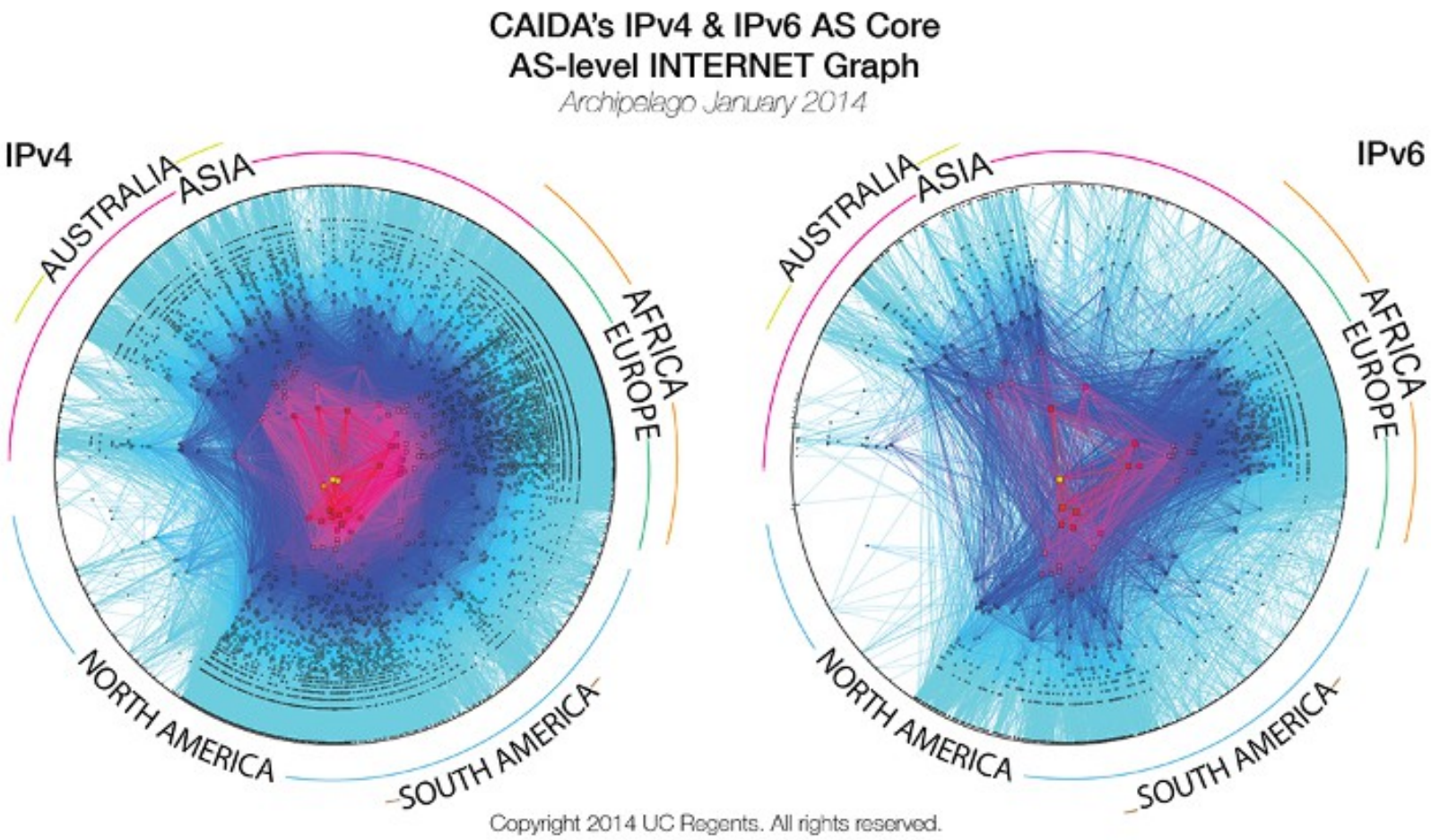
Through the Looking-Glass, and what Eve found there

