



2017 中国互联网安全大会
China Internet Security Conference

态势感知中的威胁情报

韩志立

zenmind

360威胁情报中心



中国互联网安全大会



360互联网安全中心

目录

态势感知

威胁情报

小结

态势感知

•概述

•关键因素

•关键技术

态势感知历史发展

20世纪80年代 美国空军

分析空战环境信息，快速判断当前及未来形势并做出正确反应开始态势感知的研究

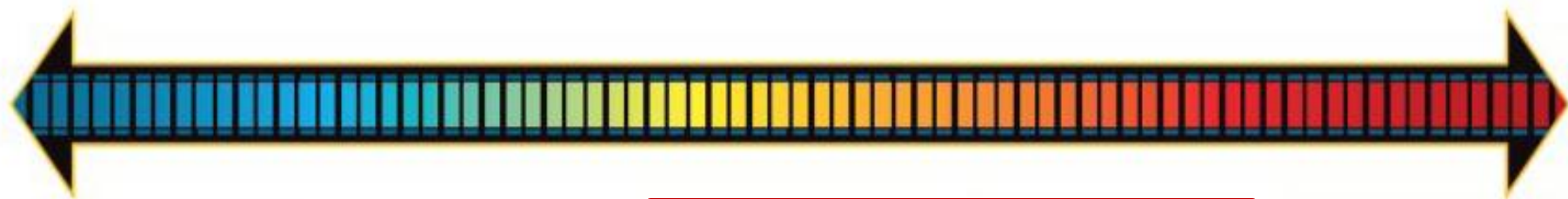
20世纪90年代 进入信息安全领域

在一定的时间和空间范围内，对组织的安全态势及其威胁环境的**感知**。**理解**这两者的含义以及意味的风险，并对他们未来的状态进行**预测**。

2016. 4. 19

全天候全方位感知网络安全态势。。。感知网络安全态势是最基本最基础的工作。。。要建立统一高效的网络安全**风险报告机制、情报共享机制、研判处置机制**，准确把握网络安全风险发生的规律、动向、趋势

