

THE  
CURIOUS  
CASE OF  
FAKE  
BRITISH LIRS

**RIPE 78**  
Reykjavík, Iceland  
20 - 24 May, 2019

# ABOUT



SECURITY CONSULTANT



15 YEARS EXPERIENCE IN  
VARIOUS SECURITY DISCIPLINES



# AGENDA

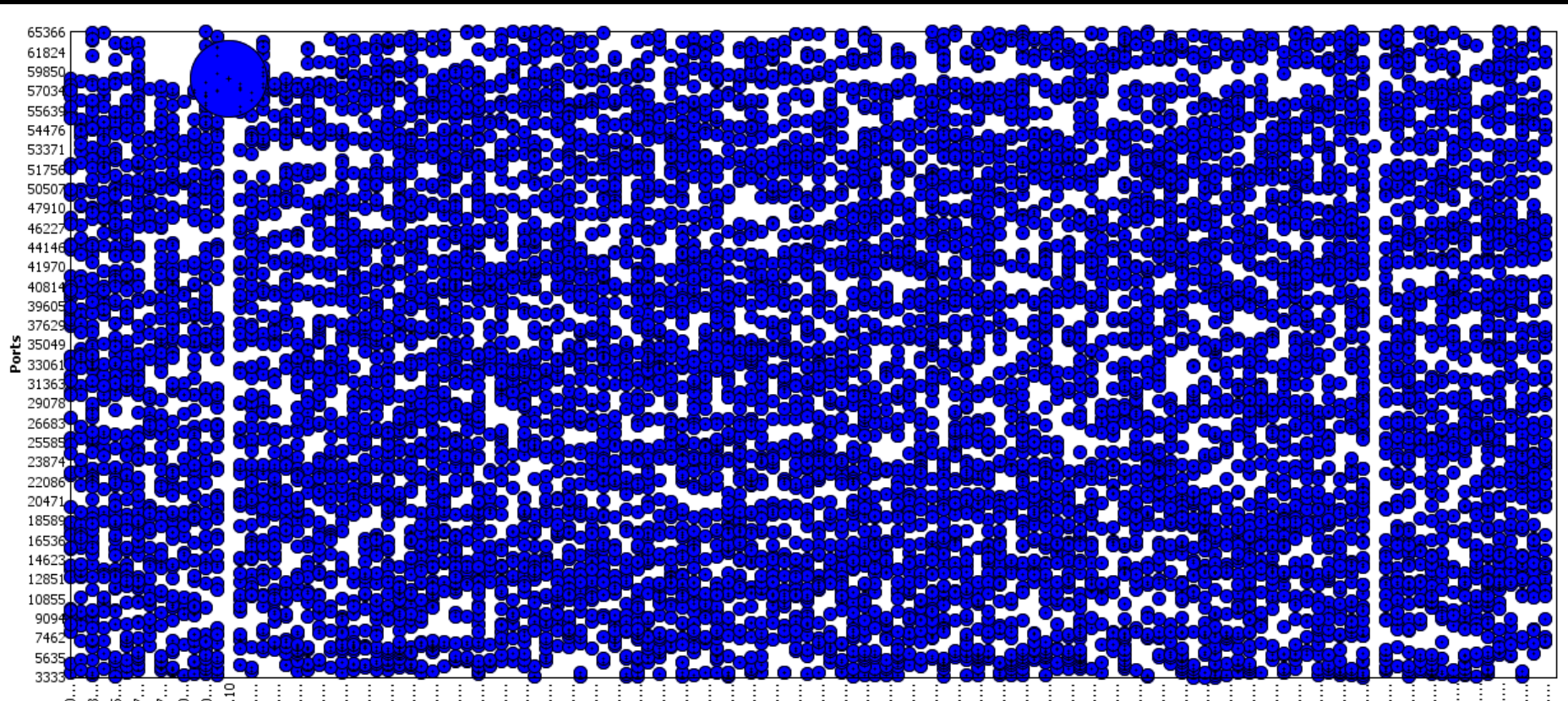
- Demonstrate a few case studies for abuse cases
- Highlight the importance of accurate RIPE DB records



# DISCLAIMER

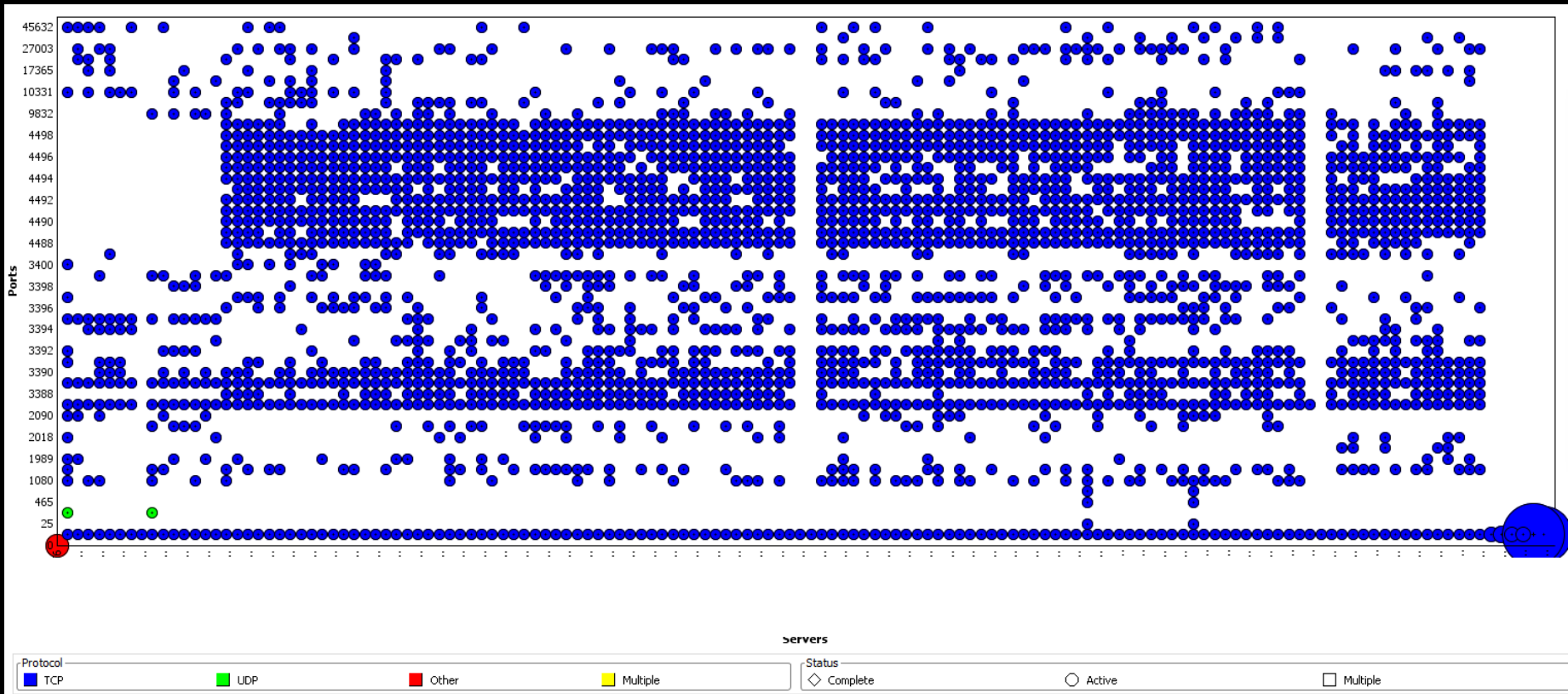
Names of persons and organisations within this presentation are included for completeness. No implication of guilt or association should be implied.