Luca Bruno, Mariano Graziano,
Davide Balzarotti, Aurélien Francillon
EURECOM, France

http://www.s3.eurecom.fr/lg/

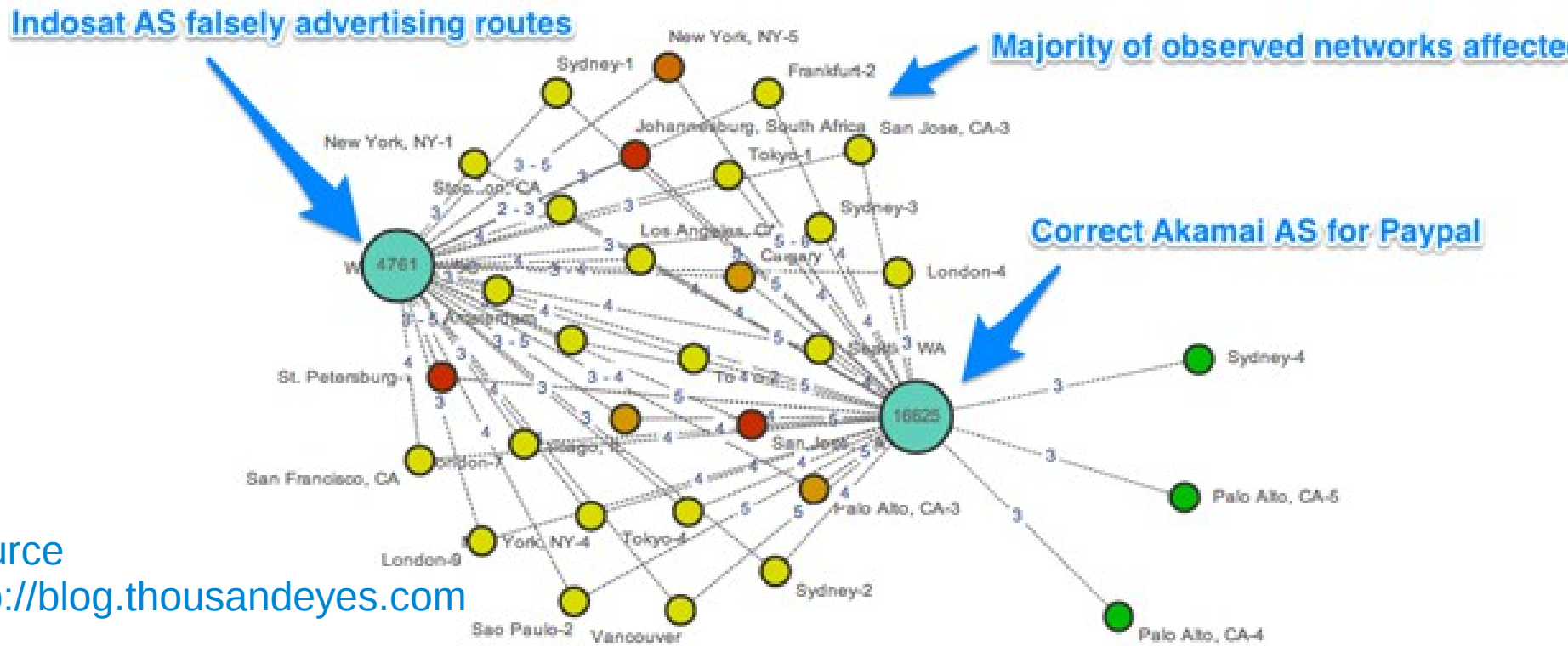
The Internet is made of AS

- A network of networks, glued by BGP



Internet is not uniform

- BGP is worldwide, each AS routing table is a (partial) local view
- What you see depends on where you are



