

La facilité de pirater une entreprise

D'une recherche Google à une brèche complète!

Patrick Mathieu, Hackfest.ca
Novembre 2020

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: @patheti

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>



Infosec Jobs

<https://infosecjobs.ca>



HACKFEST.ca

GET
INVOLVED

info@hackfest.ca



DISCORD

<https://discord.gg/39fRfa6>

Parlons tout d'abord de hacking!





Pas ça!

HACKING IN PROGRESS

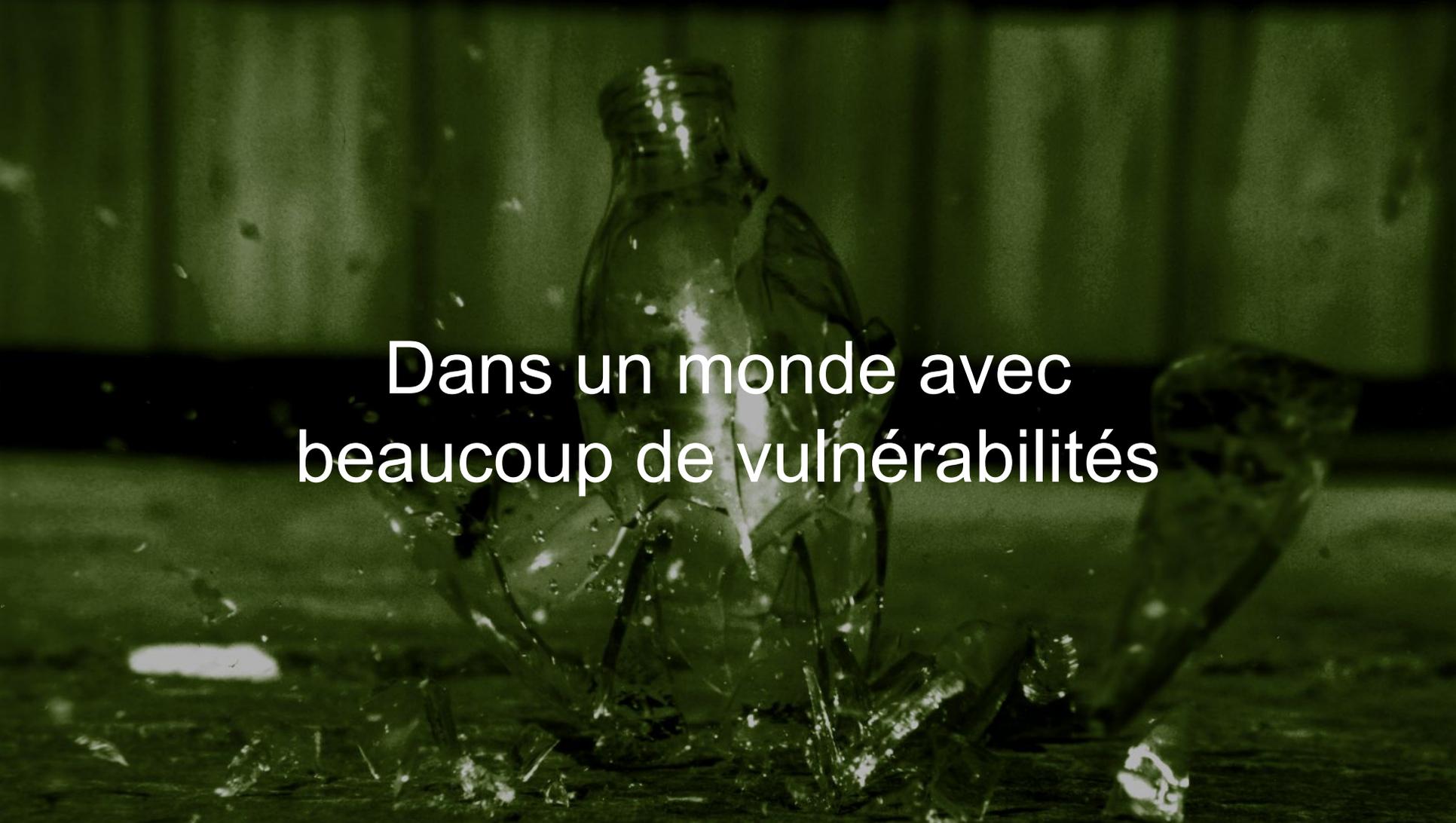
Ni a!

Quelque chose comme ça!



Ou encore... ça ...!



A photograph of a shattered glass bottle lying on a dark, reflective surface. The bottle is broken into several large and small pieces, with some shards still attached to the main body. The entire scene is bathed in a monochromatic green light, creating a somber and dramatic atmosphere. The background is dark and out of focus, suggesting an indoor setting with a wall or door.

Dans un monde avec
beaucoup de vulnérabilités

A photograph of a busy city street at night. The scene is filled with people walking across a crosswalk. In the background, a large building is illuminated with a grid pattern and features two signs that say "KKBOX". To the left, there is a large, dark, rounded tree and a brightly lit storefront. The overall atmosphere is one of a bustling urban environment.

Nous sommes tous à risque!

LONGUE LISTE DE VICTIMES

Des dizaines d'organisations publiques et privées ont été touchées au cours de la dernière semaine.

STM

En octobre, la Société de transport de Montréal a subi une attaque de ransomware qui a compromis des données de voyageurs.

Wendake

La Nation huronne-wendate a subi une attaque de ransomware qui a compromis des données d'élèves d'un centre scolaire.

Ministère de la Justice du Québec

Des pirates ont réussi à voler des courriels électroniques à des citoyens l'ayant contacté.

Revenu Canada

Des fraudeurs ont attaqué les dossiers de 9041 utilisateurs en ligne.

Inonotech-Execaire

La firme d'entretien d'aéronefs a été touchée par une attaque de ransomware 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 de restauration a subi l'attaque de se propager davantage à travers le monde.



