NSFOCUS

TECHWORLD2019

绿 盟 科 技 技 术 嘉 年 华

探索 · DISCOVERY

NSFOCUS TECHWORLD

现网威胁猎杀与跟踪

NSFOCUS

TECHWORLD2019 绿盟科技技术嘉年华

伏影实验介绍

伏影实验室

NSFOCUSFUYING LAB

专注于安全威胁与监测技术研究

涵盖威胁识别技术，威胁跟踪技术，威胁捕获技术，威胁主体识别技术。

研究目标：

僵尸网络威胁、APT 、 DDOS对抗、WEB对抗、流行服务系统脆弱利用威胁、 身份认证威胁、数字资产威胁、黑色产业威胁及新兴威胁。

通过掌控现网威胁来识别风险、缓解威胁伤害，为威胁对抗提供决策支撑。

防御威胁，必须发现威胁

- 建立在高级安全专家持续研究的基础上

- 人的精力是有限，威胁出现区域有差异、时间有先后、威胁程度有大有小、威胁具有流窜性

- 特征过滤式防御往往滞后威胁发生，对于一个新型威胁，往往混迹于浩如烟海的网络事件中
- 漏报已知威胁---有过，对抗未知威胁---无指标

- 跟踪其发展、变化、规模、手法变更。不会因为一个漏洞被修复而停止攻击，不会因为代码和原理被披露而停止攻击，反而更泛滥

NSFOCUS

TECHWORLD2019 绿盟科技技术嘉年华

威胁猎杀系统

TTP,IOC,APT.

威胁跟踪（bothunter、APT活动分析与监测）

现网威胁捕获（诱捕）

TIS (威胁事件知识共享）

高危资产标识（遥测）

威胁检测（给设备提供特定插件或高危特征）

设备数据 (传统日志)

威胁分类及标识

威胁评估（NetFlow、DNS、设备）

绿盟大数据中心

情报清洗

专项威胁调查（神盾）

情报分析与挖掘（InXight）

情报校验系统

威胁 && 影响范围 && 证据

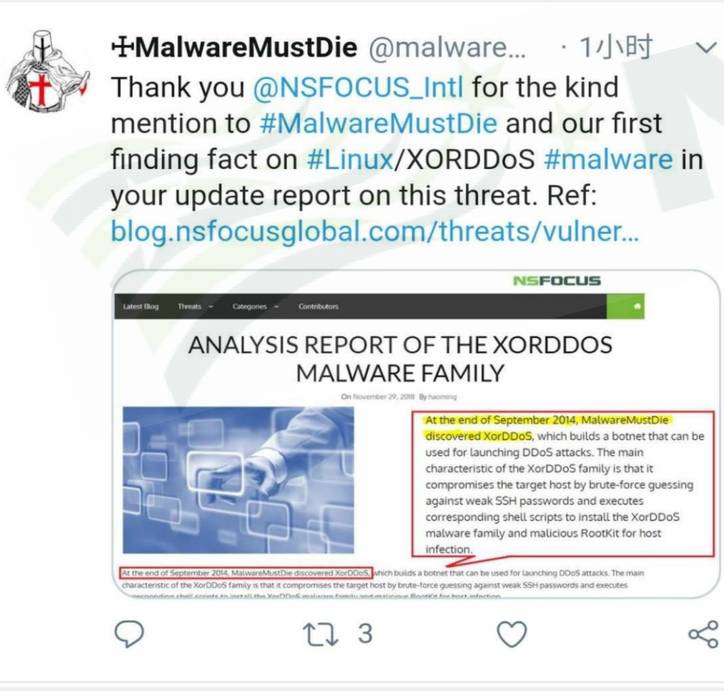
绿盟威胁情报中心

NSFOCUS

TECHWORLD2019 绿盟科技技术嘉年华

威胁跟踪运营

- ✓ 持续迭代与运营
- ✓ 获国际同行业认可
- ✓ 活跃家族数量增加至168个
- ✓ 家族类型：
  - ✓ DDOS
  - ✓ 挖矿
  - ✓ APT
  - ✓ 银行木马
  - ✓ 广告点击



通信命令

监控到通信命令30.5W+条

下载指令共计4100余条

下载1100活跃病毒/组件/漏洞利用工具

监控攻击指令

监控到攻击命令22W+条:

有效攻击目标：17W+个

去重后攻击目标：3.5W个

新增C2

增加活跃C2 3434个，大多数为高质量C2，活跃时间长，指令丰富

样本&恶意IP

日处理样本：14W+个

监测恶意IP数量：428W+个

新增家族（24.4%增长）

新增活跃家族数量：33个

恶意域名

监控恶意活跃域名数量：8000+个

NSFOCUS

TECHWORLD2019 绿盟科技技术嘉年华 | 近期发布报告以及文章

Botnet年报、解读平台采访

网络安全江湖“百晓生”为你揭密僵尸网络的江湖排名

绿盟科技 | 38 文章 | 5695 总阅读 | 查看TA的文章>

2019-03-06 19:53 | 公司 | 互联网 | 科技

桃李春风一杯酒，江湖夜雨十年灯。

DOIT

Botnet趋势解读之刻不容缓的物联网安全

2019-03-28 分类：业界 / 安全

VIRUSTOTAL

TUESDAY, 7 MAY 2019

VirusTotal Multisandbox += NSFOCUS POMA

We are pleased to announce that the multisandbox project has partnered with NSFOCUS POMA. This brings VirusTotal up to six integrated sandboxes. The NSFOCUS sandbox gives us insight into the behaviour of samples that run on Windows 7 and XP SP3.

In their own words:

> NSFOCUS POMA, as an integral part of the NSFOCUS Threat Intelligence (NTI) system, is a cloud-based malware analysis engine built by the NSFOCUS Security Lab. It can take various types of files and perform both static and dynamic analysis on them to detect potentially malicious behavior, and produce analytic reports in many formats (including STIX). This service can help a user to protect his environment from various threats, such as 0-day attacks, advanced persistent threats (APTs), ransomware, botnets, cryptocurrency mining and other malware.
>
> We are very honored and proud to bring such values to the VirusTotal users and community.

