KCon

2019

知道创宇404实验室发布

打造世界领先网络空间测绘能力

演讲人：

heige@0x557
hei@knownsec.com

目录
CONTENTS

01 PART 01 Xmap 2.0 发布

02 PART 02 节点分析

03 PART 03 ZoomEye“5000节点计划”

04 PART 04 IPv6 测绘

05 PART 05 ZoomEye全球蜜罐识别

两个关键

- 获取更多数据
- 赋予数据灵魂

“探测资源及技术已经成为网络空间测绘的核心竞争力！”

–heige

PART.01

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.

Xmap 2.0 发布

Xmap 2.0 发布

- Xmap是ZoomEye核心探测引擎（IP）

- IP探测引擎的疼点

a. 单一追求速度，而忽略了效果

b. 速度快意为着高并发，同时意味着高丢包

c. 扫描节点IP被拦截、拉黑

Xmap 2.0 发布

- 效果平均每月提升了6.4倍的数据量
- 一键部署安装，给500节点计划打下基础

KCon

PART.02

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.

节点分析

Shodan节点分析

- Shodan 现有节点分析

a. 2019.03 fdns/rdns记录提取去重外网ip数：131个
b. 其中带”census“的记录提取去重外网ip数：77个
c. 集中分布在荷兰、法国、罗马尼亚、美国、冰岛等

- 从某些端口扫描行为推测Shodan可能存在通过某些代理池技术进行扫描

Censys节点分析

- Censys 现有节点分析

a. 2019.03 fdns/rdns记录提取去重外网ip数：406个
b. 其中带”worker”的记录提取去重外网ip数：304个
c. 主要集中在198.108.66.*/198.108.67.* [“美国","密歇根州","","","merit.edu"]

- 2019.03 从某些端口扫描行为分析发现活动ip数：86个

PART.03

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.

ZoomEye“500节点计划”

ZoomEye“500节点计划”

- 基于最新Xmap 2.0架构
- 目前部署约200个节点，将扩充到500个节点
- 节点分布广泛：美国，日本，新加坡，泰国，俄罗斯，印度等

“多维度的数据关联才能得到更丰满的数据灵魂”

–heige

PART.04

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.

IPv6 测绘

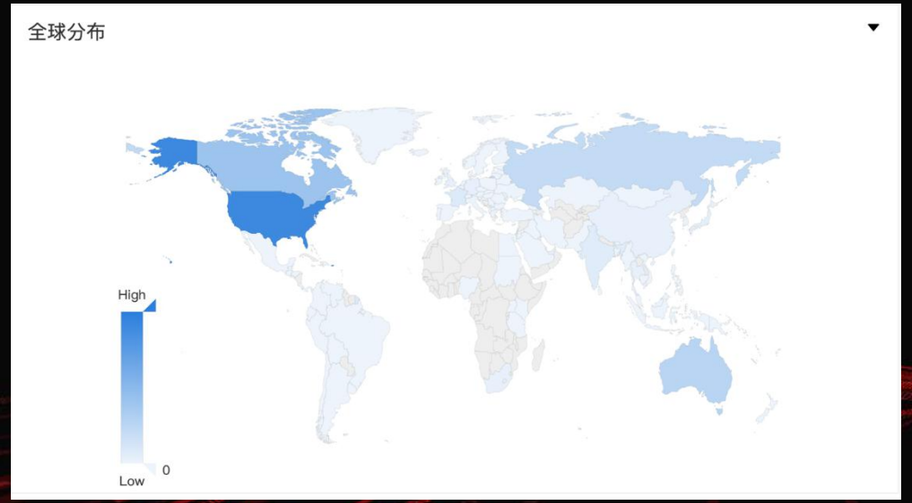
IPv6 测绘

- 域名 —> IPv4 — > 暗网 — > IPv6
- 目前接近1亿的IPv6地址库，最近平均每周增加7万
- 数据合作+自主爬虫
- 探测引擎Xmap -IPv6版

