

网络空间测绘技术的应用与展望

BaCde [Insight-labs] & 白帽汇安全研究院

ID: BaCde

就职于北京华顺信安科技有限公司白帽汇安全研究院。

网络安全爱好者

安全组织Insight labs成员。

FREEBUF专栏作者

2015年尝试将机器学习技术应用于webshe11查杀中。

主要擅长网络空间测绘技术、Webshe11查杀技术、Web漏洞挖掘。

现专注网络空间测绘技术的实践与研究。



华顺信安



白帽汇安全研究院

大家都知道比特币。

那么大家知道比特币的用户都在哪里么？

挖矿的矿机哪里最多呢？

100家汽车厂商数据泄露，泄露了147G资料，47000份文件

2015年12月网络恢复创业公司UpGuard风险分析师克里斯·维克利Chris Vickery发现，美国共和党3家承包商编译的1TB数据(包含1.98亿选民信息，约占美国人口的61%)，被存放在错误配置的数据库中，可能被任何人访问。

- 美军特种作战司令部（SOCOM）发生11GB数据泄漏
- 9300万墨西哥选民数据泄漏
- 220万恐怖分子嫌疑人数据泄漏
- Hello Kitty 网站遭攻击 330 万用户数据泄露
- HIV患者约会APP泄漏用户敏感数据
- 线上交易公司 AMP 数据泄露, 上万客户信用报告、护照扫描信息曝光
- Verizon数据泄露 数TB文件暴露在公网 1400万客户敏感信息公开下载
- 艾滋病阳性单身人士约会软件Hzone5000名用户信息遭泄露
- 美国TigerSwan泄露 9400份敏感简历



data breach hunter
数据泄漏猎人

2016年8月12日 - **Chris Vickery** has found data breaches in everything from US voter ... He uses freely available software like search engine **Shodan** and network ...

2017年4月26日 - Using search engines for internet-connected devices, like **Shodan**, and tools that scan common ports where data typically live, Vickery can tick ...

2016年1月18日 - We are here with **Chris Vickery**, a security researcher who explores the dark ... I came across using **Shodan**, a search engine that searches for ...

2016年4月23日 - In the morning of April 14, **Chris Vickery**, a security researcher, was browsing **Shodan**, a search engine for internet-connected devices and ...

2015年12月22日 - As a pastime, IT helpdesk professional **Chris Vickery** likes to poke around **Shodan**, the infamous search engine site for IoT devices. "There are ...

Chris Vickery under attack after disclosing open DB for uKnowKids ... although the information collected by **Shodan.io** suggests that the database had been up ...

2016年12月17日 - **Chris Vickery**, lead researcher for the security team at MacKeeper, spotted it exposed while performing random scans with the **Shodan** search ...

2016年7月23日 - Last week bits&digits was afforded the opportunity to speak with the famous **Shodan** Sleuth, Security Researcher **Chris Vickery**. For those who ...

2016年11月2日 - **Chris Vickery**, security researcher and internet watchdog ... He also was familiar with **Shodan**, a search engine that finds and indexes ...

Hadoop服务器造成5PB数据泄露，中国、美国受波及最大

2017年8月，John Matherly发现了4487个HDFS服务器实例，这些服务器可通过公共IP地址获得，而且不需要身份验证。这些服务器总共泄露了超过5120TB的数据。

47820个MongoDB服务器只泄露了25TB的数据。从这个角度来看，与MongoDB服务器相比，HDFS服务器泄露的数据要多200倍，而与此同时，MongoDB服务器的数量是后者的10倍。2015年公布的一份报告显示，在当时Redis、MongoDB、Memcached和ElasticSearch服务器的数据只泄露了1.1PB的数据。



101.88.235.57

China Telecom Shanghai

Added on 2017-11-07 22:45:51 GMT

China, Shanghai

Details

database



MongoDB Server Information

```
{
  "process": "mongod",
  "pid": 824,
  "connections": {
    "current": 110,
    "available": 709,
    "totalCreated": 4190
  },
  "locks": {
    "Metadata": {
      "acquireCount": {
        "w": 1
      }
    }
  },
  ...
}
```

211.152.62.227

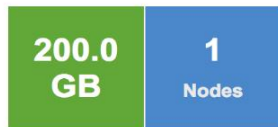
China Telecom Shanghai

Added on 2017-11-08 04:54:43 GMT

China, Shanghai

Details

database



HTTP/1.1 200 OK

content-type: application/json; charset=UTF-8

content-length: 327

以上是网络空间测绘技术应用中
一个非常典型的场景：**泄露数据抓取**

然而，事情远非如此

- 掌握全球工控设备对互联网的开放数量，国家分布
- 窃取大量国家机密数据
- 做一个民间的摄像头天眼系统
- 做一个全网范围的漏洞精确打击和控制系统

以上并非危言耸听，而是已经实现了的现状

Shodan划时代的意义在于：
将侦查与渗透分开

侦查过程轻量级，对应到单台设备无感知
即使有感知，也无法定义违法

渗透过程一击致命

网络空间测绘是什么？
它在安全领域能做什么？

攻击永远比防护容易
攻击是点
防护是面

如何黑客有一套攻击GPS系统，他们会做什么？

- 通过对全球网络对外开放服务的资产进行主动或被动方式探测、抓取、存储，分析整理不同种类的网络空间资产指纹信息（规则），并对符合规则的资产进行统计分析，进而快速检索全球网络空间资产。
- 它能够帮助用户迅速进行网络资产匹配，快速开展网络空间威胁态势感知、漏洞影响范围分析、应用分布统计、应用流行度排名统计等工作。
- 对外的展现形式是一个**搜索引擎**。

查找摄像头

The image displays a web application interface for finding webcams. On the left, there is a sidebar with filters for '类型分布' (Type Distribution), '年份' (Year), '国家排名' (Country Ranking), '端口排名' (Port Ranking), and 'Server排名' (Server Ranking). The main area shows search results for the query 'header=webcamXP || title=webcamXP || server="webcamXP 5"'. The results list various IP addresses and their corresponding webcam feeds. A detailed view of one result shows the IP 109.220.69.23, which is located in France and is running webcamXP 5. To the right, a browser window shows the live video feed from this IP, displaying a room with a large window and a potted plant. The browser's address bar shows the IP address, and the page title is 'webcamXP 5'. The bottom of the browser window shows the status 'POWERED BY WEBCAMXP V5.6.10.0'.

