KCon

2019

物联网资产变化研究

演讲人：桑鸿庆
绿盟科技 资深安全研究员

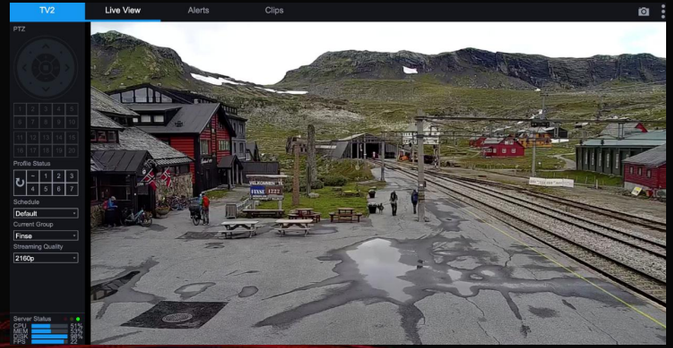
目录

CONTENTS

PART 01

网络空间引擎与物联网资产识别简介

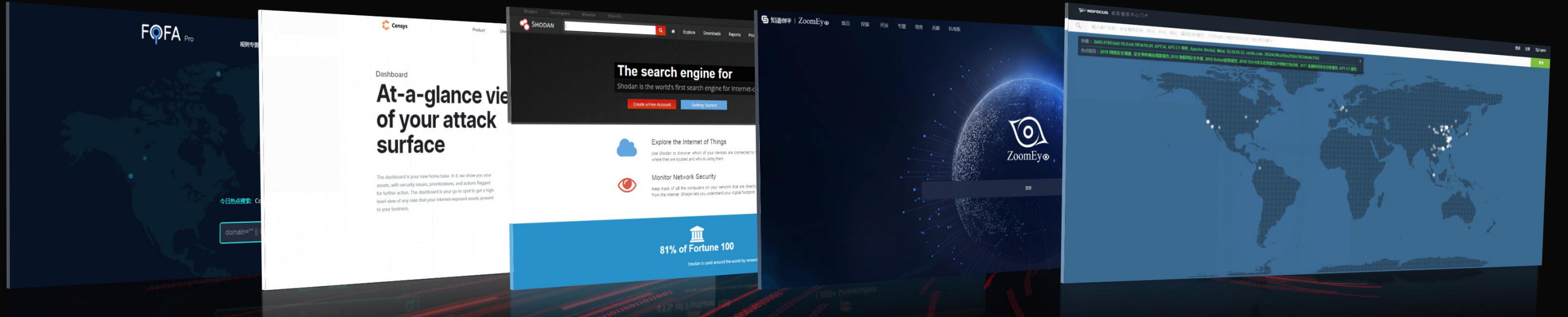
《唐人街探案2》中片段



挪威 Finse 1222酒店

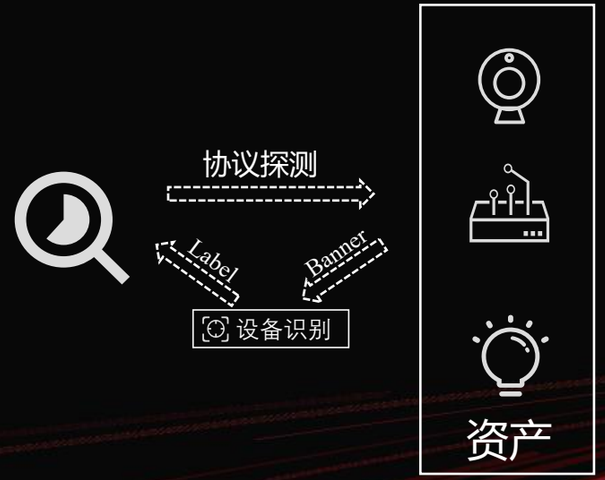
图片来源于网络

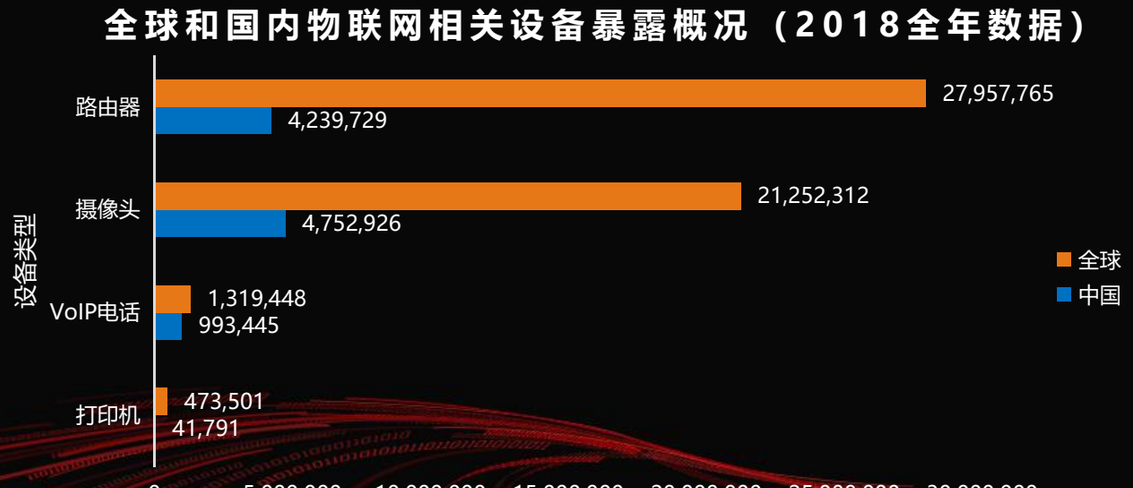
网络空间搜索引擎


FOFA Pro
Censys
Dashboard
At-a-glance vie
of your attack
surface
SHODAN
The search engine for
Shodan is the world's first search engine for Internet-
Create a Free Account
Getting Started
Explore the Internet of Things
Monitor Network Security
81% of Fortune 100
ZoomEye
NSFOCUS

