



# Autopsie d'une attaque de ransomware

David Hétu | Chef de la recherche, Flare Systems inc.

Matthieu Chouinard | Président et chef de la direction / CEO chez In Fidem & Forensik

Juillet 2020

Évolution

Infection

Modèles  
d'affaires

Étude de cas

## Notre **mission**

Comprendre la **chaîne d'attaque** des ransomwares et **apprendre des meilleures stratégies** de prévention

# Introduction

# Une evolution **inquiétante** et au fort potentiel de **perturbation**



Des rançons qui  
deviennent de plus en  
plus **dispendieuses**

## Baltimore transfers \$6 million to pay for ransomware attack considers insurance against hacks



By LUKE BROADWATER

BALTIMORE SUN | AUG 28, 2019 AT 12:32 PM



# Des ransomwares qui font bien **plus que** **demandeur des rançons**

- Vol de mots de passes
  - Fureteurs
  - FTP
  - Messageries instantannées
  - Courriels
  - Windows RDP
- Vol de fichiers
- Vol de l'historique de navigation
- Vol de *cookies*
- Vol de clés privées de portefeuilles
- Enregistreur de frappe
- Enregistreur vidéo
- Console de commande
- Nettoyage de logiciels malveillants
- Élévation de compte
- Persistance
- Alertes par Jabber

# Des enchères pour mettre de la **pression**, augmenter les **profits**

## Group

Group is a group of companies engaged in crop production and agriculture in Canada.

Contains accounting documents, and accounts, plus a lot of important information that may be of value to competitors or interested parties. All files of actual information. Also in the archive you will get several databases that are no less interesting.

Archive in zip format

1. Files pdf,docx,xlsx - 22328
2. Database - 3

When the auction is over, you will be provided with a download link from the cloud with the following deletion.















<b>Minimum deposit:</b>	\$5,000	<b>Top bet:</b>	--
<b>Start price:</b>	\$50,000	<b>Blitz price:</b>	\$100,000

