HACKINBO®
Spring 2018 Edition

DETECTING PHISHING FROM pDNS

HackInBo, May 26th, Bologna, Italy

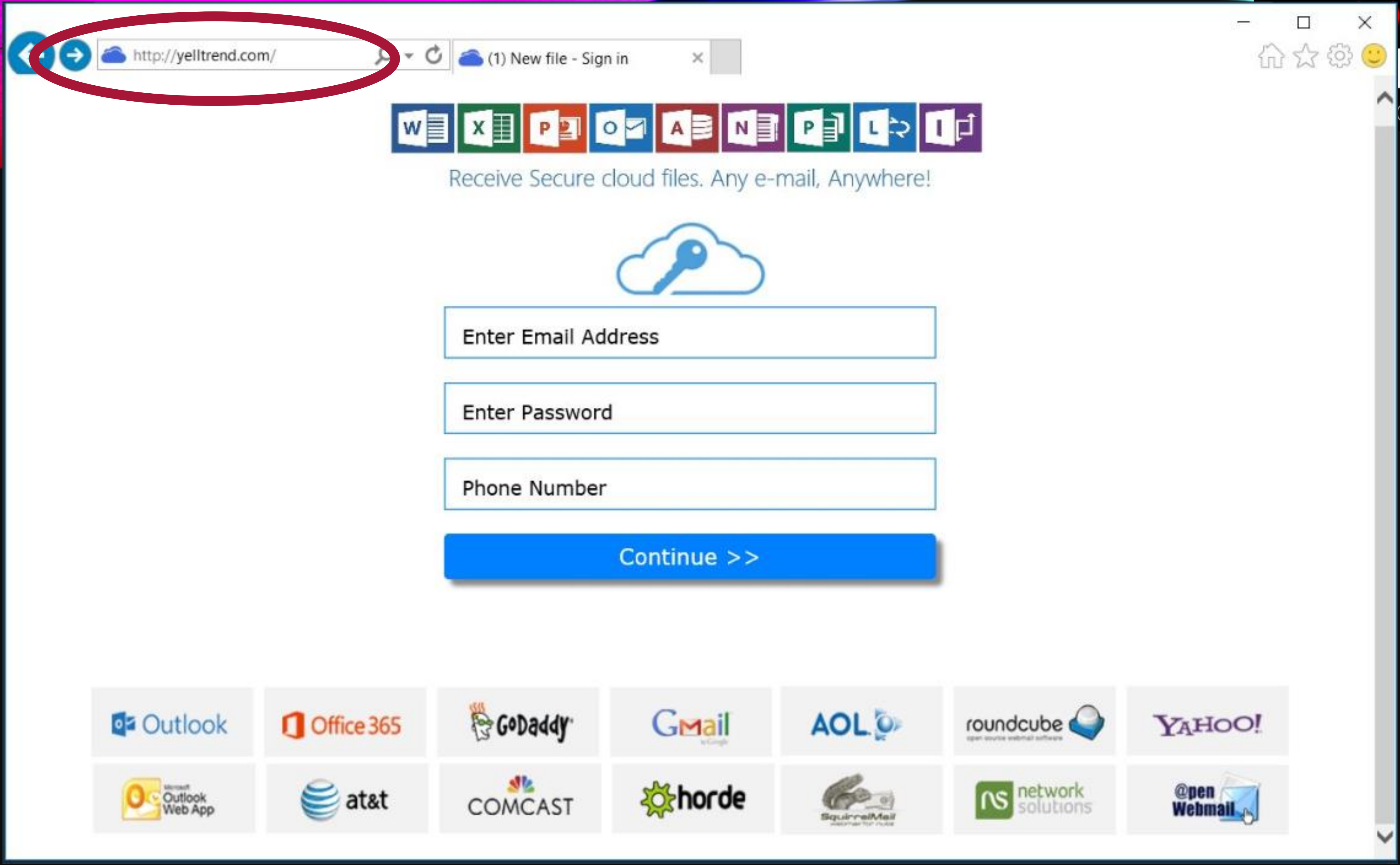
WHO AM I

- Founder of damsky.tech CTI research, training and consulting
- Ex IDF, Served in the intelligence forces, Captain in reserve
- MSc Computer science
- Participant of multiple intelligence sharing groups
- Twitter: @DamskyIrena
- LinkedIn: www.linkedin.com/in/irenadam/

PHISHING

> “*Phishing - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.*”