物联网资产暴露概况

资产发现过程

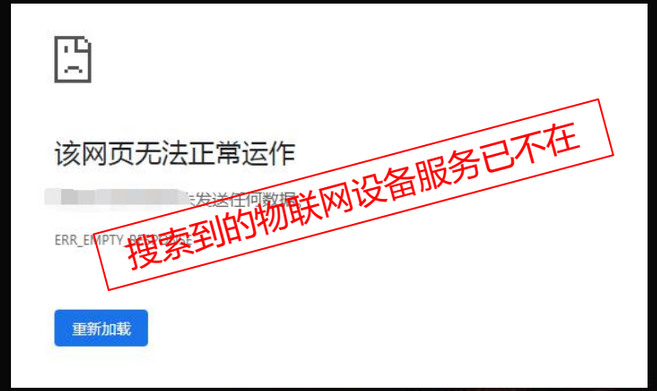


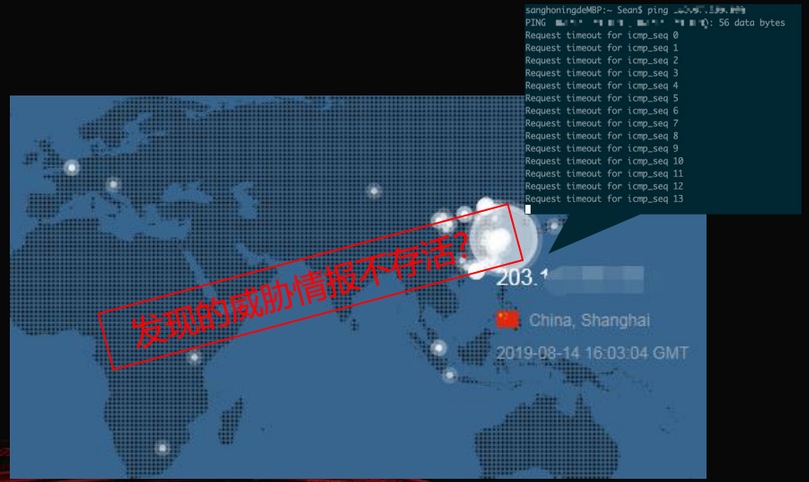


Mirai变种仍然在活跃的发动攻击

利用路由器和摄像头的反射攻击事件飙升

图片来源于网络


该网页无法正常运作
:发送任何数据。
ERR_EMPTY_RESPONSE
重新加载
搜索到的物联网设备服务已不在


sanghongdeMBP:~ Sean$ ping
PING : 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
Request timeout for icmp_seq 10
Request timeout for icmp_seq 11
Request timeout for icmp_seq 12
Request timeout for icmp_seq 13
203.
China, Shanghai
2019-08-14 16:03:04 GMT
发现的威胁情报不存活?

一起攻击事件感染范围真有这么大？

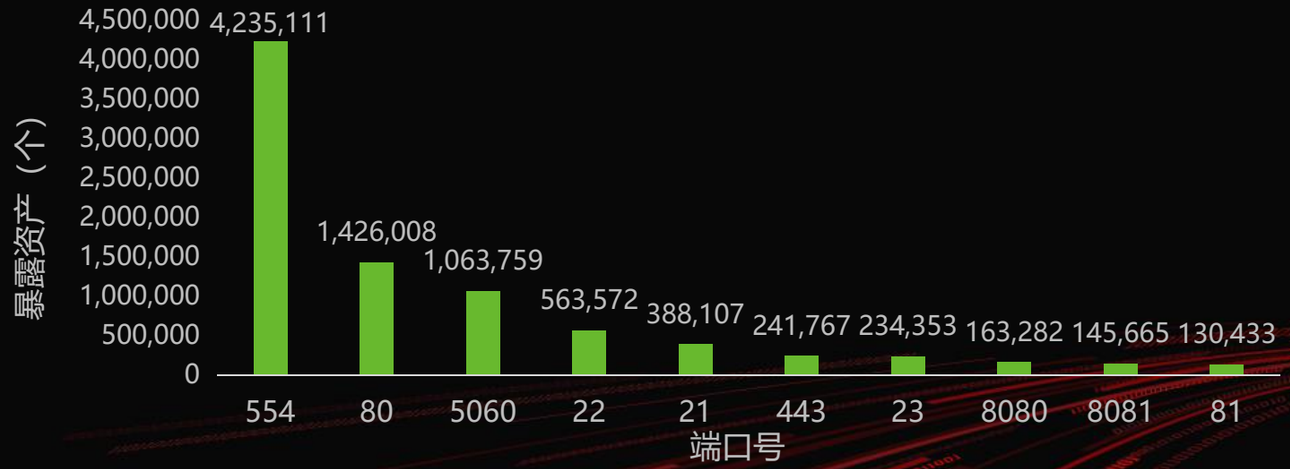
为什么大量服务、威胁情报不存活?

