2018

新形势下高校信息安全建设再思考

北京启明星辰信息安全技术有限公司

安全设备的这些报警是真实的攻击吗？是否可能误报？

面对这些报警该如何去分析它？

这些威胁可能造成的影响有哪些？范围有多广？有多深？

今天的这条攻击和3个月前的某一条攻击有关系吗？

这么多的威胁报警，到底有没有已失陷的主机？攻击者的意图是什么？

趋势：已知+未知+分析

已知检测 + 未知检测 + 深度分析

特征检测　　静态/动态检测　　入侵分析中心

威胁情报辅助

高级威胁检测的优势

传统检测	高级检测
单点 看不清全貌	**大数据+威胁情报** 看清“黑客画像”
依赖特征 无法发现新型威胁	**机器学习+动态检测** 覆盖95%新型变种
耗时 人工分析数周-数月	**秒级发现** 缩减99%人工时间

智能关联

深度检测

快速发现

北京某高校案例

北京某高校遭遇白象组织攻击

盗取大量信息！ 高级

- 定向攻击
- 多阶段攻击
- 高级逃逸技术

2018年3月

被盗取的部分信息

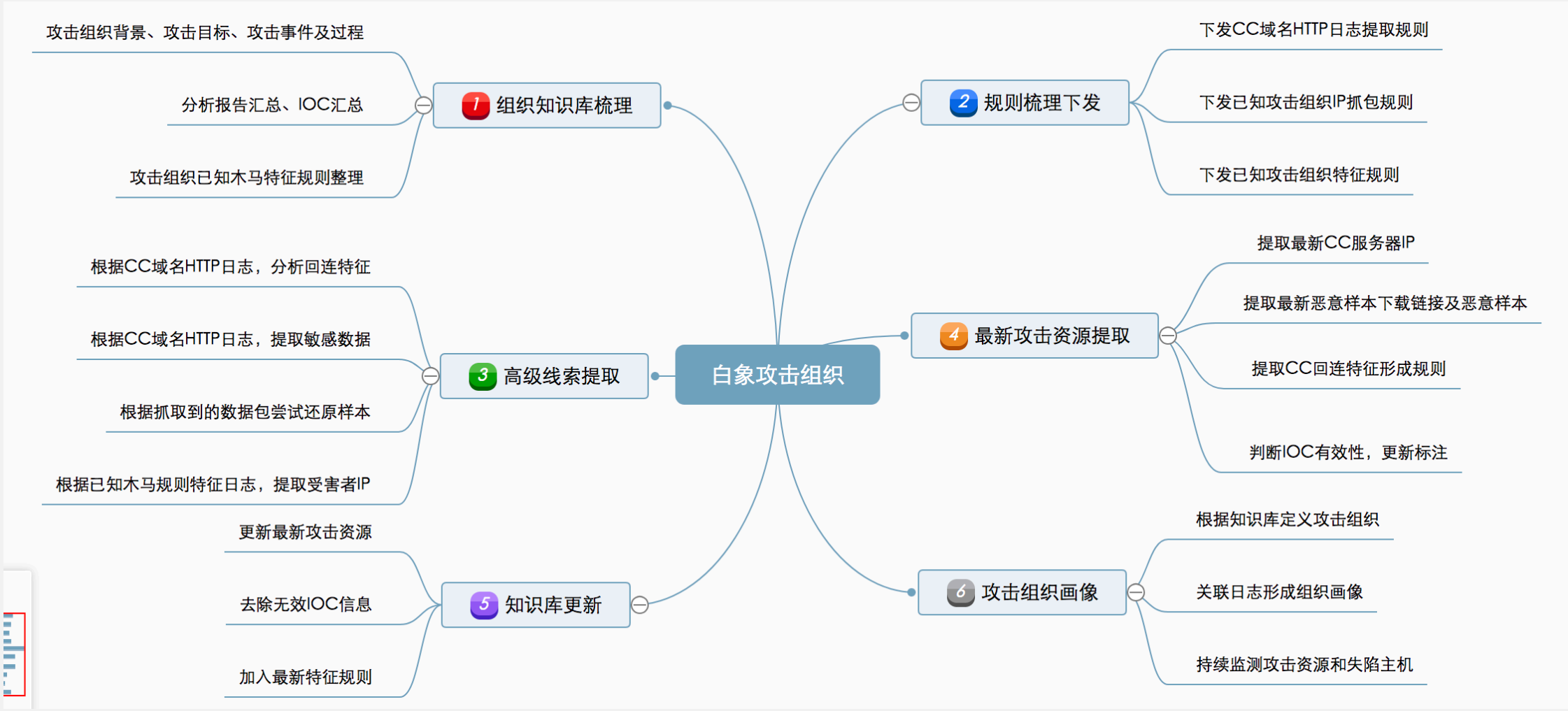
CAU Measures of Annual Review of Chinese Government Scholarship Status(final).pdf
CGS Annual Evaluation form中国政府奖学金年度评审表.docx
Data_Exer1.csv
CGS Extension Form中国政府奖学金生延长奖学金期限申请表.docx
Data_Cluster_Marker.csv
Data_Cluster_Pheno.csv
Supervisor-College form学院导师意见表.docx
[redacted]大学-中国政府奖学金年度评审实施细则(Final).pdf
Data_Lect4_1.csv
Information_Letter1.docx
Data_Lect5_2.csv
Eigen.csv
Data_RegCorr.csv
Data_VarComp.csv
EigenVec.csv
2015-Teaching schedule of Invasion Biology.pdf
CASE STUDY CAAS.docx
CASE STUDY CAUPQL.docx
CASE STUDY FOREST UNIVERSITY LAB.docx
CASS.docx
Fang 2014_Aphelenchoides rotundicaudatus.pdf
geb12214.pdf
Hongmei Esteya 2014-Morphological_ molecular and__ biological characterization of Esteya vermicola.pdf