From dictionary.com



http://yelltrend.com/

(1) New file - Sign in

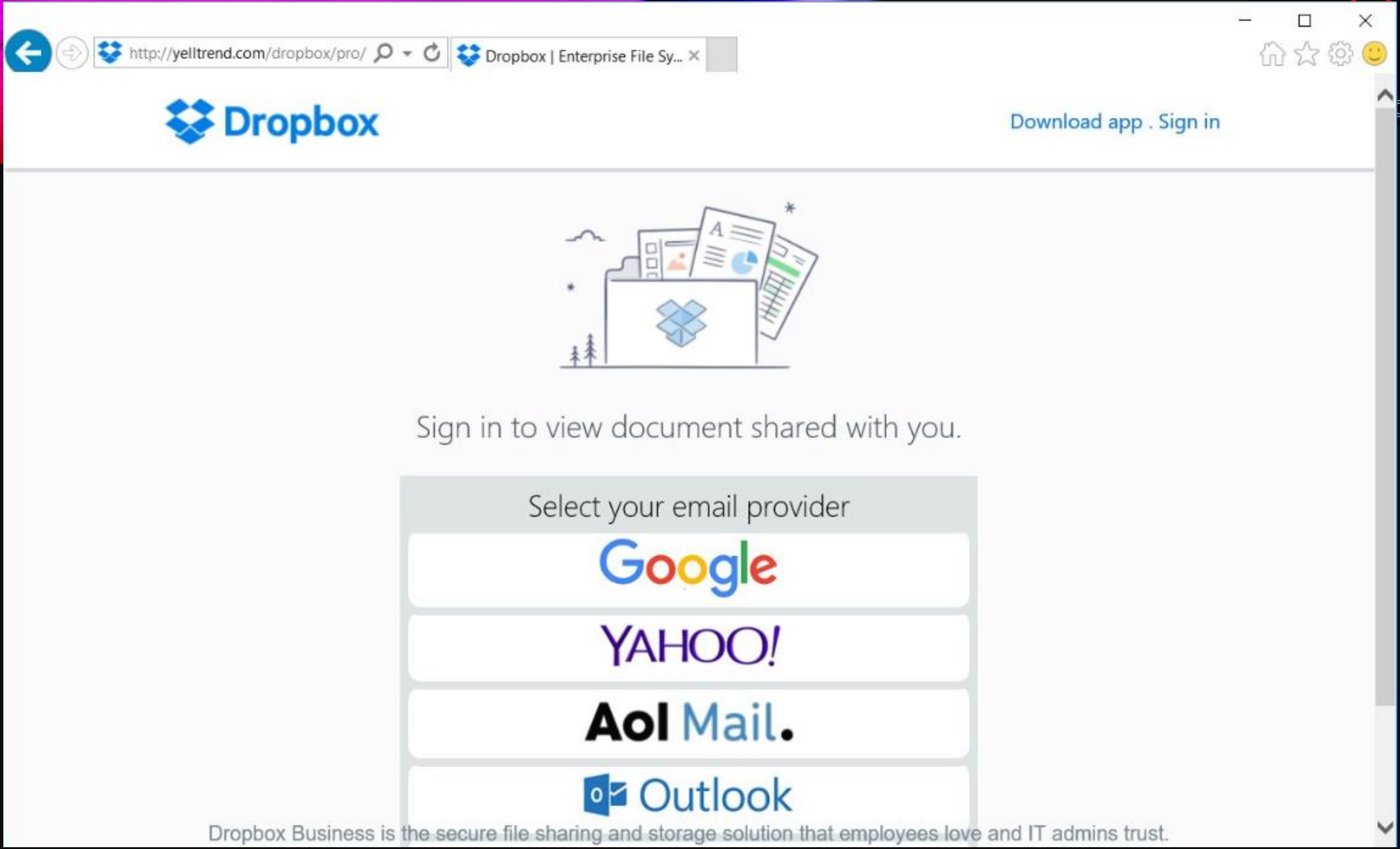
Receive Secure cloud files. Any e-mail, Anywhere!

Enter Email Address

Enter Password

Phone Number

Continue >>



http://yelltrend.com/dropbox/pro/

Dropbox | Enterprise File Sy...

Dropbox

Download app . Sign in

Sign in to view document shared with you.

Select your email provider

Dropbox Business is the secure file sharing and storage solution that employees love and IT admins trust.

DNS

WHAT IS DNS?