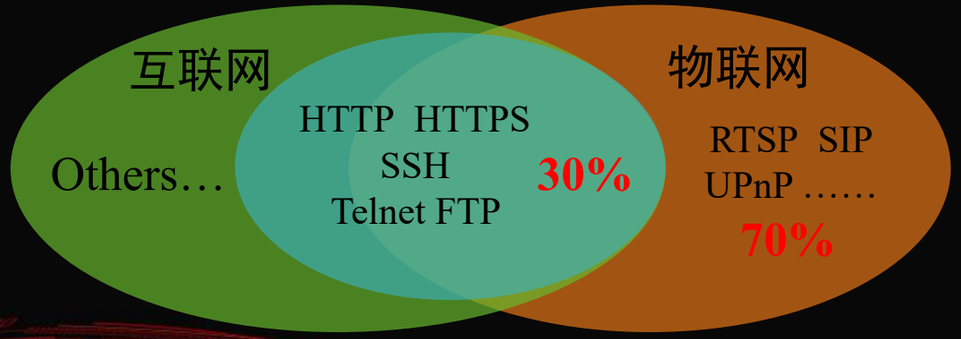
暴露数量真的是这样的吗？

PART 02

国内物联网资产IPv4网络地址变化情况

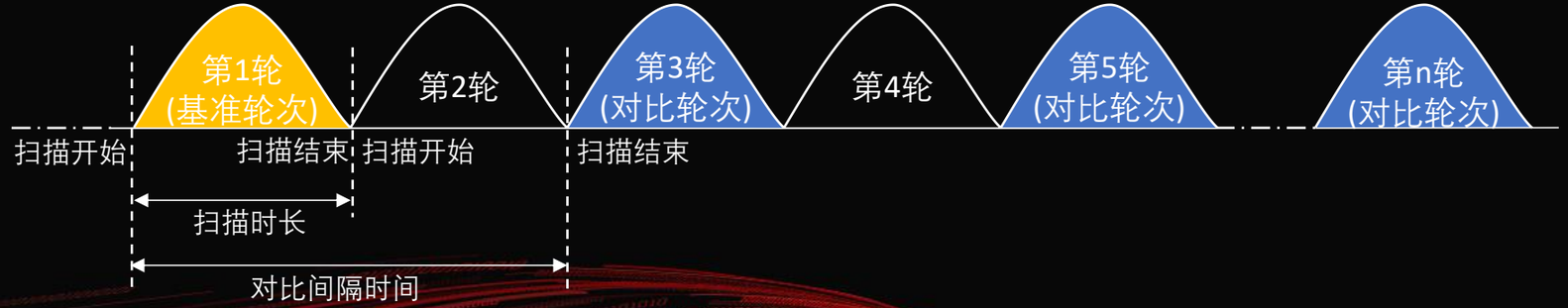
国内物联网资产暴露的端口及协议分布情况





国内暴露的物联网资产协议分布情况

基于多轮扫描结果对比的资产变化研究方法

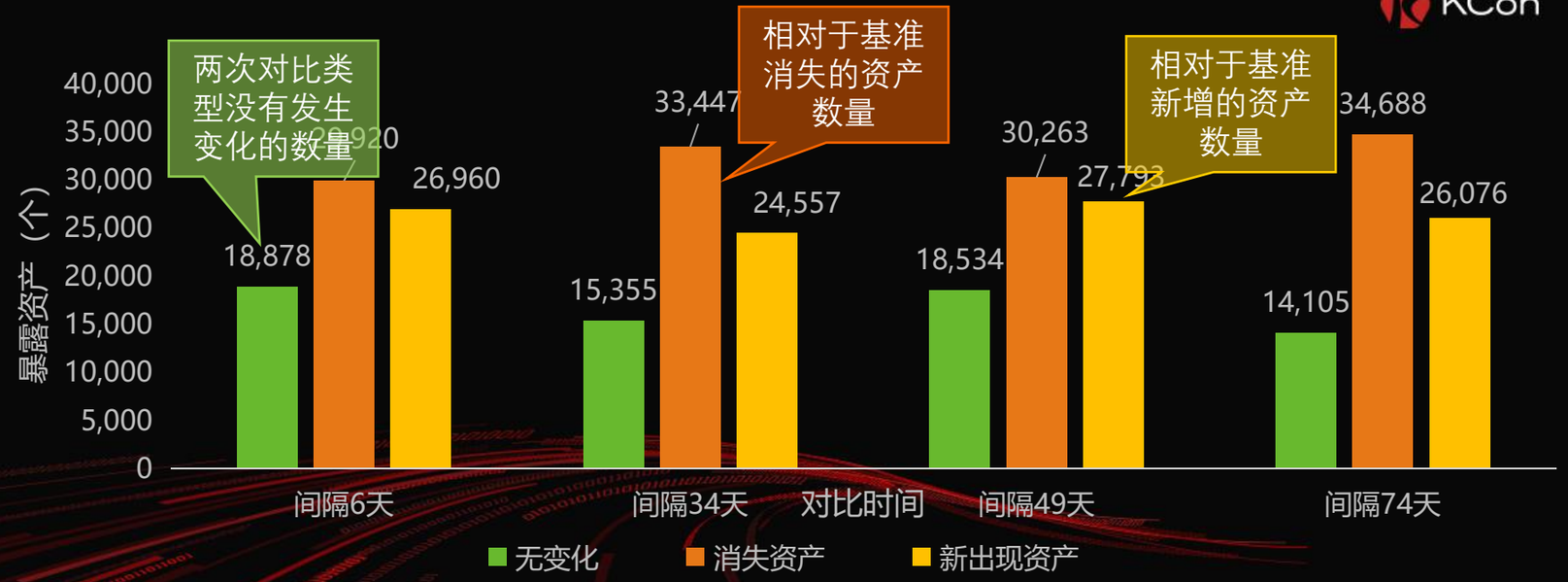


路由器变化情况

80端口路由器

- 平均扫描周期3天
- 总量约5万

◆ 变化的资产数量相对稳定， 约有**3.3**万路由器网络地址发生过变化，约占总量的**68%**

