Attack methodology and phases

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Hacking phases

1. Reconnaissance
    1. Passive (public info)
    2. Active (engaging the target – calls, emails,…)
2. Scanning
3. (enumeration)
4. Gaining Access
5. Maintaining access/escalating privileges
6. Clearing traces

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Reconnaissance

ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

Hacking phases

1. **Reconnaissance**
   a. **Passive (public info)**
   b. **Active (engaging the target – calls, emails,…)**
2. Scanning
3. (enumeration)
4. Gaining Access
5. Maintaining access/escalating privileges
6. Clearing traces

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Reconnaisance

- First step in all attacks and penetration tests
- Goal: Getting all the available information about the target
- Two key phases:
  - Footprinting (gathering general and technical information about the target)
  - Scanning (gathering in depth information about the ICT resources of the target)

FOOTPRINTING

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Footprinting

- Passive and active information gathering
- Information gathered:
  - IP addresses
  - Namespaces
  - Devices, operating systems and applications in use
  - Employee information
  - Phone numbers
  - Physical security measures
  - …

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Footprinting methodology

- Collect publicly available information about the target (company, employees, addresses, workforce capabilities, knowledge and experience, organizational model,…)
- Collect technical data about the ICT resources (IP addresses, domains, servers, ICT services, service model – in house or outsourced,…)
- Collect technical data about the network connectivity, security policy, devices in use
- Locate potential vulnerabilities

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Information about the organization

- Website, contacts, location, local addresses and phones
- Job posts – ICT skills asked (can indicate devices and software in use)
- Employees – names, positions
- News and press releases
- Social media (facebook, twitter, linkedin,…)

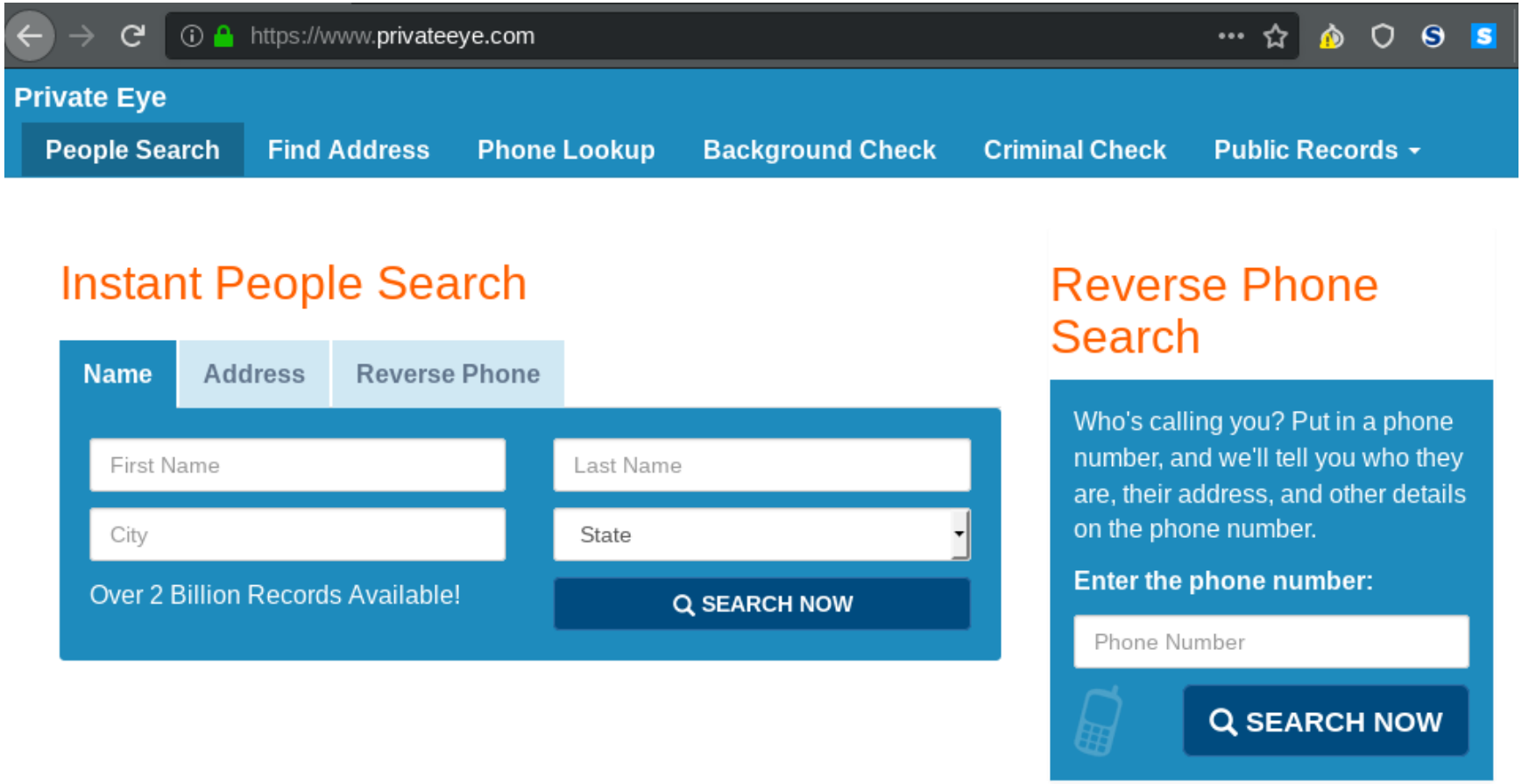
Social Networking and Information Gathering

- Look for people on social networks like facebook, twitter, instagram, linkedin
- Echosec / TBD
- Maltego
- “Hacking humans”
  - Eavesdropping
  - Phishing
  - Shoulder surfing
  - Dumpster diving
- Job sites
- Company business analysis

ISSES

Co-funded by the Erasmus+ Programme of the European Union

People search



ISSES
Co-funded by the Erasmus+ Programme of the European Union

People search

Intelius

From Wikipedia, the free encyclopedia

This article needs to be **updated**. Please update this article to reflect recent events or newly available information. *(September 2013)*

Intelius, Inc. is a public records business headquartered in Seattle, Washington, United States.[1] It provides information services, including people and property search, background checks and reverse phone lookup. Users also have the ability to perform reverse address lookups to find people using Intelius' services and an address.[2] Intelius, founded by former InfoSpace executives, was started in 2003. Intelius was ranked as the best background check service by TopTen Reviews in 2017. [3]

Contents [hide]

1 History
2 Information services
3 Philanthropy
4 Class action lawsuits
5 Consumer complaints
6 References

Intelius

Type	Privately held company
Industry	Information commerce
Genre	Electronic commerce
Founded	January 2003
Founder	Naveen Jain and others
Headquarters	Seattle, Washington, United States
Area served	United States
Key people	Abani Heller, CEO & President
Services	People Search, Background checks
Number of employees	Approximately 150
Parent	PeopleConnect, Inc.
Website	http://www.intelius.com

ISSES

Co-funded by the Erasmus+ Programme of the European Union

People search

PeopleFinders.com

From Wikipedia, the free encyclopedia

Coordinates: 38°34′11.2″N 121°29′5.6″W

For the project set up in response to Hurricane Katrina, see Katrina PeopleFinder Project.

