La facilité de pirater une entreprise

D’une recherche Google à une brèche complète!

Patrick Mathieu, Hackfest.ca

Novembre 2020

NOVIPRO

FlickR CC: charlie-wales

Qui suis-je?

Bonjour!

Patrick Mathieu

- Hacker depuis 20+ ans
- Senior Offensive Security Manager @ LogMeIn.com
- Co-fondateur de Hackfest.ca depuis 12 ans
- R&D / Hobby / Community / Medias / OSINT

Twitter: @pathetiq
LinkedIn: https://www.linkedin.com/in/patrickrmathieu/
Email: patrick@hackfest.ca

Hackfest: https://hackfest.ca
Podcast: https://securite.fm


Shameless plugs

Podcast international sur la sécurité et le hacking. Nouvelles et opinions du Québec et de l'Europe!

https://securite.fm

InfosecJobs

https://infosecjobs.ca


HACKFEST.ca
GET
INVOLVED
info@hackfest.ca

https://discord.gg/39fRfa6

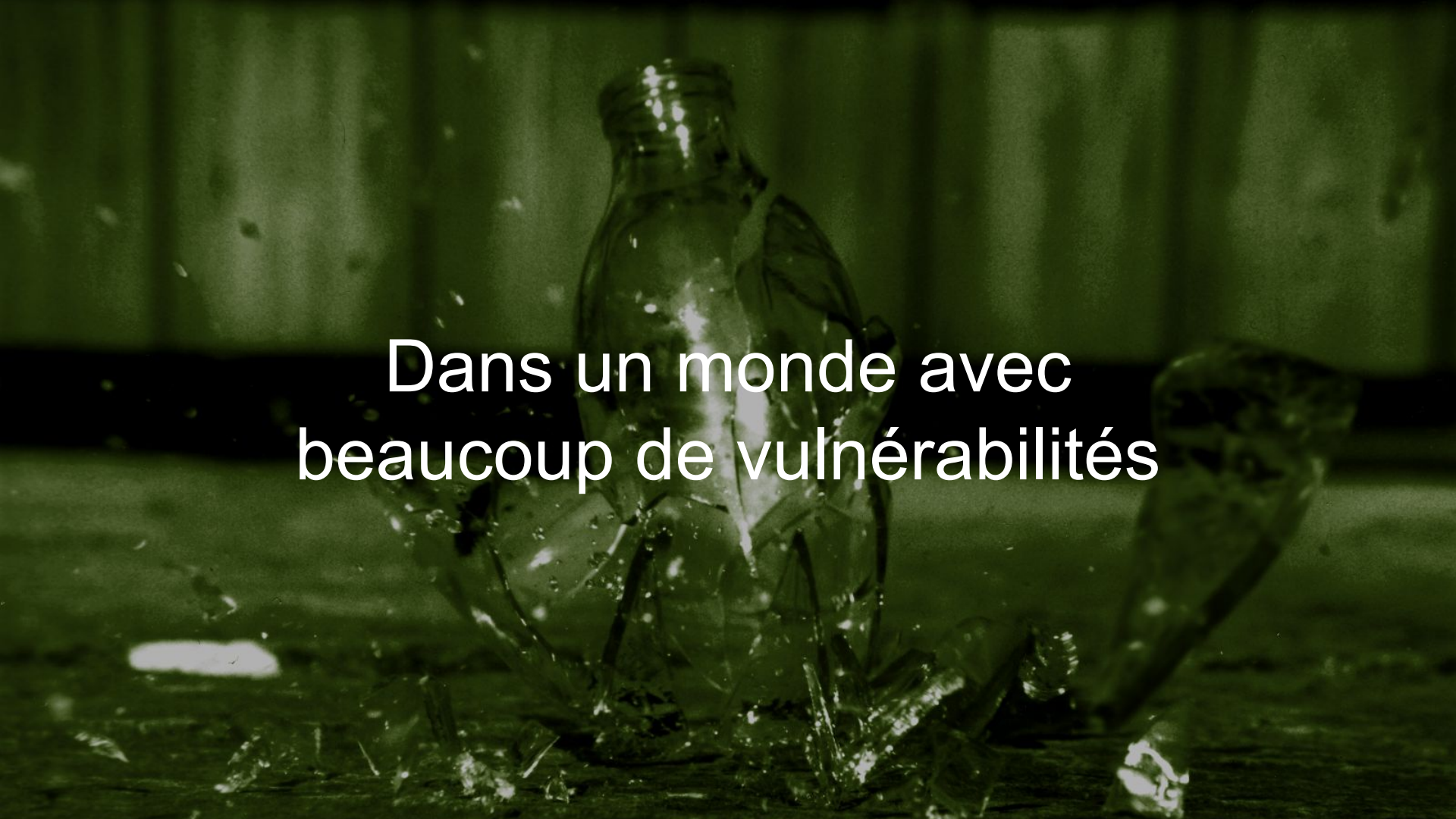
Parlons tout d’abord de hacking!


Pas ça!
HACKING IN PROGRESS


Ni ça!


Quelque chose comme ça!

Ou encore… ça …!


Dans un monde avec
beaucoup de vulnérabilités

Nous sommes tous à risque!

LONGUE LISTE DE VICTIMES

Des dizaines d'organisations publiqu
rançongiciels au cours de la dernièr

STM

En octobre, la Société de transport de M
se remettre d'une attaque perpétrée à
rançongiciel RansomExx.

Wendake

La Nation huronne-wendate a subi un
en ligne des dossiers d'élèves d'un cen

Ministère de la Justice du Québec

Des pirates ont réussi à voler des cour
maliciels à des citoyens l'ayant contact

Revenu Canada

Des fraudeurs ont attaqué les dossiers
mots de passe de 9041 utilisateurs en a

Inonotech-Execaire

La firme d'entretien d'aéronefs---- a ét
qui a publié les données volées en ligne

Dans la Rue

Vol de données massif à la Québec

Une enquête criminelle est en cours

La société de victime d'un

Le développeur de populaires franchises
l'attaque de se propager davantage à tr

Une attaque informatique cible d hôpitaux canadiens et américains

Le ministère de la Santé du Québec fait partie d
victimes de cette campagne agressive de dema
rançon.

Capital One : des données personnelles de 6 millions de Canadiens ont été volées

Plus de 3000 lecteurs de «L'actualité» piratés

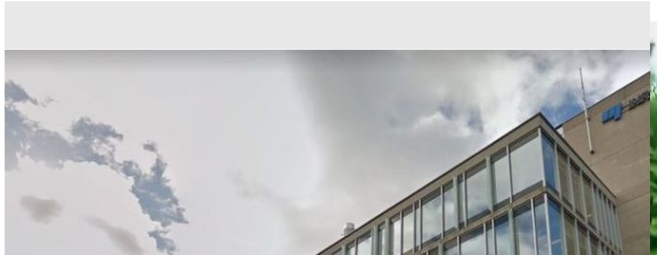
Arnaud Koenig Soutière | Le Journal de Québec | **Publié le 15 septembre 2019 à 23:03** - Mis à jour le 15 septembre 2019

Les renseignements personnels de 2,9 millions de membres Desjardins divulgués

TVA Nouvelles et Agence QMI | **Publié le 20 juin 2019 à 14:01** - Mis à jour le 20 juin 2019 à 15:16

L'INRS ciblé par des pirates informatiques

Martin Lavoie | Journal de Québec | **Publié le 19 juillet 2019 à 15:27** - Mis à jour le 19 juillet 2019 à 15:31



Un ancien employé de l'armée aurait commis une importante fraude à Valcartier

Bell Customer Info Breached In Hacking Attack

CP | By The Canadian Press
Posted: 02/02/2014 11:13 am EST | Updated: 02/02/2014 11:59 am EST

HACKING

The Statistics Canada Site Was Hacked By an Unknown Attack

Bar ouvert pour les vo

Une faille informatique aurait permis de localiser sans mot de Canadiens

Signage is displayed outside of a BCE Inc. Bell Canada store in Toronto, Ontario, Canada, on Wednesday, Aug. 8, 2012. BCE Inc., Canada?s second-largest wireless carrier, topped second-quarter profit estimates and increased its annual forecast after adding more smartphone subscribers on lucrative long-term contracts. Photographer: Brent Lewin/Bloomberg via Getty Images | Bloomberg via Getty Images

19 Share | 24 Tweet | 9 +1 | 3 Email | 0 Comment

GET CANADA BUSINESS NEWSLETTERS:
Enter email SUBSCRIBE

FOLLOW: Video, Bell Canada, Nullcrew Bell, Nullcrew Hack, Bell Nullcrew, Bell Canada Hack, Bell Hack, Bell Information Hacked, Cp, Nullcrew, Canada Business News

THE CANADIAN PRESS

TORONTO - Bell Canada says 22,400 of its small business customers have had their account information compromised by hackers.

Canadian Forces recruiting website hacked

Main landing page for would-be recruits redirects users to Chinese state-run website

By Murray Brewster, John Paul Tasker, CBC News Posted: Nov 17, 2016 3:19 PM ET | Last Updated: Nov 17, 2016 5:28 PM ET

40 Million Credit Card account massive data breach at 'Target' Black Friday

by **Swati Khandelwal** on Thursday, December 19, 2013

ICI COLOMBIE-BRITANNIQUE–YUKON
+ DE RÉGIONS

ACCUEIL | SOCIÉTÉ | ZONE YUKON

L'Agence du revenu perd la quasi-totalité de ses données sur les Yukonais

PUBLIÉ LE VENDREDI 3 FÉVRIER 2017

EXCLUSIF **Publié le 20 janvier 2017 à 05h00** | Mis à jour le 20 janvier 2017 à 06h18

Comment un escroc a volé 5,5 millions à La Coop fédérée

Québec victime d'un logiciel de rançon

17 à 07h15 | Mis à jour le 07 mars 2017 à 07h15

Revenu Québec victime d'un logi rançon

Revenu Québec a été victime d'un rançongiciel, ou «ransomware», le 6 décembre der

PHOTO ANDRÉ PICHETTE, ARCHIVES LA PRESSE

Dishwasher has directory traversal bug

Thanks a Miele-on for making everything dangerous, Internet of Things firmware slackers

Agenda (index.php)

- Qu’est-ce que la surface d’attaque
- Étapes d’une attaques
- OSINT (Open Source INTelligence)
- Les attaquants
- Vos risques
  - OSINT
  - No tech hacking
- Exemples de données découvertes
- Démo


Qu’est-ce que la surface d’attaque?

Le passé - Le périmètre


Aujourd’hui
c’est Zerotrust et les nuages


Étapes d’une attaque

OSINT
Open Source INTelligence


Les attaquants

Hackers

Bon ou méchant, ils sont présents

Script Kiddies

Connaissances de bases, ils appuient sur tous les boutons

Hacktivistes

Généralement des Scripts Kiddies avec une cause

State Sponsored

États-Unis, Europe, Russie, Chine, ...

Démo - Exemples

Surface d’attaque

Techniques de reconnaissances

- Subdomains
- Leaked Passwords
- Scans des serveurs
  - Et ses vulnérabilités
- Technology Stack
  - Et ses vulnérabilités
- Réseaux Sociaux
  - Users, technologies, etc.
- Activités physiques ou sociales

Subdomains

- Crt.sh
- Virustotal
- Securitytrails
- Linux tools
- ...

Leaked Passwords

- Hacking forums
- Darkweb
- Have I Been Pwned? (et services similaires)
- Pastebin
- ...

Scans des serveurs

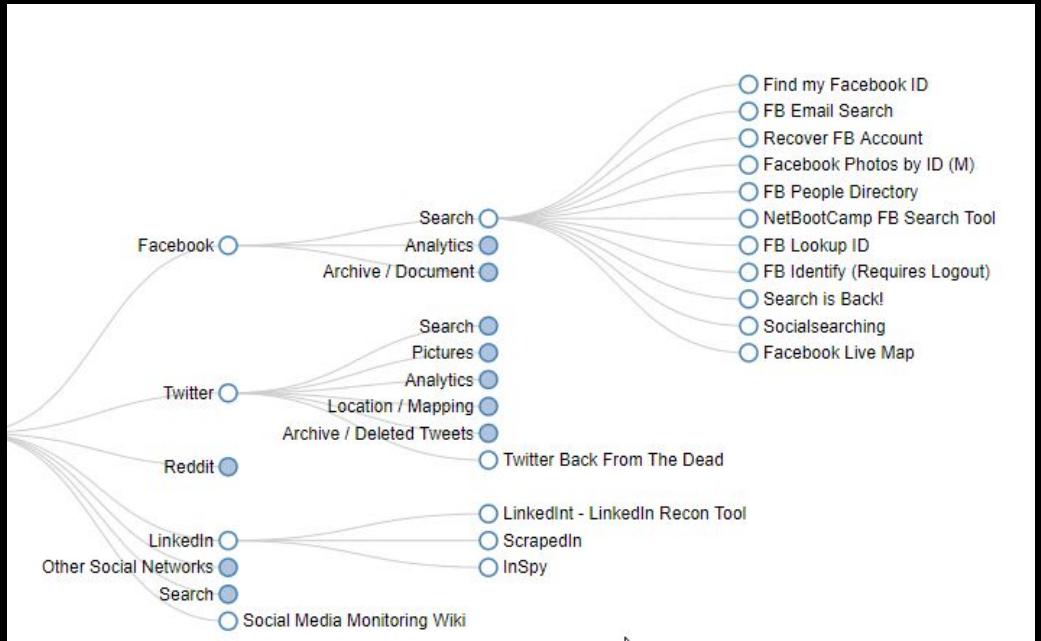
- Nmap
- Masscan
- Shodan.io
- ...

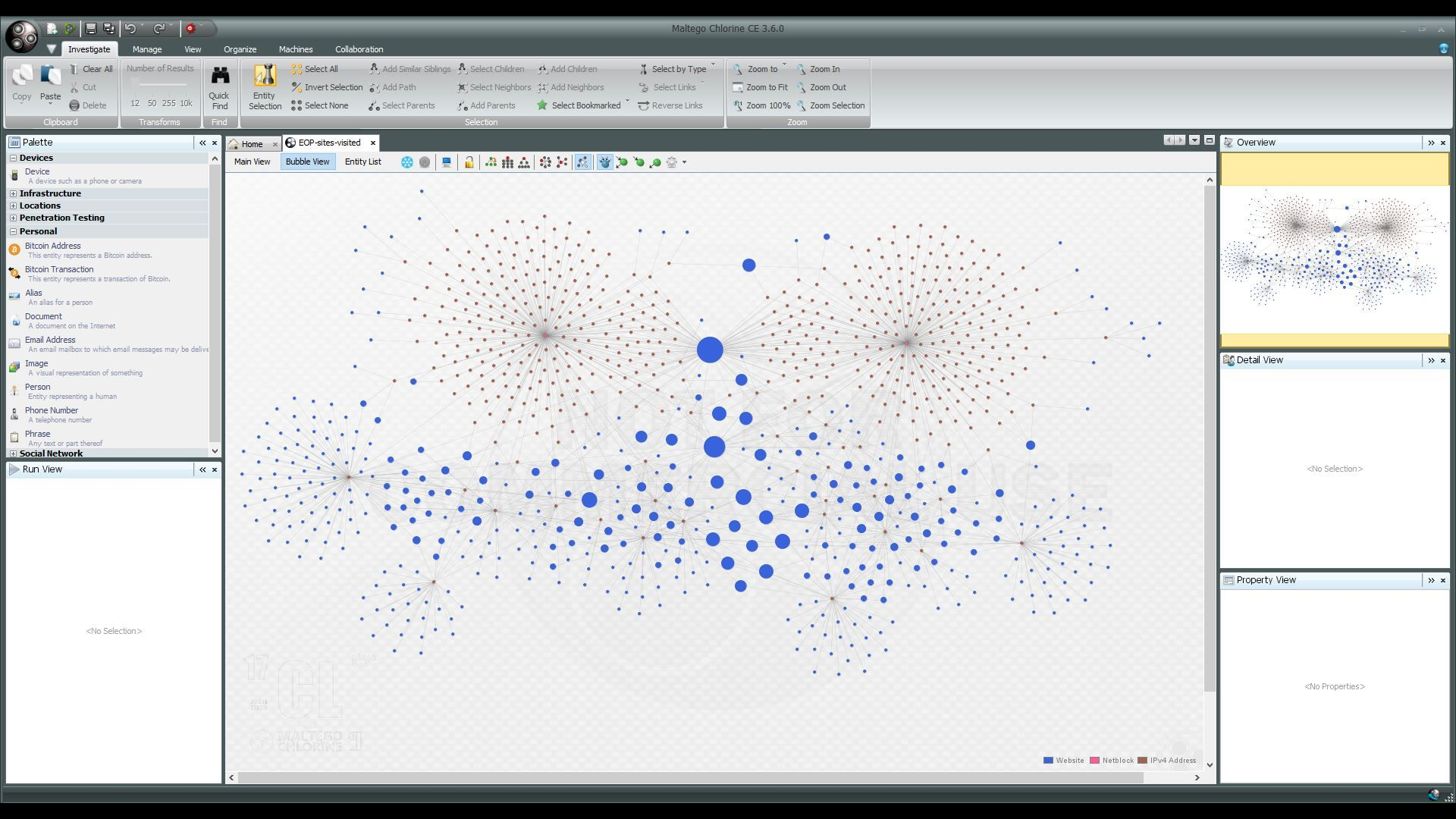
Technology Stacks

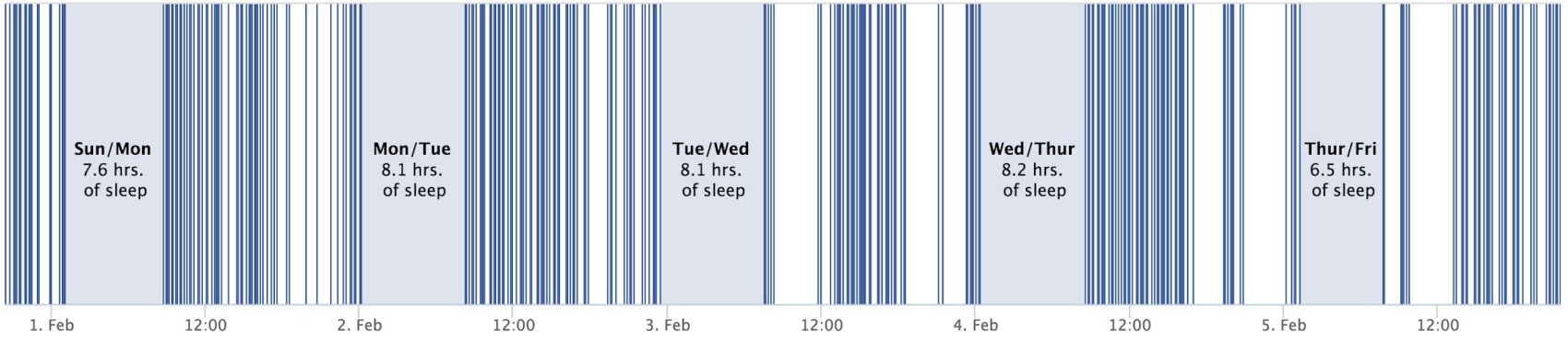
- Urlscan.io
- RiskIQ
- ...

Réseaux Sociaux

- Les réseaux directement avec de faux comptes
  - Soit pour regarder les comptes ou ajouter des ami(e)s
- Scanner de réseaux sociaux:




Maltego Chlorine CE 3.6.0
Investigate
Manage
View
Organize
Machines
Collaboration
Copy
Paste
Clear All
Cut
Delete
Clipboard
Number of Results
12 50 255 10k
Transforms
Quick Find
Find
Entity Selection
Select All
Invert Selection
Select None
Add Similar Siblings
Add Path
Select Parents
Select Children
Select Neighbors
Add Parents
Add Children
Add Neighbors
Select Bookmarked
Select by Type
Select Links
Reverse Links
Selection
Zoom to
Zoom to Fit
Zoom 100%
Zoom In
Zoom Out
Zoom Selection
Zoom
Palette
Devices
Device
A device such as a phone or camera
Infrastructure
Locations
Penetration Testing
Personal
Bitcoin Address
This entity represents a Bitcoin address.
Bitcoin Transaction
This entity represents a transaction of Bitcoin.
Alias
An alias for a person
Document
A document on the Internet
Email Address
An email mailbox to which email messages may be delive
Image
A visual representation of something
Person
Entity representing a human
Phone Number
A telephone number
Phrase
Any text or part thereof
Social Network
Run View
<No Selection>
Home
EOP-sites-visited
Main View
Bubble View
Entity List
Website
Netblock
IPv4 Address
Overview
Detail View
<No Selection>
Property View
<No Properties>

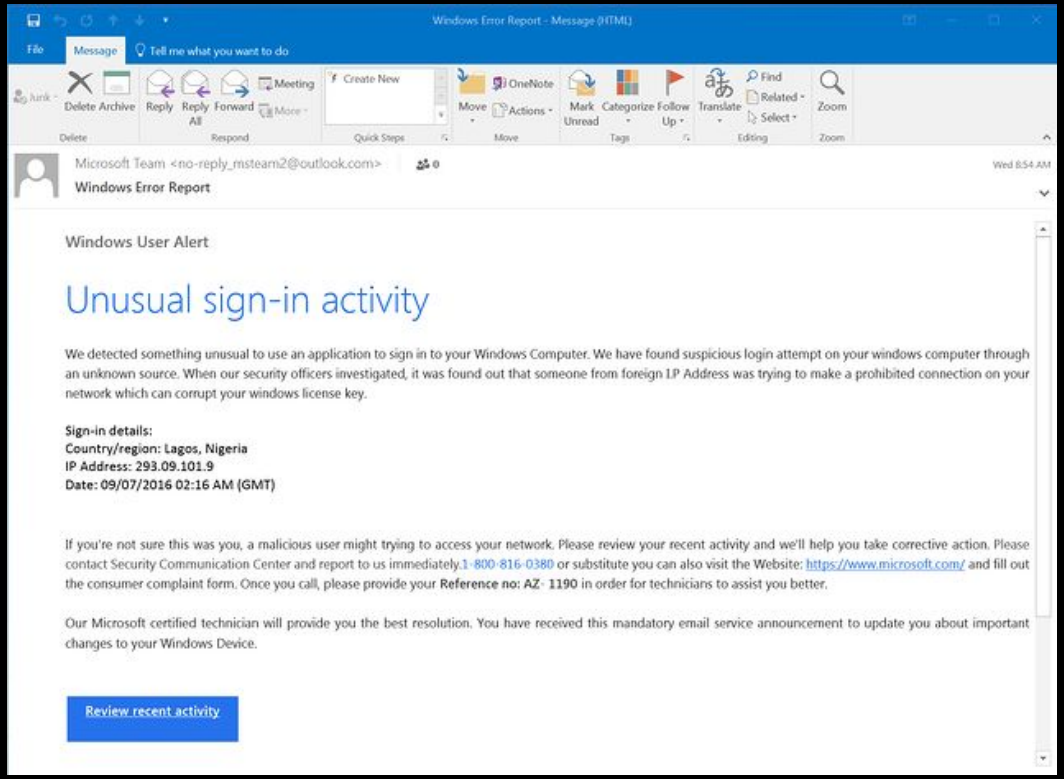


Night after	Period	Duration
Saturday, Jan 30	06:45-11:25	4.7 hours
Sunday, Jan 31	01:02-08:40	7.6 hours
Monday, Feb 01	00:02-08:11	8.1 hours
Tuesday, Feb 02	23:20-07:26	8.1 hours
Wednesday, Feb 03	00:20-08:30	8.2 hours
Thursday, Feb 04	01:10-07:37	6.5 hours
Sunday, Feb 07	22:25-06:32	8.1 hours
Monday, Feb 08	22:08-06:18	8.2 hours
Tuesday, Feb 09	23:52-06:17	6.4 hours
Wednesday, Feb 10	23:47-06:31	6.7 hours