组织跟踪与分析 4篇

Computrace黑白一线间，组合威胁渐现江湖

about a month ago 伏影实验室

Computrace BY AbsoluteSoftware

APT34攻击全本分析

3 months ago 伏影实验室

Gafgyt魔高一尺-BaaS模式的僵尸网络

6 months ago 伏影实验室

从通信流量日志看Gafgyt僵尸网络趋势

about a month ago 伏影实验室

漏洞研究文章4篇

Fastjson<=1.2.47远程代码执行漏洞处置手册及技术分析

3 days ago 伏影实验室

WordPress 5.0.0 远程代码执行漏洞分析CVE-2019-8942、CVE-2019-8943

2 months ago 伏影实验室

WORDPRESS

绕过 RestrictedUnpickler

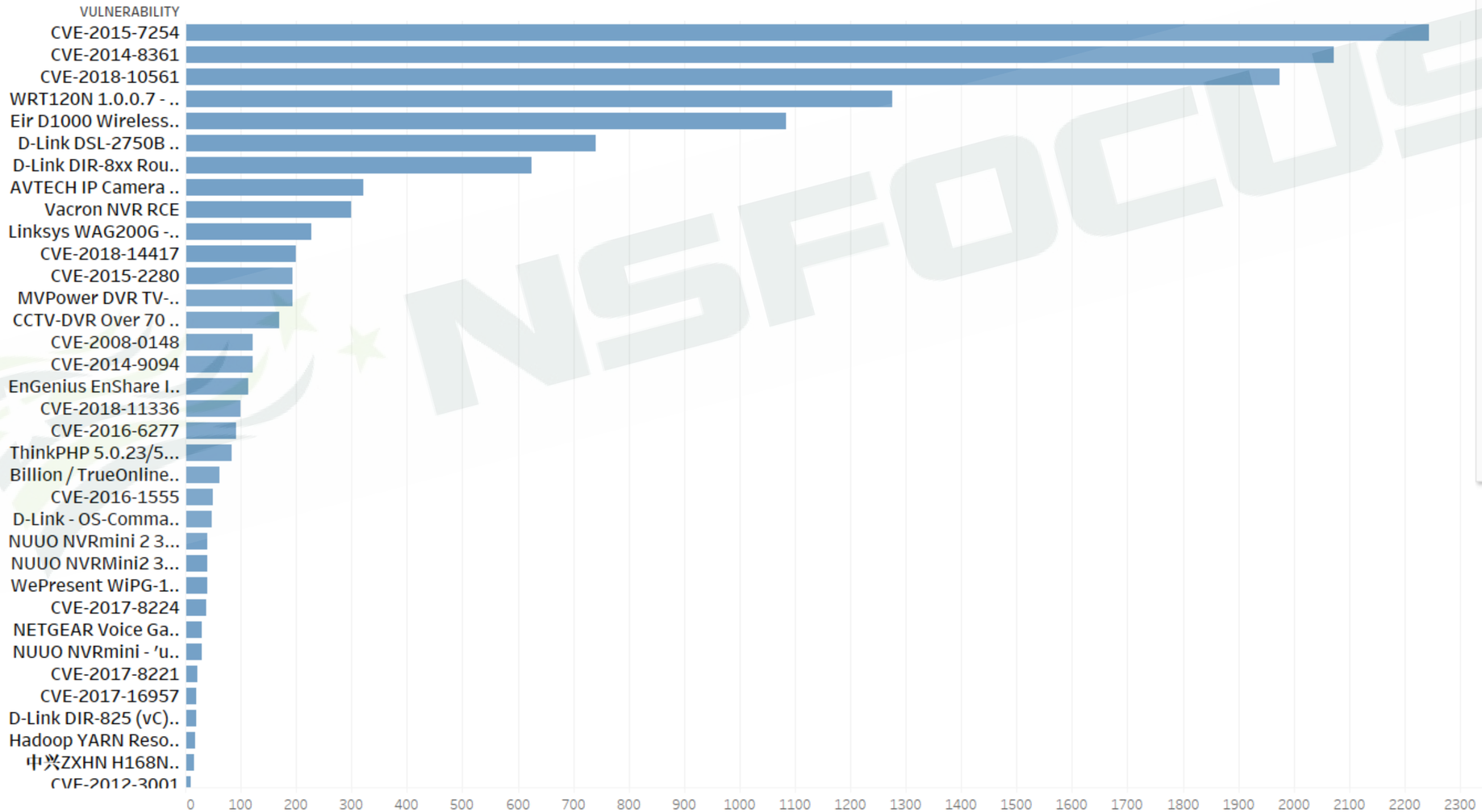
7 days ago idai

ThinkPHP 5.0.x-5.0.23、5.1.x、5.2.x 全版本远程代码执行漏洞分析

3 months ago 伏影实验室

ThinkPHP®

Gafgyt家族漏洞利用频度分布



NSFOCUS

TECHWORLD2019 绿盟科技技术嘉年华

威胁捕获

- 感知节点遍布世界五大洲，覆盖了28个国家其中包括了俄罗斯，美国等这些传统网络安全强国。500+个感知节点服务类型，覆盖通用服务 、 IOT服务、工控服务等。
- 形成了以全端口模拟为基础，智能交互服务为辅的混合型感知架构，紧跟当前CVE漏洞构造陷阱，以漏洞捕获威胁。
- 通过掌控现网威胁来识别风险，缓解威胁伤害，为威胁对抗提供决策支撑。系统每天从互联网中捕获大量的鲜活威胁情报，实时感知黑客活跃攻击工具、攻击手法、攻击演变、攻击组织发展、0day应用等威胁。
- 现今系统已捕获攻击探2亿+次，中高危攻击行为日达数千次，捕获鲜活高价值样本上万个，有效的提升现网威胁捕获能力及感知能力。

威胁捕获---攻击者的“敏捷实践”

