

Ransomware et DDoS : les deux font la paire

Comment accentuer la pression sur les victimes de *ransomwares* ? En recourant au déni de service.

On avait vu émerger [cette tendance](#) il y a quelques mois. Suncrypt fut le premier groupe cybercriminel à s'y inscrire officiellement, au sens où il avait ajouté une entrée « DDOS » dans la fiche de chacune des victimes listées sur son site « vitrine ».

After SunCrypt (thread: <https://t.co/cbi0idOf5y>) started (or better said, first did it publicly), now there is another ransomware gang that is threatening victim companies with DDOS...

— MalwareHunterTeam (@malwrhunterteam) [October 16, 2020](#)

Lock date	2020-09-29
Phone	1([REDACTED]) 5
Address	520 [REDACTED] 7523-8291
Full dump	No
DDOS	<input checked="" type="checkbox"/> YES

Ragnar_Locker avait ensuite fait de même. REvil avait pour sa part reconnu « songer » à adopter le modèle.

Ce modèle, on le retrouve désormais aussi chez Avaddon. Avec, comme premier exemple, une PME polonaise dont le site est effectivement hors service à l'heure où nous écrivons ces lignes.

Next

6 Days 11 : 56 : 45

update:

A [REDACTED] Inc, the company does not want to cooperate with us, so we give them 240 hours to change its decision. If you do not cooperate with us, we will leak your entire database, these are personal data of customers and employees, as well as financial documents.

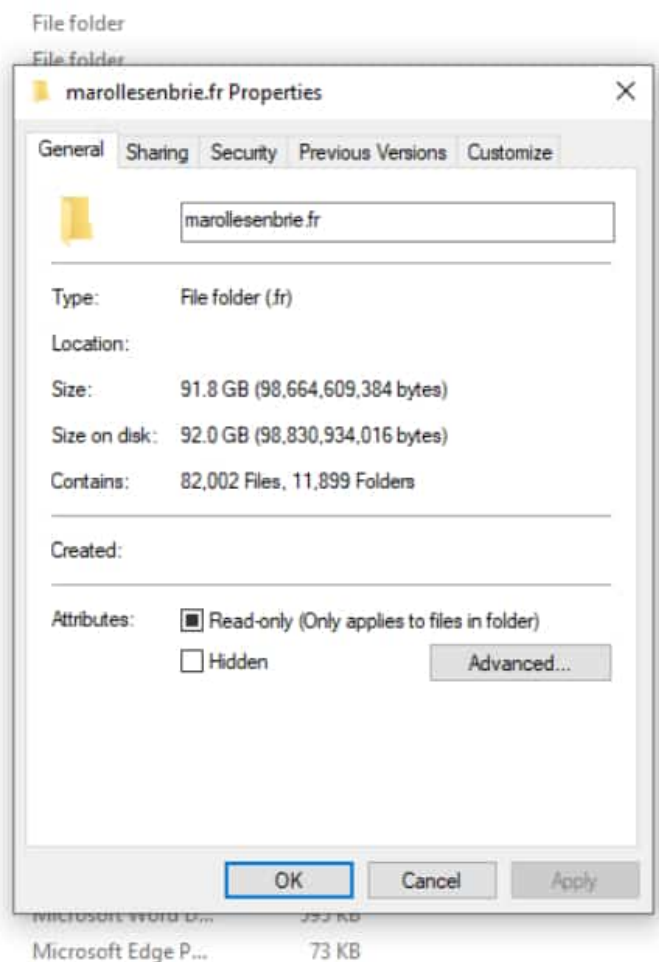
Also, their site is currently under **DDoS Attack**, we will attack it until they contact us. We still have many ideas on how to make problems for the company and their clients. Think about the company's reputation.

We have approximately **~44 GB** of company information including confidential documents, personal data of customers and employees, as well as financial documents, they will be available here soon (:

Sur la liste des victimes revendiquées d'Avaddon, il y a aussi une commune française : Marolles-sur-Brie (Val-de-Marne).

Voilà deux semaines que cette dernière a fait état d'une « cyberattaque sur ses systèmes d'information ». Survenue dans la nuit du 17 au 18 décembre 2020, elle est « de type rançongiciel » et « accompagnée d'une demande de rançon ».

La demande de rançon n'a visiblement pas donné suite. Des données ont en tout cas été publiées. Il y en a pour environ 20 Go, en deux archives, dont une en treize parties.



Certaines de ces données sont à caractère personnel. Elles concernent, entre autres, des recrutements d'agents municipaux. Apparaissent, pêle-mêle, des noms, des numéros de téléphone, des adresses postales ou encore des salaires.

Certaines données sont sensibles à d'autres titres. Par exemple, le plan envisagé pour le dispositif de sécurité d'un poste de police. En l'occurrence, celui que la commune a [ouvert l'an dernier](#).

Illustration principale © Andrey Armyagov – shutterstock.com