PeopleFinders.com is a public records business located in Sacramento, California. The company offers a variety of public records including address histories, phone numbers and background checks.

Contents [hide]

1 History
2 Products and services
3 Blog
4 Growth
5 References

History [edit]

Rob Miller worked as a private investigator for Intel Corporation, but he left in 1986 to start Confi-Chek. This was a privately held corporation that provided public records and investigative information to attorneys, private investigators and other licensed professionals. According to the website bizjournals.com,[2] Confi-Chek only supplies public records to other businesses.

PeopleFinders, Inc.

peoplefinders™ find anyone, anywhere

Type	Privately held company
Industry	online data broker
Genre	electronic commerce
Founded	May 22, 2002; 17 years ago[1]
Founder	Robert Miller
Headquarters	Sacramento, California, U.S.
Area served	United States
Key people	Robert Miller, CEO Bryce Lane, President and COO Eddie Lau, VP of Information Technology
Services	background checks, identity theft protection
Website	http://www.peoplefinders.com

ISSES

Co-funded by the Erasmus+ Programme of the European Union

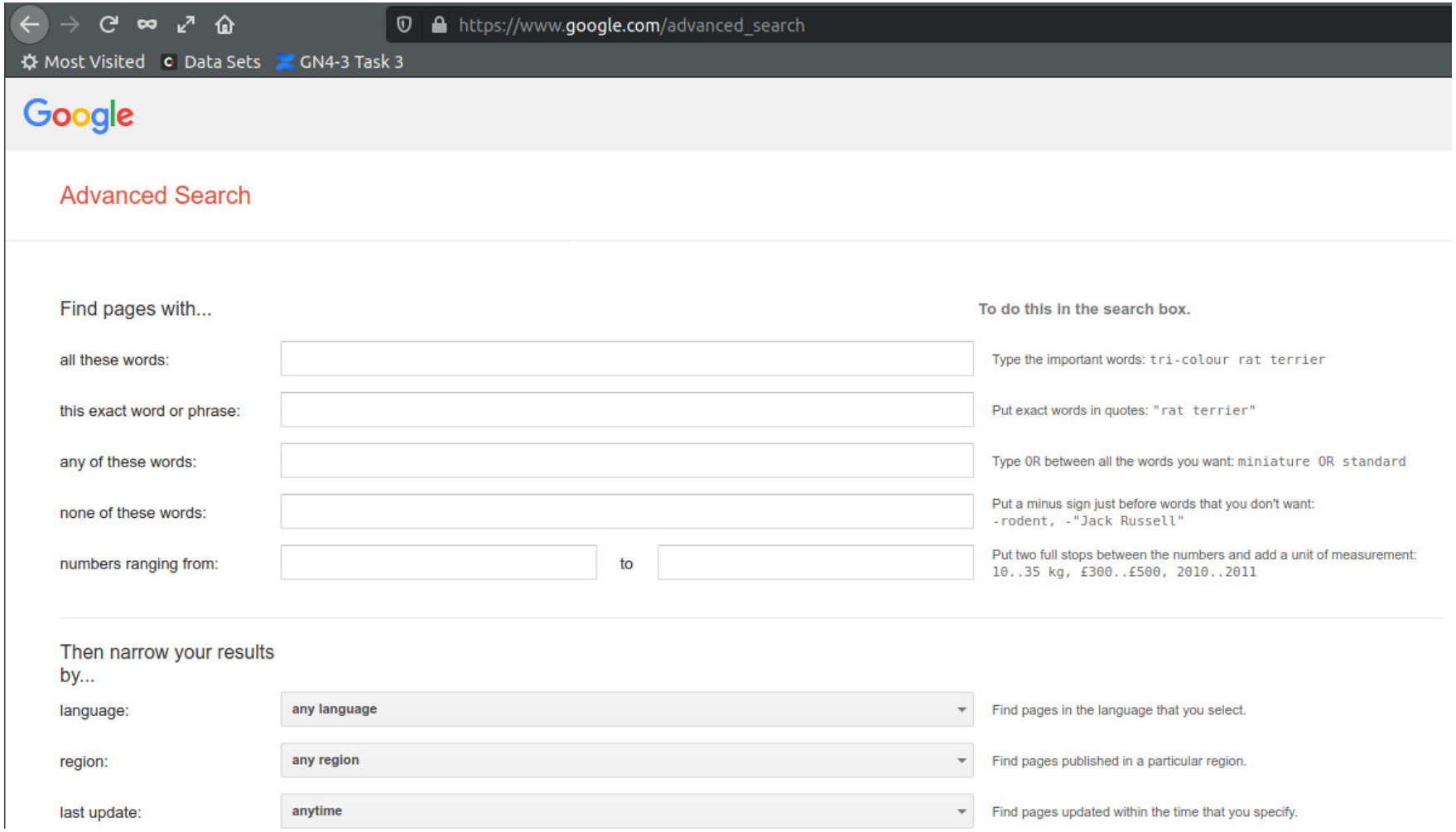
“search engine hacking”

- Explore data publicly available in search engines
- Using advanced operators to fine-tune the results
- Don’t look just the first page of results
- Use different search engines (duckduckgo, baidu, yandex,…)
- Look at the older version of the site: https://archive.org/
- https://www.exploit-db.com/google-hacking-database/

Google operators

- https://ahrefs.com/blog/google-advanced-search-operators/
- Some examples:
  - **cache** Displays the version of a web page that Google contains in its cache instead of displaying the current version. Syntax: cache:<website name>
  - **site** Restricts the search to the location specified. Syntax: <keyword> site:<website name>
  - **allintitle** Returns pages with specified keywords in their title. Syntax: allintitle: <keywords>
  - **allinurl** Returns only results with the specific query in the URL. Syntax: allinurl: <keywords>
- Google can shut down queries using advanced operators if too many appear in a short period of time.