Une attaque informatique cible d'hôpitaux canadiens et américains

Le ministère de la Santé du Québec fait partie des victimes de cette campagne agressive de demande de rançon.



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



Plus de 3000 lecteurs de «L'actualité» piratés

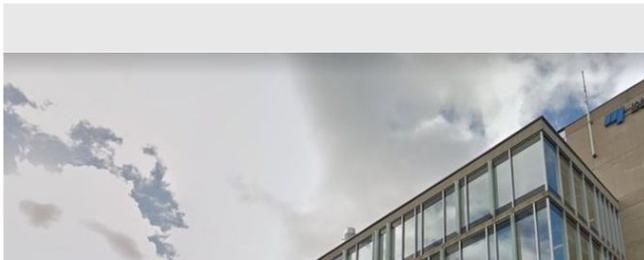
Arnaud Koenig Soutière | Le Journal de Québec | Publié le 15 septembre 2019 à 23:03 - Mis à jour le 15 septembre 2019

Les données personnelles de plus de 3000 utilisateurs de l'ancien site web du magazine «L'actualité» ont été...



L'INRS ciblé par des pirates informatiques Un ancien employé de l'armée aurait commis une importante fraude à Valcartier

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



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



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



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	24	9	3	0
Share	Tweet	+1	Email	Comment

GET CANADA BUSINESS NEWSLETTERS:

Enter email

SUBSCRIBE

FOLLOW: Video, Bell Canada, Hultcrew Bell, Hultcrew Hack, Bell Hultcrew, Bell Canada Hack, Bell Hack, Bell Information Hacked, Cp, Hultcrew, 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.

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

HACKING

The Statistics Canada Site Was Hacked By an Unknown Attack

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

Important Notice: unauthorized access payment card data in stores



Bar ouvert pour les Vo

Une faille informatique aurait permis de localiser sans mot de Canadiens

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 2017. 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

A dramatic sunset over the ocean. The sun is a bright, glowing semi-circle on the horizon, casting a warm orange and red glow across the sky. A large, dark, textured cloud is positioned in the center, partially obscuring the sun. The sky is filled with various cloud formations, some catching the light of the setting sun. The ocean is dark and calm, reflecting the colors of the sky.

Aujourd'hui
c'est Zerotrust et les nuages

A photograph of a staircase with green and red steps and metal railings. The text "Étapes d'une attaque" is overlaid in the center.

Étapes d'une attaque

An aerial, top-down view of a white USAF surveillance aircraft, likely a Boeing RC-135, flying over a landscape of clouds. The aircraft features a large, black, circular sensor pod mounted on its upper fuselage. The wings are marked with "USAF" and a star insignia. The text "OSINT" and "Open Source INTelligence" is overlaid in white on the aircraft's fuselage.

OSINT
Open Source INTelligence

Les attaquants





Hackers

Bon ou méchant, ils sont présents

A photograph of two young children dressed as Mario and Luigi. The child on the left is wearing a green cap and shirt, sitting in a blue toy car with a white 'L' on the front. The child on the right is wearing a red cap and shirt, sitting in a red toy car with a white 'M' on the front. Both cars have a steering wheel and a small Mario logo on the front. The background is slightly blurred, showing other people and what appears to be an outdoor event.

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

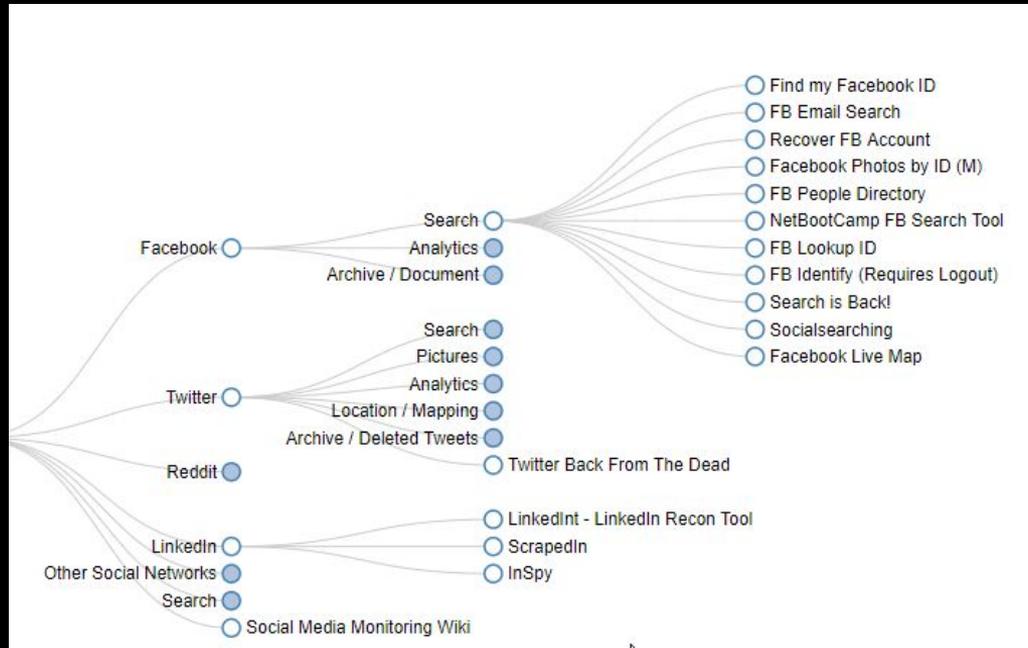
- Nmap
- Masscan
- Shodan.io
- ...

