# Peut-on neutraliser un ransomware lancé sur des milliers de machines en même temps ?

tehtris.com/fr/peut-on-neutraliser-un-ransomware-lance-en-tant-que-system-sur-des-milliers-de-machines-en-meme-temps/

July 22, 2020

Comme chacun le sait, les cybercriminels ne se reposent jamais et il y a actuellement une recrudescence d'attaques par ransomwares dans le monde entier. Les cybercriminels n'ont pas fait de trêve malgré la pandémie Covid-19, et certains ne semblent pas avoir pris de congés pendant la période estivale en cours.

D'un point de vue renseignement et cyber, il est très intéressant de constater que dans le passé, les mois de juillet-août étaient très chargés en actualités comme en 2003 avec MSBlast, ou au contraire, plutôt calmes : quand les cybercriminels profitent non pas des plages de ports TCP/UDP, mais des plages sablées, notamment dans certains lieux bien identifiés…

Dans un pays que nous ne citerons pas, il existe une grande infrastructure protégée et surveillée par TEHTRIS à distance depuis son **SOC** en France, et qui a été prise pour cible, avec l'arme très connue nommée SODINOKIBI. Dans cet article, nous allons partager avec vous quelques éléments sur ce sujet.

## Que se passe-t-il quand un ransomware avec un binaire inconnu, est lancé en mode SYSTEM sur tout ou partie d'un parc, et que tous les produits traditionnels sont contournés (antivirus local, etc.) ?

En général, c'est ce que redoutent tous ceux qui ont compris les enjeux liés à la protection des postes de travail. Nous utiliserons ici l'exemple de l'infrastructure surveillée par TEHTRIS, sans nommer le pays cible, ni les méthodes offensives, pour ne pas déranger les enquêtes en cours.

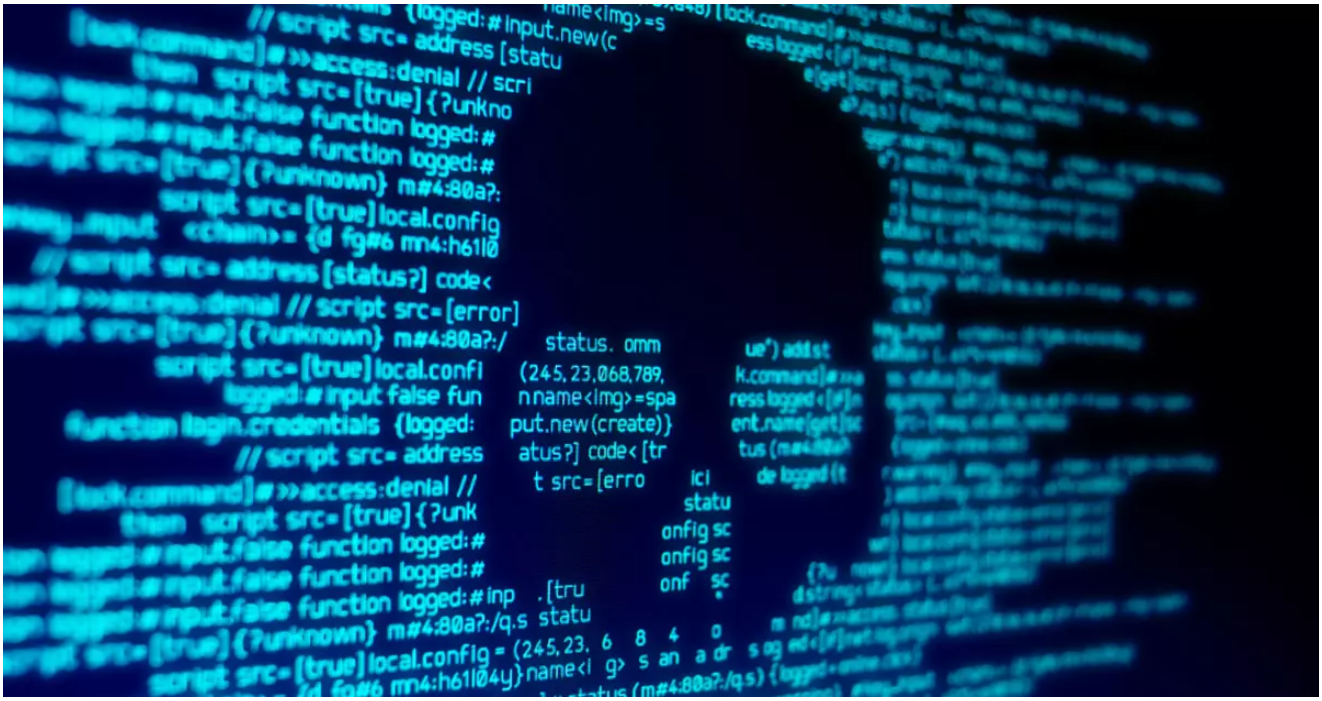
Lorsque le binaire inconnu en question se lance sur des milliers de machines, les agents **TEHTRIS EDR** présents dans les systèmes d'exploitation (agents qui intègrent une capacité de suspension de l'exécution via un driver noyau) remontent l'information à leur manager **EDR**.