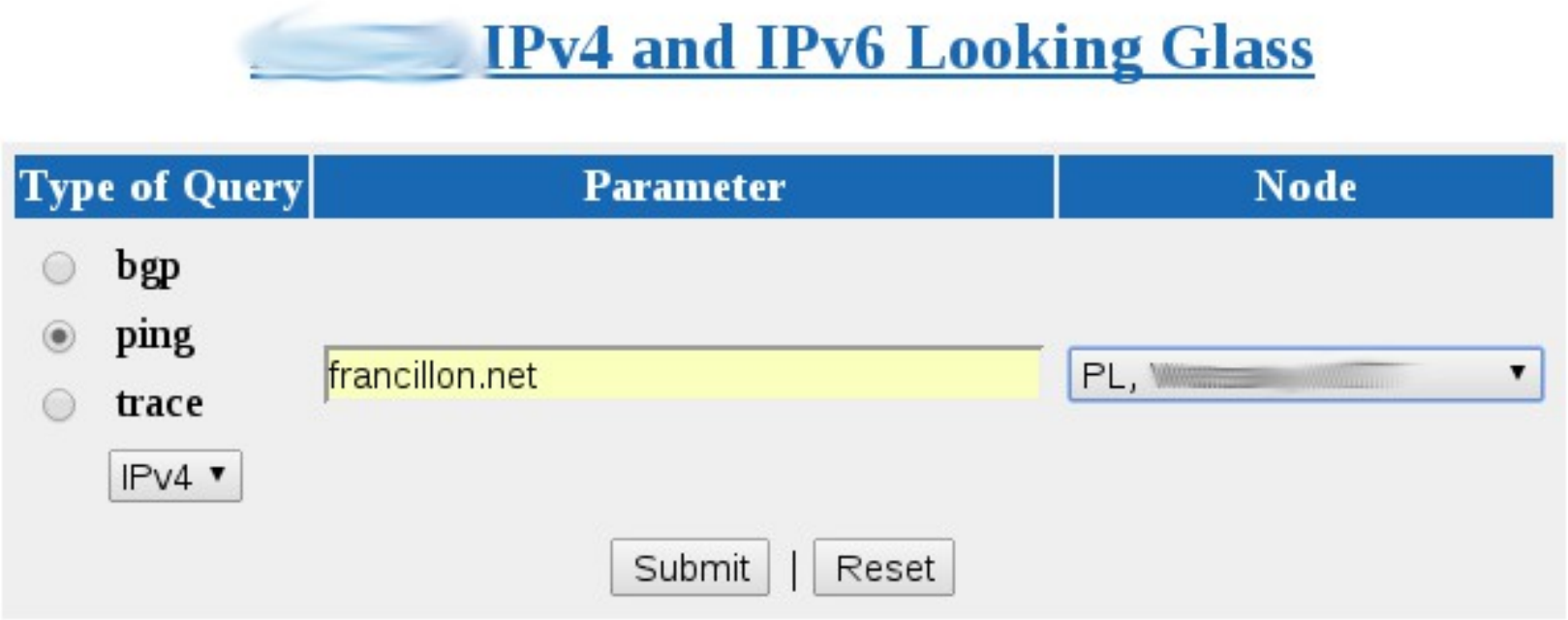
Source
http://blog.thousandeyes.com

Connectivity troubleshooting

- NOC tools for troubleshooting:
  - Distributed BGP probes, e.g., RIPE Labs
  - Private shells exchange, e.g., NLNOG
  - Limited web-access to routers:

    looking glasses

A looking glass example



A looking glass example

IPv4 and IPv6 Looking Glass

ping inet count 5 francillon.net

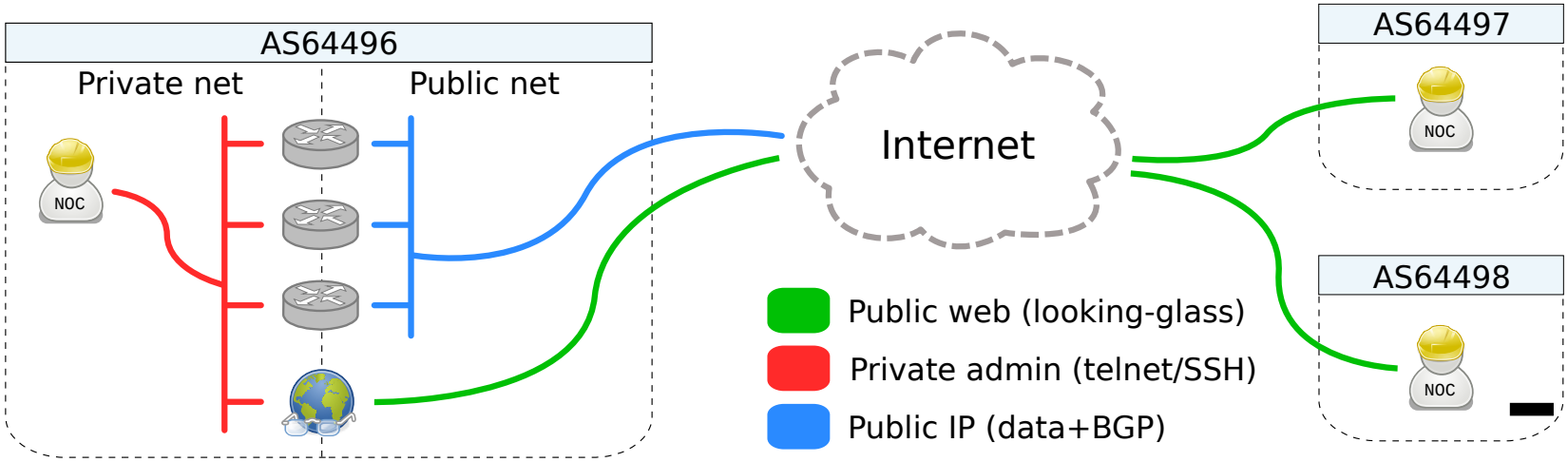
Router: [redacted]
Site: PL, [redacted]
Command: ping inet count 5 francillon.net

```
PING francillon.net (5.39.88.208): 56 data bytes
64 bytes from 5.39.88.208: icmp_seq=0 ttl=56 time=37.267 ms
64 bytes from 5.39.88.208: icmp_seq=1 ttl=56 time=35.697 ms
64 bytes from 5.39.88.208: icmp_seq=2 ttl=56 time=35.599 ms
64 bytes from 5.39.88.208: icmp_seq=3 ttl=56 time=35.652 ms
64 bytes from 5.39.88.208: icmp_seq=4 ttl=56 time=36.567 ms

--- francillon.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 35.599/36.156/37.267/0.660 ms

{master}
```

How does it work



Study

- Source code review of open source LG's
- Collected a list of LGs deployments
  - Public LG Lists
  - Searched for known patterns (Google dorks)
- Impact evaluation

Common looking glass “design”

- A simple '90s style web-script:
  - Usually PHP or Perl
  - Single file, can be dropped in webroot
  - Direct connection to SSH/telnet router console
  - Configuration (i.e., credentials)

Possible Problems

- 90' web scripts => CSS, Injections...
- Misconfigured/not hardened servers
- Not protected files credentials, configuration
- Improper network configurations