https://github.com/sqren/fb-sleep-stats


Physique et Social

Phishing


Windows Error Report - Message (HTML)
File
Message
Tell me what you want to do
Delete Archive
Reply
Reply All
Forward
Meeting
Create New
Move
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
Microsoft Team <no-reply_msteam2@outlook.com>
Wed 8:54 AM
Windows Error Report
Windows User Alert
Unusual sign-in activity
We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.
Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)
If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your Reference no: AZ- 1190 in order for technicians to assist you better.
Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.
Review recent activity


GoPhish

localhost:3333

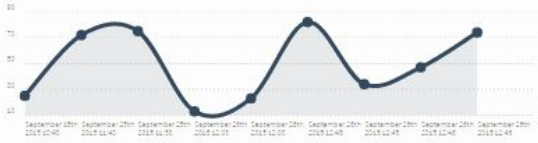
gophish

Dashboard | Campaigns | Users & Groups | Email Templates | Landing Pages | Settings | API Documentation | admin

- Dashboard
- Campaigns
- Users & Groups
- Email Templates
- Landing Pages
- Settings
- API Documentation

Dashboard

Phishing Success Overview



Average Phishing Results

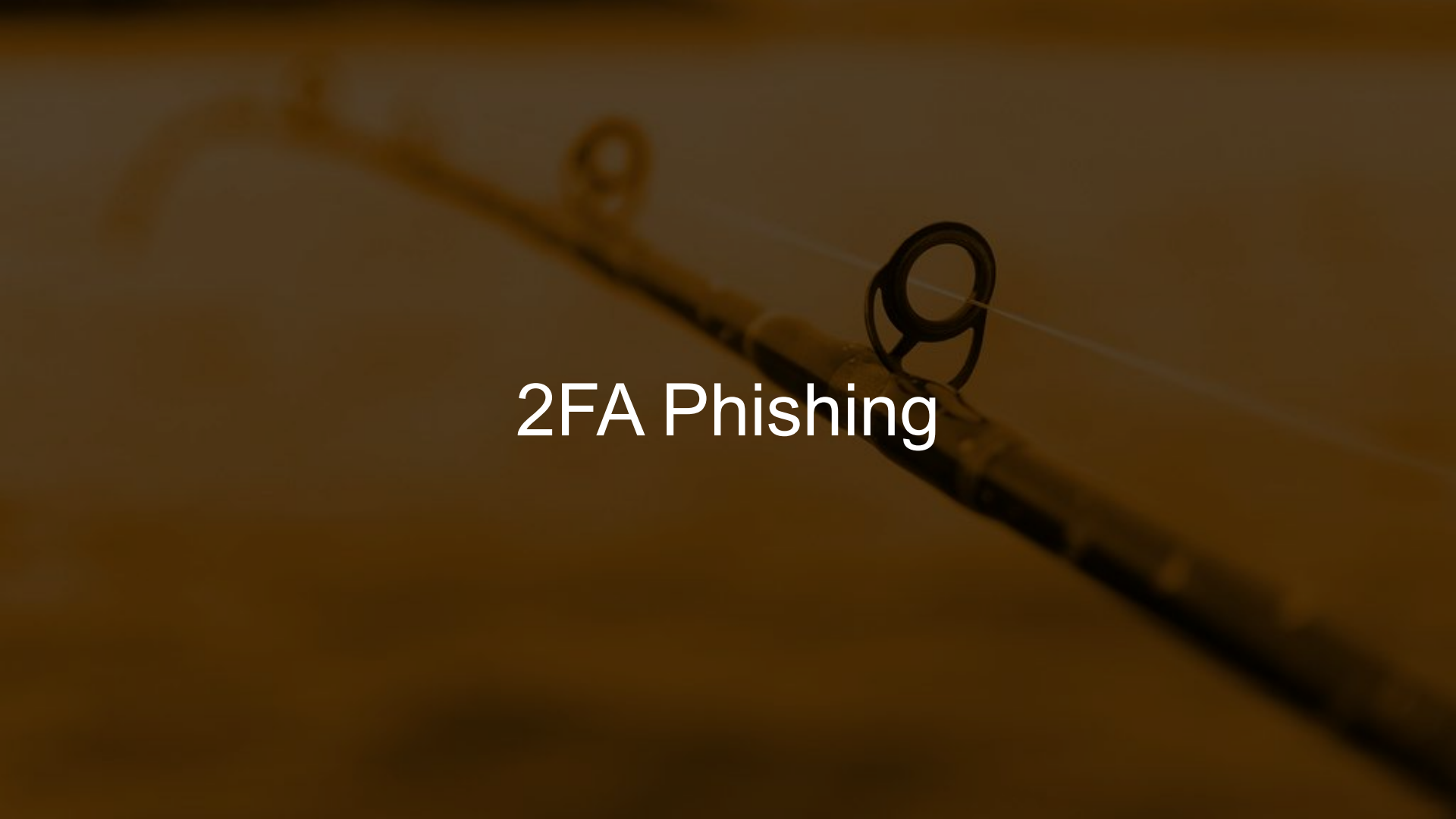
Recent Campaigns

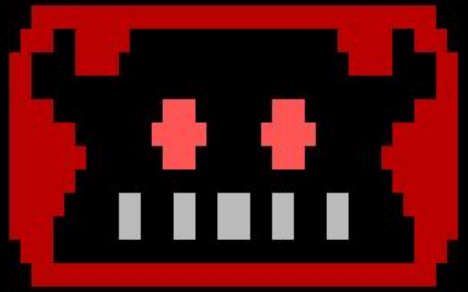
View All

Show 10 entries

Search:

Name	Created Date	Status
Deckow-Stanton Fake Campaign	September 26th 2015 12:03	In progress
Generic Campaign	September 25th 2015 11:40	In progress
Johnston and Sons Fake	September 26th 2015 12:45	Emails Sent


2FA Phishing



no nginx - pure evil

by Kuba Gretzky (@mrgretzky) version 2.0.0

```
[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-almost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+-----+-----------+----------+----------+--------+----------------+---------------------+
| id  | phishlet  | username | password | tokens |   remote ip    |        time         |
+-----+-----------+----------+----------+--------+----------------+---------------------+
| 19  | google    |          |          | none   | [redacted]     | 2018-05-28 08:23    |
+-----+-----------+----------+----------+--------+----------------+---------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+-----+-----------+-------------------------+----------------+----------+----------------+---------------------+
| id  | phishlet  |        username         |    password    |  tokens  |   remote ip    |        time         |
+-----+-----------+-------------------------+----------------+----------+----------------+---------------------+
| 19  | google    | [redacted]@gmail.com    | [redacted]     | captured | [redacted]     | 2018-05-28 08:24    |
+-----+-----------+-------------------------+----------------+----------+----------------+---------------------+

:
```

Ingénierie Sociale - Téléphone

Concours au Hackfest

Qui a été piégé?