白象攻击组织追踪

“白象”又名“Patchwork”，“摩诃草”，疑似来自南亚某国，自2012年以来持续针对中国、巴基斯坦等国进行网络攻击，长期窃取目标国家的科研、军事资料。其先导攻击手段多为鱼叉式钓鱼邮件，发送带有格式漏洞文档的链接。

攻击来源	南亚某国（疑似印度）
受害范围	中国，巴基斯坦
攻击目的	窃密、网络间谍
攻击目标	科研教育机构、政府部门

威胁狩猎思维


白象攻击组织
1 组织知识库梳理
攻击组织背景、攻击目标、攻击事件及过程
分析报告汇总、IOC汇总
攻击组织已知木马特征规则整理
2 规则梳理下发
下发CC域名HTTP日志提取规则
下发已知攻击组织IP抓包规则
下发已知攻击组织特征规则
3 高级线索提取
根据CC域名HTTP日志，分析回连特征
根据CC域名HTTP日志，提取敏感数据
根据抓取到的数据包尝试还原样本
根据已知木马规则特征日志，提取受害者IP
4 最新攻击资源提取
提取最新CC服务器IP
提取最新恶意样本下载链接及恶意样本
提取CC回连特征形成规则
判断IOC有效性，更新标注
5 知识库更新
更新最新攻击资源
去除无效IOC信息
加入最新特征规则
6 攻击组织画像
根据知识库定义攻击组织
关联日志形成组织画像
持续监测攻击资源和失陷主机

白象威胁狩猎过程


监测组织关联情报获取最新CC，提取http日志
发现文件回传、加密发送主机信息等线索
制定行为特征，持续监控
3.12
3.21
3.26
3.28
3.30
4.8
白象组织活跃期
爆发大量回传受控主机文件事件
输出报告给甲方
甲方高度重视并要求对数据进行精细处理
提取受害者信息，回传文件列表，受害主机信息列表等

