

利用高级组合语法拓线发掘某工控系统

0x01 线索

近日，我们留意到一个新闻：[以色列供水设施ICS遭伊朗黑客入侵](#)

原文地址如下：<https://www.otorio.com/blog/what-we-ve-learned-from-the-december-1st-attack-on-an-israeli-water-reservoir/>

在原文中，OTORIO团队提到了一个供水设施工业控制系统的互联网的人机接口（HMI），指出了该HMI系统未经授权暴露在整个互联网上，直接通过Web界面即可访问。

其实在很多国外的安全文章中，都会使用Shodan给出某个具体IP或产品名用于佐证。安全研究人员经常会对这些文章中提到线索进行追溯、分析，下面将给出一个实际的例子。

0x02 分析

在OTORIO团队原文中截图如下：



IP被作者隐藏了，那么我们如何通过上图信息进行挖掘找到真正的系统呢？我们从上图中提取出3点要素：

1. ASN为 16116；
2. 同时开放80端口、502端口；
3. 协议分别是http协议和modbus协议。

Quake检索系统中主要有两大部分，分别是 服务数据 和 主机数据：

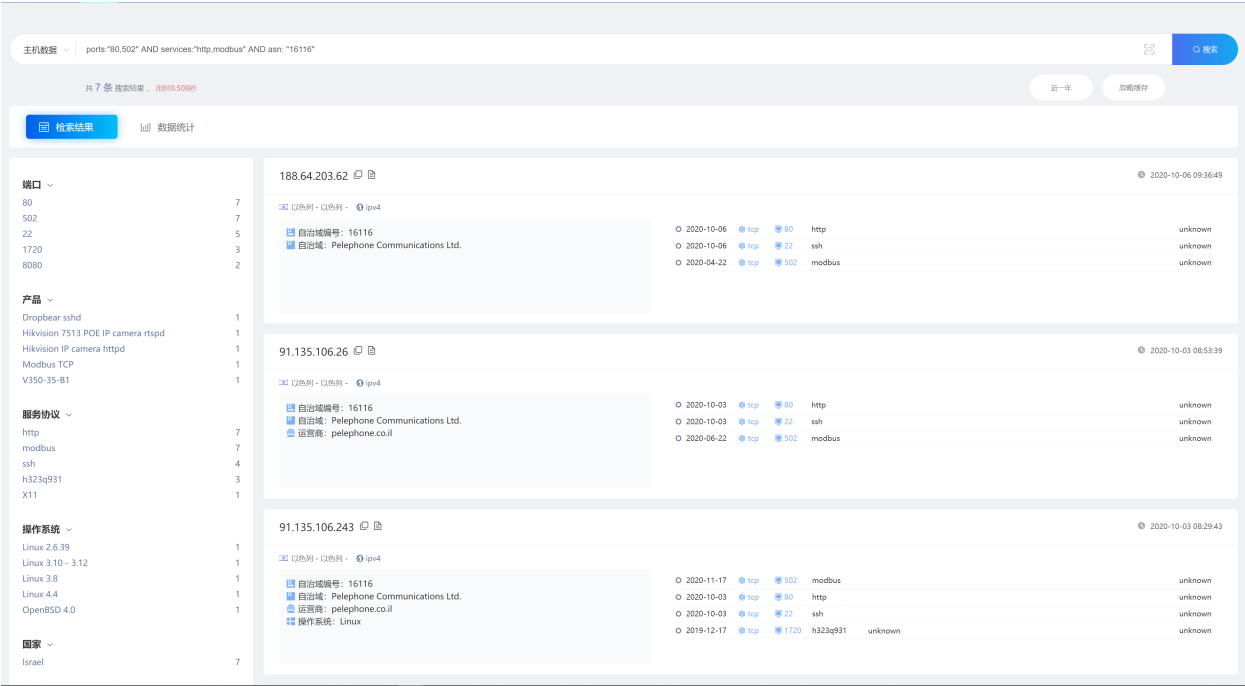
- 服务数据 是保留端口返回response和协议返回内容的地方，会以 累计 的形式保存全量历史数据，用于刻画一个IP的全部历史活动痕迹；
- 主机数据 是删除端口返回、协议详情的地方，会以 去重 的形式保存全量数据，用于刻画一个IP的完整端口及其对应信息；

