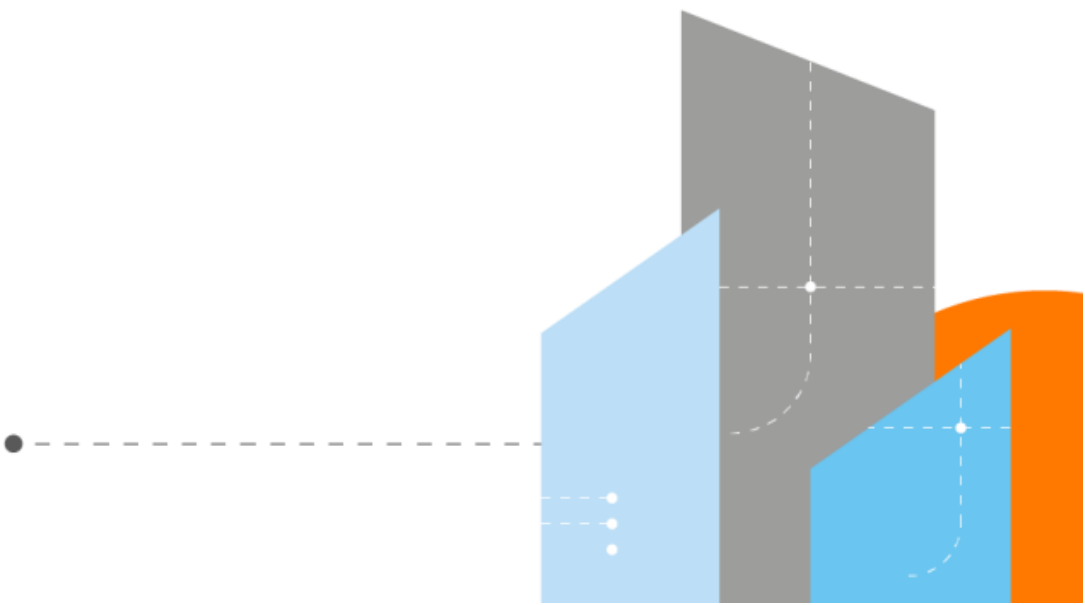
Orange
Cyberdefense

Analyse d'une malveillance

Interne

9 février 2021



Fiche de contrôle

Historique	Date	Etat
v 1.0	9 février 2021	Création du document

Rédacteurs	Fonction	Contact
LEROY Romain	Responsable technique - BU Endpoint	romain.leroy@orange.com

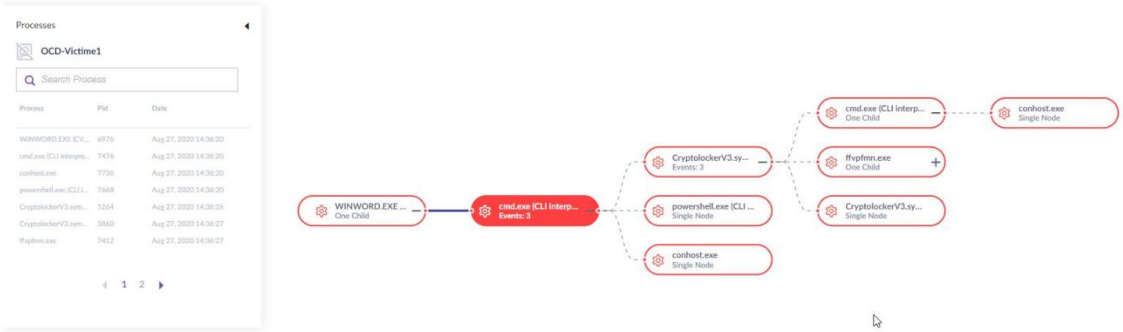
Destinataires	Fonction	Contact

1 Schéma de l'attaque

Bonjour,

Vous trouverez ci-dessous le détail d'une attaque que nous avons détecté via nos outils.

Nous sommes en train de rechercher ce qu'il a bien pu se passer…

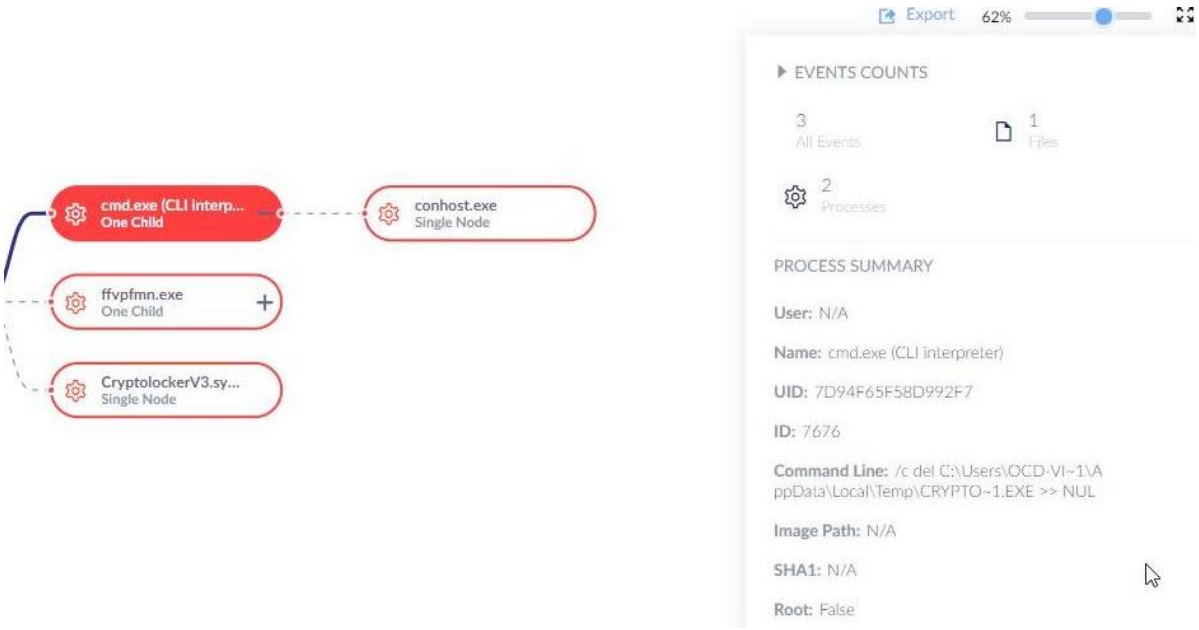


Cependant, au vue de la source de l'attaque, nous pensons fortement à une attaque de type …….. Cela n'explique pas encore la finalité de l'attaque.

Les détails de la cmd rouge est la suivante :

Nous sommes en mesure de déterminer le nom du binaire malveillant …….. provenant de l'adresse ip ……..

La seconde occurrence de cmd.exe sert probablement à …….. la charge malicieuse. Très malin !.



En finalité, nous sommes bien face à un malware communément appelle en anglais ……..

Nous avons correctement mitigé l'attaque.

Il s'agit d'une des attaques les plus répandus, mais également les plus dévastatrices.

N'hésitez pas à nous contacter pour plus d'informations.