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:



Investigate Manage View Organize Machines Collaboration

Clipboard: Copy, Paste, Cut, Delete

Transforms: Clear All, Number of Results: 12 50 255 10k

Find: Quick Find

Select All, Add Similar Siblings, Select Children, Add Children, Select by Type

Invert Selection, Add Path, Select Neighbors, Add Neighbors, Select Links

Select None, Select Parents, Add Parents, Select Bookmarked, Reverse Links

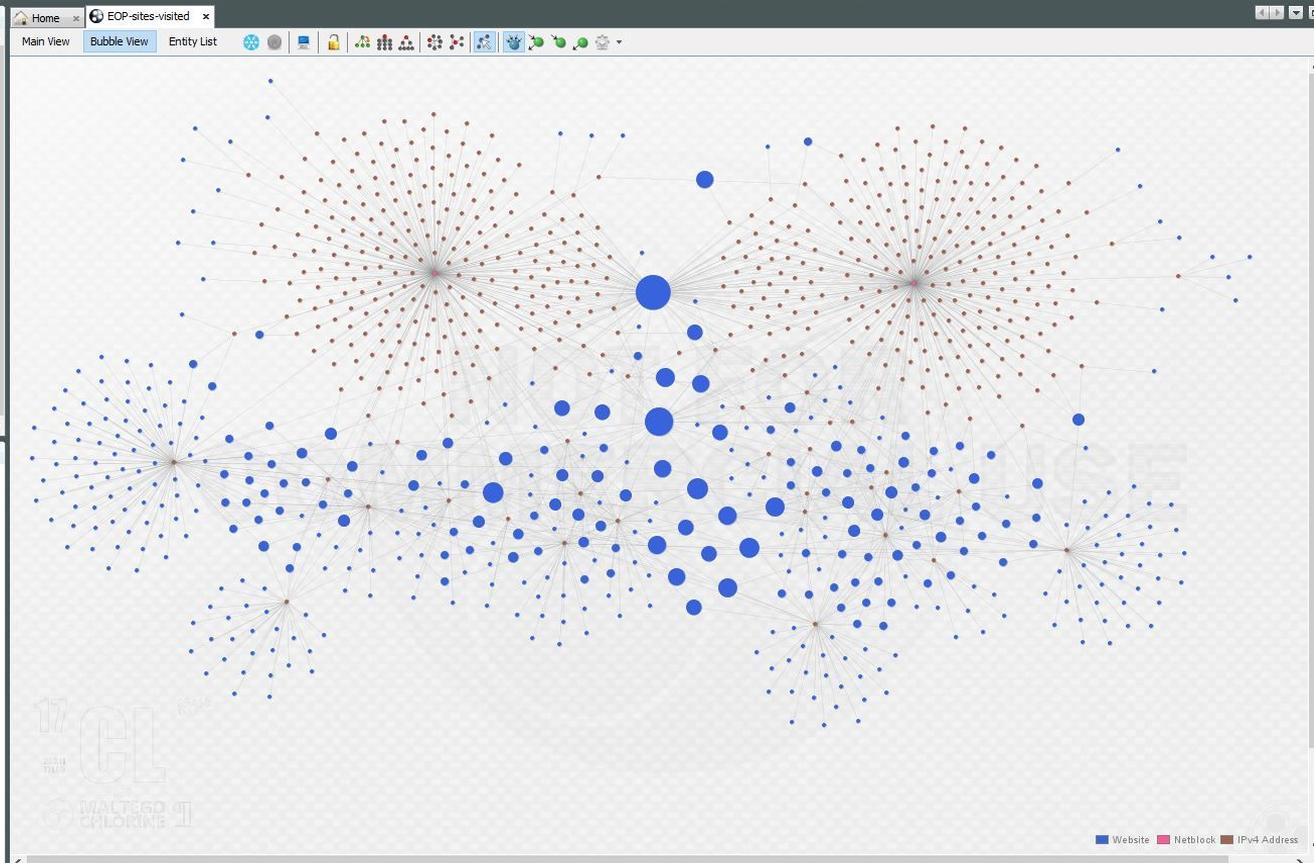
Selection

Zoom to, Zoom In, Zoom to Fit, Zoom Out, Zoom 100%, 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 delivered
 - Image: A visual representation of something
 - Person: Entity representing a human
 - Phone Number: A telephone number
 - Phrase: Any text or part thereof
- Social Network



Overview

Detail View

<No Selection>

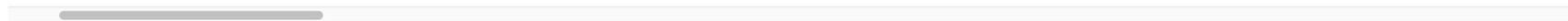
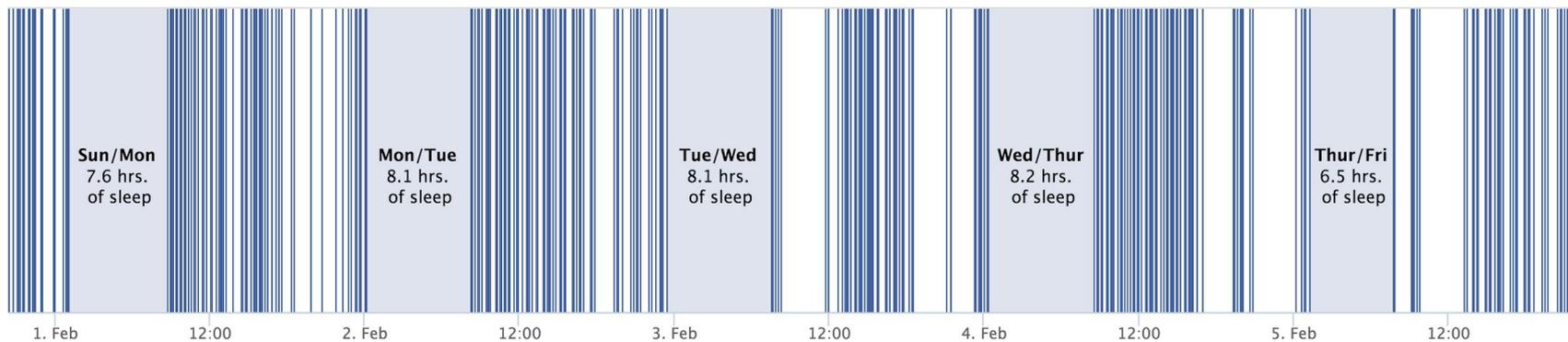
Property View