- Hydro-Québec
- Bell Canada
- La Banque
- Nationale du Canada
- La Banque de Montréal
- Shell Canada
- Les chemins de fer nationaux du Canada
- Metro Inc.
- Télé-Québec

Matériel non conforme

WIFI PINEAPPLE

$99.99

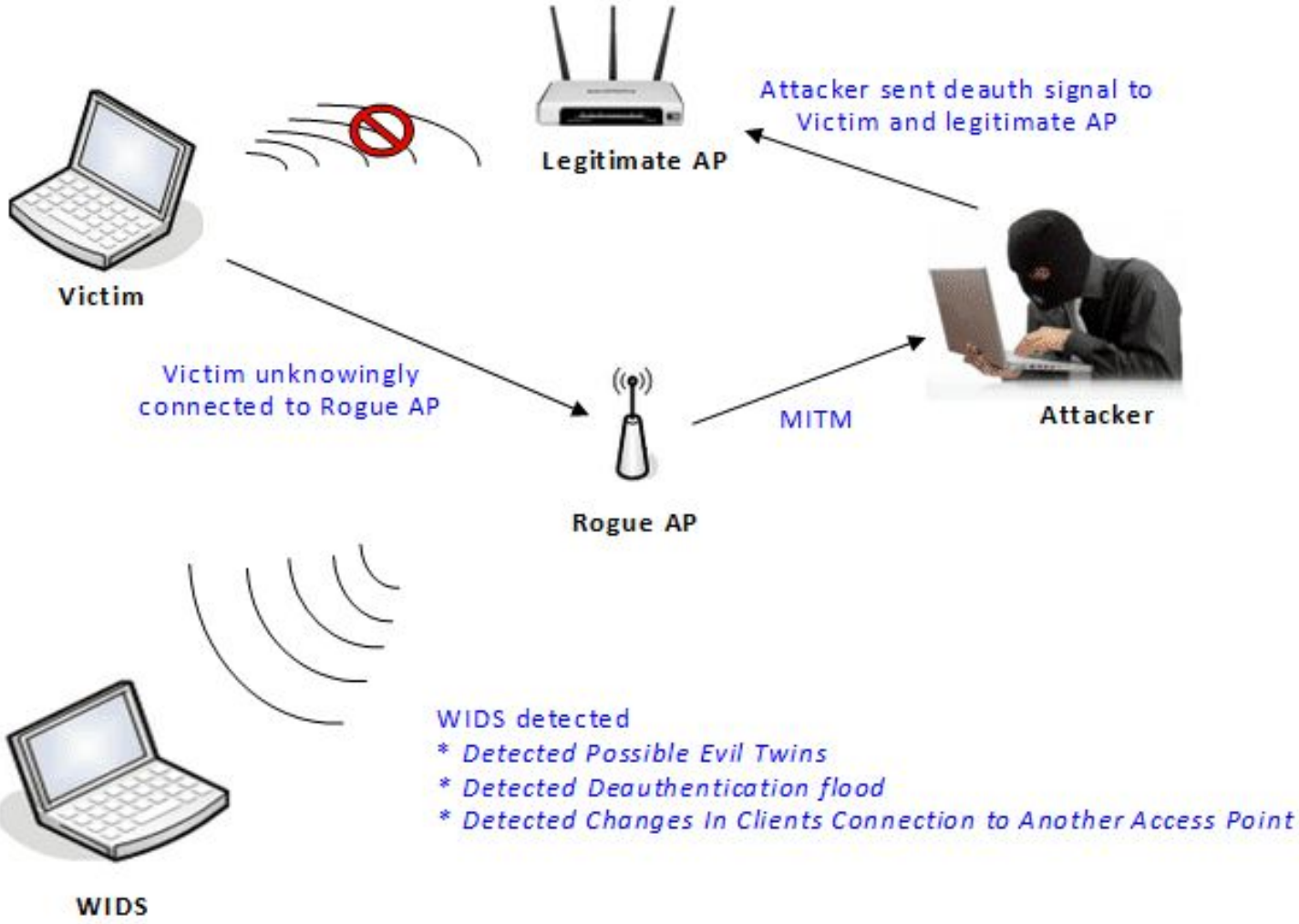
The industry standard pentest platform has evolved. Equip your red team with the WiFi Pineapple® Mark VII. Newly refined. Enterprise ready.

Automate WiFi auditing with all new campaigns and get actionable results from vulnerability assessment reports. Command the airspace with a new interactive recon dashboard, and stay on-target and in-scope with the leading rogue access point suite for advanced man-in-the-middle attacks.

Next-gen network processors combine with multiple role-based radios and the Hak5 patented PineAP suite to deliver impressive results. Hardened and stress tested for the most challenging environments.

The new WiFi Pineapple Mark VII features incredible performance from a simple web interface with an expansive ecosystem of apps, automated pentest campaigns, and Cloud C2 for remote access from anywhere.

MARK VII BASIC	MARK VII TACTICAL
$99.99	$119.99

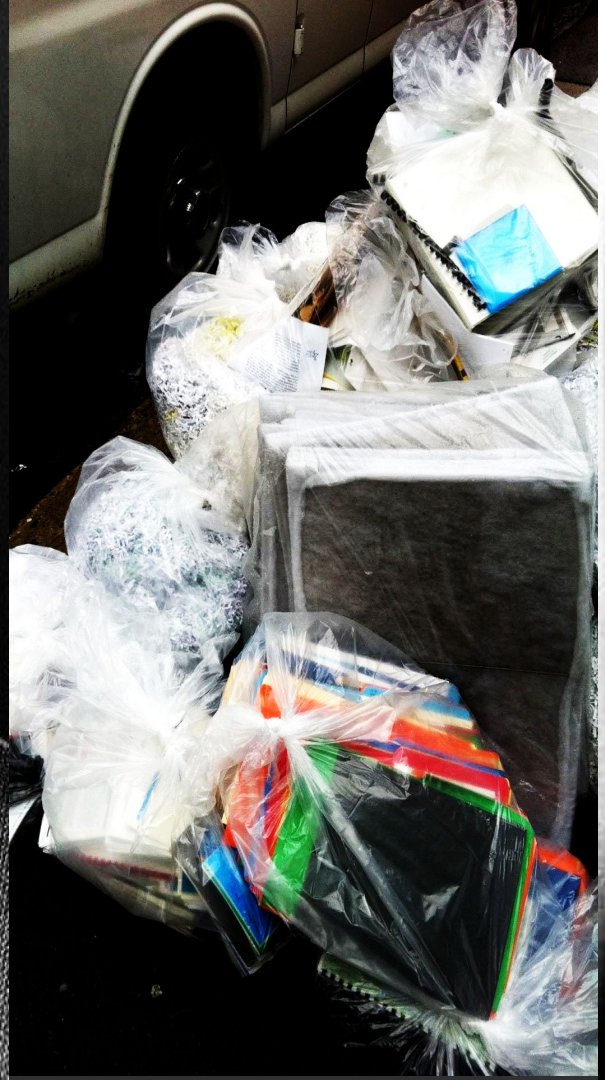

Legitimate AP
Attacker sent deauth signal to
Victim and legitimate AP
Victim
Victim unknowingly
connected to Rogue AP
MITM
Attacker
Rogue AP
WIDS
WIDS detected
* Detected Possible Evil Twins
* Detected Deauthentication flood
* Detected Changes In Clients Connection to Another Access Point