态势感知兴起时建设阶段的必然



在系统规划、建设和维护的过程中充分考虑安全防护

架构安全

自身足够强壮

在无人介入情况下，附加在系统架构上可提供持续威胁防御或威胁洞察的系统

被动防御

提高攻击门槛，将大多数攻击拒之门外

分析人员对处于防御网络中的威胁进行监控、响应、学习和应用知识的过程

积极防御

发现有针对性攻击或者未知的攻击面、防御弱点

收集数据，将数据利用转化为情报，并将信息生产加工

情报

对对手有足够的了解，产生针对性的情报

对抗攻击者进行法律反制措施、自卫反击行为

进攻

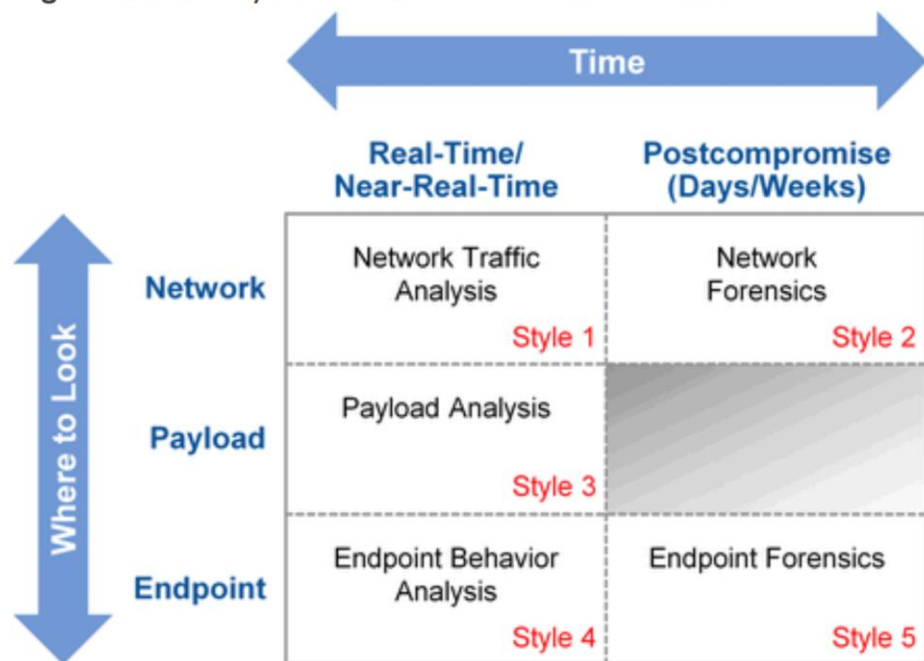
威慑与反制

安全态势感知

关键要素——全天候、全方位

1. 基于流量特征的实时检测；
(WAF、IPS、NGFW等)
2. 基于流量日志的异常分析机制；
(流量传感器、Hunting、UEBA)
3. 针对内容的静态、动态分析机制；
(沙箱)
4. 基于终端行为特征的实时检测；
(ESP)
5. 基于终端行为日志的异常分析机制；
(EDR、Hunting、UEBA)

Figure 1. Five Styles of Advanced Threat Defense



Source: Gartner (August 2013)

态

全局角度看到的现状

1. 是真实的攻击吗，是否可能误报，是否把扫描识别为真实攻击？
2. 是什么性质的攻击，定向或者随机？
3. 可能的影响范围和危害？
4. 缓解或者清除的方法及难度？
5. 重要的事件都体现出来了吗？

势

未来可能的事件或状态

基于情报分享和情报分析

1. 是新的攻击团队还是已知团伙；
2. 攻击者的意图；
3. 攻击者的技战术水平及特点；
4. 是否属于一次大型战役的一部分；

PALANTIR 的观点

1. THE DATA COMES FROM MANY DISPARATE SOURCES
2. THE DATA IS INCOMPLETE AND INCONSISTENT
3. YOU' RE LOOKING FOR SOMEONE OR SOMETHING THAT DOESN' T WANT TO BE FOUND, AND THAT CAN ADAPT TO AVOID DETECTION.

误判与机器学习



- 传统侦测误判率
 - 1/10,000,00
- 机器学习误判率
 - 1/1,000 ~ 1/10,000
- 扫描计算机里的所有档案?
 - 1只恶意软件VS 20,000个良性软件 → 1正判/2~20误判
- 扫描所有的下载文件?
 - 1只恶意软件VS 100个良性软件 → 1正判/0.1~0.01误判