搜索 `header=webcamXP || title=webcamXP || server="webcamXP 5"` 获得 1821 条匹配结果, 用时 212 毫秒, 模式: extended. 默认只显示一年内的数据, 点击 all 链接查看所有.

207.118.210.112 %

webcamXP 5
207.118.210.112
2018-07-05
United States / Taylor
webcamXP 5

HTTP/1.1 200 OK
Connection: close
Content-Length: 8069
Cache-Control: no-cache, must re
Content-Type: text/html; charset
Date: Wed, 04 Jul 2018 23:23:35
Expires: Wed, 04 Jul 2018 23:23:35
Pragma: no-cache

109.220.69.23 %

webcamXP 5
109.220.69.23
2018-07-04
France /
webcamXP 5

HTTP/1.1 200 OK
Connection: close
Content-Length: 7446
Cache-Control: no-cache, must re
Content-Type: text/html; charset
Date: Wed, 11 Jul 2018 11:34:19
Expires: Wed, 11 Jul 2018 11:34:19
Pragma: no-cache

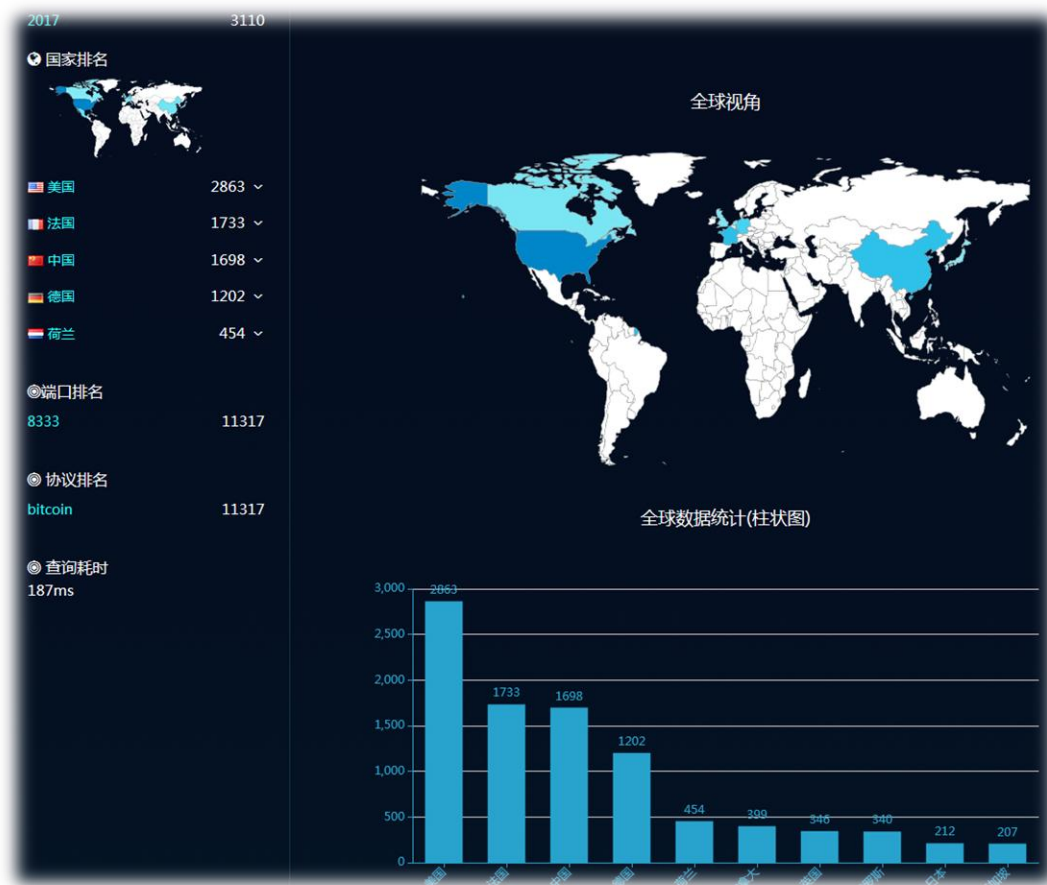
Source 1 JavaScript

Live View

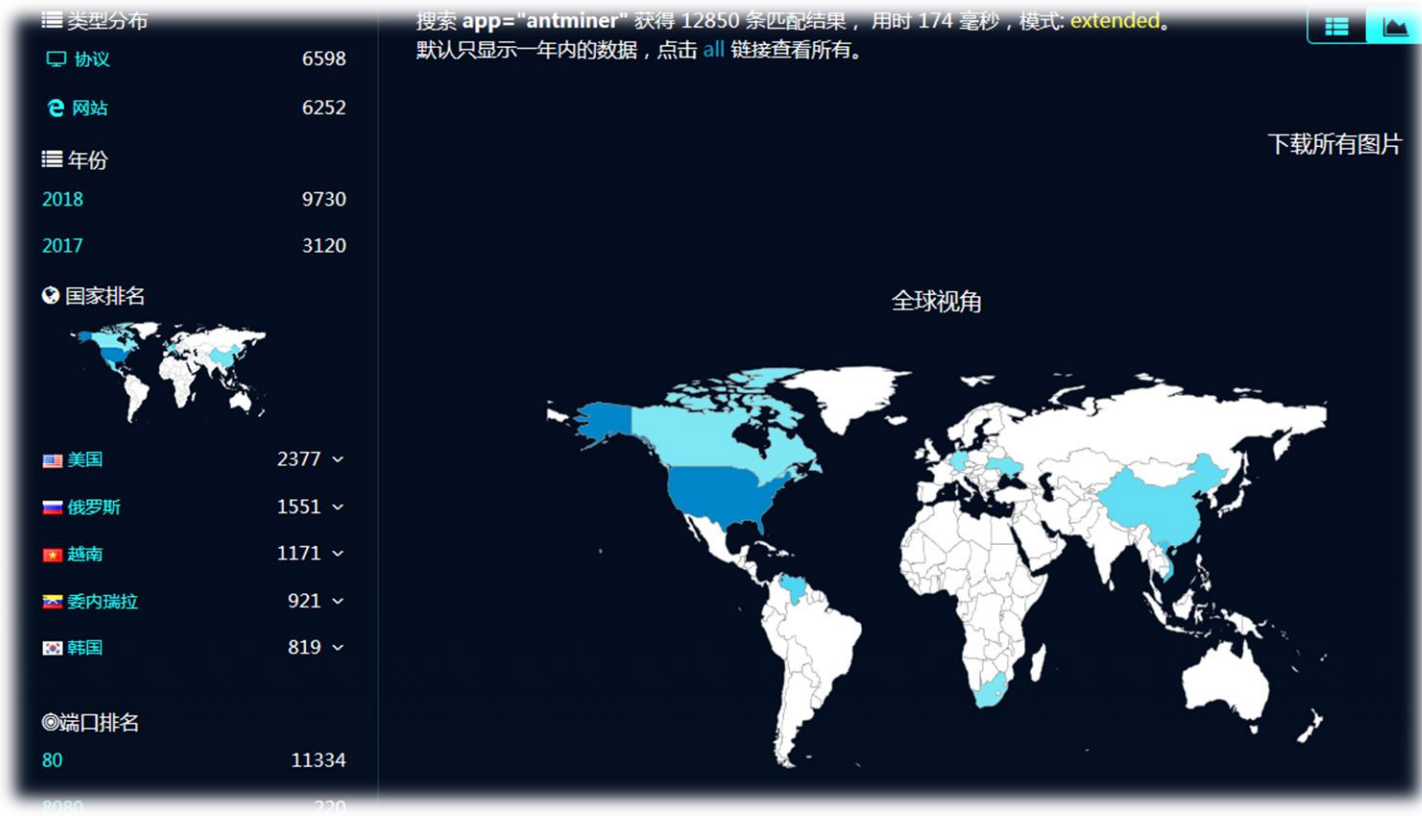
109.220.69.23

POWERED BY WEBCAMXP V5.6.10.0

比特币客户端



蚂蚁矿机的分布



针对特定系统的玩法

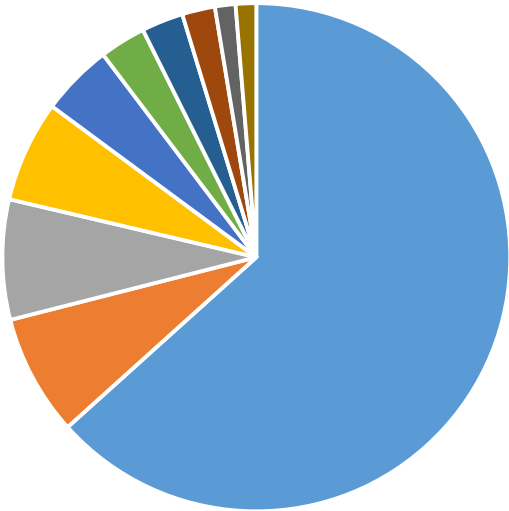


除了上面那些还有么？

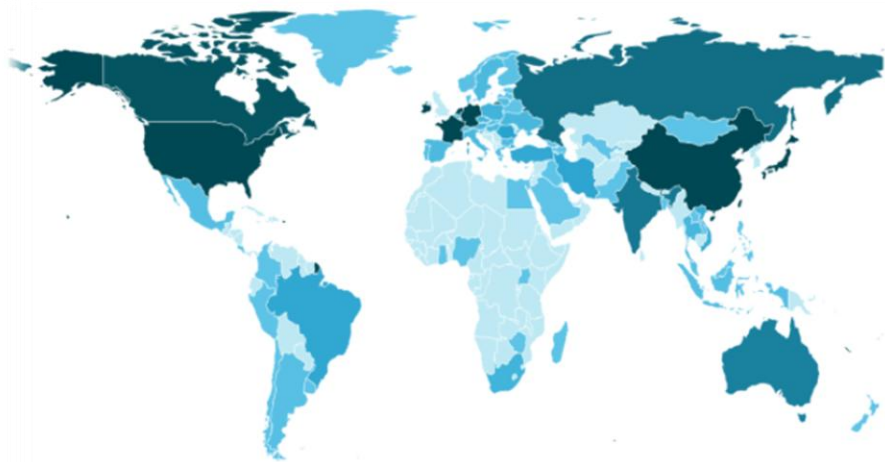
摄像头路由器分布TOP 10 饼图

华为路由器	6241378
海康威视（Hikvision）	758643
DVR Streamer	752991
mikrotik	635964
雄迈	450366
D-Link DCS	289542
NETSurveillance	261936
大华摄像头	206437
ZyXEL	128745
Ruckus	128745

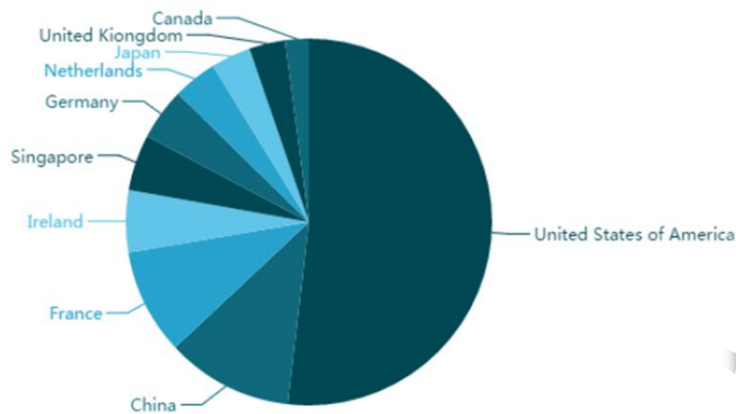
摄像头和路由器 top 10



- 华为路由器
- 海康威视（Hikvision）
- DVR Streamer
- mikrotik
- 雄迈
- D-Link DCS
- NETSurveillance
- 大华摄像头
- ZyXEL
- Ruckus



