RANSOMWARES ET CHARGEURS DE PROGRAMMES MALVEILLANTS

TÉLÉCHARGEZ LE DOCUMENT COMPLET ICI

PAYSAGE DES RANSOMWARES

Les ransomwares ont pris de l'ampleur et gagné en intensité en 2022, s'adaptant continuellement aux évolutions géopolitiques ainsi qu'aux efforts déployés par les acteurs de la cybersécurité et les forces de l'ordre. Dans ce contexte dynamique, certains groupes ont changé de nom, interrompu leurs activités et formé de nouveaux partenariats stratégiques. Cisco Talos a observé plusieurs tendances connexes en 2022.

Talos suit plus d'une douzaine de groupes utilisant les « ransomwares en tant que service » (RaaS) – **(Figure 1)**. D'après nos conclusions, LockBit a été le groupe le plus actif en 2022, représentant plus de 20 % du nombre total des publications de victimes sur le dark web, suivi de près par Hive et Black Basta. Ces résultats suggèrent une démocratisation accrue de l'usage des ransomwares, ce qui constitue un changement global par rapport aux années précédentes où seuls quelques groupes monopolisaient le paysage. Les cellules orchestrant les attaques par ransomware ne sont plus structurées en silos, mais œuvrent désormais entre plusieurs groupes. Aussi, les opérateurs disposant de compétences uniques peuvent intervenir dans une multitude de campagnes et d'organisations.

Les frictions se sont également intensifiées au sein de la communauté, la guerre en Ukraine ayant contraint de nombreux hackers à choisir un camp et à diriger leurs opérations contre des cibles pro-russes ou pro-ukrainiennes. Le groupe Conti RaaS a été l'un des acteurs les plus virulents, menaçant d'attaquer quiconque qui tenterait d'interférer dans l'invasion menée par la Russie. Un individu proche de Conti s'est vengé du groupe en divulguant des informations, dont le code source de programmes malveillants ainsi que des conversations internes entre ses membres. Dans le cadre d'un autre événement, Talos a eu connaissance de la fuite d'un builder

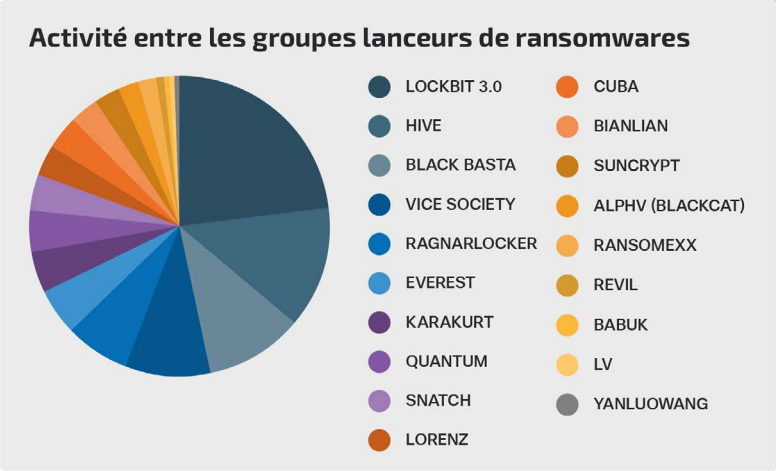

Figure 1. *Nombre de publications effectuées sur des sites de fuite de données suivis par Talos, de janvier à octobre.*

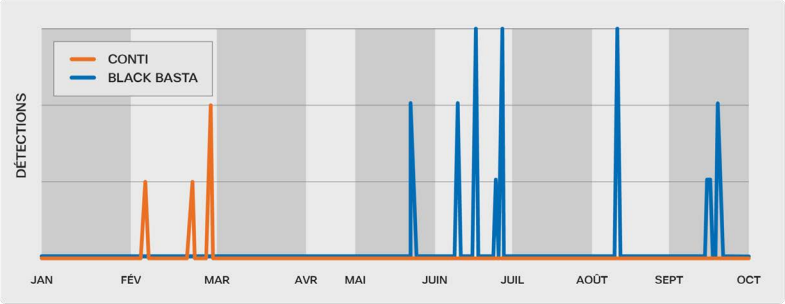

Figure 2. *Détections d'indicateurs de comportement dans Secure Malware Analytics pour les modifications du registre apportées par Black Basta et Conti.*

du ransomware de chiffrement LockBit 3.0, baptisé « LockBitBlack ». La personne revendiquant la responsabilité est un développeur présumé de LockBit qui, selon le groupe, était mécontent de la structure de paiement en place.