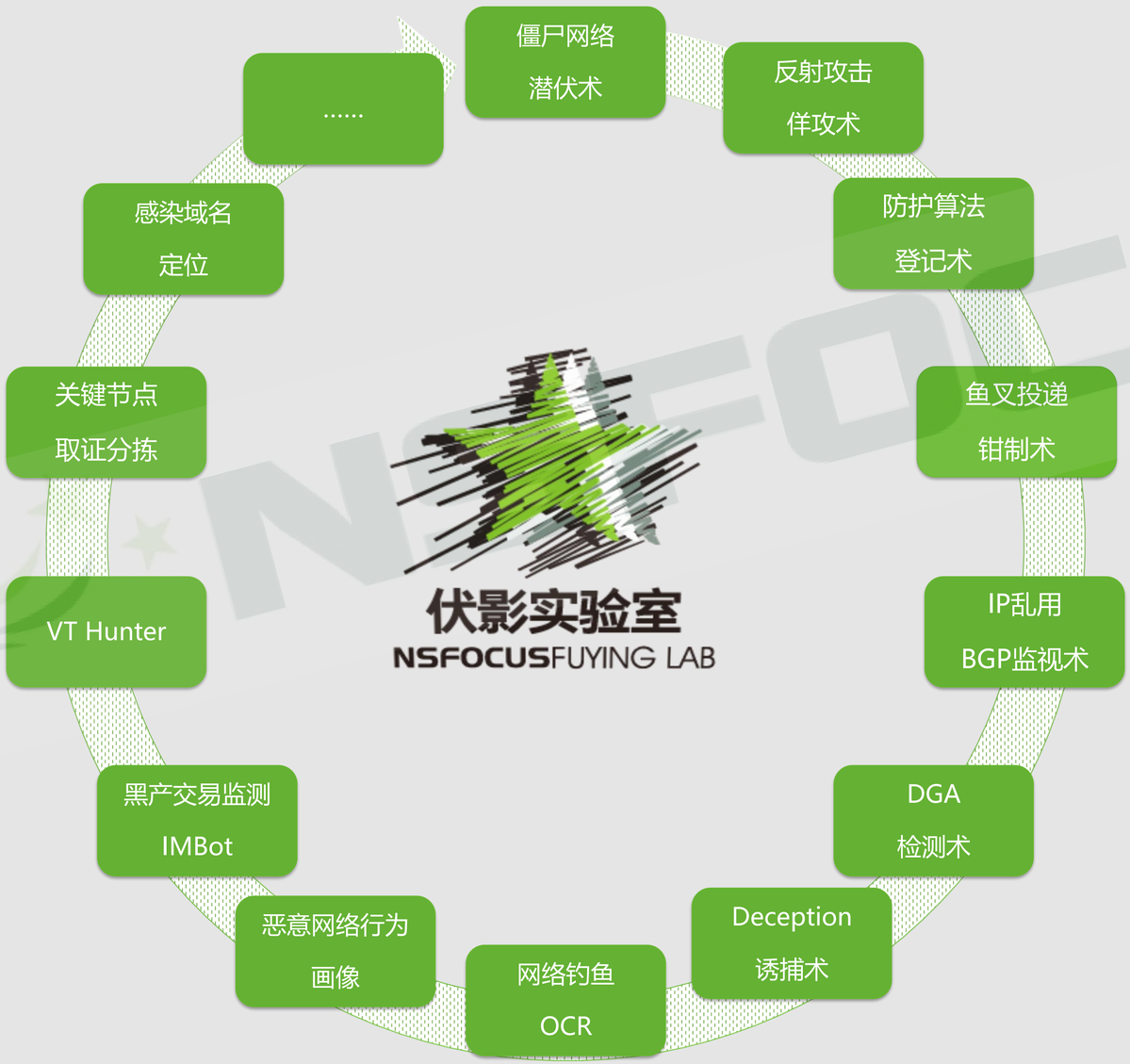
威胁感知节点俘获一个新的家族感染目标广泛，携带多种漏洞利用代码。

- 捕获当日　　17个漏洞
- 2次日后　　21个漏洞
- 1周后　　22个漏洞
- ……

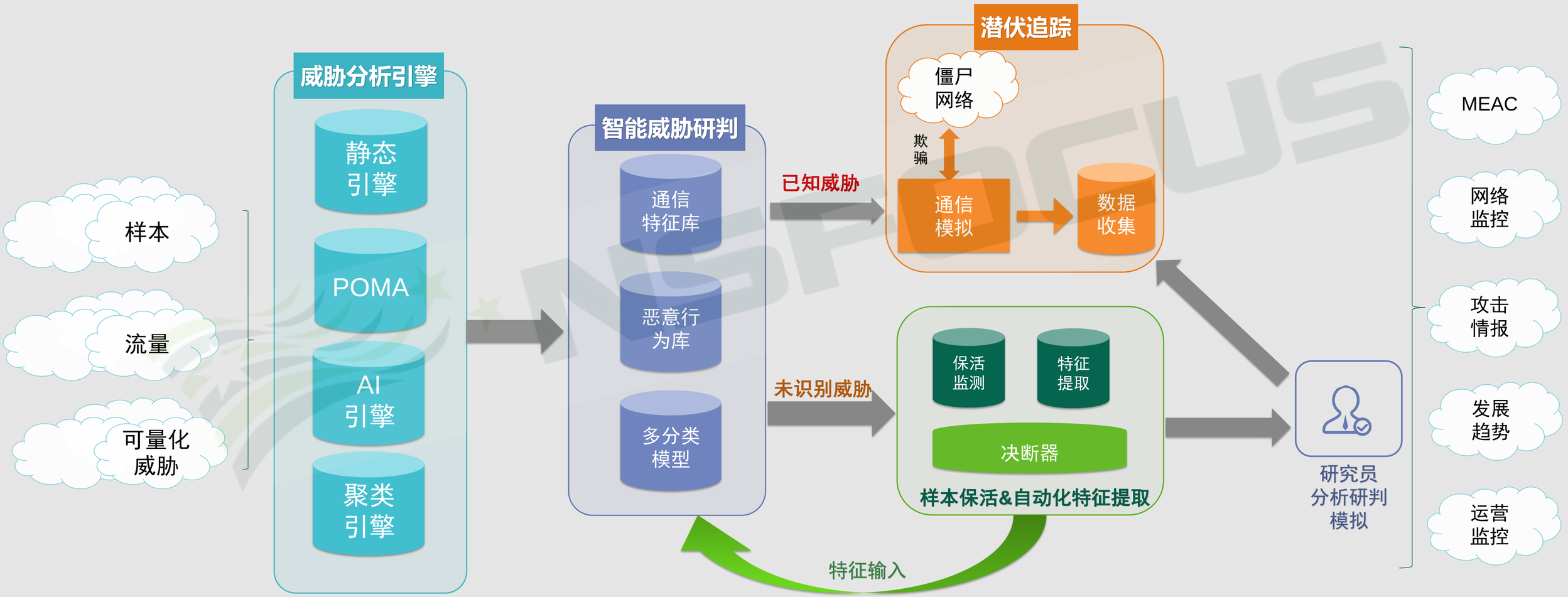
涉及的设备有Linux服务器,有WEB漏洞、D-Link UPnP-命令注入漏洞、CCTV-DVR、HNAP、华为HG532路由器、NetGear路由器、WordPress-CVE-2014-9094等多种漏洞。

