Mass-analyzing a chunk of the Internet: The Romanian IT landscape

George-Alexandru Andrei

OWASP

The Open Web Application Security Project

About Me

- About Me
- Hello.
- I am an IT Security fanatic.
- 6 years of hands on IT Security(penetration testing, physical security, threat hunting, security audits, etc.)
- IT Security masters student

BIT SENTINEL

ccsir

Mass-analyzing: The Romanian IT landscape

- Why do it ?
- From a defensive point of view:
  - to see how many systems are vulnerable to the latest and greatest exploits (Practical)
  - Survey SSL certificates in use in Romania (Practical)
  - To see how many users are affected by vulnerable routers (I am looking at you D-Link)

Mass-analyzing: The Romanian IT landscape

- Why do it ?
- From an offensive point of view:
  - to see how many systems can be weaponized to perform DDoS attacks (Theoretical)
  - To see how easy we can compromise systems (Theoretical)
  - To find out if we can exfiltrate information (Think databases – Still theoretical)

- Why do it ? – From my point of view
- Because it’s fun & informative
- Because it’s a wide scope so there is a big chance to have something vulnerable
- Because of the legal challenges

Mass-analyzing: The Romanian IT landscape

- Getting down to business: Vulnerable systems.
- Number of assets scanned by third parties: **1,600,727**
- **Number of assets that have Windows XP (directly connected to the internet) : 721. Bucharest has 59 of these assets . Global Number of XP assets: 292,536**
- **On a national scale these XP systems are used as:**
    - **Web Servers (38 – IIS web server, 19 – Apache web server)**
    - **VNC 13 instances found**
    - **TeamViewer – 6 instances**
    - **MySQL – 6 Instances**

- MS08-67 Critical Vulnerability that can allow remote command execution could affect these systems (Not tested just an assumption)

Mass-analyzing: The Romanian IT landscape

- SSL Certificates (Port 443 only implementation)
- Total number of assets: 119026
  - SSL v2 : **59,461**
  - **SSL v1: 28**
  - **TLSv1.2: 59,537**

- **Unfortunately all the proper implementations of SSL (TLSv1.2) had backwards compatibility meaning they allow connection on weak or deprecated encryption cyphers.**

Mass-analyzing: The Romanian IT landscape

OWASP
The Open Web Application Security Project

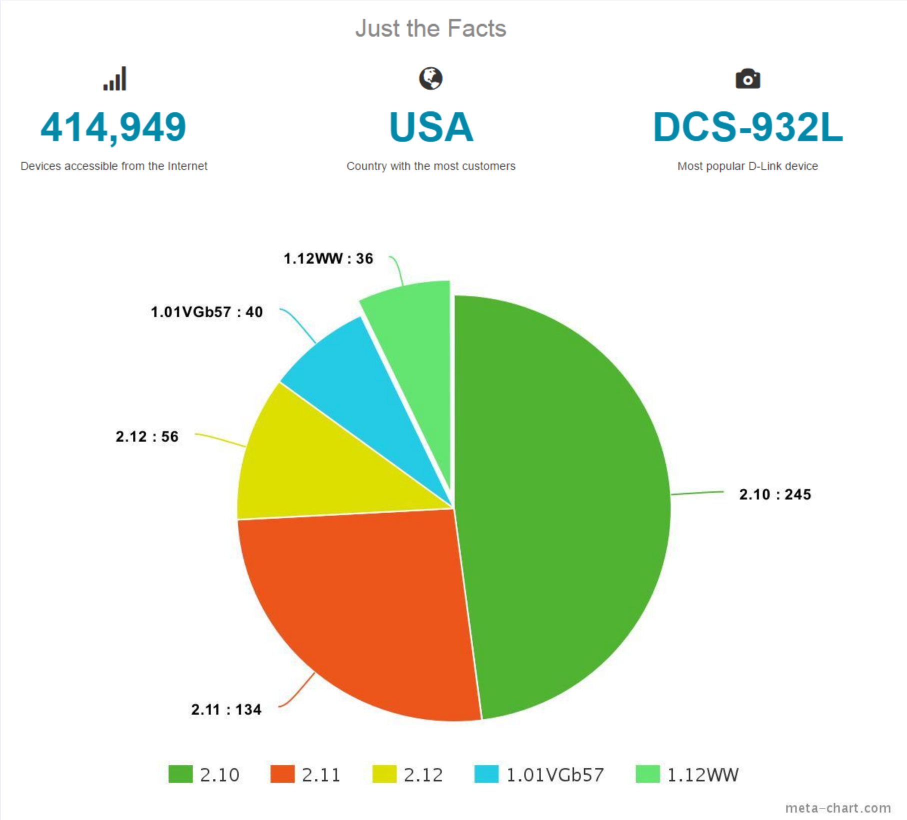
- SSL Certificates: Heartbleed
- Number of Heartbleed vulnerable assets in Romania : 819
- HTTPS - 660 Victims of Heartbleed in Romania are : National Institutions , City Halls,
- cPannel / WHM + SSL - 67 Hosting providers that have **VMware ESXi externally facing**
- WebMin - 36 **OpenVPN servers that are unpatched**
- HTTPS(port 8080) - 18 **Gateways Firewalls that have SSL enabled and are vulnerable**

Mass-analyzing: The Romanian IT landscape

OWASP
The Open Web Application Security Project

Mass-analyzing: The Romanian IT landscape

- D Link Routers
- **1,997 D Link routers in Romania**
- Vulnerable routers: 511 were identified as having vulnerable firmware installed on them



Just the Facts

414,949
Devices accessible from the Internet

USA
Country with the most customers

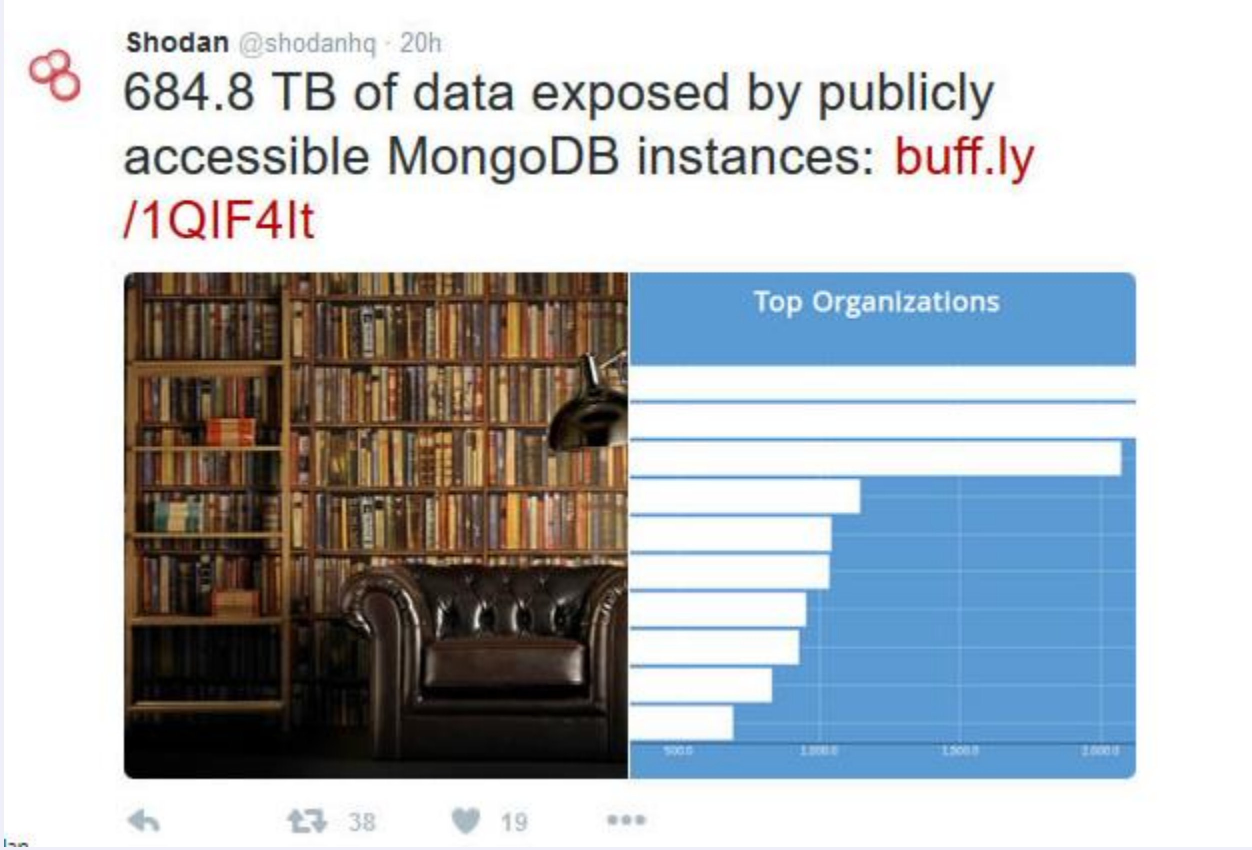
DCS-932L
Most popular D-Link device

Mass-analyzing: The Romanian IT landscape

- Getting Offensive: DDoS Attacks
- Romanian Webcams: ~3000 (most of them with default administrative credentials or even worse with no password
- Why stop there: 4,995 NTP Servers that could be used in an NTP DDoS attack
- Dream Box TV set tops : 188

And many other IoT devices that are “vulnerable by design” .

Mass-analyzing: The Romanian IT landscape



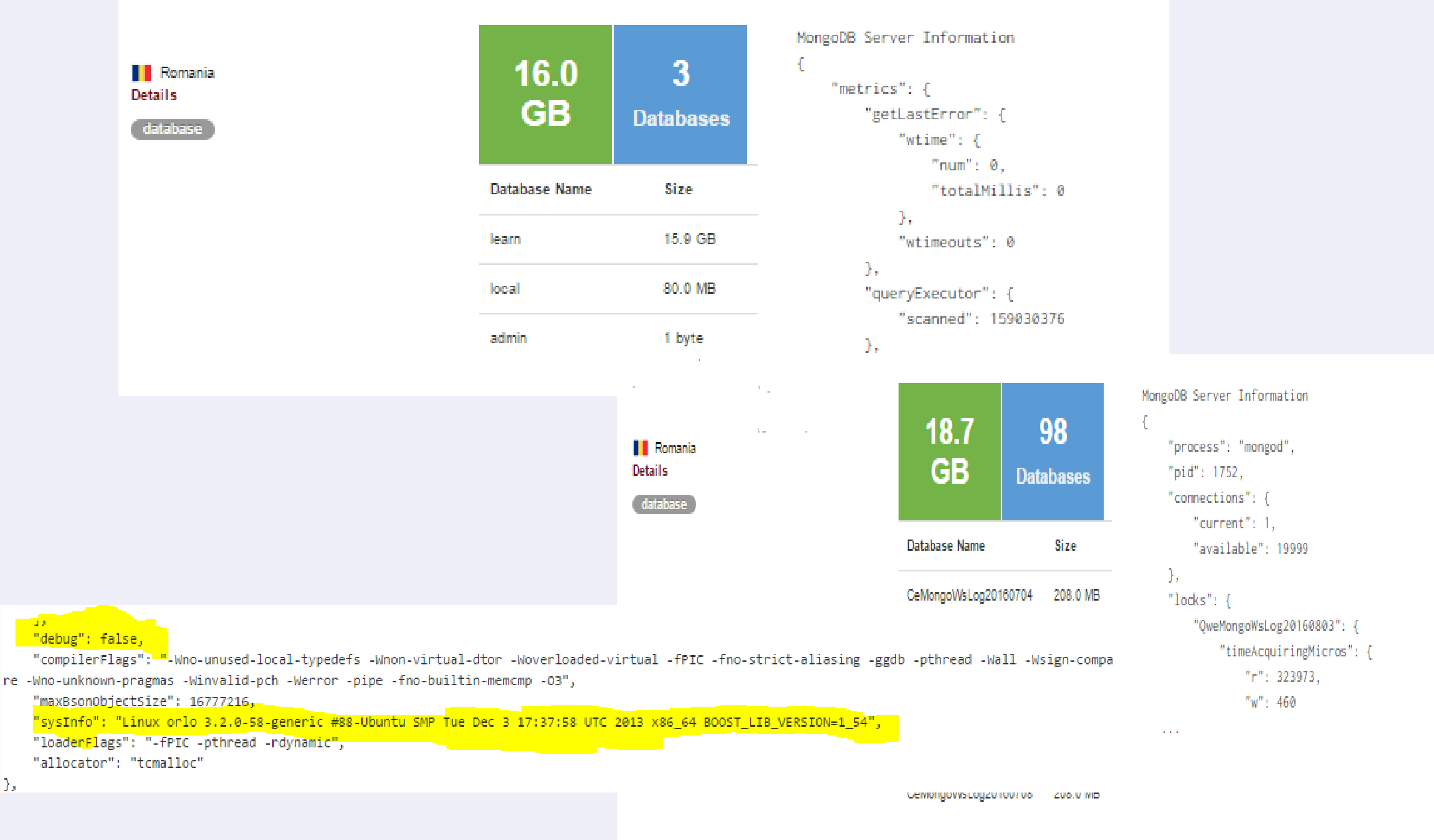
Shodan @shodanhq · 20h

684.8 TB of data exposed by publicly accessible MongoDB instances: buff.ly/1QIF4lt

38 19

Mass-analyzing: The Romanian IT landscape

OWASP
The Open Web Application Security Project



Romania
Details
database

16.0 GB | 3 Databases

Database Name	Size
learn	15.9 GB
local	80.0 MB
admin	1 byte

```
MongoDB Server Information
{
    "metrics": {
        "getLastError": {
            "wtime": {
                "num": 0,
                "totalMillis": 0
            },
            "wtimeouts": 0
        },
        "queryExecutor": {
            "scanned": 159030376
        },
```

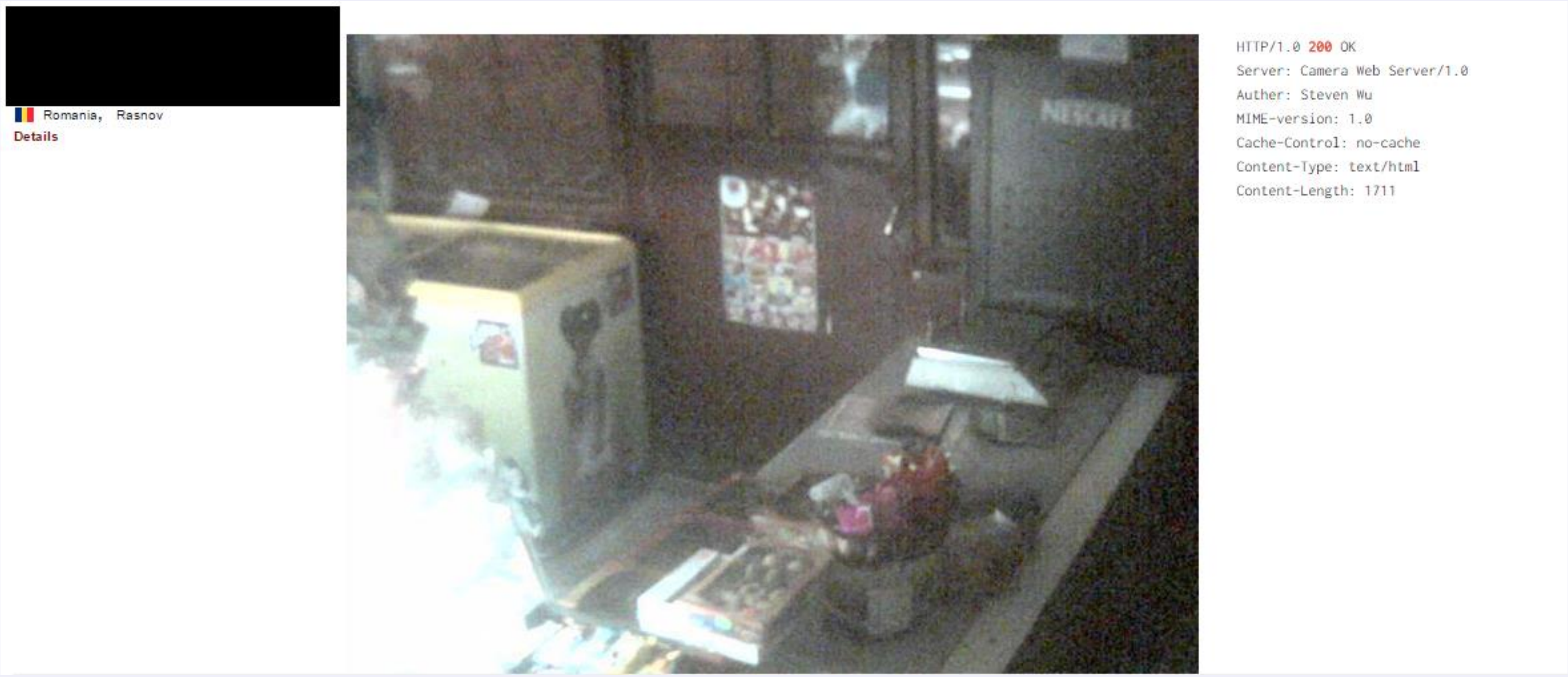
Romania
Details
database

18.7 GB | 98 Databases

Database Name	Size
CeMongoWsLog20160704	208.0 MB

```
MongoDB Server Information
{
    "process": "mongod",
    "pid": 1752,
    "connections": {
        "current": 1,
        "available": 19999
    },
    "locks": {
        "QweMongoWsLog20160803": {
            "timeAcquiringMicros": {
                "r": 323973,
                "w": 460
    ...
```

```
    },
    "debug": false,
    "compilerFlags": "-Wno-unused-local-typedefs -Wnon-virtual-dtor -Woverloaded-virtual -fPIC -fno-strict-aliasing -ggdb -pthread -Wall -Wsign-compa
re -Wno-unknown-pragmas -Winvalid-pch -Werror -pipe -fno-builtin-memcmp -O3",
    "maxBsonObjectSize": 16777216,
    "sysInfo": "Linux orlo 3.2.0-58-generic #88-Ubuntu SMP Tue Dec 3 17:37:58 UTC 2013 x86_64 BOOST_LIB_VERSION=1_54",
    "loaderFlags": "-fPIC -pthread -rdynamic",
    "allocator": "tcmalloc"
},
```

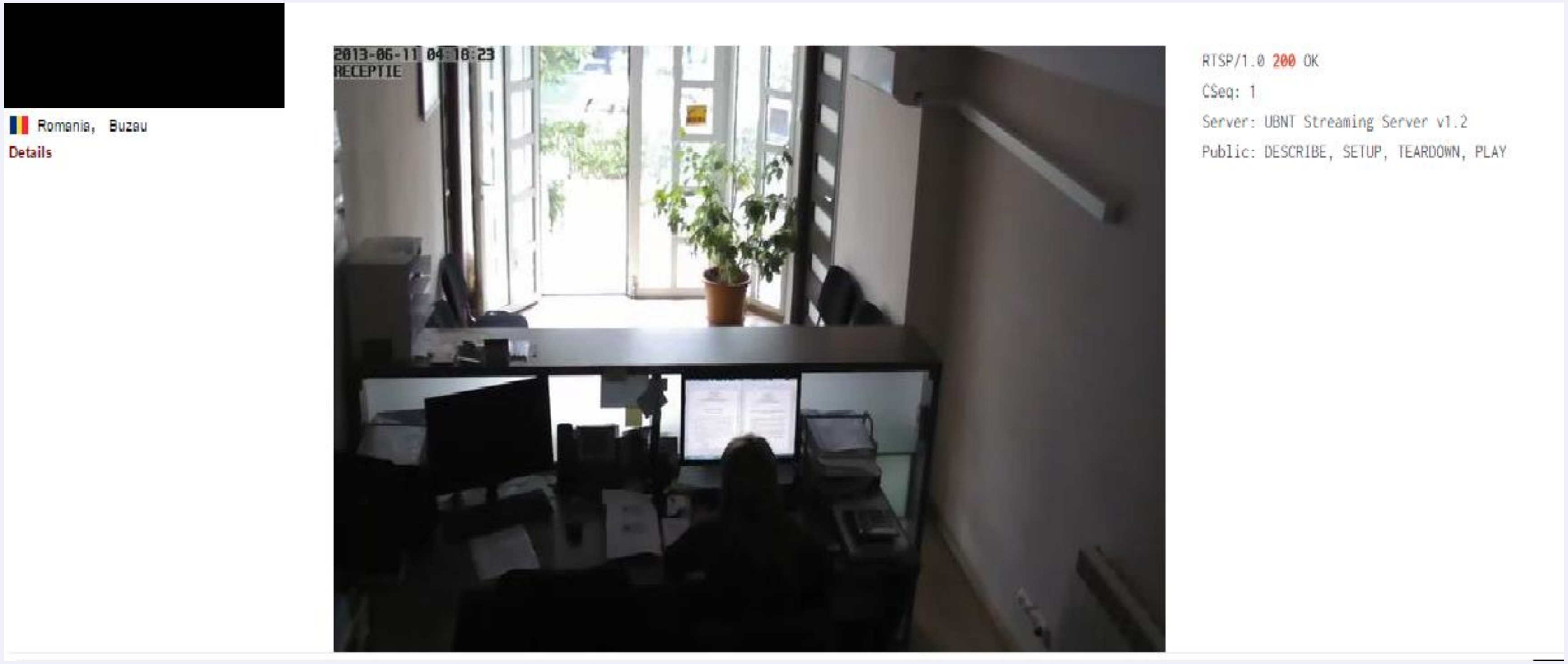


[redacted]

Romania, Rasnov

Details

```
HTTP/1.0 200 OK
Server: Camera Web Server/1.0
Auther: Steven Wu
MIME-version: 1.0
Cache-Control: no-cache
Content-Type: text/html
Content-Length: 1711
```

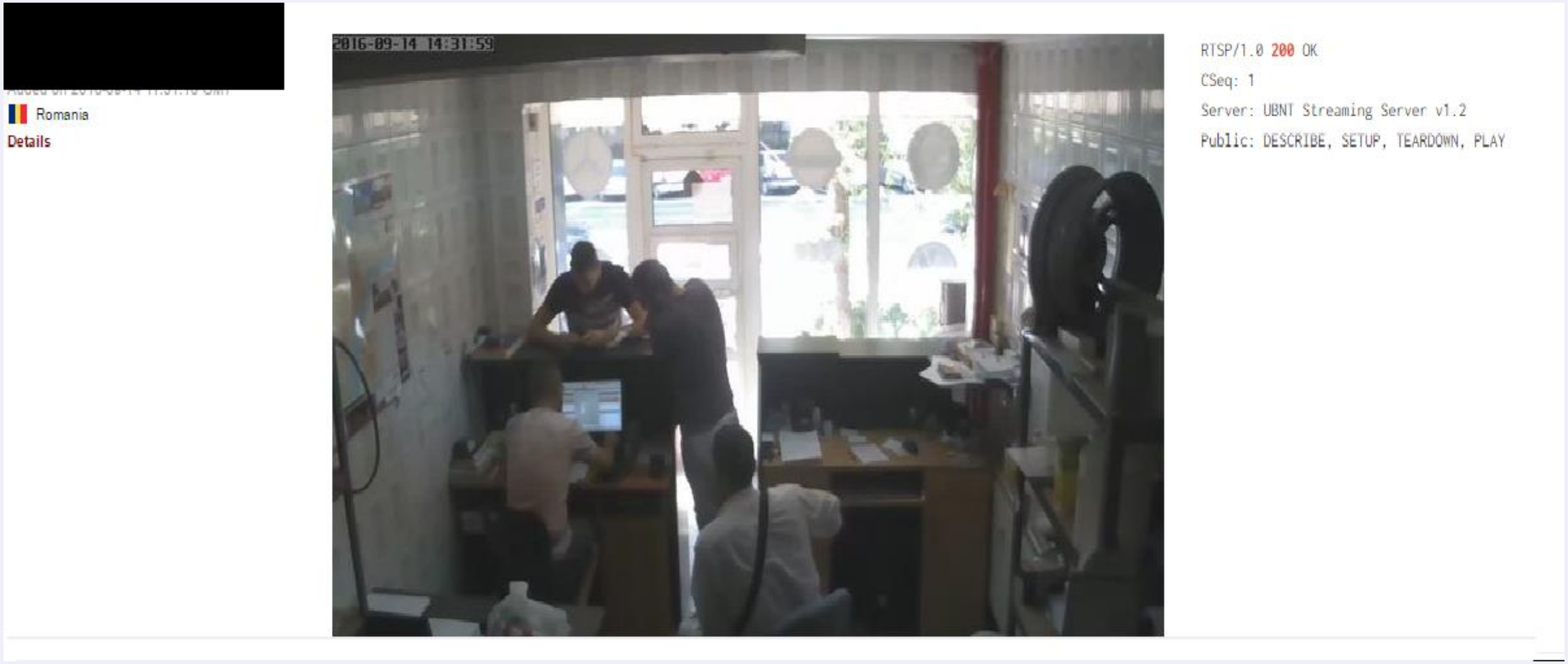


[redacted]

Romania, Buzau

Details

```
RTSP/1.0 200 OK
CSeq: 1
Server: UBNT Streaming Server v1.2
Public: DESCRIBE, SETUP, TEARDOWN, PLAY
```

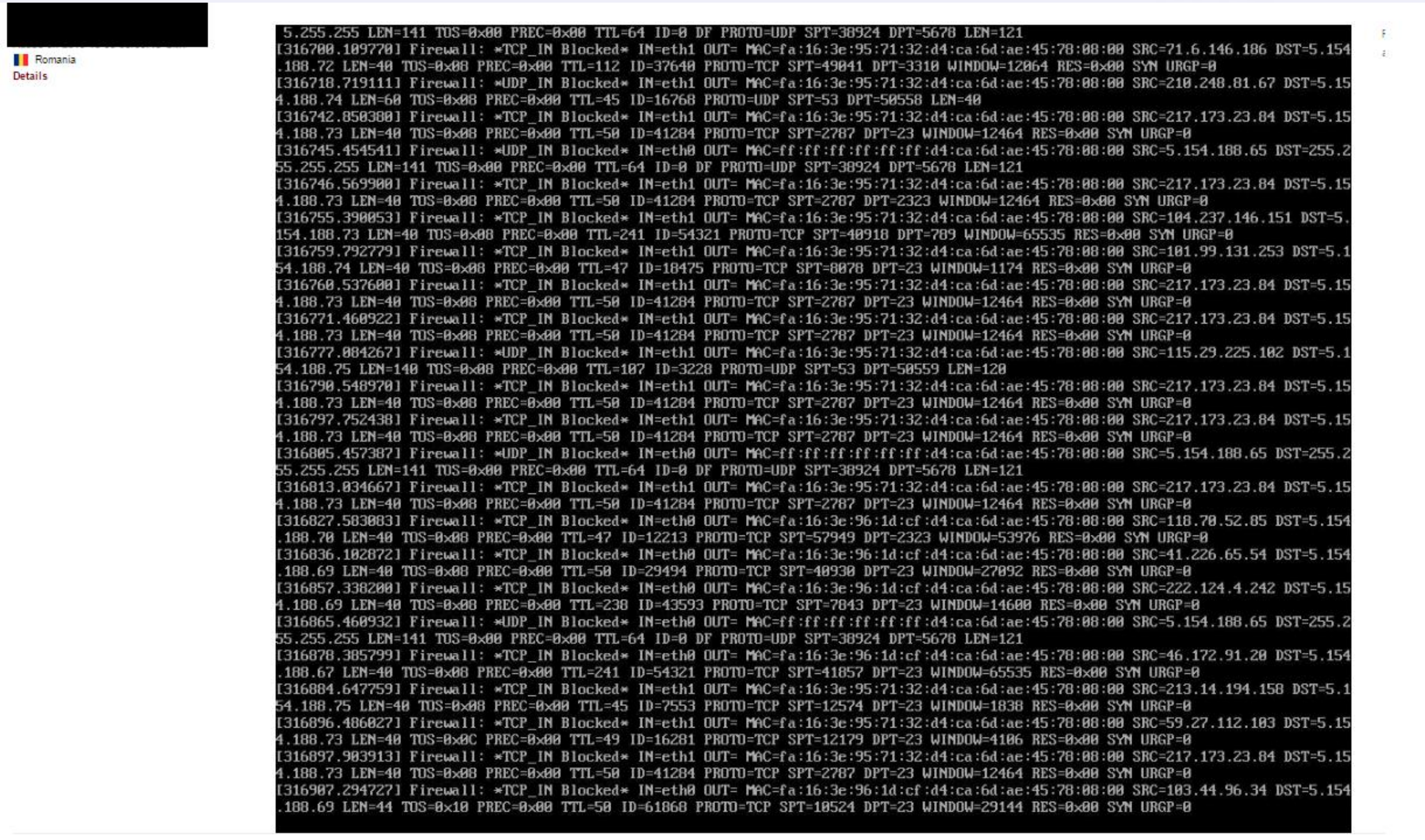


[redacted]

Romania

Details

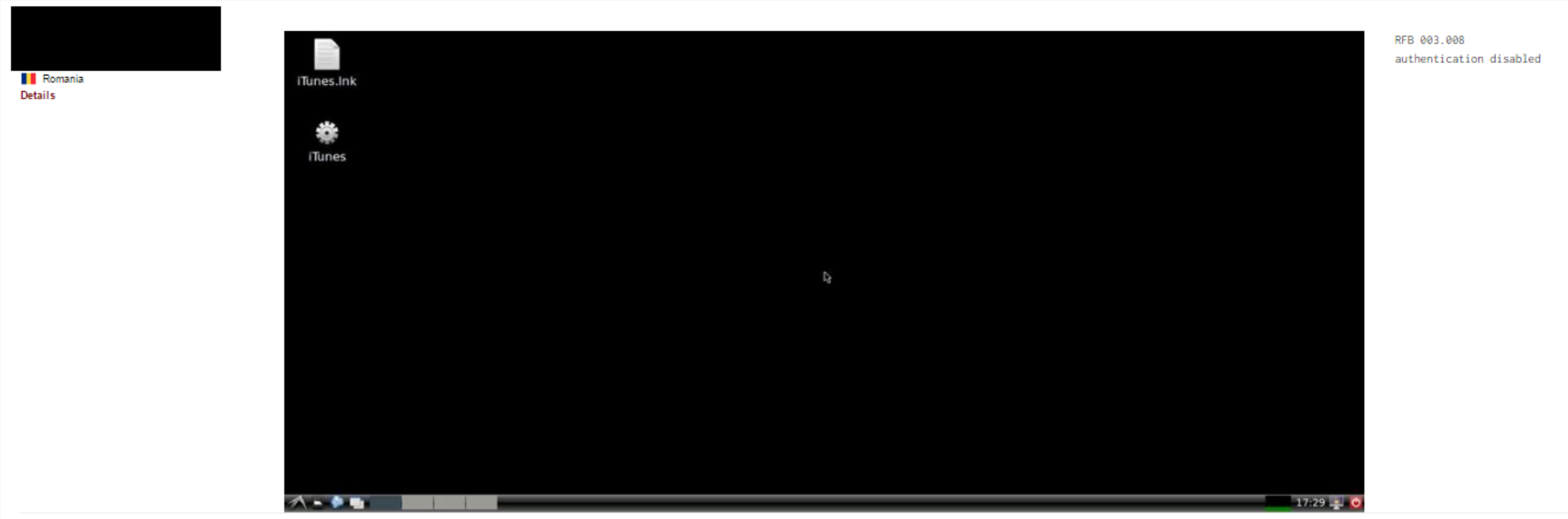
```
RTSP/1.0 200 OK
CSeq: 1
Server: UBNT Streaming Server v1.2
Public: DESCRIBE, SETUP, TEARDOWN, PLAY
```



[redacted]

Romania
Details

```
 5.255.255 LEN=141 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=38924 DPT=5678 LEN=121
[316700.109770] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=71.6.146.186 DST=5.154
.188.72 LEN=40 TOS=0x08 PREC=0x00 TTL=112 ID=37640 PROTO=TCP SPT=49041 DPT=3310 WINDOW=12064 RES=0x00 SYN URGP=0
[316718.719111] Firewall: *UDP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=210.248.81.67 DST=5.15
4.188.74 LEN=60 TOS=0x08 PREC=0x00 TTL=45 ID=16768 PROTO=UDP SPT=53 DPT=50558 LEN=40
[316742.850380] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=217.173.23.84 DST=5.15
4.188.73 LEN=40 TOS=0x08 PREC=0x00 TTL=50 ID=41284 PROTO=TCP SPT=2787 DPT=23 WINDOW=12464 RES=0x00 SYN URGP=0
[316745.454541] Firewall: *UDP_IN Blocked* IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:d4:ca:6d:ae:45:78:08:00 SRC=5.154.188.65 DST=255.2
55.255.255 LEN=141 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=38924 DPT=5678 LEN=121
[316746.569900] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=217.173.23.84 DST=5.15
4.188.73 LEN=40 TOS=0x08 PREC=0x00 TTL=50 ID=41284 PROTO=TCP SPT=2787 DPT=2323 WINDOW=12464 RES=0x00 SYN URGP=0
[316755.390053] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=104.237.146.151 DST=5.
154.188.73 LEN=40 TOS=0x08 PREC=0x00 TTL=241 ID=54321 PROTO=TCP SPT=40918 DPT=789 WINDOW=65535 RES=0x00 SYN URGP=0
[316759.792779] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=101.99.131.253 DST=5.1
54.188.74 LEN=40 TOS=0x08 PREC=0x00 TTL=47 ID=18475 PROTO=TCP SPT=8078 DPT=23 WINDOW=1174 RES=0x00 SYN URGP=0
[316760.537600] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=217.173.23.84 DST=5.15
4.188.73 LEN=40 TOS=0x08 PREC=0x00 TTL=50 ID=41284 PROTO=TCP SPT=2787 DPT=23 WINDOW=12464 RES=0x00 SYN URGP=0
[316771.460922] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=217.173.23.84 DST=5.15
4.188.73 LEN=40 TOS=0x08 PREC=0x00 TTL=50 ID=41284 PROTO=TCP SPT=2787 DPT=23 WINDOW=12464 RES=0x00 SYN URGP=0
[316777.084267] Firewall: *UDP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=115.29.225.102 DST=5.1
54.188.75 LEN=140 TOS=0x08 PREC=0x00 TTL=107 ID=3228 PROTO=UDP SPT=53 DPT=50559 LEN=120
[316790.548970] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=217.173.23.84 DST=5.15
4.188.73 LEN=40 TOS=0x08 PREC=0x00 TTL=50 ID=41284 PROTO=TCP SPT=2787 DPT=23 WINDOW=12464 RES=0x00 SYN URGP=0
[316797.752438] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=217.173.23.84 DST=5.15
4.188.73 LEN=40 TOS=0x08 PREC=0x00 TTL=50 ID=41284 PROTO=TCP SPT=2787 DPT=23 WINDOW=12464 RES=0x00 SYN URGP=0
[316805.457387] Firewall: *UDP_IN Blocked* IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:d4:ca:6d:ae:45:78:08:00 SRC=5.154.188.65 DST=255.2
55.255.255 LEN=141 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=38924 DPT=5678 LEN=121
[316813.034667] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=217.173.23.84 DST=5.15
4.188.73 LEN=40 TOS=0x08 PREC=0x00 TTL=50 ID=41284 PROTO=TCP SPT=2787 DPT=23 WINDOW=12464 RES=0x00 SYN URGP=0
[316827.583083] Firewall: *TCP_IN Blocked* IN=eth0 OUT= MAC=fa:16:3e:96:1d:cf:d4:ca:6d:ae:45:78:08:00 SRC=118.70.52.85 DST=5.154
.188.70 LEN=40 TOS=0x08 PREC=0x00 TTL=47 ID=12213 PROTO=TCP SPT=57949 DPT=2323 WINDOW=53976 RES=0x00 SYN URGP=0
[316836.102872] Firewall: *TCP_IN Blocked* IN=eth0 OUT= MAC=fa:16:3e:96:1d:cf:d4:ca:6d:ae:45:78:08:00 SRC=41.226.65.54 DST=5.154
.188.69 LEN=40 TOS=0x08 PREC=0x00 TTL=50 ID=29494 PROTO=TCP SPT=40930 DPT=23 WINDOW=27092 RES=0x00 SYN URGP=0
[316857.338200] Firewall: *TCP_IN Blocked* IN=eth0 OUT= MAC=fa:16:3e:96:1d:cf:d4:ca:6d:ae:45:78:08:00 SRC=222.124.4.242 DST=5.15
4.188.69 LEN=40 TOS=0x08 PREC=0x00 TTL=238 ID=43593 PROTO=TCP SPT=7843 DPT=23 WINDOW=14600 RES=0x00 SYN URGP=0
[316865.460932] Firewall: *UDP_IN Blocked* IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:d4:ca:6d:ae:45:78:08:00 SRC=5.154.188.65 DST=255.2
55.255.255 LEN=141 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=38924 DPT=5678 LEN=121
[316878.385799] Firewall: *TCP_IN Blocked* IN=eth0 OUT= MAC=fa:16:3e:96:1d:cf:d4:ca:6d:ae:45:78:08:00 SRC=46.172.91.20 DST=5.154
.188.67 LEN=40 TOS=0x08 PREC=0x00 TTL=241 ID=54321 PROTO=TCP SPT=41857 DPT=23 WINDOW=65535 RES=0x00 SYN URGP=0
[316884.647759] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=213.14.194.158 DST=5.1
54.188.75 LEN=40 TOS=0x08 PREC=0x00 TTL=45 ID=7553 PROTO=TCP SPT=12574 DPT=23 WINDOW=1838 RES=0x00 SYN URGP=0
[316896.486027] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=59.27.112.103 DST=5.15
4.188.73 LEN=40 TOS=0x0C PREC=0x00 TTL=49 ID=16281 PROTO=TCP SPT=12179 DPT=23 WINDOW=4106 RES=0x00 SYN URGP=0
[316897.903913] Firewall: *TCP_IN Blocked* IN=eth1 OUT= MAC=fa:16:3e:95:71:32:d4:ca:6d:ae:45:78:08:00 SRC=217.173.23.84 DST=5.15
4.188.73 LEN=40 TOS=0x08 PREC=0x00 TTL=50 ID=41284 PROTO=TCP SPT=2787 DPT=23 WINDOW=12464 RES=0x00 SYN URGP=0
[316907.294727] Firewall: *TCP_IN Blocked* IN=eth0 OUT= MAC=fa:16:3e:96:1d:cf:d4:ca:6d:ae:45:78:08:00 SRC=103.44.96.34 DST=5.154
.188.69 LEN=44 TOS=0x10 PREC=0x00 TTL=50 ID=61868 PROTO=TCP SPT=10524 DPT=23 WINDOW=29144 RES=0x00 SYN URGP=0
```



[redacted]

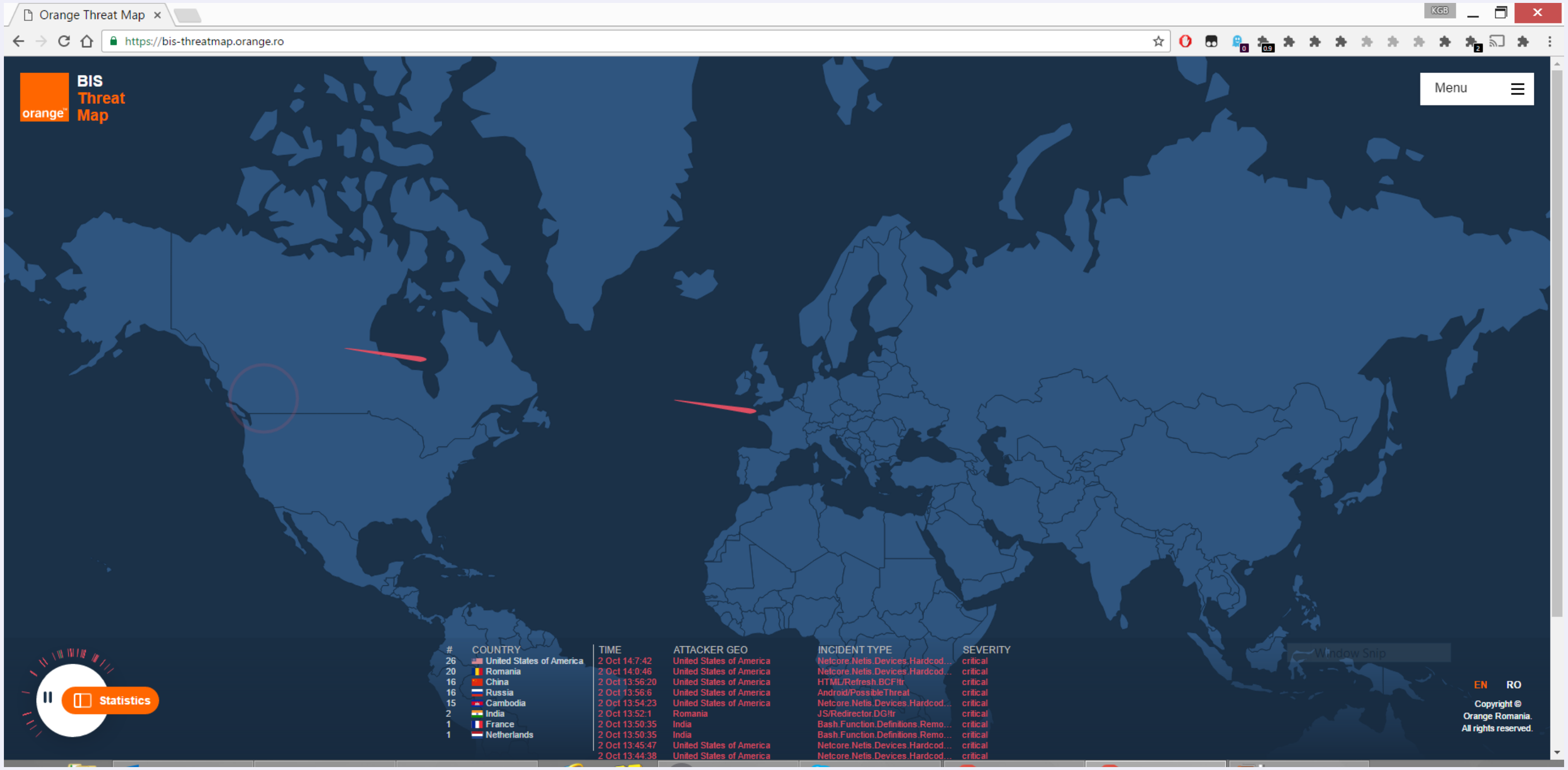
Romania

Details

RFB 003.008
authentication disabled

A different approach

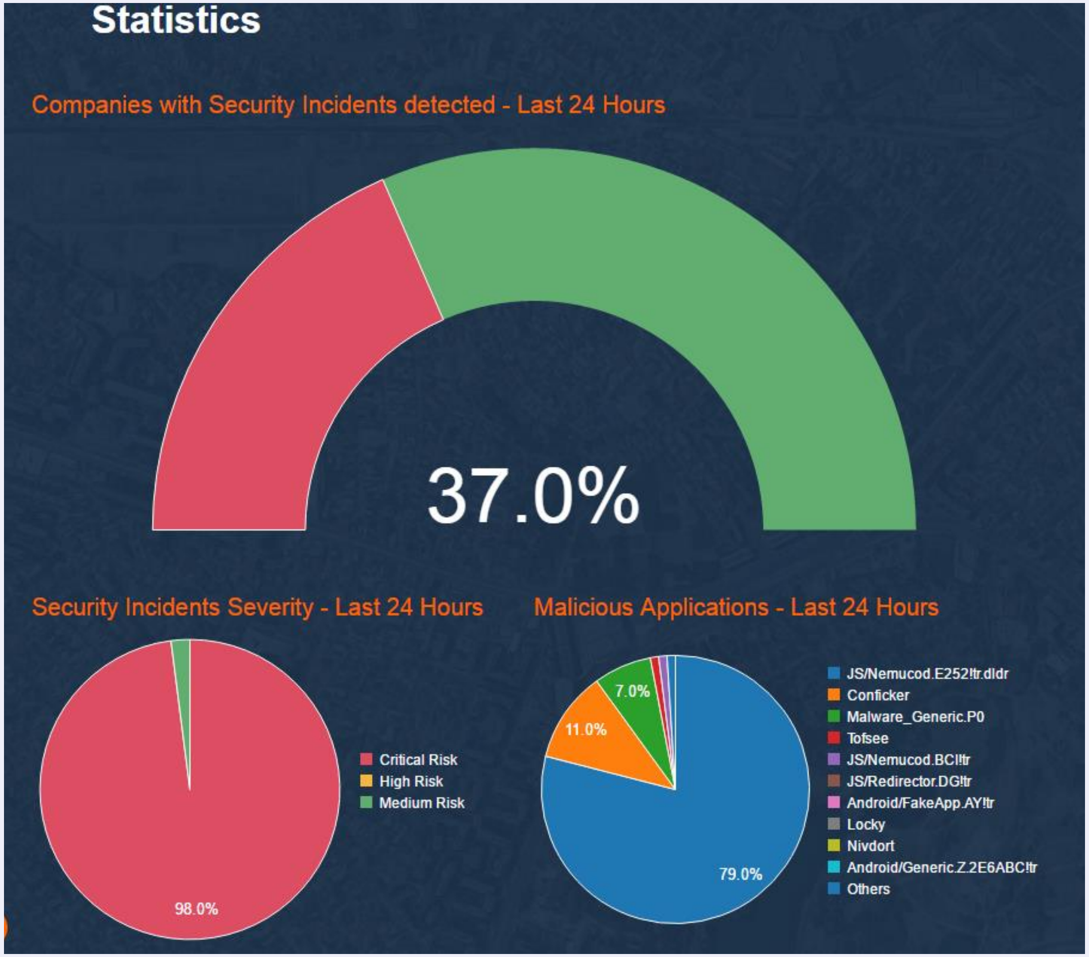
- https://bis-threatmap.orange.ro/



#	COUNTRY
26	United States of America
20	Romania
16	China
16	Russia
15	Cambodia
2	India
1	France
1	Netherlands

TIME	ATTACKER GEO	INCIDENT TYPE	SEVERITY
2 Oct 14:7:42	United States of America	Netcore.Netis.Devices.Hardcod…	critical
2 Oct 14:0:46	United States of America	Netcore.Netis.Devices.Hardcod…	critical
2 Oct 13:56:20	United States of America	HTML/Refresh.BCF!tr	critical
2 Oct 13:56:6	United States of America	Android/PossibleThreat	critical
2 Oct 13:54:23	United States of America	Netcore.Netis.Devices.Hardcod…	critical
2 Oct 13:52:1	Romania	JS/Redirector.DG!tr	critical
2 Oct 13:50:35	India	Bash.Function.Definitions.Remo…	critical
2 Oct 13:50:35	India	Bash.Function.Definitions.Remo…	critical
2 Oct 13:45:47	United States of America	Netcore.Netis.Devices.Hardcod…	critical
2 Oct 13:44:38	United States of America	Netcore.Netis.Devices.Hardcod…	critical

Copyright ©
Orange Romania.
All rights reserved.



Statistics

Companies with Security Incidents detected - Last 24 Hours

Security Incidents Severity - Last 24 Hours

Malicious Applications - Last 24 Hours

Q
&
A

Thank you