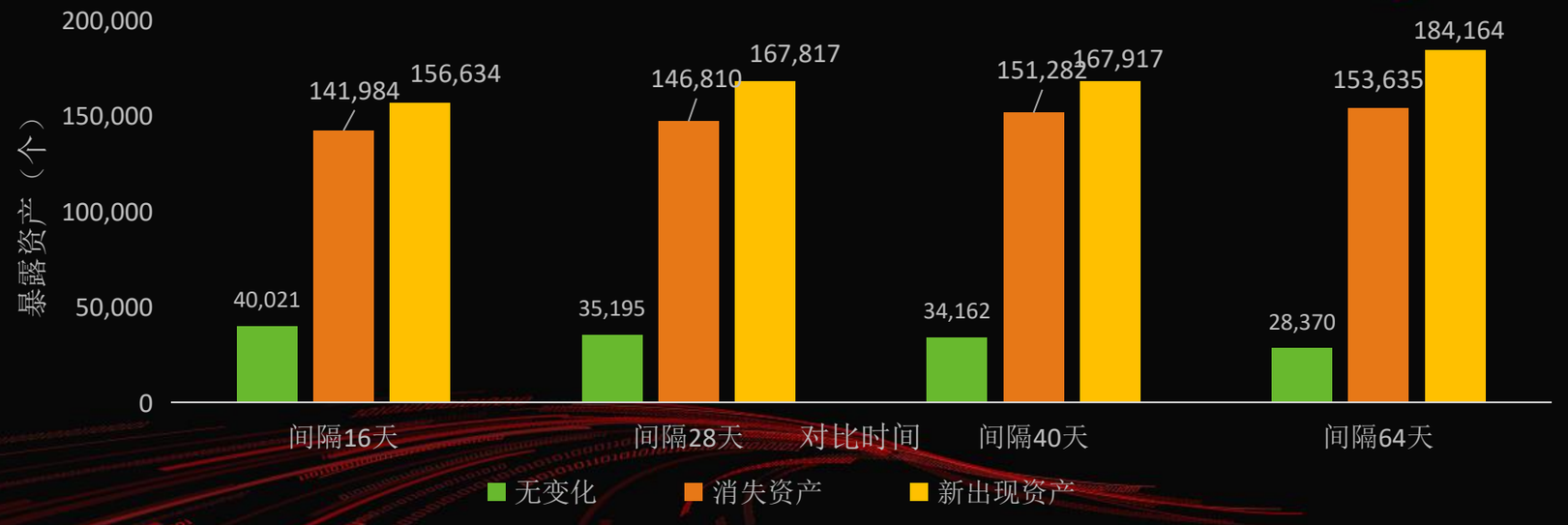


VoIP电话变化情况

5060端口VoIP电话

- 平均扫描周期3天
- 总量约18万

◆ 变化的资产数量相对稳定， 约有**15**万VoIP电话网络地址发生过变化，大约占总资产量的**80%**

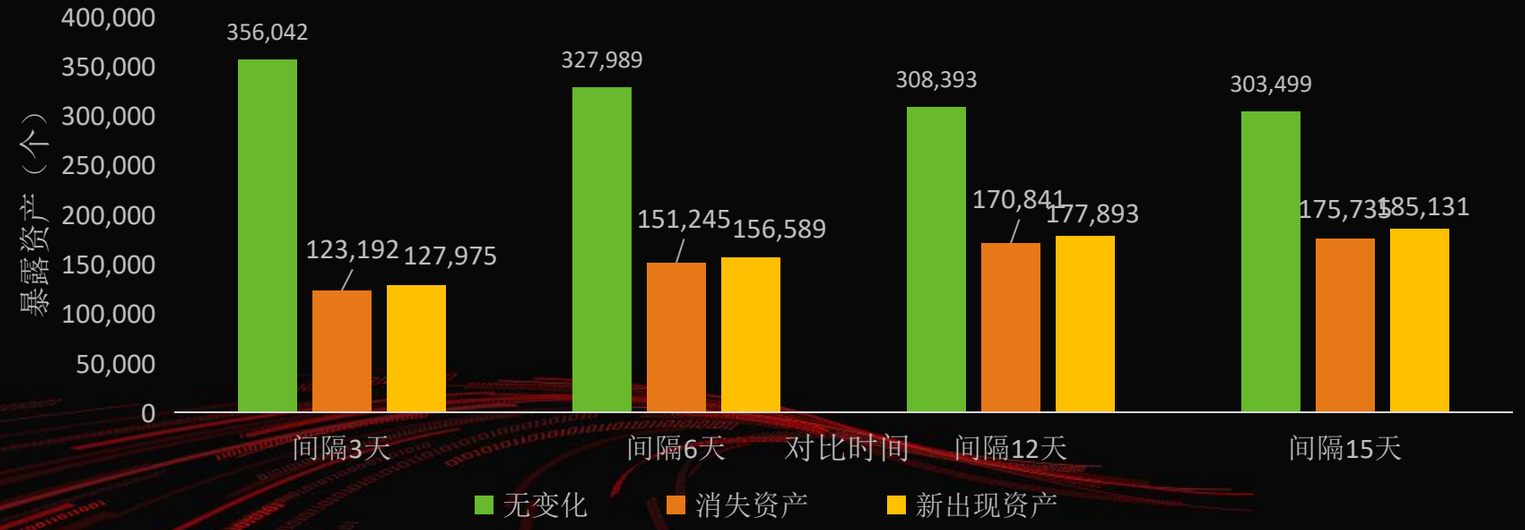


摄像头变化情况

554端口摄像头

- 平均扫描周期3天
- 总量约47万

◆ 约有**15**万摄像头网络地址发生过变化，占总资产量的**25%**



观察发现： 互联网上的暴露物联网资产网络地址，根据类型的不同均存在着不同程度的变化，并且新增和消失的数量几乎平衡，变化量随着时间的推移缓慢递增

