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

铁流鏖戰

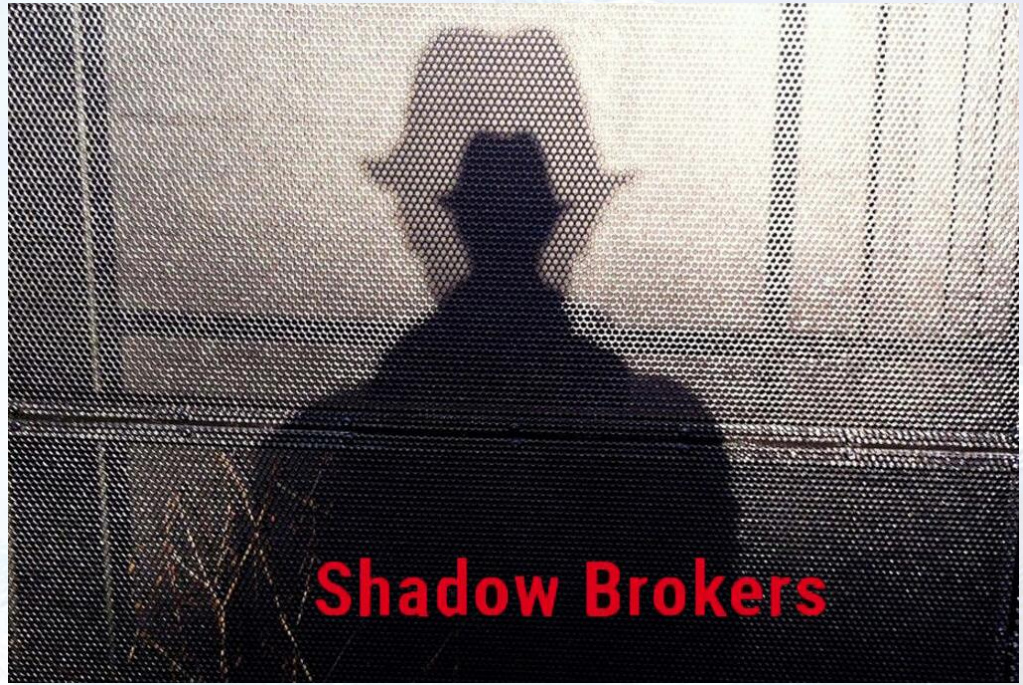
目录

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。

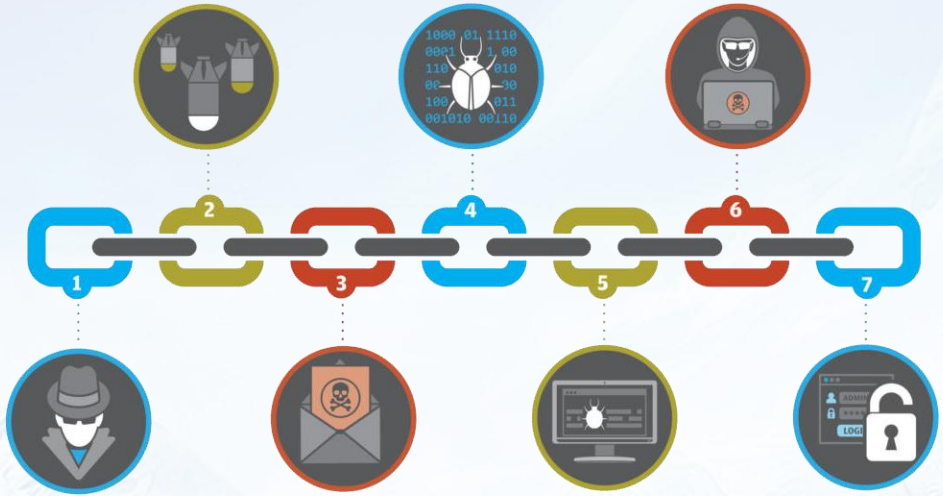


目前能否做到：知己知彼，百战不殆?