- 最早的漏洞出现在2008年，最新的就在当月跨度10年。
- 漏洞利用代码以可加载模块出现。
- 攻击功能多达13种。
- 勒索、信息窃取、资金窃取怎么办?

威胁猎杀技

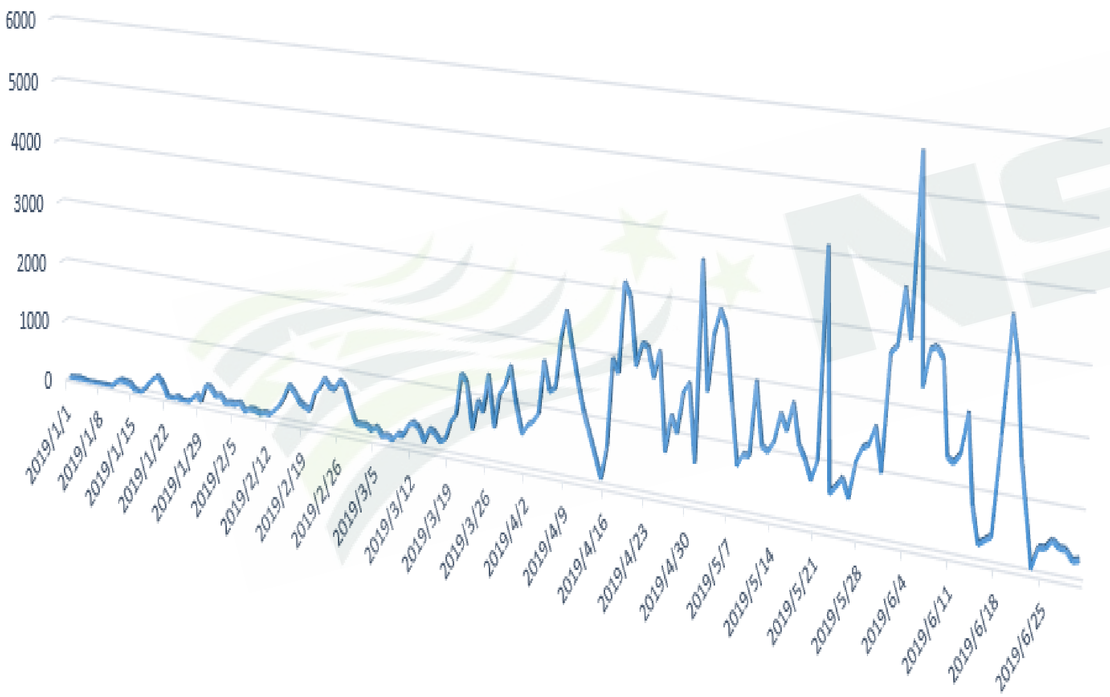

僵尸网络
潜伏术
反射攻击
佯攻术
防护算法
登记术
鱼叉投递
钳制术
IP乱用
BGP监视术
DGA
检测术
Deception
诱捕术
网络钓鱼
OCR
恶意网络行为
画像
黑产交易监测
IMBot
VT Hunter
关键节点
取证分拣
感染域名
定位
.....
伏影实验室
NSFOCUSFUYING LAB