80 %

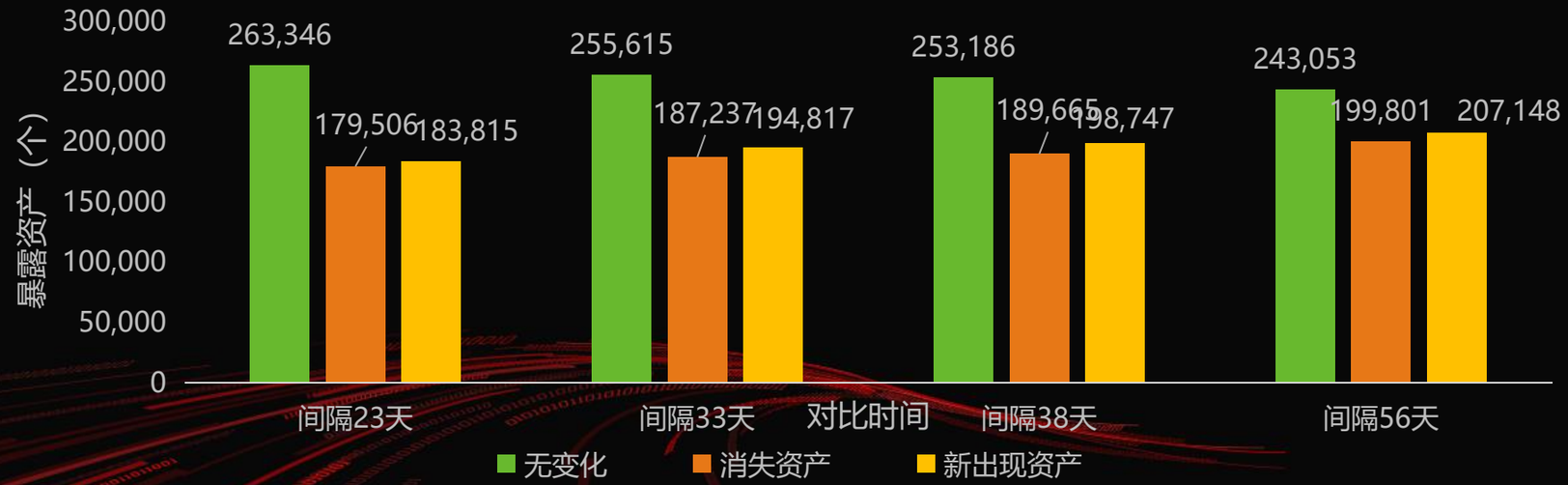
68 %

25 %

摄像头变化情况（平均扫描周期增加到7天）

554端口摄像头

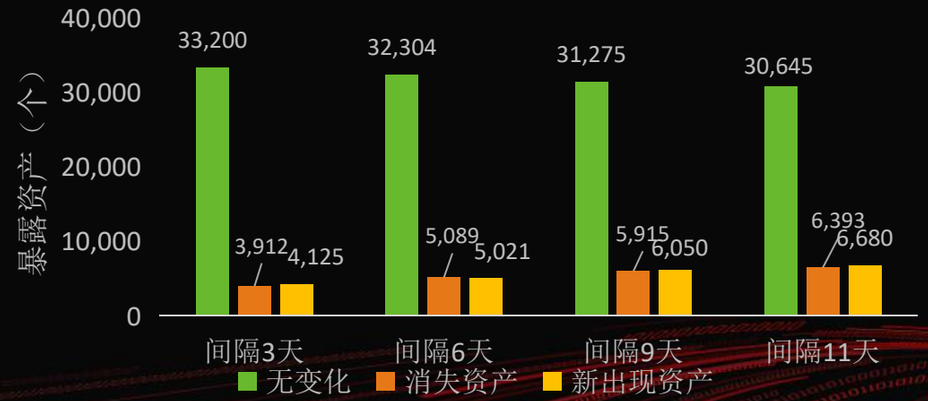
- 扫描周期增加到7天
- 增加平均扫描周期，相比之前间隔3天，资产的变化量45%，相比之前3天扫描周期增加20%；但有24万资产，间隔56天未发生变化



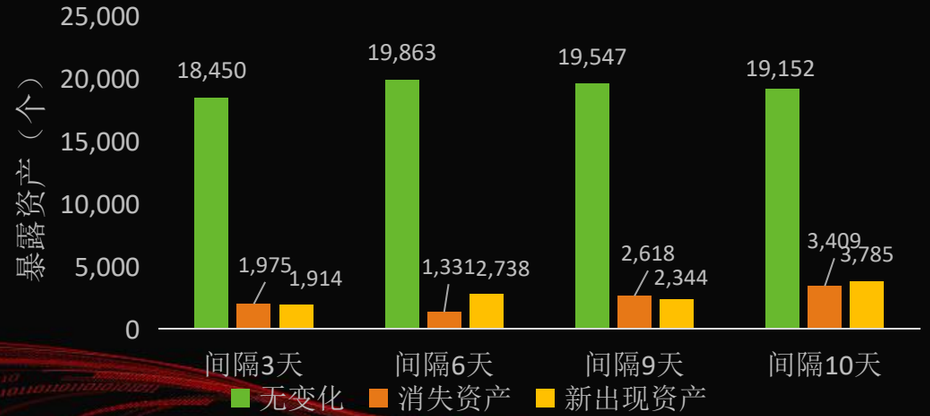
观察发现：在一定范围内，缩短国内资产平均扫描周期，可以减少资产变化数量；同样有一部分物联网资产地址在观测时间内一直都没有变化

