针对网络空间关键基础设施情报收集的组织行为分析报告

灯塔实验室

2016 年 5 月

labs@plcscan.org

目录

一、背景

随着 Shodan 类网络空间搜索引擎的出现，基于主动探测的工控安全态势感知技术倍受研究者追捧。Shodan 搜索引擎 7*24 小时在网络空间搜索爬取互联网外部端口数据，并且根据扫描结果实时更新数据库，这其中不乏针对工控协议的探测。ZMap、MASSCAN 等基于异步无状态扫描工具的出现，使得快速探测整个 IPV4 空间变成可能，加上基于工控设备通信协议的识别探测，则可以迅速在网络空间中定位工控系统。

网络空间中的工控系统作为真正的关键基础设施是重要的战略和情报资源，而根据灯塔实验室的数据统计，自 2014 年以来，针对工控设备软硬件的扫描与探测的类型和次数有逐年增多的趋势。

本报告则主要介绍了目前专注于网络空间中工控关键基础设施情报搜集的国内外组织，通过我们长期跟踪部分组织的扫描引擎动作行为，对其关注的工控资产类型和历史动作行为进行了分析。

二、情报收集的通用原理与技术

2.1 通用原理介绍

在传统网络中一般情况下需要鉴定一些服务、系统，往往可以通过端口扫描的方式来完成，比如检查一些知名端口的开放情况。通过端口开放的情况能大概了解目标系统运行了那些服务以及操作系统类型。具体要验证一些服务则可以使用对应的协议，去交互请求对应的内容。而在传统网络中大量的协议都是标准并公开的。

在工控系统这个情况则不一样，工控的设备、软件的数据传输广泛的使用了行业专有与私有通信协议，如 Modbus、IEC101/104、DNP3 等通用工控协议，当然也存在大量的私有协议。我们曾经在 “使用 Wireshark 分析工控协议” 中总结过工控网络中协议的几种类型，即标准协议，私有公开，私有不公开情况三种。

总体来说探测并定位工控软硬件可以使用其支持的协议来完成精确识别或模糊匹配，具体可以通过如下几种方式。

- 利用标准且公开的工控协议对工控系统进行定位

在一些标准的协议规范中如 Modbus、OPCUA、EtherNet/IP 等协议中，通常约定了固定的 Function code 读取应用及模块信息，这样我们便可以准确识别目标设备的厂商信息或产品信息，而不支持读取设备、应用信息的协议也可以确认目标开放并运行了工控相关的协议，如下列举了几种常见标准协议识别设备、应用的方式。

协议名	默认端口	请求功能	响应内容
MMS	102	请求厂商和模块信息	厂商和模块信息
Modbus	502	43 功能码	设备厂商和产品模块信息
IEC104	2404	启动连接	启动确认
DNP3	20000	请求链路状态	连接确认
OPCUA	4840	查找服务器请求	应用名称信息
EtherNet/IP	44818	枚举设备信息	制造厂商、模块信息、串号等信息

BACnet	47808	枚举设备信息	制造厂商、模块信息等信息

- 利用私有协议精确识别设备

私有协议一般用于对软硬件进行远程管理，数据传输，私有协议具有唯一性，通过私有协议可以准确的识别一个厂商及系列的设备类型，私有协议中特定的功能往往可以直接读取到设备的模块信息。如下是知名的几个工控厂商所使用的私有协议与识别设备信息的方式。

协议名	默认端口	请求功能	响应内容
Siemens S7	102	读 SZL	PLC 的模块信息、版本、串号等
Codesys	1200	读系统信息	系统信息
Mitsubishi MELSEC	5007	读 CPU 信息	PLC 的模块信息
Omron FINS	9600	读 CPU 单元信息	PLC 的模块信息
GE SRTP	18245	读 CPU 单元信息	PLC 的模块信息

- 利用传统服务特征对软硬件进行设备识别

另外工控的设备常常会开放一些传统服务，如 Web，SNMP 等服务，用于监视设备的运行状态或管理设备。如下为一些设备不同服务上的特征标识，这些标识可以用于识别设备。

厂商	设备	服务（端口）	特征
Siemens	S7 1200	HTTP（80）	Location: /Default.mwsl
		SNMP(161)	Siemens, SIMATIC S7, CPU-1200
	S7 300	HTTP（80）	Location: /Portal0000.htm
		SNMP(161)	Siemens, SIMATIC NET
Hollysys	LK Series	FTP(21)	Welcome to LK FTP services.
Mitsubishi	Q Series	FTP(21)	QnUDE(H)CPU FTP server ready.
Moxa	NPort	HTTP（80）	Server: MoxaHttp

更多可以参考，ICS 搜索 Dork。

2.2 工具与技术介绍

Redpoint 是由 Digitalbond 于 2014 年 3 月创建的 ICS 枚举工具，Redpoint 是一个基于 Nmap NSE 的脚本库，用户在使用 Nmap 扫描时可以选择如下脚本可获得枚举 ICS 设备的能力。

插件名称	端口	概述
BACnet-discover-enumerate.nse	47808	识别和枚举 BACnet 设备
atg-info.nse	10001	读取液位仪状态信息
codesys-v2-discover.nse	1200	识别和枚举 Codesys v2 控制器
cspv4-info.nse	2222	识别 PLC5/SLC 500 控制器
dnp3-info.nse	20000	识别 DNP3 协议
enip-enumerate.nse	44818	识别和枚举 EtherNet/IP 协议设备
fox-info.nse	1911	识别 Niagara Fox 软件
modicon-info.nse	502	枚举施耐德 PLC 信息
omrontcp-info.nse	9600	识别和枚举欧姆龙 PLC 信息
omronudp-info.nse	9600	识别和枚举欧姆龙 PLC 信息

pcworx-info.nse	1962	识别和枚举菲尼克斯 PLC 信息
proconos-info.nse	20547	识别和枚举使用 Proconos 的控制器
s7-enumerate.nse	102	识别和枚举西门子 S7PLC 信息

另外除了 Redpoint 发布的上述脚本之外，还有如下一些针对 ICS 的枚举和识别脚本，我们也在之前发布过三菱 Q 系列 PLC、Moxa 串口服务器识别与枚举脚本。

插件名称	端口	
mms-identify.nse	102	识别和枚举支持 IEC61850 协议的设备信息
modbus-discover.nse	502	识别和枚举 Modbus 设备信息
cr3-fingerprint.nse	789	识别和枚举红狮控制器信息
moxa-enum.nse	4800	识别和枚举 MoxaNPort 设备信息
melsec-discover.nse	5007	识别和枚举三菱 Q 系列 PLC 信息
melsecq-discover-udp.nse	5006	识别和枚举三菱 Q 系列 PLC 信息

