

Cybercriminalité et protection des données



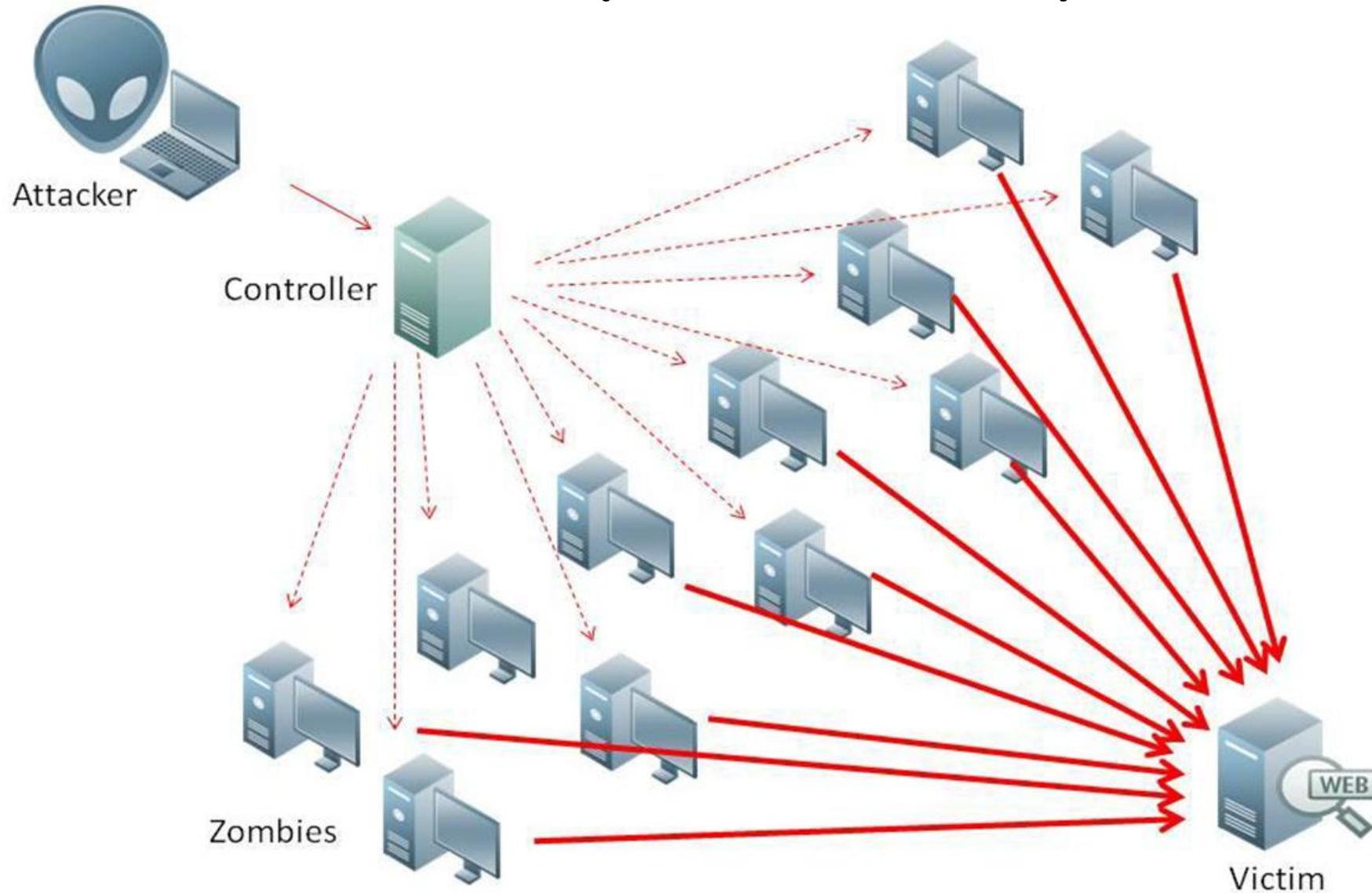
Jean-François De Rico, Langlois avocats

Et

Luc Lefebvre, Landry & Associés



1- Déni de service (ou « DDoS »)



LCCJTI – C-I-A



TÉLÉCOMMUNICATIONS XITTEL INC.

et

9116-6033 QUÉBEC INC., société légalement constituée faisant affaires sous le nom
de **LES SYSTÈMES INFORMATIQUES CONCEPTA**
Demanderesses

c.

