



网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

主动防御在威胁狩猎中实战应用



神州网云（北京）信息技术有限公司
宋超

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖战

目录

- 01 被动防御目前面临的瓶颈
- 02 网络杀伤链能否解决所有问题
- 03 构建战术型态势感知主动防御
- 04 主动防御&被动防御总体构架
- 05 案例分析

01

被动防御目前面临的瓶颈

01 被动防御面前的瓶颈

影子经纪人

是一个比较神秘的黑客组织。2016年，成功黑掉“方程式小组”，并使“方程式小组”的黑客工具大量泄漏。2017年5月影子经纪人称将放出更多美国国安局病毒代码。

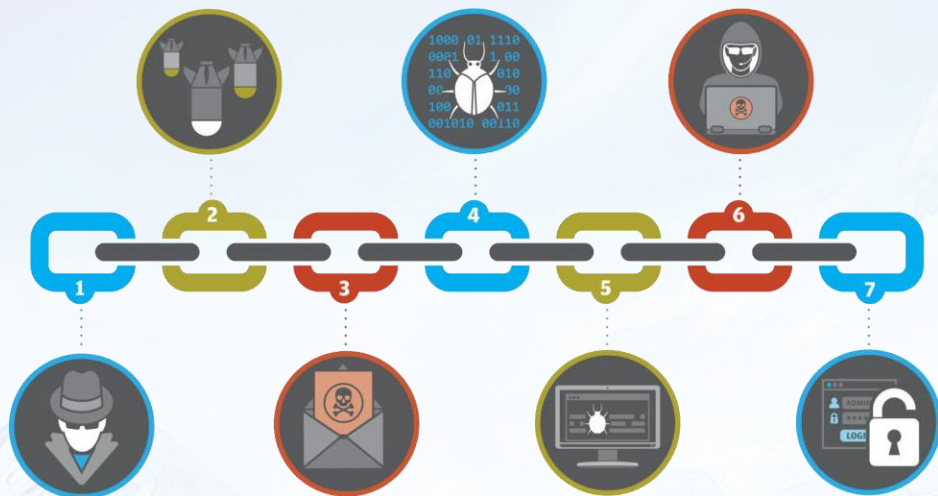
目前能否做到：知己知彼，百战不殆？

随着网络大杀器的公开，让我们看到目前的对手比以往任何时候更有能力，使用的武器更先进，被动的防御战术已不能全面监测追踪这些攻击者。



02 网络杀伤链能否解决所有问题

02网络杀伤链能否解决所有问题



攻击者获得的信息越少，其他人就越不可能使用这些信息来完成接下来的攻击过程。该理念最初是由洛克希德·马丁公司提出的，描述了有针对性的攻击阶段。同样，防御者也可以利用它们来保护组织的网络。