- Domain Name System (not Domain Name Server)
- Distributed database mainly used to translate domains to IPs
- Why? Cause it makes life easy (easier)
- First RFC 882, 883 published in November 1983 by Paul Mockapetris
  - Updated by RFC 1034, 1035 (1987)
  - Updated by RFC 7719 (2015)
- (Mainly) Port 53 traffic over UDP

WHAT CAN I DO WITH DNS?

- Assign friendly names to sites or machines
- Create (commercial) online presence
- Buy, sell, auction domain names

- Share (sell) the data with my company, friends, government and your adversaries

- Can use the data to analyze it and build products

SOME DEFINITIONS

www.example.com → Fully Qualified Domain Name == FQDN.

These are globally unique in the public DNS

And each part of the FQDN? www.example.com.

www.example.com == www.eample.com. → Usually ignore root server at .

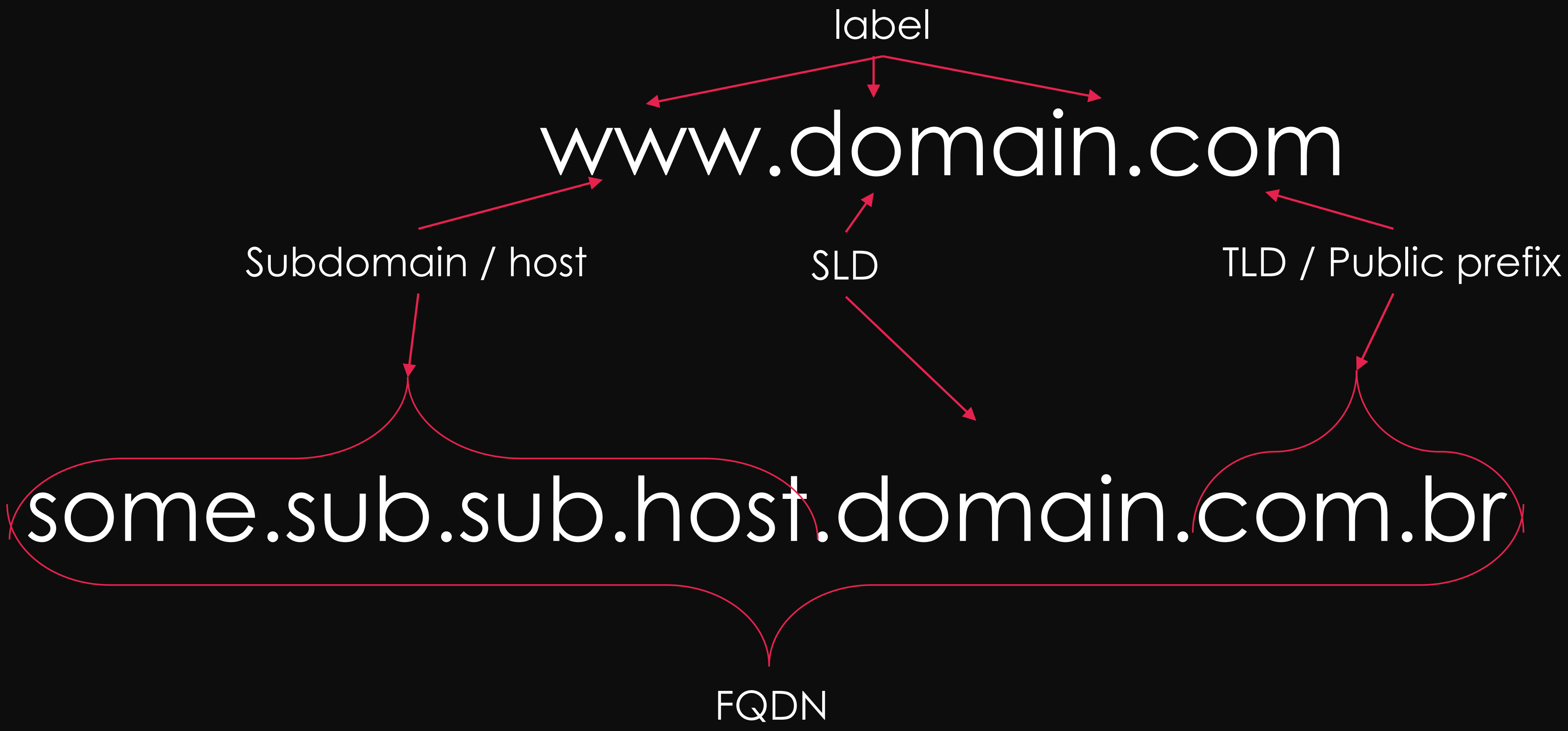
com. → the Top Level Domain (TLD) part

example.com. → Second Level Domain (SLD)

www.example.com. → 3rd level domain (and so on…)