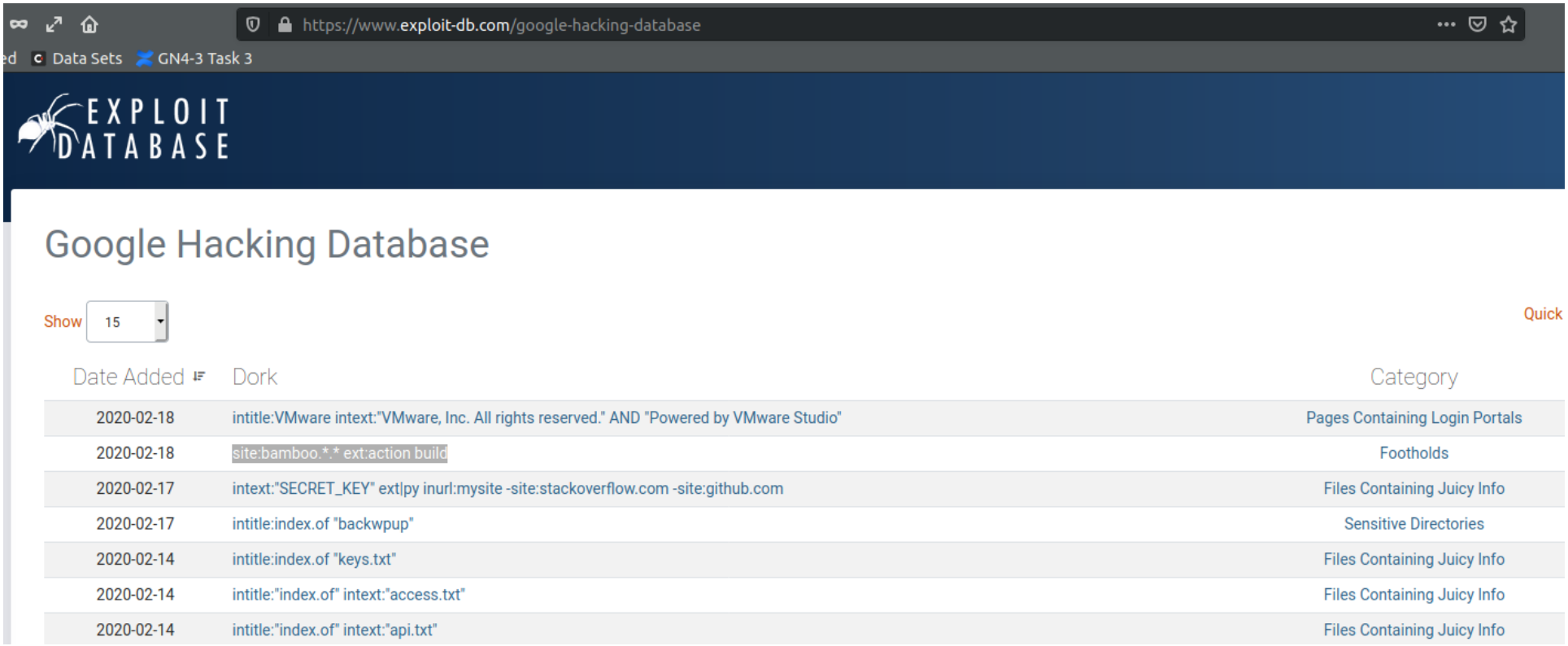
Advanced google search



ISSES

Co-funded by the Erasmus+ Programme of the European Union

Google hacking database



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Location and Geography

- Look for the office location, position, nearby restaurants, etc. Useful for:
  - Dumpster diving,
  - Social engineering
  - Physical penetrations
- Use
  - Google Earth, maps or other maps
  - Webcams
  - Websites like: bele strane, spokeo, yabasearch, wink, intelius

Finding the IP addresses

- ping www.domain.com
- ping can be blocked, but the IP address is resolved
- MANY companies host their web servers at the CDNs (outsourced service)
- Ping gives IP address, round-trip-time, framesize
- traceroute (tracert) – path to the target

```
pavle@pavle-ideapad:~$ ping www.microsoft.com
PING e13678.dspb.akamaiedge.net (2.18.70.63) 56(84) bytes of data.
64 bytes from a2-18-70-63.deploy.static.akamaitechnologies.com (2.18.70.63): icmp_seq=1 ttl=56 time=14.7 ms
64 bytes from a2-18-70-63.deploy.static.akamaitechnologies.com (2.18.70.63): icmp_seq=2 ttl=56 time=18.7 ms
64 bytes from a2-18-70-63.deploy.static.akamaitechnologies.com (2.18.70.63): icmp_seq=3 ttl=56 time=16.9 ms
```

```
pavle@pavle-ideapad:~$ ping www.ftn.uns.ac.rs
PING www.ftn.uns.ac.rs (147.91.175.214) 56(84) bytes of data.
64 bytes from 147.91.175.214 (147.91.175.214): icmp_seq=1 ttl=56 time=3.05 ms
64 bytes from 147.91.175.214 (147.91.175.214): icmp_seq=2 ttl=56 time=2.18 ms
64 bytes from 147.91.175.214 (147.91.175.214): icmp_seq=3 ttl=56 time=3.15 ms
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

DNS records

- Address Mapping record (A Record)—also known as a DNS host record, stores a hostname and its corresponding IPv4 address.
- IP Version 6 Address record (AAAA Record)—stores a hostname and its corresponding IPv6 address.
- Canonical Name record (CNAME Record)—can be used to alias a hostname to another hostname. When a DNS client requests a record that contains a CNAME, which points to another hostname, the DNS resolution process is repeated with the new hostname.
- Mail exchanger record (MX Record)—specifies an SMTP email server for the domain, used to route outgoing emails to an email server.
- Name Server records (NS Record)—specifies that a DNS Zone, such as “example.com” is delegated to a specific Authoritative Name Server, and provides the address of the name server.
- Reverse-lookup Pointer records (PTR Record)—allows a DNS resolver to provide an IP address and receive a hostname (reverse DNS lookup).
- Certificate record (CERT Record)—stores encryption certificates—PKIX, SPKI, PGP, and so on.
- Service Location (SRV Record)—a service location record, like MX but for other communication protocols.
- Text Record (TXT Record)—typically carries machine-readable data such as opportunistic encryption, sender policy framework, DKIM, DMARC, etc.
- Start of Authority (SOA Record)—this record appears at the beginning of a DNS zone file, and indicates the Authoritative Name Server for the current DNS zone, contact details for the domain administrator, domain serial number, and information on how frequently DNS information for this zone should be refreshed.

DNS tools

- nslookup,
- host,
- dig,
- www.dnsstuff.com
- centralops.net
- dig web tools:
  - https://toolbox.googleapps.com/apps/dig
  - https://www.digwebinterface.com/

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Browsing DNS records

- Look for the names of people, devices, software, purpose of the device (servers) in DNS records
- Name and Mail servers in the domain