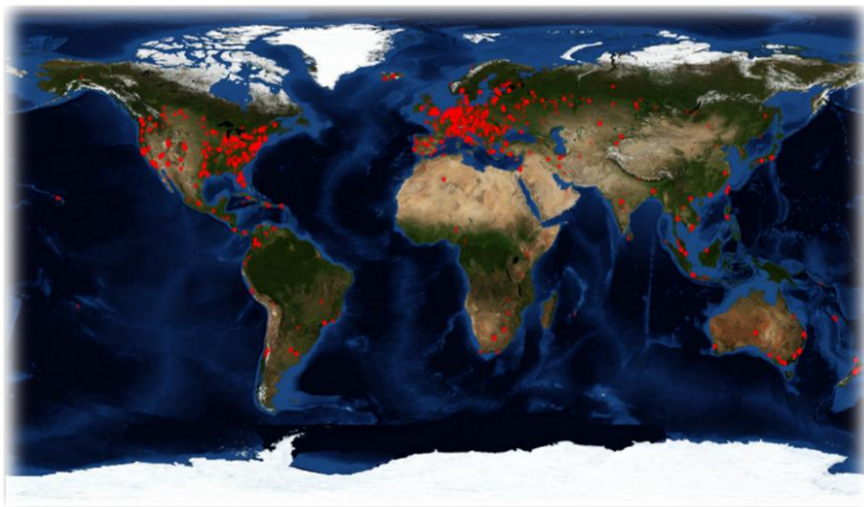
全球数据统计



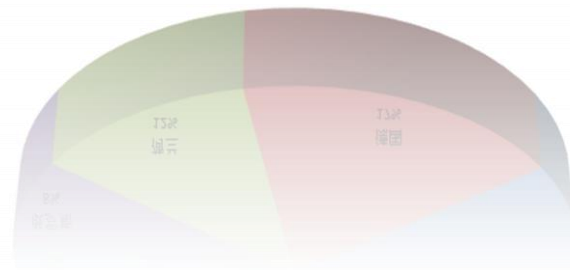
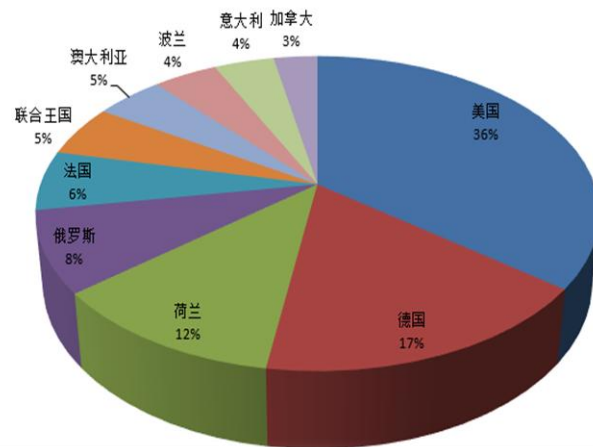
全球数据统计(饼状图)

全球共有**9750**台存在勒索信息。其中此次被删除的数据达到超过**500亿条**，被删除数据大小攻击**450TB**。最多的为**美国4380**台，其次是**中国第二, 944**台。法国787台，爱尔兰462台，新加坡418台。

Joomla! 用户特权提升漏洞影响范围分析



Joomla! (CVE-2016-8869&CVE-2016-8870)存在漏洞国家top 10





Western Digital MyCloud

安全 | https://www.exploitee.rs/index.php/Western_Digital_MyCloud#Remote_Command_Execution_23

log in

page | discussion | view source | history

exploitee.rs

Western Digital MyCloud

"Although the information we release has been verified and shown to work to the best of our knowledge, we can't be held accountable for bricked devices or roots gone wrong."

Contents [hide]

1 About

2 Purchase

3 Models

4 Firmware

5 Reversing Firmware

6 Firmware Contents

7 Web Server

8 Writing To LCD Display

9 Vulnerabilities

9.1 Login Bypass Vulnerability

9.1.1 login_checker.php (pre 12/20/2016)

9.1.2 login_checker.php (post 12/20/2016)

9.1.3 network_mgr.cgi (added 8/6/2017)

9.2 Arbitrary Root File Write

9.2.1 /web/addons/upload.php

9.2.2 /jquery/uploader/multi_uploadify.php (added 08/06/2017)