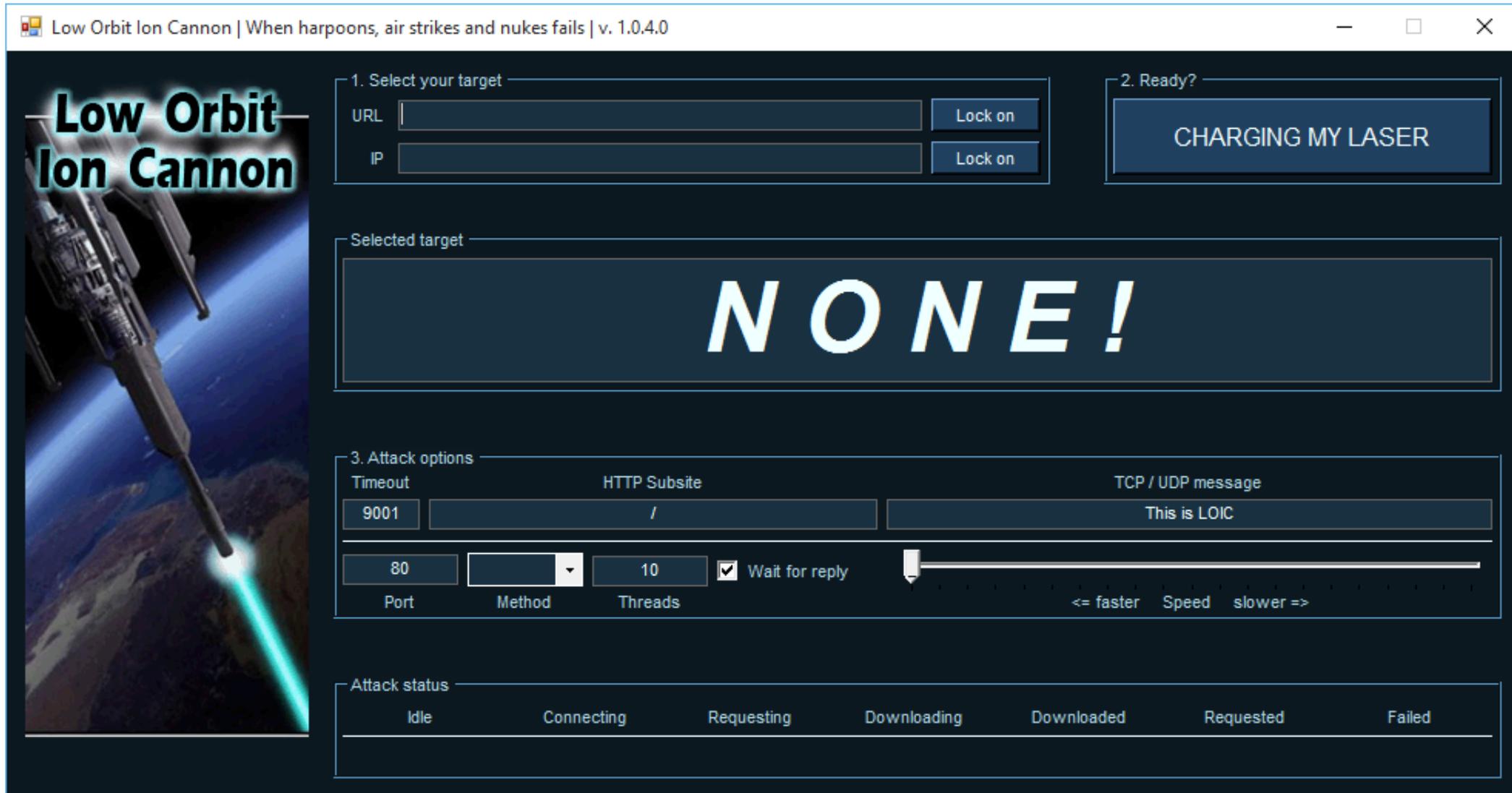
KEVIN COURTOIS



1- « DDoS » - services



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.4.0



The image shows the graphical user interface of the Low Orbit Ion Cannon (LOIC) tool. On the left, there is a vertical banner with the text 'Low Orbit Ion Cannon' and an image of a futuristic space weapon firing a blue laser beam. The main interface is divided into several sections:

- 1. Select your target:** Contains two input fields for 'URL' and 'IP', each with a 'Lock on' button.
- 2. Ready?:** A large blue button labeled 'CHARGING MY LASER'.
- Selected target:** A large dark box with the word 'NONE!' written in white, indicating that no target has been selected.
- 3. Attack options:** A section for configuring the attack. It includes:
 - Timeout:** A field set to '9001'.
 - HTTP Subsite:** A field containing a forward slash '/'.
 - TCP / UDP message:** A field containing the text 'This is LOIC'.
 - Port:** A field set to '80'.
 - Method:** A dropdown menu.
 - Threads:** A field set to '10'.
 - Wait for reply:** A checked checkbox.
 - Speed:** A horizontal slider with labels '<= faster', 'Speed', and 'slower =>'.
- Attack status:** A progress bar at the bottom with seven stages: 'Idle', 'Connecting', 'Requesting', 'Downloading', 'Downloaded', 'Requested', and 'Failed'.