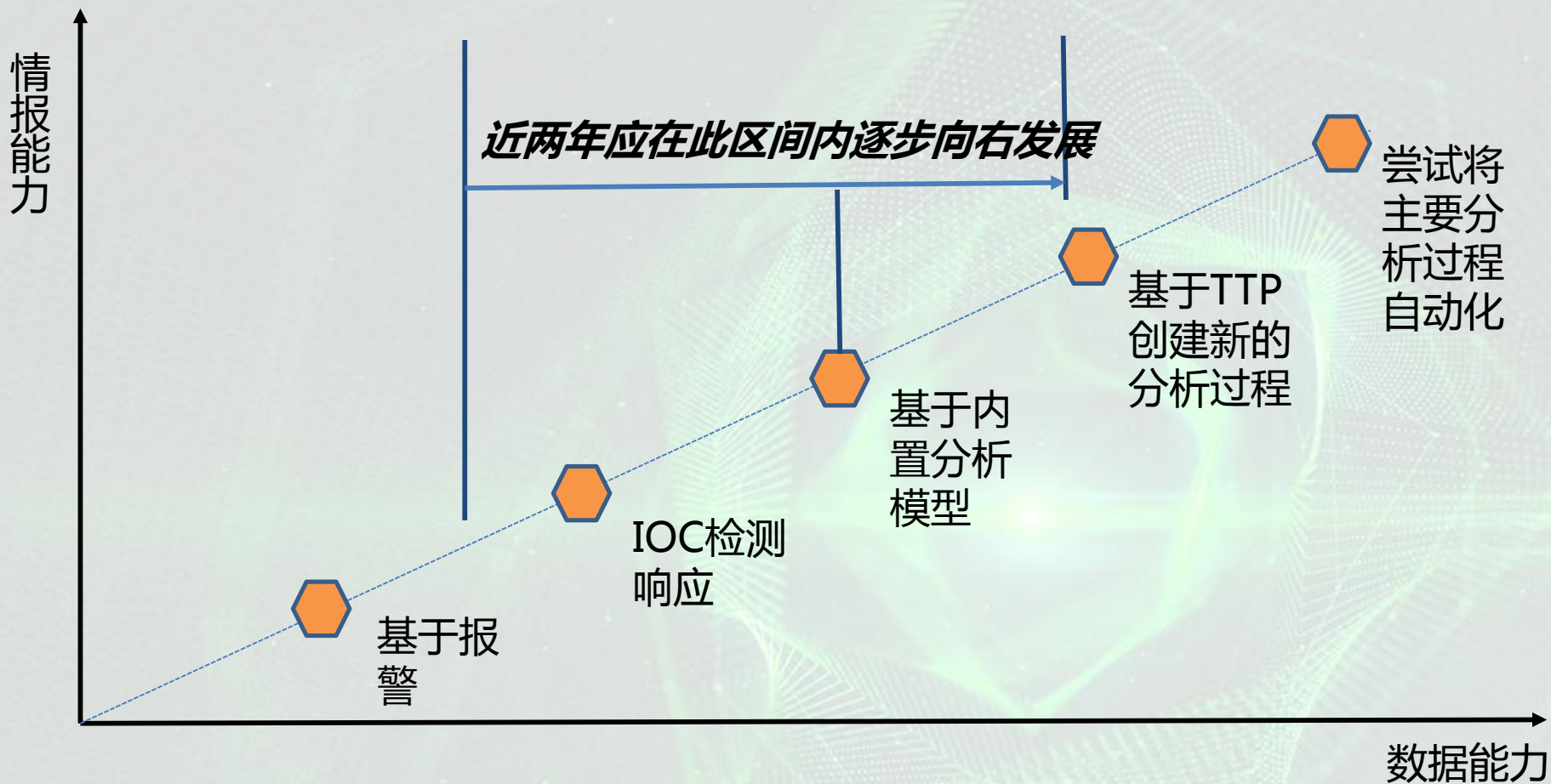
关键技术分析



中国互联网安全大会



360互联网安全中心





中国互联网安全大会



360互联网安全中心

目录

态势感知

威胁情报

小结

威胁情报

- 检测中的作用
- 事件响应中的作用
- 预警、预防

- **失陷检测情报**

有关APT事件、木马后门、僵尸网络、黑客工具使用的远控服务器信息

- **文件信誉**

利用云端更多检测机制对文件的综合判定信息，包括是否恶意、恶意类型、家族信息、C2地址等

- **IP信誉**

已知恶意IP（扫描、撞库等）、IP白名单（不同类型的网关）、IP的上下文（事件历史、开发端口、OS、应用、基本属性等）

响应环节的威胁情报——威胁分析平台



报警研判

360威胁情报中心

web.thoitetvietnam.org

Q

简体中文

👤

web.thoitetvietnam.org

APT CVE-2012-0158 RTF

流行度☆☆☆☆☆

动态域名否

隐私保护是

白名单否

创建时间2016/07/25

更新时间2017/03/14

过期时间2019/07/25

最近看到2017/09/01

相关安全报告:

没有数据

高级可视化分析

威胁情报 3

域名解析 6

注册信息 2

关联域名 4

定制搜索

开源情报

情报源	最近看到	威胁类型
OSINT	2017/08/29	MALWARE SITE
SKYEYELABS	2017/06/09	C2

相关样本

样本HASH	最早看到	最近看到	恶意类型	家族信息
FD95AC4545273B0AA1D87EDFB9251B2C	2017/08/22	2017/08/23	黑市工具	RTF-0BFSSTRM

关联URL

没有数据

可视化分析

域名: web.thoitetvietnam.org

响应环节的威胁情报——威胁分析平台



中国互联网安全大会



360互联网安全中心

攻击定性

360威胁情报中心

songdenghui.6655.la

Q

简体中文

songdenghui.6655.la

威胁情报 3 域名解析 3 注册信息 4 关联域名 100+ 定制搜索

PIGEON

开源情报

恶意家族

恶意类型

远控木马

风险等级

影响平台

Windows

其他名称

Huigezi

描述

Pigeon是一种运行于Windows系统下的恶意程序，是国内一款著名后门。灰鸽子客户端和服务端都是采用Delphi编写。服务端对客户端连接方式有多种，使得处于各种网络环境的用户都可能中毒，包括局域网用户（通过代理上网）、公网用户和ADSL拨号用户等。

