

4C E2 80 99 65 6E 73 65 6D 62 6C 65 20 64 65 73 20 6D 61 74 C3 A9 72 69 65 6C  
73 20 65 74 20 64 65 73 20 6C 6F 67 69 63 69 65 6C 73 20 71 75 69 20 63 6F 6E  
73 74 69 74 75 65 6E 74 20 6C 65 20 73 79 73 74 C3 A8 6D 65 20 49 6E 74 72 61  
6E 65 74 20 2F 20 49 6E 74 65 72 6E 65 74 20 64 65 20 6C 61 20 4D 61 69 72 69  
65 20 64 65 20 52 6F 75 65 6E 20 65 73 74 20 75 6E 20 6E 6F 75 76 65 6C 20 6F  
75 74 69 6C 20 64 65 20 72 65 63 68 65 72 63 68 65 20 65 74 20 64 65 20 63 6F  
6D 6D 75 6E 69 63 61 74 69 6F 6E 20 71 75 69 20 76 61 20 66 61 63 69 6C 69 74  
65 72 20 6C 65 20 74 72 61 76 61 69 6C 20 64 65 20 6C E2 80 99 65 6E 73 65 6D  
62 6C 65 20 65 73 20 63 6F 6C 6C 61 6E 6F 72 61 74 65 75 72 73 20 74 72 61  
76 61 69 6C 61 6E 74 65 69 75 72 6C 65 20 6D 70 65 20 64 65  
20 6C 61 20 65 69 6E 6E 61 6E 73 20 64 65 69 65 75 73 73 69 20  
6C 65 75 72 20 70 69 72 6D 65 74 74 72 65 20 64 65 20 6E 69 65 75 78 20 72 C3  
A9 70 6F 6E 64 72 65 20 61 75 78 20 64 65 6D 61 6E 64 65 73 20 64 65 20 72 65  
6E 73 65 69 67 6E 65 6D 65 6E 74 73 20 65 74 20 64 65 20 73 65 72 76 69 63 65  
73 20 64 65 20 6C 6E 69 70 61 72 74 20 64 65 73 69 68 69 74 6F 79 65 6E 73 2E  
0A 4C 27 57 69 6C 69 61 74 69 6E 64 65 20 65 6E 6E 79 73  
74 C3 6D 6E 20 6E 66 6F 71 6D 64 69 71 65 65 6E 6E 76 6E 69 73  
C3 A9 20 65 6E 20 72 C3 A9 73 65 61 75 20 73 75 70 70 6F 73 65 20 6C 65 20 72  
65 73 70 65 63 74 20 64 27 75 6E 20 63 65 72 74 61 69 6E 20 6E 6F 6D 62 72 65  
20 64 65 20 72 C3 A8 67 6C 65 73 20 70 61 72 20 73 65 73 20 75 74 69 6C 69 73  
61 74 65 75 72 73 20 65 6E 20 76 75 65 20 64 65 20 6D 61 69 6E 74 65 6E 69 72  
20 6C 61 20 73 C3 A9 63 75 72 69 74 C3 A9 20 64 65 73 20 64 6F 73 73 69 65 72  
73 20 65 74 20 6C 61 20 70 65 72 66 6F 72 6D 61 6E 63 65 20 64 65 73 20 74 72  
61 69 74 65 6D 65 6E 74 73 20 69 6E 66 6F 72 6D 61 74 69 71 75 65 73 2E 20 4C  
E2 80 99 6F 75 76 65 72 74 75 72 65 20 76 65 72 73 20 6C 65 20 6D 6F 6E 64 65