<No Properties>

Run View

<No Selection>





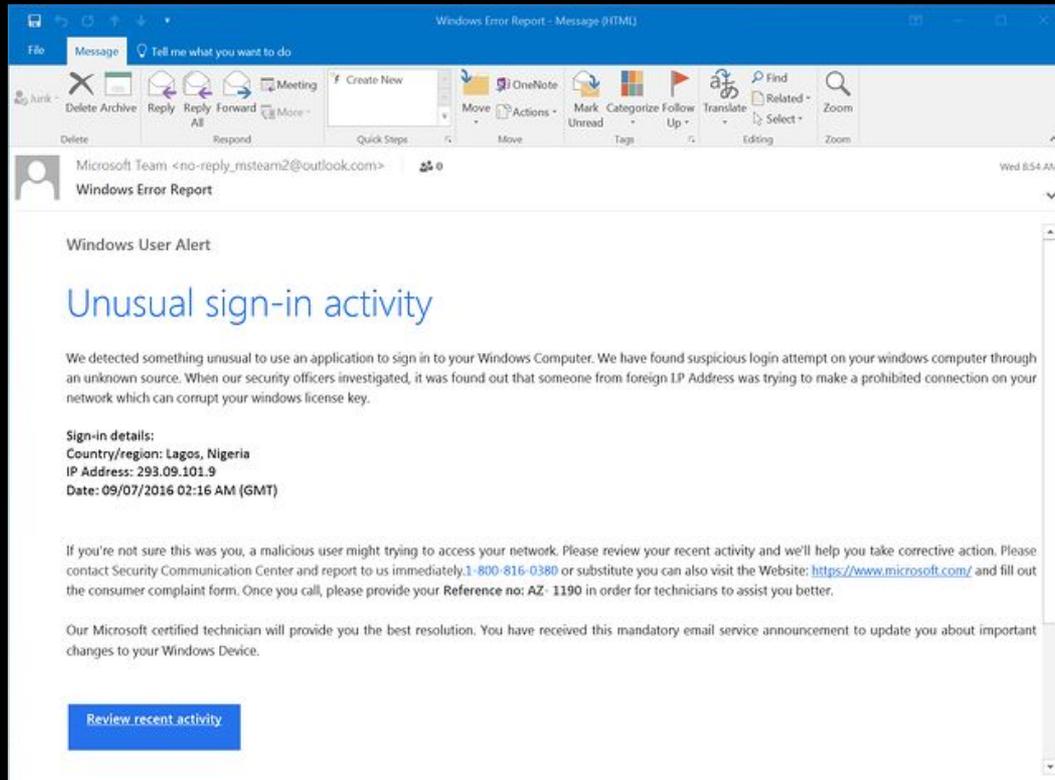
Night after	Period	Duration
Saturday, Jan 30	06:45-11:25	4.7 hours
Sunday, Jan 31	01:02-08:40	7.6 hours
Monday, Feb 01	00:02-08:11	8.1 hours
Tuesday, Feb 02	23:20-07:26	8.1 hours
Wednesday, Feb 03	00:20-08:30	8.2 hours
Thursday, Feb 04	01:10-07:37	6.5 hours
Sunday, Feb 07	22:25-06:32	8.1 hours
Monday,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