WHAT IS A DOMAIN

- A domain is a collection of labels separated by dots



label

www.domain.com

Subdomain / host

SLD

TLD / Public prefix

some.sub.sub.host.domain.com.br

FQDN

SAY MY (DOMAIN) NAME

- As a domain name, any 8-bit value is valid
- For a host name, see IETF RFC 1123
  - [0-9a-zA-Z-]
  - underscore not strictly allowed, but often used
- On-wire max domain name length is 255 octets
  - max label length is 63 octets
- Some second-level domains behave like TLDs
  - e.g. co.uk.
  - related: http://publicsuffix.org/
- IDN strings begin with `XN--`

TOP LEVEL DOMAINS (TLDS)

gTLD – Generic TLDs

.com .org .net

ccTLDs – Country-Code TLDs

.nl .pl .cc

New gTLDs

.tech .paypal .moscow

IDN – Internationalized Domain Names

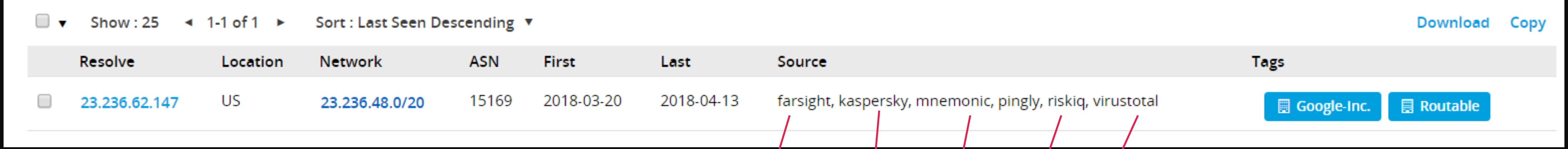
.香港 (Hong Kong) مصر (Egypt)

PASSIVE DNS (pDNS)

pDNS

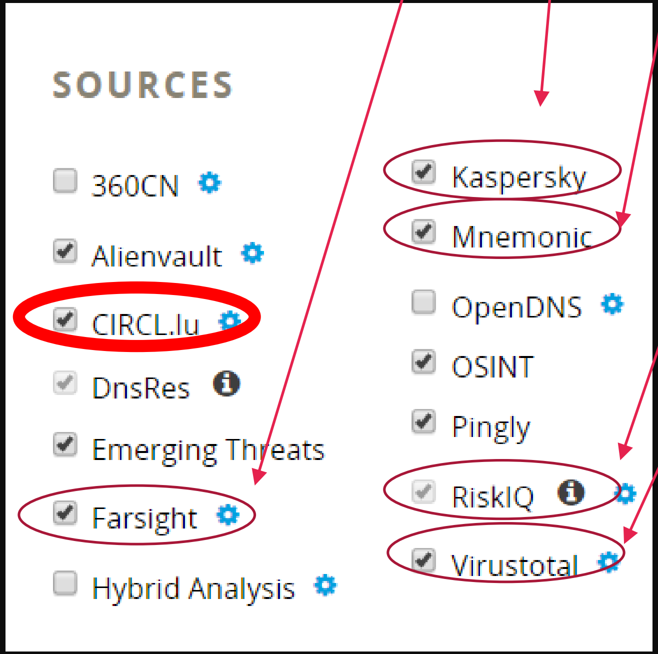
- Invented in 2004 by Florian Weimer
- Historical DB of DNS resolutions
- Collected using multiple sensors on the internet.
- Passively collected – no active resolutions are made
  - Only Cache misses are collected
- Data changes based on the DB!