Si l'on traduit le langage de nos robots pour des humains, cela donne ceci : "*Je suis l'agent EDR XXX, et SYSTEM souhaite lancer tel logiciel que je ne connais pas, dans tel contexte, et ma politique m'impose de demander l'autorisation à mon manager EDR*".

Ce dernier regarde immédiatement dans sa base de machine learning, qui correspond à l'activité totale connue et apprise sur le parc depuis les premières secondes d'installation.

Le manager **TEHTRIS EDR** réalise que lui-même ne connaît pas ce binaire, tombant dans un scénario particulier qui déclenche un playbook de notre **SOAR** intégré à la **TEHTRIS XDR Platform**.

Ce playbook existe depuis 2014 chez TEHTRIS : il associe l'agent TEHTRIS EDR à notre CTI (Cyber Threat Intelligence). Ce playbook est efficace avec une intégration complète à notre EDR et une présence constante dans nos usages.



Neutraliser un ransomware n'est pas une affaire à prendre à la légère

## Hyper Automatisation x Cybersécurité !

Ce playbook fonctionne efficacement lorsqu'il est évidemment paramétré : en cas de présence d'un binaire inconnu, les robots TEHTRIS ont alors toute la légitimité pour effectuer des analyses en direct, de façon automatique, que des humains n'auraient pas le temps de mener, sans parler des cas où une attaque aurait lieu la nuit, le week-end, etc. La cyberguerre ne fait pas de pause et les robots TEHTRIS appliquent les politiques planifiées et décidées par les humains en avance de phase lors des déploiements.

Ces robots, à eux seuls, envoient ainsi le binaire sur des antivirus hébergés par TEHTRIS hors-ligne, ou sur des bacs à sable par exemple hors-ligne appartenant à TEHTRIS, ou sur notre moteur d'intelligence artificielle qui est issu de nos recherches en mode Deep Learning. Ce dernier est le premier outil français à avoir été accepté sur Google VirusTotal.

Dans notre l'exemple, la partie qui contribue à cette automatisation en mode SOAR, au cœur de la **TEHTRIS XDR Platform**, reçoit donc des résultats en très peu de temps, en provenance des capteurs sollicités du côté de la **CTI**. Sans appel, le diagnostic tombe,

indiquant que le binaire inconnu est identifié comme un ransomware inconnu, avec une certitude de 100%.

Les responsables et experts en charge de cette grande infrastructure ont eu la sagesse de faire confiance au triplet gagnant : la TEHTRIS XDR Platform équipée de son SOAR + les agents TEHTRIS EDR + la capacité d'analyse TEHTRIS CTI. En effet, ils ont paramétré de façon prévisionnelle et résiliente l'autorisation de neutraliser en direct, sans humain, le moindre ransomware. En parlant en cyber langage à la James Bond, ce serait comparable au fameux "permis de tuer".

## Bilan final ?

**TEHTRIS EDR** a neutralisé tout seul, automatiquement une charge de ransomware totalement inconnue, variante de SODINOKIBI qui avait pu contourner les autres mesures défensives en place (antivirus local).

