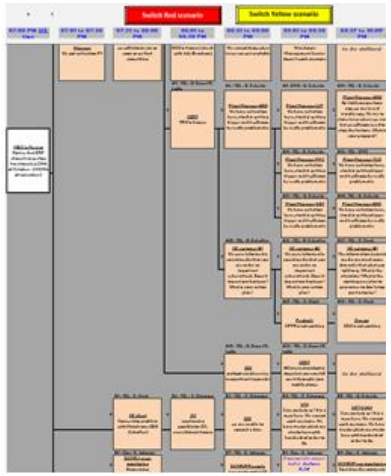
Cyber-crise : Comment évaluer la qualité de la décision ?

Pierre RAUFAST (CERT Michelin)

La crise, nous connaissons…



Mais qui a déclenché tout cela ? …

6 heures plus tôt…

Roy, le gars du CERT d'astreinte.
(tout seul)

Roy doit décider (rapidement)

Des événements

Roy
(toujours tout seul)

Ne pas déclencher de crise
Traiter en marche courante

Déclencher l'alerte

Isoler tous les sites
du réseau et d'internet

Le dilemme (urgent) de Roy

Je sais ce que je coupe
Et les impacts business

Je ne connais pas la gravité de l'attaque et ses impacts potentiels

Hydro

"The malicious virus attack caused many of Hydro's IT-systems to be shut down, not because they were infected but to contain the virus and prevent it from spreading further.

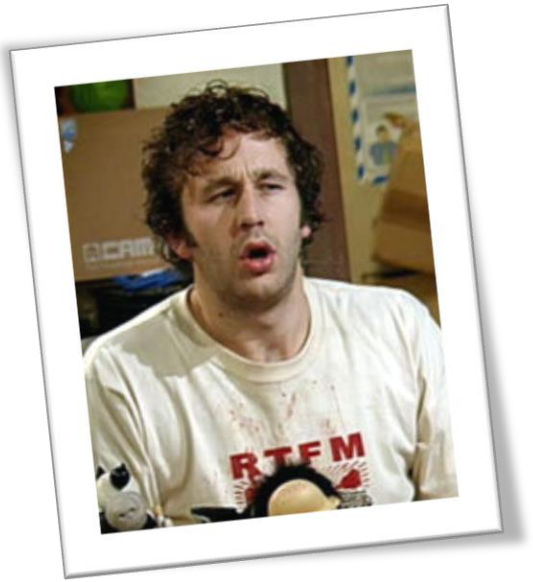
La loi de la pression

$$P.V = n.RT$$

Pression Visible
sur une équipe CERT

Nombre de Retweets

Objectifs



- Comment **préparer** Roy à ce genre de décision ?
- Comment éviter qu'il **sous-estime** ou **surestime** l'attaque ?
- Qu'est-ce qu'une bonne décision ?
- Comment ne pas perdre de temps ?

Mise en situation ludique

- **Scénario** : « Lundi 17h. Vous lisez sur Twitter que Coca-Cola et Caterpillar sont touchés par une cyber-attaque. La cyber-météo est jaune depuis ce matin à cause d'une vulnérabilité sur les bases Oracle (en cours d'étude).
  À 17h45, un article sur LeMonde.fr parle d'une 3e cible (Nestlé) sans autre détails techniques.
  Vous avez un rendez-vous privé important à 18h30. Que faites-vous ? »

- Scénario volontairement succinct, pas toutes les informations… comme dans la vraie vie
- L'objectif n'est pas une simulation de crise complète, mais de tester les décisions initiales de l'équipe CERT

Mise en situation ludique

- Qui : 2-3 analystes CERT + 1 middle manager + 1 top-manager + 1 animateur
- Règle du jeu :
  - Discussion **ouverte** sur les actions possibles
  - Pas de **bonne réponse**
  - Chacun **s'exprime** et propose
  - Chacun reste dans son **rôle**
- Déroulement
  - Calculer le « score » de l'attaque
  - Discuter / Poser des questions
  - Noter les actions prises
  - Debriefing à froid et lessons-learnt

Exercice : What do you do ?