亚太地区物联网资产变化并不明显

对比于国内，日本和新加坡的资产变化比例明显小的多，仅有不到15%的资产在变化



日本554端口摄像头变化情况



新加坡554端口摄像头变化情况

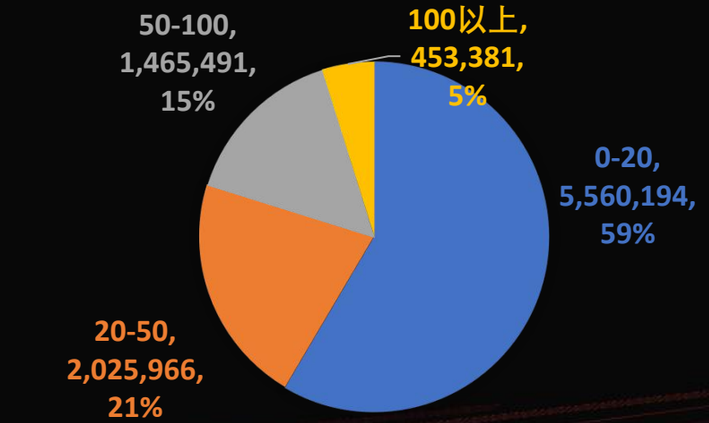
PART 03

资产网络地址变化原因分析

关于资产变化的猜想

猜想1：物联网资产的网络地址变更，导致我们看到的资产变化
猜想2：网络地址变化可能在一定范围内，并且有可能和运营商相关

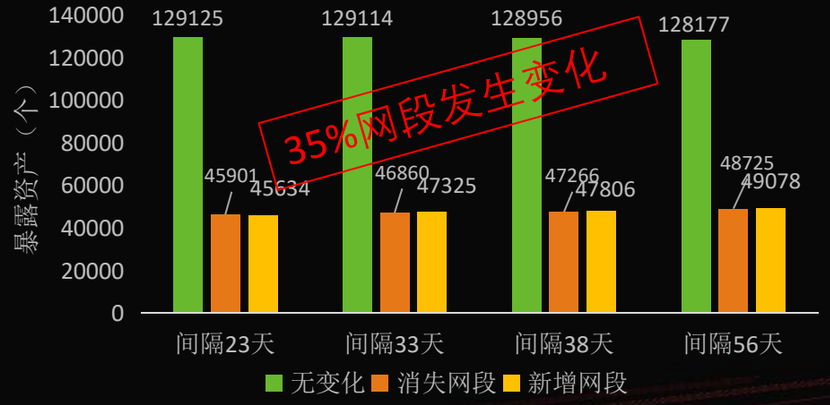
分布在同C段映射的物联网资产统计



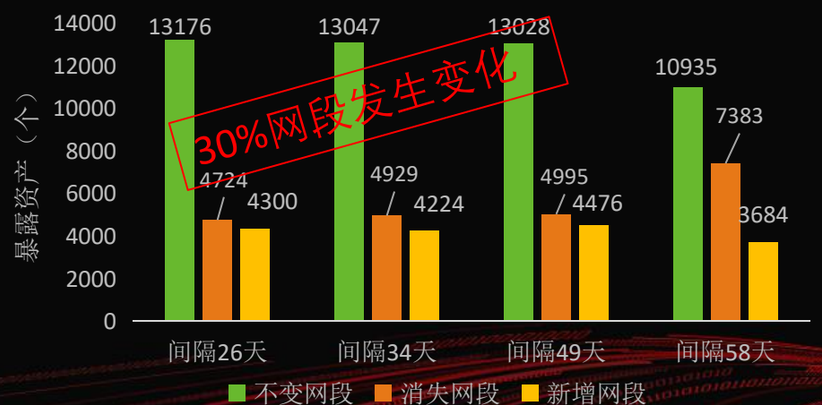
累计2个月物联网设备IP分布在同网段的数量统计

发现：同一网段物联网资产数量大于20的资产数量占总量的41%

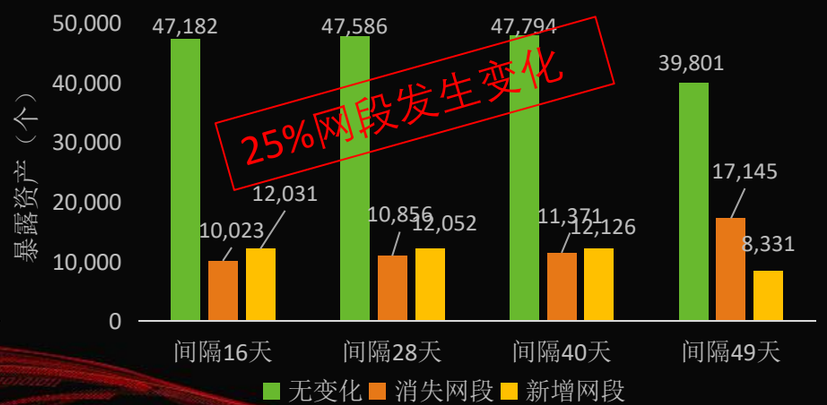
资产C段映射变化明显下降



554端口的摄像头



80端口的路由器

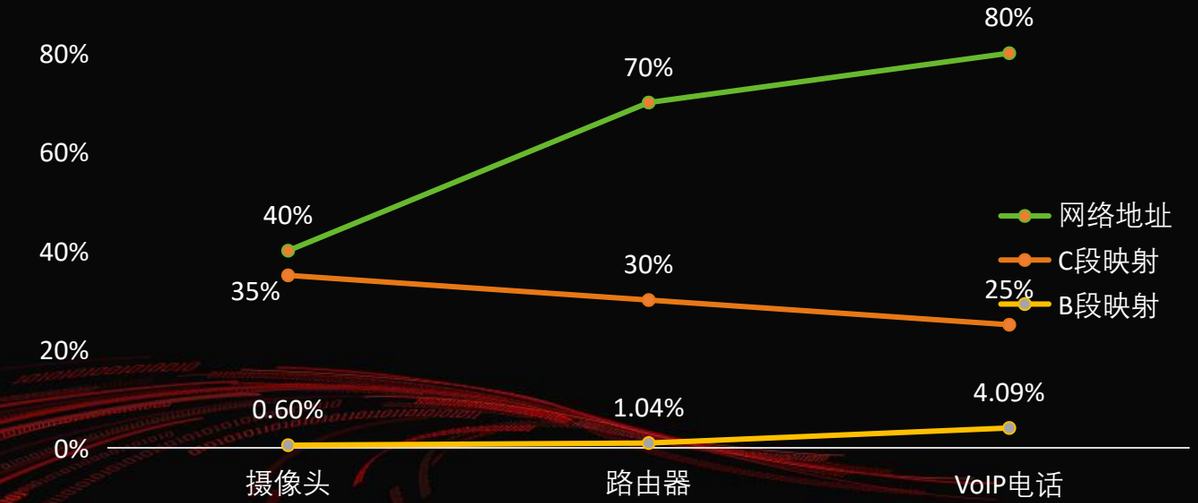


5060端口VoIP电话

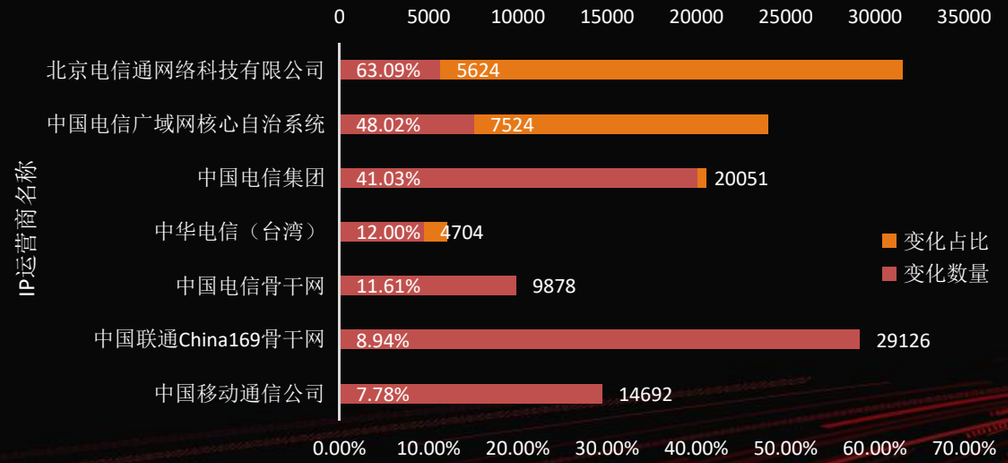
物联网资产地址变化与网段变化对比

发现： 物联网资产网络地址在一定网段内变化

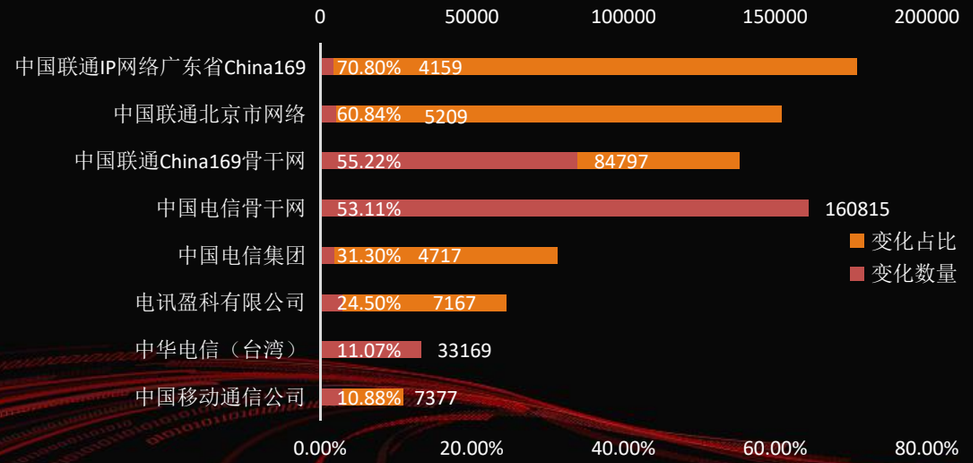
结论： 运营商采用的动态分配地址的策略导致物联网资产网络地址变化



网络地址变化资产的运营商分布情况