Très souvent, dans la presse, nous pouvons lire qu'une entreprise a été détruite en partie : stations, serveurs, etc. Depuis des mois, TEHTRIS affiche un score de 100% de résilience pour ses clients qui suivent un protocole défensif strict, y compris face aux menaces inconnues.

## Quelle sécurité choisir ?

Les solutions existent, mais il faut réussir à les trouver, ce qui demeure assez compliqué dans un marché où la science n'est hélas pas toujours le mode de pensée.
Nous pensons qu'il existe actuellement 4 catégories d'infrastructures et de protections, et voici un guide pour mesurer la catégorie où vous vous situez, et pour choisir celle où vous souhaitez vous positionner :

1) **sans EDR**, basées uniquement sur des protections traditionnelles type antivirus, antivirus next-gen : la probabilité d'être détruit est supérieure à 95% en cas d'attaque inconnue de type sabotage

2) **avec des agents EDR** essentiellement orientés sur l'expérience utilisateur (belle interface qui plaît beaucoup) et/ou avec une volonté très orientée forensics/analyses post-attaques/enquêtes : la probabilité d'être détruit est supérieure à 90% en cas d'attaque inconnue de type sabotage, car ce sont des technologies qui sont très récentes en ce qui concerne la neutralisation automatique, voire qui ne proposent pas du tout cette option

3) **avec des agents EDR efficaces**, à savoir, ceux capables de neutraliser des attaques inconnues en direct mais parfois mal paramétrés, pas assez autonomes ou ayant besoin d'être branchés à un SOAR externe complexifiant l'efficacité : la probabilité d'être détruit est supérieure à 60% en cas d'attaque inconnue de type sabotage, suivant les cas

4) **avec des agents EDR efficaces et autonomes**, à savoir ceux capables de protéger seuls les entreprises en mode SOAR intégré : la probabilité d'être détruit varie entre 0,xx % et 20% en cas d'attaque inconnue de type sabotage, suivant les produits et les paramétrages associés

Cette dernière catégorie est simple : il s'agit des **EDR rattachés à une XDR Platform**, avec du **SOAR**, de la CTI, une vocation de faire de l'hyper automatisation, et surtout, un paramétrage parfait qui permet d'indiquer ce qui doit être éliminé, quand et comment (la fameuse intégration nécessaire). Les experts et CISO avant-gardistes internationaux sont passés à ces technologies depuis quelques années.

## TEHTRIS EDR : sonde et protège les systèmes d'exploitation

Du côté de TEHTRIS, nous tenons un score complexe d'efficacité maximale, nous plaçant en tête des meilleures solutions techniques au niveau opérationnel et mondial, loin des analyses de laboratoire avec 3 exploits et 2 tests APT, mais directement en prise avec la cybercriminalité et les espions numériques.

TEHTRIS EDR fait évidemment partie de cette 4ème catégorie, puisque nous avons été dans les premiers agents au monde ayant ces capacités. Nos early adopters estiment que nous avons créé cette catégorie il y a 6 ans de cela.

Nos clients comparent d'ailleurs le côté disruptif de notre EDR à ce que l'automatisation apporte à l'Industrie 4.0 avec ses capteurs intelligents, capables d'agir sans intervention humaine.

Lorsque TEHTRIS EDR est déployé et paramétré pour neutraliser des tentatives de cyber sabotage, il peut contrer une attaque d'envergure, même pendant la nuit et continuer de protéger l'infrastructure en complète autonomie.

## "Citius, Altius, Fortius"

Dans le cas particulier présenté dans cet article, nous rappelons que SODINOKIBI est un ransomware qui menace la sécurité de milliers d'entreprises et nous avons la certitude qu'une campagne d'attaques est très certainement en cours partout dans le monde.

Les experts de TEHTRIS ont donc effectué du reverse engineering sur le binaire, et nous souhaitons partager avec le plus grand nombre une base d'IoC intéressants, afin que les experts puissent alimenter leurs capteurs et outils.

N'hésitez pas à nous contacter si vous avez des questions particulières au niveau défensif, ou à passer par nos réseaux de partenaires experts, capables de lutter efficacement contre les nouvelles menaces avec nos technologies.