# Cyberattaque au CHU de Rouen



**Vendredi 15 novembre 2019**

# Une veille de week-end

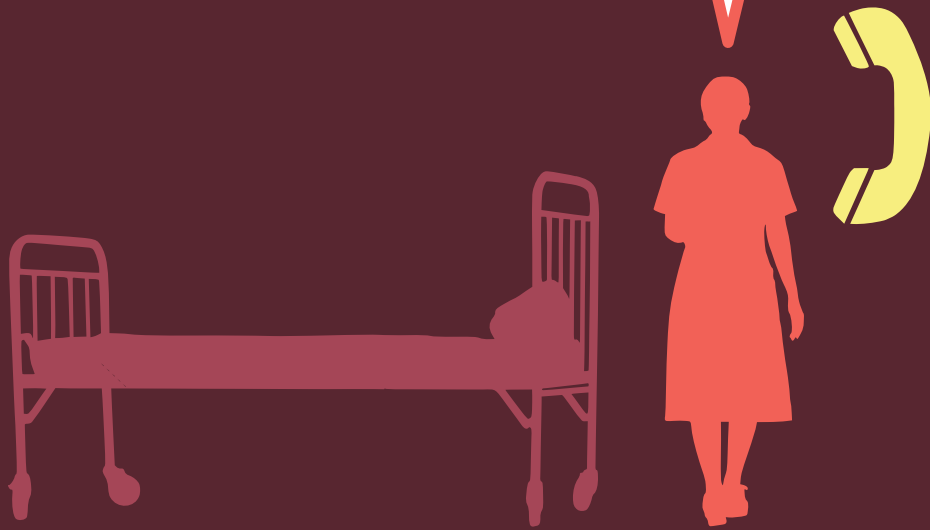


**Ah ! Enfin  
le week-end !**

19:00

# Ça ne marche pas !

**Je ne peux plus  
me connecter !**



**Avez-vous essayé  
de redémarrer  
votre ordinateur ?**



19:35

# Escalade de la hotline à la technique

**L'appli métier  
ne répond plus**