**Not paid** The secret data of the lot has been published :)

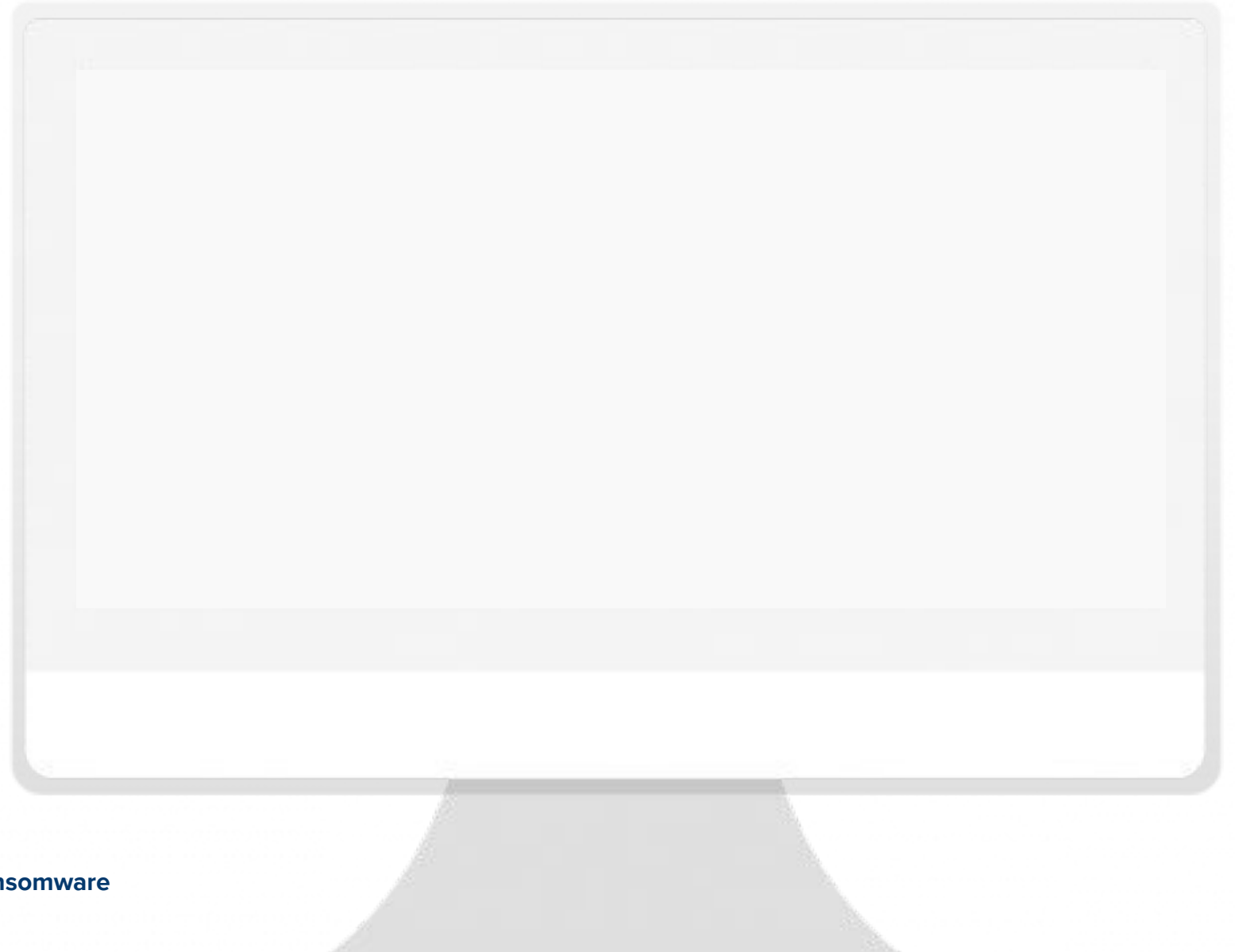


Des attaques de plus en plus difficiles à détecter selon [dyncheck.com](https://dyncheck.com)

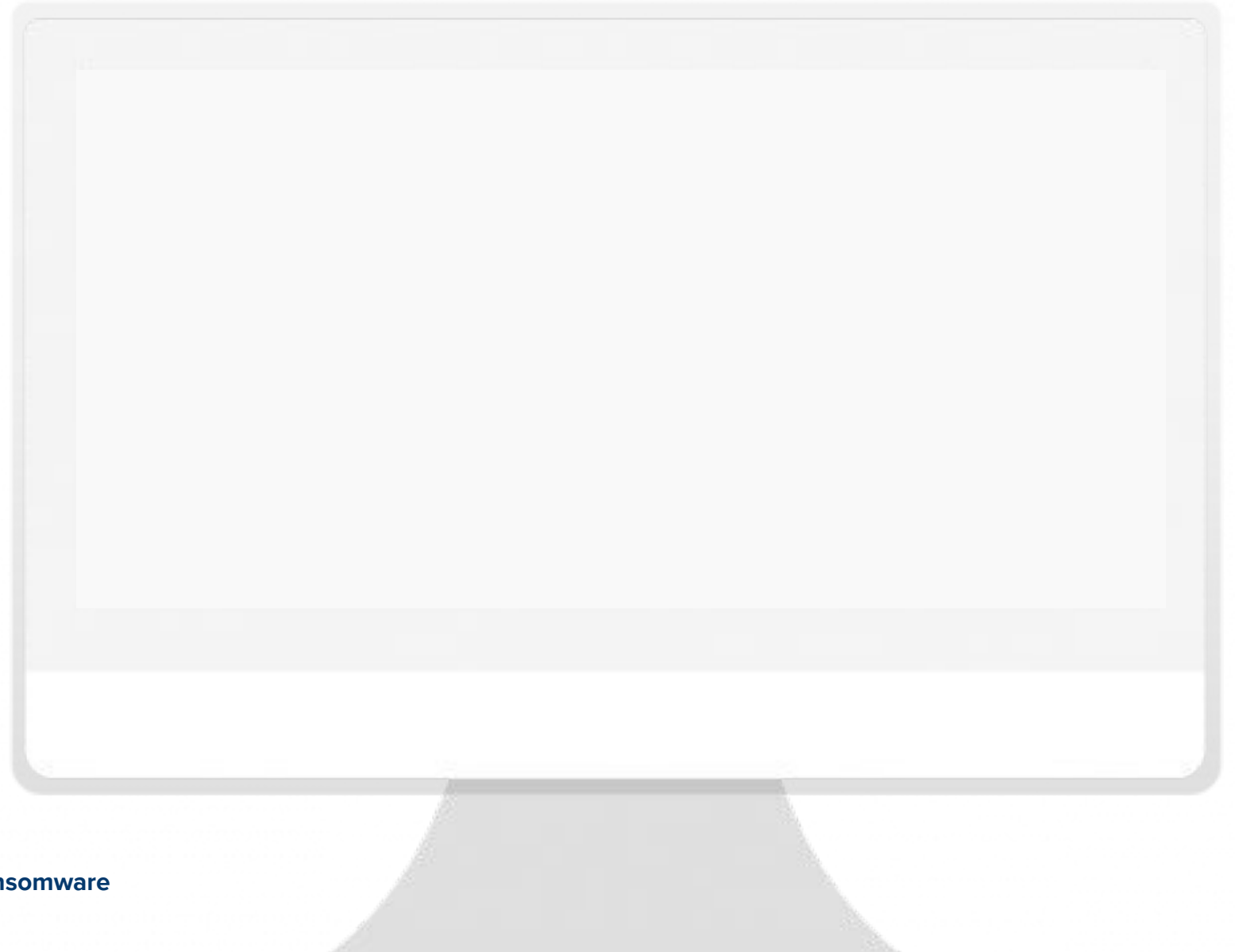
✓ Result Detection rate: 1/23

AV	Status	Alert Screen
 360 Total Security Essential	Clean	
 AVG Internet Security	Clean	
 AhnLab V3 Light	Clean	
 Avast Internet Security	Clean	
 Avira Internet Security	Clean	
 BitDefender Total Security	Clean	
 BullGuard Internet Security	Clean	

