Lockbit change de couleur

glimps.fr/dcouverte-dune-nouvelle-version-du-ramsomware-lockbit/

14 avril 2023

Dans le domaine du rançongiciel, Lockbit est un groupe qui ne cesse d'évoluer. Preuve en est, encore une fois, suite à la découverte d'une nouvelle version du ransomware Lockbit. Cette nouvelle variante semble s'appuyer cette fois sur le code source d'un autre rançongiciel bien connu : Conti.
Le ransomware Conti est apparu en 2020 et est très vite devenu un pionner dans le domaine. Avec la mise en place d'un business model très lucratif, le groupe a très vite gagné en popularité. Une de leur victimes les plus connues est la HSE (Service de santé Irlandais) en mai 2021.

En 2021, un affilié fait fuiter des documents internes à l'équipe et créé le premier scandale autour de ce groupe. En 2022, suite à la prise de position du groupe en faveur de la Russie dans la guerre qui l'oppose à l'Ukraine, un conflit interne éclate et c'est cette fois-ci le code

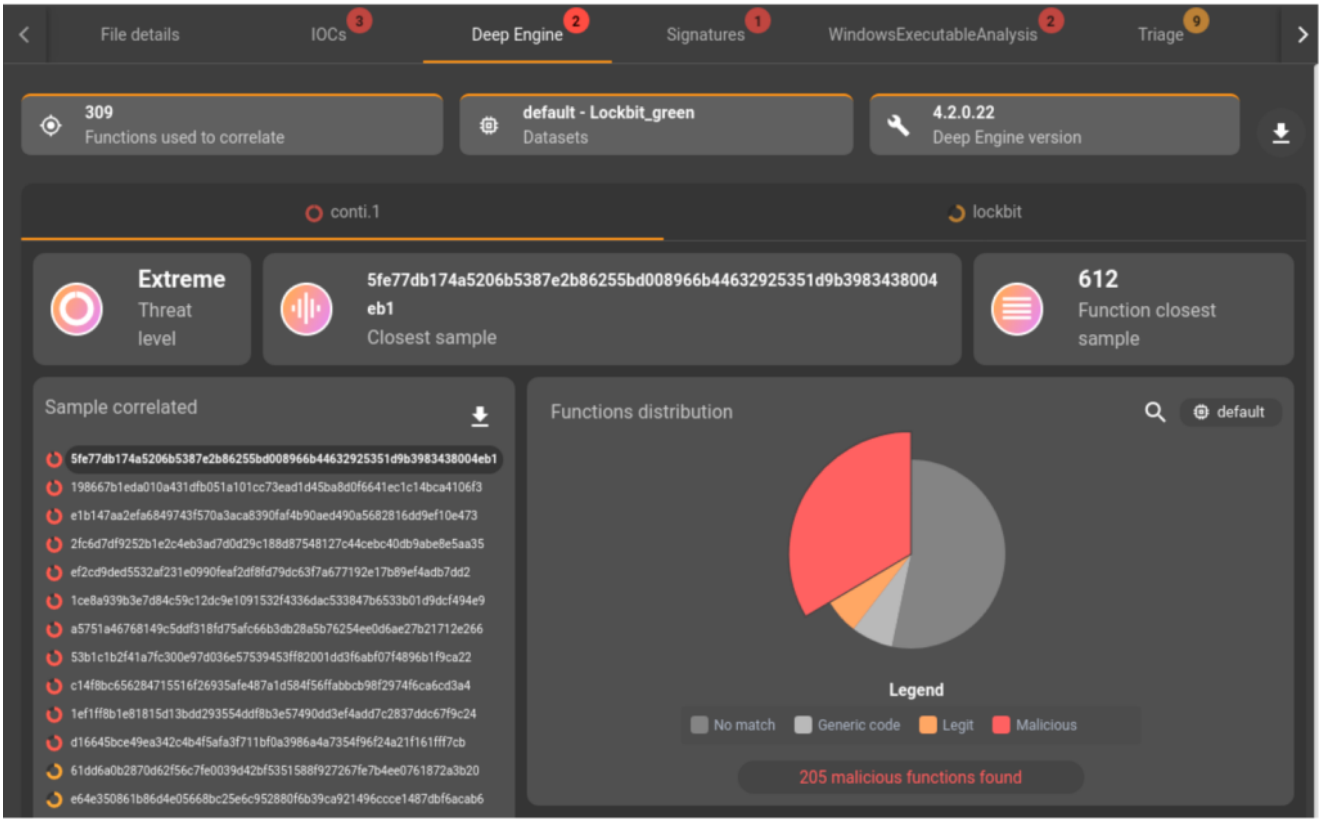
source complet du rançongiciel qui est mis en ligne. Le groupe Lockbit a profité de cette fuite pour récupérer le code source et l'intégrer au leur. La liste des victimes de Lockbit étant toujours à la hausse, cette nouvelle vague risque de ne pas abaisser la tendance.