白象组织跟踪成果

失陷主机数：	7
被偷文件数量：	200+
发现新的CC：	11
发现组织新样本：	3
提取组织特征规则：	4

监控到的上传与下载记录

高级 10000+

数据盗取 10000+

木马后门 16

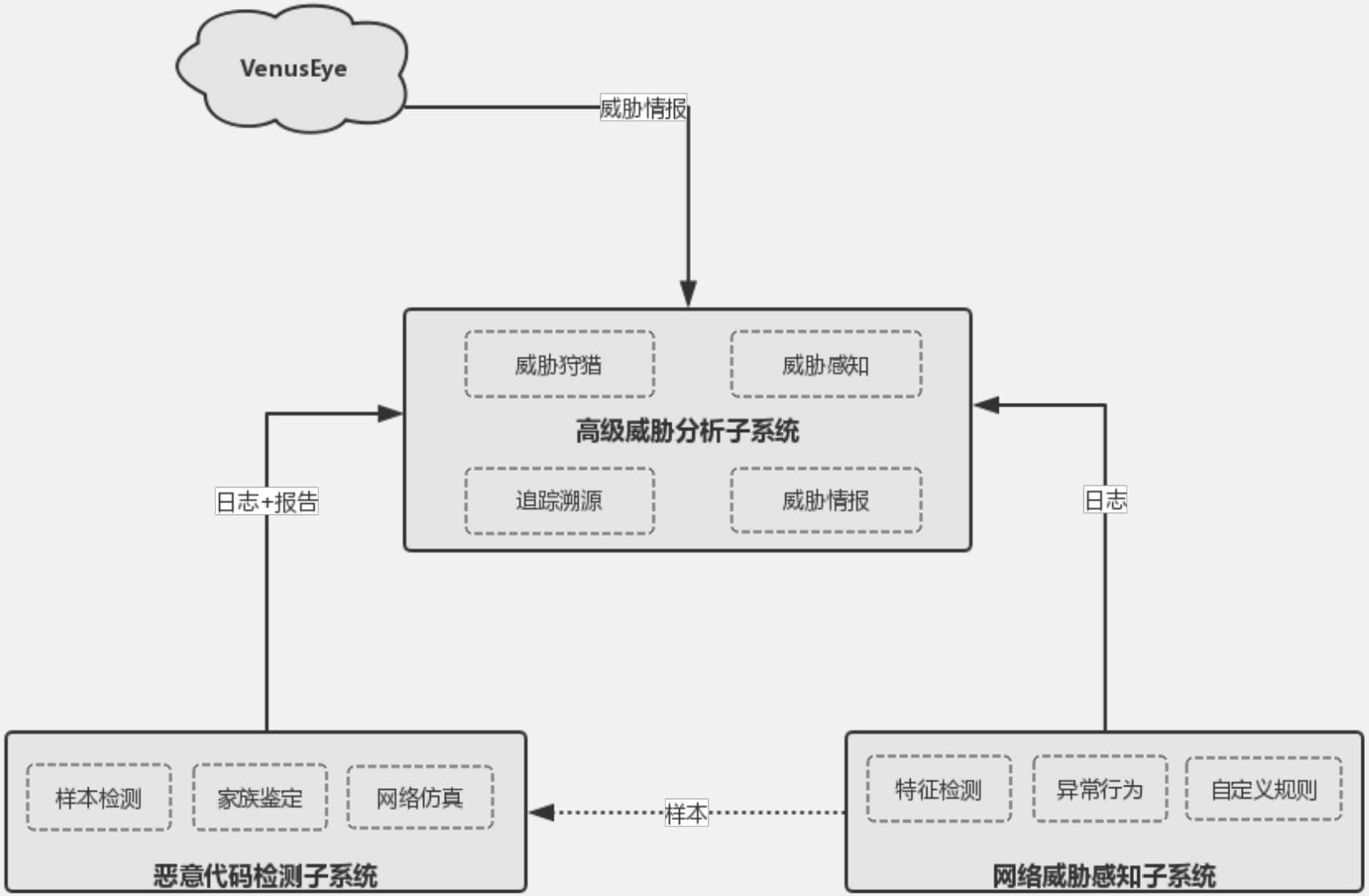
第三阶段 10000+

事件名称	发生时间	重点|普通	源IP	目的IP	阶段	事件类型	事件级别
白象木马下载更新	2018-04-27 11:19:17	普通	[redacted]	[redacted]	第三阶段	木马后门	高级
白象木马下载更新	2018-04-27 11:12:16	普通	[redacted]	[redacted]	第三阶段	木马后门	高级
白象木马下载更新	2018-04-27 11:05:14	普通	[redacted]	[redacted]	第三阶段	木马后门	高级
白象木马下载更新	2018-04-27 10:58:19	普通	[redacted]	[redacted]	第三阶段	木马后门	高级
白象木马下载更新	2018-04-27 10:51:13	普通	[redacted]	[redacted]	第三阶段	木马后门	高级
白象木马下载更新	2018-04-27 10:44:18	普通	[redacted]	[redacted]	第三阶段	木马后门	高级
白象文件上传	2018-04-25 23:59:33	普通	[redacted]	[redacted]	第三阶段	数据盗取	高级
白象文件上传	2018-04-25 23:59:31	普通	[redacted]	[redacted]	第三阶段	数据盗取	高级
白象文件上传	2018-04-25 23:59:22	普通	[redacted]	[redacted]	第三阶段	数据盗取	高级
白象文件上传	2018-04-25 23:59:12	普通	[redacted]	[redacted]	第三阶段	数据盗取	高级