纵观目前互联网上针对工控的诸多扫描探测都是基于如上 NSE 插件原理，进行此类研究的组织会在下面进行介绍。

三、关注 ICS 情报的组织介绍

3.1 国内组织介绍

- 信息安全企业

1） ZoomEye（开放式）

ZoomEye 是知道创宇打造的面向网络空间的搜索引擎，ZoomEye 于 2015 年 3 月上线了工控专题(ics.zoomeye.org)，ZoomEye 支持 12 种工控协议的数据检索，使用者也可以使用工控协议的端口和特征 Dork 关键字发现暴露在互联网的工控软硬件，对于工控协议类型的数据，ZoomEye 启用了保护策略，一般用户无法直接查看。

2） 傻蛋（开放式）

傻蛋联网设备搜索系统由湖南傻蛋科技有限公司研发，傻蛋目前并未对外宣称对工控协议进行了探测，并且系统内一般用户也无法通过工控协议端口搜索到数据，但从我们搜集到的数据来看，傻蛋的探测节点对工控协议有一定的探测抓取行为。

3） 中国网安（内部）

据公开的资料显示，中国电子科技集团网络信息安全有限公司（简称中国网安）曾发布过一款叫工业控制系统接入互联网威胁感知系统的产品，据资料介绍该系统具有扫描 ModbusTCP、EtherNet/IP、ISO-TSAP（S7）、FINS、WebSCADA 等协议的能力。

4） 绿盟（内部）

Seer 赛尔广谱平台来自绿盟科技研究院，绿盟广谱平台是一款网络空间数据与分析的搜索引擎，主要用于搜集互联网主机开放的端口，服务相关数据，绿盟曾经公开发布过“对欧姆龙设备全球统计报告”，根据其介绍该平台具有探测工控协议的能力。

- 科研院校

1） 谛听（开放式）

谛听由东北大学计算机学院编写研发，谛听主要针对于对工控设备的识别和定位，根据官网显示，目前谛听支持 12 种工控协议，使用者也可以使用 Dork 关键字在传统服务的特征中定位工控系统，该系统与知道创宇 ZoomEye 的 ICS 专题有较高的重合度。

2) 中科院信工所（内部）

据公开资料显示，信工所曾在此方面进行了研究，其“网络空间设备搜索系统”对常见的工控协议具有探测能力。

- 应急响应

1) 电子一所（内部）

据公开资料显示，自 2013 年初，电子一所开始受主管部门委托开展重要控制系统在线搜索监测工作，并建设了重要控制系统在线安全监测平台，对连接在互联网上的重要工业控制系统进行安全监测以及预警。电子一所的安全监测平台及关键技术获得了中国电子学会 2015 年科技进步奖，平台曾在 2015 年国家网络安全宣传周上展示，《焦点访谈》、《走近科学》等栏目对其有关工作进行了报导。

2) CNCERT（内部）

我们曾在“追踪 ICS 扫描者”一文中指出了 CNCERT 曾在此方面进行了研究。

3.2 国外组织介绍

1） Shodan（开放式）

Shodan 是一个联网设备搜索引擎，Shodan 于 2013 年增加了针对工控协议的探测，用户可以直接使用工控协议的端口直接检索该协议的所有数据，用户也可以使用特征 Dork 直接搜索对应设备数据。

2） Rapid7（研究项目）

Project Sonar 是 Rapid7 的一个安全研究项目，该项目通过扫描不同的服务和协议，来发现对应全球漏洞态势，Rapid7 基于此该项目曾第一时间发布过针对 ATGs 设备、MoxaNPort 设备的全网数据统计报告。

3） University of Michigan（研究项目）

Internet-Wide Scanning Research 是密歇根大学的安全研究项目，该项目通过扫描全网来了解协议或服务端口的分布和安全趋势。

4） Kudelski Security（研究项目）

Kudelski Security 是总部位于瑞士的一家信息安全公司，该公司的 K-SONAR 网络安全态势感知解决方案可以网络服务安全性进行监控，有数据显示该公司对 Modbus、BACnet 有周期的扫描探测。

3.3 各组织 ICS 探测成熟度分析

ICS 探测扫描组织的能力成熟度与组织本身的业务意图和技术能力相关，组织的业务意图决定组织需要的技术水平，并牵引组织的技术水平提升。ICS 探测扫描技术分为三个阶段，第一阶段为探索型阶段，主要验证探测扫描技术的可行性，在互联网上进行偶尔的冒烟测试或基于公开的数据进行验证；第二阶段为研究/测试型阶段，此阶段主要是对探测扫描技术的深度和广度进行验证测试，并在互联网上进行无规律的测试验证；第三阶段为运营型阶段，技术在深度和广度上已进行了非常深入的积累，并可支撑组织持续性的业务运营，持续性的提供服务，此阶段扫描行为相对比较规律。

灯塔实验室持续对 ICS 探测扫描行为进行跟踪研究，粗略对各组织进行分析如下：

组织名称	技术阶段	组织意图
Shodan	运营型	安全研究，已商业化
电子一所	运营型	行业风险通报（态势感知、应急响应）
Kudelski Security	运营型	安全研究，已实现产品化
Project Sonar(Rapid7)	研究/测试型	安全研究
ZoomEye（知道创宇）	研究/测试型	探索商业价值
University of Michigan	研究/测试型	安全研究
傻蛋（傻蛋科技）	研究/测试型	技术探索
CNCERT	探索型	应急响应
谛听（东北大学）	探索型	技术探索，试图商业化
中科院信工所	探索型	技术探索
中国网安	探索型	安全研究，试图产品化

四、ICS 情报收集的组织简要数据汇总

4.1 首次扫描时间与扫描节点 IP

目前我们已经从众多的探测扫描数据中确认了上述部分组织的 ICS 扫描行为、类型，以及该组织扫描器对应的 IP，其中追溯的时间跨度超过 2 年。根据出现的顺序我们整理了如下表。

组织名称	首次时间点	该组织扫描器 IP（红色为初次出现的 IP）
Shodan	2014-02-22	71.6.167.142 71.6.135.131 66.240.236.119 198.20.87.98 71.6.158.166 82.221.105.7 85.25.43.94 71.6.165.200* 198.20.99.130 66.240.192.138 71.6.146.185 66.240.219.146 198.20.70.113 198.20.69.98 198.20.70.114
Project Sonar(Rapid7)	2014-06-25	71.6.216.55* 71.6.216.32/27
ZoomEye（知道创宇）	2014-06-30	118.192.48.6