GoPhish

Dashboard

Campaigns

Users & Groups

Email Templates

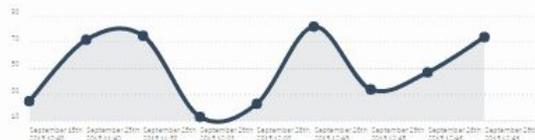
Landing Pages

Settings

API Documentation

Dashboard

Phishing Success Overview



Average Phishing Results

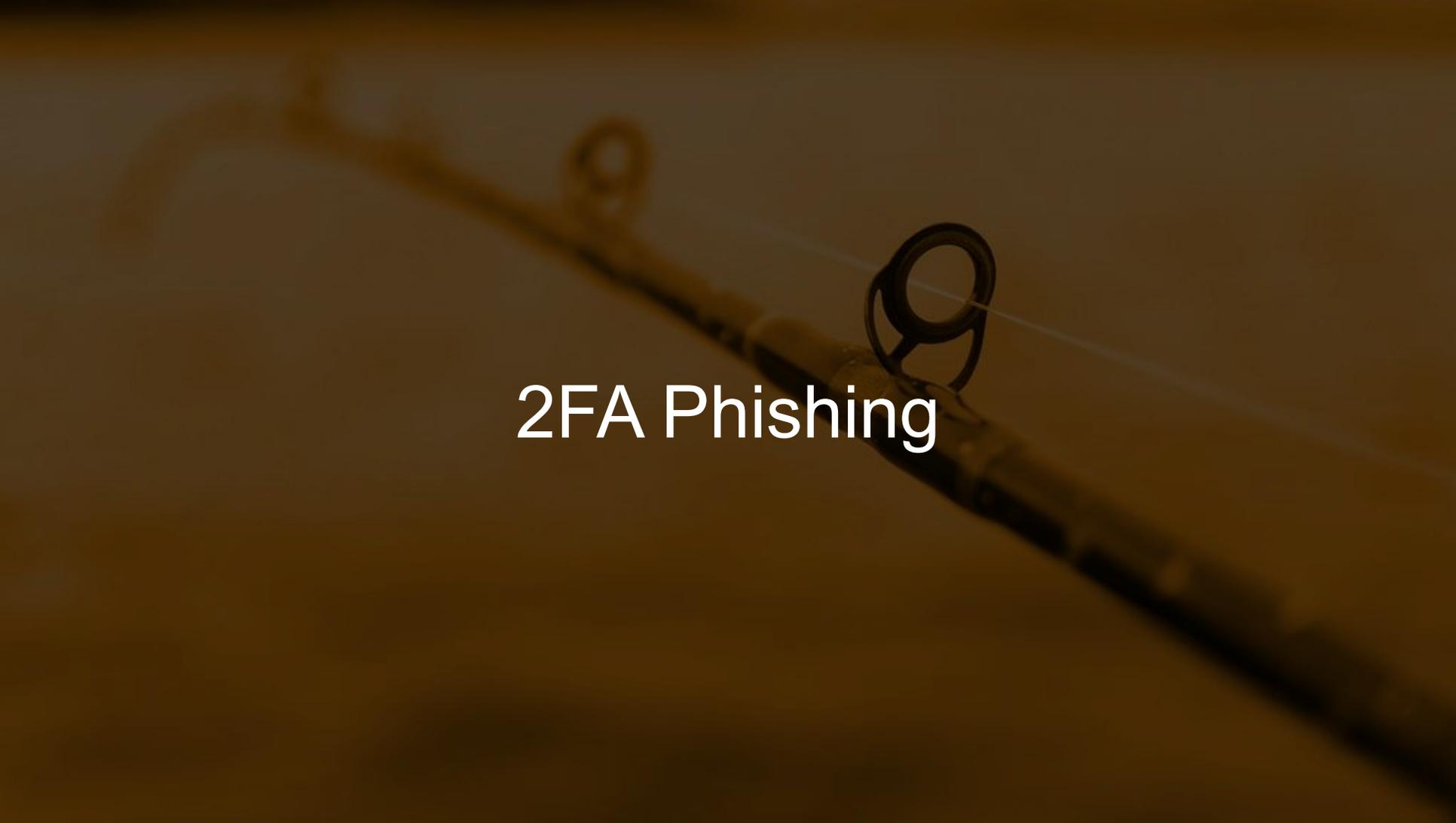


- Successful Phishes
- Unsuccessful Phishes

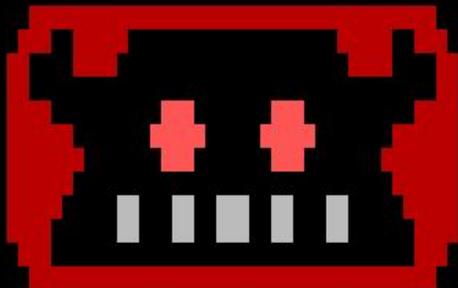
Recent Campaigns

[View All](#)Show entriesSearch:

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		

A fishing rod with a reel is shown diagonally across the frame. The image is overlaid with a semi-transparent brown filter. The text "2FA Phishing" is centered in white.

2FA Phishing



Evilginx

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] [^A] 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-alm  
ost-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] [^A] [0] Username: [redacted]@gmail.com  
[08:24:29] [^A] [0] Password: [redacted]  
[08:24:41] [^A] [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

: █

A vintage rotary telephone is shown from a top-down perspective, centered in the frame. The phone is a classic design with a circular dial and a handset. The entire image is overlaid with a semi-transparent green filter. The text "Ingénierie Sociale - Téléphone" is written in white, bold, sans-serif font across the middle of the phone's dial.

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.

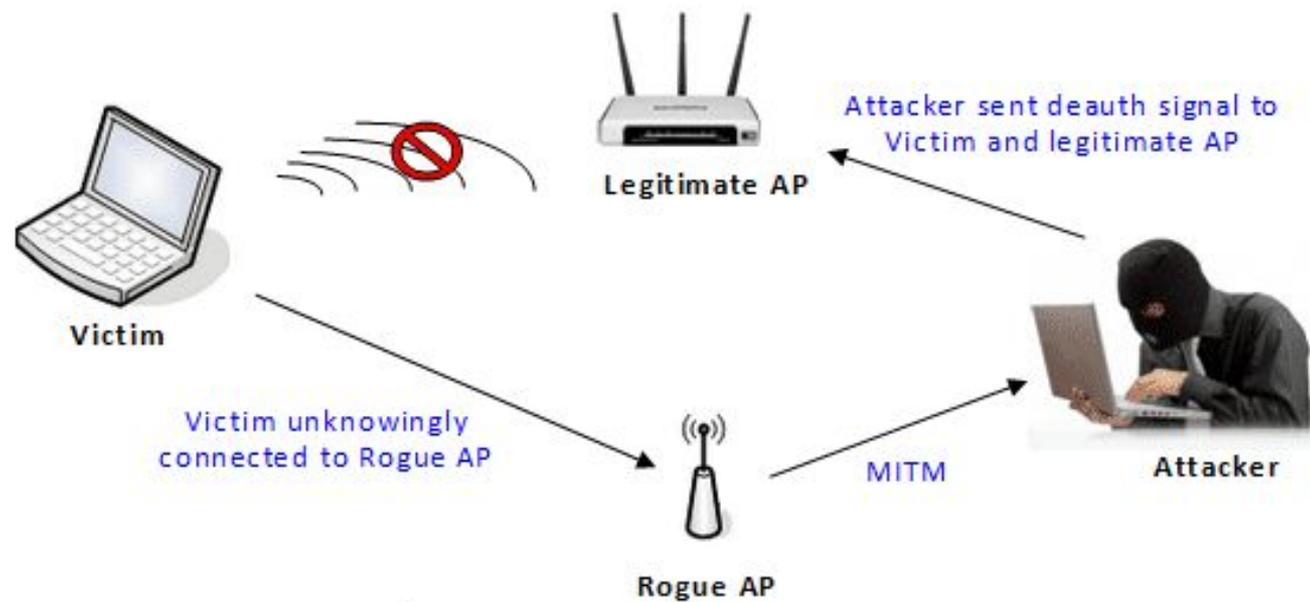
The new WiFi Pineapple Mark VII features incredible performance from a simple web interface with an expansive ecosystem of apps, automated pentest campaigns, and Cloud C2 for remote access from anywhere.