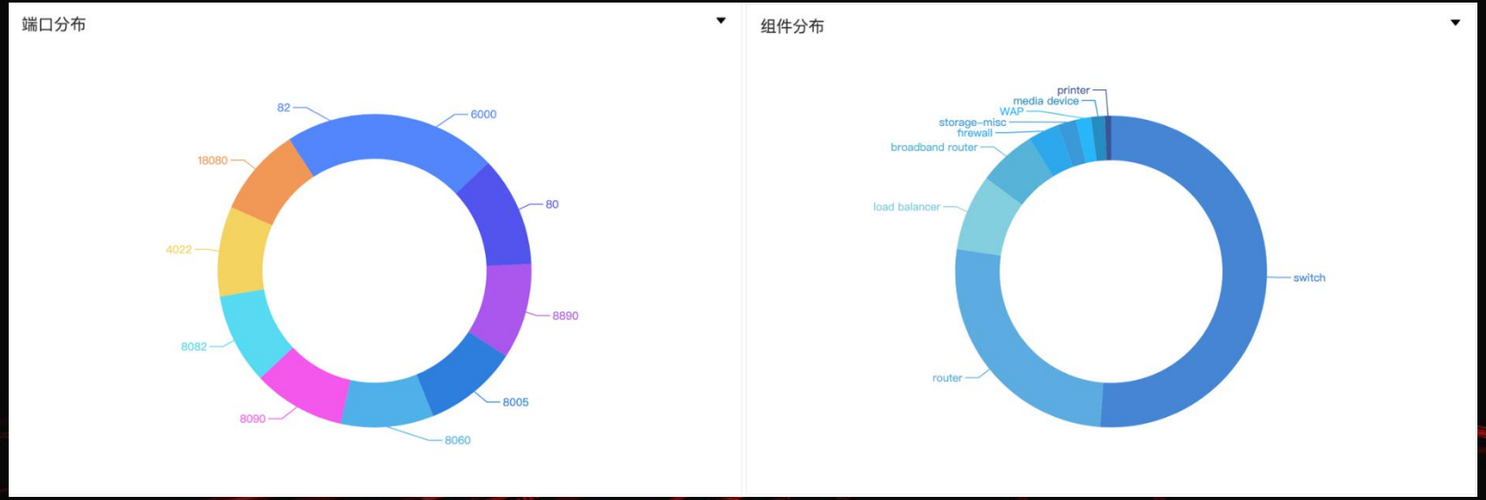
a. 支持所有ZoomEye IPv4的端口协议

b. 平均每周增加约200w条数据（跟节点资源投入相关）

IPv6 测绘



IPv6 测绘


端口分布
82
6000
18080
80
4022
8890
8082
8005
8090
8060
组件分布
printer
media device
WAP
storage-misc
firewall
broadband router
load balancer
switch
router

“蜜罐部署 vs 蜜罐识别—>网络空间测绘领域的主要对抗面”

–heige

PART.05

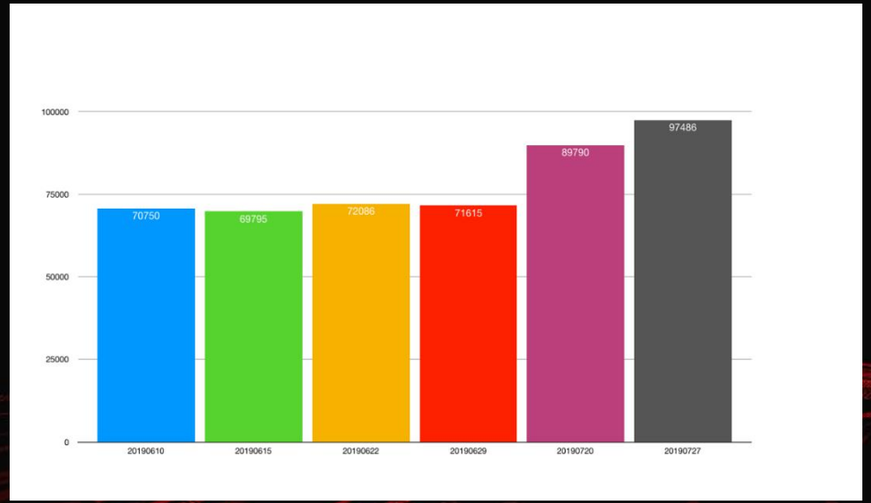
CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED TITLE WORDS.