主要分为7个阶段：侦察跟踪、武器构建、载荷投递、漏洞利用、安装植入、命令控制、达成目标。

03 构建战术型态势感知主动防御

战术型态势感知指控积极防御 协同响应猎杀威胁运行实战化

铁流鏖战

第六届安天网络安全冬训营

主+动防御相结合为威胁狩猎提供服务支撑

探测识别 →

IP地址定位 →

拓扑探测 →

资源管理 →

数据服务 →

可视化服务 →

管理控制 →

网络拓扑探测

脆弱性探测

海量信息存储

基础资产信息库构建

木马及漏洞验证引擎构建

多维度多场景数据分析模型构建

重点分析模块构建

态势感知、协同响应预警

04 主动防御&被动防御总体架构

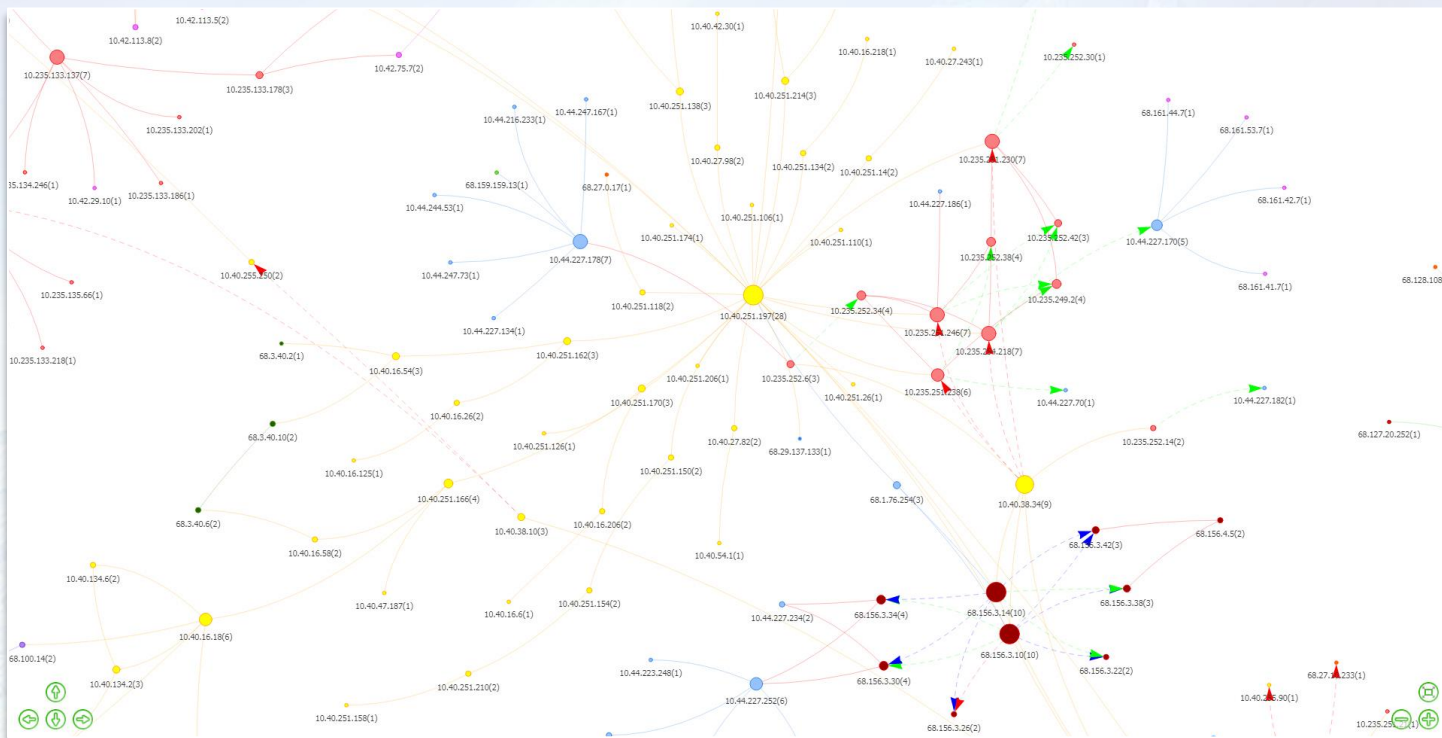
04主动防御&被动防御总体架构

通过构建网络态势底图协同积极防御，快速发现我国网络空间基础设施中的异常行为或活动，实施前瞻预警。



04主动防御&被动防御总体架构

对指定国家、区域和目标地址空间进行拓扑探测，同时，被探测IP的相邻IP也会被系统自动识别，呈现目标网络的静态和动态近实时物理和逻辑拓扑；能够对目标网络进行拓扑绘制。



05 案例分析

铁流鏖战

第六届安天网络安全冬训营

基于暗网情报识别的深度探测

目前已发现暗网隐藏服务地址总数：68 7312个；历史在线活跃的Web服务共：42 721个；已采集暗网页约6378万个，日增量约26万个页面，抓取文本文档约31.8万个，图片583万。

系统已发现92种语言的暗网网站；其中收录中文隐藏服务641个，内容主要集中在违法交易、政治谣言，色情暴力三个方面；其中英文网站 11816，俄语631，阿拉伯语14，其他语言11171。



华住泄露数据再次暗网“上架” - 安全客,安全资讯平台



2018年9月21日 - 本周三,5亿华住个人信息泄露案犯罪嫌疑人已被抓获,本以为华住数据泄露事件就此告一段落。但就在昨天,白...
<https://www.anquanke.com/post/...> - 百度快照

2018年年底暗网现生存数据年总结:数据泄露,黑客雇佣占主导

3天前 - 标签: it 暗网 互联网 人性 数据 分类: 暗网 摘要:迈克菲发布第三季度分析报告指出,继暗网市场Hansa 和 AlphaBay 被端后,Dream Markets 和 Wall Stree...
blog.sina.com.cn/s/blo... - 百度快照

AcFun泄露数千万条用户数据,网站SHELL和内网权限在暗网售卖



2018年6月13日 - 而在AcFun 发布此次数据泄露公告之前,暗网中也早有人兜售其 Shell 和内网权限,主要卖点就是数据量大以及...
<https://www.linuxidc.com/Linux...> - 百度快照