MARK VII BASIC

\$99.99

MARK VII TACTICAL

\$119.99



WIDS

WIDS detected

- * *Detected Possible Evil Twins*
- * *Detected Deauthentication flood*
- * *Detected Changes In Clients Connection to Another Access Point*







Sécuritaire selon-vous?



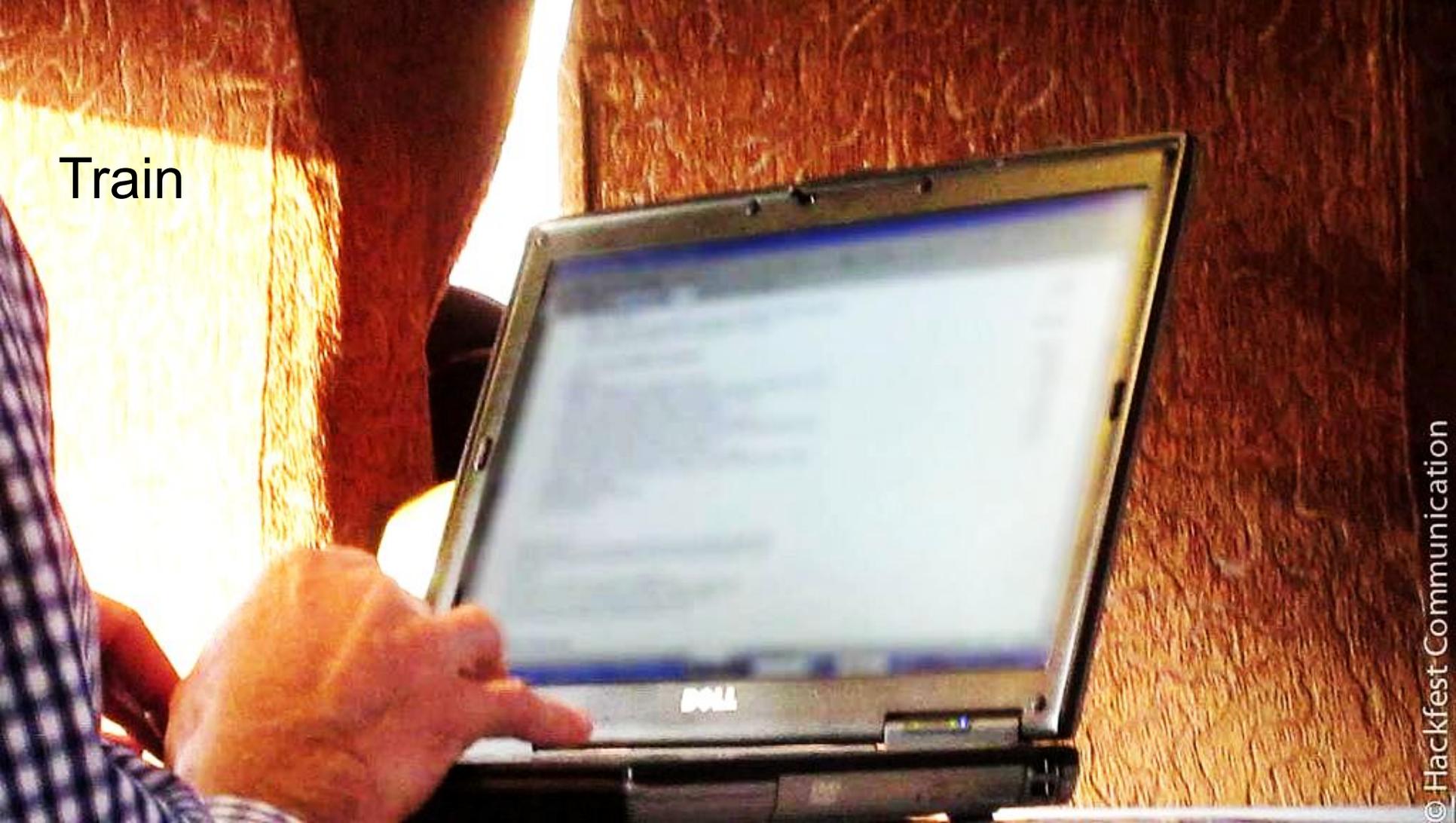
A blurred night scene with bokeh lights in the background and a basket of red poinsettias in the foreground. The text "Poubelles sécuritaire?" is overlaid in the center.

Poubelles sécuritaire?