9.3 Pre-Auth Remote Command Execution

9.3.1 /web/addons/ftp_download.php

9.3.1.1 Authentication Commented Out

9.3.1.2 Remote Command Execution

9.3.1.3 Remote Command Execution

9.3.1.4 Remote Command Execution

9.3.1.5 Remote Command Execution

9.3.1.6 Remote Command Execution

9.3.2 /web/storage/raid.cgi.php

9.3.2.1 Authentication Commented Out

9.3.2.2 Remote Command Execution

navigation

Main page

Recent changes

Community Members

Random page

Help

links

Exploitee.rs Online Store

Exploitee.rs Forum

Exploitee.rs Blog

Exploitee.rs Twitter

search

Search

Go

tools

What links here


Related changes

Special pages

Printable version

Permanent link

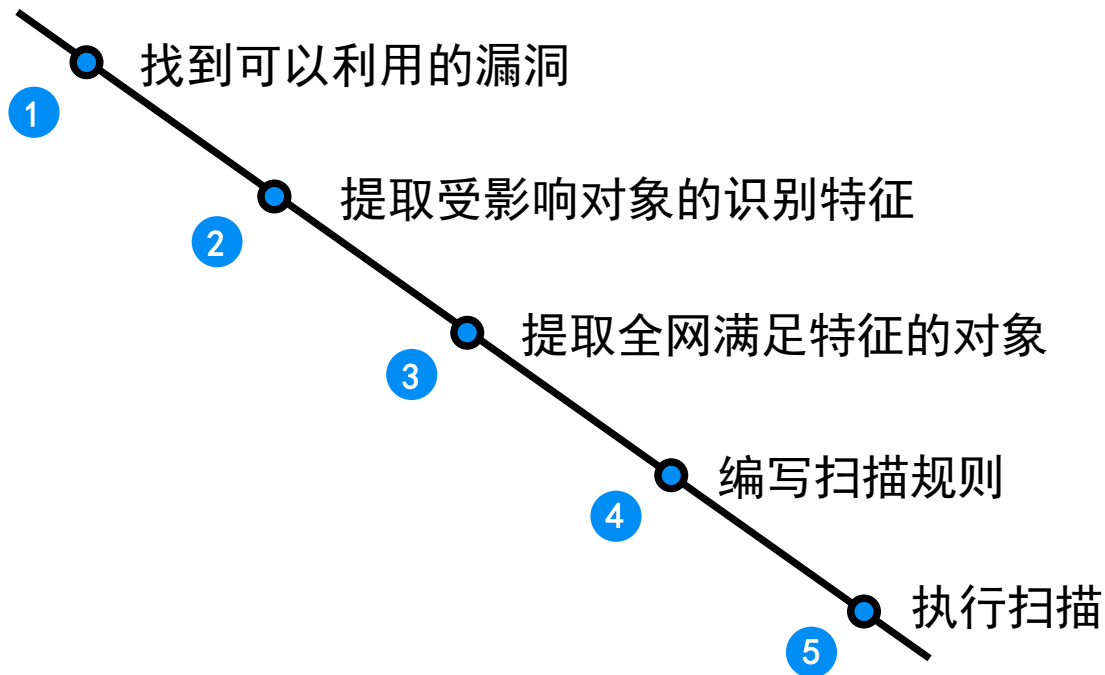
Page information



	传统扫描	全网扫描
触发方式	扫描对象	漏洞
扫描方式	全漏洞集合	一个漏洞
依赖方式	漏洞库的完整度	全球网站覆盖度
速度	慢	快
对目标影响	大	小
使用对象	特定对象渗透测试	科研调查，抓肉机
典型案例	AWVS/APPSCAN	fofacli

攻击技术的变化：极速，精准，无感知

一次完整全网扫描的步骤



2015. 11. 11



Redis CrackIT 入侵事件分析

2016. 01. 13



飞塔 (FortiGate) 存在ssh后门分析

2016. 12. 07



Joomla! cms core 任意文件上传漏洞

2017. 01. 11



Elasticsearch数据泄露报告

2017. 01. 12



威胁情报预警: Elasticsearch勒索事件

2017. 03. 07



Strut2高危远程命令执行漏洞预警

2017-至今



Couchdb勒索事件、AXIS摄像头、蚂蚁矿机、GPON光纤路由器、Weblogic、D-



link、Netgear、Joomla、Docker Remote API、CouchDB、Wordpress、

Metinfo、Onethink等诸多系统全球漏洞预警

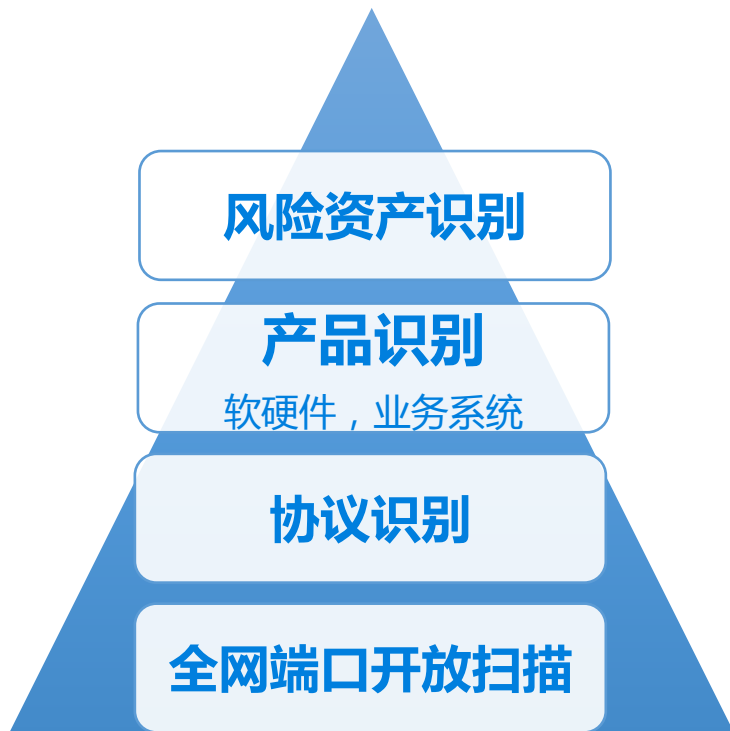
.....



.....