Nous avons pu nous procurer certaines souches de ce nouveau variant et les soumettre à notre plateforme d'analyse GLIMPS Malware. Nous présentons ici les résultats de l'analyse automatisée réalisée.

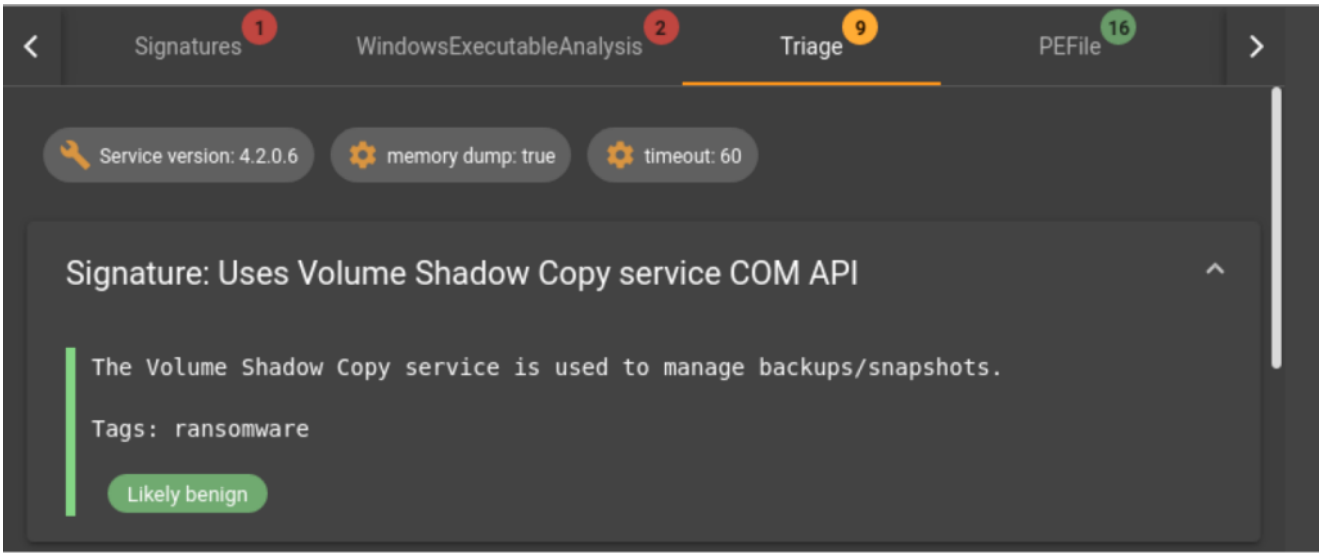
Analyse d'une première souche

45c317200e27e5c5692c59d06768ca2e7eeb446d6d495084f414d0f261f75315

Ce fichier est identifié par GLIMPS Malware comme malveillant. Le moteur d'analyse Deep Engine[1] nous indique que cet échantillon embarque des fonctions utilisées dans des binaires de la famille *Conti* ainsi que *Lockbit*. Ce lien entre *Lockbit* et *Conti* mis en lumière par notre plateforme d'analyse nous mène à pousser l'investigation.



