Monitoring e Security: due volti della stessa medaglia?

Massimo Giaimo, Würth Phoenix

12 Novembre 2020 15:00-15:45 - StreamingEdition

#securitysummit #streamingedition

20 years
2000-2020

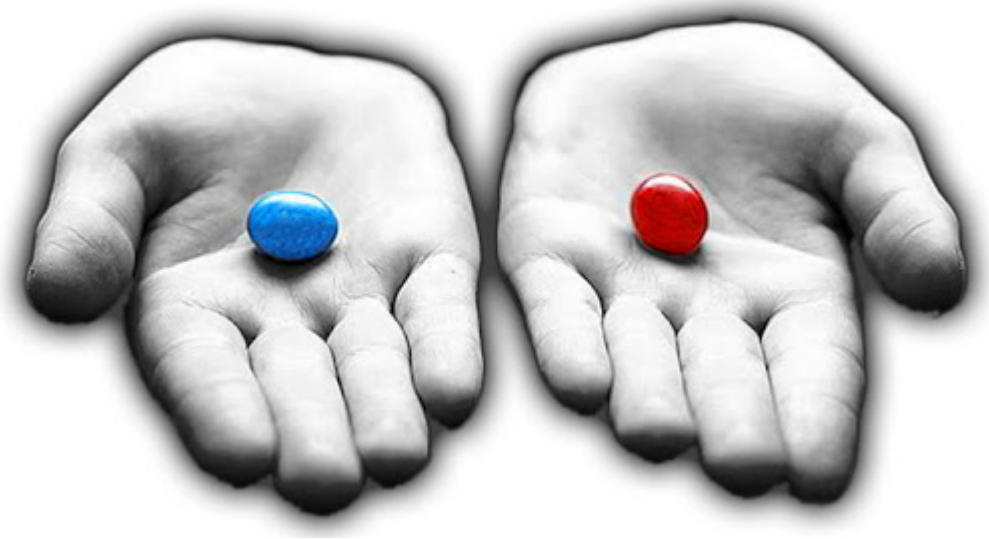
WÜRTHPHOENIX

EXPOSURE ASSESSMENT

OSINT COME ELEMENTO DI DIFESA

Massimo Giaimo

È la tua ultima occasione, se rinunci non ne avrai altre !



Pillola azzurra

fine della storia: domani ti sveglierai in camera tua, e crederai a quello che vorrai.

Pillola rossa

resti nel paese delle meraviglie, e vedrai quant'è profonda la tana del bianconiglio.

OSINT

COS' É

- Disciplina dell'intelligence
- Collezione e analisi di informazioni pubbliche, liberamente accessibili
- Esempi di fonti:

Mezzi di comunicazione | Dati pubblici
Accesso alla rete internet | Foto-audio-video|
Osservazioni dirette

Ricerca | Selezione
Analisi | Diffusione

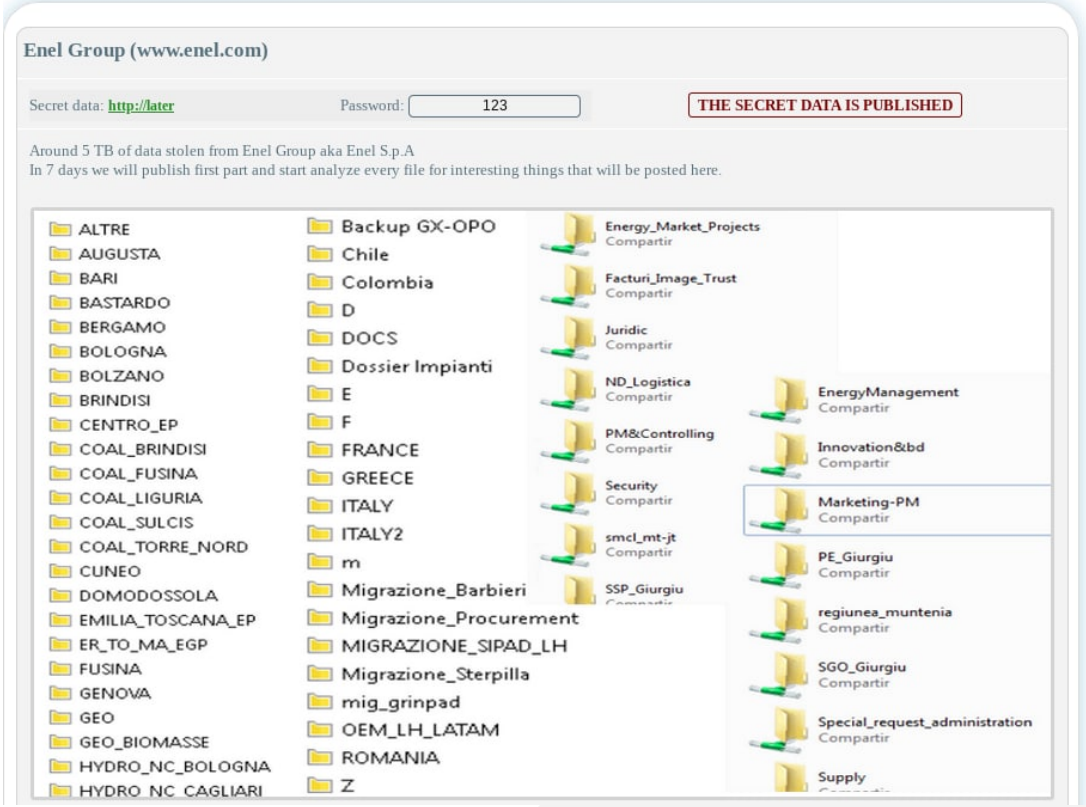
- Utilizzo di un approccio analitico basato su 4 fasi

Challenge!

Enel vittima di attacco ransomware: il riscatto richiesto è di 14 milioni di dollari (in bitcoin)

Sottratti 5TB di informazioni al Gruppo Enel: oltre alla richiesta di riscatto, anche la minaccia di divulgare informazioni e dati riservati nel giro di una settimana

- Trova queste informazioni:
  - Nome gruppo di cybercriminali autori dell'attacco
  - Link alla pagina del gruppo di cybercriminali
  - Informazioni dettagliate sul malware utilizzato per l'attacco
- Invia la soluzione a info@wuerth-phoenix.com
- Verrai contattato e ti verrà inviata una copia di "**Sulla cresta della sicurezza: 30 step per rendere sicura un'organizzazione**"



La sfida è lanciata…Siete pronti?

Domain(s) info

```
**********************************************************************
* Please note that the following result could be a subgroup of       *
* the data contained in the database.                                *
*                                                                    *
* Additional information can be visualized at:                       *
* http://web-whois.nic.it                                            *
* Privacy Information: http://web-whois.nic.it/privacy               *
**********************************************************************

Domain:                 enel.it
Status:                 ok
Signed:                 no
Created:                1996-01-29 00:00:00
Last Update:            2020-04-09 00:49:35
Expire Date:            2021-03-24

Registrant
  Organization:         enel S.p.A.
  Address:              Viale Regina MArgherita 137
                        Roma
                        00198
                        RM
                        IT
  Created:              2007-03-01 10:47:05
  Last Update:          2016-06-06 10:30:34

Admin Contact
  Name:                 Stefano Regaglia
  Address:              ENEL S.p.A. - Sistemi Informatici
                        V.le Italia, 26
                        Sesto San Giovanni
                        20099
                        MI
                        IT
  Created:              1999-03-30 00:00:00
  Last Update:          2016-06-06 10:34:55
```

TOOL used

whois command

Similar domains


```
[redacted]$ python3 dnstwist.py -r

{20190706}

Processing 1081 domain variants ........18%......34%......50%......65%......80%..

Original*       enel.it      192.230.80.63 NS:bdns.enel.it
Addition        enela.it     127.0.0.1
Addition        enelb.it     127.0.0.1
Addition        enelc.it     127.0.0.1
Addition        eneld.it     127.0.0.1
Addition        enele.it     127.0.0.1
Addition        enelf.it     127.0.0.1
Addition        enelg.it     127.0.0.1
Addition        enelh.it     127.0.0.1
Addition        eneli.it     184.168.131.241 NS:ns81.domaincontrol.com
Addition        enelj.it     127.0.0.1
Addition        enelk.it     NS:bdns.enel.it
Addition        enell.it     NS:bdns.enel.it
Addition        enelm.it     127.0.0.1
Addition        eneln.it     127.0.0.1
Addition        enelo.it     127.0.0.1
Addition        enelp.it     127.0.0.1
Addition        enelq.it     127.0.0.1
Addition        enelr.it     127.0.0.1
Addition        enels.it     127.0.0.1
Addition        enelt.it     127.0.0.1
Addition        enelu.it     127.0.0.1
Addition        enelv.it     127.0.0.1
Addition        enelw.it     127.0.0.1
Addition        enelx.it     107.154.251.0 NS:bdns.enel.it
Addition        enely.it     127.0.0.1
Addition        enelz.it     127.0.0.1
Bitsquatting    dnel.it      127.0.0.1
Bitsquatting    gnel.it      127.0.0.1
Bitsquatting    anel.it      NS:dns.agonet.it
Bitsquatting    mnel.it      127.0.0.1
Bitsquatting    unel.it      89.46.107.224 NS:dns.technorail.com MX:mx.unel.it
Bitsquatting    eoel.it      127.0.0.1
Bitsquatting    elel.it      199.59.242.153 NS:ns1.bodis.com MX:mx76.m2bp.com
Bitsquatting    ejel.it      127.0.0.1
Bitsquatting    efel.it      62.149.128.151 NS:dns.technorail.com MX:mx.efel.it
```

TOOL used: dnstwist (https://github.com/elceef/dnstwist)

Hostnames

```
$ python3 dnsrecon.
usage: dnsrecon.py [-h] -d DOMAIN [-n NS_SERVER] [-r RANGE] [-D DICTIONARY]
                   [-f] [-a] [-s] [-b] [-y] [-k] [-w] [-z] [--threads THREADS]
                   [--lifetime LIFETIME] [--tcp] [--db DB] [-x XML] [-c CSV]
                   [-j JSON] [--iw] [--disable_check_recursion]
                   [--disable_check_bindversion] [-v] [-t TYPE]

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Target domain.
  -n NS_SERVER, --name_server NS_SERVER
                        Domain server to use. If none is given, the SOA of the
                        target will be used. Multiple servers can be specified
                        using a comma separated list.
  -r RANGE, --range RANGE
                        IP range for reverse lookup brute force in formats
                        (first-last) or in (range/bitmask).
  -D DICTIONARY, --dictionary DICTIONARY
                        Dictionary file of subdomain and hostnames to use for
                        brute force. Filter out of brute force domain lookup,
                        records that resolve to the wildcard defined IP
                        address when saving records.
  -f                    Filter out of brute force domain lookup, records that
                        resolve to the wildcard defined IP address when saving
                        records.
  -a                    Perform AXFR with standard enumeration.
  -s                    Perform a reverse lookup of IPv4 ranges in the SPF
                        record with standard enumeration.
  -b                    Perform Bing enumeration with standard enumeration.
  -y                    Perform Yandex enumeration with standard enumeration.
  -k                    Perform crt.sh enumeration with standard enumeration.
  -w                    Perform deep whois record analysis and reverse lookup
                        of IP ranges found through Whois when doing a standard
                        enumeration.
```

TOOL used: dnsrecon

(https://github.com/darkoperator/dnsrecon)

Hostnames

crt.sh Identity Search

Group by Issuer

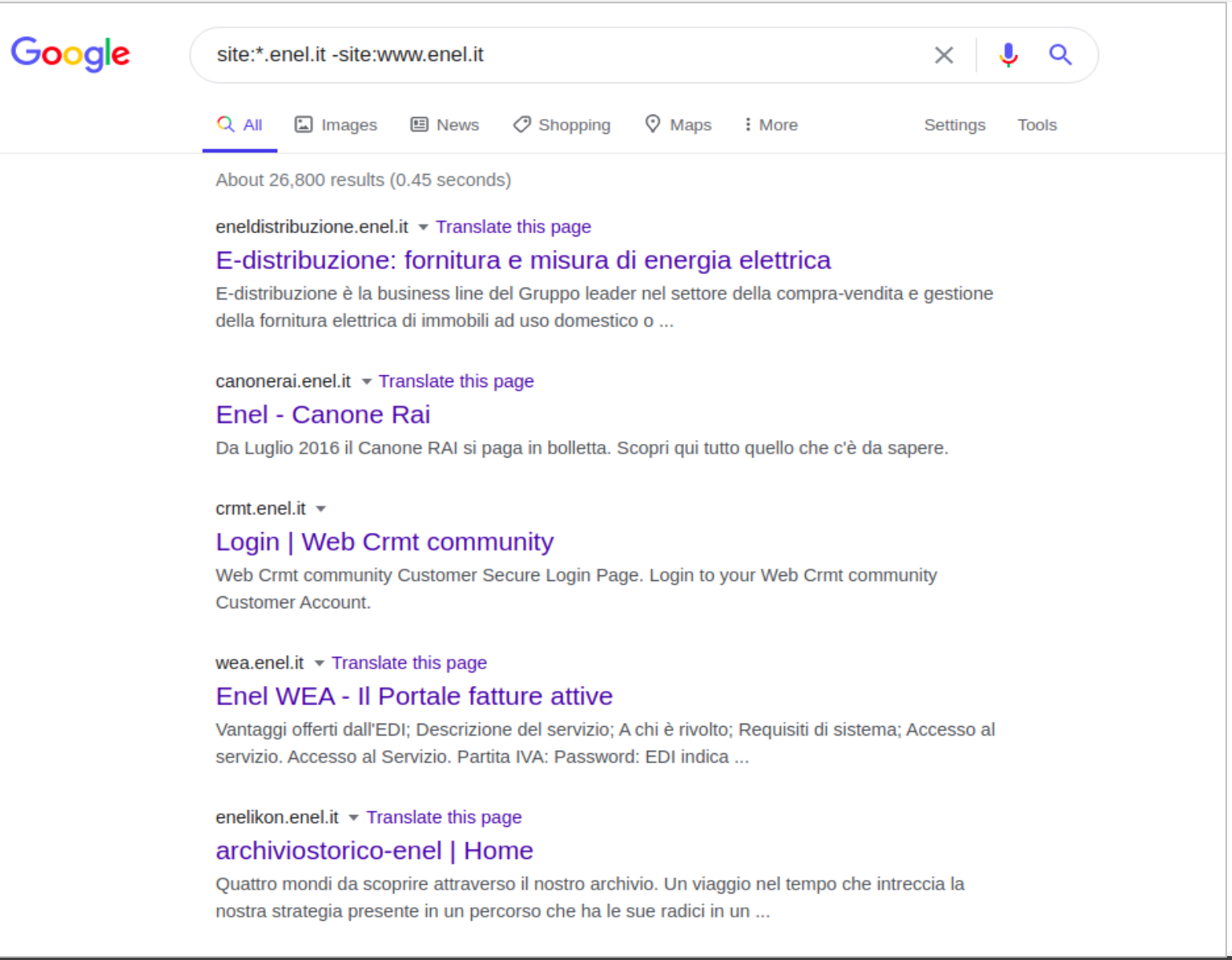
Criteria	Type: Identity Match: ILIKE Search: 'enel.it'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
3588009528	2020-11-01	2020-10-29	2021-04-30	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
3578830876	2020-10-30	2020-10-27	2021-04-28	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
3574634934	2020-10-29	2020-10-29	2021-04-30	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
3565473226	2020-10-27	2020-10-27	2021-04-28	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
3564577867	2020-10-27	2020-10-26	2021-04-26	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
3558192179	2020-10-26	2020-10-26	2021-04-26	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
3531147165	2020-10-19	2020-10-19	2021-10-19	captive.enel.it	captive.enel.it	C=IT, O=InfoCert S.p.A., OU=WSA Trust Service Provider, serialNumber=07945211006, CN=InfoCert Organization Validation 2019 CA 3
3529985228	2020-10-19	2020-10-16	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3517317357	2020-10-16	2020-10-16	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3516366995	2020-10-16	2020-10-16	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3496296545	2020-10-12	2020-09-28	2021-09-28	crmt.enel.it	crmt.enel.it	C=IT, O=InfoCert S.p.A., OU=WSA Trust Service Provider, serialNumber=07945211006, CN=InfoCert Organization Validation 2019 CA 3
3473644646	2020-10-06	2020-10-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3473643734	2020-10-06	2020-10-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3473643274	2020-10-06	2020-10-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3473643696	2020-10-06	2020-10-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3470672378	2020-10-05	2020-10-05	2021-10-05	4ele-wssf.enel.it	4ele-collaudo-wssf.enel.it 4ele-wssf.enel.it	C=IT, O=InfoCert S.p.A., OU=WSA Trust Service Provider, serialNumber=07945211006, CN=InfoCert Organization Validation 2019 CA 3
3466624069	2020-10-04	2020-10-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3466417741	2020-10-04	2020-10-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3465979400	2020-10-04	2020-10-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3464808707	2020-10-04	2020-10-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3458227133	2020-10-02	2020-09-30	2021-04-01	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
3456704491	2020-10-02	2020-10-02	2021-07-08	api.enelcrmt.uat.enel.it	api.enelcrmt.uat.enel.it	C=IT, O=InfoCert S.p.A., OU=WSA Trust Service Provider, serialNumber=07945211006, CN=InfoCert Organization Validation 2019 CA 3
3449566204	2020-09-30	2020-09-30	2021-04-01	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
3438974573	2020-09-28	2020-09-28	2021-09-28	crmt.enel.it	crmt.enel.it	C=IT, O=InfoCert S.p.A., OU=WSA Trust Service Provider, serialNumber=07945211006, CN=InfoCert Organization Validation 2019 CA 3
3430351786	2020-09-26	2020-09-24	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3420405569	2020-09-24	2020-09-24	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3408814083	2020-09-21	2020-09-18	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3408612343	2020-09-21	2020-09-18	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3397738820	2020-09-18	2020-09-18	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3397003013	2020-09-18	2020-09-18	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3391835967	2020-09-17	2020-09-15	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3387885852	2020-09-16	2020-09-14	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3386595669	2020-09-16	2020-09-16	2021-03-17	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
3384942991	2020-09-15	2020-09-15	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3380919092	2020-09-14	2020-09-14	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3372017451	2020-09-12	2020-09-09	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3372016001	2020-09-12	2020-09-10	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3364618577	2020-09-10	2020-09-10	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3360939840	2020-09-09	2020-09-09	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3296608940	2020-08-27	2020-08-25	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3289178989	2020-08-25	2020-08-25	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3237937259	2020-08-14	2020-08-11	2021-02-10	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign HV RSA DV SSL CA 2018
3222175302	2020-08-11	2020-08-11	2021-02-10	imperva.com	*.futur-e.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign HV RSA DV SSL CA 2018
3201944382	2020-08-07	2020-08-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3188655222	2020-08-04	2020-08-04	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3062762191	2020-07-09	2020-07-06	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3059212637	2020-07-08	2020-07-08	2021-07-08	api.enelcrmt.uat.enel.it	api.enelcrmt.uat.enel.it	C=IT, O=InfoCert S.p.A., OU=WSA Trust Service Provider, serialNumber=07945211006, CN=InfoCert Organization Validation CA 3
3049313100	2020-07-06	2020-07-06	2021-05-03	incapsula.com	*.sole.enel.it	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3042103518	2020-07-05	2020-06-12	2021-06-17	view.enelenergia.enel.it	view.enelenergia.enel.it	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
3042103568	2020-07-05	2020-06-12	2021-06-17	cloud.enelenergia.enel.it	cloud.enelenergia.enel.it	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA

TOOL used:crt.sh
(https://crt.sh/)

Hostnames



TOOL used: Google

(site keyword)

IP Addresses

```
[redacted]:~$ dig ftp.enel.it

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> ftp.enel.it
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43117
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ftp.enel.it.                   IN      A

;; ANSWER SECTION:
ftp.enel.it.            7094    IN      A       146.133.2.164

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Nov 02 16:27:53 CET 2020
;; MSG SIZE  rcvd: 56

[redacted]:~$ dig netscaler-na.enel.it

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> netscaler-na.enel.it
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59452
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;netscaler-na.enel.it.          IN      A

;; ANSWER SECTION:
netscaler-na.enel.it.   7200    IN      A       146.133.156.250

;; Query time: 32 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Nov 02 16:27:57 CET 2020
;; MSG SIZE  rcvd: 65
```

TOOL used: dig command

IP block

Responsible organisation: ENEL S.p.A
Abuse contact info: ripe@enel.com

☑ Highlight RIPE NCC managed values

Login to update | RIPEstat

```
inetnum:        146.133.0.0 - 146.133.255.255
netname:        ENEL-NET
org:            ORG-ES6-RIPE
descr:          V.le Italia, 26
descr:          20099 Sesto S. Giovanni (MI)
descr:          Italia
country:        IT
admin-c:        PZ542-RIPE
tech-c:         EL1045-RIPE
status:         LEGACY
mnt-by:         ENEL-LIR
mnt-by:         RIPE-NCC-LEGACY-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2016-04-14T10:13:43Z
source:         RIPE
```

Login to update | RIPEstat

```
route:          146.133.2.0/24
descr:          Enel.it Milano
origin:         AS12551
mnt-by:         ENEL-LIR
created:        2013-11-04T08:01:50Z
last-modified:  2013-11-04T08:01:50Z
source:         RIPE
```

RIPE Database Software Version 1.98

TOOL used: Regional Internet Registry database
(in this case: RIPE)

IP blocks list

Search results

This is the RIPE Database full text search service.
The RIPE Database is subject to Terms and Conditions.

Number of results - all object types	5
inetnum	5

inetnum: 146.133.0.0 - 146.133.255.255
netname=**ENEL-NET**

inetnum: 158.47.0.0 - 158.47.255.255
netname=**ENEL-NET**

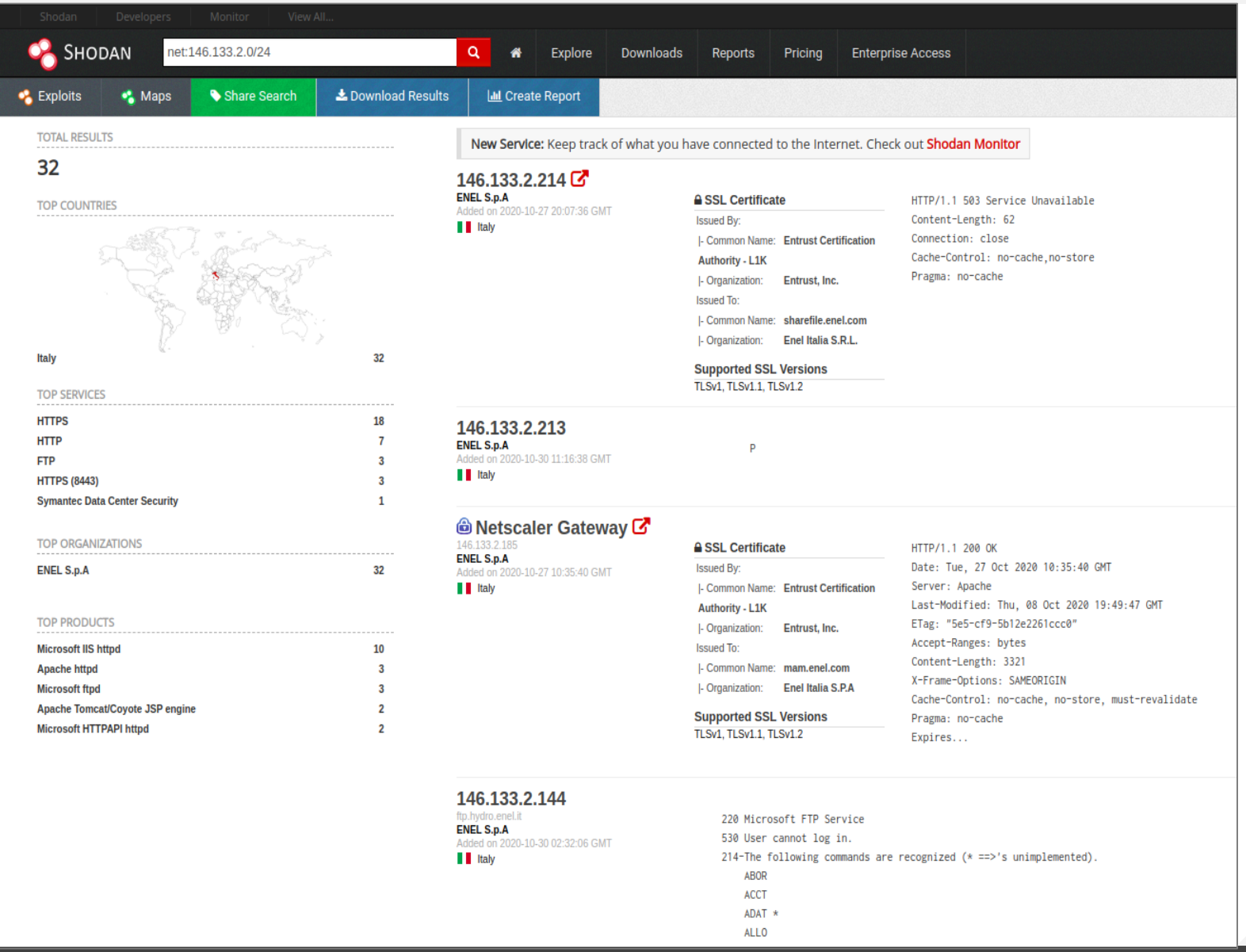
inetnum: 213.194.113.248 - 213.194.113.255
netname=**Enel-NET**

inetnum: 146.133.224.0 - 146.133.255.255
netname=**ENEL-NET**

inetnum: 93.87.17.148 - 93.87.17.151
netname=**ENEL-NET**

TOOL used: Regional Internet Registry database
(in this case: RIPE)

Ports & Services



TOOL used: Shodan
(https://www.shodan.io/)

Vulnerabilities

TOOL used: Shodan (https://www.shodan.io/)

[redacted]46.52 [redacted]-46-52.ip.[redacted].it View Raw Data

City	[redacted]
Country	Italy
Organization	[redacted]
ISP	[redacted]
Last Update	2020-10-30T06:24:26.693411
Hostnames	[redacted]
ASN	AS20[redacted]

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-3510	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2014-0076	The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

Ports

80 443

Services

80
tcp
http

Apache httpd Version: 2.2.22

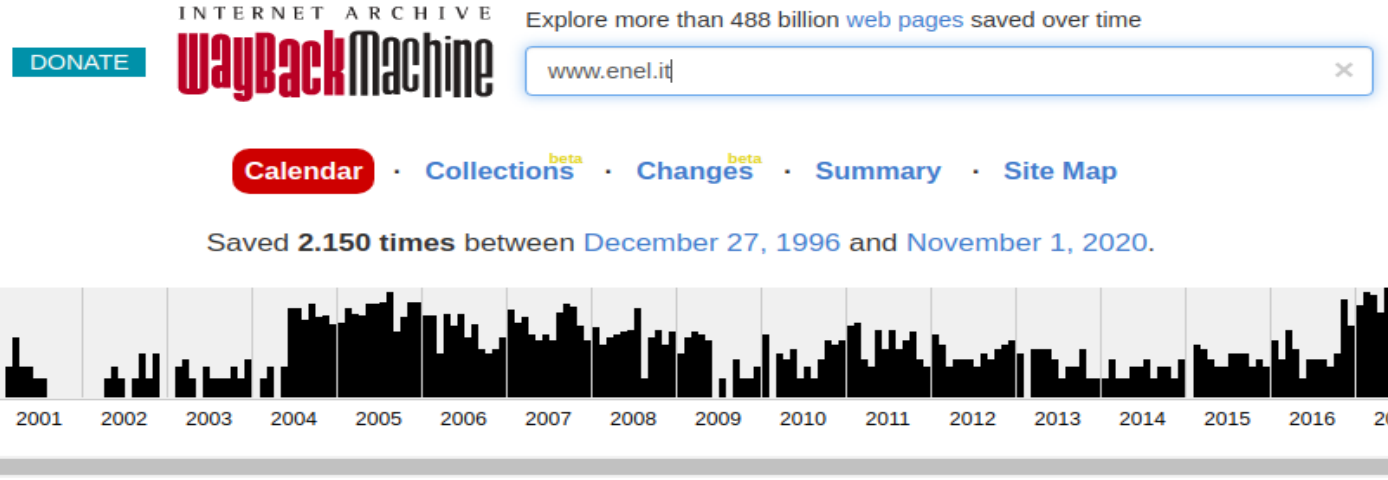
```
HTTP/1.1 403 Forbidden
Date: Fri, 30 Oct 2020 06:24:26 GMT
Server: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8t
Content-Length: 202
Content-Type: text/html; charset=iso-8859-1
```

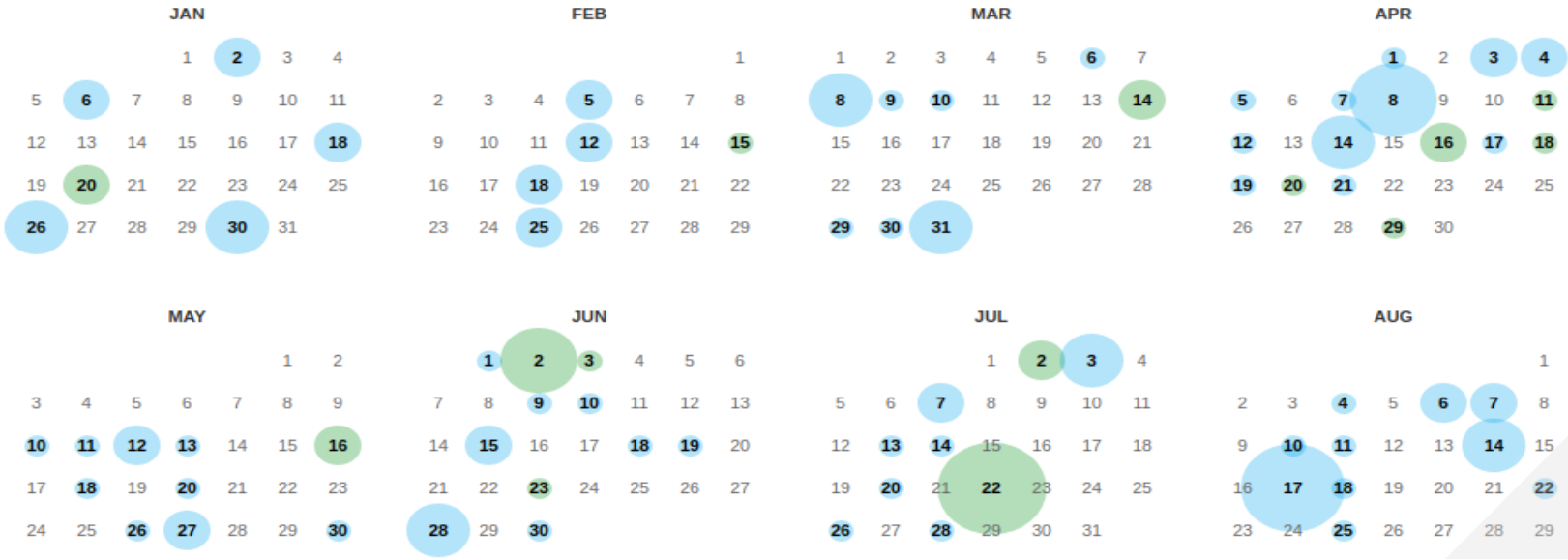
443
tcp
https

Apache httpd Version: 2.2.22

```
HTTP/1.1 403 Forbidden
Date: Mon, 26 Oct 2020 09:26:22 GMT
Server: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8t
Content-Length: 202
Content-Type: text/html; charset=iso-8859-1
```

Old web sites versions

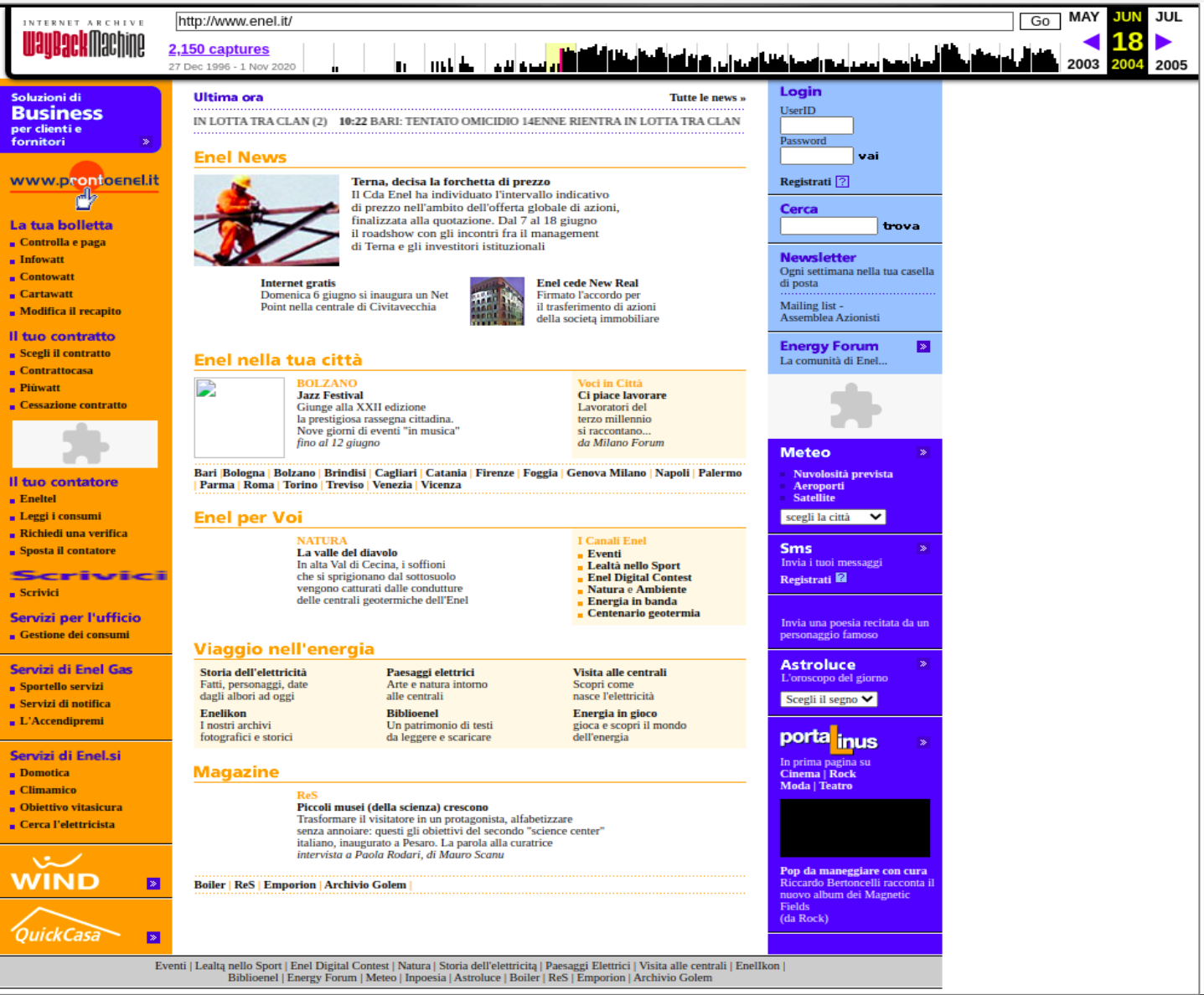




TOOL used:

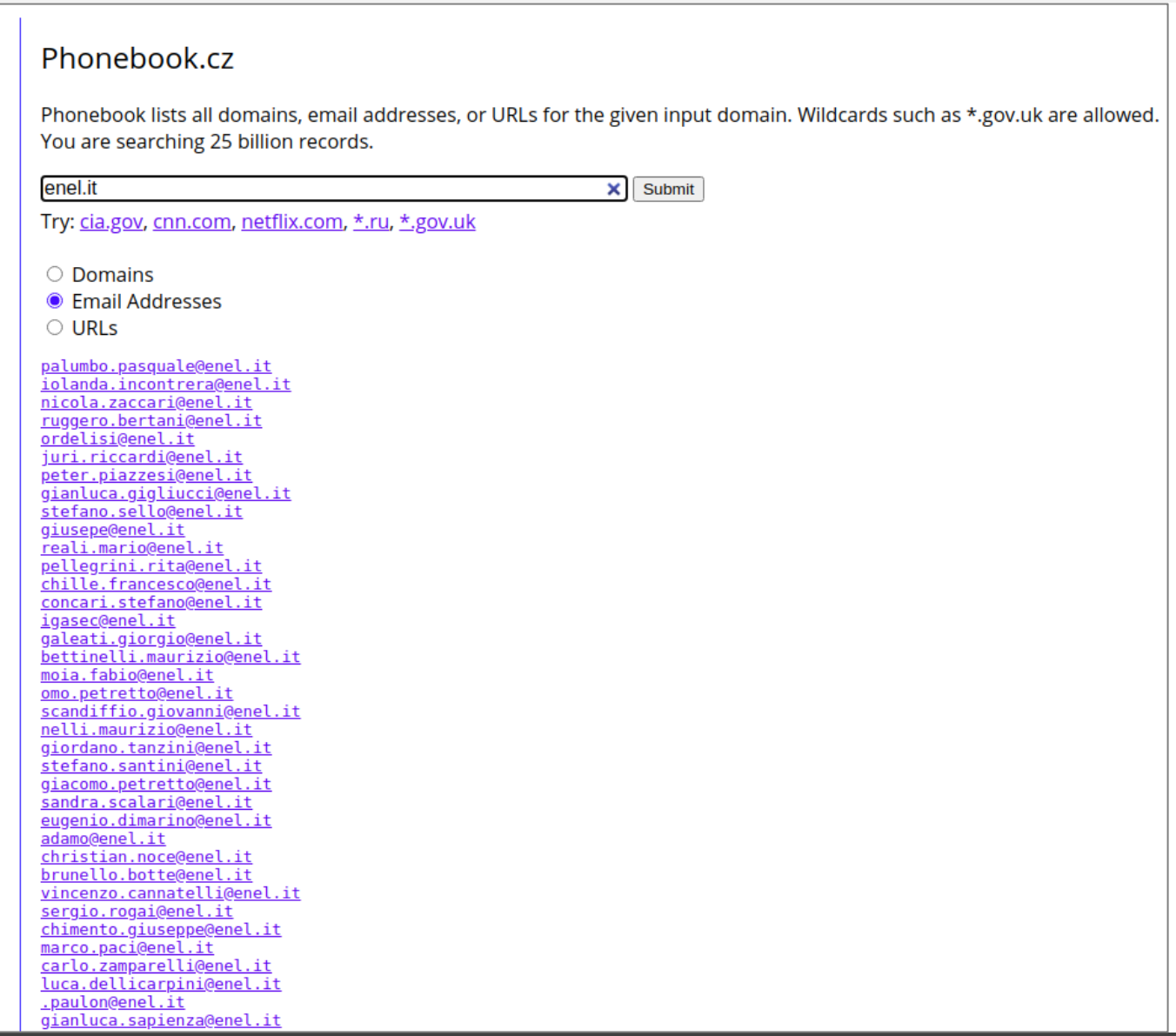
Wayback Machine (https://web.archive.org/)

Old web sites versions



TOOL used: Wayback Machine
(https://web.archive.org/)

Email accounts



Phonebook.cz

Phonebook lists all domains, email addresses, or URLs for the given input domain. Wildcards such as *.gov.uk are allowed.
You are searching 25 billion records.

enel.it Submit

Try: cia.gov, cnn.com, netflix.com, *.ru, *.gov.uk

- Domains
- Email Addresses
- URLs

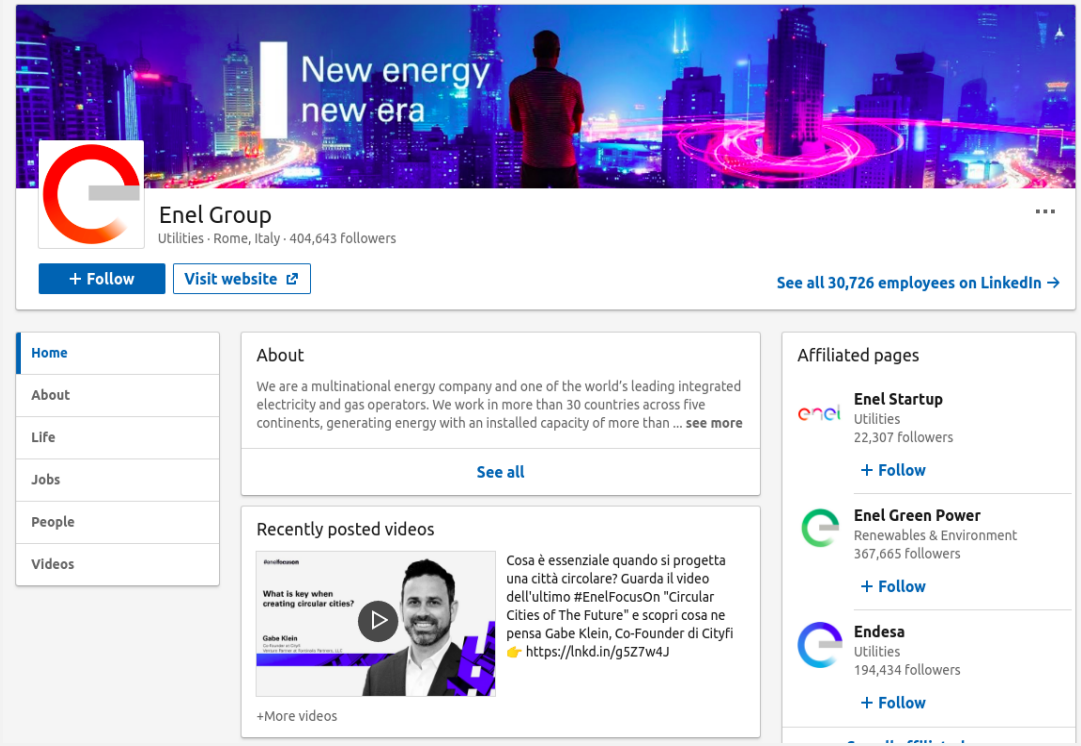
palumbo.pasquale@enel.it
iolanda.incontrera@enel.it
nicola.zaccari@enel.it
ruggero.bertani@enel.it
ordelisi@enel.it
juri.riccardi@enel.it
peter.piazzesi@enel.it
gianluca.gigliucci@enel.it
stefano.sello@enel.it
giusepe@enel.it
reali.mario@enel.it
pellegrini.rita@enel.it
chille.francesco@enel.it
concari.stefano@enel.it
igasec@enel.it
galeati.giorgio@enel.it
bettinelli.maurizio@enel.it
moia.fabio@enel.it
omo.petretto@enel.it
scandiffio.giovanni@enel.it
nelli.maurizio@enel.it
giordano.tanzini@enel.it
stefano.santini@enel.it
giacomo.petretto@enel.it
sandra.scalari@enel.it
eugenio.dimarino@enel.it
adamo@enel.it
christian.noce@enel.it
brunello.botte@enel.it
vincenzo.cannatelli@enel.it
sergio.rogai@enel.it
chimento.giuseppe@enel.it
marco.paci@enel.it
carlo.zamparelli@enel.it
luca.dellicarpini@enel.it
.paulon@enel.it
gianluca.sapienza@enel.it

TOOL used:

Phonebook

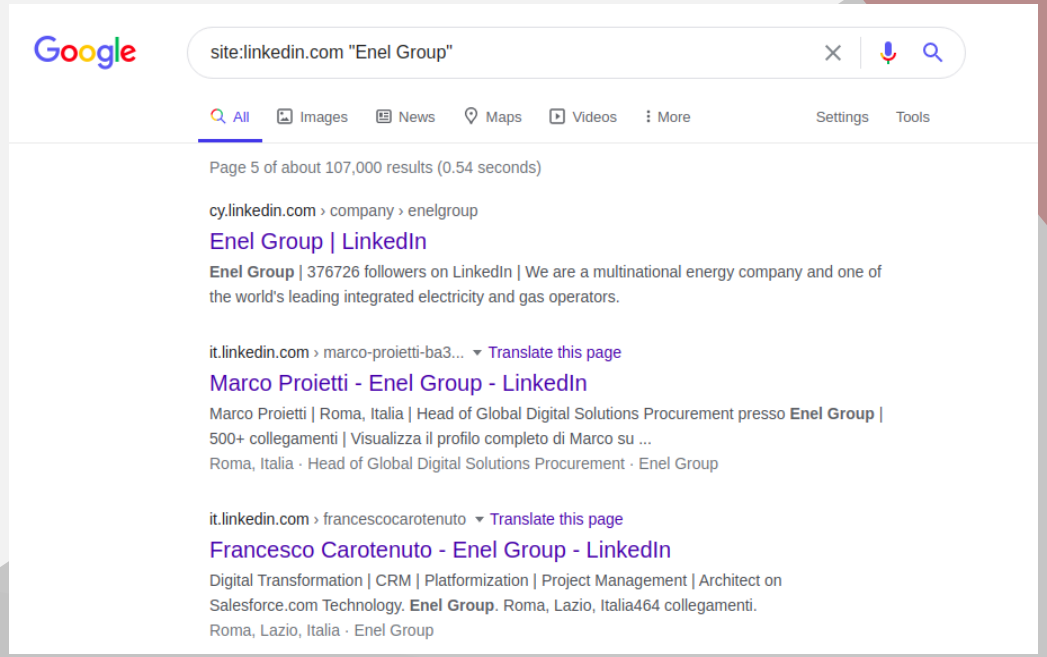
(https://phonebook.cz/)

Email accounts



TOOL used: CrossLinked
(https://github.com/m8r0wn/CrossLinked)

```
$ python3 crosslinked.py -f '{first}.{last}@enel.it' -s -j 1 -t 50 Enel Group
[*] Searching google for valid employee names at Enel
[*] 0 : https://www.google.com/search?q=site:linkedin.com/in+"Enel"&num=100&start=0
[*] 99 : https://www.google.com/search?q=site:linkedin.com/in+"Enel"&num=100&start=166
[*] 199 : https://www.google.com/search?q=site:linkedin.com/in+"Enel"&num=100&start=321
[*] Searching bing for valid employee names at Enel
[*] 0 : https://www.bing.com/search?q=site:linkedin.com/in+"Enel"&first=0
[*] 6 : https://www.bing.com/search?q=site:linkedin.com/in+"Enel"&first=37
[*] 14 : https://www.bing.com/search?q=site:linkedin.com/in+"Enel"&first=71
[*] 22 : https://www.bing.com/search?q=site:linkedin.com/in+"Enel"&first=103
[*] 25 : https://www.bing.com/search?q=site:linkedin.com/in+"Enel"&first=138
[*] 32 : https://www.bing.com/search?q=site:linkedin.com/in+"Enel"&first=173
[+] names.txt complete, 228 unique names found!
```



Public Vulnerability Disclosures

OpenBugBounty.org > OBB-650072

flume.de Cross Site Scripting vulnerability | OBB-650072

Security Researcher **metamorfosec**, a holder of 9 badges for responsible and coordinated disclosure, found a security vulnerability affecting **flume.de** website and its users.

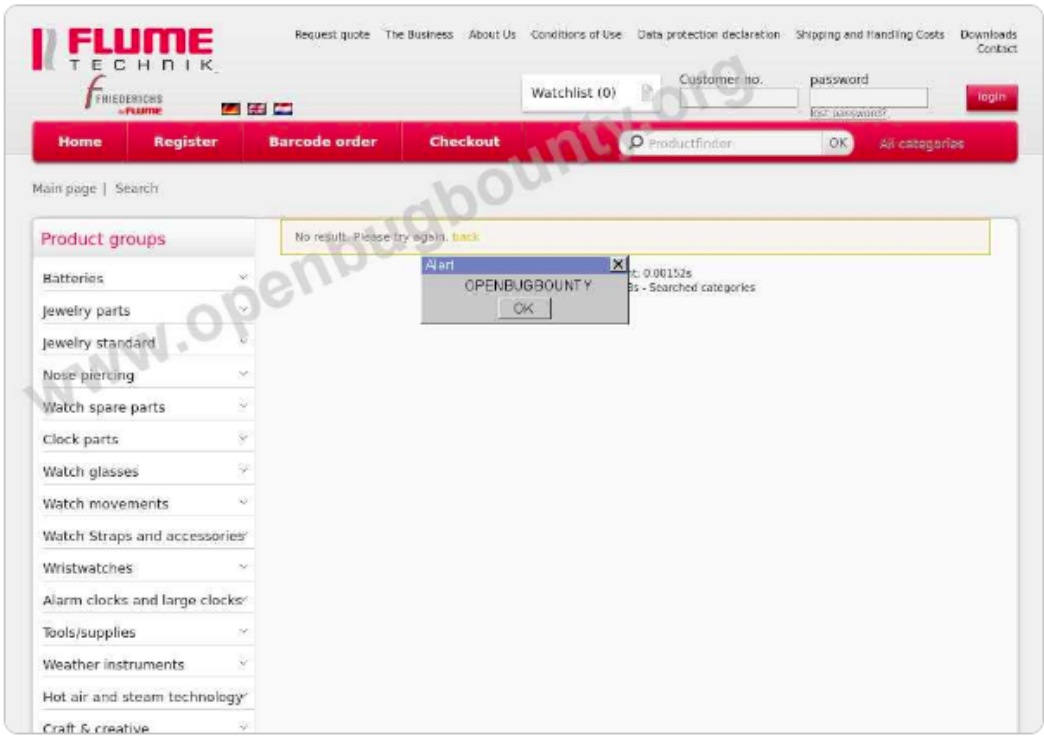
Following coordinated and responsible vulnerability disclosure guidelines of the **ISO 29147** standard, Open Bug Bounty has:

a. verified the vulnerability and confirmed its existence;
b. notified the website operator about its existence.

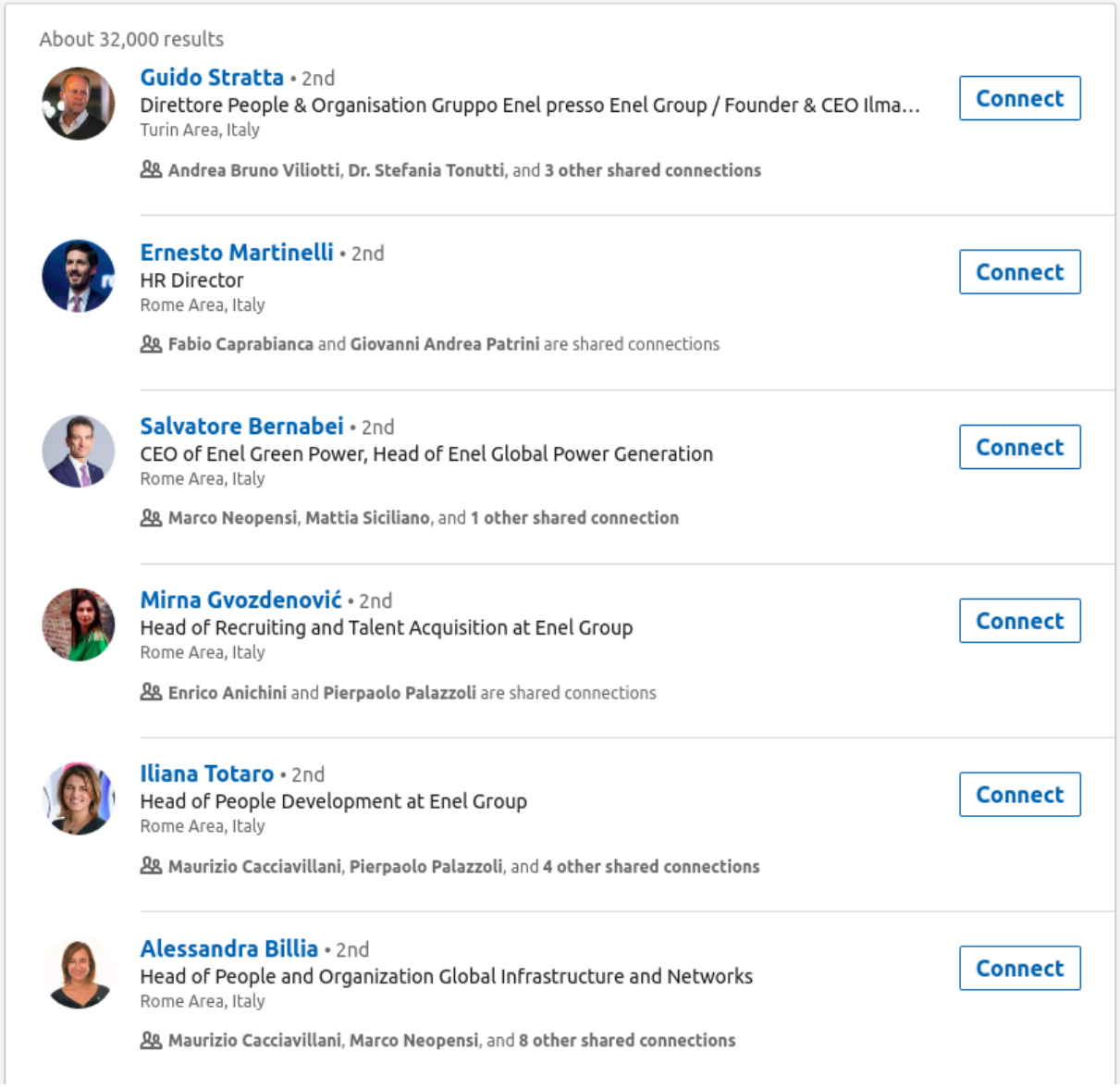
Affected Website:	**flume.de**
Open Bug Bounty Program:	**Create your bounty program now**. It's open and free.
Vulnerable Application:	Custom Code
Vulnerability Type:	**XSS (Cross Site Scripting)** / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Disclosure Standard:	Coordinated Disclosure based on **ISO 29147** guidelines
Discovered and Reported by:	**metamorfosec**
Remediation Guide:	**OWASP XSS Prevention Cheat Sheet**
Export Vulnerability Data:	Bugzilla Vulnerability Data JIRA Vulnerability Data [Configuration] Mantis Vulnerability Data Splunk Vulnerability Data XML Vulnerability Data [XSD]

TOOL used: openbugbounty (https://www.openbugbounty.org/)

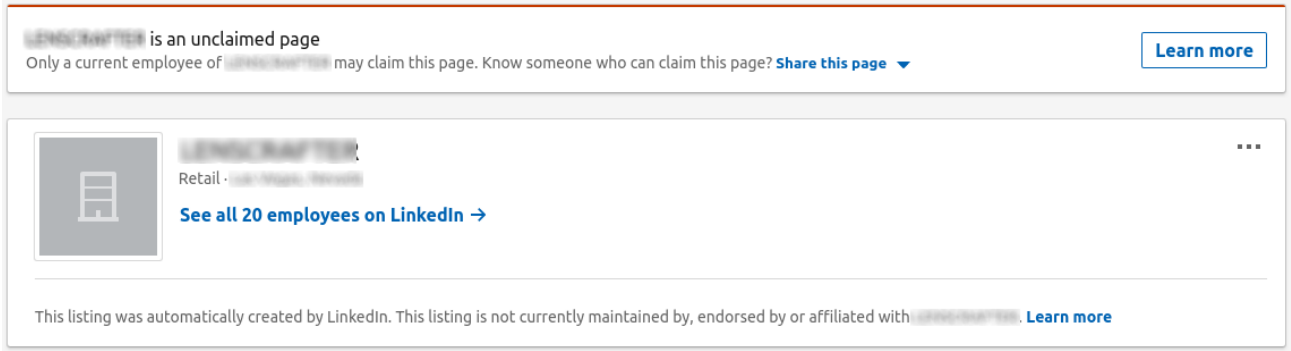
Screenshot:



Social Networks

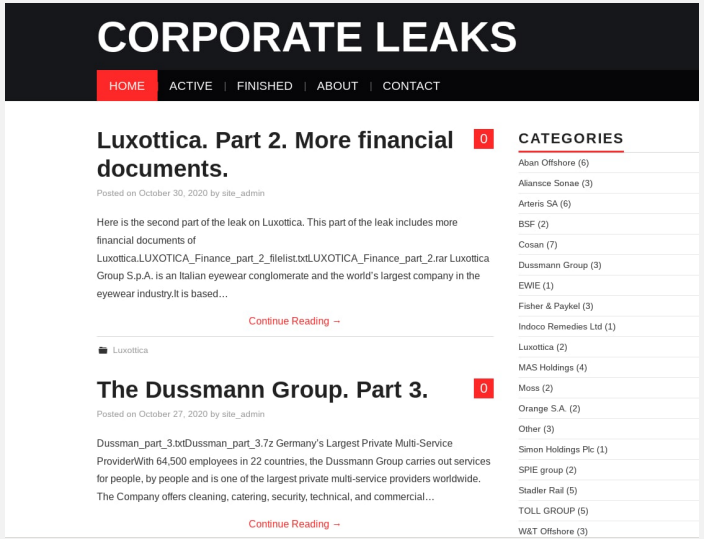


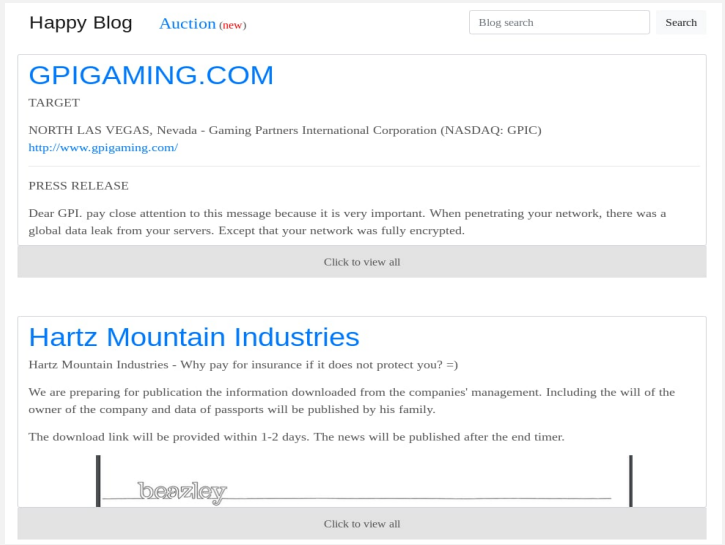
TOOL used: various social networks

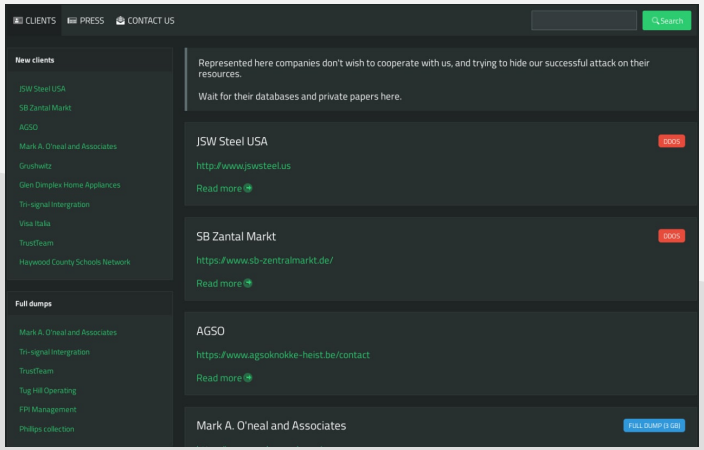


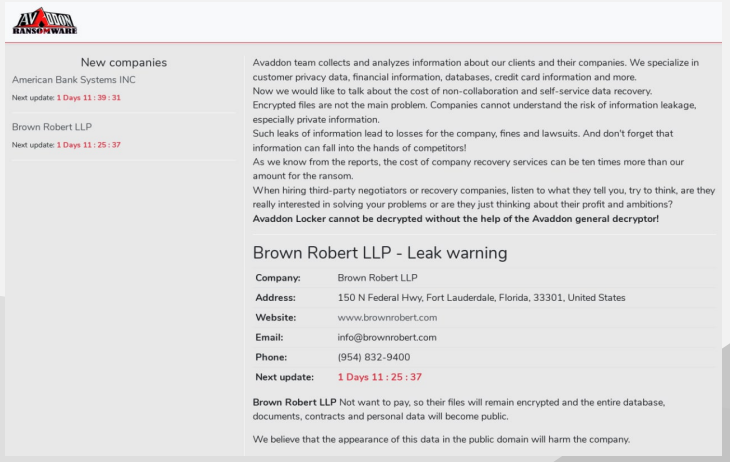
Deep & Dark Web

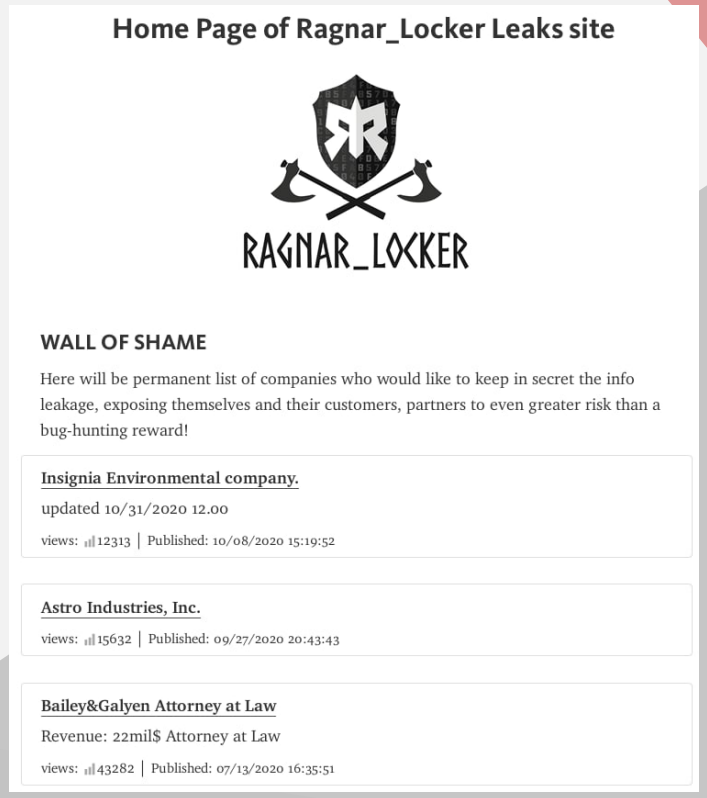
TOOL used: various cyber criminals group sites











Deep & Dark Web

Forums › Leaks › Databases › **Forum Announcement**

Mark all as read | Today's posts

Forum Announcement: Database Index [CLICK ME]

[Owner] Omnipotent

Supreme Leader

Posts 2,515
Threads 152
Joined Mar 2015

5 YEARS OF SERVICE '15

January 01, 2015 at 12:00 PM

This thread will index all the datasets we have marked as `Official` meaning they are verified by an admin and kept online 24/7/365 via our CDN.
Please note there are thousands more unofficial datasets in the Databases subforum.
This list is neither in alphabetical order neither is it only limited to database breaches, you will find some combolists here too.

Lifetime Access

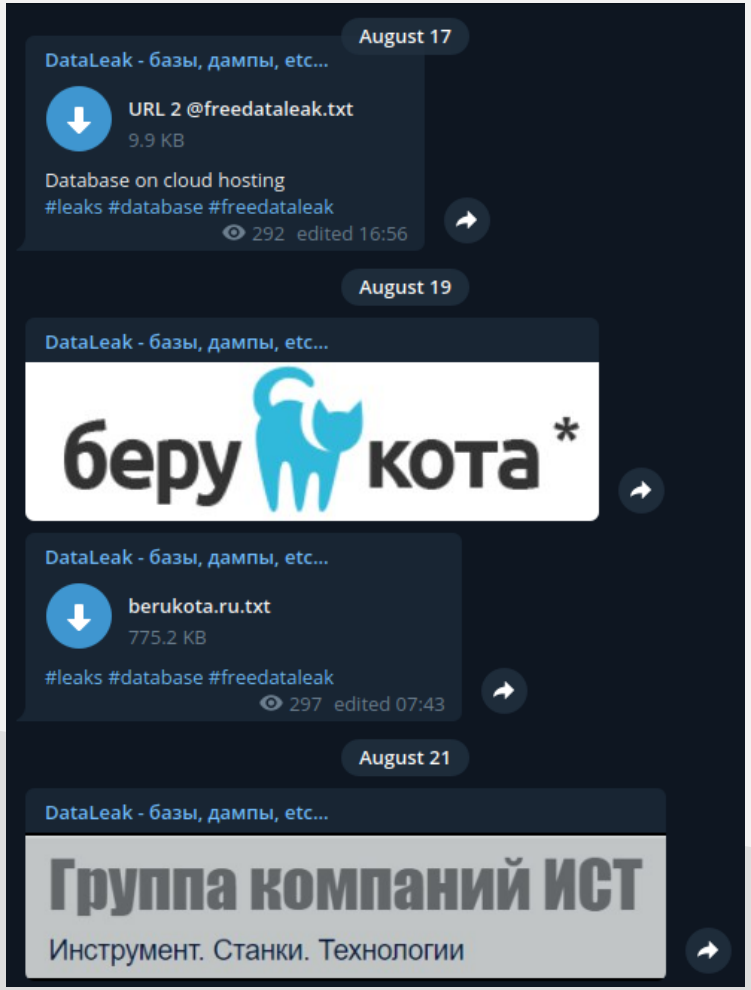
Click here to learn how to get credits.
Click here to view some basic rules.

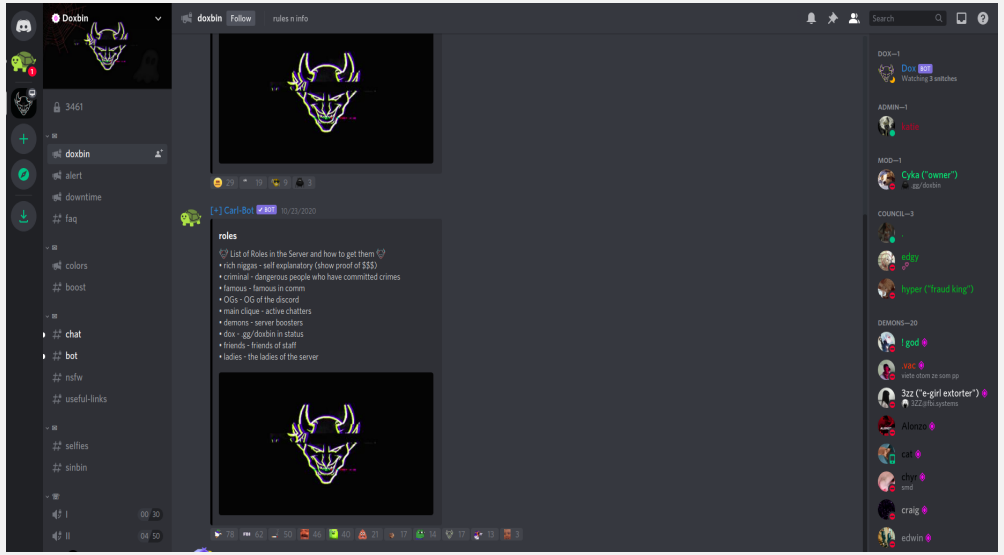
We have a total of 9,079,375,118 Records from the following 468 Datasets, free for download once you unlock them.

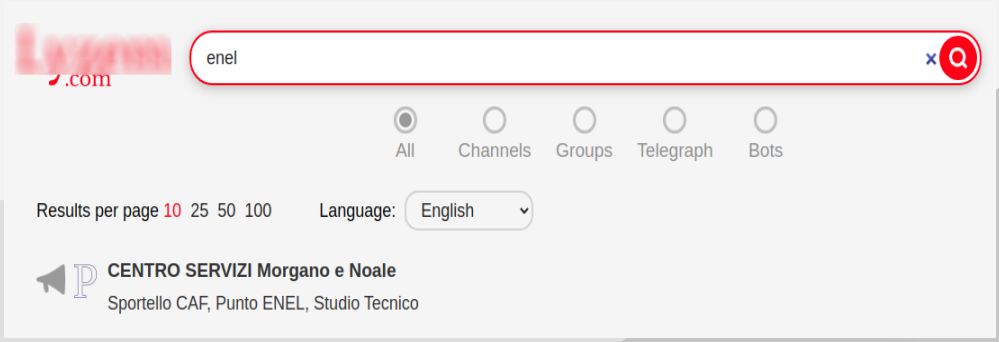
[999,999,999 Records] | 2019 - *(Collection)* Multiple Collections (1 to 5 + AntiPublic + Zabugor + Myrq) ➡ Download Here! * Download provided via Torrent
[013,545,468 Records] | 2015 - *(000webhost.com)* 000Webhost Database ➡ Download Here!
[000,018,965 Records] | 2013 - *(1337-crew.to)* 1337 Crew Database ➡ Download Here!
[000,000,586 Records] | 2014 - *(143vpn.com)* 143VPN Database ➡ Download Here!
[009,072,977 Records] | 2011 - *(178.com)* 178 Database ➡ Download Here!
[028,052,322 Records] | 2016 - *(17.media)* 17.Media (17 直播) Database ➡ Download Here!
[014,928,048 Records] | 2011 - *(7k7k.com)* 7k7k Database ➡ Download Here!
[000,782,609 Records] | 2016 - *(abandonia.com)* Abandonia Database ➡ Download Here!
[000,432,943 Records] | 2014 - *(acne.org)* Acne Database ➡ Download Here!
[152,445,165 Records] | 2013 - *(adobe.com)* Adobe Database ➡ Download Here!
[003,867,997 Records] | 2015 - *(adultfriendfinder.com)* Adult Friend Finder Database ➡ Download Here!
[000,166,380 Records] | 2014 - *(aimjunkies.com)* Aim Junkies Database ➡ Download Here!
[000,132,788 Records] | 2015 - *(alabama.gov)* Alabama Voter Database ➡ Download Here!

TOOL used: various data leak & data trading forums

Deep & Dark Web







TOOL used: various Telegram & Discord channels

EXPOSURE ASSESSMENT

One Time | SaaS | SaaS & Managed

EXPOSURE ASSESSMENT | One Time

WHAT

- ☑ Verification of exposed resources (OSINT)
- ☑ Reproduction of the attacker's point of view
- ☑ Reconnaissance phase simulation
- ☑ Mitigation and remediation actions

© Würth Phoenix

EXPOSURE ASSESSMENT | One Time

HOW

- ☑ Company inputs collection — Domain | Keywords
- ☑ Objects collection — Hostnames | IP addresses | Account e-mail
- ☑ Research of weaknesses
- ☑ Research of correlations
- ☑ Creation of a detailed report
- ☑ Report presentation (remotely)

EXPOSURE ASSESSMENT | SaaS

HOW

- ☑ Company inputs collection — Domain(s) | keywords
- ☑ Continuous objects collection — Hostnames | IP address | Account e-mail
- ☑ Research of weaknesses
- ☑ Research of correlations
- ☑ **Autonomous** use of SATAYO Portal — Graphs | Reports | Stats | Notifications
- ☑ API for Monitoring platforms — NetEye
- ☑ Notification via Telegram and e-mail
- ☑ Monthly report generation

EXPOSURE ASSESSMENT | SaaS & Managed

HOW

- ☑ Company inputs collection — Domain(s) | keywords
- ☑ **Continuous** objects collection — Hostnames | IP address | Account e-mail
- ☑ Research of weaknesses
- ☑ Correlations of weaknesses
- ☑ **Joinly use** of SATAYO Web Portal — Graphs | Reports | Stats | Notifications
- ☑ API for Monitoring platform — NetEye
- ☑ **Analysis** and **solution** proposal — Ticket | Phone call | E-mail
- ☑ Monthly report generation

www.wuerth-phoenix.com

Q&A