDR、WAF均未发现攻击
- 样本文件难以取证，通过内存执行日志溯源攻击行为
- 该设备短时间内不能断网，经确认后直接开启拦截模式
- 另一台主机发现攻击样本名称由ltcp改为Update，攻击行为链雷同，直接阻断

通过RASP运行时分析可检测变形攻击

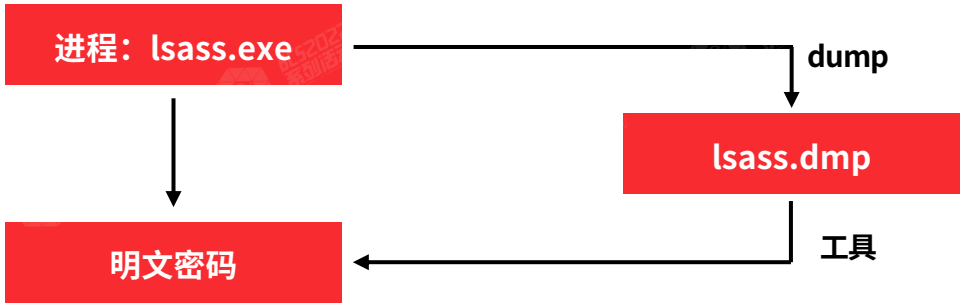
通过API hook或JAVA Agent实现异常行为监控

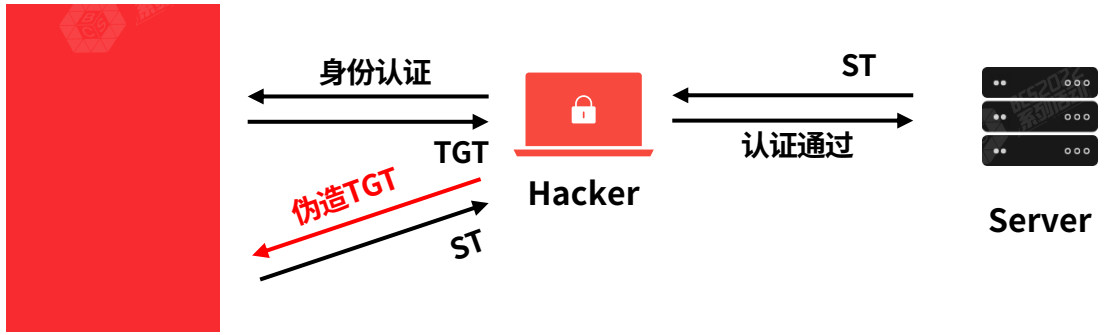
通过AgentMain方式减少业务侵入度





红队武器top之域控攻击





攻击类型

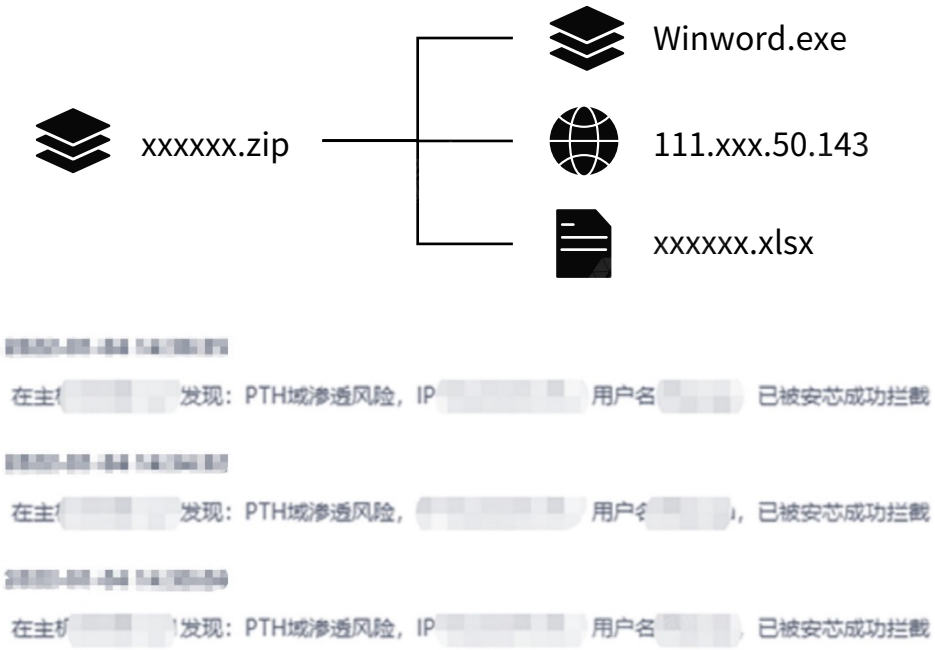
- NetLogon特权提升漏洞
- PTH（Pass-The-Hash）攻击
- Lsass进程获取明文密码
- 黄金票据
- 白银票据