威胁猎杀术——潜伏跟踪技

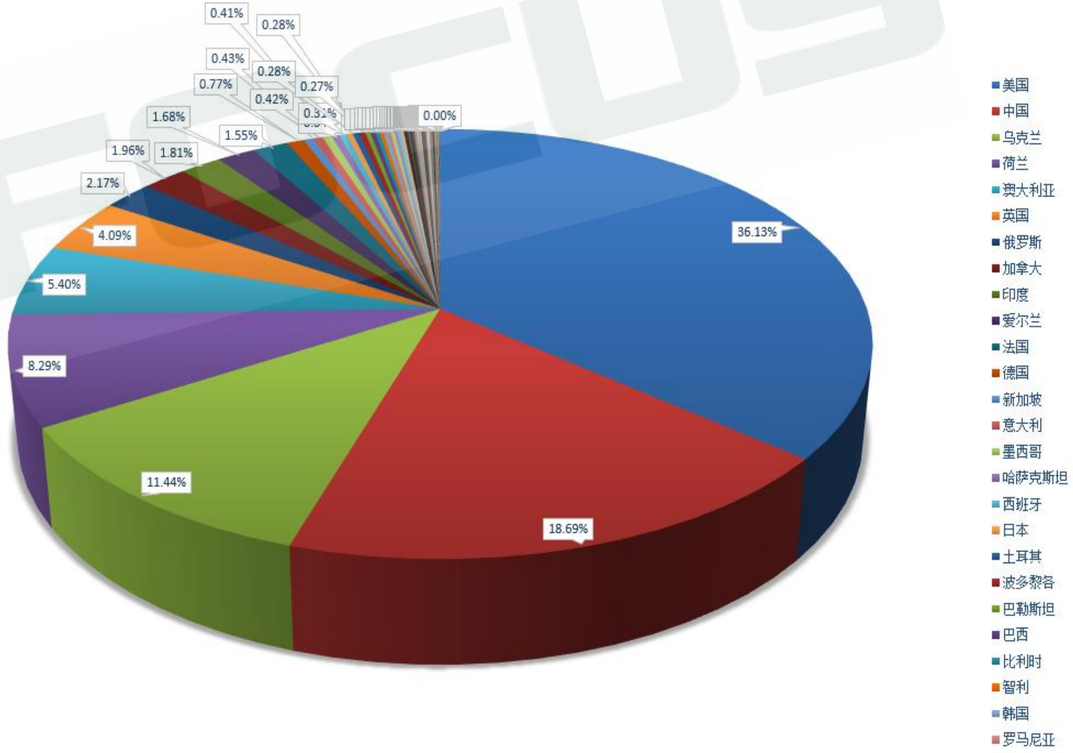

样本
流量
可量化威胁
威胁分析引擎
静态引擎
POMA
AI引擎
聚类引擎
智能威胁研判
通信特征库
恶意行为库
多分类模型
已知威胁
未识别威胁
潜伏追踪
僵尸网络
欺骗
通信模拟
数据收集
保活监测
特征提取
决断器
样本保活&自动化特征提取
特征输入
研究员
分析研判
模拟
MEAC
网络监控
攻击情报
发展趋势
运营监控