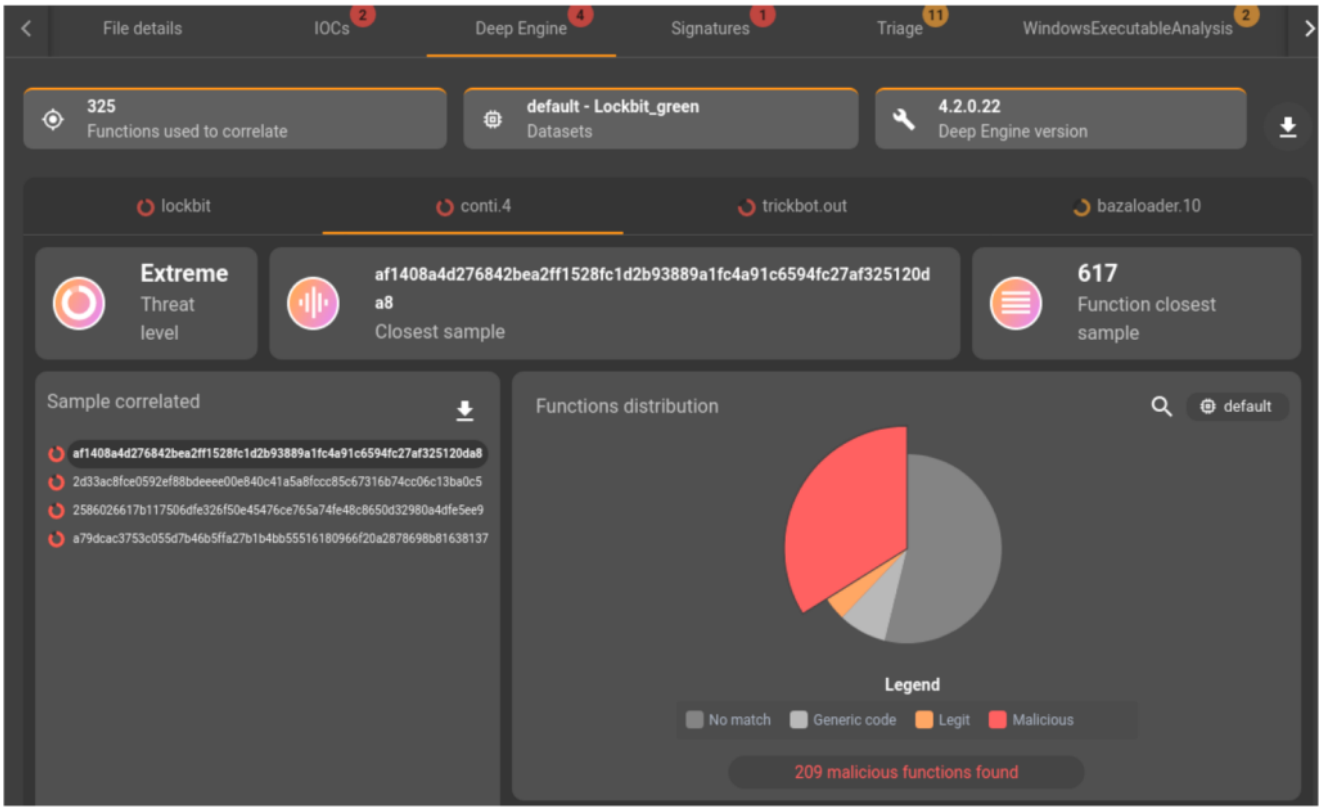
La souche est soumise en analyse dynamique via une sandbox connectée à GLIMPS Malware et nous confirme que nous sommes face à un rançongiciel sans fournir plus d'informations sur la famille à ce stade.



Analyse d'une seconde souche

fb49b940570cfd241dea27ae768ac420e863d9f26c5d64f0d10aea4dd0bf0ce3

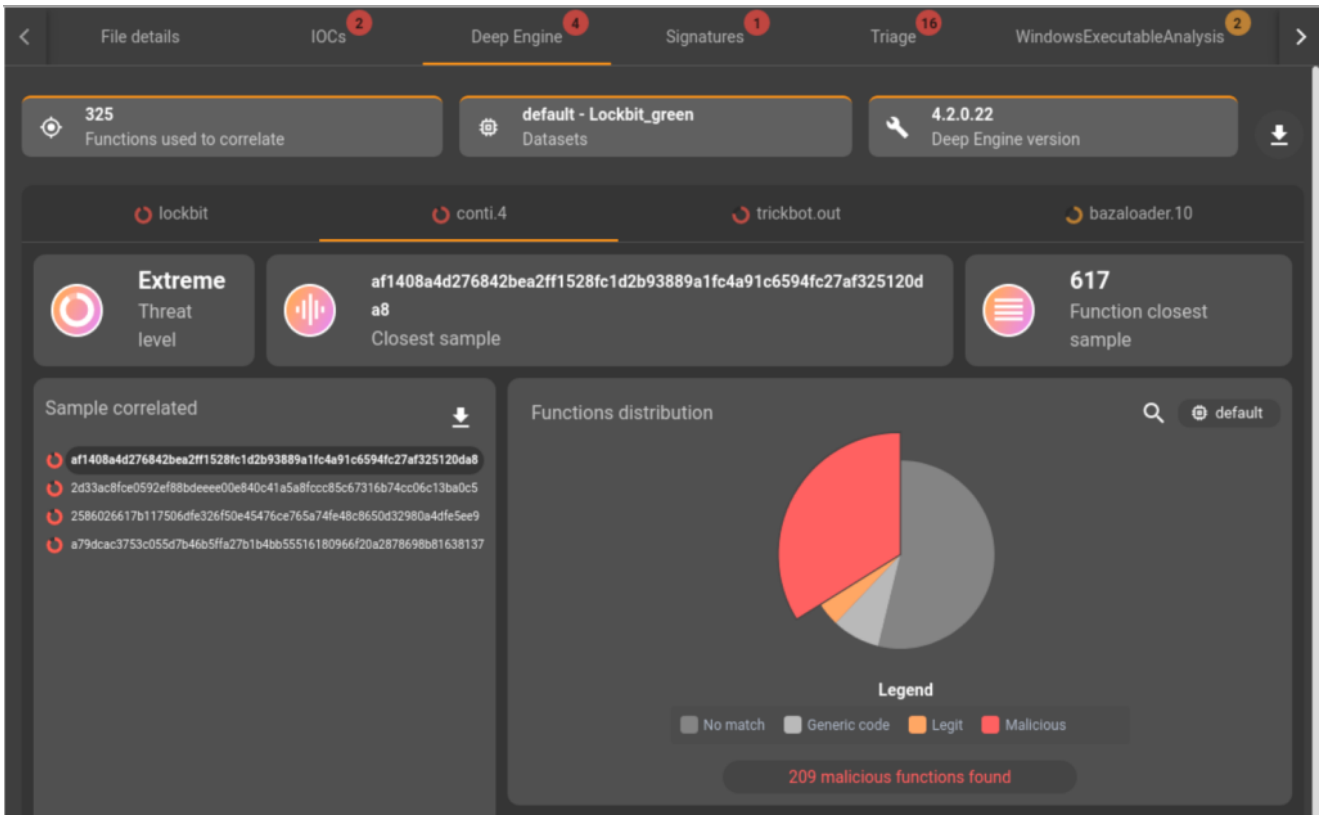
Un second fichier, associé à la même campagne que le précédent, a été analysé. A l'image de l'échantillon précédent, le Deep Engine remonte des similarités avec les familles *Conti* et *Lockbit* ainsi que des corrélations avec les familles *Trickbot* et *Bazaloader*.
Des éléments *Trickbot* sont utilisés par le groupe *Conti* lors de leurs attaques ce qui explique le lien trouvé ici. Pour *BazaLoader*, c'est un peu plus subtil : le groupe *BazaLoader* a en effet, comme *Lockbit*, utilisé le code de *Conti* qui a fuité en 2022. Les liens qui apparaissent ici montrent une transitivité dans les relations *Lockbit Green –> Conti <– BazaLoader*.



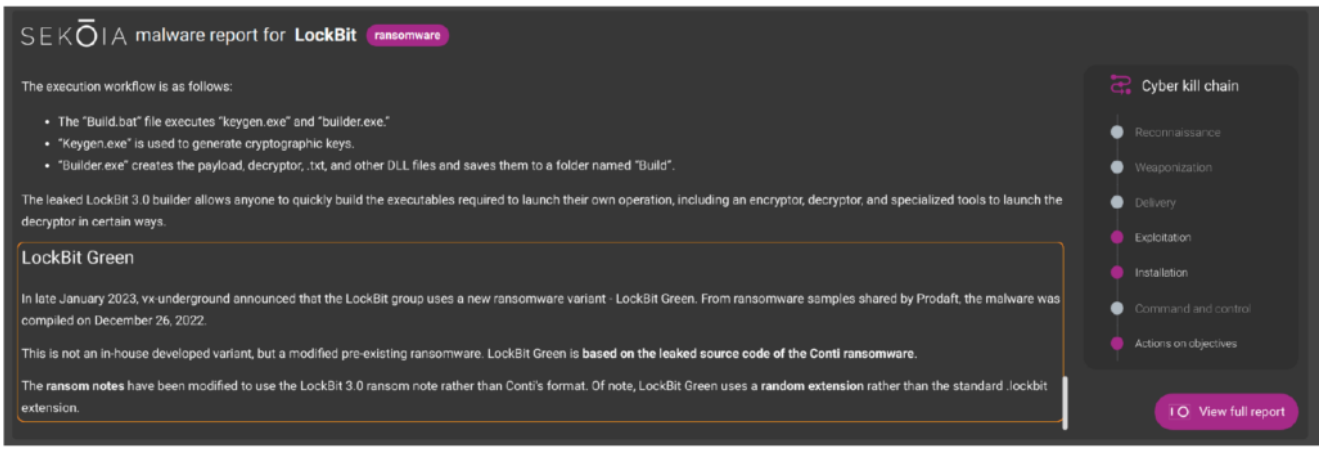
Analyse d'une troisième souche

924ec909e74a1d973d607e3ba1105a17e4337bd9a1c59ed5f9d3b4c25478fe11

Un troisième fichier, en lien avec la campagne des binaires précédemment analysés, a été soumis à notre plateforme d'analyse. Comme pour le second échantillon la technologie Deep Engine remonte des similarités avec les familles *Conti*, *Lockbit*, *Bazaloader* ainsi que *Trickbot*. Encore une fois, la corrélation avec ces familles est assez évidente au regard du lien évoqué dans l'analyse précédente.