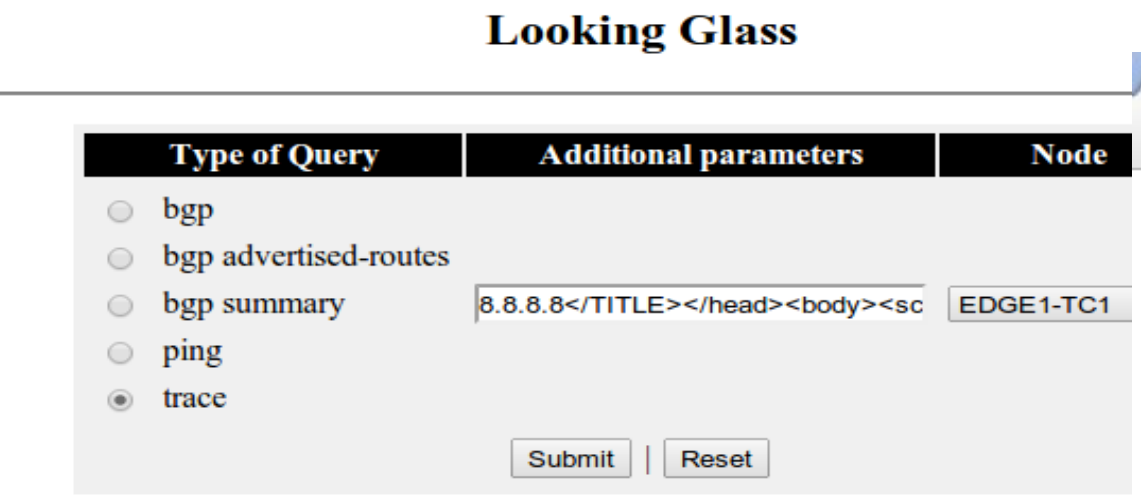
Possible Problems

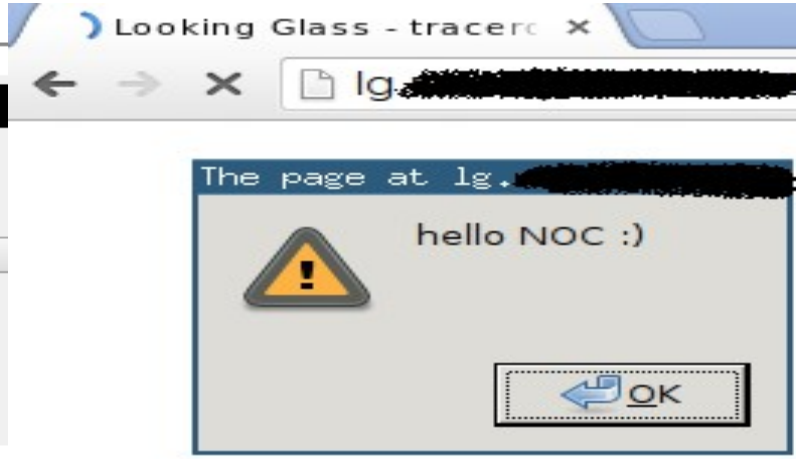
- 90' web scripts => CSS, Injections...
- Misconfigured/not hardened servers
- Not protected files credentials, configuration
- Improper network configurations

We found all of those...

XSS

- Cookie Stealing:
  - XSS vulnerabilities in LG, to target other web-apps





Default config paths

- Exposed Credentials:
  - Stored in cleartext: IPs, usernames and passwords
  - Configuration files at known URLs
- Example from Cougar LG root directory:

```
as.txt  CHANGELOG  communities.txt  COPYING  favicon.ico
lg.cgi  lg.conf  makeaslist.pl  makedb.pl  README
```

- So just crawl for it:

$BASE_LG_URL/lg.conf

Finding exposed configuration

- Google Dorks for login credentials:
  - Find LG configuration files
  - Examples:
    - *"login" "telnet" inurl:lg.conf*
    - *"login" "pass" inurl:lg.cfg*

Google Dorks – Exposing conf files

inurl:lg.conf "telnet"

Web Maps Video Immagini Shopping Altro Strumenti di ri

5 risultati (0,16 secondi)

lg.conf(5)
www.shrubbery.net/rancid/man/**lg.conf**.5.html Traduci questa pagina
and programs needed within these, such as **telnet**(1), are located. Its value is set by configure. Should it be necessary to modify PATH, note that it must include ...

lg.log ./as.db ../[redacted]logo.gif [redacted] Looking Glass favicon ...
[redacted]lg/cgi-bin/**lg.conf**
... analysis and statistics. If you don't like this policy, please disconnect now! On **telnet**:/[redacted]v3[redacted]1@[redacted]20.1 **telnet**:[redacted]v3[redacted]1@[redacted]19.254.

Google Dorks – Exposing conf files

[redacted]lg/cgi-bin/lg.conf

```
<?xml version="1.0" encoding="ISO-8859-1" ?>

<!-- $Id: lg.conf,v 1.9 2004/01/25 20:19:45 cougar Exp $ -->

<LG_Conf_File>

    <LGURL></LGURL>
    <LogFile>lg.log</LogFile>
    <ASList>./as.db</ASList>
    <LogoImage Align="center" Link="http://www.[redacted]">../[redacted]
    <HTMLTitle>[redacted] Looking Glass</HTMLTitle>
    <Favicon>favicon.ico</Favicon>
    <ContactMail>backbone@[redacted]</ContactMail>
    <RSHCmd>/usr/bin/rsh -l lg</RSHCmd>
    <HTTPMethod>POST</HTTPMethod>  <!-- use "GET" if you like to
    <TimeOut>25</TimeOut>
    <Disclaimer>All commands will be logged for possible later analys
    <SecureMode>On</SecureMode>

    <Router_List>


<!-- [redacted] (AS[redacted]) Looking Glass -->


        <Router Name="[redacted]">
            <URL>telnet://[redacted]:v3[redacted]1@[redacted]20.1</URL>
        </Router>
        <Router Name="[redacted]">
            <URL>telnet://[redacted]:v3[redacted]1@[redacted]19.254</URL>
        </Router>

    </Router_List>
</LG_Conf_File>
```