ZoomEye全球蜜罐识别

ZoomEye全球蜜罐识别

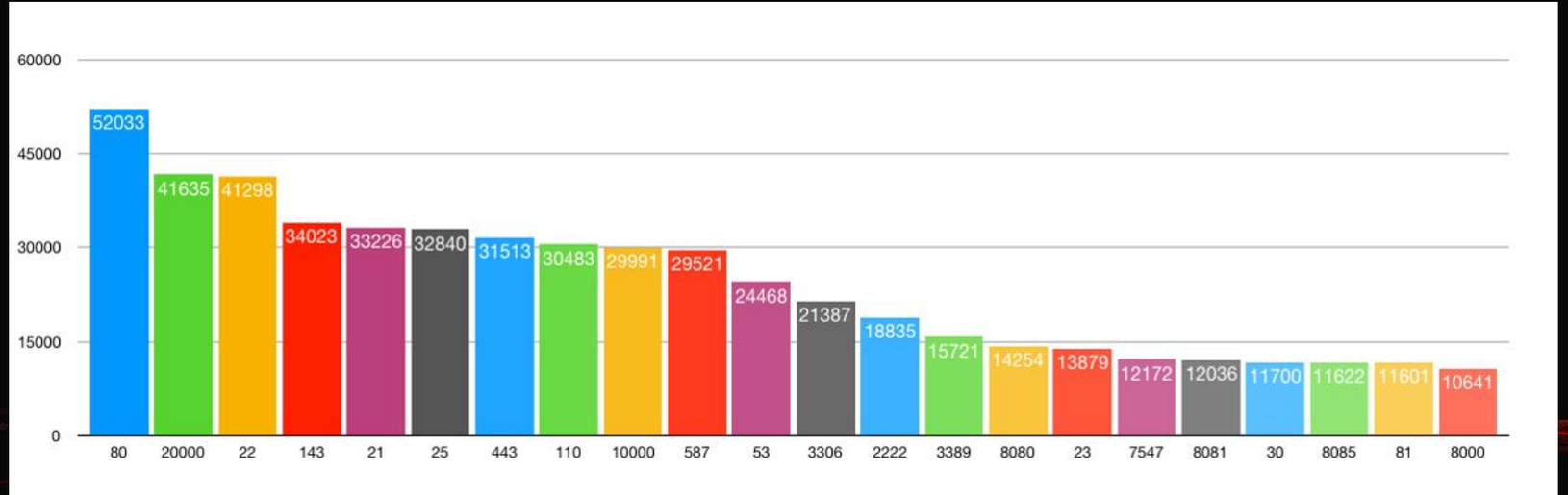
- 网络空间（外网）蜜罐主要用来对抗僵尸网络、GPT、网络空间mass扫描等攻击，是威胁情报的主要来源之一。
- 随着攻防博弈白热化，蜜罐识别诊断成为必然。
- “蜜罐”也是一种“服务”或者说“应用”，一样存在自己的特定的banner数据体现，所以蜜罐是可被识别。

ZoomEye全球蜜罐识别



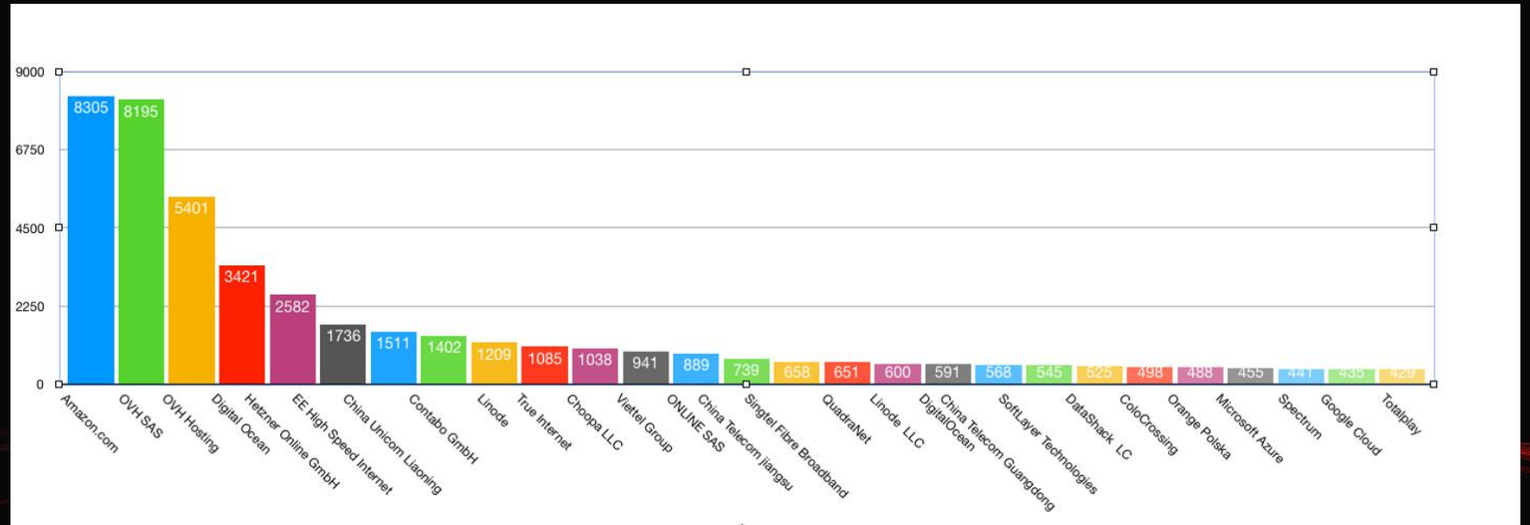
ZoomEye全球蜜罐识别

- 端口分布



ZoomEye全球蜜罐识别

- IDC分布



“ZoomEye关注一切网络空间测绘、IP 画像相关数据”