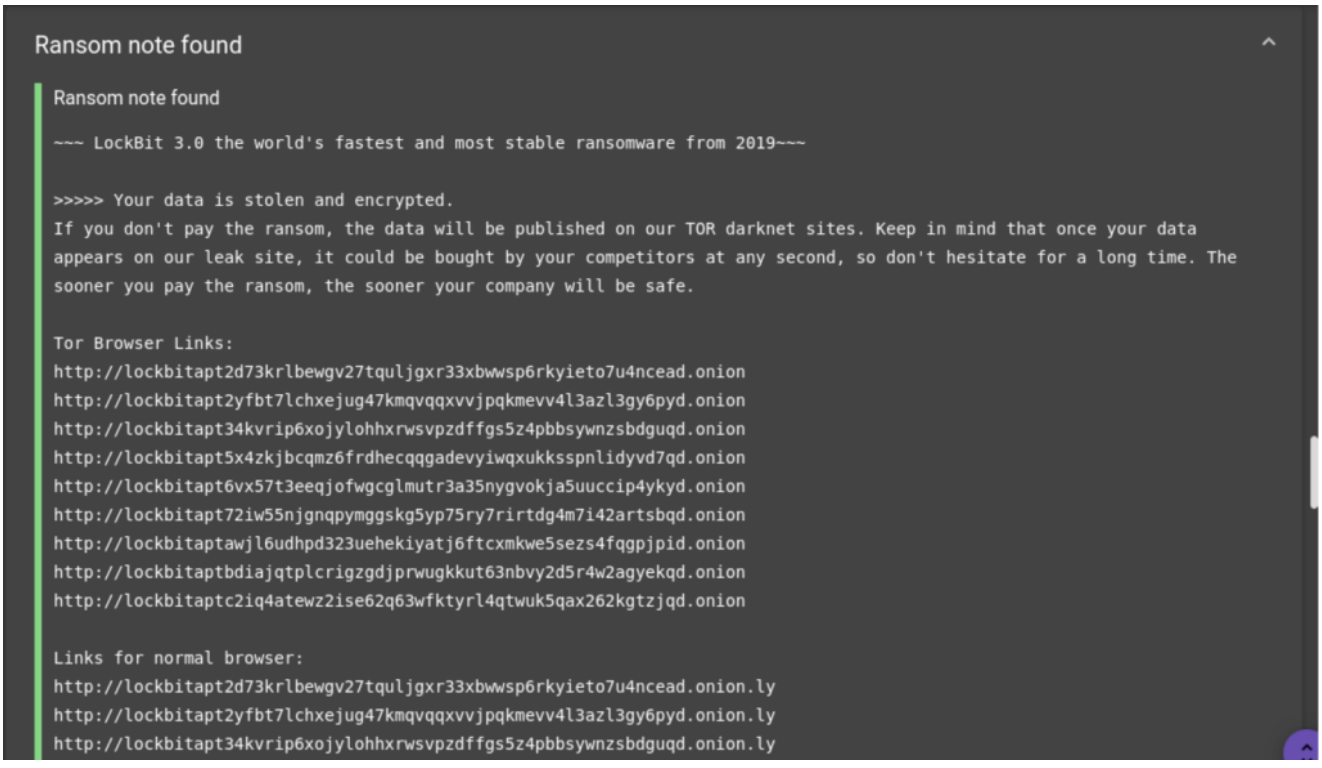


Par ailleurs, suite à la détection des familles *Lockbit*, nous pouvons grâce à notre partenariat avec la société experte en CTI *Sekoia.IO* intégrer le rapport d'analyse lié à ce groupe. Ce rapport nous permet de confirmer aussi le lien de code entre les familles *Lockbit* et *Conti*.