1- « DDoS » - services



RAGE BOOTER HOME ABOUT US PLANS & PRICING FEATURES CONTACT US LOGIN PAGE

FEATURES

 Unlimited Testing

 Great User Experience

 24/7 Live Support

 Easy Customizable

 Flexible Pricing

 VIP Support

 Affordable Plans

 Money Back Guarantee

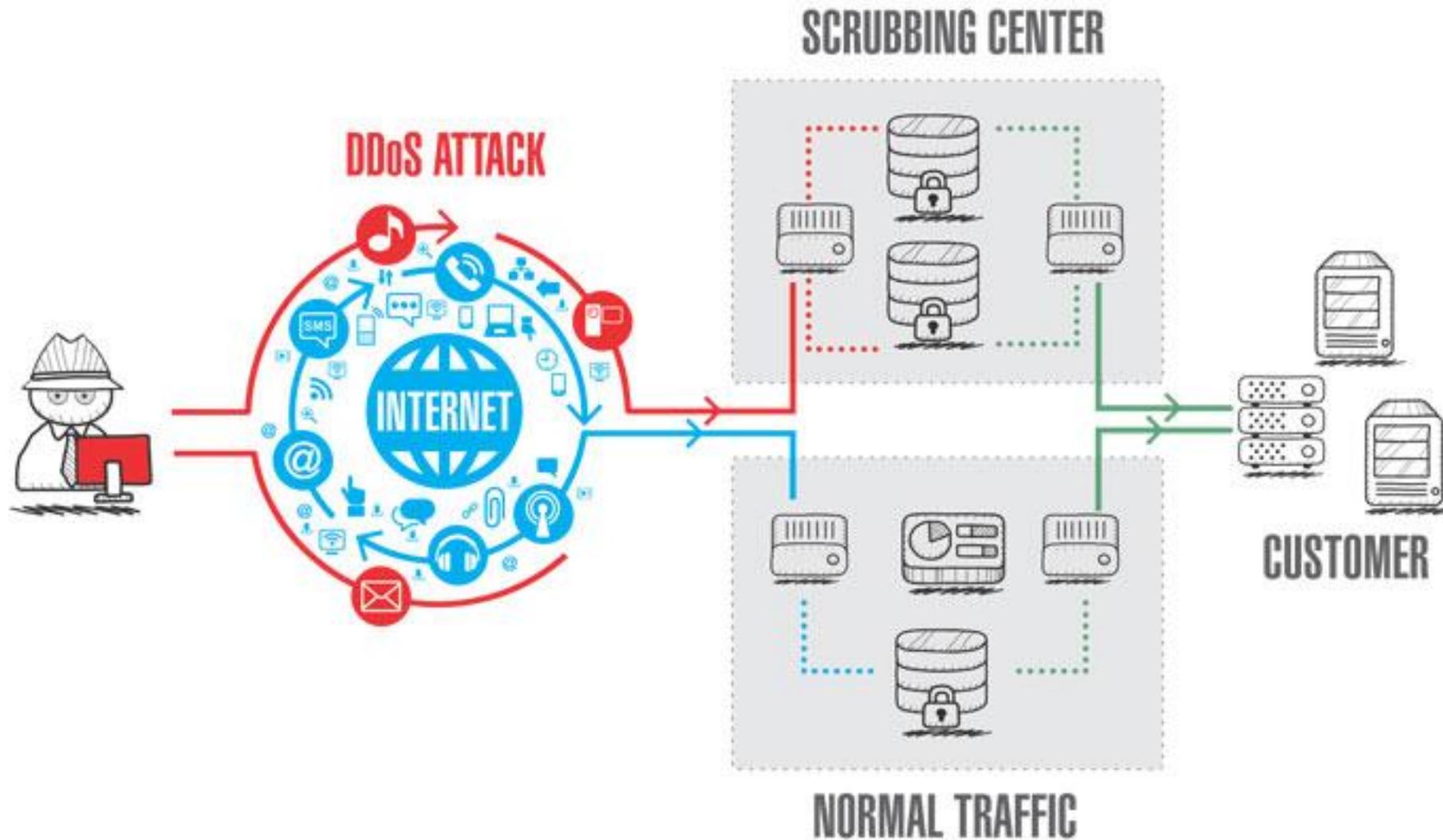
Excellent Stress Testing Services!
With Rage Booter, you never have to worry about power! We monitor our servers 24/7 to provide you a pure and strong attack to any target.

- ✓ Fast and Secure Stress Testing!
- ✓ Ticket & Live Support!
- ✓ A Variety of revolvers from Cloudflare to Skype, we have it all!
- ✓ We have been open since 2010 so you can feel peace at mind that we are not going anywhere!