```
pavle@pavle-ideapad:~$ host mx2.etf.bg.ac.rs
mx2.etf.bg.ac.rs has address 147.91.14.170
```

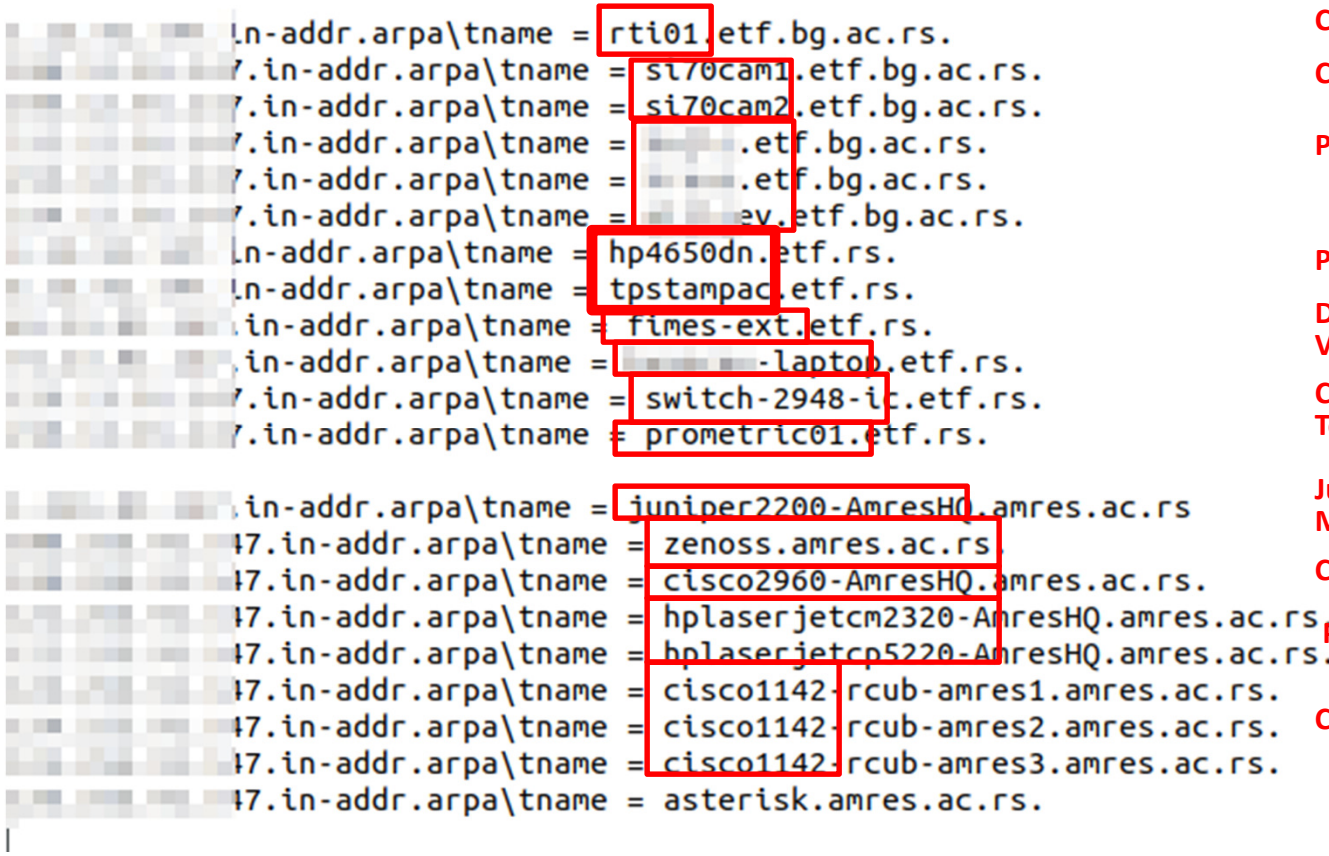
```
pavle@pavle-ideapad:~$ dig etf.bg.ac.rs ns

; <<>> DiG 9.11.3-1ubuntu1.2-Ubuntu <<>> etf.bg.ac.rs ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30740
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;etf.bg.ac.rs.                  IN      NS

;; ANSWER SECTION:
etf.bg.ac.rs.           300     IN      NS      ns2.etf.bg.ac.rs.
etf.bg.ac.rs.           300     IN      NS      ns.rcub.bg.ac.rs.
etf.bg.ac.rs.           300     IN      NS      ns.etf.bg.ac.rs.
etf.bg.ac.rs.           300     IN      NS      ns1.nic.rs.
pavle@pavle-ideapad:~$ dig etf.bg.ac.rs mx

; <<>> DiG 9.11.3-1ubuntu1.2-Ubuntu <<>> etf.bg.ac.rs mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25003
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;etf.bg.ac.rs.                  IN      MX

;; ANSWER SECTION:
etf.bg.ac.rs.           300     IN      MX      5 mx2.etf.bg.ac.rs.
etf.bg.ac.rs.           300     IN      MX      5 mx1.etf.bg.ac.rs.

;; Query time: 1 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Nov 14 13:04:15 CET 2018
;; MSG SIZE  rcvd: 81
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

https://toolbox.googleapps.com/apps/dig

```
id 46287
opcode QUERY
rcode NOERROR
flags QR RD RA
;QUESTION
etf.bg.ac.rs. IN ANY
;ANSWER
etf.bg.ac.rs. 10799 IN SOA NS1.NIC.rs. HOSTMASTER.ETF.rs. 2020020401 10800 3600 2419200 86400
etf.bg.ac.rs. 10799 IN TXT "MS=ms40738589"
etf.bg.ac.rs. 10799 IN TXT "v=spf1 mx a:mail.etf.rs a:smtp.etf.rs a:orao.etf.rs a:mx1.etf.rs a:mx2.etf.rs a:zmaj.etf.rs ?al
etf.bg.ac.rs. 10799 IN A 147.91.14.197
etf.bg.ac.rs. 10799 IN MX 5 mx2.etf.bg.ac.rs.
etf.bg.ac.rs. 10799 IN MX 5 mx1.etf.bg.ac.rs.
etf.bg.ac.rs. 10799 IN NS ns2.etf.bg.ac.rs.
etf.bg.ac.rs. 10799 IN NS ns.etf.bg.ac.rs.
etf.bg.ac.rs. 10799 IN NS NS1.NIC.rs.
etf.bg.ac.rs. 10799 IN NS ns.rcub.bg.ac.rs.
;AUTHORITY
;ADDITIONAL
```