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

03构建战术型态势感知主动防御

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

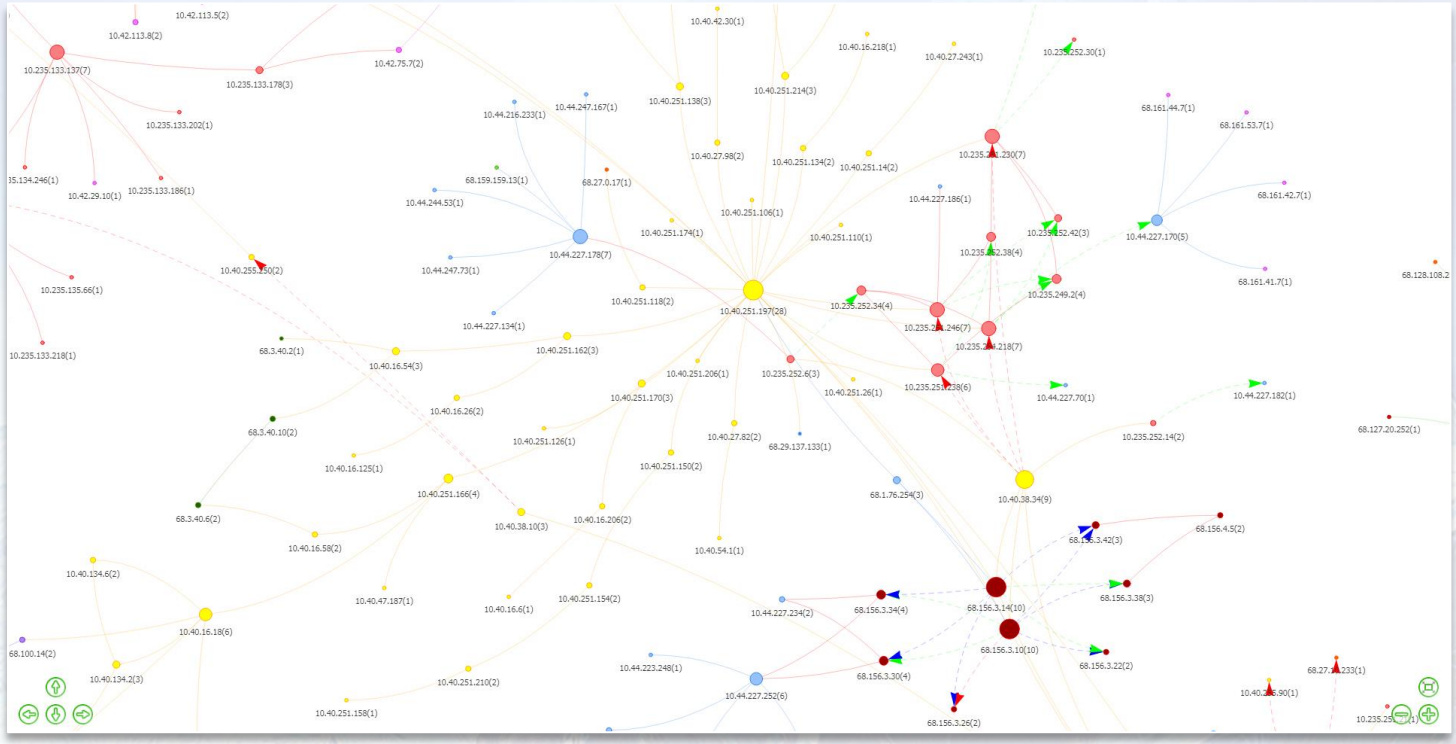
04 主动防御&被动防御总体架构

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

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：687312个；历史在线活跃的Web服务共：42721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。