« 1 2 3 4 5 6 7 8 9 10 11 12 13 ... 999

某科研机构“永恒之蓝”扩散图

某项目案例


VenusEye
威胁情报
威胁狩猎
威胁感知
高级威胁分析子系统
追踪溯源
威胁情报
日志+报告
日志
样本检测
家族鉴定
网络仿真
恶意代码检测子系统
样本
特征检测
异常行为
自定义规则
网络威胁感知子系统

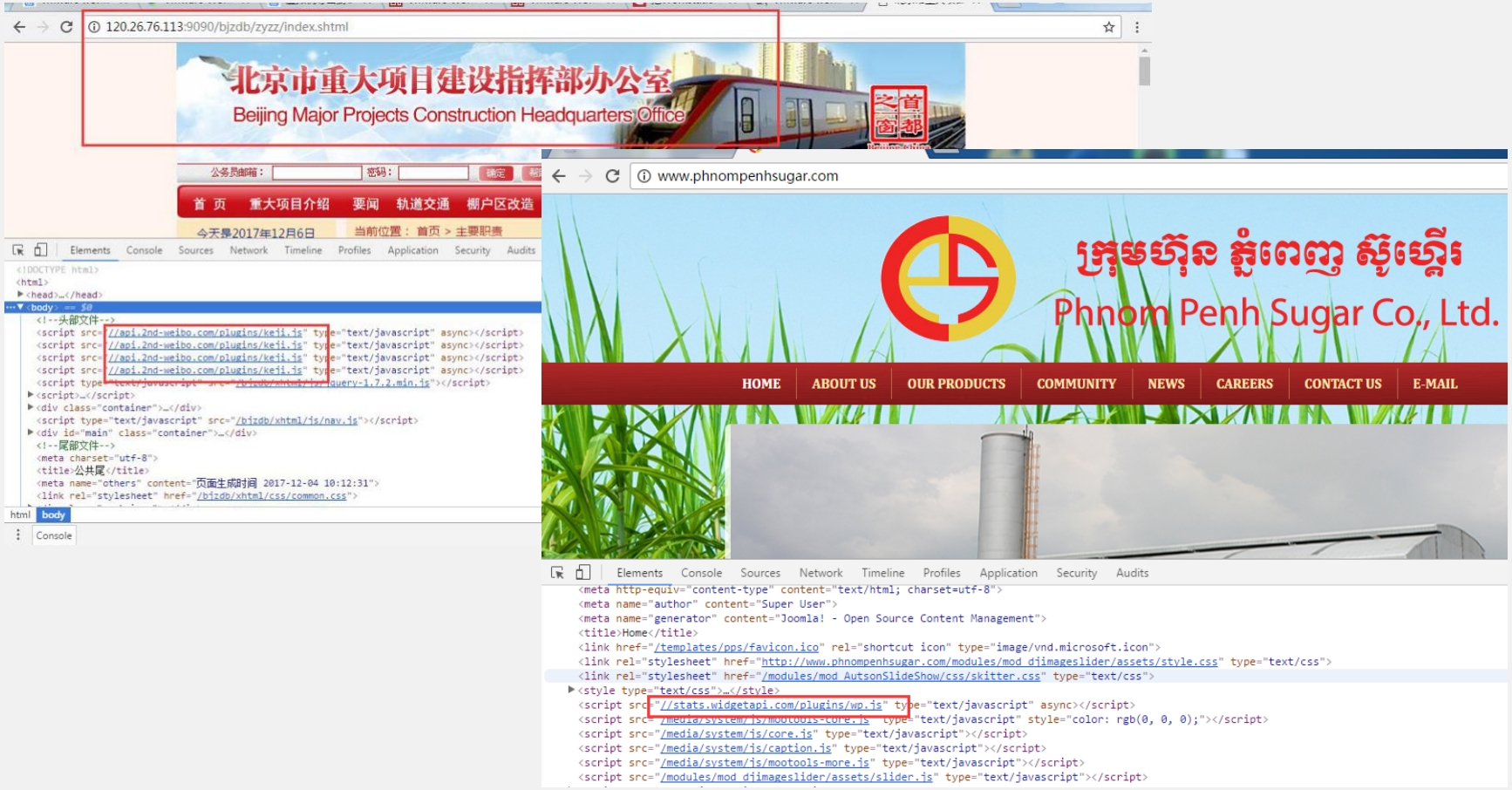
海莲花追踪-阶段成果

- 发现新的组织黑产IP 12个

IP	解析域名
208.91.197.238	api.querycore.com、 gl-appspot.org、nsquery.net
74.119.239.234	harinarach.com
216.107.152.217	blog.docksugs.org、 news.lighpress.info
91.229.78.226	untitled.po9z.com、 zone.apize.net、ssl.zin0.com
89.34.237.142	engine.lanaurmi.com、 png.eirahrlichmann.com
87.98.153.188	images.andychroeder.com、 movies.onaldest.com