威胁猎杀术——潜伏跟踪技

每日攻击事件趋势

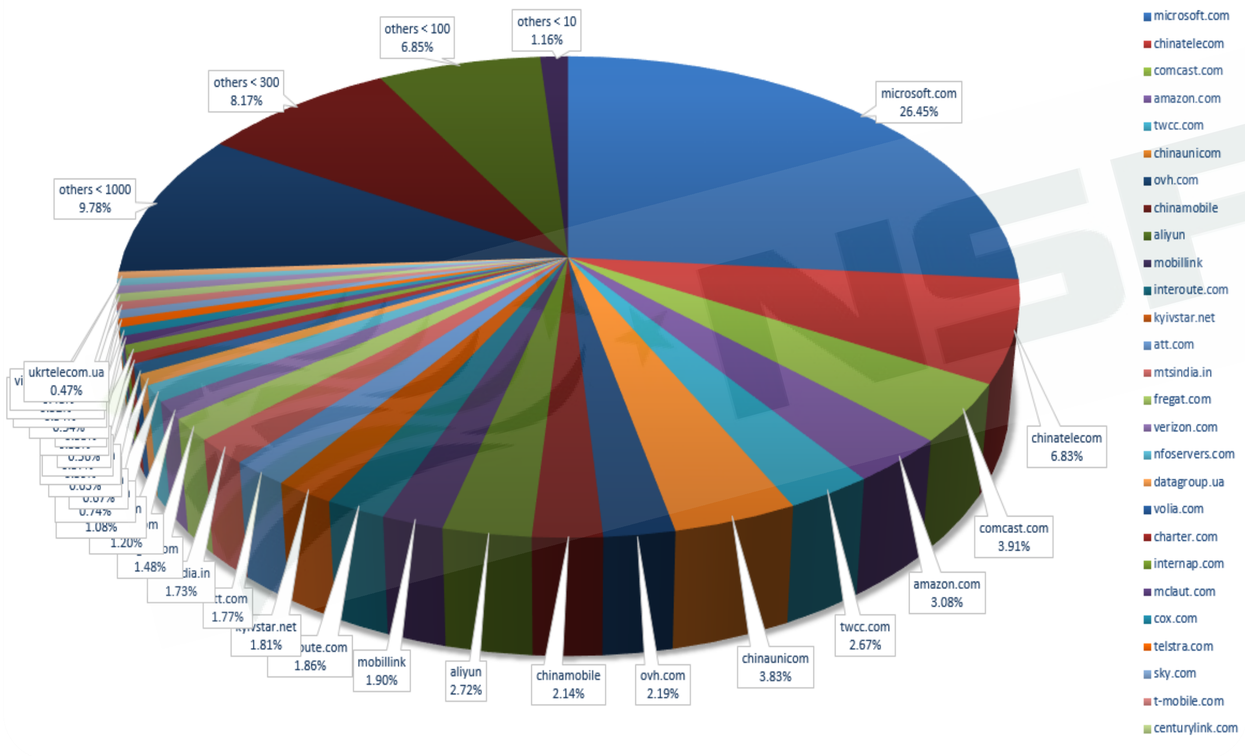


被攻击IP域名所属国家

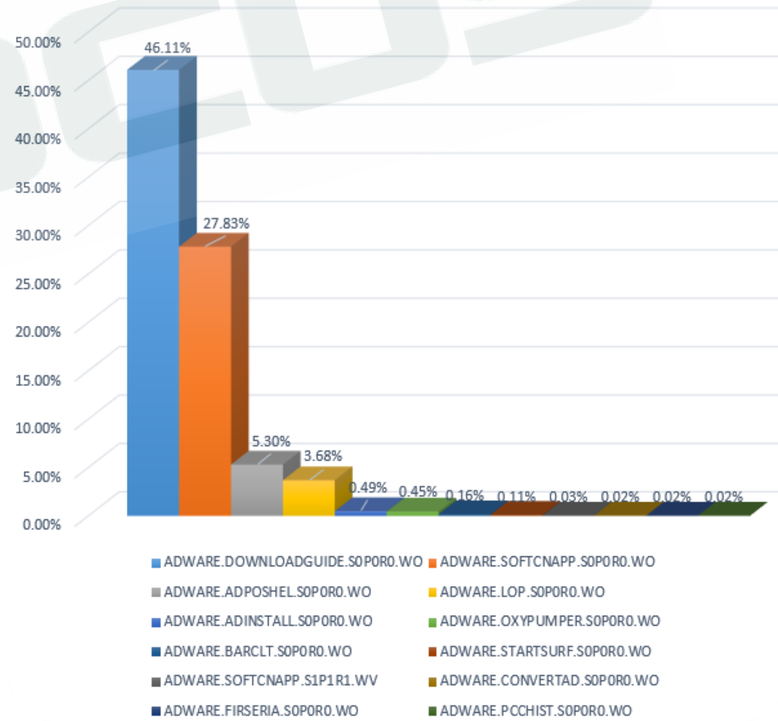


威胁猎杀术——潜伏跟踪技

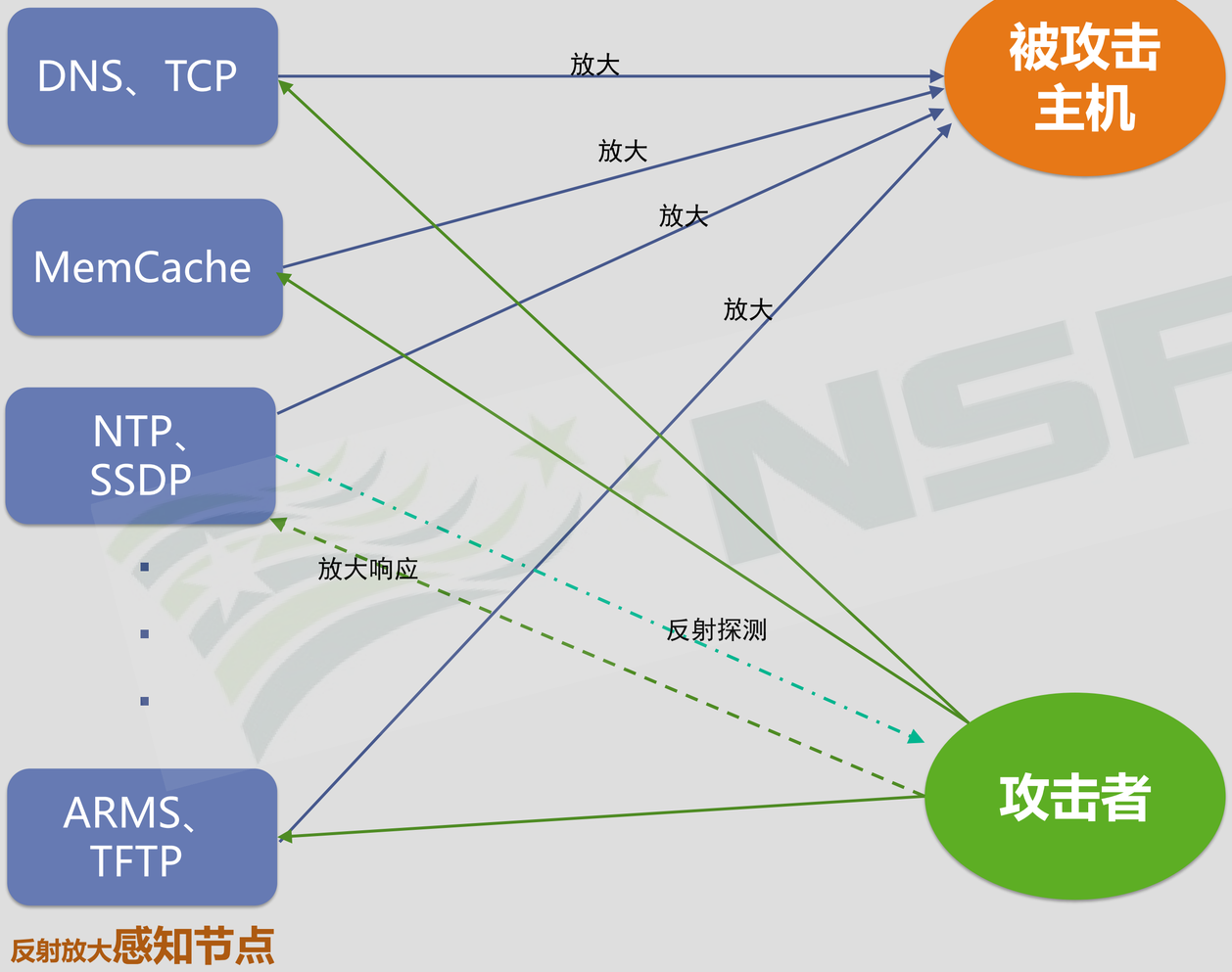