细节：

- 1.将自身拷贝到Windows目录下(C98/xp下为系统盘的windows目录，2000/NT下为系统盘的Winnt目录)
- 2.释放G_Server.dll和G_Server_Hook.dll到windows目录下，G_Server_Hook.dll负责隐藏灰鸽子。
- 3.通过截获进程的API调用隐藏灰鸽子的文件、服务的注册表项，甚至是进程中的模块名。截获的函数主要是用来遍历文件、遍历注册表项和遍历进程模块的一些函数。
- 4.释放出一个名为G_ServerKey.dll的文件用来记录键盘操作。

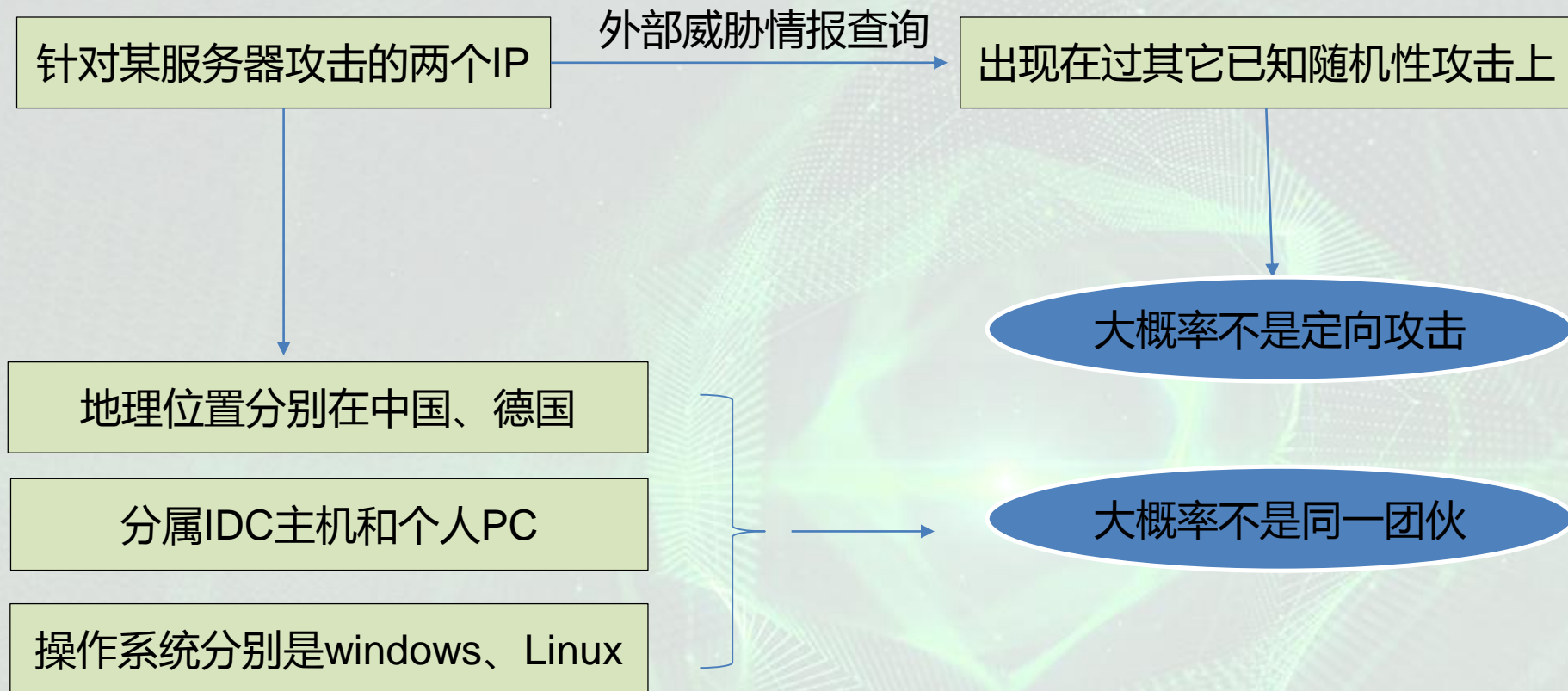
产生的威胁：

- 1.盗号、键盘记录器等手段记录用户
- 2.远程控制用户电脑上的摄像头偷窥用户隐私
- 3.敲诈，下载隐私文件敲诈
- 4.发展“肉鸡”，攻击者可控制大量“肉鸡”，进行非法获利。比如在“肉鸡”上植入点击广告的软件；利用肉鸡配置代理服务器，以此做为跳板对其它电脑发起入侵。一旦最终受害者追查时，肉鸡电脑将会成为替罪羊；此外，还可以用大量肉鸡组建僵尸网络，随时可以被用于一些特殊目的，比如发起DDoS攻击等。
- 5.盗取商业机密
- 6.间断性骚扰感染灰鸽子病毒后，远程攻击者控制用户电脑，比如任意打开和关闭文档，远程重启电脑
- 7.破坏修改注册表、删除重要文件、修改共享、开启代理服务器、下载病毒等等