优酷数亿用户密码数据泄露并暗网销售 附泄露数据查询地址-缙哥哥

2017年4月22日 - 此前有匿名用户在暗网上销售中国视频网站优酷网的数据库,这份数据库总共包含 100,759,591 条用户账户。尚不清楚是否有人支付了约 300 美元的价格购买...
<https://www.dujin.org/71...html> - 百度快照

主动发现防御

我找到了暗网中出售“12306 账号”的卖家

原创：桥的断想 四维创智 1周前



她的主页 她的相册

246 关注 114 粉丝 156 微博

11月26日 21:04 来自 微博电影

最近

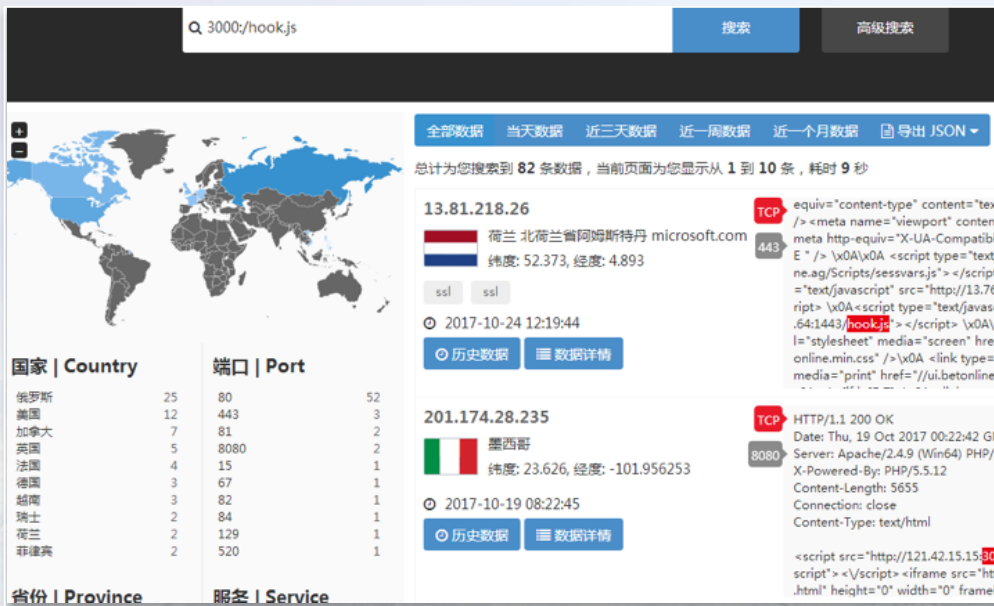
- 2016
- 2017
- 看一看微博

四维创智

追踪溯源到人

BeEF漏洞主动防御监测

BeEF是浏览器攻击框架的简称，是一款专注于浏览器端的渗透测试工具，是目前欧美最流行的web框架攻击平台，通过XSS这个简单的漏洞，BeEF可以通过一段编制好的javascript控制目标主机的浏览器，通过浏览器拿到各种信息并且扫描内网信息，同时能够配合metasploit进一步渗透主机。



Q 3000:/hookjs 搜索 高级搜索

全部数据 当天数据 近三天数据 近一周数据 近一个月数据 导出 JSON

总计为您搜索到 82 条数据, 当前页面为您显示从 1 到 10 条, 耗时 9 秒

13.81.218.26 TCP 443
荷兰 北荷兰省阿姆斯特丹 microsoft.com
纬度: 52.373, 经度: 4.893

2017-10-24 12:19:44
历史数据 数据详情

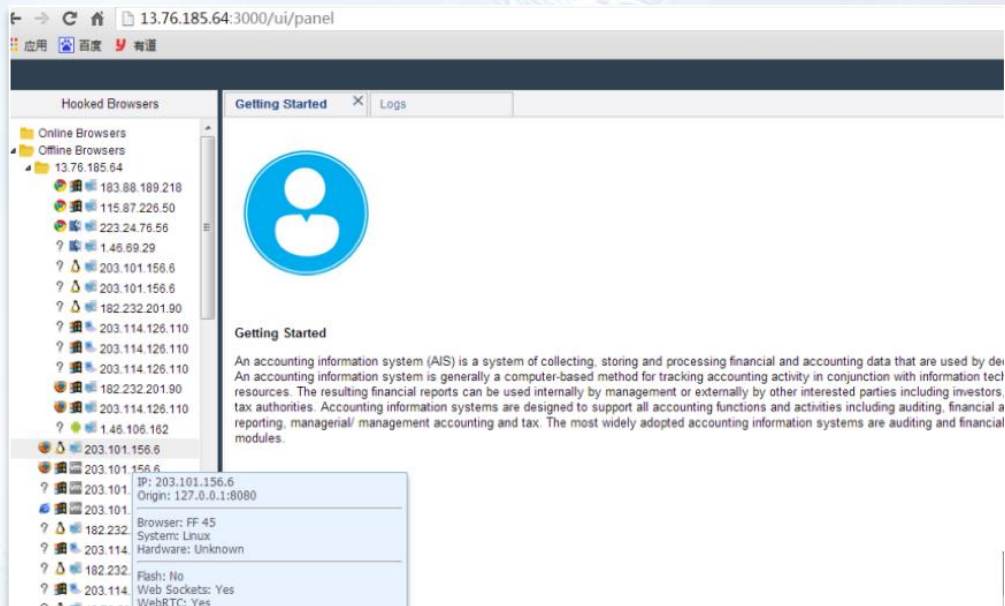
201.174.28.235 TCP 8080
墨西哥
纬度: 23.626, 经度: -101.956253