Browsing DNS records



Computer in a lab

Cameras in a lab

Professors PCs

Printers

Dedicated software
Vice deans lap top

Cisco switch
Testing software

Juniper switch
Monitoring software

Cisco switch

Printers

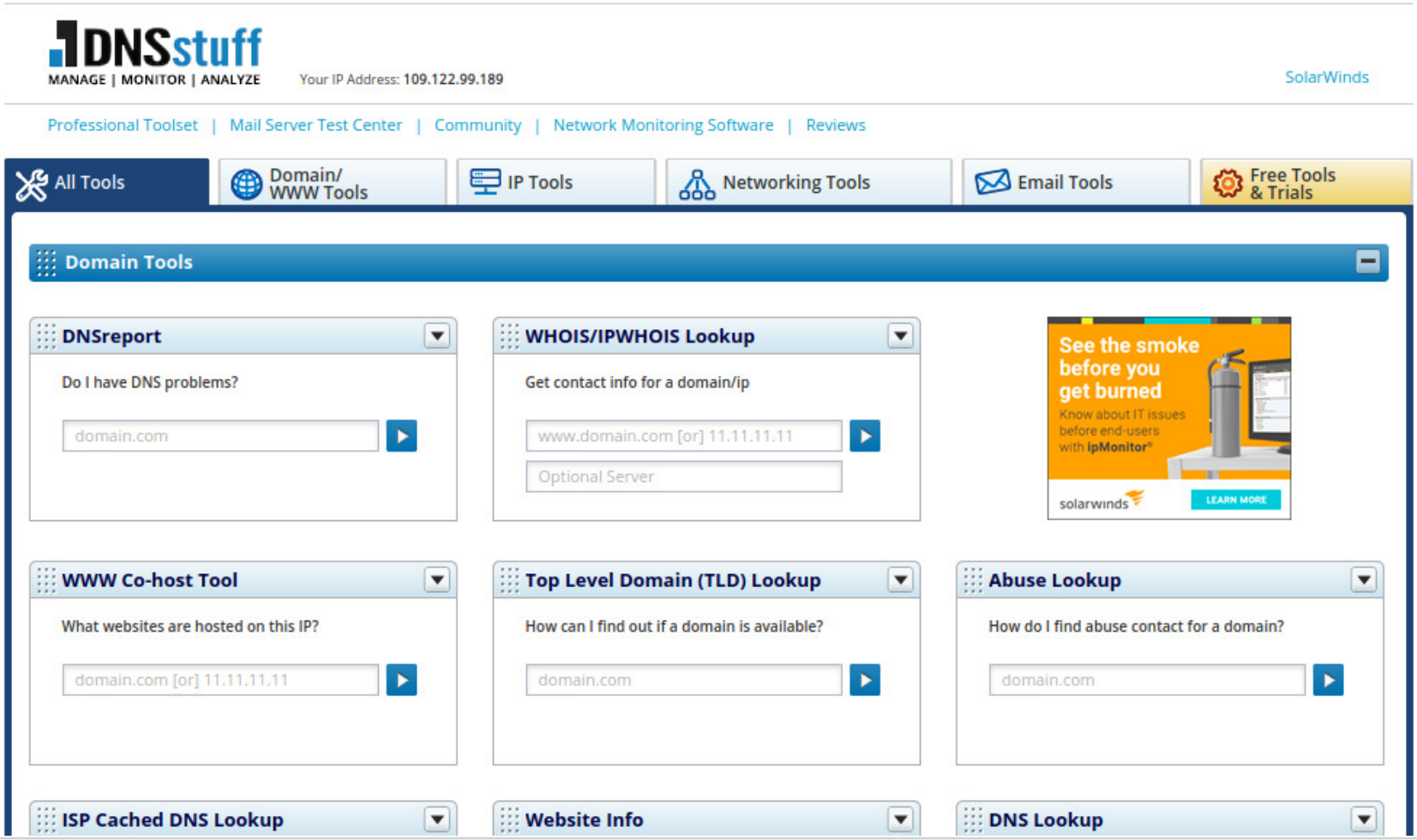
Cisco Access Points

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Ranjivost printera

CVE-ID	
CVE-2011-4785	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Directory traversal vulnerability in the HP-ChaiSOE/1.0 web server on the HP LaserJet P3015 printer with firmware before 07.080.3, LaserJet 4650 printer with firmware 07.006.0, and LaserJet 2430 printer with firmware 08.113.0_I35128 allows remote attackers to read arbitrary files via unspecified vectors, a different vulnerability than CVE-2008-4419.	



WARN	Nameserver software version	One or more nameservers responded to version queries. This can be considered a breach of security. If a malicious person or program had access to a version-specific exploit for your DNS server, displaying the version info openly will make their attack much easier. This should be removed or obscured. The nameservers that responded to version queries are: responded with "9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4" responded with no version information received esponded with "9.9.4-RedHat-9.9.4-74.el7_6.1"

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Finding the IP addresses

- If the target is LIR or has an autonomous system, search the RIR database for:
  - IP addresses
  - AS number, peering
  - Responsible persons
  - Routing information (connected to, path to)
  - Route registry: http://www.irr.net/
- https://www.robtex.com/

RIPE database – Telekom case

```
organisation:     ORG-TS21-RIPE
org-name:         TELEKOM SRBIJA a.d.
org-type:         LIR
address:          Bulevar umetnosti 16a
address:          11070
address:          Belgrade
address:          SERBIA
phone:            +381113120124
fax-no:           +381113120124
e-mail:           ripe@telekom.rs
admin-c:          DJDJ-RIPE
admin-c:          ANAK-RIPE
admin-c:          ANAV-RIPE
admin-c:          SSPR-RIPE
mnt-ref:          TELEKOM-MNT
mnt-ref:          AS8400-MNT
mnt-ref:          RIPE-NCC-HM-MNT
notify:           ripe@telekom.rs
mnt-by:           RIPE-NCC-HM-MNT
mnt-by:           TELEKOM-MNT
abuse-c:          TSA44-RIPE
created:          2004-04-17T12:25:13Z
last-modified:    2017-10-30T14:36:12Z
source:           RIPE
```

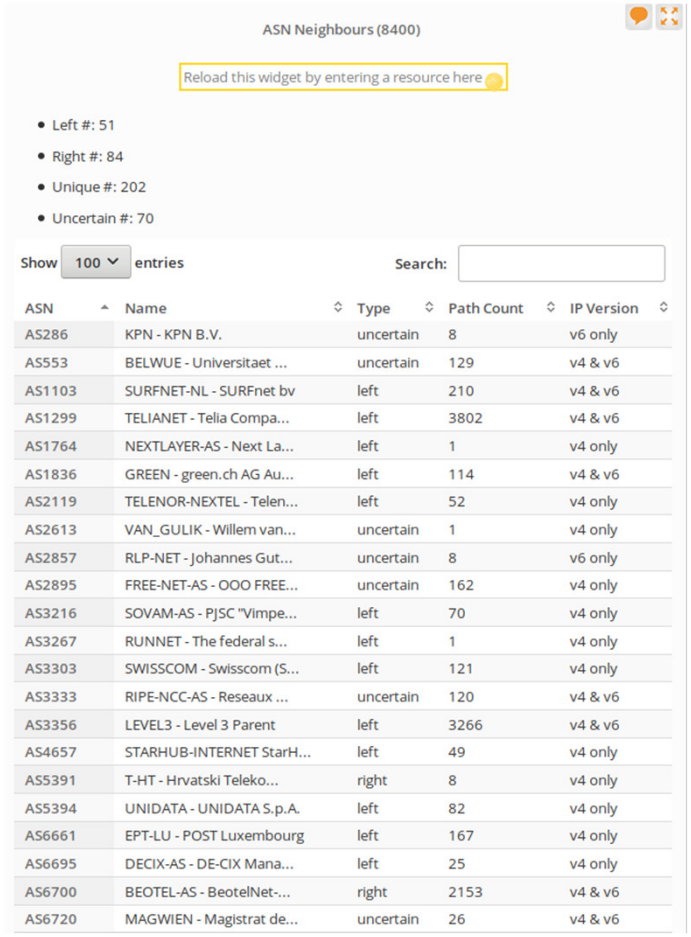
```
mntner:           TELEKOM-MNT
descr:            Maintainer for '
admin-c:          ANAV-RIPE
tech-c:           ANAK-RIPE
tech-c:           ANAV-RIPE
tech-c:           MM46608-RIPE
tech-c:           DJDJ-RIPE
tech-c:           RT3954-RIPE
tech-c:           SP16465-RIPE
tech-c:           DM14573-RIPE
tech-c:           BL2487-RIPE
tech-c:           JM7476-RIPE
tech-c:           SD5970-RIPE
tech-c:           VV2173-RIPE
tech-c:           LE1413-RIPE
tech-c:           ROSI-RIPE
tech-c:           ANAV-RIPE
tech-c:           TR3914-RIPE
tech-c:           BD6734-RIPE
tech-c:           AS33368-RIPE
tech-c:           IS5633-RIPE
tech-c:           VB5809-RIPE
tech-c:           MM41295-RIPE
tech-c:           DI1633-RIPE
tech-c:           ST10547-RIPE
```

```
person:           Jelena Markovic
address:          Telekom Srbija, Katiceva 14
phone:            +381 11 3069019
nic-hdl:          JECA-RIPE
mnt-by:           TELEKOM-MNT
created:          2009-07-13T12:17:48Z
last-modified:    2009-09-21T11:47:14Z
source:           RIPE# Filtered

person:           Sasa Djordjevic
address:          Telekom Srbija, Katiceva 1
phone:            +381 11 3069095
nic-hdl:          DJDJ-RIPE
mnt-by:           TELEKOM-MNT
created:          2009-09-21T11:56:44Z
last-modified:    2009-11-17T14:04:48Z
source:           RIPE# Filtered

person:           Ana Krstic
address:          Telekom Srbija
address:          Bulevar umetnosti 16a
address:          Beograd
phone:            +381 11 3200100
nic-hdl:          ANAK-RIPE
mnt-by:           TELEKOM-MNT
created:          2008-01-18T13:58:21Z
last-modified:    2015-07-21T09:44:06Z
source:           RIPE# Filtered
```

