


TYPE : CYBERATTACK TARGET : ALL	Reflex Sheet RANSOMWARE - MASSIVE UNAVAILABILITY OF WORKSTATIONS	
---	--	---

1. Alerting

Report of the attack (note on the desktop, unavailable files and applications...)	Notification from SOC
DO NOT DELETE ANY INFORMATION: all information will be used as evidence in the investigation	TAKE IMMEDIATELY INTO ACCOUNT THE NOTIFICATION
DO NOT OPEN CRYPTED FILES OR APPLICATIONS: the infection must be stopped	SHARE ANY INFORMATION with the SOC to assess the scope of the attack and emergency response priorities
	FOLLOW SOC INSTRUCTIONS

2. Emergency actions

- Isolate critical systems :**
 - Disconnect all networks
 - Disconnect network cable from computers
 - Disconnect WiFi connections
- Disconnect all devices**
- If you can't disconnect the computer from network, **disable all routers and Wi-Fi hotspots**
- Assess the extent of the compromise and **collect evidence**

3. Continuity solution

Provision of a virtualised work environment accessible from the Internet via any workstation in order of criticality of activities

4. Criteria for the continuity solution activation

It is the crisis cell that makes the final decision to activate the BCP

Criterion 1: 5% of workstations are unusable

Criterion 2: risk of propagation of the ransomware to other sites / entities / applications