**C'est pas normal,  
je regarde ça**



19:40

# Attaque détectée



19:45

# Coupure d'internet



20:00

# Ouverture d'une cellule de crise

**Il nous faut  
des renforts**

**Je rappelle 20 personnes**



**20:00**



# Paris, nous avons un problème

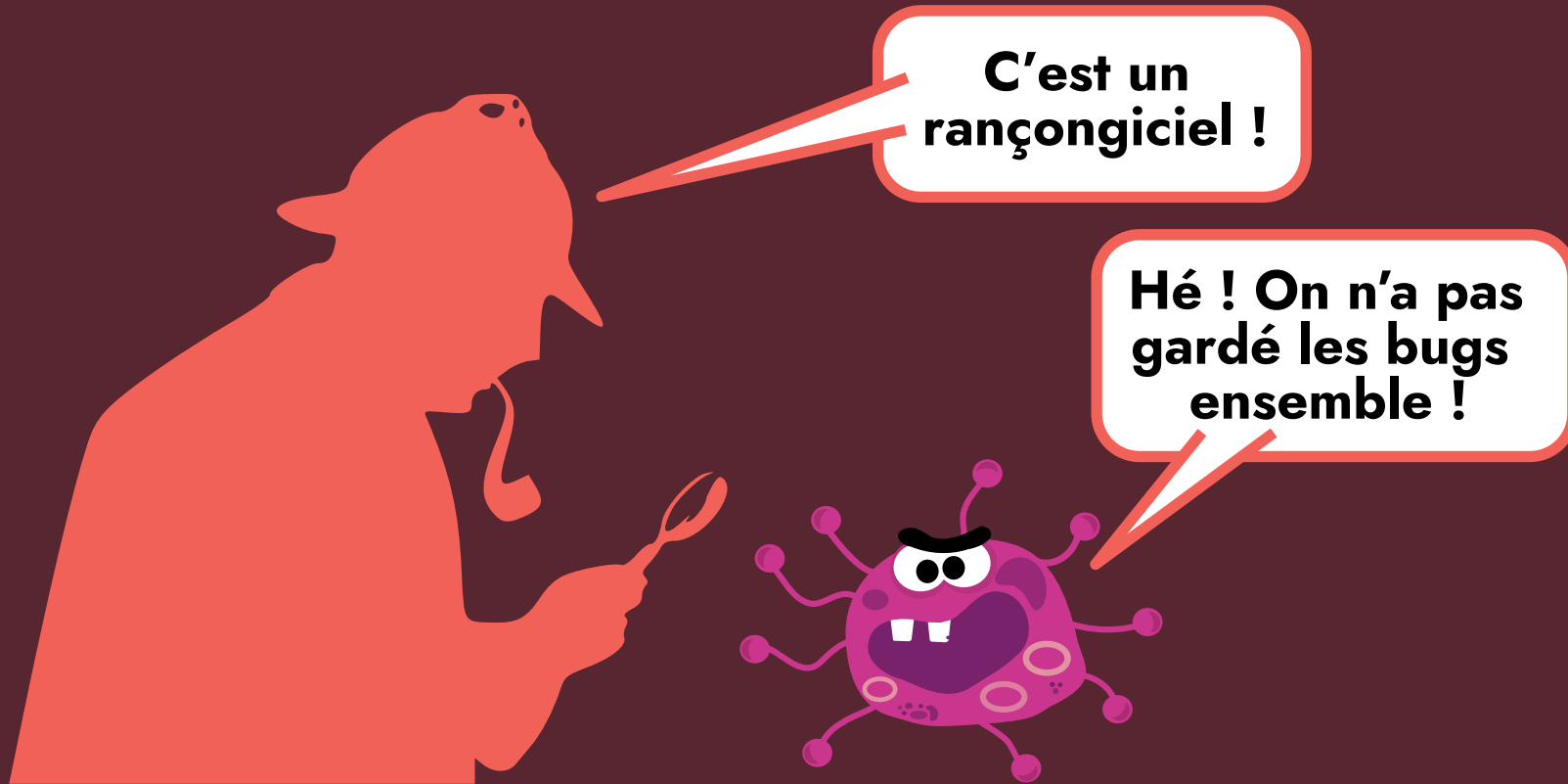
**Allo le Ministère ?  
La Cnil ? L'Anssi ?  
On est attaqué !**

**Ok ! On est  
sur le coup !**



21:30

# Attaque identifiée



**C'est un  
rançongiciel !**

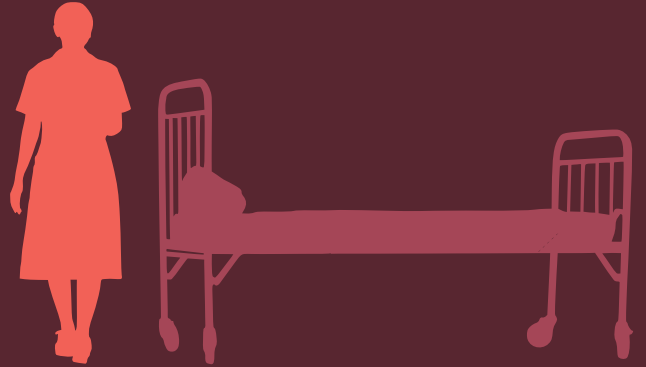
**Hé ! On n'a pas  
gardé les bugs  
ensemble !**

22:00

# Déploiement d'agents sur le terrain

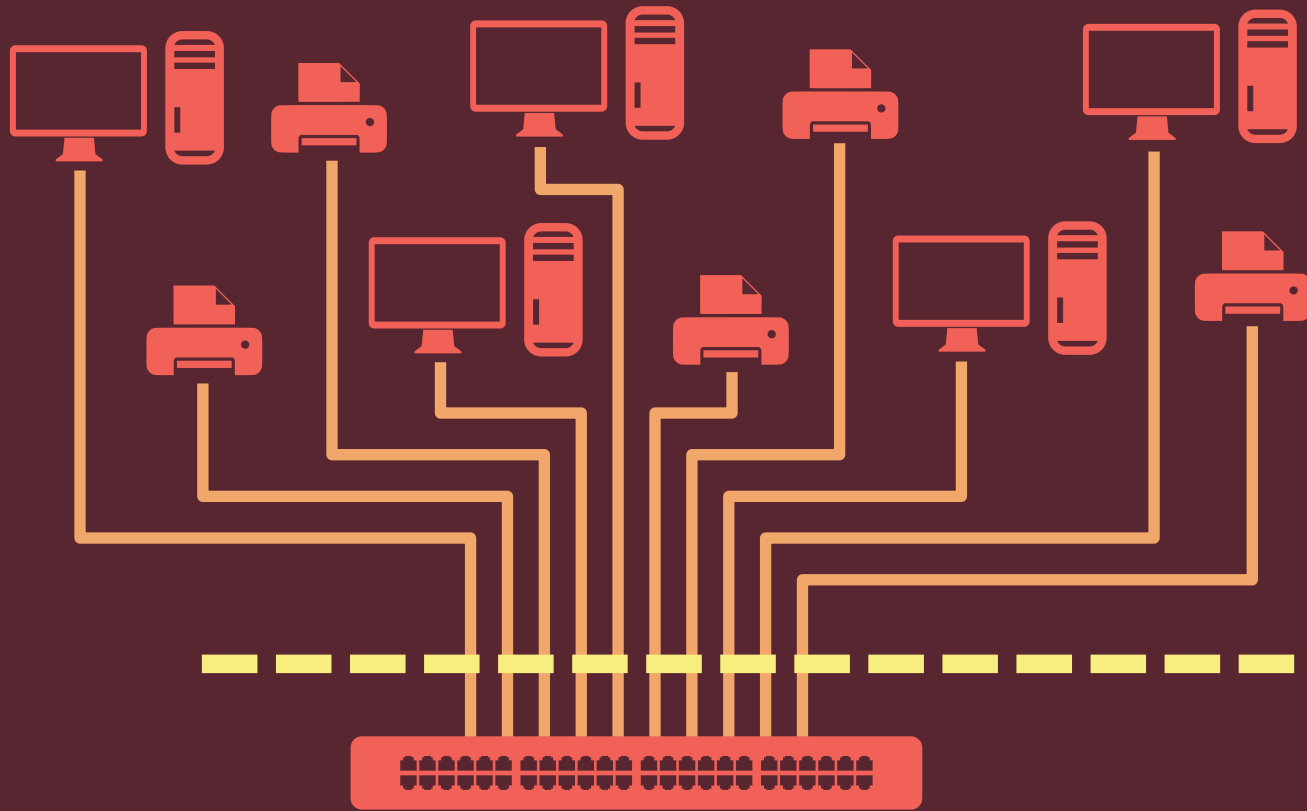
**C'est la galère,  
mais on est là  
pour vous aider**

**Ok ! Comment  
je fais sans mon  
ordinateur ?**

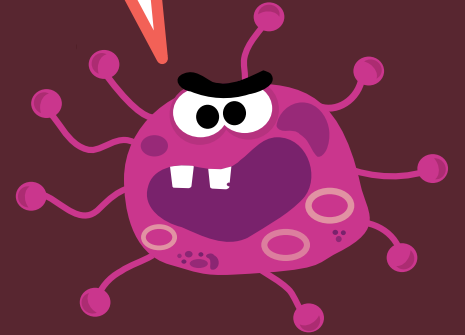


**22:00**

# Coupure de tout le réseau !



Comment  
je circule  
maintenant ?



00:00

# Des renforts supplémentaires

**On est 10, on  
vient en renfort**



**C'est pas  
de refus !**



00:00

# Back to the paper



Ça va pas  
être simple !



00:00

# Les jours suivants, la DSI est sur le pont

- **samedi** : priorité aux services critiques  
agents en coordination sur le terrain
- **dimanche** : services critiques a minima
- **lundi** : services administratifs  
ouverture d'une enquête
- **mardi** : 60~70% des applications restaurées  
pas d'internet sur les postes de travail



# 10 jours plus tard, toujours pas d'internet



plus de lolcat,  
de YouTube,  
de Facebook...

plus d'intrusion !

mais aussi plus  
de SaaS, PaaS...