62.210.115.97	mobile.pagmobiles.info、 pagmobiles.info
91.229.77.192	push.relasign.org、 high.vphelp.net、 seri.volveri.net
188.166.213.21	api.fbconnect.net
27.102.66.169	store.shoesadidas.net
46.183.70.207	eoneorbin.com
54.231.82.26	dload01.s3.amazonaws.com

海莲花追踪-阶段成果

- 发现海莲花用于收集信息的钓鱼网站、挂马网站、伪造政府网站等



- 发现新的C&C通道、敏感数据传输

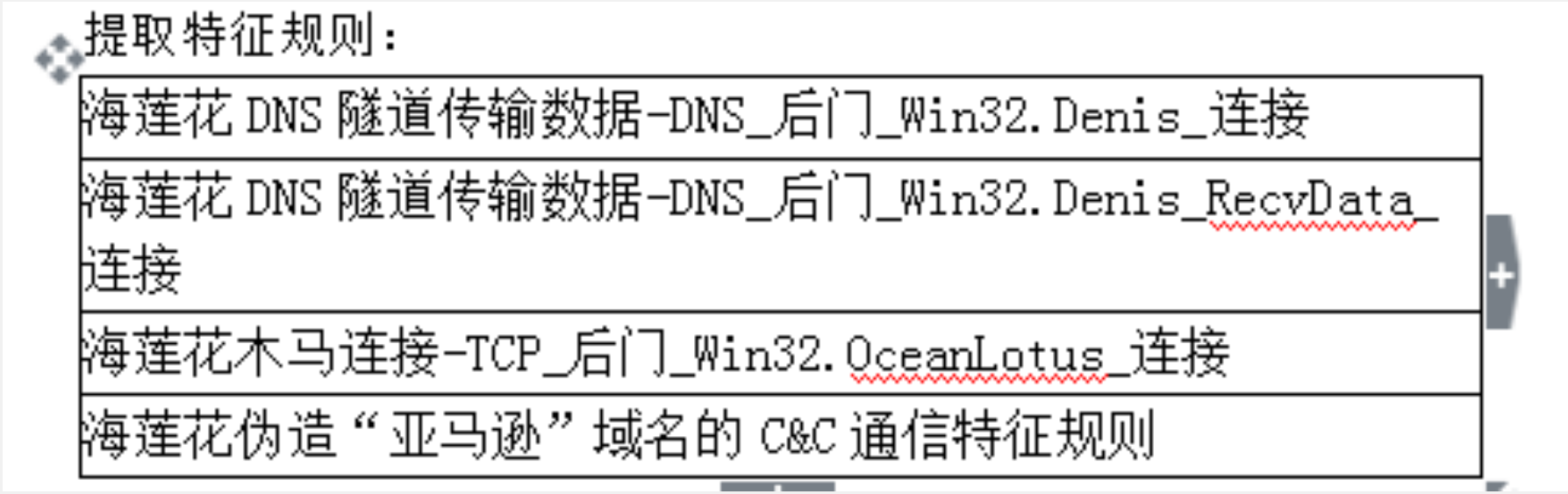
海莲花追踪-阶段成果

- 解密海莲花木马回传的加密数据信息
- 例

- 确定已被攻击成功的受害者若干

海莲花追踪-阶段成果

- 提取海莲花木马网络行为特征4条



提取特征规则：

海莲花 DNS 隧道传输数据-DNS_后门_Win32.Denis_连接
海莲花 DNS 隧道传输数据-DNS_后门_Win32.Denis_RecvData_连接
海莲花木马连接-TCP_后门_Win32.OceanLotus_连接
海莲花伪造“亚马逊”域名的 C&C 通信特征规则