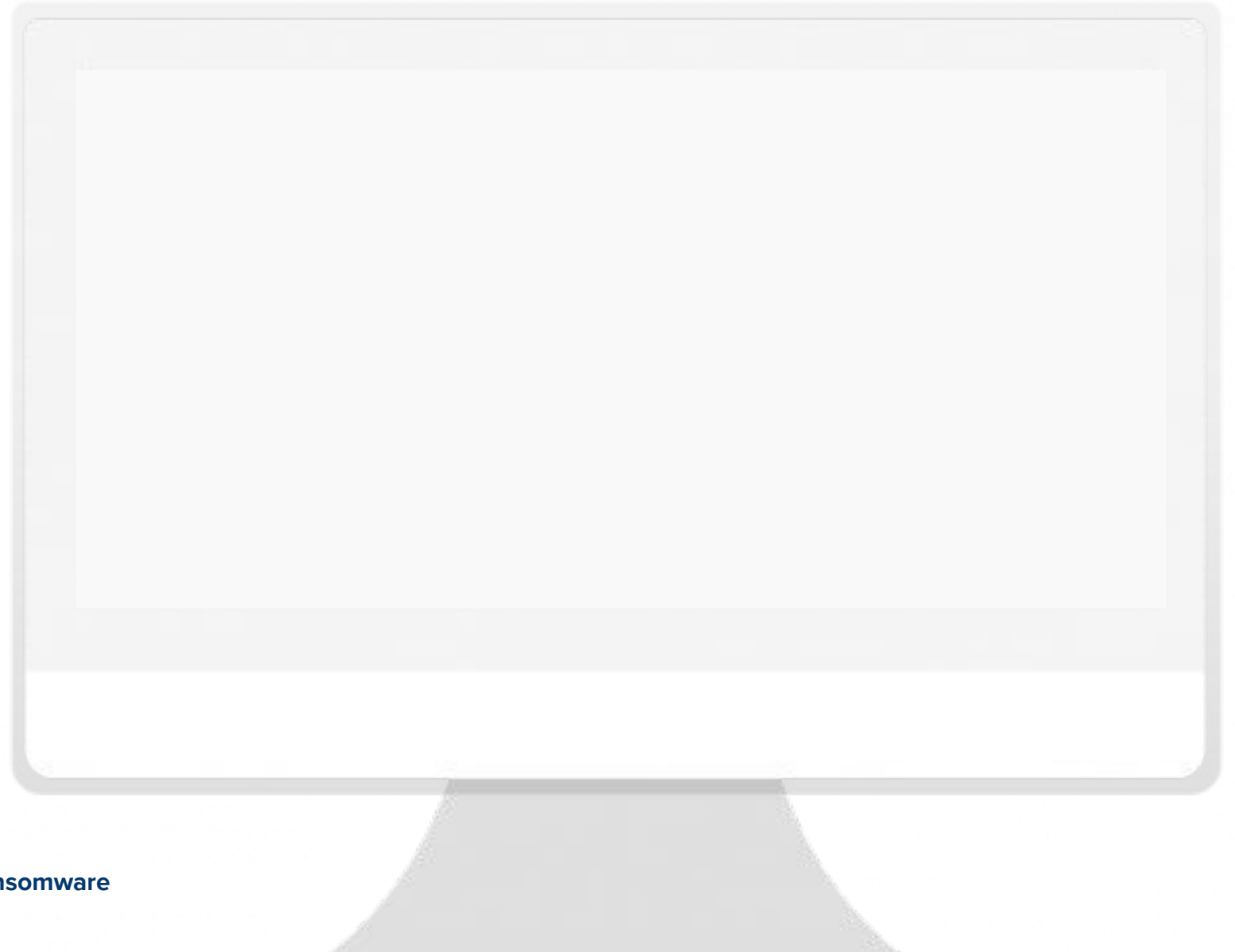
**Des attaques de  
plus en plus  
difficiles à bloquer**



# Des attaques de plus en plus difficiles à bloquer (2)



# Des attaques de plus en plus difficiles à investiguer

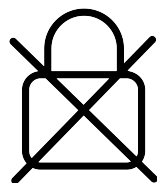


# Les vecteurs d'infection

# Des vecteurs d'infection diversifiés



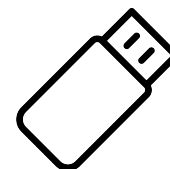
Spam par courriel,  
SMS



Attaque de RDP



Infection de site web



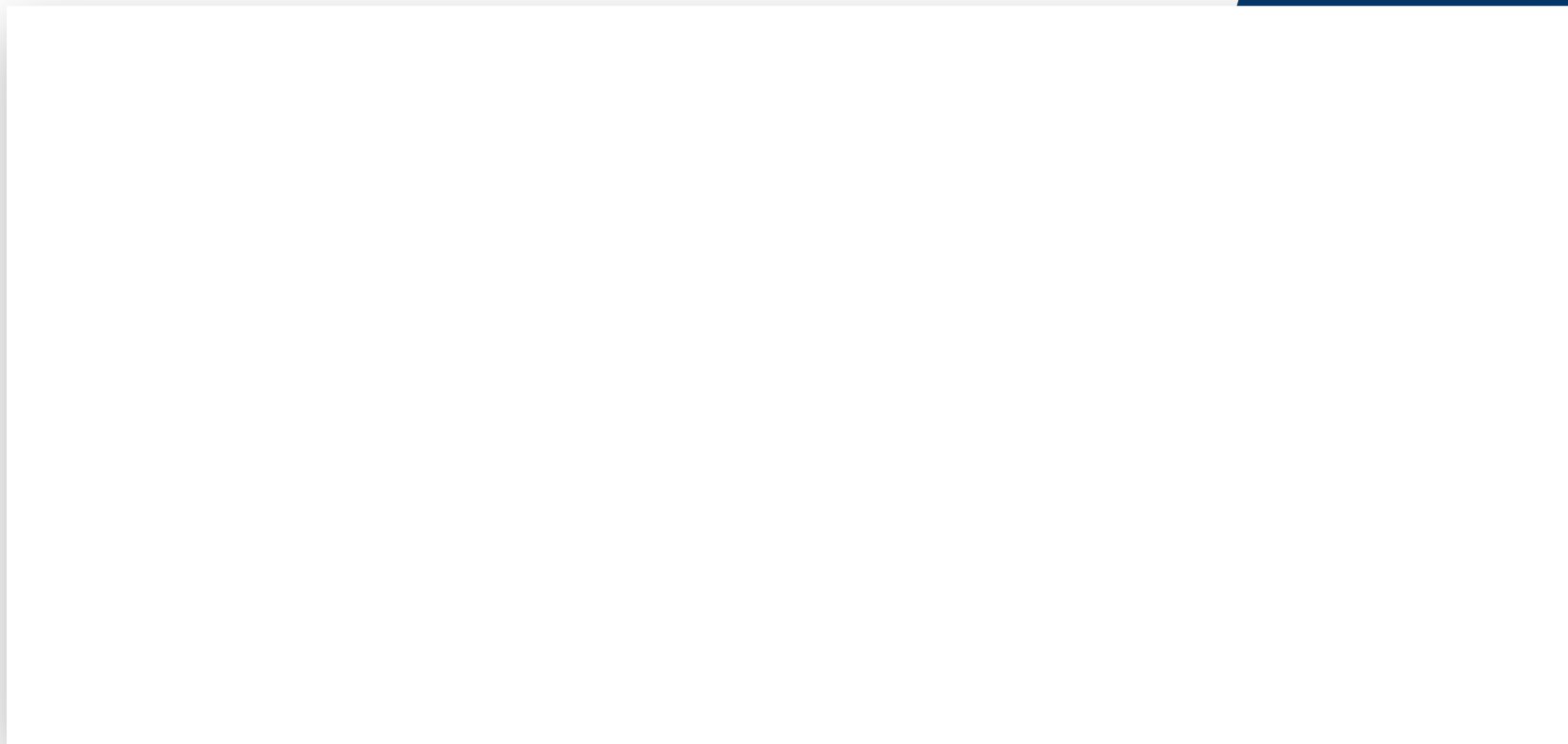
USB



Réseau local

# Les modèles d'affaires

# Développement en communauté





# Quand même nécessaire de recourir à des services connexes



## Coûts d'achat et de location de ransomwares

Acteurs malicieux offrent des forfaits

**USD\$2,500**

Coût pour **acheter un SaaS** avec mise à jour hebdomadaire ou mensuelle

**USD\$800**

Coût de location **par mois** pour un SaaS

**USD\$250 / 35%**

Coût **par machine infectée** pour les services hébergés



# RÉPONSE AUX INCIDENTS NUMÉRIQUES ET CYBERATTAQUES AUTOPSIE D'UNE ATTAQUE DE RANSOMWARE

9 JUILLET 2020 – WEBINAIRE IN FIDEM ET FLARE SYSTEMS

# QUI SUIS-JE?

## Matthieu Chouinard

Président et CEO

Équipe de Réponses aux  
Incidents et Cyberenquête  
Forensik inc. et In Fidem inc.



Entrepreneur

Vice-président In-Sec-M

22 ans en cybersécurité



+

+

# LE CONTEXTE

+

+

+

# PREMIERS SYMPTÔMES

Vendredi  
20 décembre  
4h22



“Check ça,  
il y a un problème”

L'administrateur essaie  
de comprendre ce qui  
se passe, l'étendu des  
dommages.

Il essaie de savoir si tout est  
chiffré, espère que c'est  
localisé et que certains sont  
récupérables.

# Demande de rançon



To unlock files, you need to pay 43 bitcoin.