DIFFERENT DB – DIFFERENT RESULTS



☐ ▾ Show : 25 ◂ 1-1 of 1 ▸ Sort : Last Seen Descending ▾ Download Copy

	Resolve	Location	Network	ASN	First	Last	Source	Tags
☐	23.236.62.147	US	23.236.48.0/20	15169	2018-03-20	2018-04-13	farsight, kaspersky, mnemonic, pingly, riskiq, virustotal	Google-Inc. Routable



SOURCES

- ☐ 360CN
- ☑ Alienvault
- ☑ CIRCL.lu
- ☑ DnsRes
- ☑ Emerging Threats
- ☑ Farsight
- ☐ Hybrid Analysis
- ☑ Kaspersky
- ☑ Mnemonic
- ☐ OpenDNS
- ☑ OSINT
- ☑ Pingly
- ☑ RiskIQ
- ☑ Virustotal

WAYS OF COLLECTING pDNS

Using sensors

- [Usually] Placed above a recursive resolver – user is anonymized
- Only cache misses are collected
- Only live traffic is collected – if no one accessed this domain it will not be noted
- First time – time of first (noted) activity

Using scraping zone files

- Not connected to user traffic
- Only on when the zones are published
- Sometimes domains that have been mapped but never accessed will be noted
- Not all registered domains will be noted
- First seen – time of mapping

WHERE CAN YOU GET pDNS?

FARSIGHT SECURITY	RISKIQ	Netlab 360.com
CIRCL Passive DNS	BFK	VirusTotal Inside VirusTotal's back pocket
mnemonic	SPAMHAUS	

BUT WHAT IF I WANT MY OWN pDNS?

- Create your own
    - Analyze
        - DNS Servers
        - Port 53 traffic (also 5353, 5003)
    - Store in DB
        - (domain, IP)
        - Minimum meta data
            - First seen
            - Last seen
        - Additional meta data
            - Number of times seen - forever
            - Number of times seen last X days
            - What Server provided the resolution
            - Where (GEO) the query was made from

SYMPTOMS OF PHISHING

SYMPTOMS OF PHISHING

- Multiple sub labels
- Repetitive labels
- Suspicious TLDs
- Hyphenated TLDs ?
- DNS twists
  - (including) Typosquatters
- Mixture of scripts

EXAMPLE / ANALYSIS SET

- Queried DNSDB (by Farsight) for
  - microsoft.*
- Limited data set for the past 24 hours
- 7495 domains

SYMPTOMS OF PHISHING

- Multiple sub labels
  - More than 2 hosts is suspicious
  - More than 5 hosts is likely
  - More than 10 - *I* never seen it not to be phishing

  - Need to whitelist certain services
    - whoisbucket.com microsoft.co.il.whoisbucket.com. ← legitimate

SYMPTOMS OF PHISHING

- Multiple sub labels
- Repetitive labels

microsoft.com.error.bluescreen.critical-error.dont.touch.your.computer.its.may.ge.t.crash. \
microsoft.com.error.bluescreen.critical-error.dont.touch.your.computer.its.may.ge.t.crash. \
18545484145.18548158.df51d5xyz.pcwarning.us.

microsoft.asp.dot.net.coding.strategies.with.the.microsoft.asp.dot.net.team.

microsoft.com.zzzzzzzzzzzzzzzzzzzzzz.is.a.great.company.itrebal.com.w3snoop.com.

SYMPTOMS OF PHISHING

- Multiple sub labels
- Repetitive labels
- Suspicious TLDs
  - New TLDs are highly prone to phishing
    - They will get a likely score
  - Some ccTLDs are prone to phishing:
    - For example
      - ru
      - pw
      - in
      - cc
      - ly
    - They will get a suspicious score

TLD	Count
com	3687
net	515
ru	429
org	172
xyz	163
download	138
review	136
bid	111
info	107
science	105
trade	103
stream	89
win	89
us	82
loan	69
date	64
accountant	59
faith	59
racing	54
men	52

microsoft.com.0ssncn0besla7seq.review.
microsoft.com.1gavvtmuqcta.review.
microsoft.com.2fjf44ba7lkbs3vbnj9ma.review.
microsoft.com.2oqlyv3kxh5s8l2shye.review.
microsoft.com.3ld23rtpy6u2hqw2yg.review.
microsoft.com.4ehzbsm5iemwl8bopeqnxhrx.review.
microsoft.com.4gmmtxbsddizyrunybhp1p4.review.
microsoft.com.4ldfiwj6k09r4p0p.review.
microsoft.com.5zlcvzvo7gtbat6tuoh5ig.review.
microsoft.com.6fumbjai6erd.review.
microsoft.com.6o4aoqk3qcehq0sc6fm.review.
microsoft.com.92ewhwtpnkhz.review.
microsoft.com.achieve-new-smartphones.review.