基于高级搜索语法（**Quake高级会员、终身会员特有**，语法仅能在 主机数据 中使用，）：

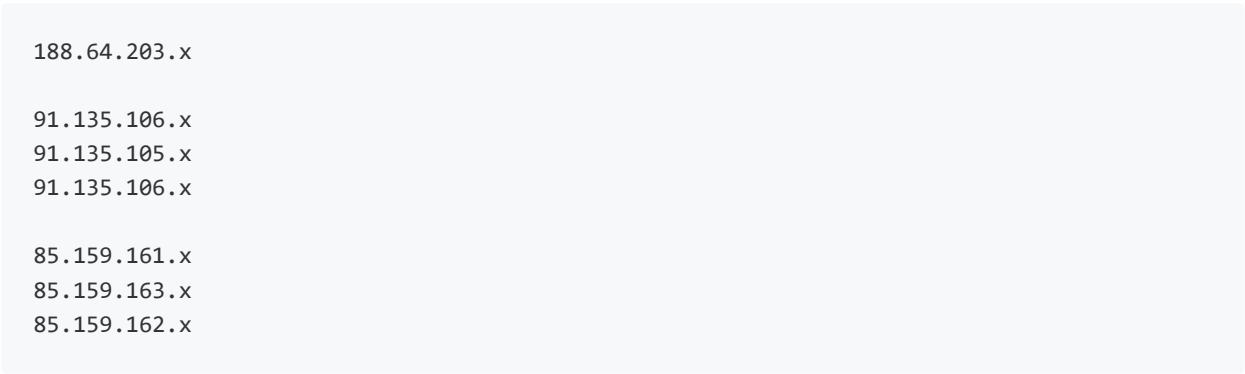
- ports ，表示某个IP同时开放了哪些端口；
- services ，表示某个IP同时使用了哪些协议；

基于上述信息，在 "主机数据"中 使用搜索语法如下：

ports:"80,502" AND services:"http,modbus" AND asn: "16116"



得到7个独立IP地址



搜索这些IP在 Quake服务数据 中的502端口，可以看到modbus协议解析内容和Shodan的一致：

(ip:"188.64.203.x" OR ip:"91.135.106.x" OR ip:"91.135.105.x" OR ip:"91.135.106.x" OR ip:"85.159.161.x" OR ip:"85.159.163.x" OR ip:"85.159.162.x") AND port: "502"

QUAKE 检索 区域 专题 产品 报告 漏洞 探索 统计 会员 帮助 管理后台 云震2001

服务数据 (ip:"188.64." OR ip:"91.135." OR ip:"91.135." OR ip:"91.135.1." OR ip:"85.15." OR ip:"85.15." OR ip:"85.159." OR ip:"85.159." OR ip:"85.159." OR ip:"85.159." AND port:"502") 50 50 50 50 检索

共 19 条 搜索结果 (7个独立IP) , 耗时1.234s 近一年 导出数据 忽略缓存

检索结果 数据统计

端口	数量
502	19

产品	数量
Modbus TCP	8

服务协议	数量
modbus	19

操作系统	数量
Linux 4.4	2
Cisco Unified Communications Manager VoIP ada...	1
Linux 2.6.18	1

国家	数量
Israel	19

省份	数量
Israel	17
Hefa	1
Tel Aviv	1

91.135.105.61 以色列 - 特拉维夫区 - 特拉维夫 2020-11-26 05:35:44

502 tcp ipv4

ASN: 16116 组织: Pelephone Communications Ltd. 运营商: Pelephone Communications Ltd.

服务协议: modbus

端口响应

Unit ID: 1
- Slave ID Data: Illegal Function (Error)
- Device Identification: Illegal Function (Error)

91.135.106.243 以色列 - 特拉维夫区 - 特拉维夫 2020-11-17 16:19:03

502 tcp ipv4

ASN: 16116 组织: Pelephone Communications Ltd. 运营商: Pelephone Communications Ltd.