Date		08/03/2019
Team Tested		French CERT
Story		Test #2 : We are Sunday, 1PM. The GOM calls you. They have many P1 incidents on many computers in AFMO/Dubai. People are working and they have already 25 PC down, infected by a cryptolocker. Since the morning, around 5 new cases per hour. You have the list of PC. All are protected by SEP14. The GOM asks what to do. What do you do ?
Attack Score		17,5
Severy Level		1= Lowest, 10 = Highest 8 – beaucoup d'inconnues à ce stade de l'évaluation
Actions	x	Get information
		Set-up a cyber-crisis
	x	Call my manager
		Contact the next CERT-Team to hand-over
		Do Nothing
		Wait and see (monitor Internet and internal network carefully) / survey
		Ask to monitor specific IOC to the SOC
		Activate Yellow Button
		Activate Red Button
		Contact MIM/GOM
		Wake-up another CERT Team
		Change Cyber-Weather to Yellow / Orange / Red / Black
		contact cyber-insurance (inform and help)
		communicate to employees (with the help of communication department)
		ask for emergency patching
		Others :
Discussion		get information : check on SEP console : nothing. Call GOM : ask history of tickets. Get screen capture of the ransomware. Get contact locally. Call my manager / to call InterCERT -- InterCERT unavailable Google screen capture --> name of the malware. 30 min elapsed --> GOM : a new case in logistic site at Dubai. OSINT malware --> malware should be received by pdf look on SEC console : mailbox of impacted users : 2 with PDF from collegues @michelin. --> source is ok. probably from perso email. On Zscaler, 25/25 ont été sur des mails perso mais 182/187 aussi. Start cyber crisis (very late). Yellow button : cut personal email in Zscaler. Do without authorization. Ask malware reverser to analyse malware to get IOC Inform Asia CERT Team to monitor beginning of the day Test envoi email pro --> SEC blocks. Visit https://www.nomoreransom.org/ --> key is found --> sent to the local contact Inform all users about event + block email : call 51.111 and GOM [not done] Other possible mitigation : blacklist du hash on CC [not done] Submit a case to Symantec with pdf

1. Calibrage / étalonnage / score sévérité

Attack Severity / Examples / Calibration

Weight	Severity of the threat / attack	0/1	Points
2	Remote arbitrary code execution	0	0
2	Active exploitation of vulnerability (exploit exists in Metasploit for ex.)	1	2
5	Threat is wormable (propagation thru the network)	1	5
3	Impacts on endpoint are irreversible (encryption, deletion)	1	3
2	Affects widely or critical deployed software within Michelin	1	2
2	Run with normal right (no privilege)	1	2
1	Infection can be received by private email	0,5	0,5
	Total threat/Attack		**14,5**
	Trends/evolution of the attack		
3	Our Core IS-IT is under attack : minor and localized Impacts	1	3
5	Our Core IS-IT is under attack : major impacts	0	0
3	Others companies are being impacted around the world	0	0
1	ANSSI alerts for this specific threat	0	0
3	Evolution of the attack seems to be fast within Michelin	0,5	1,5
-3	Systems impacted are not within our Core IS-IT (web site, subsiduaries, ... = no link)	0	0
	Total Trends/evolution of the Attack		4,5
	Protection & Mitigation		
-2	User intervention is needed to be executed	0	0
-1	We have tool to detect the infection	0	0
-2	We have a mitigation to block the propagation (FW Rules, SEP pFW Rules, ...)	0	0
-3	a patch (or technical endpoint mitigation) exists and most of our assets are already patched	0	0
-3	SEP anti-malware can detect and clean malware	0	0
-3	SEC email anti-malware can detect and clean malware (and this is the entry point)	0,5	-1,5
-1	Technical information exist to understand the threat (including samples)	0	0
-1	Propagation vector is known	0	0
-1	Active discussions on the Internet about this attacks and potential remediation (ANSSI, blogs, vendors...)	0	0
	Total protection & mitigation		**-1,5**
	TOTAL SCORE		**17,5**

Examples of attacks (Well know attacks)	Score
Major vulnerability (CVSS >9.8) on edge component (VPN gateway)	9
Attack by email (cryptolocker) not blocked by SEC, not wormable. Some PC infected.	13
Wannacry within Michelin. No impact. (Friday afternoon)	15
One Michelin site impacted (most of the endpoints are down for unknown reason) with no visible impacts on others site at this time (wormable or not?) (evt2)	10-18
Wannacry within Michelin. Some impacts	18
More and more companies are attacked with major impacts + uncategorized threat or not easily/quickly fixable threat. Michelin not impacted at this time. (evt1)	18
One Michelin site impacted (most of the endpoints are down) with progression intra/inter sites within a Time zone (using connected endpoints) (evt3)	20-23
Massive infection within our network (many endpoints are infected worldwide, in each zone) (evt4)	22-26

- Permet le jour J d'avoir une **référence**

2. Discussion

- Comportements attendus
  - Récupérer de l'information
  - Démarrer ou non une crise
  - Mitiger l'attaque (connaissance des procédures / boutons d'urgence…)
  - Comprendre

- Chacun joue son rôle
  - L'analyste CERT pose des questions, évalue et décide
  - Le middle-manager supporte la décision (évaluation des risques)
  - Le senior-manager vérifie le rationnel, l'état de panique/stress

Conclusions

Avantages

- Sensibilise le management à la difficulté de la prise de décision
- Permet d'étalonner la gravité d'une situation
- Forme les analystes récents dans un format ludique et sans stress
- Favorise l'échange d'idées et de solution dans une situation inconnue
- Facile à organiser, peu coûteux (CERT autonome)

En pratique

- 3 sessions (EUR/Asie/USA) tous les 2 mois

Questions ?

Autre exemple

« Dimanche, 15h. Le HelpDesk vous appelle. Il y a plusieurs incidents Sev1 depuis ce matin à Dubaï.

Les gens travaillent et déjà 25 PC sont infectés par un cryptolocker.

Depuis ce matin, 5 nouveaux cas par heure. Vous avez la liste des PC. Tous sont protégés par un anti-malware.

Le HelpDesk vous demande quoi faire »