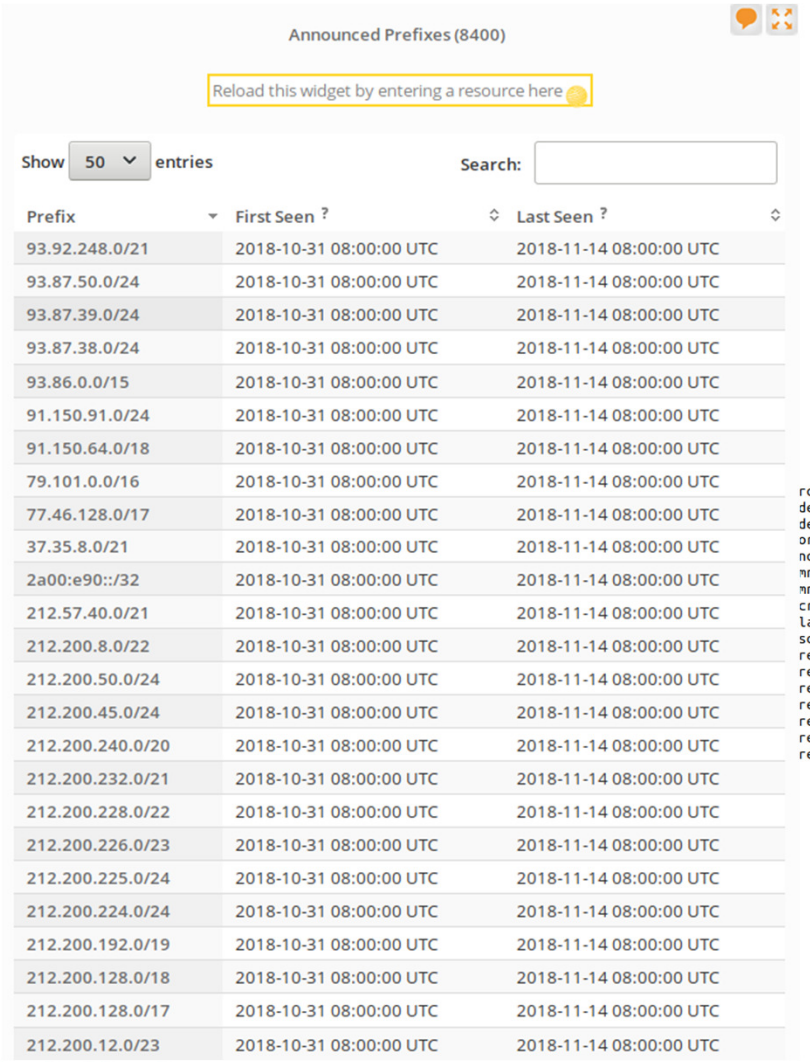
ISSES

Co-funded by the Erasmus+ Programme of the European Union

AS and routing information – Telekom



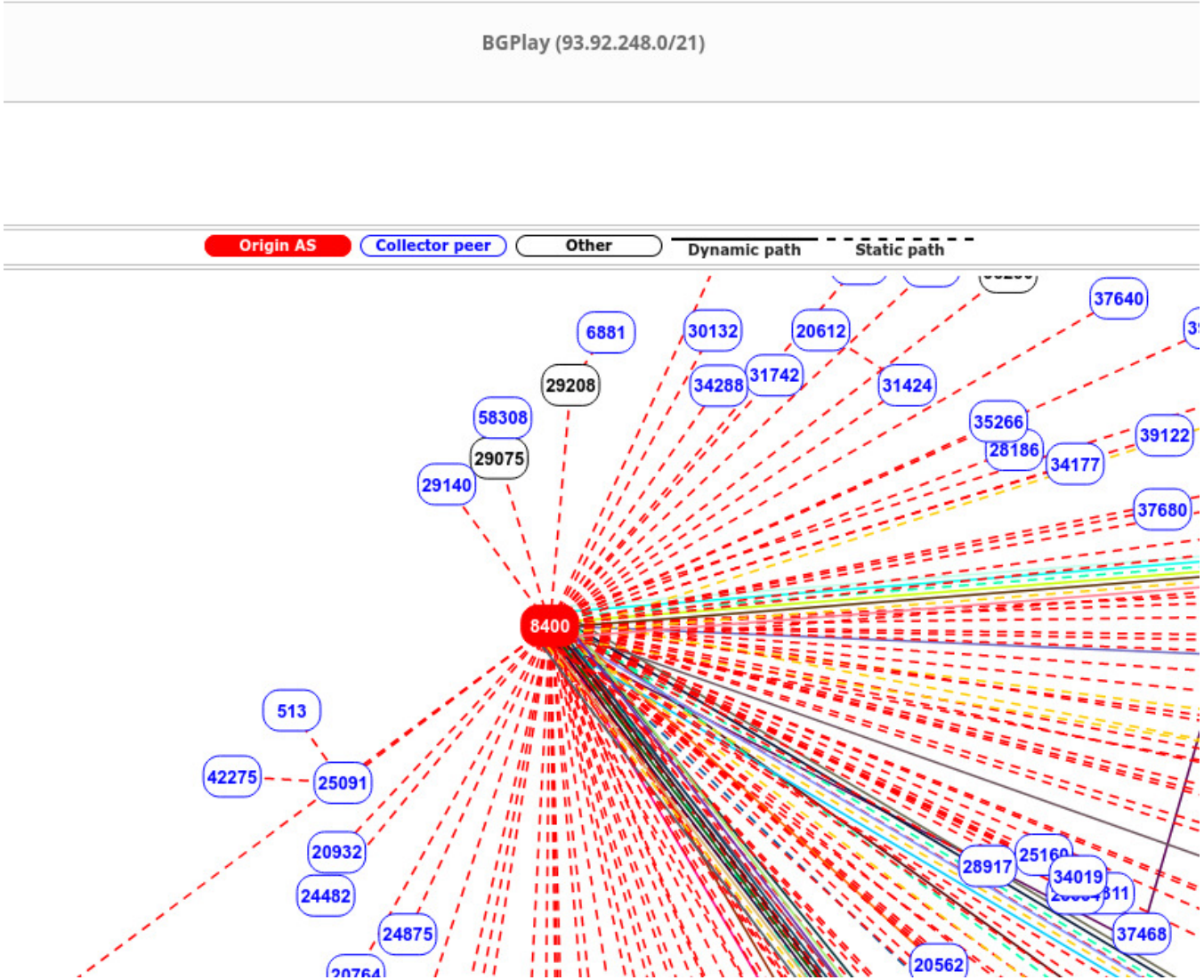
ASN	Name	Type	Path Count	IP Version
AS286	KPN - KPN B.V.	uncertain	8	v6 only
AS553	BELWUE - Universitaet ...	uncertain	129	v4 & v6
AS1103	SURFNET-NL - SURFnet bv	left	210	v4 & v6
AS1299	TELIANET - Telia Compa...	left	3802	v4 & v6
AS1764	NEXTLAYER-AS - Next La...	left	1	v4 only
AS1836	GREEN - green.ch AG Au...	left	114	v4 & v6
AS2119	TELENOR-NEXTEL - Telen...	left	52	v4 only
AS2613	VAN_GULIK - Willem van...	uncertain	1	v4 only
AS2857	RLP-NET - Johannes Gut...	uncertain	8	v6 only
AS2895	FREE-NET-AS - OOO FREE...	uncertain	162	v4 only
AS3216	SOVAM-AS - PJSC "Vimpe...	left	70	v4 only
AS3267	RUNNET - The federal s...	left	1	v4 only
AS3303	SWISSCOM - Swisscom (S...	left	121	v4 only
AS3333	RIPE-NCC-AS - Reseaux ...	uncertain	120	v4 & v6
AS3356	LEVEL3 - Level 3 Parent	left	3266	v4 & v6
AS4657	STARHUB-INTERNET StarH...	left	49	v4 only
AS5391	T-HT - Hrvatski Teleko...	right	8	v4 only
AS5394	UNIDATA - UNIDATA S.p.A.	left	82	v4 only
AS6661	EPT-LU - POST Luxembourg	left	167	v4 only
AS6695	DECIX-AS - DE-CIX Mana...	left	25	v4 only
AS6700	BEOTEL-AS - BeotelNet-...	right	2153	v4 & v6
AS6720	MAGWIEN - Magistrat de...	uncertain	26	v4 & v6