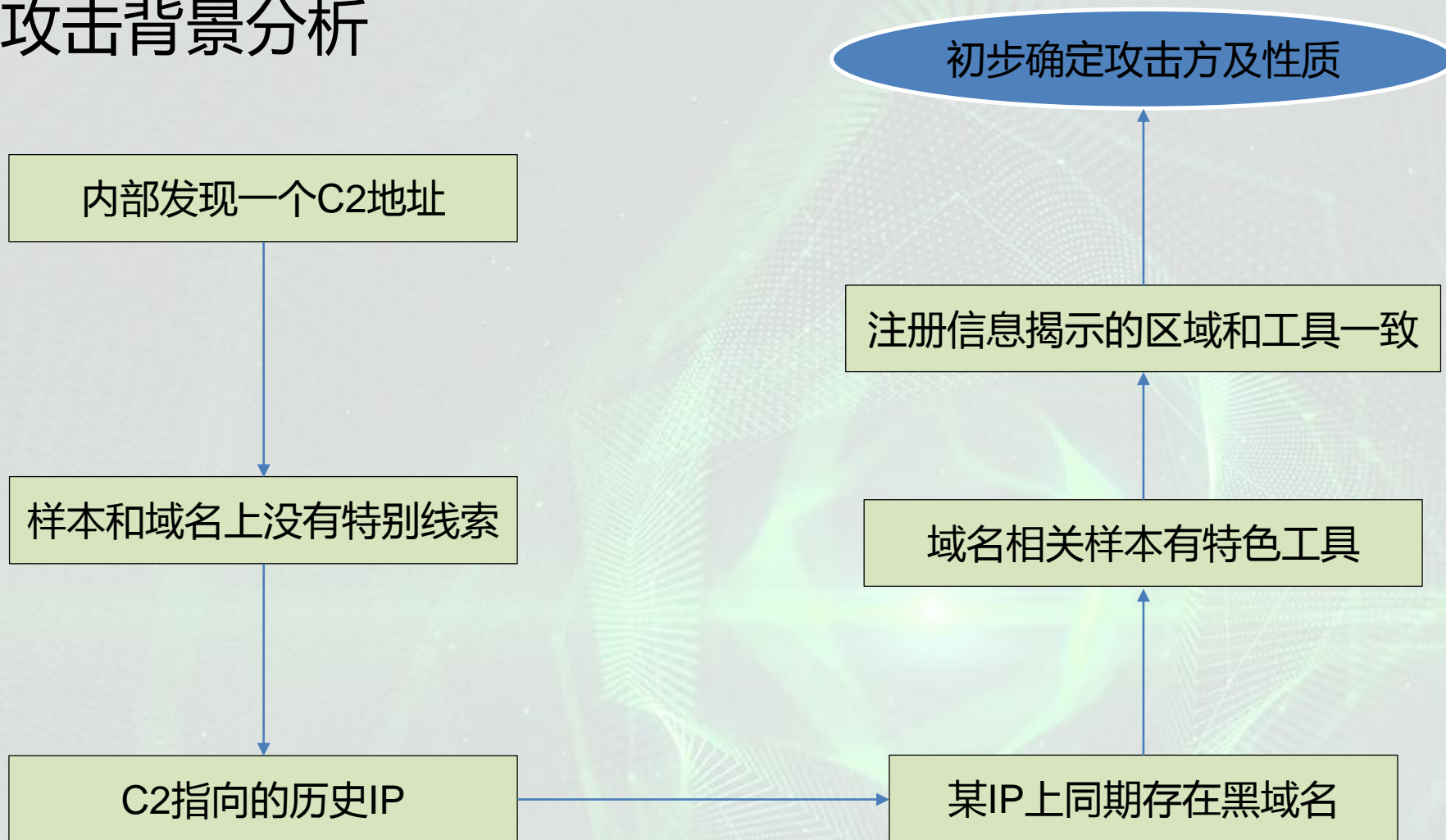
参考链接

<http://boike.baidu.com/view/812460.htm>
<http://tech.163.com/07/0316/00/39LR00SV000917H1.html>