Ce type de tension est souvent à l'origine du changement de nom des groupes ou bien de l'émergence de nouvelles structures. Lorsque Conti a cessé ses activités et déconnecté son infrastructure, nous avons constaté une baisse générale des détections dans notre télémétrie. Cependant, peu de temps après, le groupe a réapparu sous la bannière de « Black Basta ». Les chercheurs estiment que les deux entités ont des modes de communication ainsi que des sites web de paiement et de fuite de données similaires – **Figure 2**.

RANSOMWARES ET CHARGEURS DE PROGRAMMES MALVEILLANTS

CHARGEURS DE PROGRAMMES MALVEILLANTS

Les chargeurs (ou « loaders »), c'est-à-dire des chevaux de Troie commerciaux qui déploient des programmes malveillants de deuxième niveau, représentent une menace constante qui continue d'avoir un impact mondial. Initialement développés comme des chevaux de Troie bancaires conçus pour compromettre des entités à des fins financières, ils se sont adaptés au fil du temps à des contrôles de sécurité plus stricts, jusqu'à devenir des menaces beaucoup plus sophistiquées. Ils fonctionnent désormais principalement avec des fonctions modulables, ce qui permet aux hackers de travailler avec une gamme d'outils open source et de nouveaux programmes malveillants. Selon notre analyse de plusieurs jeux de télémétrie de réseaux et de terminaux, les quatre chargeurs les plus actifs en 2022 ont été Qakbot, Emotet, IcedID et Trickbot – **Figure 3**.

Bien que nos analyses télémétriques aient détecté une activité associée à Trickbot, nous estimons qu'elle a été probablement générée par d'anciens terminaux infectés. En effet, les opérateurs de ce programme malveillant demeurent silencieux depuis début 2022. De son côté, et ce même s'il est toujours opérationnel, Emotet reste beaucoup moins actif qu'il ne l'était avant le démantèlement du botnet par les forces de l'ordre début janvier 2021. D'autres programmes malveillants ont comblé le vide en devenant plus populaires, à l'image de Qakbot et d'IcedID.

D'après une tendance générale observée en 2022, les opérateurs ont plus fréquemment déployé Qakbot, Emotet et IcedID via des fichiers ISO, ZIP ou LNK dans le but de déjouer les efforts de Microsoft pour bloquer les documents prenant en charge les macros. Talos a également remarqué que ces mêmes opérateurs téléchargeaient et lançaient des charges utiles malveillantes à l'aide de fichiers binaires de type « living-off-the-land » (LoLBins) trouvés dans les environnements des victimes. Dans certains cas, les hackers utilisant Qakbot et Emotet ont affiné leur séquence d'attaque en expérimentant différents LoLBins afin d'augmenter leurs chances de passer inaperçus.

Chargeurs de programmes malveillants

	Qakbot	IcedID	Emotet	Trickbot
Pseudonymes	Quackbot, Qbot, Pinkslipbot	BokBot	Geodo, Heodo	S.o.
Affiliations	Programmes malveillants de base probablement développés par des cybercriminels eurasiens	Aucune information	Programmes malveillants de base développés par Mummy Spider, un groupe de cybercriminels défendant les intérêts de la Russie	Programmes malveillants de base développés par Wizard Spider, un groupe de cybercriminels défendant les intérêts de la Russie
Activité depuis	2007	2014	2017	2016

Objectifs

- Obtenir un accès initial et établir la persistance pour faciliter les intrusions ultérieures.
- Déployer des programmes malveillants de niveau supérieur, y compris des ransomwares.

Victimologie

- Cible tous les secteurs dans le monde entier.
- Depuis la guerre entre la Russie et l'Ukraine, Trickbot a menacé de riposter contre les attaques visant le peuple russe.

TTP notables

- Hameçonnage, spams malveillants, ingénierie sociale, exploitation des vulnérabilités, vol de données (telles que les informations financières et d'identification) et propagation de vers.
- Hautement modulables, permettant aux opérateurs de mener un large éventail d'attaques.

Programmes malveillants et outils

- Les variantes se déploient et sont déployées par diverses familles de programmes malveillants, y compris les unes par les autres.
- Usage d'outils commerciaux comme Cobalt Strike et de LoLbins à différentes étapes du cycle de vie des attaques.

Figure 3. *Matrice des menaces liées aux chargeurs de programmes malveillants.*

Bien que nos analyses télémétriques aient détecté une activité associée à Trickbot, nous estimons qu'elle a été probablement générée par d'anciens terminaux infectés. En effet, les opérateurs de ce programme malveillant demeurent silencieux depuis début 2022. De son côté, et ce même s'il est toujours opérationnel, Emotet reste beaucoup moins actif qu'il ne l'était avant le démantèlement du botnet par les forces de l'ordre début janvier 2021. D'autres programmes malveillants ont comblé le vide en devenant plus populaires, à l'image de Qakbot et d'IcedID.

Un examen détaillé de chaque chargeur est disponible dans le rapport complet.