To confirm our honest intentions, we will unlock two files for free.

Send us 2 different random files and you will get it back already decrypted.

You can choose files from different computers on your network - so you will be sure that one key decrypts everything.

Files size should not exceed 5Mb.

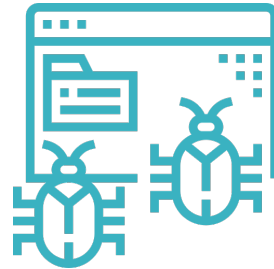
Waiting for 43 bitcoin to close the problem. Then you will receive decryption software that would completely recover all your files.

It's simple windows executable that needs Administrator privileges to be used. The cure procedure contains next steps:

- 1) Turn off any AV running;
- 2) Turn off internet connection (it will help to avoid any improper decryption - question of your safety);
- 3) Start that exe on each workstation or server; wait for it's prompt that "operation complete" (it takes time depending on amount of data on current system)
- 4) Check that all is fine and get back to normal work.

# LE CHOC

Vendredi  
20 décembre  
5h35



HOUSTON :  
"nous avons un gros problème"

Ryuk est partout  
sur tous les postes  
et tous les serveurs  
Windows

Début de l'escalade



# PANIQUE À BORD



Évaluation des  
dommages

Aucun serveur, ni  
système  
fonctionnel

Plein de questions,  
peu de réponses. Par  
où commencer?

Seul espoir :  
le back up sur tape  
est ok

# L'ESCALADE ET LE PLAN



Mais, quel plan?

Plein de questions.  
Peu de réponses

On improvise

# TENTATIVE DE RÉTABLIR DES OPÉRATIONS



Essayer par soi-même



Essais / erreurs



Attention : *ne pas tomber en détresse* (perte de contrôle) vs *être en stress* (sentiment d'urgence)

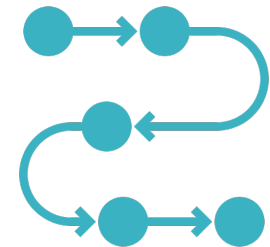
**EMERGENCY**

**STRESS EN  
GESTION  
D'INCIDENTS**



# APPEL DE DÉTRESSE QUI ENTRE EN JEU

Vendredi  
20 décembre  
14h20

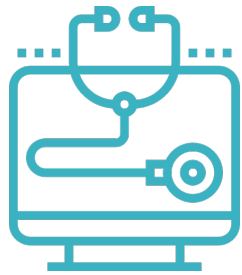


Le triage

Quel est le statut  
des systèmes?

À quelle étape êtes-vous?  
Qu'avez-vous tenté, fait ou  
pas fait?

# PRISE EN CHARGE



Diagnostic et  
Organisation du travail



Ryuk = Emotet  
dans quasi la  
totalité des cas +  
autres variantes de  
maliciels



1ères instructions

# DÉPLOIEMENT D'UNE ÉQUIPE D'INTERVENTION

Vendredi  
20 décembre  
16h43

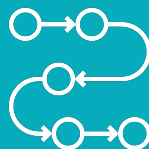


- Leader Technique DFIR
- Coordonnateur
- Équipe multi disciplinaire
- Directeur conseil
- Breach coach

# COFFRE À OUTILS



- Assigner des responsabilités
- Former
- Pratiquer
- Chasser pour confirmer/infirmier



- Simples
- Disponibles
- Connus
- Testés



- Journalisation
- Métriques
- Capture de paquets
- Indexation et synthèse des flux
- Surveillance de l'état de santé

contribuent au succès





# REPRENDRE LE CONTRÔLE

Établir les priorités



Rôles et responsabilités de tous



Sauvegarder les évidences



Valider les copies de sauvegarde



Commencer à rebâtir le réseau



# ÉCUEILS RENCONTRÉS

Temps de  
recuperation des  
copies de  
sauvegarde

Incapacité  
d'automatiser

Prioriser  
des actifs

Épuisement +  
les congés

Préserver la  
preuve vs  
remettre en état  
l'actif

# RETOUR À LA « NORMALE »

- Jeudi 2 janvier 2020, le retour aux opérations normales s'effectue tranquillement.
- **Statistiques de 2019 :**