**Un rançongiciel**

# Rançongiciel, ransomware, cryptolocker...

- **Il chiffre vos fichiers**  
avec un chiffrement asymétrique très costaud
- **Vous payez pour les déchiffrer**  
1 bitcoin par machine... à 7500 € le bitcoin en 11/19
- **Il se répand sur votre réseau**  
pour que les collègues en profitent
- **Les pirates communiquent à votre place**  
au cas où vous voudriez rester discrets



# Il est trop tard quand vous lisez ceci

Hello Martin.

Your network was hacked and encrypted.

No free decryption software is available on the web.

Email us at PIRATE@EXAMPLE.COM (or) SAINT@EXAMPLE.COM to get the ransom amount

Keep our contacts safe. Disclosure can lead to impossibility of decryption.

Please, use your company name as the email subject.

TAIL: BCVx54EqrS=

KEY: MIIEowIBAAKCAQEAr/gdloS7z7KYfdpK9fw+LHIAJMSYWJ0st+GtDA/8PEKc/ELw  
RD4Gi6M/obn5MEwibwuCTUoXKYadV+HabFtRpYrubguVxVrvAG0vOHjjqqNQCot3  
06x7mX3M5Ff0Ph6Yb/7MZxkIrcgTh9/AanVHi8su0DYSXGESkjbFG862LQfxunfD  
sZrF50lwJHS16g8gCPkAVHvo1G9pv20vGEcUCcy4c1/GRS0wkYV1dhoby8911m+Z  
/xowBEu4IqVsN0B0KIreFNoSBJZkq00S71Z96J4hZPslgzBDv2/pN1pHK1IR9165  
P+qUrKt/FAU0N09p6dkYzxt51IWuSxsi6AW3jQIDAQABAoIBAFhm8ZZYgHHLa0hu  
jhId8q4pZ2ERUufRr1GCkojozvMHFA63IjVmY6trC+CXqVRWK0ZWJdPmUNSPyCQK  
Vszw44ei0D2AnHFVVSZSMf86DDP0Apo1lnzTfZgiqZnCGnAAhJru86bpgn7e00CGe  
iu/wk0zrek0nnPnD54gdk9BwfJ0=

comment contacter  
les pirates

clé unique  
correspondant  
à une machine

# Où est la faille ?

- **Une pièce jointe dans un mail ?**  
hameçonnage / phishing
- **Un compte utilisateur sur le marché noir ?**  
mot de passe trop faible, utilisé plusieurs fois...
- **Une sécurité insuffisante ?**  
forte sécurité **vs** utilisation quotidienne



**Une attaque se prépare**

# Février 2019



JANVIER						
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

FÉVRIER						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28			

MARS						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

AVRIL							
	1	2	3	4	5	6	7
8	9	10	11	12	13	14	
15	16	17	18	19	20	21	
22	23	24	25	26	27	28	
29	30						

MARS						
					6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

AOÛT							
				1	2	3	4
5	6	7	8	9	10	11	
12	13	14	15	16	17	18	
19	20	21	22	23	24	25	
26	27	28	29	30	31		

- **Première apparition de Clop**  
rançongiciel utilisé contre le CHU
- **Chiffre fortement les fichiers**  
mais nécessite une intervention humaine pour se propager

SEPTEMBRE							
	2	3	4	5	6	7	8
9	10	11	12	13	14	15	
16	17	18	19	20	21	22	
23	24	25	26	27	28	29	
30							

OCTOBRE								
		7	8	9	10	11	12	13
14	15	16	17	18	19	20		
21	22	23	24	25	26	27		
28	29	30	31					

NOVEMBRE						
					2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

DÉCEMBRE							
							1
2	3	4	5	6	7	8	
9	10	11	12	13	14	15	
16	17	18	19	20	21	22	
23	24	25	26	27	28	29	
30	31						

# Avant septembre 2019

JANVIER						
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

FÉVRIER						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28			

MARS						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

AVRIL						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

MAI						
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

JUIN						
				1	2	
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

JUILLET						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

AOÛT						
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

- **Des sites web spécialisés sont piratés**

Symposium Veith, Congrès EFIC, Hospitalier.net, France pathologie...