05案例分析

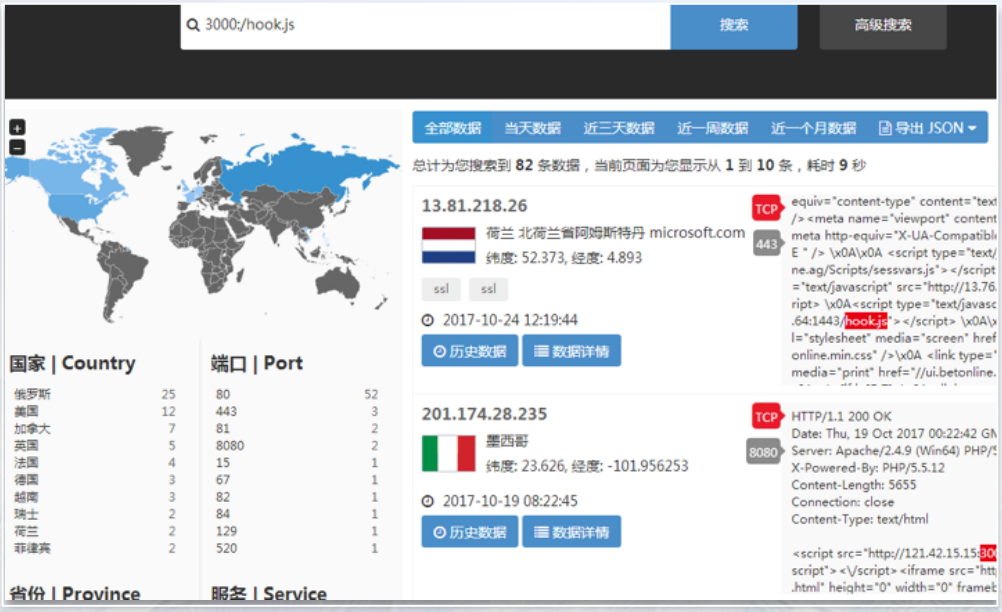
主动发现防御

追踪溯源到人

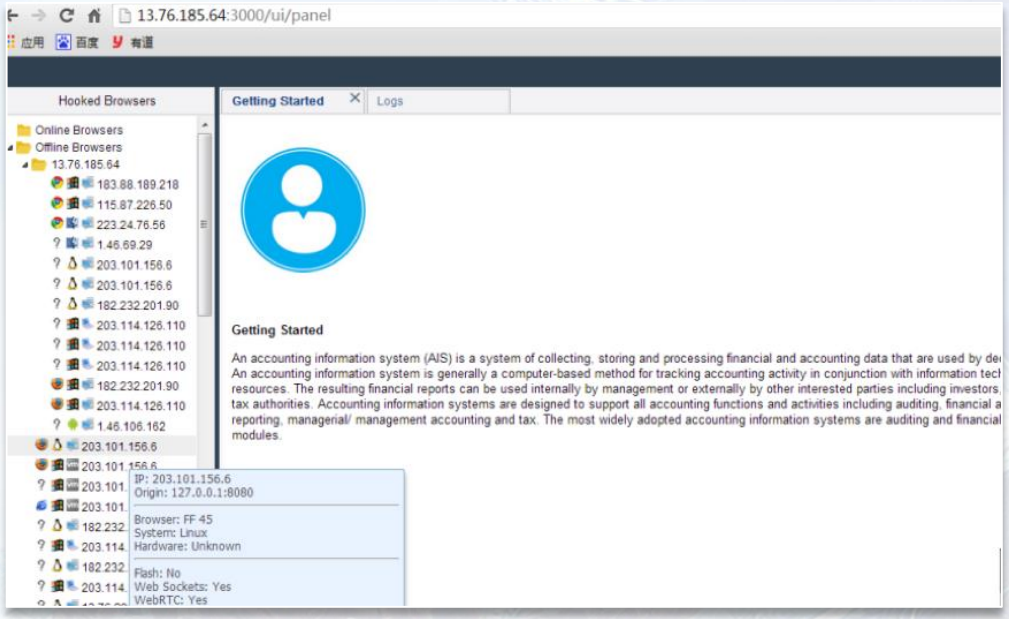
BeEF漏洞主动防御监测

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。

05案例分析



主动发现防御



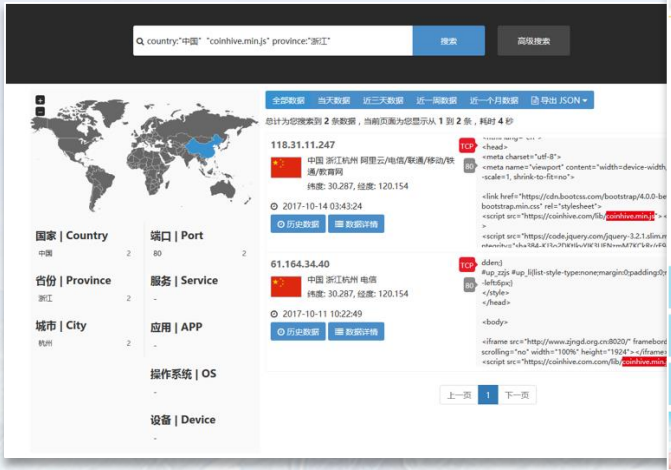
溯源&反制

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：

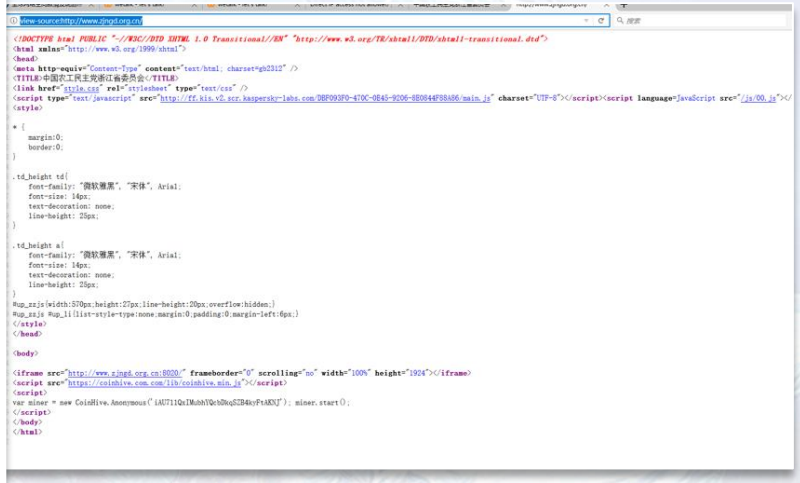
利用网页内嵌的Javascript程序（一段JS代码），“借用”浏览者的电脑用作挖掘虚拟货币的用途，也就是挖矿。该行为会使在网站的浏览者在浏览网站时，挖矿程序的JS代码就会运行，导致浏览插入挖矿代码网站CPU占用率很高，甚至100%满负荷运行！

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

铁流鏖戰