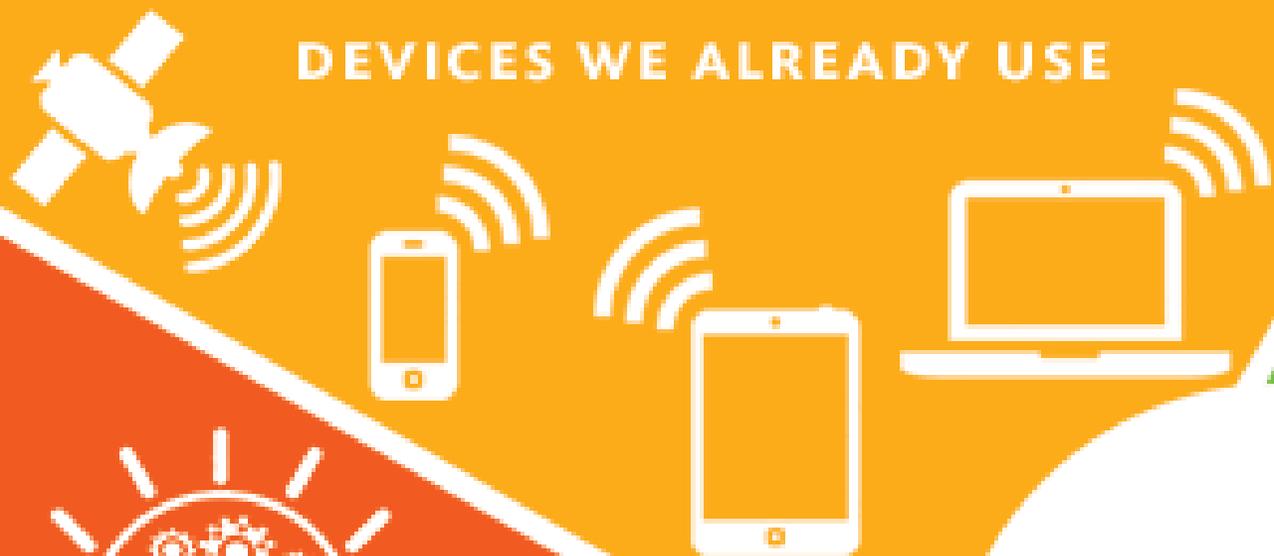
Instant Attacks!
Unlike other stressers who use SSH2, We utilize IRC (Internet Relay chat) to send all attacks. Attacks are instant and sent fast using this.

IF YOU HAVE ANY QUESTIONS? [CONTACT SUPPORT](#)

1- « DDoS » - mitigation



DEVICES WE ALREADY USE



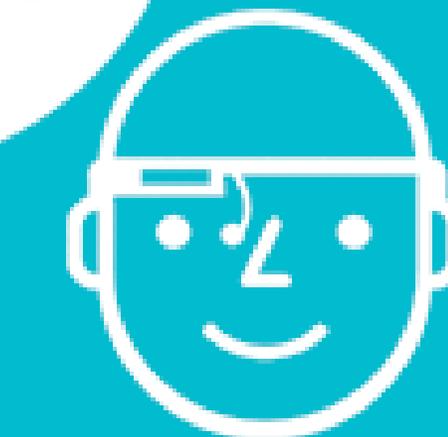
DEVICES USING
CONNECTIVITY IN
NEW WAYS



Internet of things

CAPITA

DEVICES PREVIOUSLY
INACTIVE, BUT NOW
INTELLIGENT



COMPLETELY NEW DEVICES

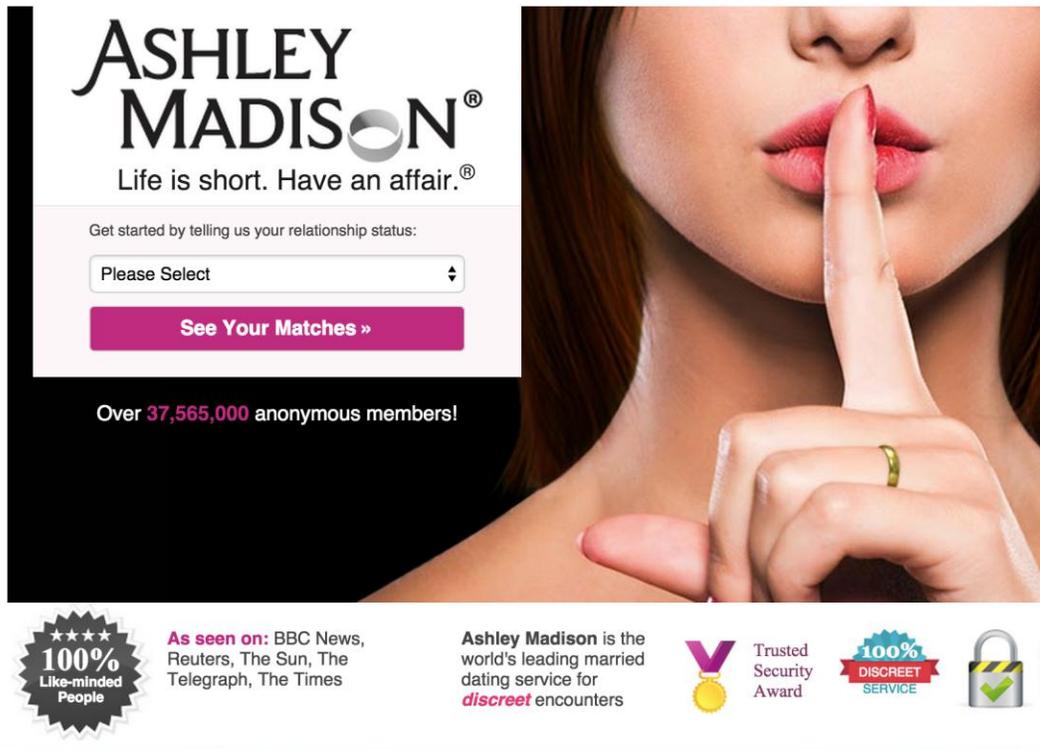
1- « DDoS » - responsabilité



En janvier 2012, un hacker a identifié une faille dans la sécurité d'un système de télésurveillance , qui a ensuite été exploitée par des "confrères" qui ont diffusé/rendu accessible le contenu de 700 caméras.