# HOW HAS THIS STARTED?



# CABLE COM DATA CABLING SERVICES LTD

## 5.188.10.0/24



# CABLE COM DATA CABLING SERVICES LTD

role: CABLE COM DATA CABLING SERVICES Contact Role  
address: 13 Bosworth Close, Milton Keynes, MK3 7UB  
address: United Kingdom  
phone: +44 7441922479  
fax-no: +44 7441922479  
abuse-mailbox: abuse@cablecom.org  
nic-hdl: CCDC7-RIPE  
mnt-by: cablecom-mnt  
created: 2017-11-08T19:54:37Z  
last-modified: 2017-11-08T19:54:37Z  
source: RIPE# Filtered

---

person: Roy Bray  
address: 13 Bosworth Close, Milton Keynes, MK3 7UB, United Kingdom  
phone: +44 7441922479  
nic-hdl: RB29150-RIPE  
mnt-by: cablecom-mnt  
created: 2017-11-08T19:52:06Z  
last-modified: 2017-11-08T19:52:06Z  
source: RIPE



---

# CABLE COM DATA CABLING SERVICES LTD

¿Website?



# CABLE COM DATA CABLING SERVICES LTD

role: CABLE COM DATA CABLING SERVICES Contact Role  
address: 13 Bosworth Close, Milton Keynes, MK3 7UB  
address: United Kingdom  
phone: +44 7441922479  
fax-no: +44 7441922479 **Voxbone SA Allocation**  
abuse-mailbox: abuse@cablecom.org  
nic-hdl: CCDC7-RIPE  
mnt-by: cablecom-mnt  
created: 2017-11-08T19:54:37Z  
last-modified: 2017-11-08T19:54:37Z  
source: RIPE# Filtered

---

person: Roy Bray  
address: 13 Bosworth Close, Milton Keynes, MK3 7UB, United Kingdom  
phone: +44 7441922479  
nic-hdl: RB29150-RIPE  
mnt-by: cablecom-mnt  
created: 2017-11-08T19:52:06Z  
last-modified: 2017-11-08T19:52:06Z  
source: RIPE

Domain Name: CABLECOM.ORG

Registry Domain ID: D402200000004145606-LROR

Registrar WHOIS Server: whois.bizcn.com

Registrar URL: www.bizcn.com

Updated Date: 2018-10-16T15:50:53Z

Creation Date: 2017-11-08T17:54:52Z

Registry Expiry Date: 2019-11-08T17:54:52Z

Registrar Registration Expiration Date:

Registrar: Bizcn.com, Inc.

Registrar IANA ID: 471

Registrar Abuse Contact Email: abuse@bizcn.com

Registrar Abuse Contact Phone: +86.5922577888

Reseller:

Domain Status: clientTransferProhibited  
<https://icann.org/epp#clientTransferProhibited>

Registrant Organization: Wuxi Yilian LLC

Registrant State/Province: Fujian

Registrant Country: CN

Name Server: NS1.CABLECOM.ORG

Name Server: NS2.CABLECOM.ORG

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form <https://www.icann.org/wicf/>

>>> Last update of WHOIS database: 2018-12-10T15:10:32Z <<<

# WHOIS

# CABLE COM DATA CABLING SERVICES LTD

## CABLE COM DATA CABLING SERVICES LTD

Company number **10987600**

Follow this company

File for this company

Overview

Filing history

People

Officers

Persons with significant control

### Filter officers

Current officers

**1 officer / 0 resignations**

### [BRAY, Roy Victor](#)

Correspondence address

**23 York House, Kenilworth Drive, Bletchley, Milton Keynes, England, MK3 6AH**

Role **ACTIVE**

**Director**

Date of birth

**August 1958**

Appointed on

**29 September 2017**

Nationality

**British**

Country of residence

**England**

Occupation

**Data Engineer**

# CABLE COM DATA CABLING SERVICES LTD



# CABLE COM DATA CABLING SERVICES LTD



# CABLE COM DATA CABLING SERVICES LTD



Companies  
House



Contract sent  
via recorded  
mail

- Online or paper registration
- Tax office sends UTR to registered address



# CABLE COM DATA CABLING SERVICES LTD

inetnum: 5.188.10.0 -5.188.11.255  
netname: CableCom-net  
descr: VPS and webhosting  
country: GB  
org: ORG-CCDC6-RIPE  
admin-c: CCDC7-RIPE  
tech-c: CCDC7-RIPE  
status: ASSIGNED PA  
mnt-by: **MNT-PINSUPPORT**  
mnt-domains: cablecom-mnt  
mnt-routes: cablecom-mnt  
mnt-routes: MNT-NFORCE  
created: 2017-11-08T16:23:29Z  
last-modified: 2018-01-06T12:32:24Z  
source: RIPE

## Petersburg Internet Network Ltd.

Babushkina st. 3, office 215.