## Demande de rançon

- Moyenne : 3 000 000\$
- Maximale : 30 000 000\$



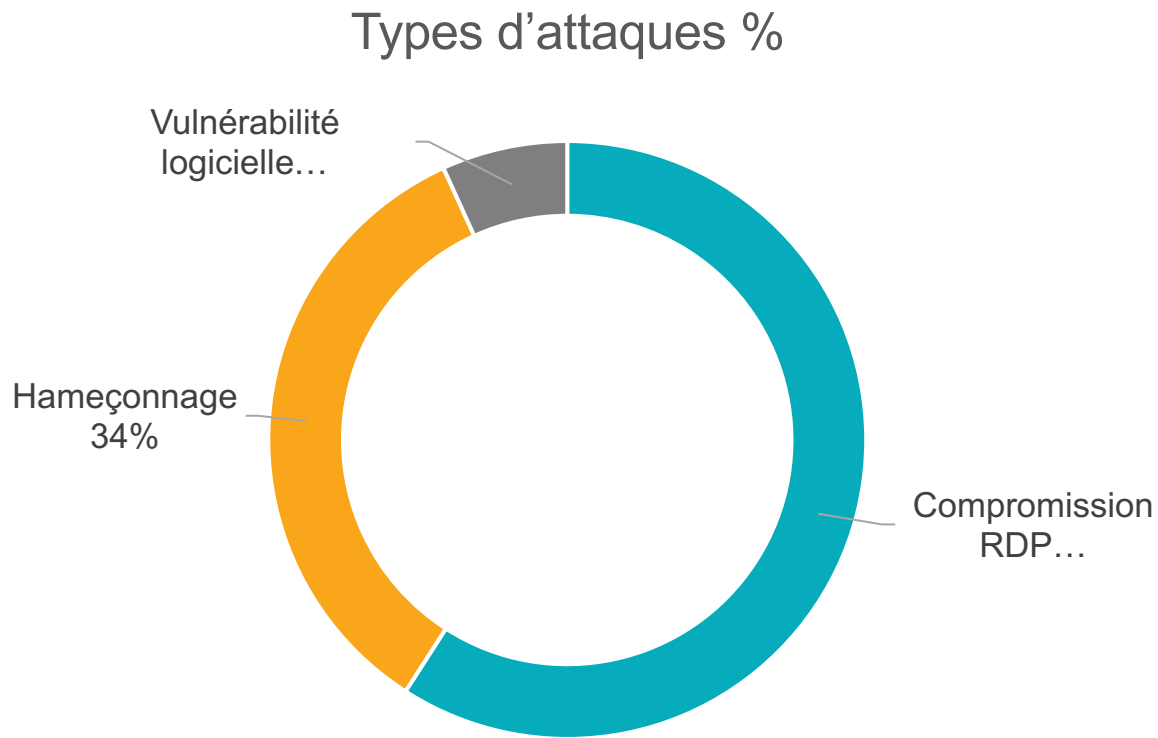
## Interruption

- Moyenne : 10 jours
- Maximale : 90 jours



Durée moyenne avant la  
détection d'une intrusion :  
206 jours

# Par quels moyens l'attaque est-elle perpétrée ?



Source : État de la menace rançongiciel, ANSSI, Janvier 2020

A close-up photograph of a person's hands interacting with a white tablet. The person is wearing a light blue shirt. The background is blurred, showing other people and a meeting environment. A semi-transparent grey rectangle is overlaid on the left side of the image. A bright orange square is overlaid on the right side, containing the text 'ENQUÊTE ET RAPPORT'. Several small grey plus signs are scattered around the image.

# ENQUÊTE ET RAPPORT

# INVESTIGATION

## Retracer l'origine de l'incident

- Patient zero
- Depuis quand
- Que s'est-il passé d'autres ?
- Y a t-il eu fuite de données ? Si oui, lesquelles ?