	传统意义的资产管理	网络空间测绘
侧重点	硬件和IP资产 如：投影仪，上网卡	IP上承载的业务系统 如：docker系统，金蝶财务，用友OA管理软件
实时性	慢 依赖管理手段	快 技术手段实时更新
覆盖度	少 很多私搭服务器	全 全网段，多端口，多协议
准确度	低 业务切换，导致大量信息失真	高 应用层识别

网络空间测绘技术梳理网络资产

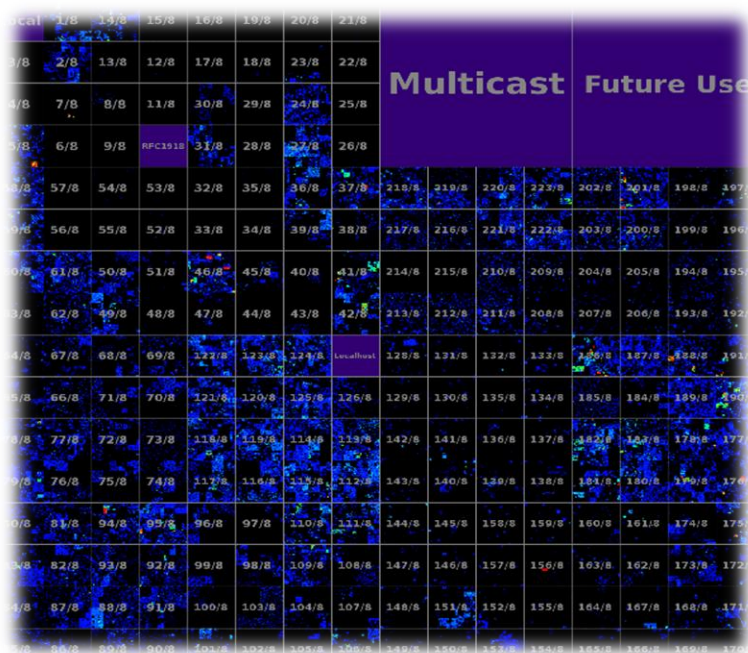


- 通过漏洞信息，进行有针对性的风险资产识别。全网扫描器引擎，风险识别达到极速。
- 固化字段的查询语法，保存为规则集，可以直接标注产品，包括硬件，软件，OA，CRM，财务系统等。
- 通过协议的交互解析，来提取协议字段。这样保证了准确度，同时为下一步分析做准备。
- 几十年都是这么做的，nmap技术根深蒂固。但是有几类问题：慢，不准，单一。端口扫描不叫网络空间测绘。21端口就一定对应FTP吗？

- masscan和zmap技术的诞生：
- 支持跑满带宽：
10G带宽情况下针对全网跑完一个端口时间为数分钟
- 半连接扫描：以太网层处理，没有内核层开销，无会话无等待
- 随机IP分布请求，减少目标的感知
- 支持TCP/UDP协议
- 与nmap的区别：一个是做多端口少目标的扫描，一个则是多目标少端口
- 注意：
- 全网扫描必须接受一定比例丢包率的情况
- 大协议端口与小协议端口的组合：80，443要与502之类的偏门端口结合

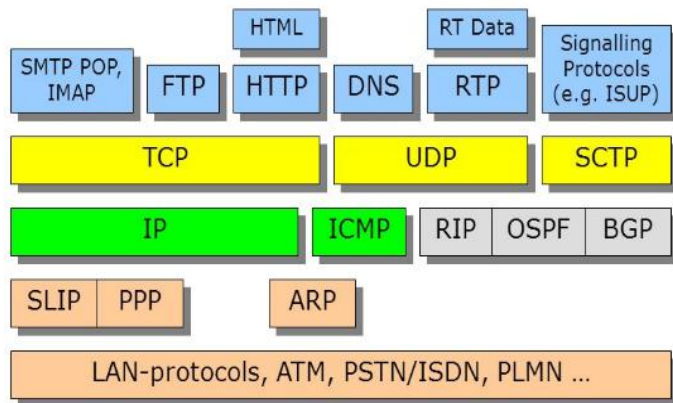
全网扫描对应多少IP地址？

地址段	用途	地址数	备注
0.0.0.0/8	保留	16777216	表示本地网络，0.0.0.0/32表示本机（windows不支持）
1.0.0.0/8-9.0.0.0/8	公网	150994944	
10.0.0.0/8	保留	16777216	私有
11.0.0.0/8-126.0.0.0/8	公网	1946157056	
→ 100.64.0.0/10	保留	4194304	私有
127.0.0.0/8	保留	16777216	回路
128.0.0.0/8-169.253.0.0/16	公网	704512000	
169.254.0.0/16	保留	65536	本地链路
169.255.0.0/16-172.15.0.0/16	公网	34668544	
172.16.0.0/16-172.31.0.0/16	保留	1048576	私有
172.32.0.0/16-192.167.0.0/16	公网	344457216	
→ 192.0.0.0/24	保留	256	IETF Protocol Assignments
→ 192.0.2.0/24	保留	256	TEST-NET-1
→ 192.88.99.0/24	保留	256	6to4 Relay Anycast
192.168.0.0/16	保留	65536	私有
192.169.0.0/16-223.0.0.0/8	公网	525795328	
→ 198.18.0.0/15	保留	131072	Network Interconnect Device Benchmark Testing
→ 198.51.100.0/24	保留	256	TEST-NET-2
→ 203.0.113.0/24	保留	256	TEST-NET-3
224.0.0.0/4	保留	268435456	广播
240.0.0.0/4	保留	268435456	未分配，未来使用
255.255.255.255/32	保留	1	Limited Broadcast



- IPv4的总地址池大小约为**43亿**，在里面又分为两部分：公网地址段（分配和未分配），保留网段（私有网段和特殊用途）。
- **实际的公网IP大约是37亿地址空间**

- 正常情况下，一个IP能够开放**1-65535个端口**
- 考虑到实际的扫描周期，没有任何一个平台会选择针对大范围进行**65535个端口**的端口扫描探测
- 通常大家会维护一个常见开放端口的列表，如果对应HTTP的**80端口**，对应HTTPS协议的**443端口**，对应SSH协议的**22端口**，对应FTP协议的**21端口**，对应SMTP的**25端口**等等。
- 扫描**246个端口**



- 漏洞并非对应端口，而是对应产品应用
- 协议识别是为了更精准的识别产品
- 标准端口不一定对应标准协议
- 非标准端口不一定就是私有协议（每个系统由自己的常用端口）
- 协议分类：
 - 常见服务：ftp, ssh, telnet, http, snmp.....
 - 数据库：mysql, mssql, oracle, db2, mongodb, elasticsearch.....
 - 工控：modbus, bacnet, s7, dnp3, melsecq.....
- 提取banner, cert等基础字段，无差别存储
- 协议的暴力遍历

协议识别内容

IP、端口

根据IP和端口确定资产

协议分析

针对资产端口运行协议进行分析识别Banner信息

证书字段

深度提取证书协议字段

https证书: Signature Algorithm、Public Key Algorithm、Modulus...