		118.192.48.17 118.192.48.18 118.192.48.27* 118.192.48.33 118.192.48.40 89.248.167.159 125.64.94.200 183.60.244.29
CNCERT	2014-11-09	202.108.211.62* 202.108.211.63*
Kudelski Security	2015-06-03	185.35.62.11* 185.35.62.1/22
谛听（东北大学）	2015-09-18	202.118.19.31 202.118.19.45* 202.118.19.95 202.118.19.125 202.118.19.148 202.118.19.197 202.118.19.188
中科院信工所	2015-11-17	54.238.133.8* 111.204.219.194 54.138.110.7 134.223.22.11 125.0.15.89
University of Michigan	2015-12-05	141.212.121.143* 141.212.121.0/24 141.212.122.0/24
傻蛋（傻蛋科技）	2015-12-24	113.240.250.155* 113.240.250.154 113.240.250.156 113.240.250.157
360	2016-01-09	61.240.144.65* 61.240.144.64 61.240.144.66 61.240.144.67
中国网安	2016-01-28	110.185.210.152*

4.2 扫描节点 IP 与关注的 ICS 协议

我们以 Shodan 当前支持的工控协议对标，分析了如上组织在扫描探测中关注的工控协议类型，如下表为该组织与对应扫描节点关注的协议类型。

注：根据我们的分析 Shodan 当前扫描了超过了 29 个工控或 IOT 类型软硬件的端口，

在我们目前已标注的组织中，绝大部分未超过该数量，所以我们选择了以 Shodan 当前支持的协议端口作为基准分析模版。

Shodan 当前支持端口	描述	关注此协议的其他组织 IP(部分)
102	Siemens S7/MMS	141.212.122.0/24（UMICH） 141.212.121.0/24（UMICH） 118.192.48.6（ZoomEye） 118.192.48.27（ZoomEye） 118.192.48.40（ZoomEye） 113.240.250.156（傻蛋） 113.240.250.155（傻蛋） 54.238.133.8（信工所） 61.240.144.65（360） 110.185.210.152（中国网安）
502	Modbus	141.212.122.0/24（UMICH） 141.212.121.0/24（UMICH） 118.192.48.6（ZoomEye） 118.192.48.40（ZoomEye） 185.35.62.220（Kudelski） 185.35.62.1/24（Kudelski） 113.240.250.156（傻蛋） 110.185.210.152（傻蛋） 202.118.19.31（谛听） 61.240.144.65（360） 110.185.210.152（中国网安）
771	RealPort	-
789	Red Lion	202.118.19.31（谛听） 118.192.48.40（ZoomEye）
1200	Codesys	-
1911	Tridium Fox	141.212.122.0/24（UMICH） 141.212.121.0/24（UMICH） 113.240.250.156（傻蛋） 202.118.19.31（谛听） 54.238.133.8（信工所） 118.192.48.40（ZoomEye） 110.185.210.152（中国网安）
1962	PCWorx	113.240.250.156（傻蛋） 202.118.19.31（谛听） 118.192.48.27（ZoomEye） 110.185.210.152（中国网安）
2123	GPRS Tunneling	-
2152	GPRS Tunneling	-
2404	IEC104	113.240.250.156（傻蛋） 202.118.19.31（谛听） 118.192.48.27（ZoomEye）

		118.192.48.40（ZoomEye） 110.185.210.152（中国网安）
2455	Codesys	-
3386	GPRS Tunneling	-
4800	Moxa NPort	-
4911	Tridium Fox SSL	-
5006	Mitsubishi MELSEC	-
5007	Mitsubishi MELSEC	202.118.19.31（谛听） 113.240.250.156（傻蛋） 118.192.48.27（ZoomEye） 118.192.48.40（ZoomEye）
5094	HART-IP	-
9600	OMRON FINS	113.240.250.156（傻蛋） 202.118.19.31（谛听） 125.64.94.200（ZoomEye）
10001	ATGs Devices	71.6.216.41（Rapid7）
17185	Vxworks WDB	118.192.48.33（ZoomEye） 71.6.216.44（Rapid7）
18245	GE SRTP	-
18246	GE SRTP	-
20000	DNP3	141.212.122.0/24（UMICH） 141.212.121.0/24（UMICH） 113.240.250.156（傻蛋） 113.240.250.155（傻蛋） 110.185.210.152（中国网安） 202.118.19.31（谛听） 118.192.48.40（ZoomEye）
20547	ProConOS	113.240.250.156（傻蛋） 202.118.19.31（谛听） 125.64.94.200（ZoomEye） 110.185.210.152（中国网安）
30718	Lantronix	-
34962	Profinet	-
37777	Dahua Dvr	113.240.250.155（傻蛋） 54.238.133.8（信工所） 61.240.144.64（360）
44818	EtherNet/IP	113.240.250.156（傻蛋） 113.240.250.155（傻蛋） 118.192.48.27（ZoomEye） 118.192.48.40（ZoomEye） 125.64.94.200（ZoomEye） 202.118.19.31（谛听） 110.185.210.152（中国网安）

47808	BACnet	141.212.122.0/24（UMICH） 141.212.121.0/24（UMICH） 185.35.62.1/24（Kudelski） 113.240.250.156（傻蛋） 202.118.19.31（谛听） 54.238.133.8（信工所） 71.6.216.55（Rapid7）