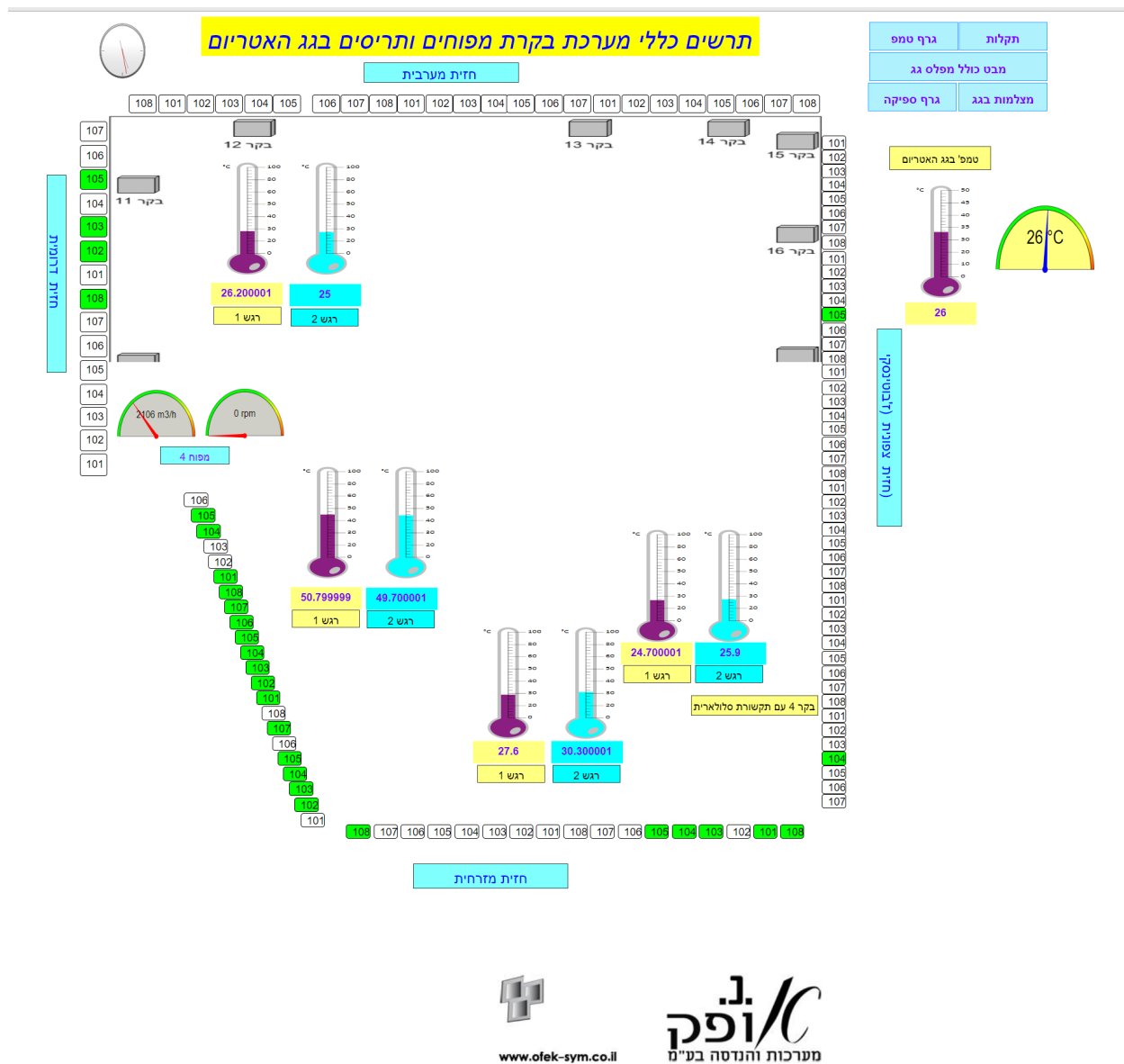
服务协议: modbus

端口响应

Unit ID: 1
- Slave ID Data: Illegal Function (Error)
- Device Identification: Illegal Function (Error)