192029 Saint-Petersburg

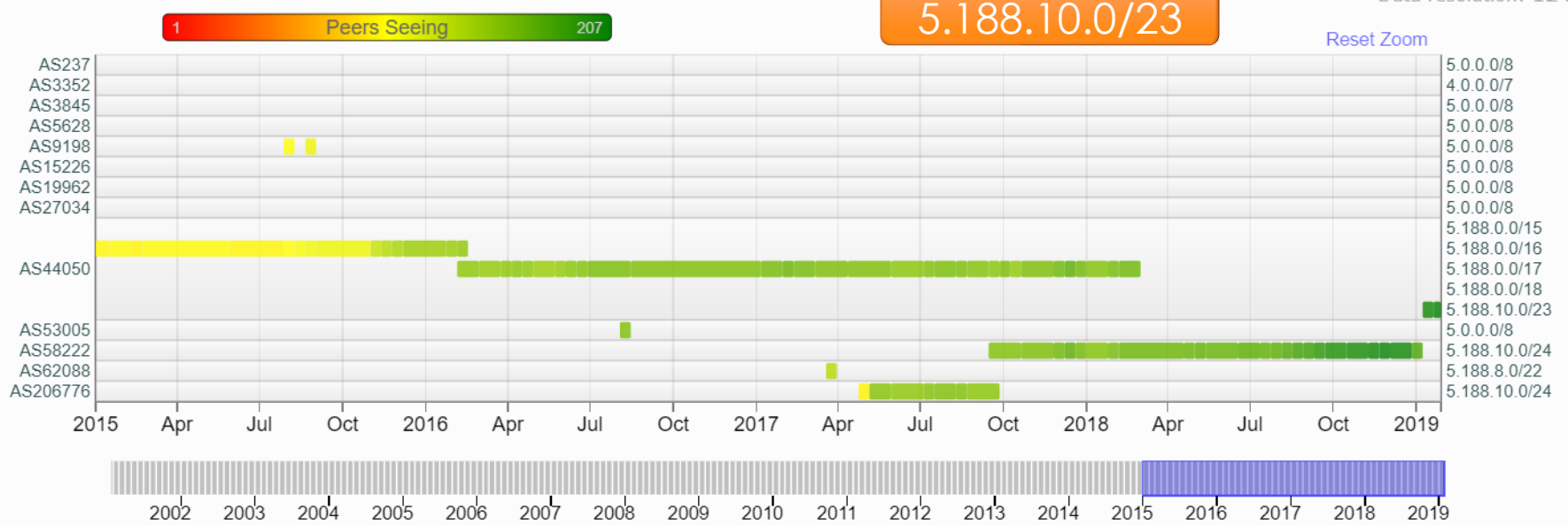
RUSSIAN FEDERATION

phone: +78126772525

fax: +78123093916

e-mail: [info \(at\) pinspb \(dot\) ru](mailto:info@pinspb.ru)

Areas serviced: RU

**AS206776**

Histate Global Corp (BVI)

Histate.net registered with Tapi.net (DE) – Sept 2016

LIR created in Nov 2016

**AS62088**

SinaroHost LTD (NL)

sinarohost.com registered with the Regional Network Information Center (RU) – January 2014

LIR created in Feb 2014

**AS58222**

Solar Invest UK LTD (UK)

dedinet.biz registered with a Eranet.com (HK) – Sept 2017

LIR created in Sept 2017

**AS44050**

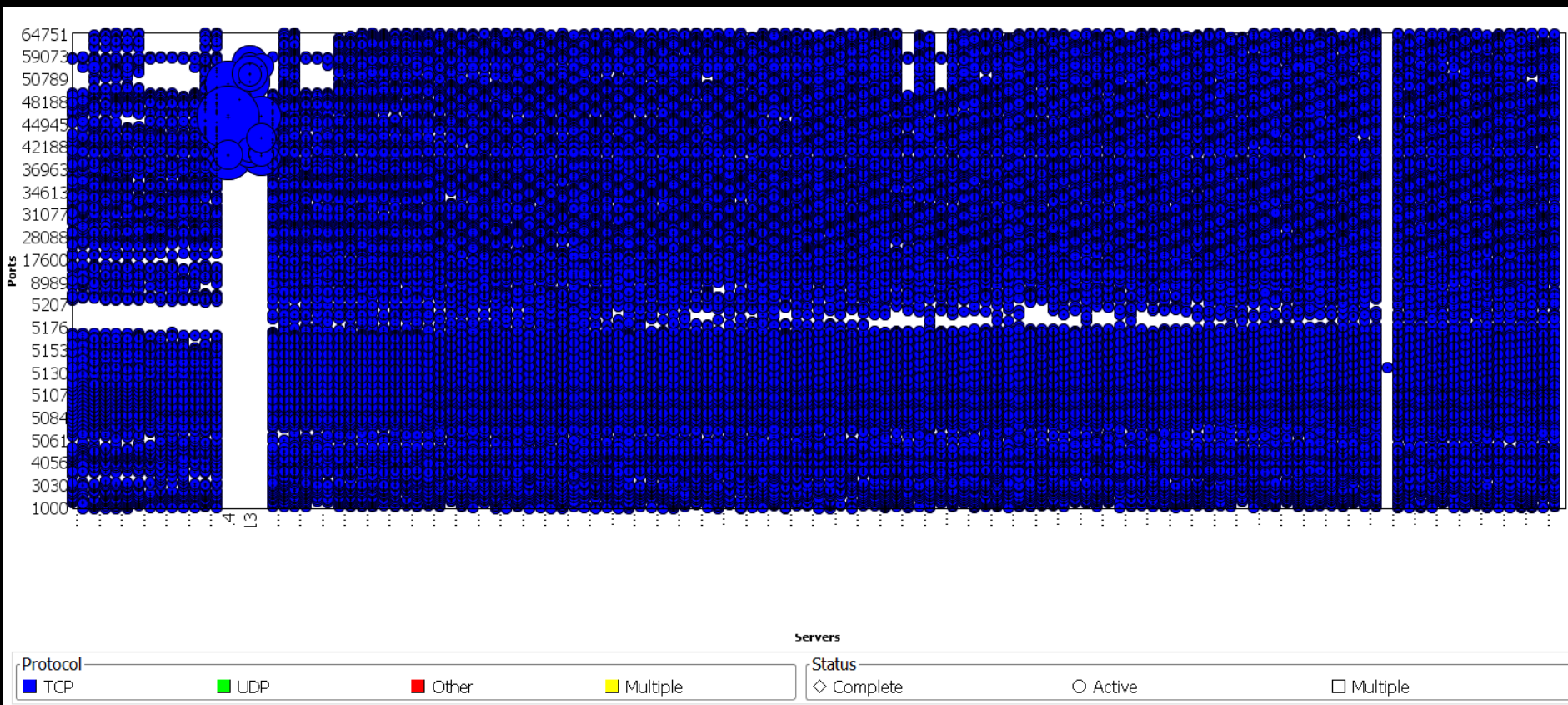
Petersburg Internet Network (RU)