安芯网盾域控攻击防护

攻击类型	说明	能力模块
NetLogon特权提升漏洞	部分用户不能及时升级补丁； 利用方式简单，几乎所有的windows服务器操作系统都受到影响	漏洞防御
PTH（Pass-The-Hash）攻击	攻击者不需要获取明文密码，只需要获得域管理员密码的NTLM哈希值，就可以发起攻击	威胁防御
Lsass进程获取明文密码	通过读取lsass.exe进程的内存就有机会获得域控管理员的密码	内存数据保护
黄金票据攻击	由于与正常的请求混淆，具有很高的隐秘性，检测难度高	内存数据保护 威胁防御
白银票据攻击	由于与正常的请求混淆，具有很高的隐秘性，检测难度高	内存数据保护 威胁防御

攻防演练案例四：域控防护

21 年 11 月 6 日，用户现场的安芯神甲平台发现多起 PTH 攻击风险事件，和客户沟通得知涉及到AD和 exchange 服务器。其中域控服务器受到攻击的攻击源 IP 为内网 IP，涉事IP 负责人近期点击过匿名邮件，随即对邮件进行分析，确认该邮件为钓鱼邮件。



检测原理

- 钓鱼邮件被打开
- 恶意附件从本地电子邮件客户端获取凭据、释放二进制执行文件，并外联（IP：111.xxx.50.143）
- 利用NTLM认证本身缺陷进行攻击
- 针对域控本身缺陷，安芯产品能够检测不合规的域控认证行为，并进行告警和阻断

实现效果

- 传统域控防御方案无法实时拦截
- 解决域控环境中内存数据不可见问题
- 在威胁造成损坏之前进行有效告警和阻断

红队武器top之工具魔改

Cobalt Strike　Mimikatz　Psexec　冰蝎/哥斯拉/蚁剑　MSF

攻防演练场景安芯产品能力

高级威胁防护

内存保护系统应用多项创新性技术，可以对一些新的攻击手段、病毒变种进行有效检测与防护。

漏洞防护

存保护系统建立一种即使在没有补丁情况下，依旧能够对漏洞利用攻击进行检测的机制。

无文件攻击防护

无文件攻击盛行，内存保护可以对灰色工具型、潜伏型、脚本型等无文件攻击进行检测与防护。

内存攻击防护

内存保护系统专注于解决内存安全相关问题，基于底层核心技术可有效发现内存威胁，例如ROP、傀儡进程等。

内存Webshell防护

内存Webshell又称内存马，内存保护系统可有效防护JAVA、PHP等内存马攻击，从而保障业务系统安全。

域控场景防护

域控是一个典型集权系统，其容易成为被攻击对象，内存保护为其提供一套完整的防护方案。

风险发现

内存保护可对进程风险、内核风险、账号风险等进行检测，发现潜在风险防止遭受进一步攻击。

威胁溯源

内存保护系统可对高级威胁攻击链进行全方位溯源，包括内存行为、系统行为、应用行为等。

攻防演练场景服务能力

风险评估

从风险管理的角度，为客户分析信息系统中存在的安全威胁和漏洞，并给出修复建议。

专家咨询

攻防演练前夕，为客户提供专业的咨询服务，形成预防阶段的具体网络安全检查和完善思路。

战前演练

攻防演练前夕，模拟攻防对抗，真实检验用户安全防护能力，发现防护弱点，为网络安全能力强化提供依据。

安全驻场

对抗阶段，指派专业的安全服务人员，为用户提供安全事件监控、分析、处置及溯源等服务。

应急响应

攻防演练阶段，以远程或现场形式为用户提供网络安全突发事件应急处置服务，提升用户应急响应能力。

即刻扫码申请，立享王牌服务

THANKS