攻击优先级分析

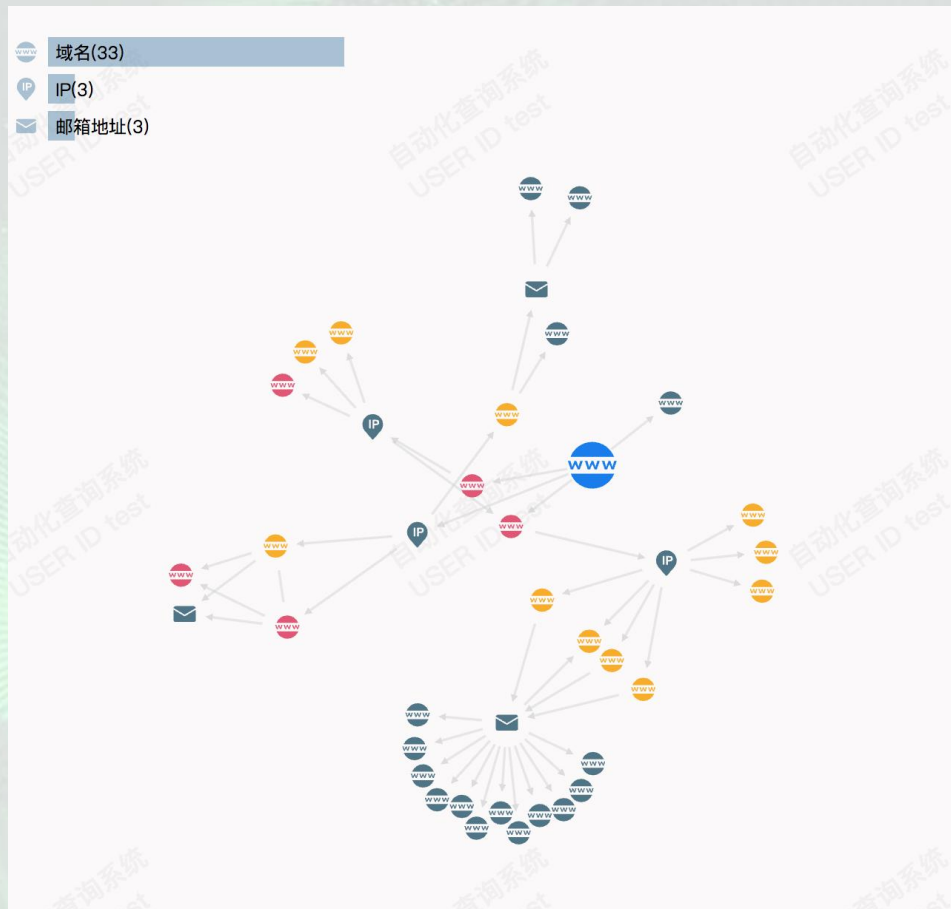


攻击背景分析



自动化关联分析演示

[https://ti.360.net/analyse?type=domain&value=web.t
hoitietvietnam.org](https://ti.360.net/analyse?type=domain&value=web.t
hoitietvietnam.org)



- 攻击事件分析 / 预警
- 恶意样本分析 / 预警
- 漏洞分析建议 / 预警
- 关键性内容：
 1. 危害
 1. 影响范围
 2. 机制
 3. 检查和防范措施

Xshell事件

FireBall 事件

供应链安全分析报告

威胁情报全景



中国互联网安全大会



360互联网安全中心

运营情报TTP

- 攻击事件分析 / 预警
- 恶意样本分析 / 预警
- 漏洞分析建议 / 预警



战术情报

- IOC
 - IP信誉
 - 文件信誉
- 威胁分析平台

- 威胁分析平台

威胁情报是现阶段保障态势感知项目实效，最有力的工具

多种类型的威胁情报保障安全生命周期全过程

关联分析平台的作用不仅是攻击溯源，可以通过多种方式对攻击进行定性分析

研究类网站：[HTTPS://TI.360.NET/BLOG/](https://ti.360.net/blog/)

分析平台：[HTTPS://TI.360.NET](https://ti.360.net)

微信公众号:360威胁情报中心



谢 谢



中国互联网安全大会



360互联网安全中心