分别访问80端口发现，有3个无法访问，2个系统加了HTTP认证（通过服务数据交叉验证，就是OTORIO团队原文中提到的系统）。

同时我们发现了同网段**另一个新的**供水设施工业控制系统存在未授权访问：

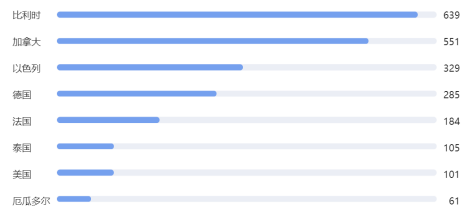
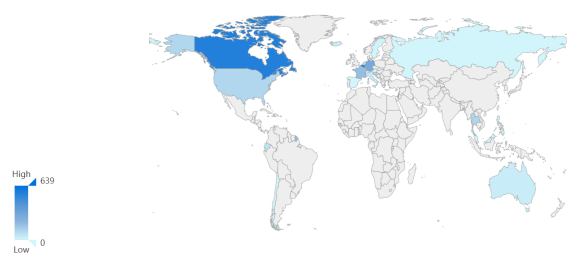


0x03 拓线

另外，OTORIO安全团队通过分析判定该系统为Ovarro公司的 T-Box 系统。基于上述相关线索，我们进行扩展发现，该系统对应的指纹如下：

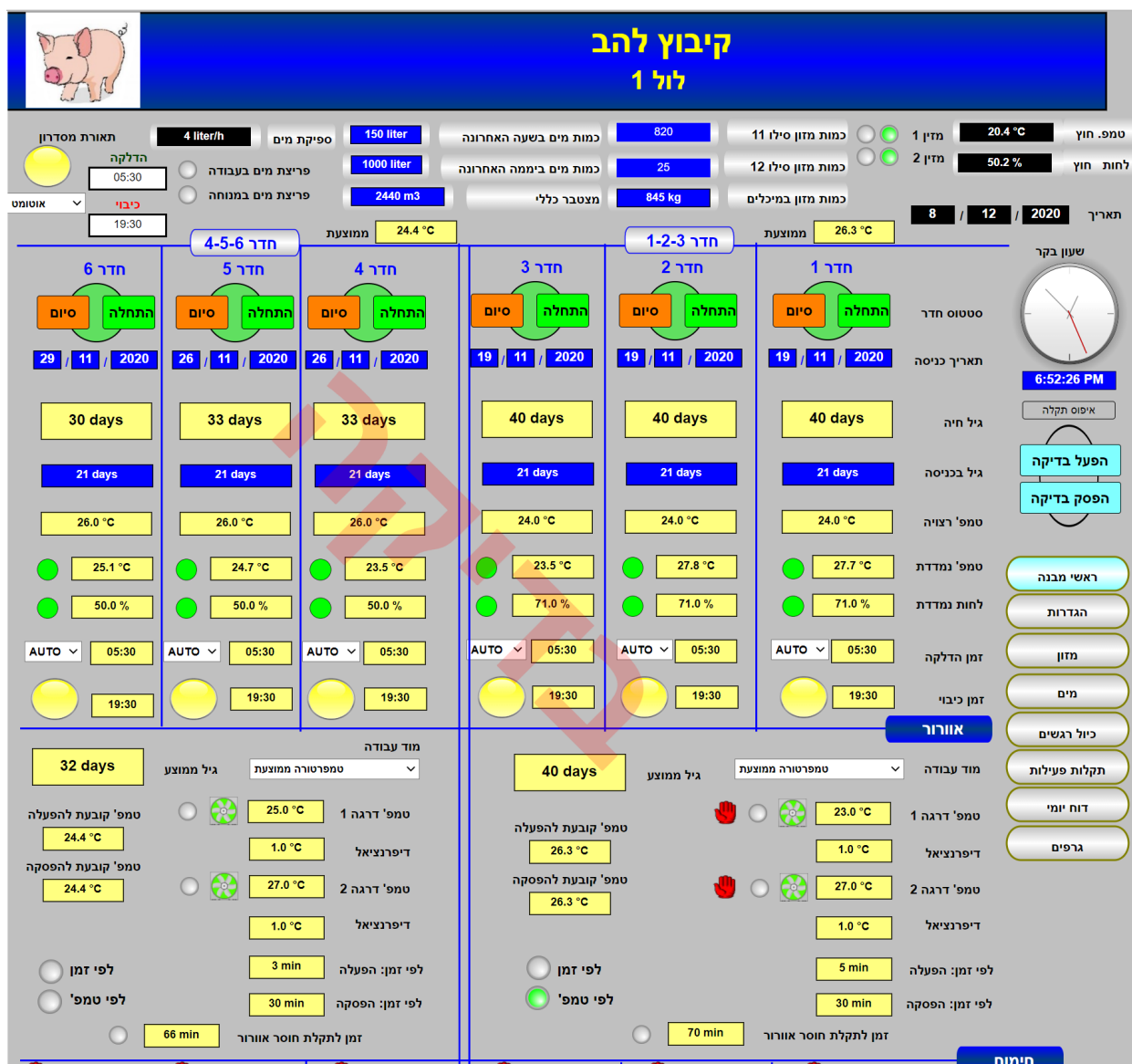
```
response:"<body style=\"margin:0;padding:0\">" AND response:"<iframe src=\"index.xhtml\" AND response:\"content=\"text/html; charset=utf-8\"/>"
```