Previous history for routes hijacking



# SOLAR INVEST UK LTD

## 109.248.9.0/24



# SOLAR INVEST UK LTD WHOIS

Registrar URL: [www.bizcn.com](http://www.bizcn.com)

Updated Date: 2018-05-29T11:40:02Z

Creation Date: 2018-05-24T11:40:02Z

Registry Expiry Date: 2019-05-24T11:40:02Z

Registrar: Bizcn.com, Inc.

Registrar IANA ID: 471

Domain Status: clientTransferProhibited  
<https://icann.org/epp#clientTransferProhibited>

Registrant Organization: Moris Adam

Registrant State/Province: Tiraspol

Registrant Country: gb

Name Server: ns4.cnmsn.com

Name Server: ns3.cnmsn.com

Many empty fields have been removed here

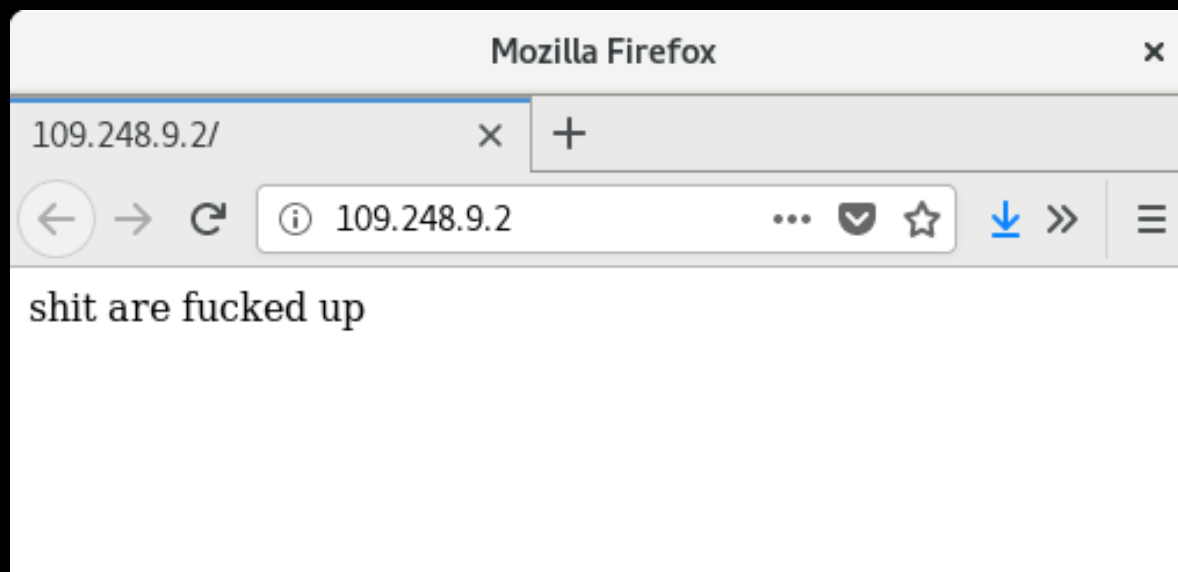
# SOLAR INVEST UK LTD

inetnum: 109.248.9.0 -  
109.248.9.255  
netname: SOLARNET  
country: GB  
org: ORG-SIUL1-RIPE  
status: ASSIGNED PA  
admin-c: TZ2321-RIPE  
tech-c: TZ2321-RIPE  
mnt-by: MNT-NETART  
mnt-routes: SOLARINVEST  
mnt-domains: SOLARINVEST  
created: 2017-09-12T14:27:28Z  
last-modified: 2017-09-18T14:34:27Z  
source: RIPE

organisation: ORG-SIUL1-RIPE  
org-name: Solar Invest UK LTD.  
org-type: OTHER  
address: 1st Floor, Unit 9 Old Field  
Road, Bocam Park,  
address: Pencoed, Bridgend,  
Wales, CF35 5LJ  
address: United Kingdom  
phone: +44.8458710942  
fax-no: +44.8458710943  
abuse-c: abuse@solarnet.biz  
mnt-ref: SOLARINVEST  
mnt-by: SOLARINVEST  
created: 2017-09-10T09:24:56Z  
last-modified: 2018-05-24T15:54:10Z  
source: RIPE # Filtered

# EXAMPLE OF RUNNING SERVICES

shodan.io



```
graph TD; A["AS58222  
Solar Invest UK LTD"] --> B["109.248.9.0/24  
Solar Invest UK Ltd"]; A --> C["5.188.10.0/24  
Cable Com Data  
Cabling Service Ltd"]
```

AS58222  
Solar Invest UK LTD

109.248.9.0/24  
Solar Invest UK Ltd

5.188.10.0/24  
Cable Com Data  
Cabling Service Ltd


60.0.0.0/13  
China Unicom Hebei  
Province Network

60.2.28.238

AS58222  
Solar Invest UK LTD

109.248.9.0/24  
Solar Invest UK Ltd

5.188.10.0/24  
Cable Com Data  
Cabling Service Ltd



Redis key-value store Version: 3.2.9

```
# Server
redis_version:3.2.9
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:2e87aa2ac1b4005e
redis_mode:standalone
os:Linux 3.10.0-957.1.3.el7.x86_64 x86_64
arch_bits:64
multiplexing_api:epoll
gcc_version:4.9.2
process_id:1
run_id:a129eb974380f7c61978fb2b56799a3ea607a981
tcp_port:6379
uptime_in_seconds:360835
uptime_in_days:4
hz:10
lru_clock:15028064
executable:/data/redis-server
config_file:
```

shodan.io

```
# Connected Clients
addr=[REDACTED]:61924 fd=328 name= age=7217 idle=4 flags=N db=0 sub=0 psub=0 multi=-1 q
buf=0 qbuf-free=0 obl=0 oll=0 omem=0 events=r cmd=hset
addr=[REDACTED]:61925 fd=304 name= age=7217 idle=4 flags=N db=0 sub=0 psub=0 multi=-1 q
buf=0 qbuf-free=0 obl=0 oll=0 omem=0 events=r cmd=set
addr=[REDACTED]:61926 fd=332 name= age=7217 idle=2 flags=N db=0 sub=0 psub=0 multi=-1 q
buf=0 qbuf-free=0 obl=0 oll=0 omem=0 events=r cmd=set
addr=[REDACTED]:53948 fd=336 name= age=0 idle=0 flags=N db=0 sub=0 psub=0 multi=-1
qbuf=0 qbuf-free=32768 obl=0 oll=0 omem=0 events=r cmd=client
```