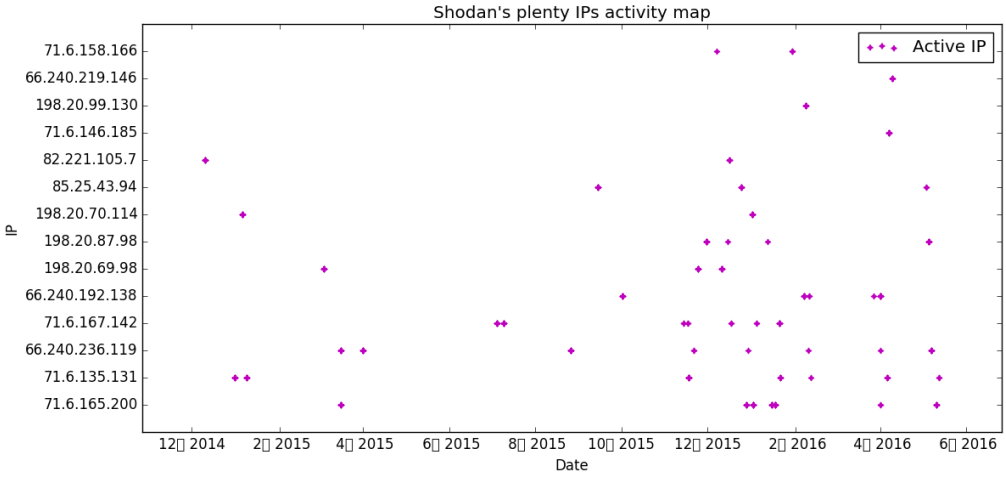
五、国外组织探测扫描行为分析

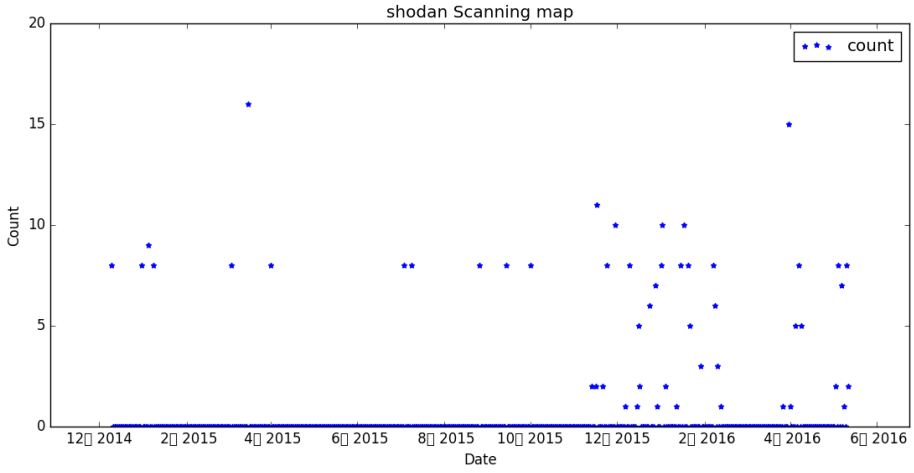
5.1 Shodan(Shodan.io)

5.1.1 针对扫描节点的行为统计

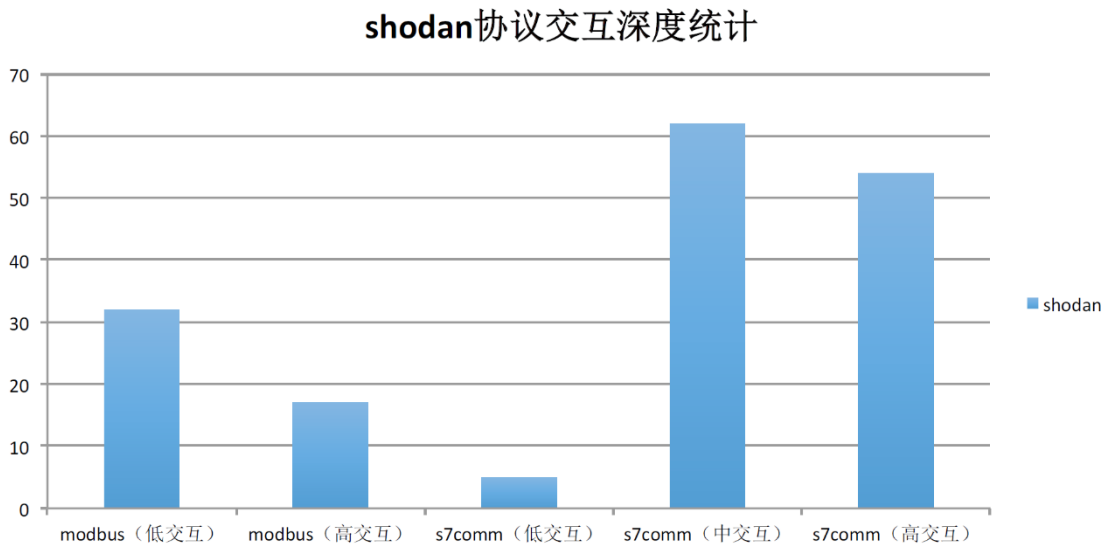
IP 地址	开始统计时间	活跃结束时间	会话次数	针对协议	存在高交互行为
71.6.167.142	2015/07/04 23:25	2016/1/20	10 次	s7comm(9) modbus(1)	√
71.6.135.131	2014/12/31 07:08	至今	12 次	s7comm(7) modbus(5)	√
66.240.236.119	2015/11/21 10:10	至今	13 次	s7comm(10) modbus(3)	√
198.20.87.98	2015/11/30 09:53	2016/5/5	8 次	modbus(6) s7comm(2)	×
71.6.158.166	2015/12/7 08:13	至今	5 次	modbus(2) s7comm(3)	√
82.221.105.7	2014/12/10 05:29	2015/12/16	1 次	s7comm(1)	√
85.25.43.94	2015/12/24 16:08	至今	5 次	s7comm(3) modbus(2)	√
71.6.165.200	2015/03/16 10:59	2016/5/11	15 次	s7comm(12) modbus(3)	√
198.20.99.130	2016/2/8 10:02	2016/2/8	1 次	s7comm(1)	√
66.240.192.138	2015/10/01 12:58	2016/3/31	11 次	modbus(7) s7comm(4)	√
71.6.146.185	2016/4/7 05:46	2016/4/7	4 次	modbus(4)	×
66.240.219.146	2016/4/9	2016/4/9	1 次	s7comm(1)	√

	21:45				
198.20.70.113	2015/1/5 19:12	2016/01/01	5 次	s7comm(5)	√
198.20.69.98	2015/3/4 04:59	2015/11/24	6 次	s7comm(6)	√
198.20.70.114	2015/1/5 19:12	2016/1/1	5 次	s7comm(5)	√





5.1.2 协议交互深度统计



5.1.3 组织行为分析

从我们收集的数据来看，Shodan 针对 Modbus 与 S7comm 协议进行扫描的 IP 地址存在 15 个（不完全统计），遍布美国、德国、荷兰等不同地域，同时具备强大的分布式调度能力。从针对工控专用协议扫描探测的过程来看，Shodan 扫描引擎对工控协议的情报收集可以追溯到 2014 年。据不完全统计，截至目前 Shodan 已经支持了超过 29 个工控协议。