554端口摄像头变化资产ASN分布情况



80端口路由器变化资产ASN分布情况

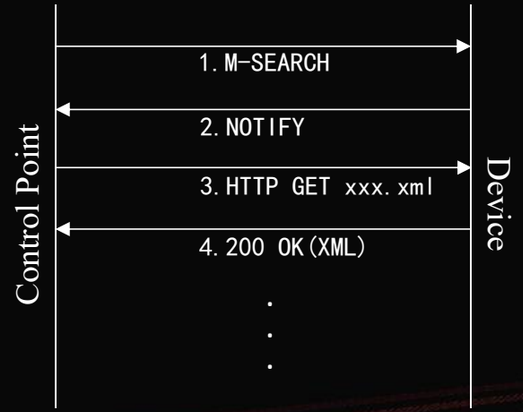
PART 04

IPv6 物联网资产网络地址变化情况

IPv6网络地址探测的困难性

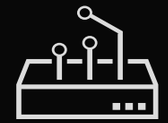
- IPv6地址数量是IPv4的2^96倍，IPv6可以地球上每一粒沙分配一个IP，而且还有剩余
- 目前IPv6地址使用的实际数量较少，并且地址分布的随机性较大
- 通过对全网扫描发现IPv6资产，从时间和资源上都不切实际

利用UPnP发现双栈物联网资产



UPnP工作流程

```
NOTIFY * HTTP/1.1
Host:239.255.255.250:1900
 Cache-control:max-age=1800
Location:http://[{{our_ipv6}}]/?{{target_ipv4}}
Nt:upnp:rootdevice
Nts:ssdp:alive
Usn:uuid:{uuid} ::upnp:rootdevice
```



IoT Devices

HTTP GET
404

```
2806:105e:8:92f5:bead:28ff:fee0:**** - -
[02/Aug/2019:13:53:17 +0800]
"GET /?189.142.**.*** HTTP/1.1" 404 177
"-" "Linux/3.0.8, UPnP/1.0,
Portable SDK for UPnP devices/1.6.18"
```