2- Intrusion et sécurité des bases de données



ASHLEY MADISON
Life is short. Have an affair.[®]

Get started by telling us your relationship status:

Please Select

See Your Matches »

Over **37,565,000** anonymous members!

★★★★★
100%
Like-minded People

As seen on: BBC News, Reuters, The Sun, The Telegraph, The Times

Ashley Madison is the world's leading married dating service for **discreet** encounters

Trusted Security Award

100% DISCREET SERVICE

Have I Been Pwned (Troy Hunt) [AU] | <https://haveibeenpwned.com/PwnedWebsites>

accounts	790,724	Brazzers accounts	
myspace 359,420,698	MySpace accounts	777,387	Black Hat World accounts
网易 NetEase 234,842,089	NetEase accounts	745,355	Android Forums accounts
in 164,611,595	LinkedIn accounts	738,556	WildStar accounts
152,445,165	Adobe accounts	699,793	mSpy accounts
badoo 112,005,531	Badoo accounts	657,001	PokéBip accounts
vk 93,338,602	VK accounts	648,231	Domino's accounts
Рамблер/ 91,436,280	Rambler accounts	620,677	Final Fantasy Shrine accounts
dropbox 68,648,009	Dropbox accounts	616,882	Comcast accounts
tumblr. 65,469,298	tumblr accounts	612,414	ThisHabbo Forum accounts
Modern Business Solutions 58,843,488	Modern Business Solutions accounts	611,070	HLTV accounts
zoosk 52,578,183	Zoosk accounts	599,080	Nulled accounts
iMesh 49,467,477	iMesh accounts	590,954	Paddy Power accounts
Fling.com 40,767,652	Fling accounts	583,503	CloudPets accounts
last.fm 37,217,682	Last.fm accounts	568,340	BTC-E accounts
NETPROSPEX 33,698,126	NetProspex accounts	530,270	Battlefield Heroes accounts
32,939,105	SC Daily Phone Spam List accounts	530,147	Unreal Engine accounts
30,811,934	Ashley Madison accounts	518,966	vBulletin accounts

2- Intrusion et sécurité des bases de données



[*] HACKED BY Cyber Islamic State [*]

لا إله إلا الله

الله
رسول
محمد

[*] HACKED BY Cyber Islamic State [*]

Read This,

Soon, soon, you will see the wondrous sight, A fierce conflict. And you will see, There will be battles in the heart of your abode. To destroy you, my sword has been sharpened. We have marched by night, to cut and slaughter. By the knife of revenge is a road for whoever is suitable. With the spears of night and the young men of ferocity, And an explosion of war, that he may be defeated. You have begun to fight me with the ally of shelter, so taste my curse when it has fired up. You will remain for a while, and you will suffer in my war. With what will you meet a youth made mighty? When the horse has reared, raised its head, and leaped forth, Then it has become a lighted blaze, The bullets blaze, the revenge has come. So where is the escape from the sparks of the mortals? We will come to you with slaughter and death. With fright and silence we will tear the bonds. You have failed publicly, so taste loss. And return in flight, under cover of night. When disbelief has agitated, frothed, and stirred up. We have filled the roads with red blood. With the darkness of bayonets, with the striking of the necks, To heap up the dogs when they murther. We have come, we have come, we have marched with determination. In surmount we have striven to ascend the peaks. We embark on the deaths, we close ranks. We die standing, as lions of courage. **expect us!**

We Are : /Moustanika Attackwe - /L'Alouk-Da - /DooMxam

Khilafah Will Transform The World

LCCJTI – C-I-A

2- Intrusion et sécurité des bases de données



- **Tests d'intrusions (pentests)**
 - Hackers éthiques
 - Standards à suivre : ISO 27000, PCI DSS
 - Méthodologies à suivre: NIST framework, OWASP
- **Pour éviter dans le futur?**
 - Chiffrement
 - Audit indépendant
 - Rapport de transparence
 - Modèle d'affaire

2- Intrusion et sécurité des bases de données



UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data
Security Breach Litigation

MDL No. 14-2522 (PAM/JJK)

This Document Relates to:
All Financial Institutions Cases

**CONSOLIDATED CLASS
ACTION COMPLAINT**

Umpqua Bank, Mutual Bank, Village Bank,
CSE Federal Credit Union, and First
Federal Savings of Lorain, Individually and
on behalf of a class of all similarly situated
financial institutions in the United States,