从协议扫描深度来看，Shodan 基于 Modbus 协议的扫描已经深入到可识别 PLC 上具体项目文件信息，同时 Shodan 针对 Modbus 信息的获取仅依赖 4 个包含 90 功能码数据包，在保证获取相同信息的同时极大程度提高了扫描效率，由此可见 Shodan 团队对于协议的分析理解程度极高。

从扫描方式上来看，Shodan 在针对 Modbus 协议进行扫描时，在判断 502 端口开放后先进行了通过 17 功能码进行的确认帧，在收到了正确的响应后才正式开始发送数据包；针对 S7 协议扫描时，同样也会先进行 TPKP 和 COTP 连接，再确认连接无误后，重新进行正式扫描行为，该处理细节能保证扫描行为的精准性和高效性，避免设备端口接受到非匹配协议数据而产生隐患。

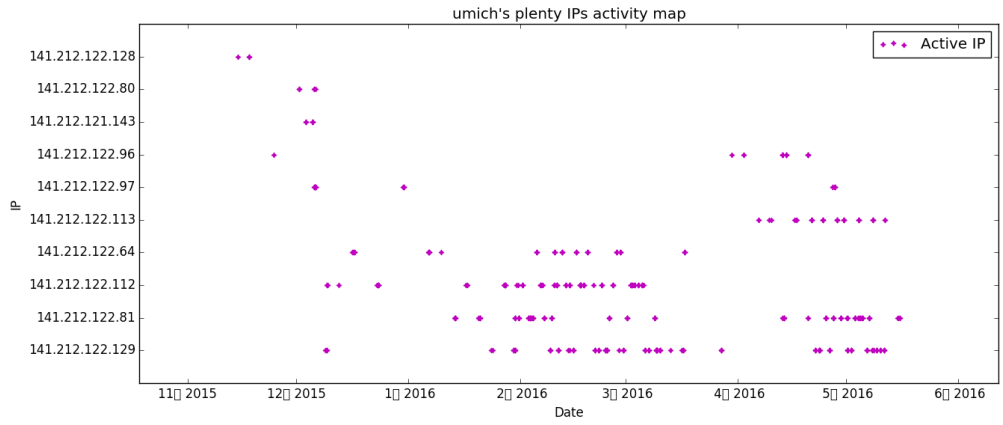
从行为的时间分布上来看，Shodan 团队针对工控协议的扫描具有明显的时间规律，Shodan 同时对社区关注极高，目前已经集成了我们曾经发布的 GE SRTP、MELSEC-Q、MoxaNPort 探测识别方法。

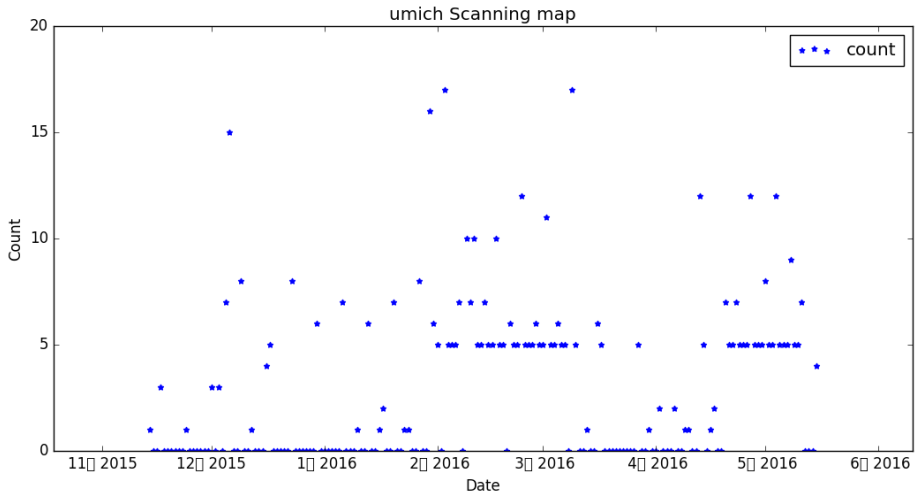
另外，值得关注的是 Shodan 还具备针对工控协议蜜罐的识别机制，该机制依赖 IP 基础位置信息、开放端口情况、蜜罐默认配置信息等进行综合评判，通过产生量化的系数来进行蜜罐甄别。

5.2 University of Michigan

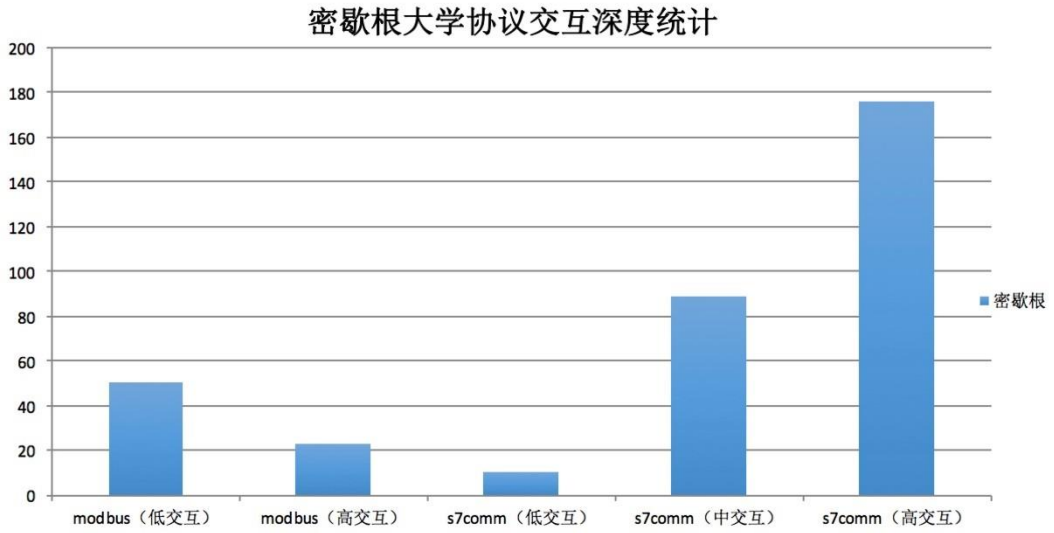
5.2.1 针对扫描节点的行为统计

IP 地址	开始统计时间	活跃结束时间	会话次数	针对协议	存在高交互行为
141.212.122.128	2015/11/14 23:18	2015/11/17	2 次	modbus(2)	√
141.212.122.96	2015/11/24 18:22	2016/4/2	7 次	modbus(3) s7comm(4)	√
141.212.122.80	2015/12/1 21:54	2015/12/6	4 次	modbus(4)	×
141.212.122.143	2015/12/3 14:56	2015/12/3	4 次	modbus(3) s7comm(1)	√
141.212.122.97	2015/12/6 1:06	2014/4/27	9 次	s7comm(9)	√
141.212.122.129	2015/12/9 0:48	至今	44 次	modbus(15) s7comm(29)	√
141.212.122.81	2016/1/13 17:33	至今	39 次	modbus(7) s7comm(32)	√
141.212.122.113	2016/4/6 18:29	至今	15 次	modbus(5) s7comm(10)	×
141.212.122.64	2015/12/16 13:38	2016/1/10	15 次	modbus(1) s7comm(14)	×
141.212.122.112	2015/12/9 10:36	2016/3/5	38 次	modbus(10) s7comm(28)	√