Prefix	First Seen ?	Last Seen ?
93.92.248.0/21	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
93.87.50.0/24	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
93.87.39.0/24	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
93.87.38.0/24	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
93.86.0.0/15	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
91.150.91.0/24	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
91.150.64.0/18	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
79.101.0.0/16	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
77.46.128.0/17	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
37.35.8.0/21	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
2a00:e90::/32	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.57.40.0/21	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.8.0/22	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.50.0/24	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.45.0/24	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.240.0/20	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.232.0/21	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.228.0/22	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.226.0/23	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.225.0/24	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.224.0/24	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.192.0/19	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.128.0/18	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.128.0/17	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC
212.200.12.0/23	2018-10-31 08:00:00 UTC	2018-11-14 08:00:00 UTC

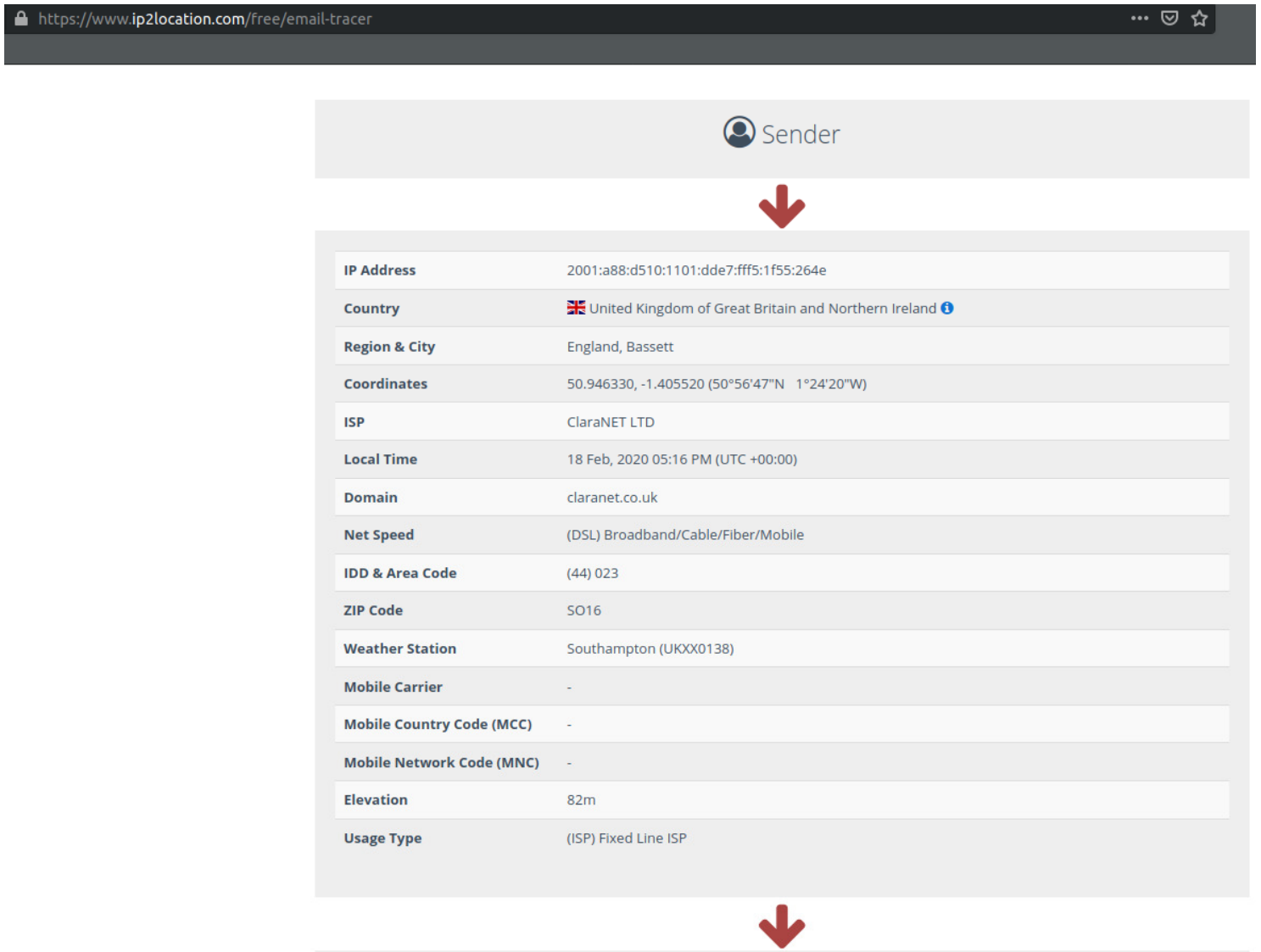
```
route:          195.178.32.0/19
descr:          TELEKOM-SRBIJA
descr:          Telekom Srbija Internet Backbone Ne
origin:         AS8400
notify:         admin@telekom.rs
mnt-by:         TELEKOM-MNT
mnt-by:         AS8400-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2010-04-20T08:19:32Z
source:         RIPE
remarks:        ****************************
remarks:        * THIS OBJECT IS MODIFIED
remarks:        * Please note that all data that is
remarks:        * data has been removed from this o
remarks:        * To view the original object, plea
remarks:        * http://www.ripe.net/whois
remarks:        ****************************
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union


BGPlay (93.92.248.0/21)
Origin AS
Collector peer
Other
Dynamic path
Static path
6881
30132
20612
37640
29208
34288
31742
31424
58308
35266
39122
29075
28186
34177
29140
37680
8400
513
42275
25091
20932
24482
24875
28917
34019
37468
20562

Email analysis

- politemail.com
- whoreadme.com
- https://www.ip2location.com/free/email-tracer
- …



ISSES
Co-funded by the Erasmus+ Programme of the European Union

IP Address	104.47.17.177
Country	Netherlands
Region & City	Noord-Holland, Amsterdam
Coordinates	52.374030, 4.889690 (52°22'27"N 4°53'23"E)
ISP	Microsoft Corporation
Local Time	18 Feb, 2020 06:16 PM (UTC +01:00)
Domain	microsoft.com
Net Speed	(COMP) Company/T1
IDD & Area Code	(31) 020
ZIP Code	1000
Weather Station	Amsterdam (NLXX0002)
Mobile Carrier	-
Mobile Country Code (MCC)	-
Mobile Network Code (MNC)	-
Elevation	6m
Usage Type	(DCH) Data Center/Web Hosting/Transit

ISSES
Co-funded by the Erasmus+ Programme of the European Union

IP Address	146.101.78.189
Country	United Kingdom of Great Britain and Northern Ireland
Region & City	England, Cambridge
Coordinates	51.733330, -2.366670 (51°43'60"N 2°22'0"W)
ISP	Telstra Dedicated Hosting
Local Time	18 Feb, 2020 05:16 PM (UTC +00:00)
Domain	telstra.com.au
Net Speed	(COMP) Company/T1
IDD & Area Code	(44) 01453
ZIP Code	CB4
Weather Station	Stroud (UKXX1066)
Mobile Carrier	-
Mobile Country Code (MCC)	-
Mobile Network Code (MNC)	-
Elevation	14m
Usage Type	(DCH) Data Center/Web Hosting/Transit

ISSES
Co-funded by the Erasmus+ Programme of the European Union

IP Address	83.97.92.155
Country	United Kingdom of Great Britain and Northern Ireland
Region & City	England, Cambridge
Coordinates	51.733330, -2.366670 (51°43'60"N 2°22'0"W)
ISP	GEANT Vereniging
Local Time	18 Feb, 2020 05:16 PM (UTC +00:00)
Domain	geant.org
Net Speed	(COMP) Company/T1
IDD & Area Code	(44) 01453
ZIP Code	CB2
Weather Station	Stroud (UKXX1066)
Mobile Carrier	-
Mobile Country Code (MCC)	-
Mobile Network Code (MNC)	-
Elevation	14m
Usage Type	(DCH) Data Center/Web Hosting/Transit

You

Social engineering and physical security

ISSES

Co-funded by the Erasmus+ Programme of the European Union

SOCIAL ENGINEERING

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Social engineering

- Targeting human beings rather than technology
- Humans are often the weakest link in the security of a system
- Human beings tend to trust each other, but also the attacker can abuse moral obligations or ignorance, threat the victim, promise easy gains…
- Human beings also tend to develop routines and to do many things without thinking