2017-10-19 08:22:45
历史数据 数据详情

国家 Country	端口 Port
俄罗斯	80 52
美国	12 443 3
加拿大	7 81 2
英国	5 8080 2
法国	4 15 1
德国	3 67 1
越南	3 82 1
瑞士	2 84 1
荷兰	2 129 1
菲律宾	2 520 1

省份 Province	服务 Service
俄罗斯	80 52
美国	12 443 3
加拿大	7 81 2
英国	5 8080 2
法国	4 15 1
德国	3 67 1
越南	3 82 1
瑞士	2 84 1
荷兰	2 129 1
菲律宾	2 520 1

主动发现防御



13.76.185.64:3000/ui/panel

Hooked Browsers

- Online Browsers
- Offline Browsers
- 13.76.185.64
 - 183.88.189.218
 - 115.87.226.50
 - 223.24.76.56
 - 1.46.69.29
 - 203.101.156.6
 - 203.101.156.6
 - 182.232.201.90
 - 203.114.126.110
 - 203.114.126.110
 - 203.114.126.110
 - 182.232.201.90
 - 203.114.126.110
 - 1.46.106.162
 - 203.101.156.6
 - 203.101.156.6
 - 203.101.156.6
 - 203.101.156.6
 - 203.101.156.6
 - 182.232.201.90
 - 203.114.126.110
 - 182.232.201.90
 - 203.114.126.110
 - 182.232.201.90
 - 203.114.126.110

Getting Started

Getting Started

An accounting information system (AIS) is a system of collecting, storing and processing financial and accounting data that are used by de... An accounting information system is generally a computer-based method for tracking accounting activity in conjunction with information tec... resources. The resulting financial reports can be used internally by management or externally by other interested parties including investors, tax authorities. Accounting information systems are designed to support all accounting functions and activities including auditing, financial a... reporting, managerial/ management accounting and tax. The most widely adopted accounting information systems are auditing and financial modules.

IP: 203.101.156.6
Origin: 127.0.0.1:8080
Browser: FF-45
System: Linux
Hardware: Unknown
Flash: No
Web Sockets: Yes
WebRTC: Yes

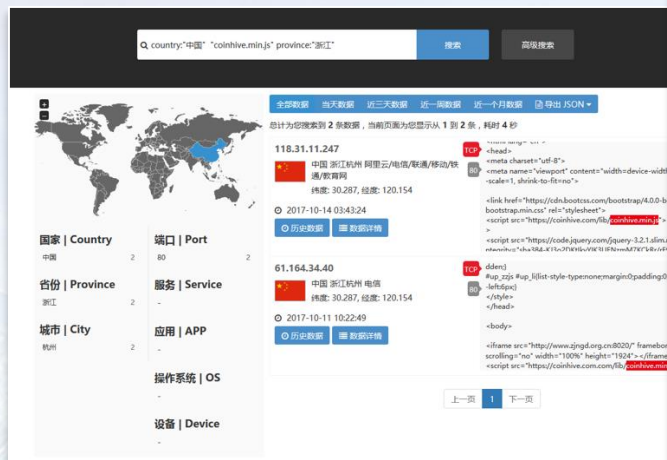
溯源&反制

网页JS挖矿恶意代码

coinhive 通过JS代码在网站上挂挖矿程序介绍:

利用网页内嵌的Javascript程序（一段JS代码），“借用”浏览者的电脑用作挖掘虚拟货币的用途，也就是挖矿。该行为会使在网站的浏览者在浏览网站时，挖矿程序的JS代码就会运行，导致浏览插入挖矿代码网站CPU占用率很高，甚至100%满负荷运行！

05案例分析



主动检测多个目标



定位失陷网站



清理战场修补漏洞



网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

THANKS



扫码关注冬训营动态

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖战