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

George-Alexandru Andrei

OWASP
The Open Web Application Security Project
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
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)
• 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 ciphers.
• SSL Certificates: Heartbleed
• Number of Heartbleed vulnerable assets in Romania : 819
• HTTPS - 660 Victims of Heartbleed in Romania are : National Institutions , City Halls,
• cPanel / 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

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

684.8 TB of data exposed by publicly accessible MongoDB instances: buff.ly/1QIF4I7
Mass-analyzing: The Romanian IT landscape

**OWASP**
The Open Web Application Security Project

![MongoDB Server Information](image)

**16.0 GB**
3 Databases

- **learn**
  - Size: 15.0 GB
- **local**
  - Size: 80.0 MB
- **admin**
  - Size: 1 byte

![MongoDB Server Information](image)

**18.7 GB**
98 Databases

- **CemMongodbLog20160704**
  - Size: 208.0 MB
- **CemMongodbLog20160704**
  - Size: 208.0 MB

```
"debug": false,
"compilerFlags": 
"maxbsonObjectSize": 16777216,
"sysInfo": "Linux 4.1.4-58-geneli-3 2.0.42-0ubuntu SMP Tue Dec 3 17:37:58 UTC 2013 x86_64 BOOST_LIB_VERSION=1_64",
"ldflags": 
  "-fpic "-pthread -Ddynamic",
"allocator": "tcmalloc"
```
A different approach

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

Companies with Security Incidents detected - Last 24 Hours

37.0%

Security Incidents Severity - Last 24 Hours

Malicious Applications - Last 24 Hours
Thank you