ATMEL

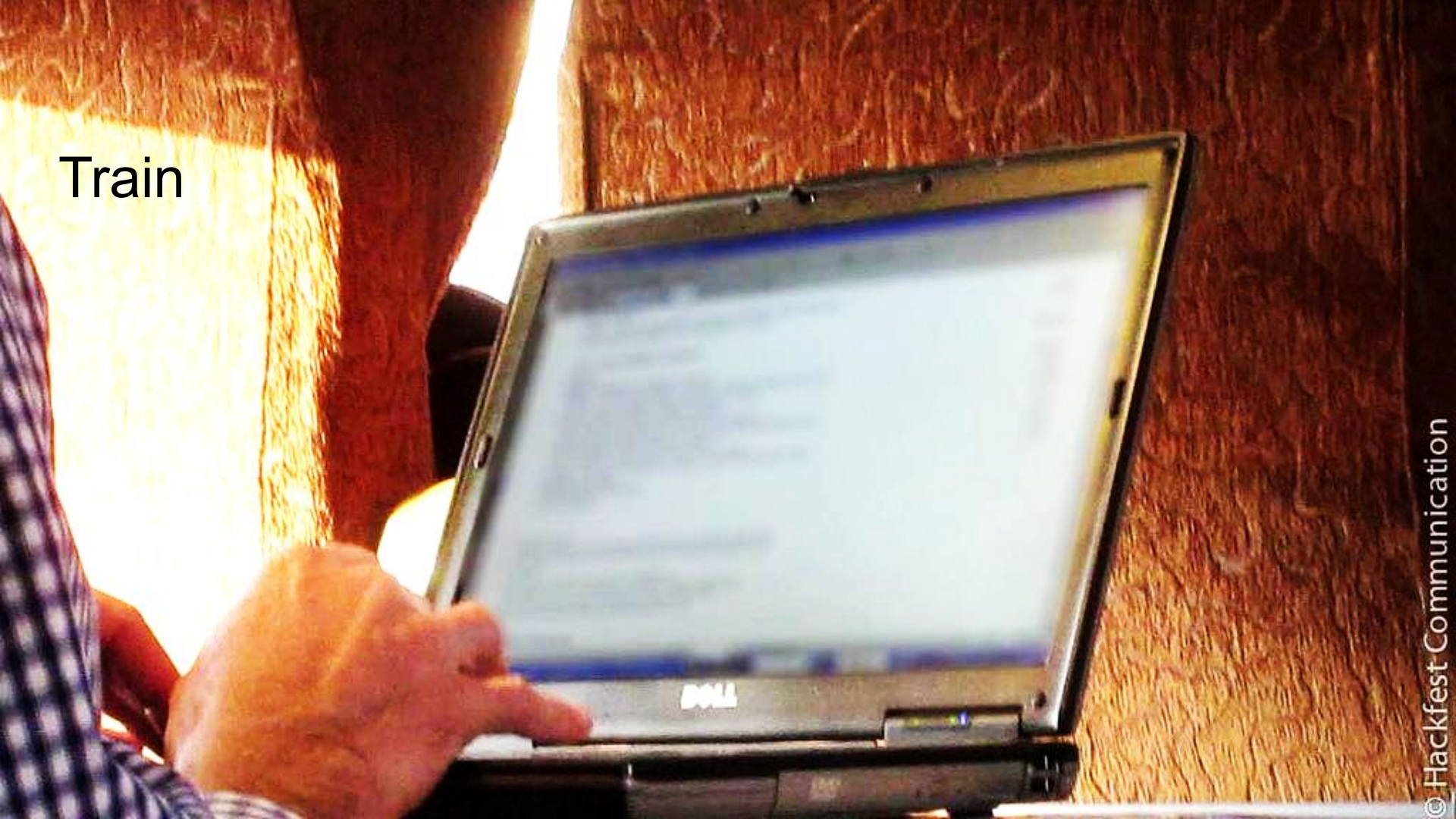

O.MG
www.MG.LOL
ONLY INSERT
O.MG CABLE

Sécuritaire selon-vous?

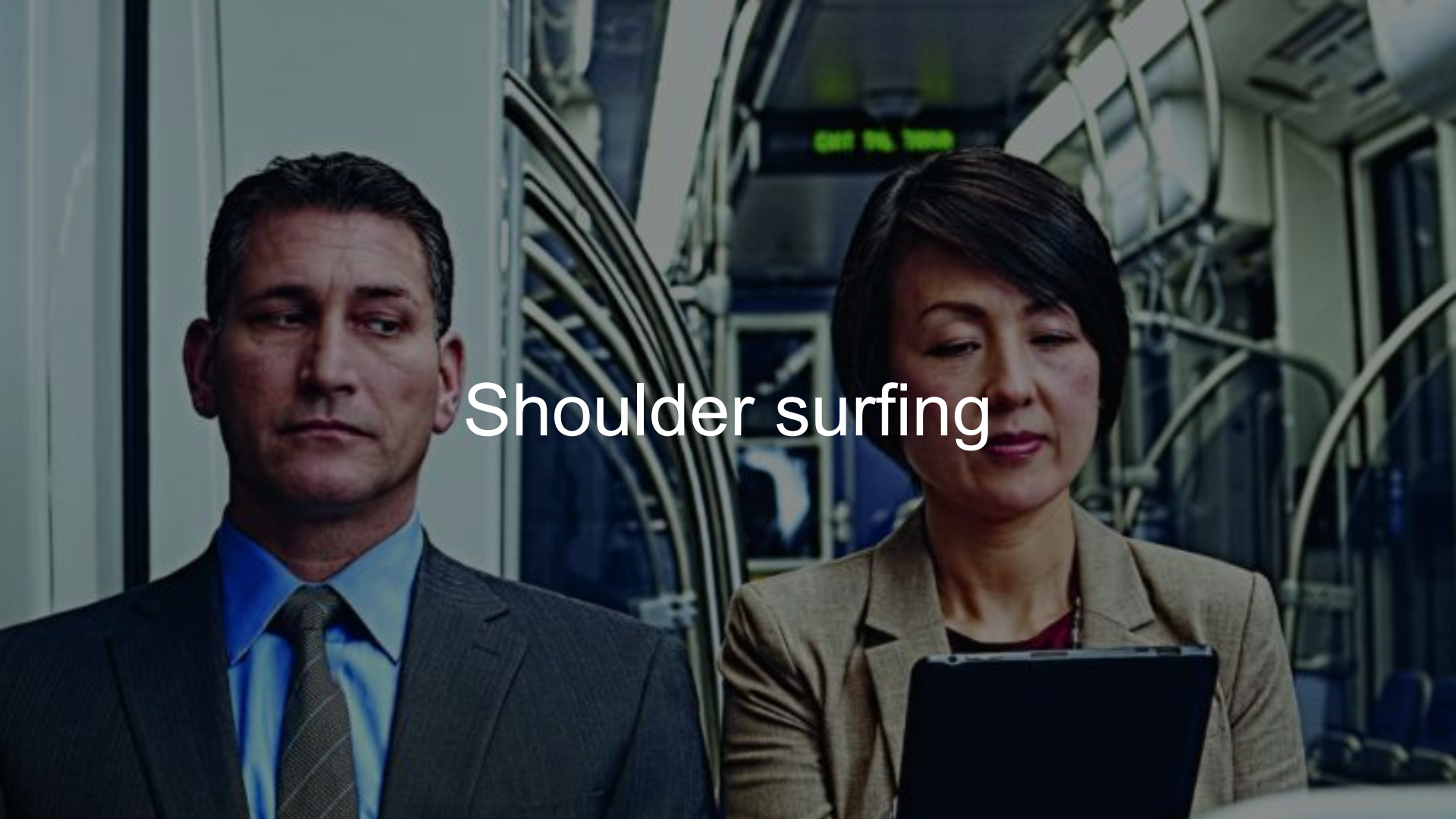

Poubelles sécuritaire?