5.2.2 协议交互深度统计



5.2.3 组织行为分析

从当前数据来看 Censys 平台数据依赖于密歇根大学的 Internet-Wide Scanning 项目，Internet-Wide Scanning 项目具备细粒度的时间轴态势感知能力以及成熟稳定的工程化数据采集能力。

从行为出口 IP 地址数量来看，仅针对 Modbus 于 S7comm 协议的地址存在 10 个（不限于），该扫描引擎具备分布式管理调度能力。从协议扫描深度来看，其引擎具备稳定的交互协议扫描深度。

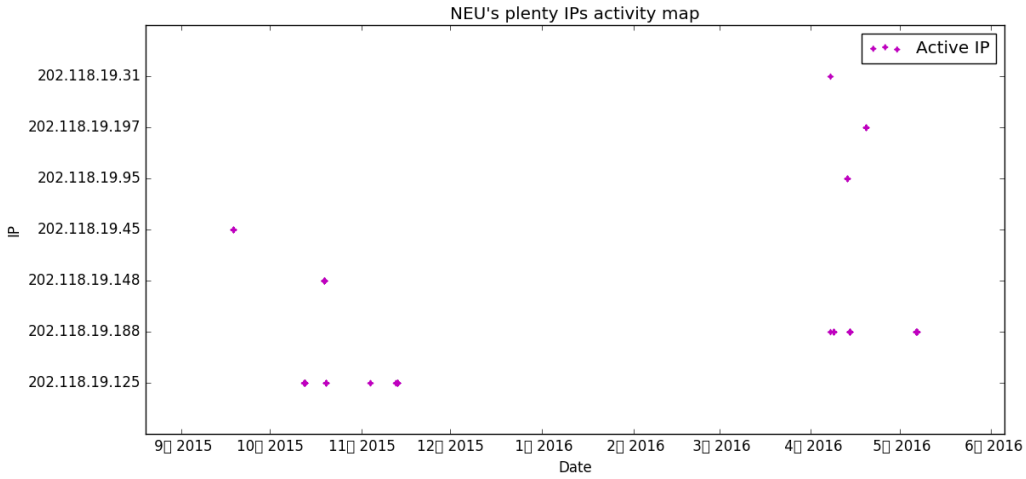
从扫描方式上看，该引擎采取了简单、稳定的扫描方式，具备较高的效率。从行为的时间分布上来看，所有扫描节点都具备很高的时间规律性，相比同类扫描引擎具有较高的扫描频率，其具备时间轴上更加细粒度的扫描探测能力。

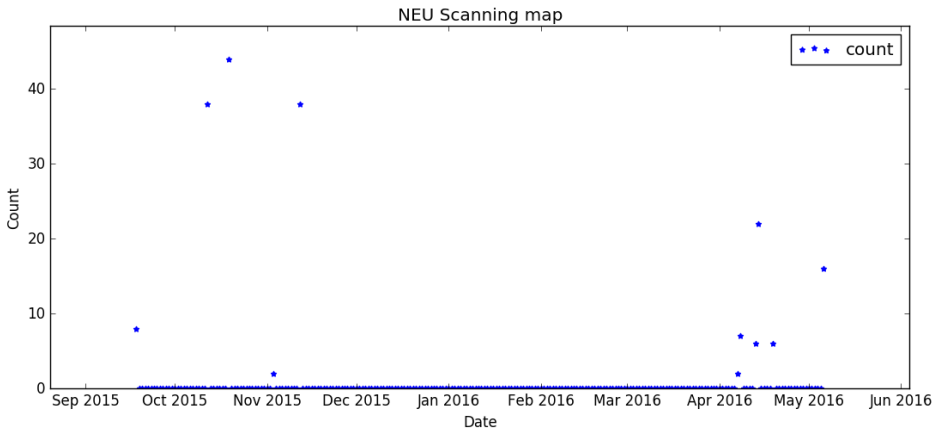
六、国内组织探测扫描行为分析

6.1 谛听（icsfind.com）

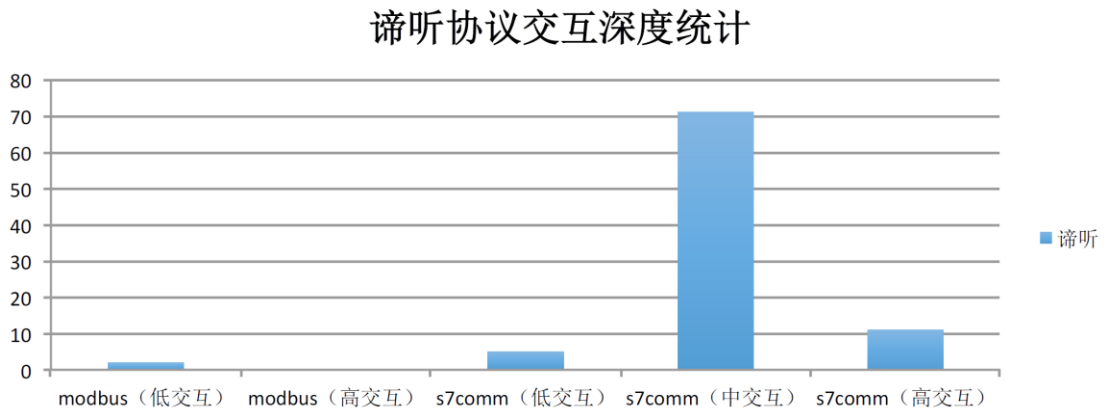
6.1.1 针对扫描节点的行为统计

IP 地址	开始统计时间	活跃结束时间	会话次数	针对协议	存在高交互行为
202.118.19.31	2016/4/7 14:11	2016/4/7	1 次	s7comm(1)	×
202.118.19.45	2015/9/18 12:35	2015/9/18	2 次	s7comm(1)	√
202.118.19.95	2016/4/13 03:13	2016/4/13	2 次	modbus(2)	√
202.118.19.125	2015/10/12 11:06	2015/11/12	41 次	s7comm(41)	√
202.118.19.148	2015/10/19 03:43	2015/10/19	18 次	s7comm(18)	×
202.118.19.197	2016/04/19 15:08	2016/4/19	2 次	s7comm(2)	√
202.118.19.188	2016/04/07 12:44	至今	15 次	s7comm(15)	√





6.1.2 协议交互深度统计



6.1.3 组织行为分析

谛听网络空间工控设备搜索平台原名 426 网络空间安全搜索引擎工控篇，最早于 2015 年 12 月被媒体报道。从我们的数据分析来看，该搜索引擎从 2015 年 9 月 18 号开始针对工控协议扫描，然而该团队行为活跃到 2015 年 11 月后就没有了明显行为，直到 2016 年 4 月 19 号重新出现。

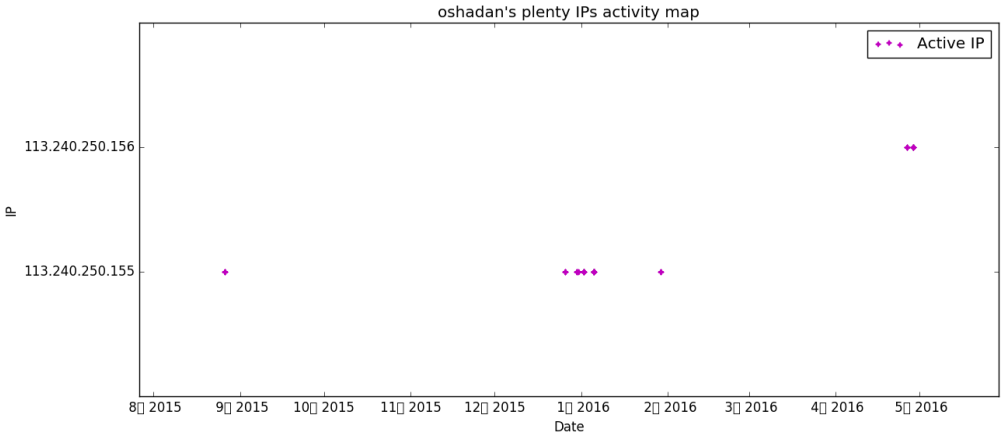
根据在平台查找 Modbus、S7 数据，显示数据获取时间为 2015 年 10 月 19、20 日，可以看出谛听搜索平台公开数据过于陈旧，相比于同类引擎从数据总量与时间轴感知能力方面欠缺，同时平台数据的存量也不及同类平台。

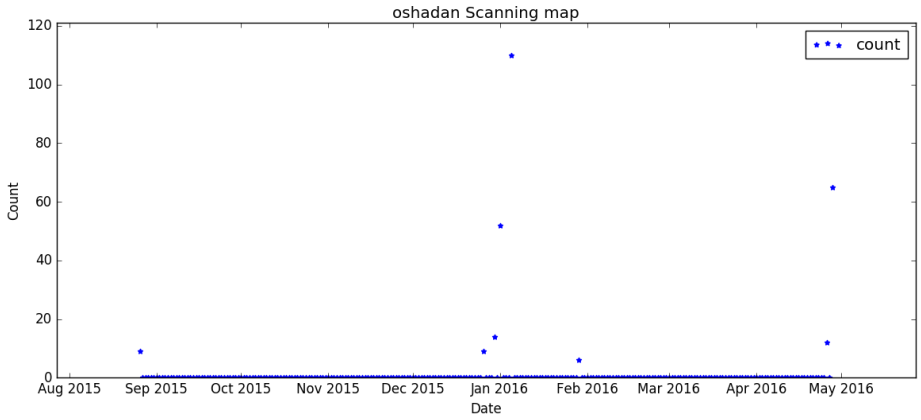
从协议交互深度与扫描行为方式上看，该引擎 Modbus 协议交互程度较低，S7 协议使用了 SCADA Strange Love 发布的 plcscan 脚本相同的交互方式。

6.2 傻蛋（oshadan）

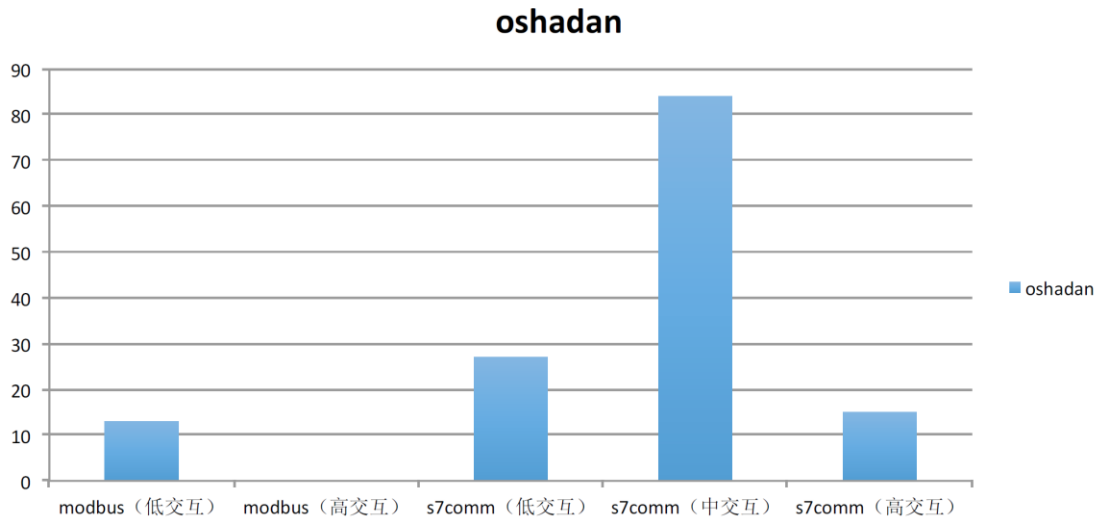
6.2.1 针对扫描节点的行为统计

IP 地址	开始统计时间	活跃结束时间	会话次数	针对协议	存在高交互行为
113.240.250.155	2015/8/26 10:36	2016/1/29	99 次	modbus(13) s7comm(86)	√
113.240.250.156	2016/4/28 17:53	2016/4/28	27 次	s7comm(27)	×