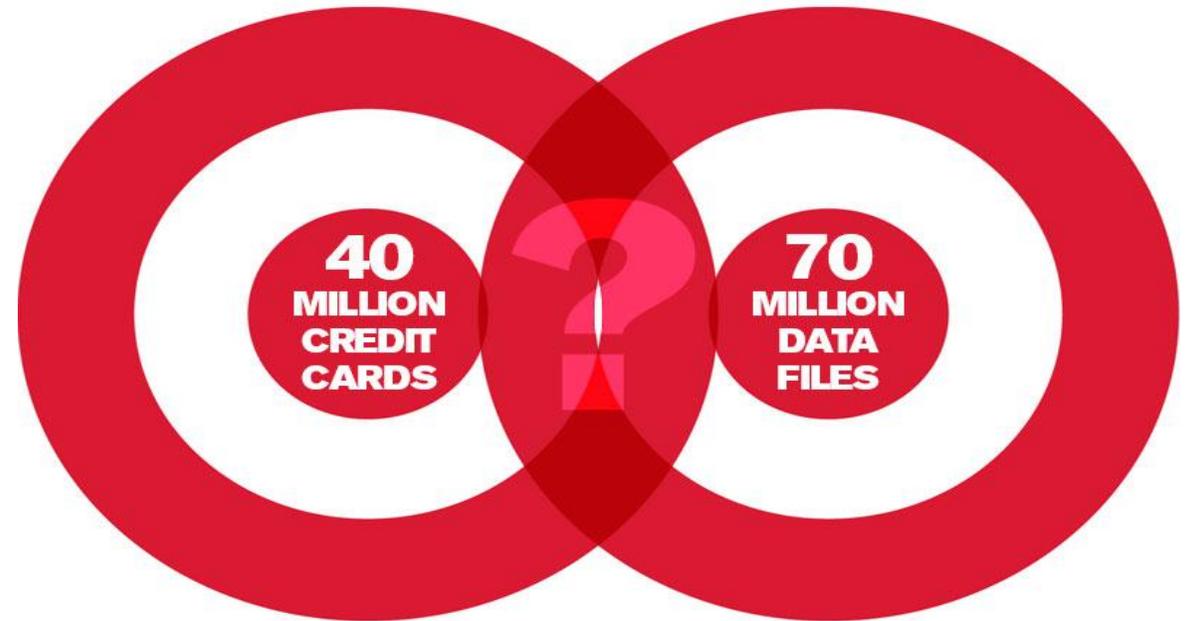
Plaintiffs,

JURY TRIAL DEMANDED

v.

Target Corporation,

Defendant.





In re: Target Corporation Customer Data Security Breach Litigation,

RÉGLEMENTS INTERVENUS

- \$39 million avec les banques visées par le recours collectif
- \$67 million avec VISA
- \$10 million avec des clients

AM AND EM MUST SHUT DOWN IMMEDIATELY PERMANENTLY



**We are the Impact Team.
We have taken over all systems in your entire office and production domains,
all customer information databases, source code repositories, financial records, emails**

**Shutting down AM and EM will cost you, but non-compliance will cost you more:
We will release all customer records, profiles with all the customers' secret
sexual fantasies, nude pictures, and conversations and matching credit card
transactions, real names and addresses, and employee documents and emails.
Avid Life Media will be liable for fraud and extreme harm to millions of users.**

Avid Life Media runs Ashley Madison, the internet's #1 cheating site, for people who are married or in a relationship to have an affair. ALM also runs Established Men, a prostitution/human trafficking website for rich men to pay for sex, as well as cougar life, a dating website for cougars, man crunch, a site for gay dating, swappernet for swingers, and the big and the beautiful, for overweight dating.

Trevor, ALM's CTO once said "Protection of personal information" was his biggest "critical success factors" and "I would hate to see our systems hacked and/or the leak of personal information"

Well Trevor, welcome to your worst fucking nightmare.

We are the Impact Team. We have hacked them completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all

2- Intrusion et sécurité des bases de données



CRITÈRES D'ANALYSE:

- Les mesures de sécurité doivent être proportionnellement élevées:
 - Sensibilité des renseignements personnels détenus par ALM
 - Conséquences négatives prévisibles pour les utilisateurs du piratage de leurs RP
 - Déclarations faites par ALM en ce qui a trait à la sécurité de ses systèmes d'information,

QUESTIONS:

- L'organisation avait-elle un motif raisonnable pour conserver les renseignements personnels touchés par la brèche?
- L'organisation conservait-elle les renseignements conformément à la LPRPDÉ et à la PIPA?
- L'organisation avait-elle mis en place des mesures de sécurité raisonnables afin de protéger les renseignements personnels qu'elle conservait?
- Examen:
 - Étendue et conformité de la conservation
 - Mesures de protection de sécurité sans fil en place au moment de la brèche
 - Mesures adoptées après l'incident