IRON MOUNTAIN
1-800-463-1405

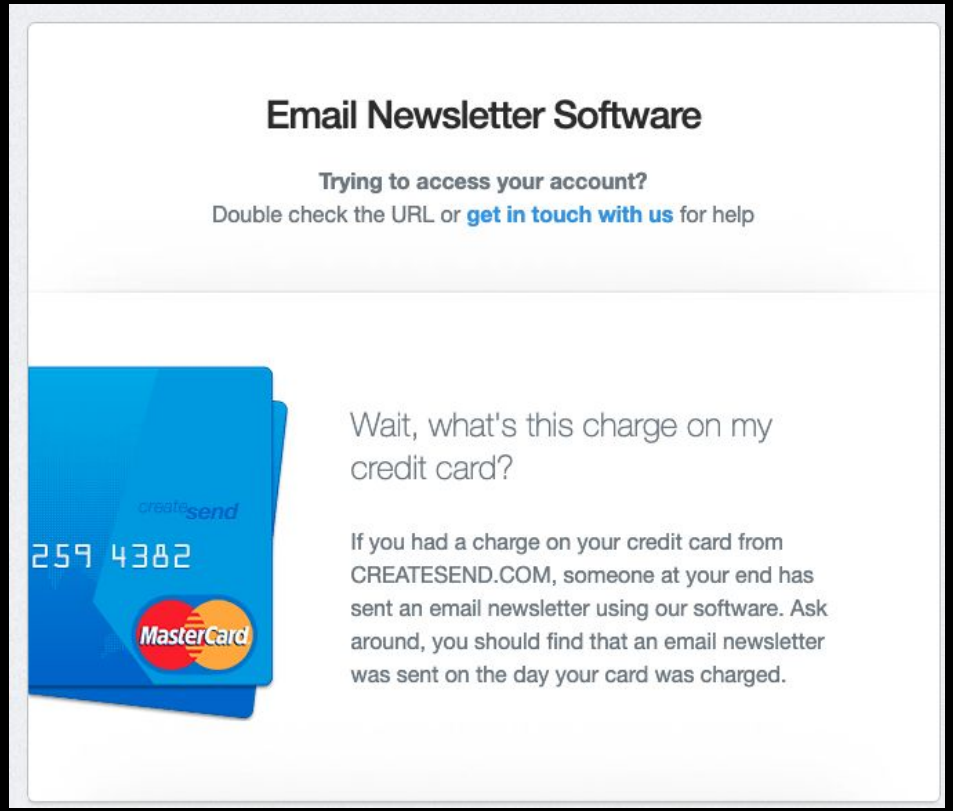

Train
©Hackfest Communication

Clean desk/windows


Shoulder surfing


Exemples

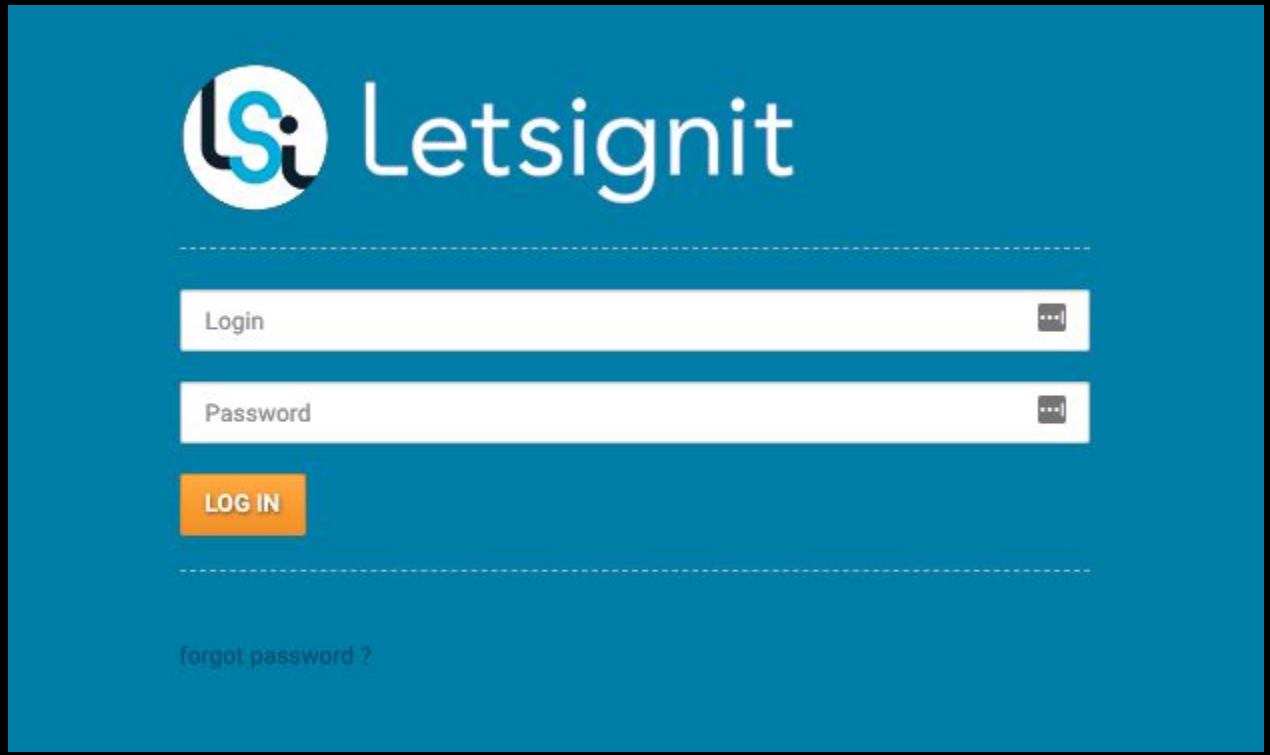
Surface d’attaque



Surface d’attaque

```
User-agent: *
Disallow: /_hcms/preview/
Disallow: /hs/manage-preferences/
```