# 公安视频图像信息综合应用平台

登录


记住用户名

登录

证书登录

↓ 点击查看工具下载

← → ↻ 🏠 ⓘ Not secure | 60.2.28.238:81/cas/login ☆ 👤 ⋮



# 公安视频图像信息综合应用平台

登录

👤 用户名

🔒 密码

记住用户名

登录 证书登录

📄 点击查看工具下载

Google Translate

Public security video image  
information comprehensive  
application platform





# 公安视频图像信息综合应用平台

登录

记住用户名

点击查看工具下载



Emblem of the People's Police of the PRC (with branches outside the Public Security organs)

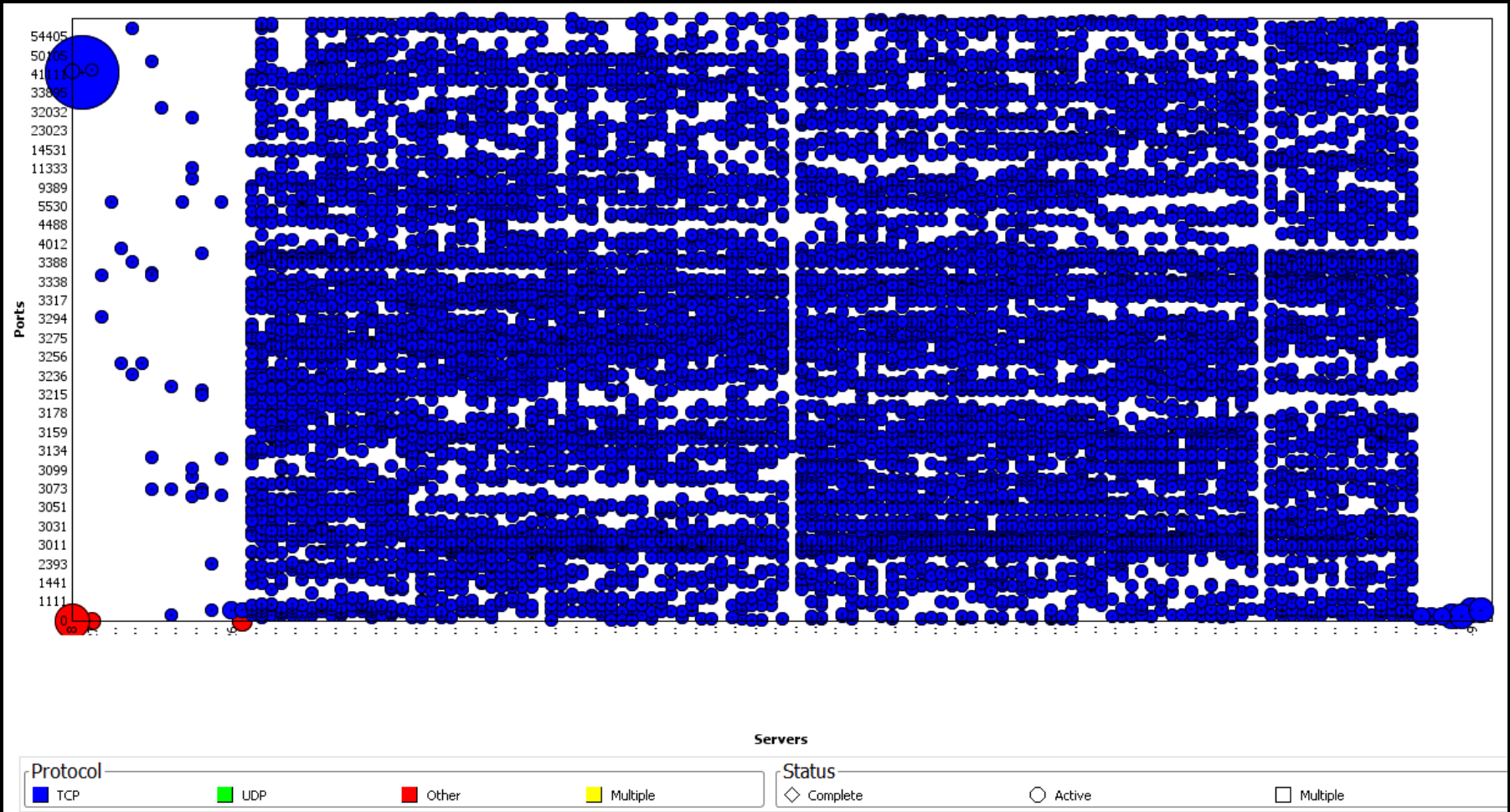
Wikipedia

Google Translate

Public security video image information comprehensive application platform

# UNITED PROTECTION (UK) SECURITY LIMITED

## 77.72.85.0/24



# UNITED PROTECTION (UK) SECURITY LIMITED

inetnum: 77.72.85.0 -  
77.72.85.255  
netname: UPUKS-NET  
country: BG  
admin-c: UPSL1-RIPE  
org: ORG-UPSL4-RIPE  
mnt-routes: histate  
tech-c: UPSL1-RIPE  
status: ASSIGNED PA  
mnt-by: MNT-NETUP  
mnt-by: UPUKS-MNT  
created: 2017-09-09T18:37:51Z  
last-modified: 2017-09-12T16:50:24Z  
source: RIPE

role: United Protection Security (UK)  
Ltd.  
address: 141-149 Lower Bryan Street  
Hanley, Stoke On Trent, Staffordshire,  
England, ST1 5AT  
address: UK  
org: ORG-UPSL4-RIPE  
abuse-mailbox: abuse@ups-service.co.uk  
phone: +44.8456448840  
fax-no: +44.8456448841  
nic-hdl: UPSL1-RIPE  
mnt-by: UPUKS-MNT  
created: 2017-01-26T09:06:26Z  
last-modified: 2018-10-04T22:35:18Z  
source: RIPE # Filtered

# UNITED PROTECTION (UK) SECURITY LIMITED WHOIS

Domain name:

ups-service.co.uk

Data validation:

Nominet was not able to match the registrant's name and/or address against a 3rd party source on 02-Oct-2018

Registrar:

Namecheap, Inc. [Tag = NAMECHEAP-INC]

URL: <https://www.namecheap.com>

Relevant dates:

Registered on: 02-Oct-2018

Expiry date: 02-Oct-2020

Last updated: 03-Oct-2018

Registration status:

Registered until expiry date.