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 213609529 (0x48563639)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=cn, ST=\xE5\xB9\xBF\xE4\xB8\x9C\xE7\x9C\x80\xBA\xE7\xA7\x91\xE6\x8A\x80, CN=172.16.2.158
Validity
Not Before: Jun 16 09:45:29 2008 GMT
Not After : Sep 14 09:45:29 2008 GMT
Subject: C=cn, ST=\xE5\xB9\xBF\xE4\xB8\x9C\xE7\x9C\x80\xBA\xE7\xA7\x91\xE6\x8A\x80, CN=172.16.2.158
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
Modulus:
00:9e:3f:46:a3:58:46:5e:cc:44:cf:1f:9c:4e:e3:
f1:63:95:14:6e:2a:9f:6c:65:29:0a:c4:10:8a:fb:
c8:4c:a3:ec:11:e8:ea:74:87:57:79:49:17:54:b8:
be:0a:d6:ca:cd:8b:57:5b:77:26:c9:16:4a:52:6f:
ef:3d:aa:02:0c:be:00:08:7f:7a:f8:c5:84:d4:5b:
88:b4:ba:90:c3:bb:16:21:06:6a:83:ac:18:68:7a:
e5:c9:07:af:37:ba:50:d3:8a:46:35:b6:f4:14:49:
61:ea:72:c6:ba:f2:1a:80:7a:21:1a:04:7f:60:1b:
1b:f1:b2:ec:8e:38:0c:30:43
Exponent: 65537 (0x10001)
Signature Algorithm: sha1WithRSAEncryption
57:ce:2a:61:99:60:cf:33:61:84:b9:33:83:7a:10:b9:94:e4:
b8:91:f5:46:64:d2:74:5c:00:2a:d8:ba:67:47:28:14:77:4f:
b9:4c:89:a1:f9:29:68:de:8b:47:8a:fd:00:b4:51:d6:b1:01:
8c:14:ed:0e:be:ec:e8:3e:4c:cc:bd:13:55:51:61:1e:16:a2:
e2:4c:6c:05:d2:fb:6a:cd:54:9e:c1:d8:02:15:8b:7d:e7:34:
57:cf:04:f2:23:55:4a:6f:91:d5:37:ac:a4:f7:60:2c:88:7f:
13:5f:34:6a:cc:bb:4f:2b:39:dc:df:88:82:6e:97:01:46:f9:
```

工控协议字段

Operation System、product、Source Address、Module、Module Type、Module Name、Serial Number、Controller Mode、Version、PLC Type...

- 应用识别规则库：
 - 梭子鱼安全设备：通过body或者header
 - body=http://www.barracudanetworks.com?a=bsf_product
 - header= “BarracudaHTTP”
 - 锐捷路由器：通过body查找
 - body= “free_nbr_login_form.png”
 - Jenkins：通过header查找