- **Des données sensibles fuient**

adresses email, mots de passe...

# De juin à novembre 2019

- **Forte activité de TA505**

groupe russe ou russophone  
actif depuis 2014

- **9+ campagnes d'attaques**

groupes financiers, hôpitaux...

- **PME de la cybercriminalité**

oubliez le mythe du jeune génie isolé

aka Sectorj04 Group,  
GRACEFUL SPIDER,  
GOLD TAHOE...

MARS							AVRIL						
4	5	6	7	8	9	10	1	2	3	4	5	6	7
11	12	13	14	15	16	17	8	9	10	11	12	13	14
18	19	20	21	22	23	24	15	16	17	18	19	20	21
25	26	27	28	29	30	31	22	23	24	25	26	27	28
							29	30					

JUIN						
				1	2	
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

JUILLET						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

AOÛT						
		1	2	3	4	
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SEPTEMBRE						
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

OCTOBRE						
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

NOVEMBRE						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

DÉCEMBRE						
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					



# 7 septembre 2019



JANVIER						
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

FÉVRIER						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28			

MARS						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

AVRIL						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

MAI						
	1	2	3	4	5	
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

JUIN						
				1	2	
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

JUILLET						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

AOÛT						
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SEPTEMBRE						
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						



- **Un expert de Zataz alerte les autorités**  
Anssi, Cnil, Ministère des Affaires Sociales
- **Comptes vendus au marché noir**  
adresses email, mots de passe
- **CHU de Rouen concerné**



# Début novembre 2019

- **TA505 dans le réseau du CHU**
- **Phase de propagation manuelle**  
Clop ne sait pas se propager seul !
- **Utilisation de logiciels malveillants**  
ServHelper backdoor, FlawedAmmyy, Cobalt Strike
- **En toute discrétion...**

## JANVIER

	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

## MAI

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

## SEPTEMBRE

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

## OCTOBRE

	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

## NOVEMBRE

				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

## DÉCEMBRE

							1
2	3	4	5	6	7	8	
9	10	11	12	13	14	15	
16	17	18	19	20	21	22	
23	24	25	26	27	28	29	
30	31						

# 15 novembre 2019



JANVIER						
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

MAI						
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

SEPTEMBRE						
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

FÉVRIER						

MARS						

AVRIL						

OCTOBRE						
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

NOVEMBRE						
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

DÉCEMBRE						
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

- **À une heure propice**  
en début de soirée, la veille d'un week-end
- **TA505 lance le chiffrement**
- **Les applis métiers ne répondent plus**
- **Vous connaissez la suite !**



**Quels sont les bons gestes ?**

# Ce qui a sauvé le CHU

- **Sauvegardes**  
elles ont permis de ne perdre aucune donnée
- **Incapacité du malware à se propager seul**
- **Hétérogénéité du SI**  
le malware préférerait Windows
- **Réactivité du service informatique**
- **Cloisonnement du réseau, postes éteints**  
a limité la propagation du rançongiciel



# Bons gestes 1/2

- **Méfiez-vous des mails**
  - du nom de l'expéditeur
  - des pièces jointes
  - des demandes d'infos confidentielles
  - des liens
- **Ne partagez pas votre carnet d'adresses**
- **Votre compte **pro** doit rester **pro****



# Bons gestes 2/2

- Éteignez votre ordinateur
- N'introduisez pas d'éléments extérieurs
  - pas de PC **perso** sur un réseau **pro**
  - pas de clé **perso** ou trouvée par terre
  - pas d'appli **perso** sur le téléphone **pro**
- Ne prêtez pas votre matériel **pro**
- Et n'oubliez jamais que...





**N'oubliez jamais que...**

**PERSONNE**

**N'EST À L'ABRI**

# Un doute ?

**UN MAIL SUSPECT ?**

**UNE ALERTE SÉCURITÉ ?**

**UN PC BLOQUÉ ?**

**QUI APPELLE-T-ON ?**

**APPELEZ  
VOTRE DSI**