3- L'hameçonnage et l'harponnage

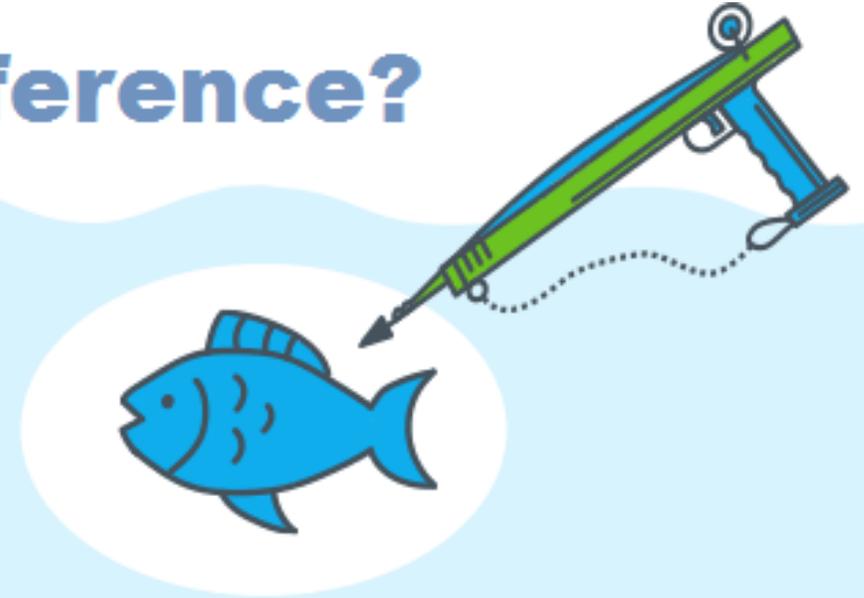


What's The Difference?



PHISHING

IS A BROAD, AUTOMATED ATTACK
THAT IS LESS SOPHISTICATED.



SPEAR-PHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC
EMPLOYEE & COMPANY

3- L'hameçonnage et l'harponnage

exemples



From: Desjardins <server@localhost.com> on behalf of Sent: Mon 13/01/2014 12:41 PM
To: @sheridanc.on.ca
Cc:
Subject: C'est une alerte pour vous aider à gérer votre compte en ligne

Desjardins AccèsD

Membres AccesD
Chers Membres AccesD: Particuliers et Entreprises
Nous avons récemment déterminé que votre compte en ligne AccesD est sur le point d'expirer. Pour conserver votre compte en ligne actif, vous devez vous identifier dès maintenant. Nous apprécions votre appui et support, car nous travaillons tous ensemble pour conserver les solutions en ligne au particulier un endroit sûr pour y effectuer ses transactions. Veuillez vous identifier en suivant ce lien:

[Faites la mise à jour dès maintenant en appuyant ici !](#)

Conjuguer avoirs et êtres
Generic non-personalized greeting
Copyright © 2014 Mouvement des caisses Desjardins. Tous droits réservés.

Desjardins AccèsD

Dear Members AccesD: Individuals and Companies
We have recently determined that your account online AccesD is about to expire. You must identify now to keep your account active online. We appreciate your support and support as we work together to keep online solutions to a particular place in order to carry out its transactions. Please log in by following this link:

[Please log in by following this link !](#)

Conjuguer avoirs et êtres
Copyright © 2014 Mouvement des caisses Desjardins. Tous droits réservés.
Hovering over the link reveals it points to a non-Desjardins site -
"http://www.pjmwilliams.com/content/wp-admin/images/screenshots/index.htm"

3- L'hameçonnage et l'harponnage

exemples



www.lapresse.ca/actualites/201701/19/01-5061353-comment-un-escroc-a-vole-55-millions-a-la-coop-federee.php

maPRESSE

Découvrez Ma Presse

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



La Coop fédérée est propriétaire notamment des quincailleries BMR et des marques de viandes Olymel. Son chiffre d'affaires avoisine les 10 milliards de dollars annuels.

4- Le rançongiciel



All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC \approx 550 USD.

Your Bitcoin address for payment: [1215PkwP2989wA752yK21A9W4C46vKz8M](#)