Index of /lg/cgi-bin ×

[redacted]/lg/cgi-bin/

Index of /lg/cgi-bin

- Parent Directory
- favicon.ico
- lg.cgi
- lg.conf
- lg.log

Best Practices :)

README sometime mentions them:

```
Then copy the lg.pl, lg.cfg and lg.html.inc files to a subdirectory on
your webserver.  Make sure that those files are readable by your webserver,
and that lg.pl is also executable. Make sure there is NO WORLD READ ACCESS
on the lg.cfg file since it contains YOUR CISCO PASSWORD (hope you get it)..

Because your Cisco password is in the configuration file, it is preferable
to run this script on a web server where noone else has access to - not
the virtualhosting server for all your customers...
```

...still, we've found 28 cases!

Exposed Private SSH Keys

www[redacted]/lg/.ss

www.[redacted]lg/.ssh/id_dsa

```
-----BEGIN DSA PRIVATE KEY-----
[redacted]BuwIBAAKBgQDC72plimrjWYXs8hJqyjyu3Vy0ZqfMuQlB10A+[redacted]
leZreIXI1PoIji0+imvt9+gM2nzZcmdg1jK+Fq+WRNWCErTmi0aaVG91DwlVANpR
inNVUF2ZG3ah9U[redacted]
cIVcF7RJ8cJc3j8OUC6wlleoO6hkBqbJveRwkj4Vya8qKo3wLYDv[redacted]
kiTsM2kCgYBermXmdvZDPT6vSO2fUJVlxIKv+UJk9wWddgnbRVRFul2H6CLWHP3x
[redacted]Jp9OG/Xm[redacted]t8W4RqjplgFrO3LgtoK6
j1RCnRRCE5YpUSClq6JyBS+pySDoEmMCJztDX28g2QYxkh1[redacted]n
[redacted]
-----END DSA PRIVATE KEY-----
```

[redacted]lg/.ssh/

Index of /lg/.ssh

Name	Last modified	Size	Description
Parent Directory		-	
id_dsa	03-Jul-2008 11:11	668	
id_dsa.pub	03-Jul-2008 11:11	615	
ssh_config	03-Jul-2008 11:11	1.2K	

Apache/2.2.14 (Ubuntu) Server at [redacted] *Port 80*

Remote Memory Corruption

- Sometime LG ships with embedded third-party binaries
- "fastping" SUID bin in MRLG
  - ICMP echo reply is used without proper validation
  - CVE-2014-3931

Router Command Injection

- HTTP to router CLI, just a newline away:)