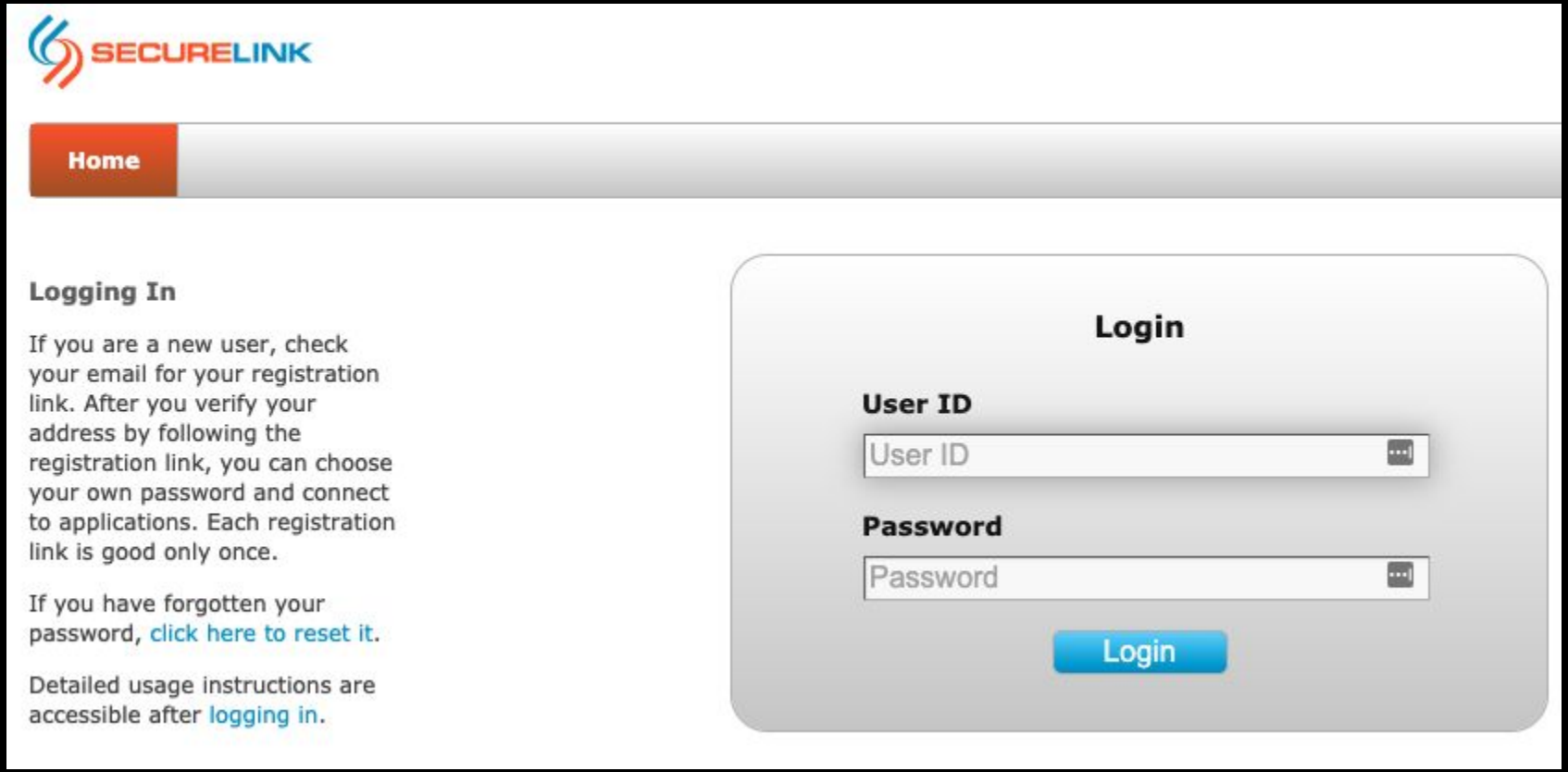
Surface d’attaque



Surface d’attaque

Proofpoint

Surface d’attaque



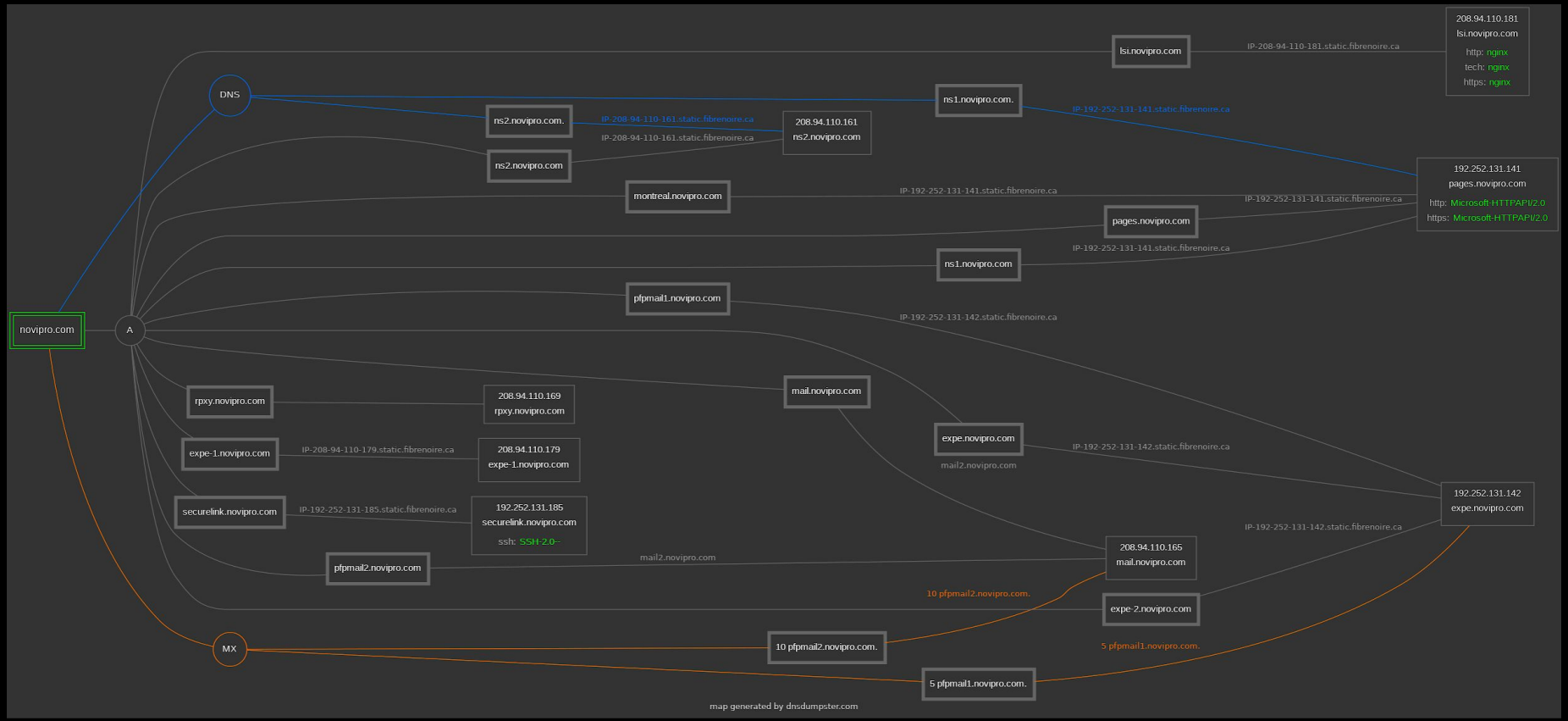
Surface d’attaque

E	F
Common Name	Matching Identities
lsi.novipro.com	lsi.novipro.com
communication.novipro.com	communication.novipro.com
blog.novipro.com	blog.novipro.com
info.novipro.com	info.novipro.com
email.novipro.com	email.novipro.com
hub.novipro.com	hub.novipro.com
*.novipro.com	*.novipro.com
securelink.novipro.com	securelink.novipro.com
observium.novipro.com	observium.novipro.com
ipam.novipro.com	ipam.novipro.com
sip.novipro.com	access.novipro.com
pool1.novipro.inc	

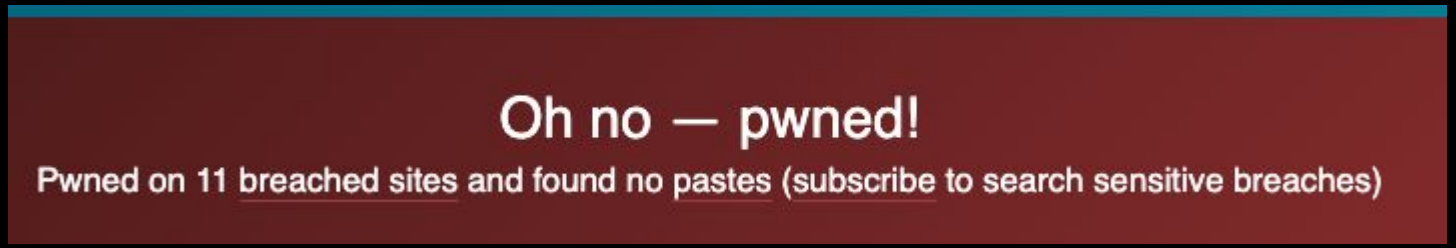
Subdomains

info.novipro.com
lsi.novipro.com
communication.novipro.com
email.novipro.com
blog.novipro.com
ns1.novipro.com
hub.novipro.com
securelink.novipro.com
ns2.novipro.com
next.novipro.com
ipam.novipro.com
observium.novipro.com
pages.novipro.com
ns4.novipro.com
antispam.novipro.com
lyncdiscover.novipro.com
exchange.novipro.com
mail.novipro.com
montreal.novipro.com
www.novipro.com

Surface d’attaque



Leaked Passwords



XSS (Censuré)


Démo Live et Rapide
Si le temps le permet!


Questions?