6.2.2 协议交互深度统计



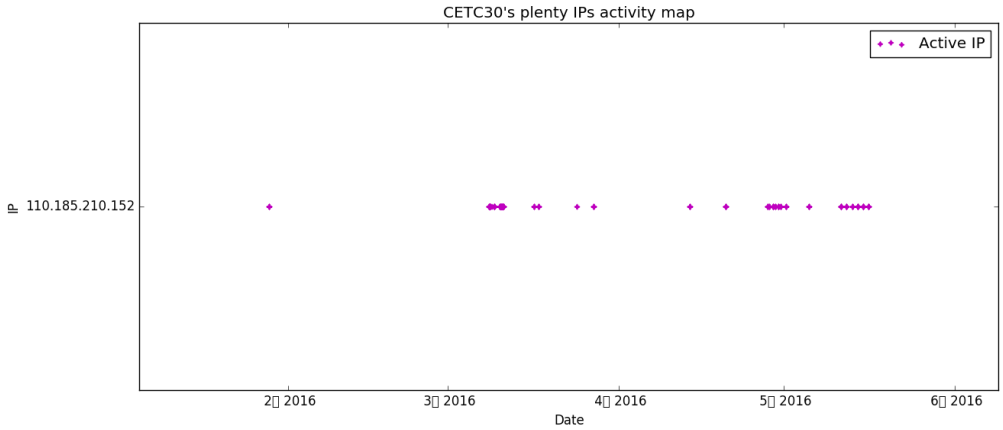
6.2.3 组织行为分析

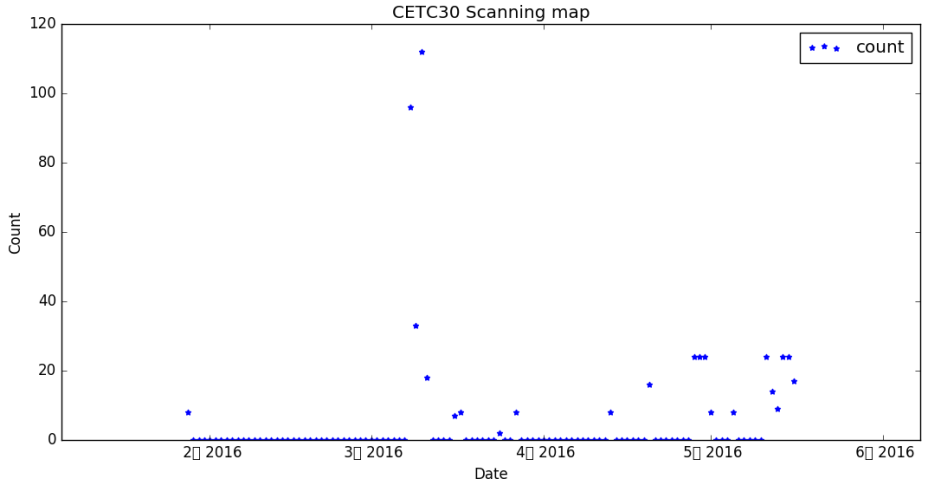
傻蛋联网设备搜索平台虽然主要针对 web 框架的搜索、识别，但从行为时间分布上，该引擎从 2015 年 8 月 26 日开始收集工控设备端口信息，其数据未在平台公开；从扫描频率及深度来看，该团队具备了稳定的针对工控协议的扫描探测能力。我们推测该团队的此类数据可能只面向特定用户或积累到一定程度后在平台公开。

6.3 中国网安

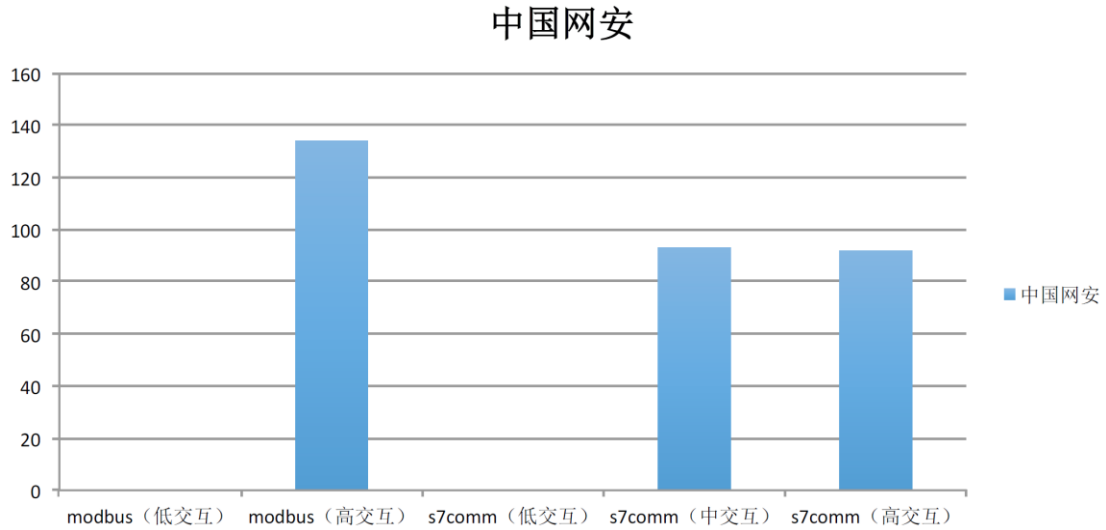
6.3.1 针对扫描节点的行为统计

IP 地址	开始统计时间	活跃结束时间	会话次数	针对协议	存在高交互行为
110.185.210.152	2016/1/28 13:44	2016/5/15 至今	104 次	modbus(11) s7comm(93)	√





6.3.2 协议交互深度统计



6.3.3 组织行为分析

从我们的数据来看，该团队于 2016 年 1 月开始针对工控设备进行识别扫描，我们注意到该团队疑似的一些测试行为，在一些时间点存在重复多次的连接与交互行为，其行为主要从 2016 年 3 月 13 日开始，110.185.210.152 在 13 日就有 19*7 次，20 日 19*24 次，15 日 19*23 次，16 日 19*15 次的高频率扫描，之后保持每日一次左右的探测行为，另外值得注意的该引擎针对 modbus 协议具备高交互扫描行为，然而该引擎的扫描脚本是基于 Redpoint 的 modicon-info 稍加改良后的版本，其携带了大量与功能标识无关的额外交互数据，这导致了扫描探测到施耐德 PLC 时交互时间长，请求数量多，相比于 Shodan 基于 modbus 的高交互扫描显得比较臃肿。