 - header= “X-Jenkins-Session” || body= “translation.bundles”
 - F5：通过cookie查找
 - header= “BIGipServer”

规则集的分类



服务器



网络设备



网络安全产品



物联网设备



云平台软件



企业应用



工控系统

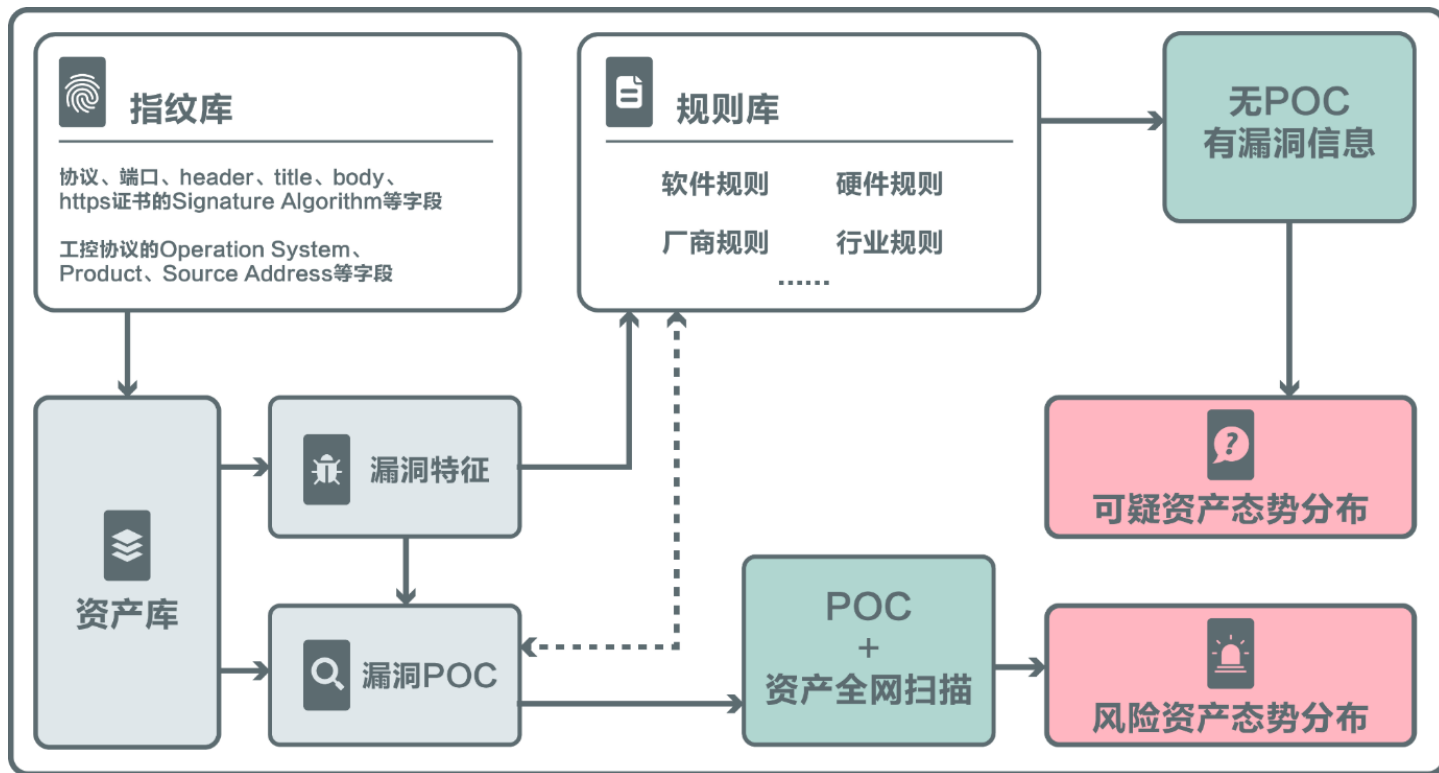


数据库



网络应用

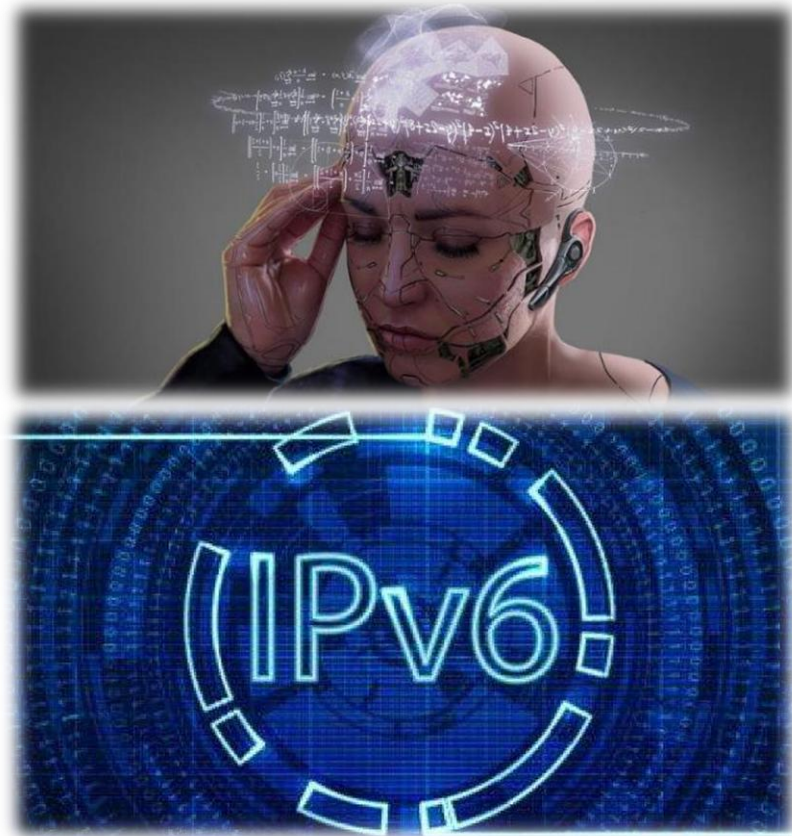
安全事件应急响应



- Nday 和 Oday
- CMS, 邮箱, 工控设备, IoT设备
- 与传统扫描规则引擎的漏洞定义不一样的地方在于:
 - 必须对接网络空间测绘系统
- 国际上最好的漏洞框架是metasploit, 如果跟网络空间测绘系统会怎么样?
- 国家战略资源

资产名称	操作系统	端口	服务	组件
10. [redacted]		80 22 443 23 161	http,ssh,https,telnet,snmp	Cisco IOS Cisco 路由器/交换机 Cisco 公司产品 交换机 网络产品
10. [redacted]		443 22 80 23	https,ssh,http,telnet	Cisco IOS Cisco 路由器/交换机 交换机 网络产品
10. [redacted]		80 554	http,rtsp	
10. [redacted]		80 443 631 515 8080 9100 161 21	http,https,lpd,printer-job-language,snmp,ftp	Conexant EmWeb HP LaserJet Printer 打印机
10. [redacted]	RedHat	21 80 161	ftp,http,snmp	Redhat Red Hat eCos Hardlink 打印服务器 打印服务器
10. [redacted]		80 23	http,telnet	
10. [redacted]		161 23	snmp,telnet	H3C 交换机 交换机 网络产品
10. [redacted]		80 23	http,telnet	路由器 网络产品
10. [redacted]		80 161 23	http,snmp,telnet	H3C 路由器 路由器 网络产品
10. [redacted]	Windows	1433 80	mssql,http	Web服务器 脚本语言 数据库
10. [redacted]		21 515 9100 161 631 443 80	ftp,lpd,printer-job-language,snmp,http,https	HP LaserJet Printer 打印机
10. [redacted]		5900	vnc	VNC 远程管理
10. [redacted]	Windows	1433 3389 21 1521 80 8888 5560	mssql,rdp,ftp,oracle,http	Web服务器 脚本语言 FTP服务器 远程管理 数据库
10. [redacted]		8080 80 3306 22 10000 2000 21	http,mysql,ssh,https,ftp	Web服务器 脚本语言 FTP服务器 中间件 数据库
10. [redacted]	RedHat	21 161 80	ftp,snmp,http	Redhat Red Hat eCos Hardlink 打印服务器 打印服务器

- AI 自动化识别
- rdp, vnc, rtsp以及网络摄像头等截图
- 流量分析自动提取
- 更多专题
- 网页截图
- IPV6的网络空间测绘
- 网页空间历史库





2018

感谢大家的聆听

Thank you very much & best regards.