Name servers:

ns1.ups-service.co.uk **195.123.224.142 >> AS: Layer6 Networks .. Announced on the same ASN as "Hosting Provider EuroHoster Ltd"**

ns2.ups-service.co.uk **195.123.224.142**

A login form for 'Vendetta World'. The form includes a logo with a Guy Fawkes mask and the text 'VENDETTA' and 'WORLD'. It has input fields for 'Username' and 'Password', with a 'Forgot a Password?' link. A captcha field shows the text '1013 d' and is labeled 'Captcha'. A blue 'Sign in' button is below the fields. At the bottom, there is a link for 'Want new account?' and a 'Sign Up' button.

### Currently active Domain

<http://vendetta.cc>

Registered through CN registrar

Previous & current domains are always fronted by Cloudflare

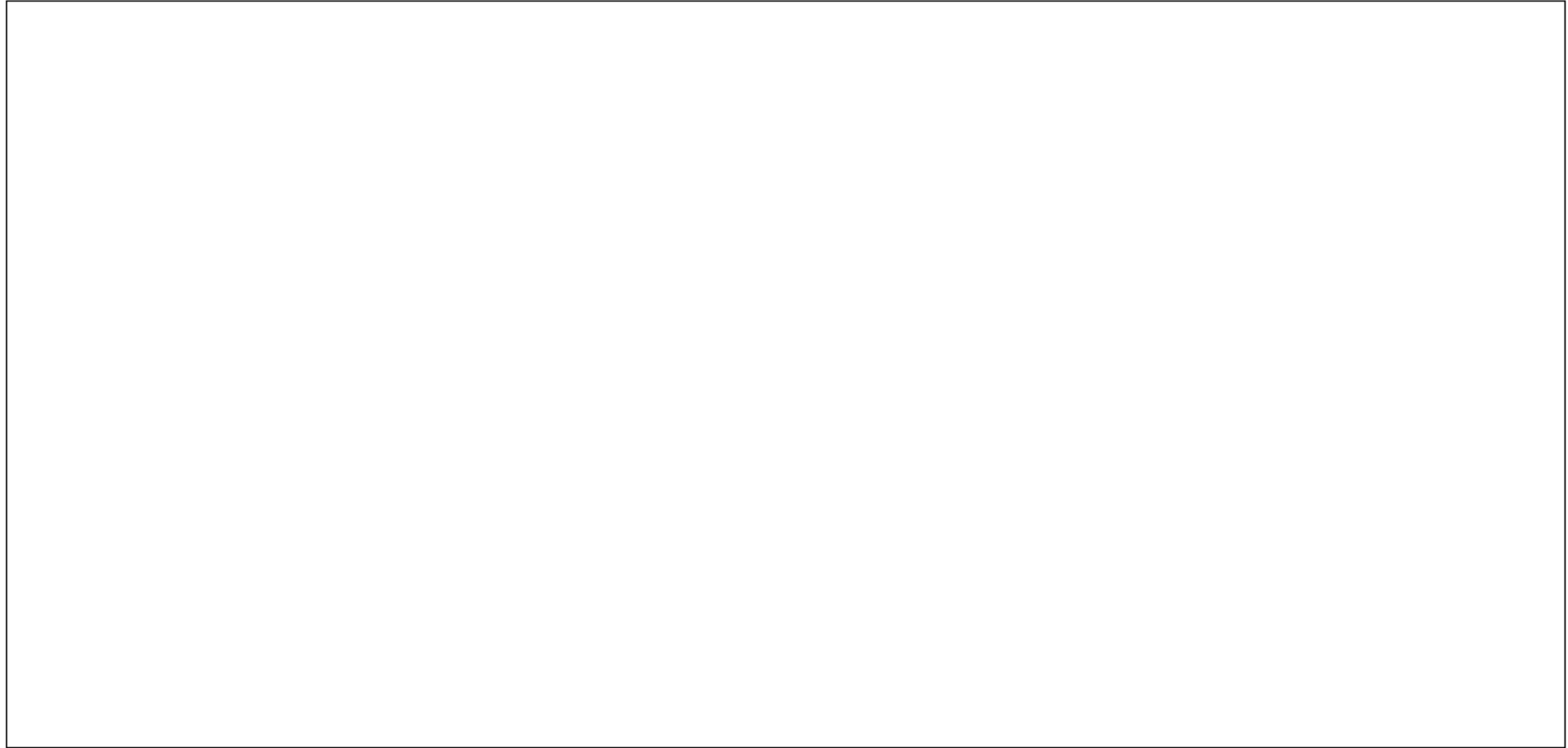
### Former Domains

<http://go7obv2tf2pm2y2i.onion/>

<http://vndt.cc>

<http://kingven.cc>

# STARTUP G LTD



## Protocol

TCP  UDP  Other  Multiple

## Status

Complete  Active  Multiple

# STARTUP G LTD

inetnum: 77.72.83.0 - 77.72.84.255  
netname: StartUPG-NET  
country: GB  
admin-c: SGNO1-RIPE  
tech-c: SGNO1-RIPE  
org: ORG-SGL37-RIPE  
mnt-routes: BACLOUD-MNT  
status: ASSIGNED PA  
mnt-by: MNT-NETUP  
mnt-by: startupgo-mnt  
created: 2017-03-29T13:20:12Z  
last-modified: 2017-04-24T09:56:54Z  
source: RIPE

role: StartUP GO Network  
Operations Centre  
address: 45 REYNOLDS WALK  
address: WOLVERHAMPTON  
address: WV11 2QD  
address: United Kingdom  
phone: +44 34189200111  
fax-no: +44 34189200111  
abuse-mailbox:  
abuse@startupgo.co.uk  
nic-hdl: SGNO1-RIPE  
mnt-by: startupgo-mnt  
created: 2017-03-22T09:35:53Z  
last-modified: 2017-03-22T09:35:53Z  
source: RIPE # Filtered

# STARTUP G LTD WHOIS

Domain name:

startupgo.co.uk

Data validation:

Nominet was not able to match the registrant's name and/or address against a 3rd party source on 16-Mar-2017

Registrar:

101domain GRS Ltd. t/a 101domain GRS Ltd. [Tag = 101DOMAIN]

URL: <https://101domain.com/uk.htm>

Relevant dates:

Registered on: 16-Mar-2017

Expiry date: 16-Mar-2019

Last updated: 20-Apr-2018

Registration status:

Registered until expiry date.