SYMPTOMS OF PHISHING

- Multiple sub labels
- Repetitive labels
- Suspicious TLDs
- Hyphenated TLDs ?

microsoft.com.de-flu9.hklmckelqf.loan.
microsoft.com.nz-now2.pick-your-gadget-reward.cricket.
microsoft.com.it-cob3.vincitore-selezionato-2017.loan.

And my favorite –
microsoft.com-maliciousattack.info.

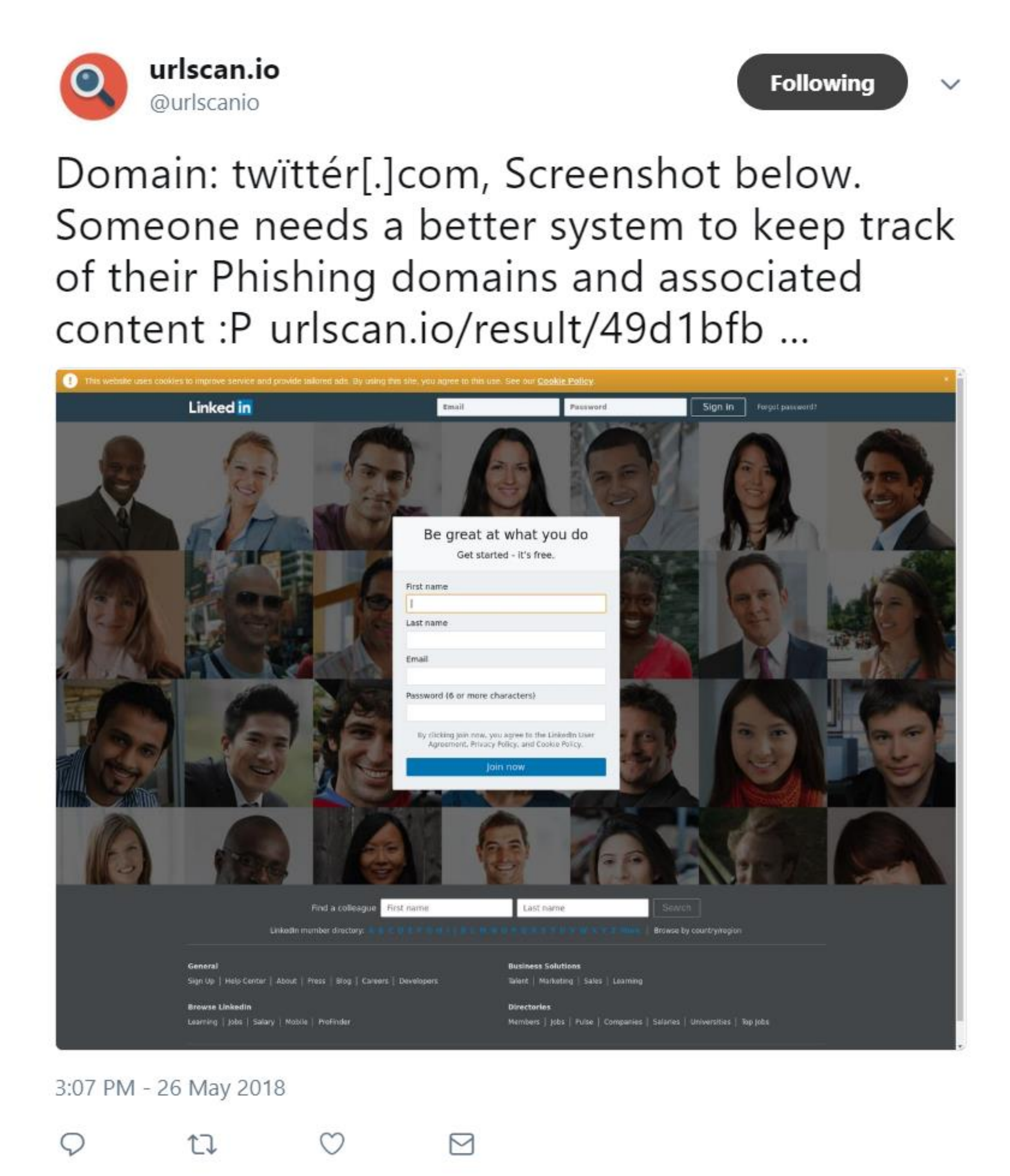
SYMPTOMS OF PHISHING

- Multiple sub labels
- Repetitive labels
- Suspicious TLDs
- Hyphenated TLDs ?
- DNS twists
  - (including) Typosquatters

- https://github.com/elceef/dnstwist

- https://dnstwister.report

  - rn→m
  - cl→d
  - cj→g
  - ci→a
  - vv→w
  - 1→l,I
  - l→i
  - 0→o



urlscan.io
@urlscanio

Domain: twïttér[.]com, Screenshot below. Someone needs a better system to keep track of their Phishing domains and associated content :P urlscan.io/result/49d1bfb ...

