MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

RIIP
RANSOMWARE
INTEGRATED
INVESTIGATION
PROCESS

PARQUET DE PARIS
JUNALCO

INITIAL INCIDENT REPORT

1. Saisine [1. OPENING CASE FILE]

1.1	Date des faits	
1.2	Service de plainte (CSP-BTA)	
1.3	Parquet local	
1.4	JUNALCO / Section J3 avisée	
1.5	DCPJ avisée	

2. Victime et premiers intervenants [2. VICTIM & FIRST RESPONDERS]

2.1	Nom de la victime	
2.2	Adresse	
2.3	N° SIRET	
2.4	Type victime	
	Secteur économique	
2.5	Point de contact	
2.6	RSSI/DSI Victime	
2.7	Nom société réponse à incident	
2.8	Responsable société réponse à incident	
2.9	Famille rançongiciel	
2.10	Souche récupérée	
	Si oui, Hash	
2.11	Extension fichiers chiffrés	
2.12	Logs (IP + date et heure + fuseau horaire)	
2.13	Logs disponibles	
2.14	Note de rançon annexée	
2.15	Impact sur l'activité de la société	
2.16	Une ou plusieurs machines du réseau sont-elles accessibles à distance ?	
	Comment ?	
2.17	Les serveurs chiffrés avaient-ils accès à Internet en direct ?	
2.18	VM en cours de chiffrement disponible (format .vmk, .vhdx, E01 etc…)	
2.19	Possibilité de mettre en place un SFTP pour la transmission des données	
2.20	Domaine public (web, VPN, Citrix,…)	
2.21	I.P. publique de la société	

Information complémentaire :
toute transmission d'exécutables ou d'outils utilisés par les pirates doit être réalisée dans un conteneur Zip protégé par le mot de passe « Infected » ; soit par SFTP, soit sur la boîte mail **sdlc@tutanota.com**
Si la société victime ou la société de réponse à incident utilise le logiciel « TheHive5 », celle-ci peut extraire le « Case » de l'incident et le transmettre à la SDLC afin de communiquer les IOC de l'incident, TheHive5 étant utilisé par la SDLC.

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

RIIP
RANSOMWARE
INTEGRATED
INVESTIGATION
PROCESS

JUNALCO

3. Infrastructure d'attaque [3. INFRA]

3.1	Vecteur d'infection	
3.2	Date de l'infection	
3.3	Identification du poste primo-infecté	
3.4	Préservation du poste primo-infecté	
3.5	Logs d'infection (IP + horodatage + fuseau horaire)	
3.6	Cheval de troie (Emotet, Dridex, Trickbot…)	
3.7	Programme de déploiement (Cobalt strike, mimikatz,…)	
3.8	Préservation des exécutables (.exe)	
3.9	Outils d'attaque utilisés	
	Extraction de ces outils	
3.10	Autres programmes d'attaque utilisés	
3.11	Date du chiffrement des données	
3.12	Destination (IP, URL) des données extraites du SI	

4. Vecteur de communication [4. COM]

4.1	Contact avec les auteurs	
4.2	Adresse ou lien de contact	
4.3	Négociations débutées	
4.4	Autorisation de négociation par forces de l'ordre	

5. Vecteur financier [5. FIN]

5.1	Paiement de la rançon	
5.2	Montant de la rançon	
5.3	Adresse de paiement	
5.4	Types de crytommonaie (BTC, MONERO, ETH,…)	

Commentaire libre