Name servers:

ns1.startupgo.co.uk 78.46.129.60 >> Hetzner Online GmbH

ns2.startupgo.co.uk 78.46.129.60



# vandalised workshop

By [Dayna Farrington](#) | [Shifnal](#) | [Crime](#) | Published: Feb 13, 2018

A family-run wooden flooring company has come to the rescue of a disability charity in Albrighton after their workshop was vandalised by burglars.



Volunteer Lol Jackson, centre, with Jake Bucknell and Carl Startup from Blueridge Flooring as they repair the workshop

## STARTUP G LTD

Company number **10106346**

[Follow this company](#)

[Overview](#)

[Filing history](#)

[People](#)

Registered office address

**5 Reynolds Walk, Wolverhampton, England, WV11 2QD**

Company status

**dissolved**

Company type

**Private limited Company**

Signature of business (SIC)

**3320 - Joinery installation**



Google

[R, Lee](#)

ence address

**5 Reynolds Walk, Wolverhampton, England, WV11 2QD**

Date of birth

**June 1987**

Appointed on

**6 April 2016**

Country of residence

**England**

Occupation

**Construction**

[R, Carl](#)

ence address

**5 Reynolds Walk, Wolverhampton, England, WV11 2QD**

**NEED**

Date of birth

**December 1982**

Appointed on

**6 April 2016**

Country of residence

**England**

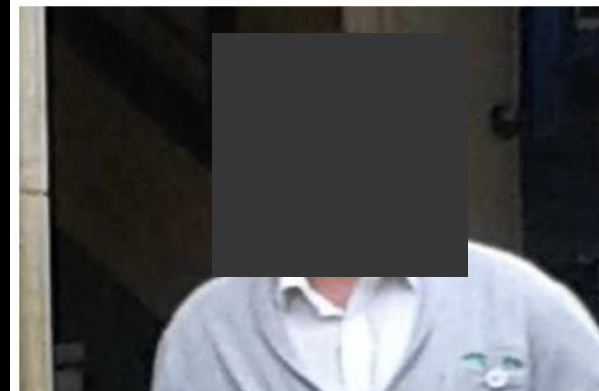
Occupation

**Construction**

## Worker in copper pipe fraud to pay off his debts

[Wolverhampton](#) | [News](#) | Published: Jun 17, 2014

A conman defrauded the company he worked for and one of its suppliers out of thousands of pounds by ordering copper piping and selling it on to scrap dealers.



Carl Startup, from Essington, bought copper piping from Grahams Builders Merchants and had it sent to Choice Heating and Plumbing (CHP), where he worked as a carpenter.

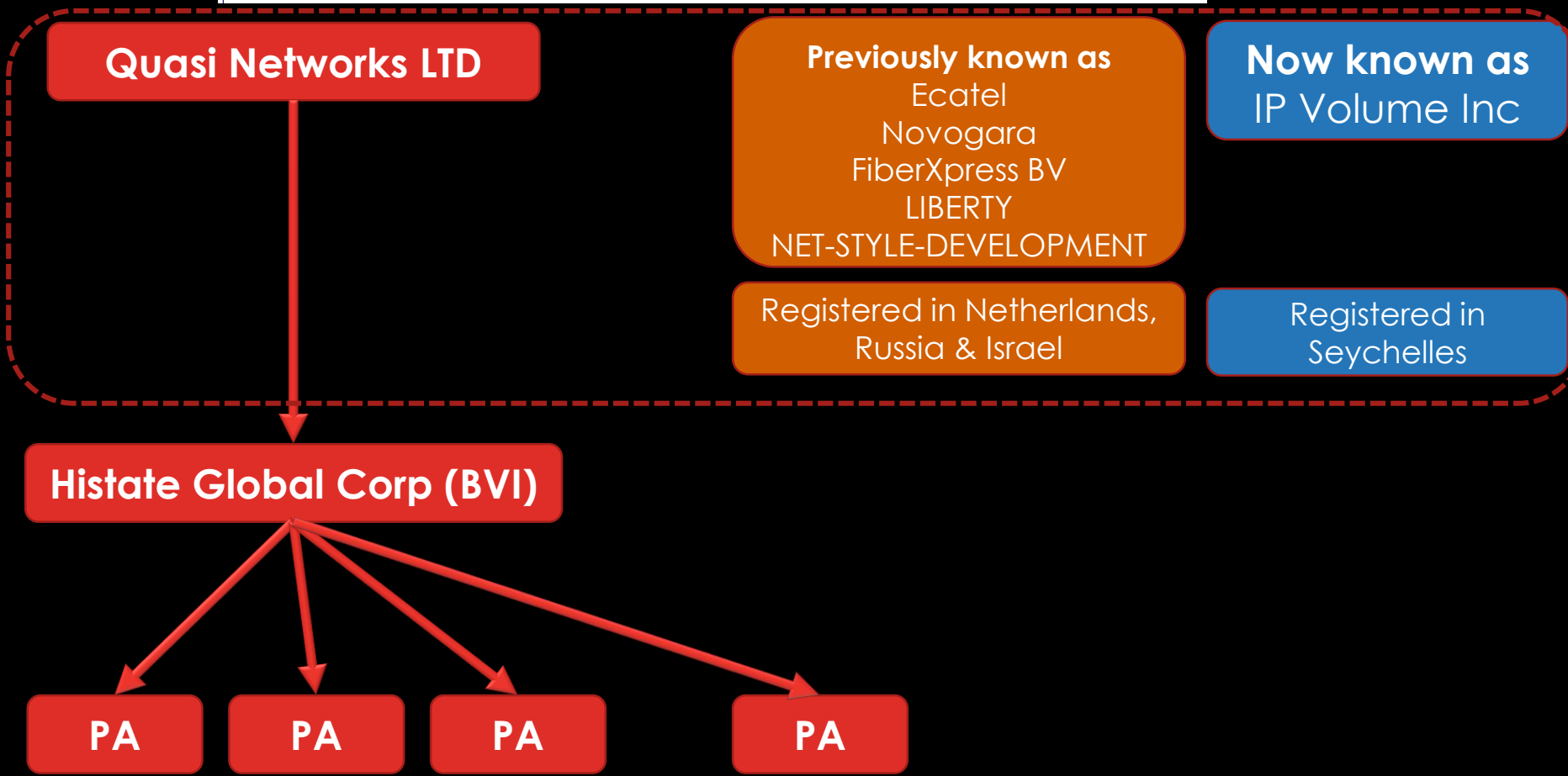
He used false order numbers to make the purchases and sold the piping to scrap metal dealers, pocketing the money for himself.