被攻击IP/域名归属服务商



广告类软件监控

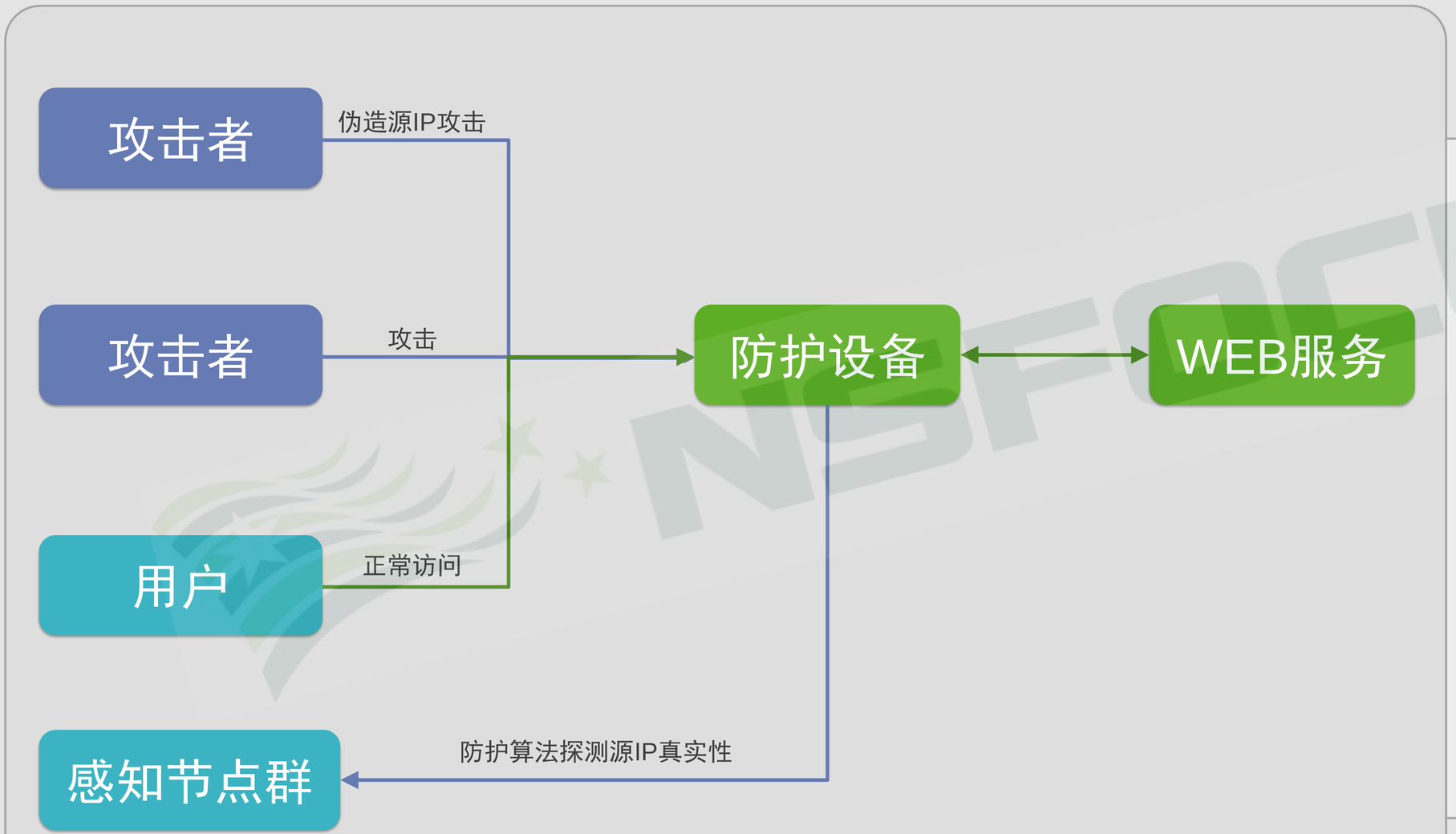


威胁猎杀术---佯攻技



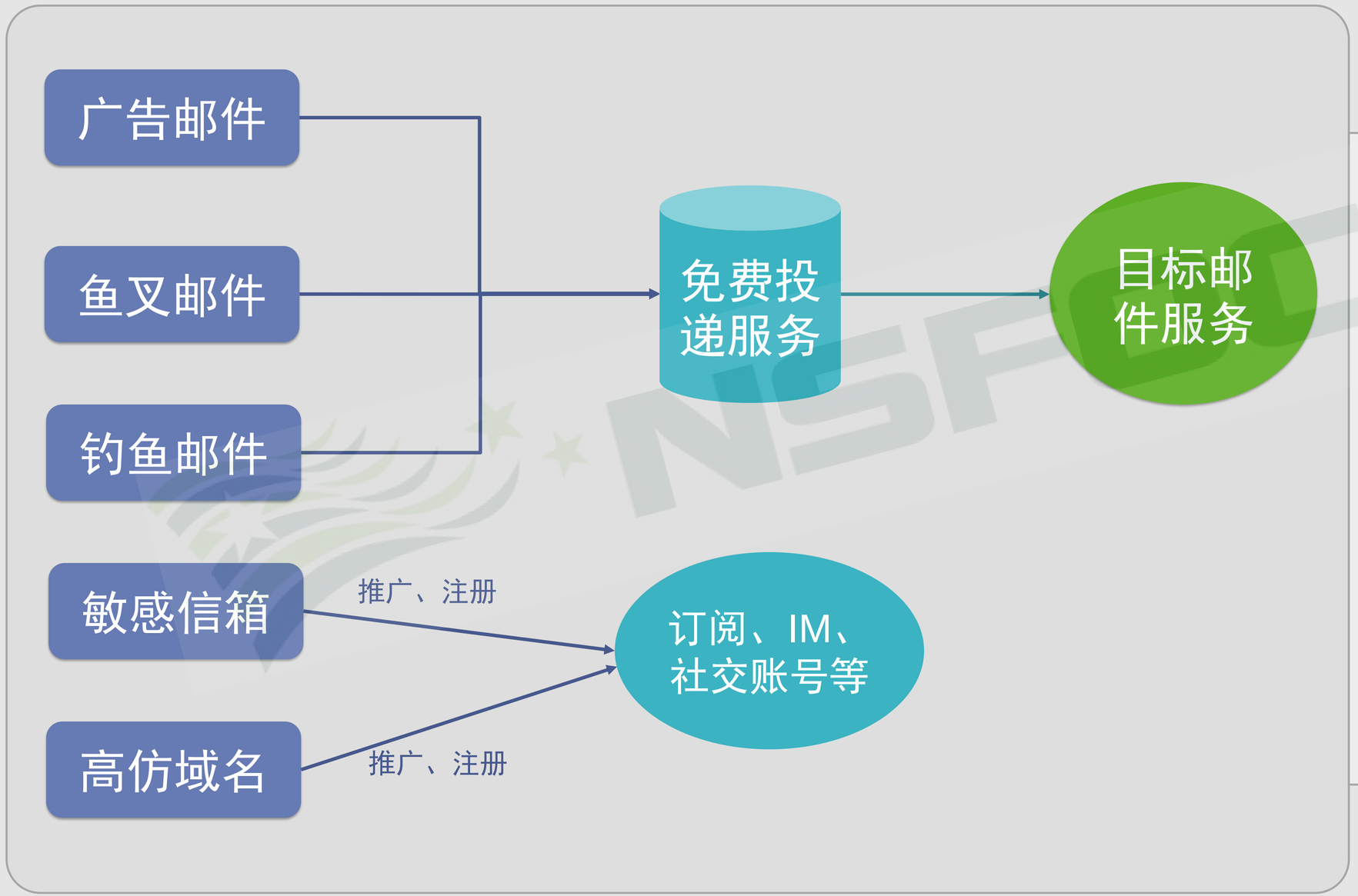
- ✓ 捕捉反射攻击事件
- ✓ 捕捉反射源探测者
- ✓ 提供反射团伙画像属性
- ✓ 提供反射源分析要素
- ✓ ……