 IRON MOUNTAIN
1-800-463-1105

Train



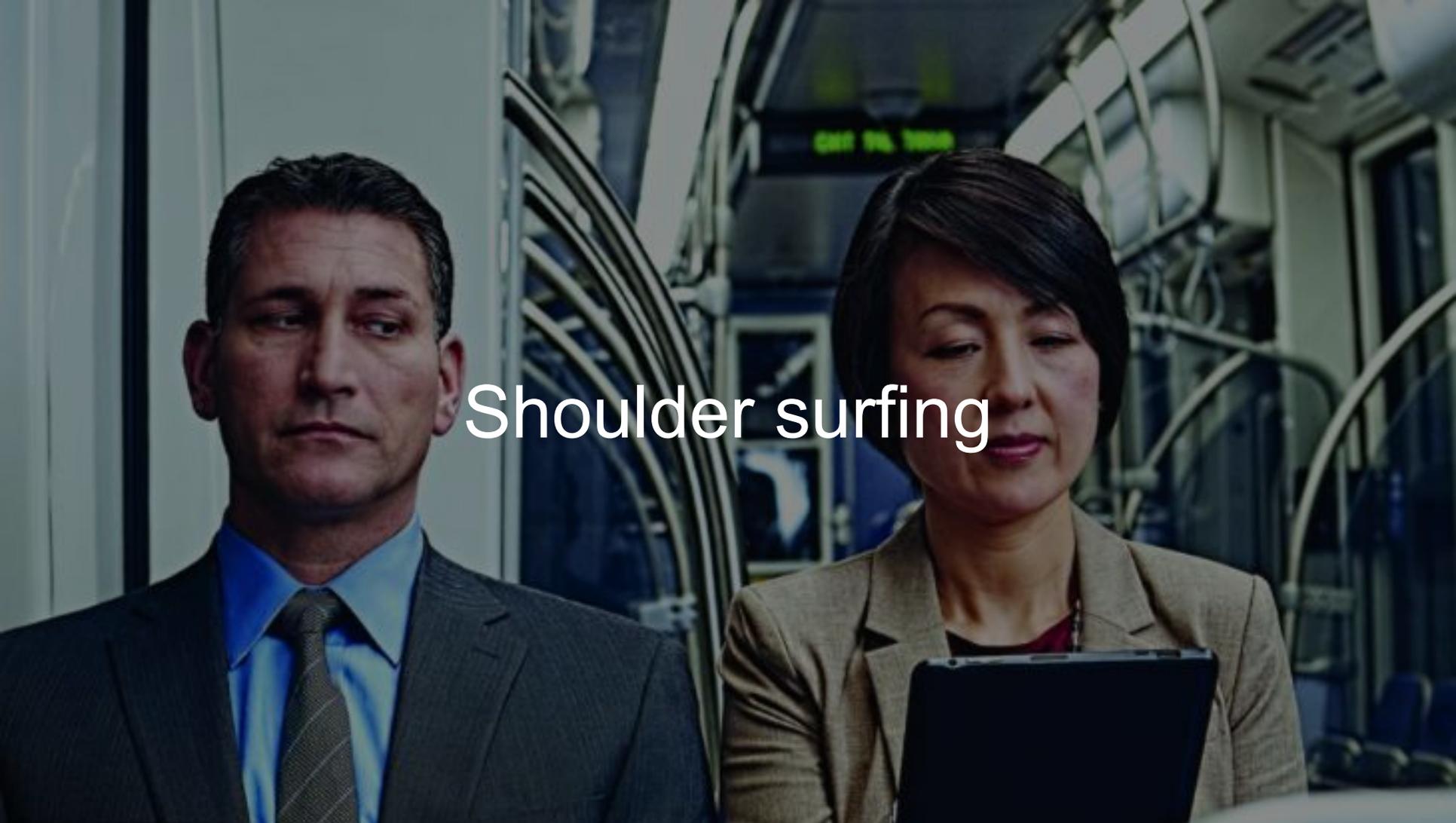
Clean desk/windows



© Hackfest Communication

© Hackfest Communication



A man in a dark suit, light blue shirt, and patterned tie stands on the left, looking over his right shoulder towards a woman on the right. The woman has short dark hair and is wearing a tan blazer over a dark top. She is looking down at a tablet computer she is holding. The background is a server room with racks of equipment and a green "EXIT" sign. The text "Shoulder surfing" is overlaid in white in the center of the image.

Shoulder surfing



Exemples

Surface d'attaque

Email Newsletter Software

Trying to access your account?

Double check the URL or [get in touch with us](#) for help



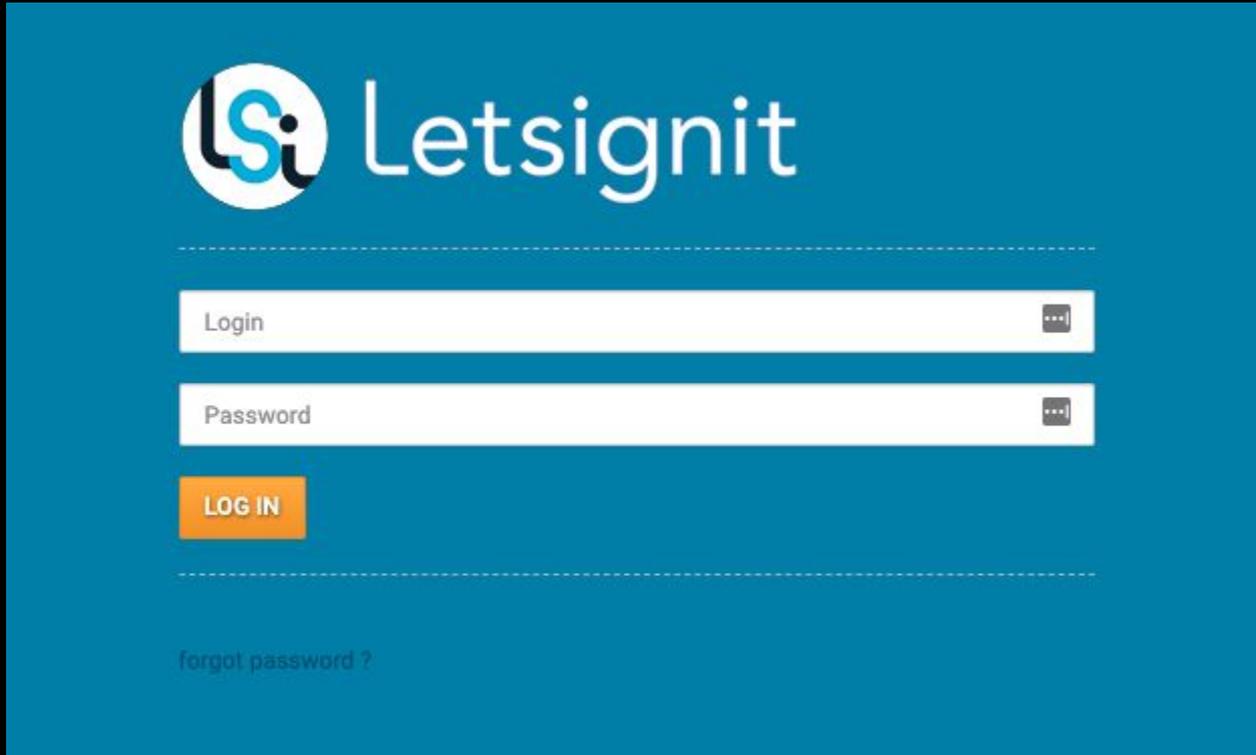
Wait, what's this charge on my credit card?