# THE FOOD CHAIN

**AS29073 Quasi Networks LTD.**

AS Info | Graph v4 | Prefixes v4 | Peers v4 | Whois | IRR

AS29073 has not been visible in the global routing table since May 14, 2019  
The information displayed is from that time.



# CLEANING THEIR TRACKS

## AS206776 Histate Global Corp.

AS Info

Graph v4

Prefixes v4

Peers v4

Whois

IRR

IX

AS206776 has not been visible in the global routing table since April 07, 2019  
The information displayed is from that time.

Company Website:

<http://histate.net/>

Country of Origin:

[Bulgaria](#)



Internet Exchanges: 3

Prefixes Originated (all): 3

Prefixes Originated (v4): 3

Prefixes Originated (v6): 0

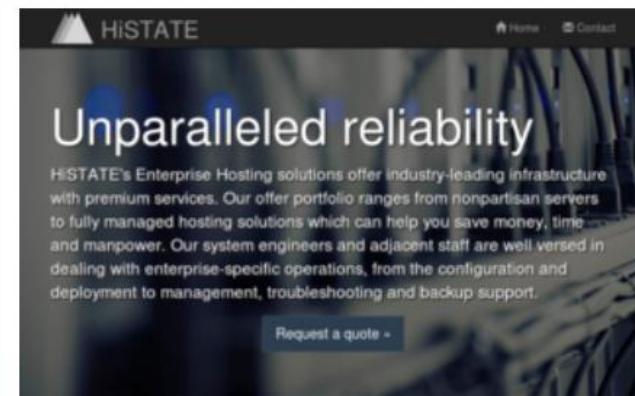
Prefixes Announced (all): 0

Prefixes Announced (v4): 0

Prefixes Announced (v6): 0

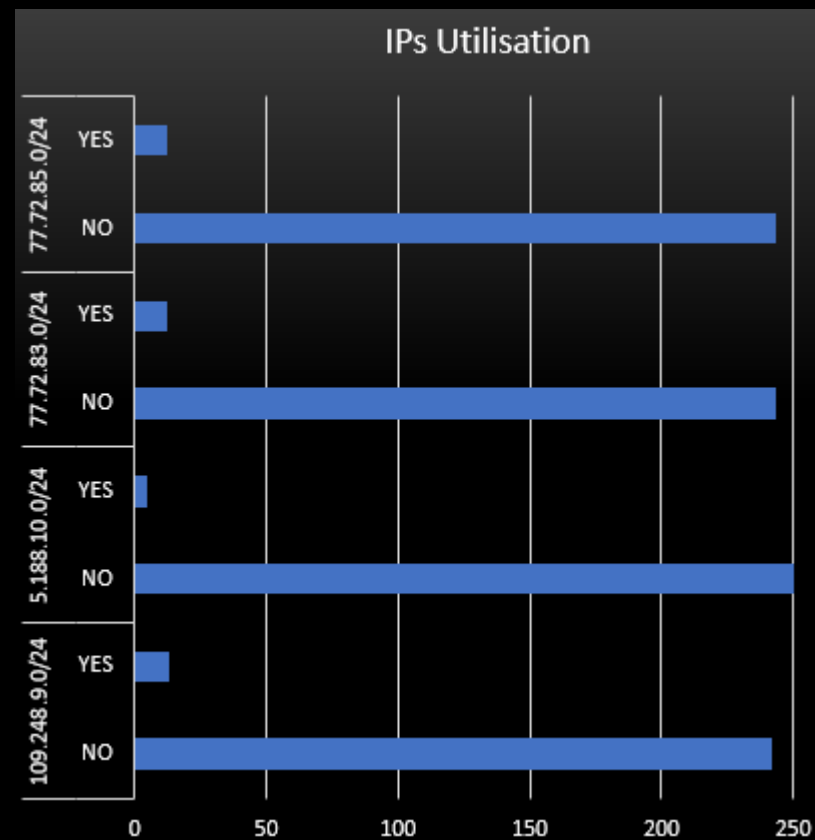
BGP Peers Observed (all): 3

BGP Peers Observed (v4): 3



# STATS

- 48 IPs identified as scanners
- 10 **Super Micro** servers
  - All on the Anonymous branded prefix
  - Hostnames resemble organised operation (Racks & Us numbers)
- 9 BitTorrent nodes
- Some specialist scanners for:
  - MySQL
  - SIP
  - SMTP
  - Telnet



Correct as of 31/01/2019

IS THIS A  
UK  
SPECIFIC  
PROBLEM



Not really



# FUTURENOW INCORPORATED

- Based in Seychelles
- Abuse contact: [abuse@fcloud.biz](mailto:abuse@fcloud.biz)
- A record for [fcloud.biz](http://fcloud.biz) points to 188.217.0.121 (Allocated PA)
  - Belongs to an Isle of Man registered business (ICME LIMITED) - ASN42237
  - Which also used to announce STARTUP G LTD prefixes



ETC.

- More countries to publicly open their registers of companies
- Tracking of differential changes in RIPE DB to monitor suspicious movements
- Improve the utilisation of RIPE DB within Open Source Intelligence (OSINT) tools



THE END