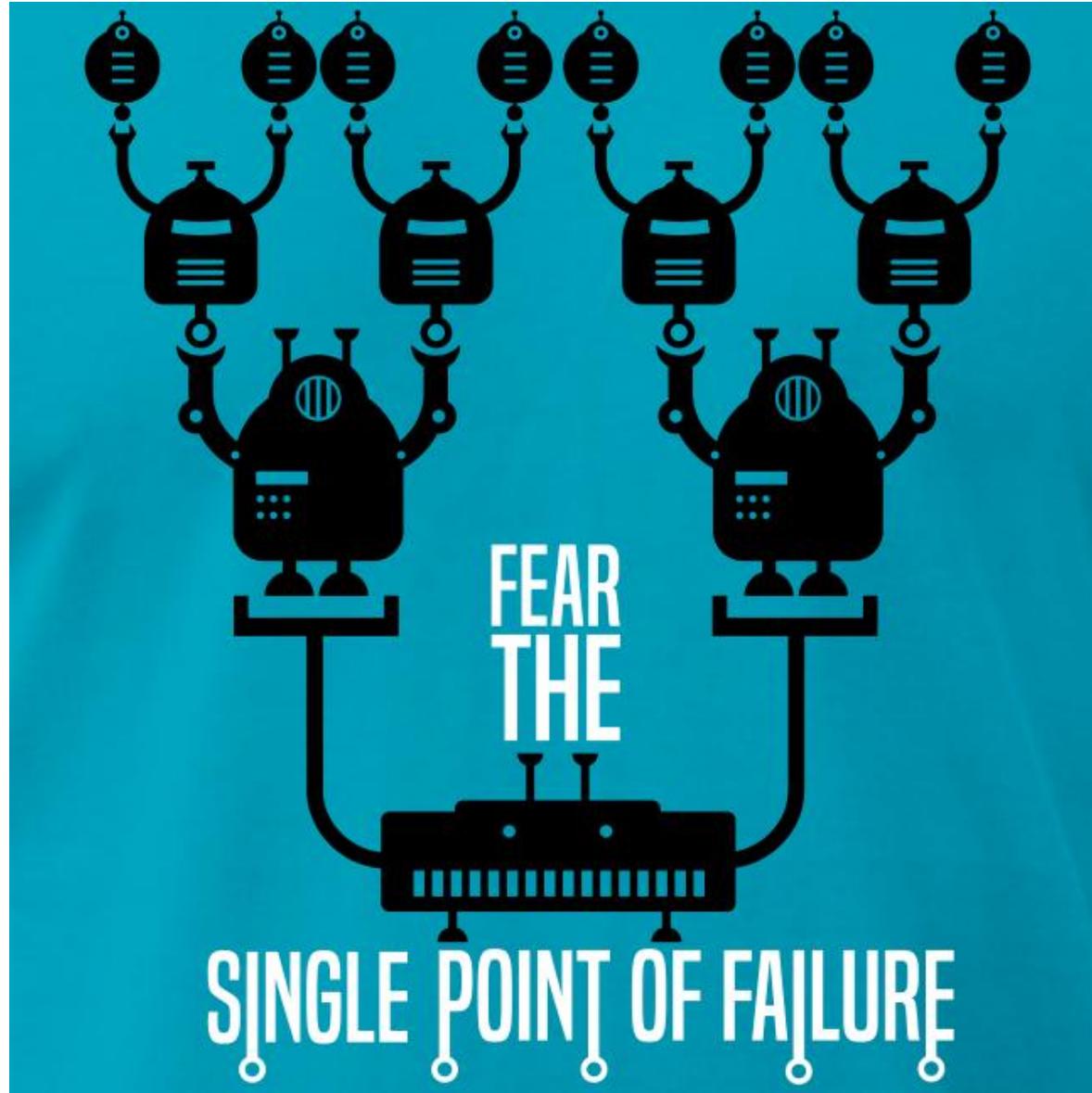
\$ PURCHASE PRIVATE KEY
WITH BITCOIN

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

4- Le rançongiciel

points faibles



4- Le rançongiciel

points faibles



4- Le rançongiciel

Assurance cyber-risques



Méthodes de prévention

- Solution techniques
 - Black list
 - Antivirus
 - Sandbox
- Formation et sensibilisation
- Tests

4- Le rançongiciel

Assurance cyber-risques



COUVERTURES MULTIPLES

- Les réclamations de tiers liées à des intrusions dans nos systèmes informatiques, incluant les réclamations liées au défaut de protéger la confidentialité des données (pour autant que cela ne fasse pas déjà partie de notre police responsabilité)
- Les coûts liés à la gestion de crise (professionnels de l'informatique, recouvrement de données, relations publiques, suivi de crédit des clients affectés, etc...)
- Coût associés à une demande de rançon par un pirate
- Pertes de revenus en raison de l'interruption d'accès aux systèmes informatiques

4- Le rançongiciel



Information
Application générale
CcQ

Obligations
contractuelles

Protection des
renseignements
personnels

Responsabilité civile

Règlements et normes
sectorielles

Criminel

télécommunications

4- Le rançongiciel



Mars 2016

**Règlement sur la notification et la
déclaration des atteintes à la pro-
tection des données**

4- Le rançongiciel

A large blue rectangular area with a pattern of white circles of varying sizes and opacities, some overlapping. A white text box is positioned in the lower right corner of this area.

Orientations gouvernementales
pour un gouvernement plus
transparent, dans le respect du
droit à la vie privée et la protection
des renseignements personnels

4- Le rançongiciel –

Principes directeurs pour les conseils d'administrations

- 1. **Understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.**
- 2. Directors should **understand the legal implications** of cyber risks
- 3. Boards should have **adequate access to cybersecurity expertise**, and it should be on the agenda and discussed.
- 4. Directors should **set the expectation that management will establish an enterprise-wide risk management framework** with adequate staffing and budget.
- 5. Board-management discussion of cyber risk should include **identification of which risks to avoid, accept, mitigate, or transfer through insurance**, as well as specific plans associated with each approach.



Questions?



- Jean-François De Rico

- Courriel: jean-francois.derico@langlois.ca
- Tél: 418-650-7923 & 514-842-9512
- Site Web: www.langlois.ca
- LinkedIn: www.linkedin.com/in/jfderico
- Twitter: @jfderico

- Luc Lefebvre

- Courriel: luc.lefebvre@landryconsulting.com
- Tél: 514-924-6726
- Site Web: www.landryconsulting.com
- LinkedIn: ca.linkedin.com/in/luclefebvre
- Twitter: @luclefebvre



LANGLOIS

AVOCATS - LAWYERS

LANDRY

+ associés | associates

**NE RIEN
LAISSER
AU HASARD®**