对分布情况进行统计如下：



可以看出该系统主要是欧洲各国使用较多，国内不存在该系统。

访问后可以看出该工控系统涉及电力、能源、水利等等领域：




Défauts

- Défaut disjoncteur prise 1
- Défaut disjoncteur prise 2
- Discordance ouverture contacteur KM1
- Discordance ouverture contacteur KM2
- Discordance fermeture contacteur KM1
- Discordance fermeture contacteur KM2

Alarmes

- Alarme comptage prise 1
- Alarme comptage prise 2

Numéro Badge	ID Badge	Consommation
Compte n°1	52101	0
Compte n°2	8411	0
Compte n°3	13037	0
Compte n°4	7383	0
Compte n°5	11495	0
Compte n°6	10981	0
Compte n°7	10724	0
Compte n°8	701	0
Compte n°9	51330	0
Compte n°10	52872	0
Compte n°11	6612	0
Compte n°12	64951	0
Compte n°13	54671	0
Compte n°14	47732	0
Compte n°15	35396	853
Compte n°16	12266	0
Compte n°17	12780	0
Compte n°18	13551	0
Compte n°19	2243	0
Compte n°20	63666	0
Compte n°21	3528	0
Compte n°22	34368	0
Compte n°23	31284	0
Compte n°24	51073	0
Compte n°25	45162	0
Compte n°26	45933	0
Compte n°27	36681	0
Compte n°28	62124	0
Compte n°29	37452	0
Compte n°30	38737	0
Compte n°31	1215	0
Compte n°32	59040	0
Compte n°33	60582	0
Compte n°34	3014	0
Compte n°35	61867	32194
Compte n°36	62638	0
Compte n°37	49531	18210
Compte n°38	48246	0
Compte n°39	46704	0
Compte n°40	53386	0
Compte n°41	54157	0
Compte n°42	50302	0
Compte n°43	52615	0
Compte n°44	49788	0
Compte n°45	46447	0
Compte n°46	64437	0
Compte n°47	0	0
Compte n°48	0	0
Compte n°49	0	0
Compte n°50	0	0
Compte n°51	0	0
Compte n°52	0	0
Compte n°53	0	0
Compte n°54	0	0
Compte n°55	0	0
Compte n°56	0	0
Compte n°57	0	0
Compte n°58	0	0
Compte n°59	0	0
Compte n°60	0	0




SMALL PUMP STATION C1

OVERVIEW

ALARM

SITES

CMMS



Date : 8 12 2020
Time : 18 53 34

TNB SUPPLY
NORMAL

SCADA PANEL DOOR
CLOSED


DC VOLTAGE
27.74V

RTU TEMPERATURE
36.50°C

SIGNAL LEVEL
BAD

PUMP CONTROL MODE
MANUAL

PS-C1



Stop

SUMP LEVEL
LEVEL HIGH
LEVEL MEDIUM
LEVEL LOW

SWTP TIONG NAM
SUMP LEVEL
LEVEL HIGH
LEVEL LOW

SMS ALARM RECIPIENT

	RECIPIENT 1	RECIPIENT 2	RECIPIENT 3	RECIPIENT 4	RECIPIENT 5
NAME	hafiz	Amin			
MOBILE NO.	0192672347	0148438865			

最后：Happy Hunting by 360-Quake.