该项目其他成果

Bitter组织：

- 发送控制命令，回传主机信息，攻击者控制的部分僵尸网络列表等

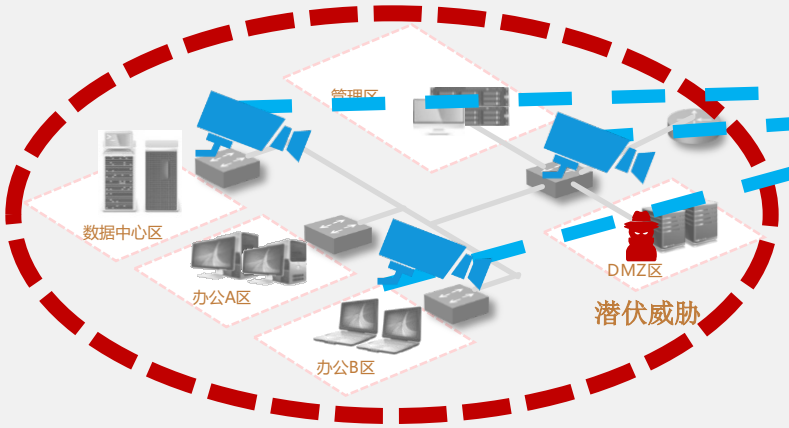
Darkhotel组织：

- 最新木马回连服务器，回传主机信息

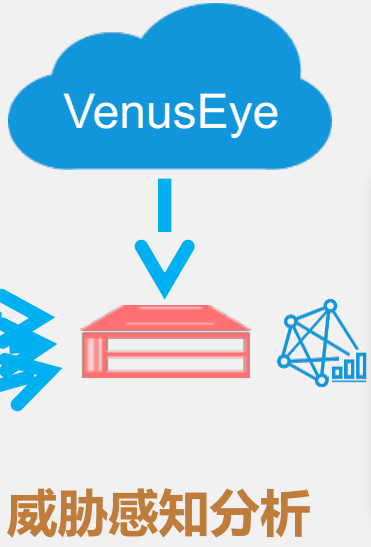
利用IoT设备漏洞的“Gafgyt”僵尸网络发现

Mykings僵尸网络发现

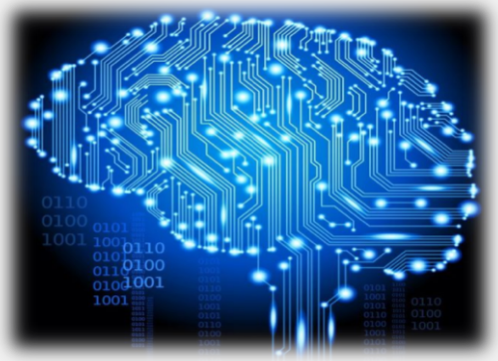
威胁感知体系



威胁感知探针



威胁感知分析



大数据、机器学习
威胁建模、行为分析

全面深入发现
各种高级威胁

威胁感知体系建设

【公司介绍】

启明星辰公司成立于1996年，是由留美博士严望佳女士创建的、拥有完全自主知识产权的网络安全高科技企业。是国内最具实力的网络安全产品、可信安全管理平台、专业安全服务与解决方案的综合提供商。

公司总部位于北京市中关村软件园启明星辰大厦，公司员工3000人，技术团队千人，在全国各省、市、自治区设立分支机构六十多个，拥有覆盖全国的渠道体系和技术支持中心。公司于2010年6月23日在深圳中小板挂牌上市。**成为中国信息安全行业规模最大、市值最高的顶级安全解决方案供应商。**

UTM、安全管理平台、IDS等产品连续多年排名市场第一

产品目录

启明星辰

- 安全域隔离与边界防护解决方案
- 内联网宏观监控解决方案
- 安全管理平台建设解决方案
- 结合萨班斯法案的4A审计解决方案
- 政府、国企领域等级保护解决方案

- TSOC 泰合信息安全运营管理中心
- ZSOC 安全域管理平台
- 4ASOC 4A平台
- MSOC 监控管理平台
- ASOC 综合审计平台

- PSS安全管理咨询服务
- PSS安全风险评估服务
- PSS应用系统安全评估服务
- CSS客户化安全服务
- MSS安全管理监控服务

- 天阗入侵检测与管理系统
- 天阗威胁检测与智能分析系统
- 天清汉马USG一体化安全网关
- 天清汉马USG防火墙
- 天清入侵防御系统
- 天清Web应用安全网关
- 天榕数据防泄密（DLP）系统
- 天榕电子文档安全系统
- 安星远程网站安全检查服务
- 天玥网络安全审计系统
- 天珣内网安全风险管理与审计系统
- 天镜脆弱性扫描与管理系统
- 天清异常流量管理与抗拒绝服务系统

THANKS

谢 谢 观 看

联系人：李小凤
联系方式：13641035422

联系人：颜艳
联系方式：18810557717