- It is easier to ask for a password than to do the dictionary or brute force attack
- A lot of malware/ransomware was installed by the victims voluntarily

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Social engineering is successful because

- There is no technological fix (there is no patch for human stupidity)
- Does not leave log traces
- Insufficient or inappropriate security polices
- Lack of training/teaching all the employees how to recognize social engineering attempts

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Social engineering phases

1. Use footprinting to get the details about a target (attacks with a lot of accurate information are more credible), social networks
2. Select a group or an individual who can have the needed information. Look for ignorant, frustrated, overconfident or arrogant individuals.
3. Create a relationship with a victim
4. Exploit the relationship with a victim

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Common targets

- Receptionists/office managers
- Help desk
- System administrators
- Executives
- Users

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Some social engineering strategies

- Clickbaits:
  - Test your IQ
  - Naked photos of ###
  - How to make a lot of money without work
- “I have inherited 1.000.000 USD and I need help”
- “Your device has been infected click to clean”
- “Your account needs an update, please send me your password”
- “I’ve recorded you doing XXX,…”

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Social engineering countermeasures

- Don’t mix personal and professional information on social networks
- Don’t connect with unknown persons
- Don’t reuse passwords
- Think about what you are posting about yourself!
- Watch for browser warnings and suspicious pop-ups and downloads
- Use private browsing
- **Educate employees about this!!!**

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Identity theft

- The attacker can behave as if he/she has the identity of the victim:
  - Cash withdrawals
  - goods/service procurements
  - Sending/receiving emails
  - Revealing victim's private information
  - Abusing victim's friends
  - Doing various criminal activities under the name of a victim

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Recent statistics

- Number of phishing URLs - increase of 38% from 2017 to 2018
- Spear phishing emails make 65% of all infection vectors. Spear phishing is the number one cyber-threat to organizations in the European Union (EUROPOL)
- Phishing attacks, which aim to trick unsuspecting users into clicking on something or providing personal information, were also on the rise, with the majority (55%) of respondents identifying a rise in phishing attacks over the last 12 months.
- Email is a common delivery mechanism for ransomware, which is having a growing impact on organizations. 53% of organizations experienced a business-disrupting ransomware attack, up from 26% in the 2018 report.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

(IDN) homograph attack

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Only one of these domains is really a bank domain. Which one?

A. https://www.kombank.com/sr
B. https://www.kombank.com/sr
C. https://www.kombank.com/sr
D. https://www.kombank.com/sr
E. https://www.kombank.com/sr
F. https://www.kombank.com/sr

Answer:

A.	https://www.kombank.com/sr	https://www.kombank.com/sr
B.	https://www.kombank.com/sr	https://www.xn--kmbank-wqf.com/sr
C.	https://www.kombank.com/sr	https://www.xn--kmbnk-6ve9g.com/sr
D.	https://www.kombank.com/sr	https://www.xn--kombnk-6nf.com/sr
E.	https://www.kombank.com/sr	https://www.xn--kmbank-i0e.com/sr
F.	https://www.kombank.com/sr	https://www.xn--kmbank-bmh.com/sr

Cyrillic o and a. greek omikron. Armenian letter o.

Less sofisticated attacks - Punnycode replacement with similar letters:

A.	https://www.kombạnk.com/sr	https://www.xn--kombnk-zc8b.com/sr
B.	https://www.kornbank.com/sr	
C.	https://www.kömbank.com/sr	https://www.xn--kmbank-ppg.com/sr

Other frauds: Typosquatting, Doppelganger domain

Misspelling: exemple.com

Typo: examlpe.com, arifrance.com

Wrong TLD: google.org

Instead mail.google.com: mailgoogle.com

PHYSICAL SECURITY

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Physical security

- Protecting personnel, hardware, applications, facilities from natural disasters, theft, insider and outsider threats.
- The attacker who has the physical access to the equipment can get any information (keyloggers, cameras, microphones, console access,…)
- Securing the physical area of the company (data centre, offices, cable ducts, portable drives, mobile devices…)
- Fences, gates, locks, walls, windows, mantraps, video surveillance
- Access using pins, cards, biometrics, keyboard dynamics
- Procedures for the access to the restricted parts of the company

ISSES
Co-funded by the Erasmus+ Programme of the European Union