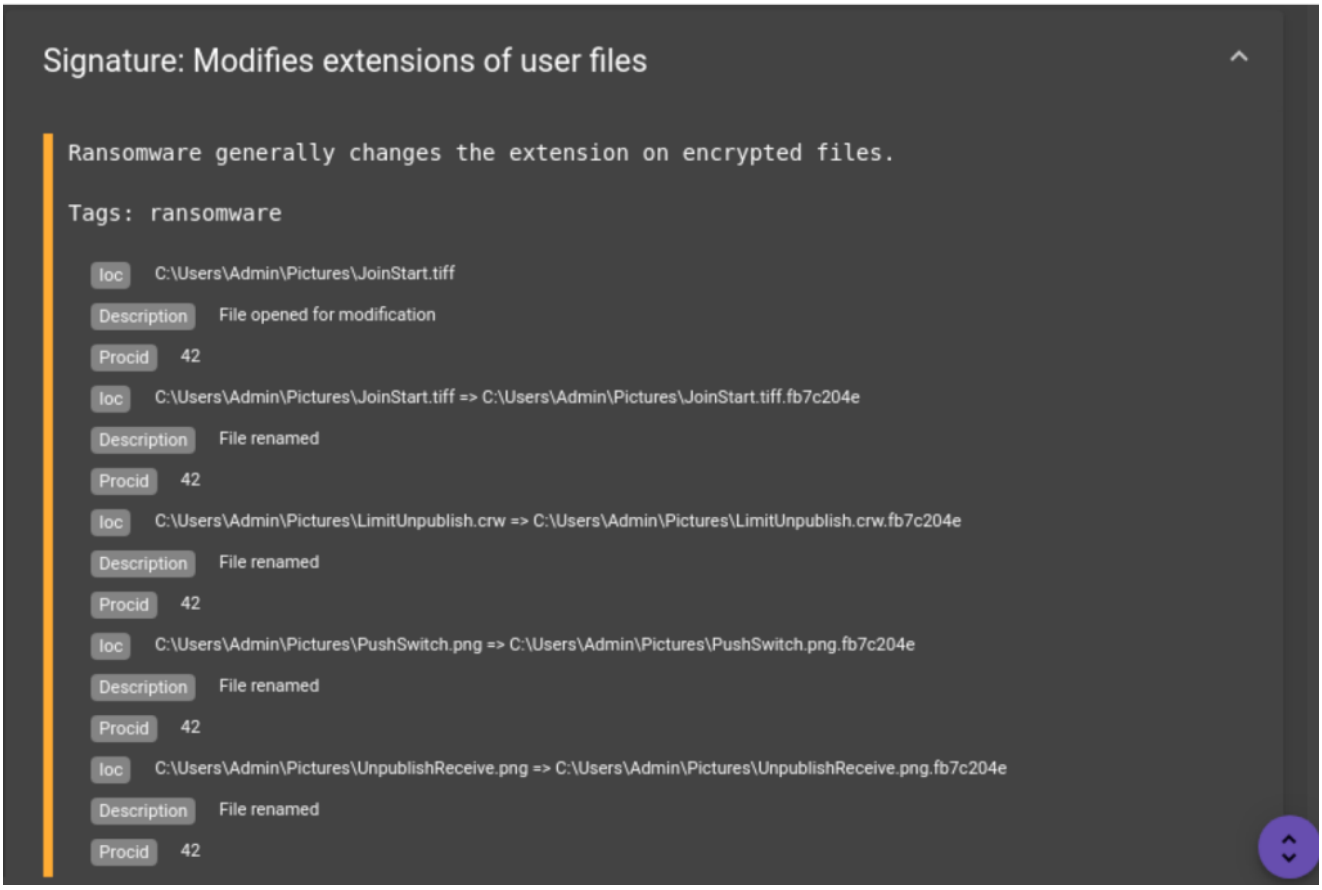


Cette fois-ci, la plateforme extrait un fichier dont les ioc sont des liens en *.onions*.

Ces liens, qui débutent par une chaîne de caractères *Lockbit*, laissent à penser qu'il s'agirait du portail de paiement de la rançon du groupe. Afin d'approfondir notre analyse et d'essorer ce malware, le fichier est soumis en analyse dynamique ce qui permet de récupérer la note de rançon du ransomware. Il semble que nous soyons bien face à un, voire plusieurs, variants *Lockbit*.



L'analyse en sandbox met aussi en avant le changement d'extension des fichiers avec une chaine de caractère aléatoire.



Contrairement aux précédentes versions, l'extension des fichiers chiffrés par *Lockbit* n'est plus ".lockbit" mais une chaîne de caractères aléatoires. La structure de la note de rançon est, quand à elle, la même que pour lockbit V3 (Lockbit Black).

Conclusion

Les différents résultats produits par les analyses combinés aux informations de CTI confirment ce que nous pensions au départ. Nous sommes effectivement face a des variants de *Lockbit* qui s'appuient sans vergogne sur du code *Conti*, la version Lockbit Green.

1. Le Deep Engine est le moteur de deep learning développé par GLIMPS, qui permet de comparer et corréler des codes informatiques. Il est utilisé au coeur de la plateforme GLIMPS Malware pour permettre la détection de logiciels malveillants, y compris lorsque les codes ont été modifiés par les attaquant.

N'hésitez pas à nous contacter pour en savoir plus : contact@glimps.re