威胁猎杀术----登记术



- ✓ 发现攻击事件
- ✓ 识别被攻击要素
- ✓ ……

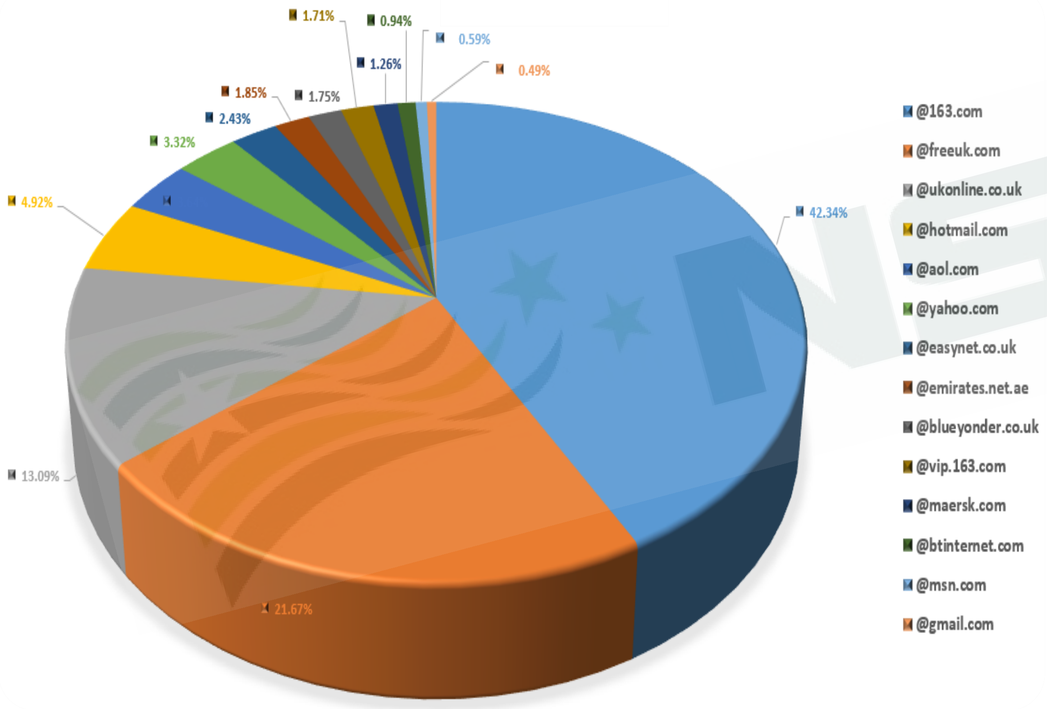
威胁猎杀术----钳制技



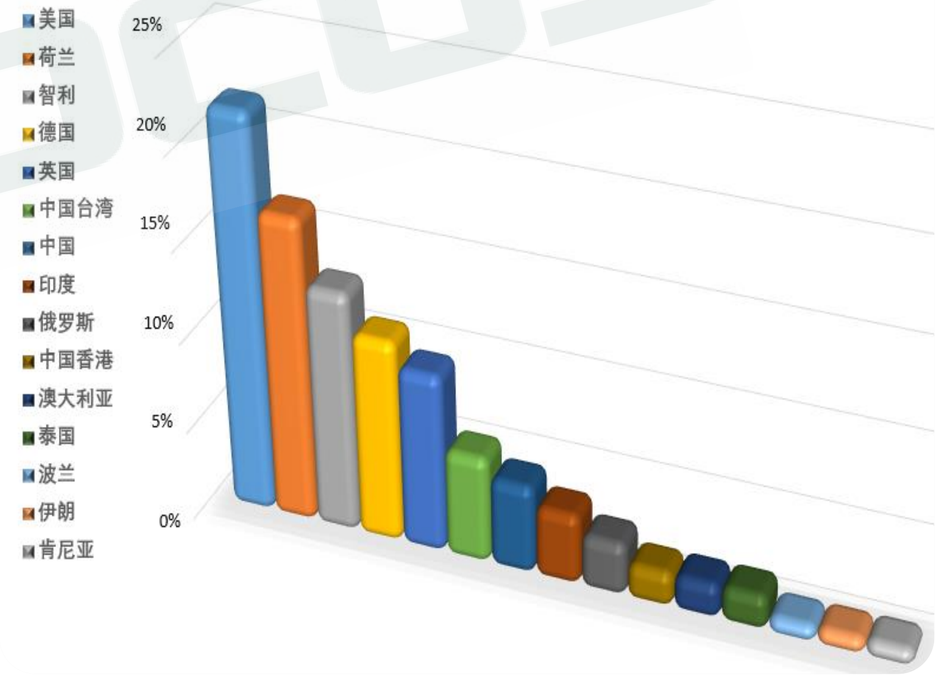
- ✓ 捕获恶意样本
- ✓ 捕获僵尸主机IP
- ✓ 捕获被社工邮件
- ✓ 捕获0day
- ✓ 捕获在野漏洞

威胁猎杀术----钳制技

目的邮件服务商占比



源邮箱国家占比



NSFOCUS

TECHWORLD2019

绿 盟 科 技 技 术 嘉 年 华

探索 · DISCOVERY

NSFOCUS TECHWORLD

感谢聆听！