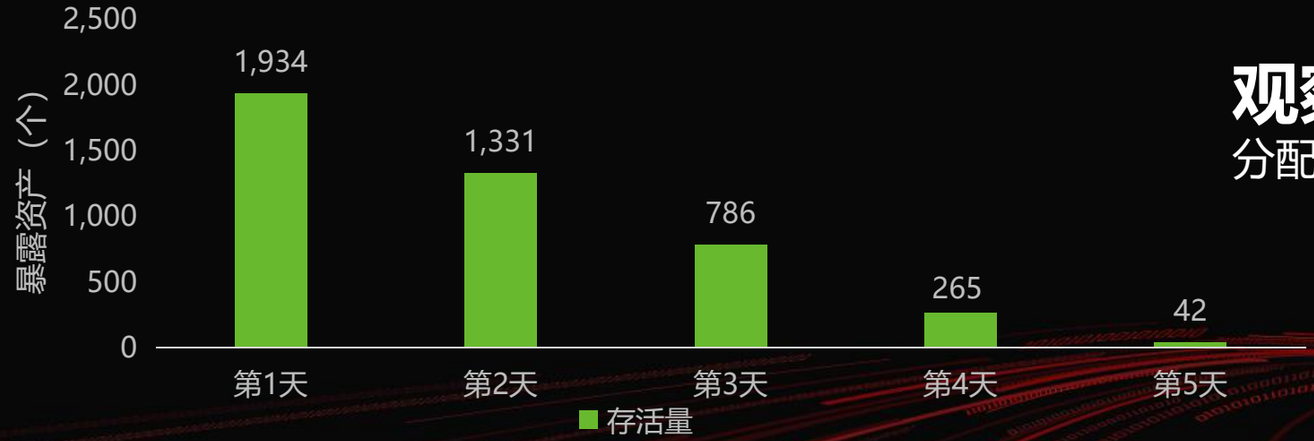
引用Cisco，Talos 实验室发表的文章
“IPv6 unmasking via UPnP“

Scanner

Nginx WEB IPv6

利用UPnP发现IPv6物联网资产

UPnP发现的IPv6资产存活情况



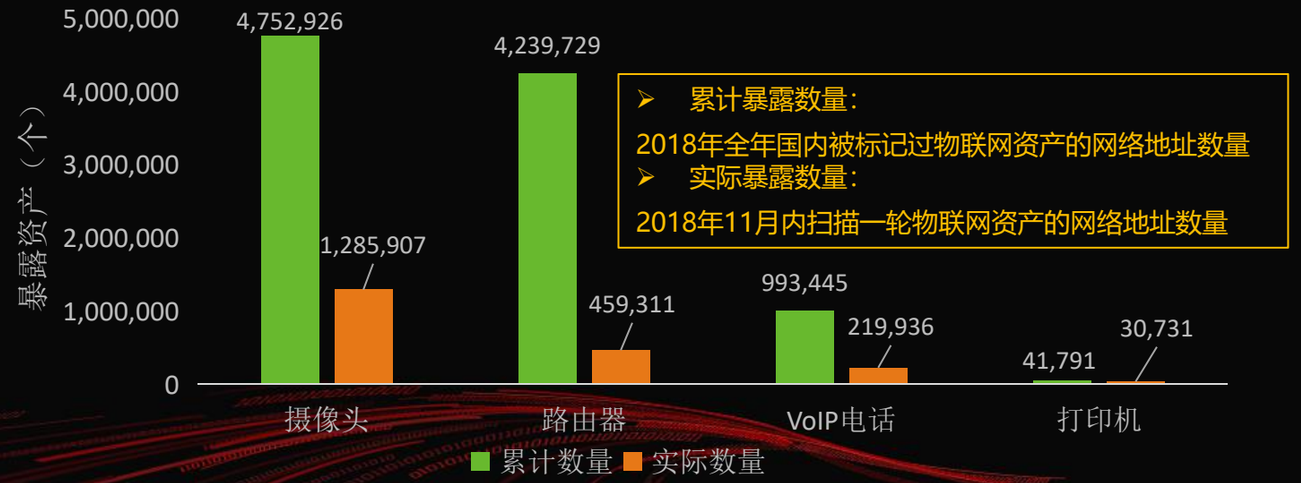
观察发现： 同样有部分IPv6地址采用动态的分配策略，资产的网络地址也在变化

PART 05

物联网资产网络地址变化影响

暴露资产数量

累计的暴露资产数据和真实暴露数量相差甚远，根据实际的业务场景来使用两者数据



资产信息准确性

资产的扫描间隔应该保证在尽可能短的时间内
并及时对历史物联网资产数据及时做老化，
不变和变化的资产差异对待
才能保证资产库的准确性

物联网威胁跟踪

良好的数据和情报是提供有效网络搜索能力的关键

所以在攻击溯源时，应考虑资产历史变化情况，

如果资产或情报处于动态分配网段，可使用网段映射进行粗粒度匹配

这样才能提高威胁跟踪的精准性

回顾

- 互联网上的暴露物联网资产网络地址，根据类型的不同均存在着不同程度的变化
- 运营商采用的动态分配地址的策略导致物联网资产网络地址变化
- 考虑物联网资产变化，可以提高资产信息和威胁跟踪精准性

一些说明

- 以上研究基于2018-2019年资产扫描数据
- 目前得出的资产变化原因，均为从真实数据的推测得出
- 物联网资产具体的变化范围，还需要与运营商实际配置策略相结合
- 获取IPv6物联网资产尚存巨大挑战，有待进一步研究

关于我们

◆ 绿盟科技创新中心

绿盟科技的前沿技术研究部门。包括云安全实验室、安全大数据分析实验室和物联网安全实验室，关注于云安全、威胁情报、数据驱动安全和物联网安全等领域。

绿盟科技研究通讯

KCon

KCon 2019 無界

谢 谢 观 看

演讲人：桑鸿庆

绿盟科技创新中心 资深研究员