This website uses cookies to improve service and provide tailored ads. By using this site, you agree to this use. See our Cookie Policy.

Be great at what you do

Get started - it's free.

By clicking Join now, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.

General
Sign Up | Help Center | About | Press | Blog | Careers | Developers

Business Solutions
Talent | Marketing | Sales | Learning

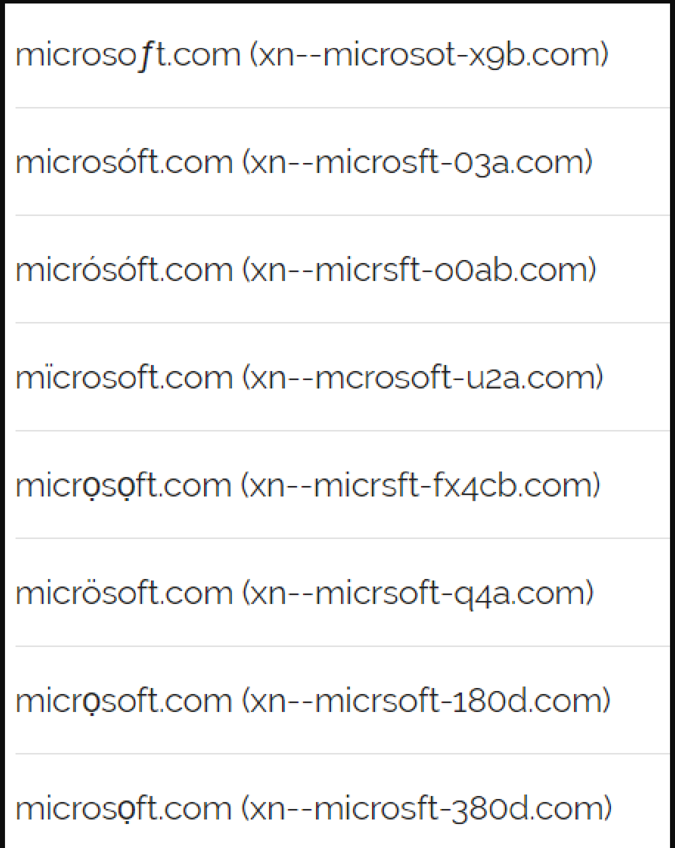
Browse LinkedIn
Learning | Jobs | Salary | Mobile | ProFinder

Directories
Members | Jobs | Pulse | Companies | Salaries | Universities | Top Jobs

3:07 PM - 26 May 2018

SYMPTOMS OF PHISHING

- Multiple labels
- Repetitive labels
- Suspicious TLDs
- Hyphenated TLDs ?
- DNS twists
  - (including) Typosquatters
- Mixture of scripts



microsoƒt.com (xn--microsot-x9b.com)

microsóft.com (xn--microsft-03a.com)

micrósóft.com (xn--micrsft-o0ab.com)

mïcrosoft.com (xn--mcrosoft-u2a.com)

micrọsọft.com (xn--micrsft-fx4cb.com)

micrösoft.com (xn--micrsoft-q4a.com)

micrọsoft.com (xn--micrsoft-180d.com)

microsọft.com (xn--microsft-380d.com)

SCORING

- Building a rule based scoring system
  - 10 points to suspicious
  - 20 points to likely
  - 50 points to “no way this is phishing”

- Sum different feature scores

- Analyze the results to look for false positives , adjust the scoring engine
- Add white lists

FUTURE WORK

- Implementing ML scoring
- Clustering of results and analyzing the underlying clusters
  - Follow up on IPs / ASNs / IP neighborhoods
  - Follow up on NSs
  - Follow up on whois?
- What will we see when we analyze the content of the pages themselves?
- Can we find who is behind the phishing based on pDNS characteristics?
- Can the phishing kit be recognized only from the (p)DNS data?

QUESTIONS?

Grazie!