–heige

ZoomEye期待更多的合作

基本信息

IP 地址	95.6.9.113
位置信息	数据信息由IPIP.net提供 IPIP
城市	
省 / 州	Turkey
国家	Turkey
坐标	38.957741, 35.431702
网络服务提供商	turktelekom.com.tr
Hostnames	95.6.9.113.static.ttnet.com.tr
组织	
自治系统编号	AS47331

“黄婆卖瓜，也得用户夸！”

–heige

ZoomEye are totally comparable to Shodan

https://www.freebuf.com/articles/network/206656.html

Daniel Cuthbert 喜欢了

Miroslav Stampar @stamparm · 2小时

Credit where credit's due. @zoomeye_team's (IoT) search engine has the best and most accurate results around (compared to others). I am using it extensively during development of identYwaf

由 Microsoft 翻译自英语

信用到期的地方。@zoomeye_team搜索引擎有(IoT)最好的和最准确的结果周围 (与其他人相比)。我在开发 identywaf 的过程中广泛使用它

3

zoomeye还是能比shadon搜到更多主机

11:30

有啥建议 可以直接跟我提

n0mad
@n0mad42

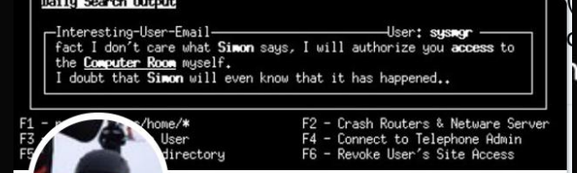
关注

zoomeye is truely a cyberspace-search-engine.

zoomeye.org/searchResult?q …
shodan.io/search?query=j …

@80vul @shodanhq @GreatDismal

#shodan #zoomeye #osint #recon



正在关注

Miroslav Stampar
@stamparm 关注了你

BOFH, penetration tester, author of @sqlmap, #infosec, developer, OSC(P|E), CTF enthusiast, CERT, $crypto # Opinions are my own and not the views of my employer

推文	正在关注	关注者
3,604	321	7,001

Revista Automática e Instrumentación @automatica_ · 1小时

Carlos Marín (@SchneiderES) subraya la importancia de indexar nuestras instalaciones en Internet, "buscarnos" en Shodan (shodan.io) y **ZoomEye** (zoomeye.org) es el primer paso. #ISAconferencia19

由Microsoft翻译自西班牙语

Carlos Marin (@SchneiderES) 强调了在互联网上为我们的设施编制索引的重要性，在 Shodan (shodan.io) 和 ZoomEye (zoomeye.org) 中找到我们是第一步。#ISAconferencia19

1 1

Huzeyfe ÖNAL @huzeyfeonal · 5月30日

Shodan yerine artık **ZoomEye** kullanmaya başladım. Shodan'da bulamadığım bir çok ip/port'a ait bilgi **ZoomEye**'da yer alıyor. Bir de hostname tabanlı (Virtual Host) arama izni verseler tadından yenmez.

zoomeye.org

由Microsoft翻译自土耳其语

我现在开始使用 Zoomeye, 而不是 Shodan。很多我在 Shodan 找不到的 ipw/端口信息都位于 ZoomEye。不使用基于主机的 (虚拟主机) 搜索权限。

zoomeye.org

Huzeyfe ÖNAL on LinkedIn: "Shodan yerine artık ZoomEye kullanmay...

May 30, 2019: Huzeyfe ÖNAL posted images on LinkedIn

linkedin.com

致谢

演讲人：
heige@0x557

- 感谢那些曾经或现在参与ZoomEye、Seebug、KCon相关的同事们!
- 感谢那些曾经或现在为知道创宇、知道创宇404团队做出贡献的兄弟姐妹们!
- 感谢那种支持帮助我们的社区朋友们!
- 以你们的曾经或者现在的工作感到自豪!