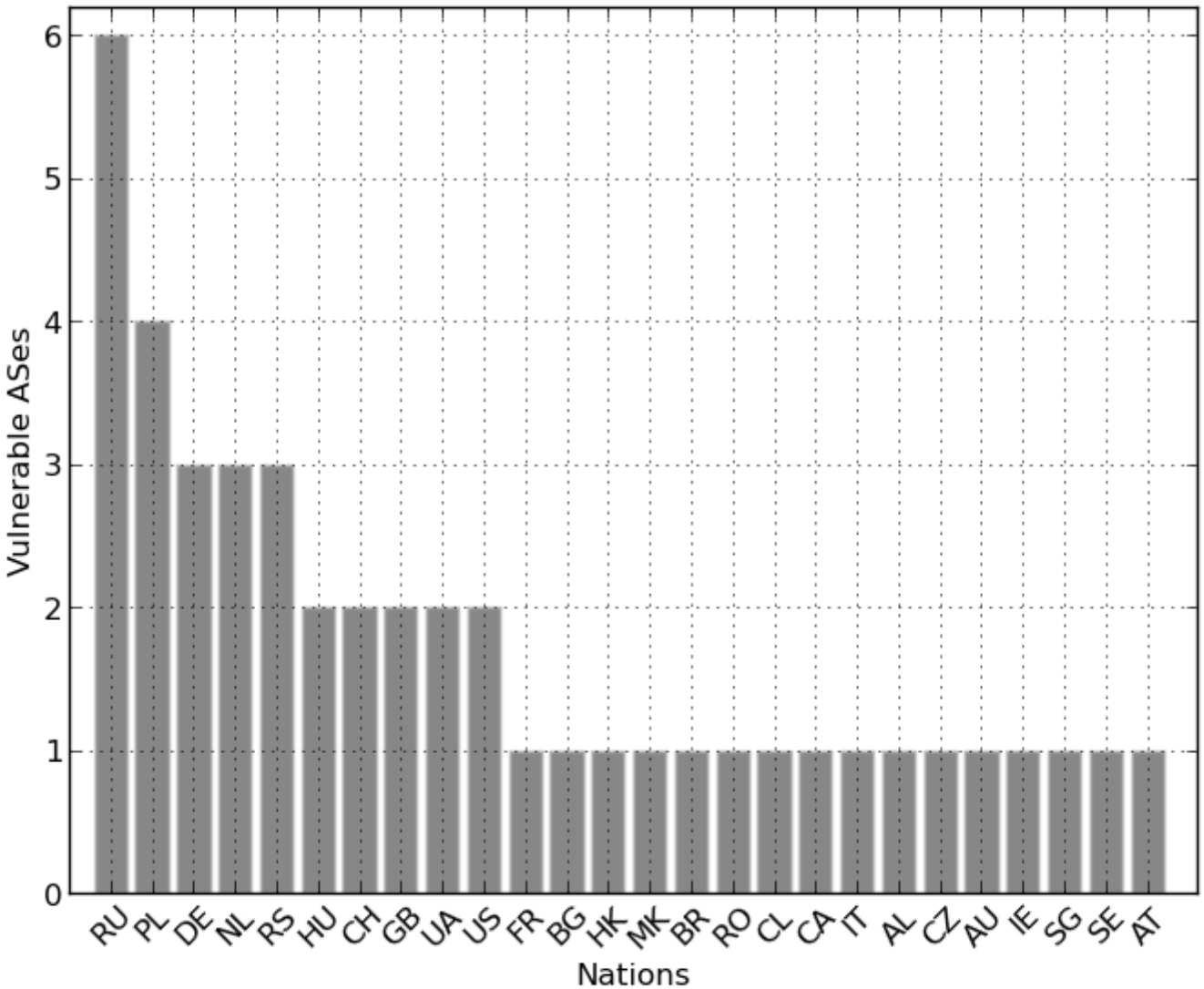
```
curl --data \
'routerid=10
&requestid=50
&argument=8.8.8.8%0Adate%0Aexit%OA'
```

Summary of reported incidents

- 6 CVEs (MRLG4PHP, Cougar LG, Cistron LG, MRLG)
- Including: Remote command injection, XSS, remote memory corruption, unsafe default configuration...

Vulnerabilities	*Affected ASes*
Exposed configuration files	28
Remote command injection	12
Misconfigured CGI	4
Exposed SSH private keys	2

Impacted AS per country



Is abuse possible ?

- In many case we can obtain a shell on a BGP Router
- Can we “break the Internet” using this?
  - Easiest way to tell is to try
  - … but obviously we did not.
- Contacts with operators, certs, .gov
- Analyzed BGP historical data to search for evidence of abuse of a vulnerable LG

  But still no clear evidence + filtering

Conclusion

- Looking Glasses are a part of the historic web that still in use in critical systems
- We uncovered many issues in Looking Glasses implementations or deployments
  - Coordinated disclosure, most hopefully fixed
- Countermeasures ?
- How many similar critical systems left with 90's grade web security?

Questions ?

http://s3.eurecom.fr/lg/

Thanks to all the members of NOPS team, who helped in bug-finding