## Importance du rapport

- Pour la direction
- Pour les avocats
- Pour les assureurs

# Investigation

## Ryuk attack chain



Source : « Human-operated ransomware attacks: A preventable disaster »  
Microsoft Threat Protection Intelligence Team, March 5, 2020



# LEÇONS APPRIS

Contrôles de bases :

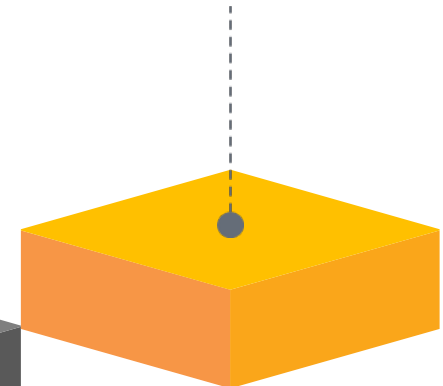
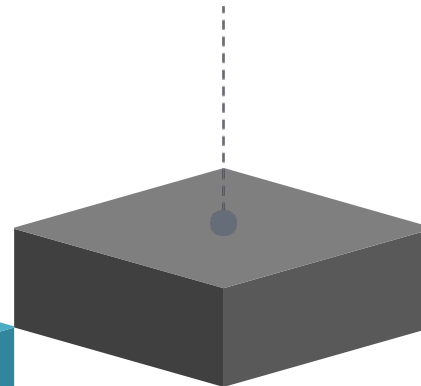
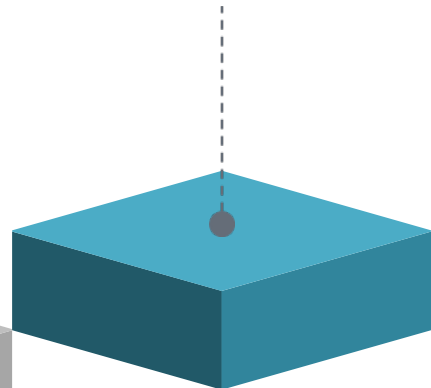
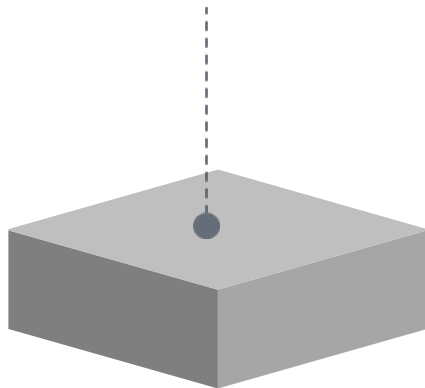
- Comptes administrateurs
- Mises à jour
- Surveillance

Avoir une copie accessible des mots de passes

Pratiquer sa capacité de relève

Priorités doivent venir de l'entreprise, pas des TI

- Actifs critiques
- Matrice de risques
- Plan de réponse





# ERREURS COURANTES D'INTERVENTION

Attendre avant  
d'appeler à l'aide

Détruire la preuve  
involontairement

Omettre de préserver des  
preuves fragiles qui donnent  
une vue unique sur les  
incidents

- La RAM change constamment
- Structure de l'OS (process, handles, ports, etc.)
- Rotation des logs
- Écrasement des enregistrements vidéo/audio



Remettre les systèmes  
dans le même état

# À PROPOS FORENSIK

Une agence en  
cybersécurité spécialisée  
en investigation numérique

- cyberenquête
- informatique judiciaire
- réponses et gestion  
d'incidents
- e-discovery



# LA FORCE DE 2 ENTREPRISES



REAKTION<sup>MC</sup>



PRÉVENTION  
STRATÉGIE

**100<sup>+</sup>**  
**EXPERTS**

# MERCI DE VOTRE PARTICIPATION

## Comment pouvons-nous vous aider?



[hello@flare.systems](mailto:hello@flare.systems) | [info@forensik.ca](mailto:info@forensik.ca)