If you had a charge on your credit card from CREATESEND.COM, someone at your end has sent an email newsletter using our software. Ask around, you should find that an email newsletter was sent on the day your card was charged.

Surface d'attaque

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

Surface d'attaque



The image shows a login interface for 'Letsignit' on a blue background. At the top left is the 'Lsi' logo, followed by the text 'Letsignit'. Below this is a horizontal dashed line. The login form consists of two white input fields: the first is labeled 'Login' and the second is labeled 'Password', each with a small icon on the right side. Below the password field is an orange button with the text 'LOG IN'. Another horizontal dashed line is positioned below the button. At the bottom left, there is a link that says 'forgot password ?'.

Surface d'attaque

Proofpoint

Services

25

tcp

smtp

554 Blocked - see <https://ipcheck.proofpoint.com/?ip=177.169.52.78>

250-pmtlavppfrrt1.novipro.inc Hello 177.169.52.78 [177.169.52.78], pleased to meet you

250 ENHANCEDSTATUSCODES

Surface d'attaque



Home

Logging In

If you are a new user, check your email for your registration link. After you verify your address by following the registration link, you can choose your own password and connect to applications. Each registration link is good only once.

If you have forgotten your password, [click here to reset it.](#)

Detailed usage instructions are accessible after [logging in.](#)

Login

User ID



Password



Login

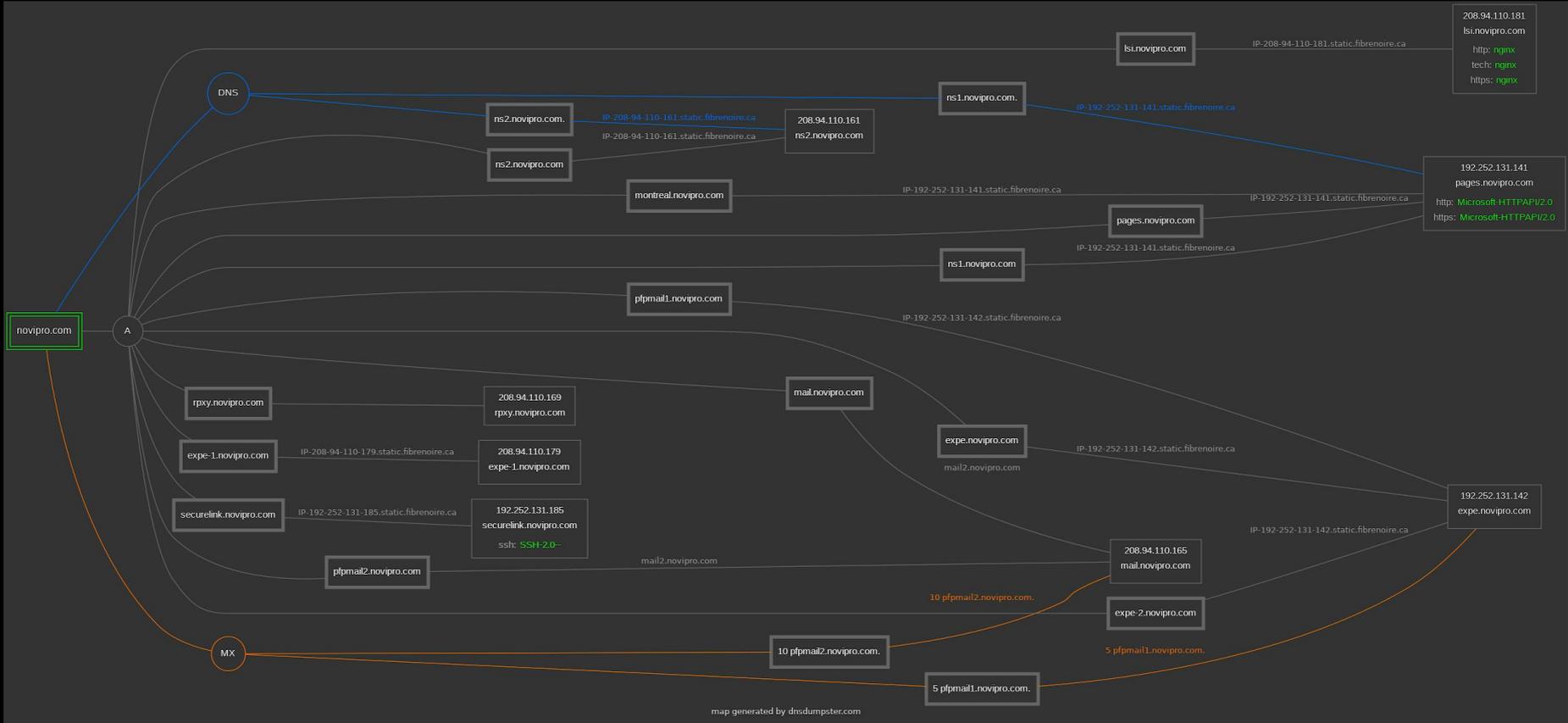
Surface d'attaque

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

Oh no — pwned!

Pwned on 11 breached sites and found no pastes (subscribe to search sensitive breaches)

Oh no — pwned!

Pwned on 19 breached sites and found no pastes (subscribe to search sensitive breaches)

Oh no — pwned!

Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

XSS (Censuré)





Démo Live et Rapide
Si le temps le permet!

A man is sitting in a lecture hall, pointing upwards with his right hand. The room is filled with rows of empty desks and chairs. The scene is lit with a strong blue light, and the word "Questions?" is overlaid in large white text across the center of the image.

Questions?