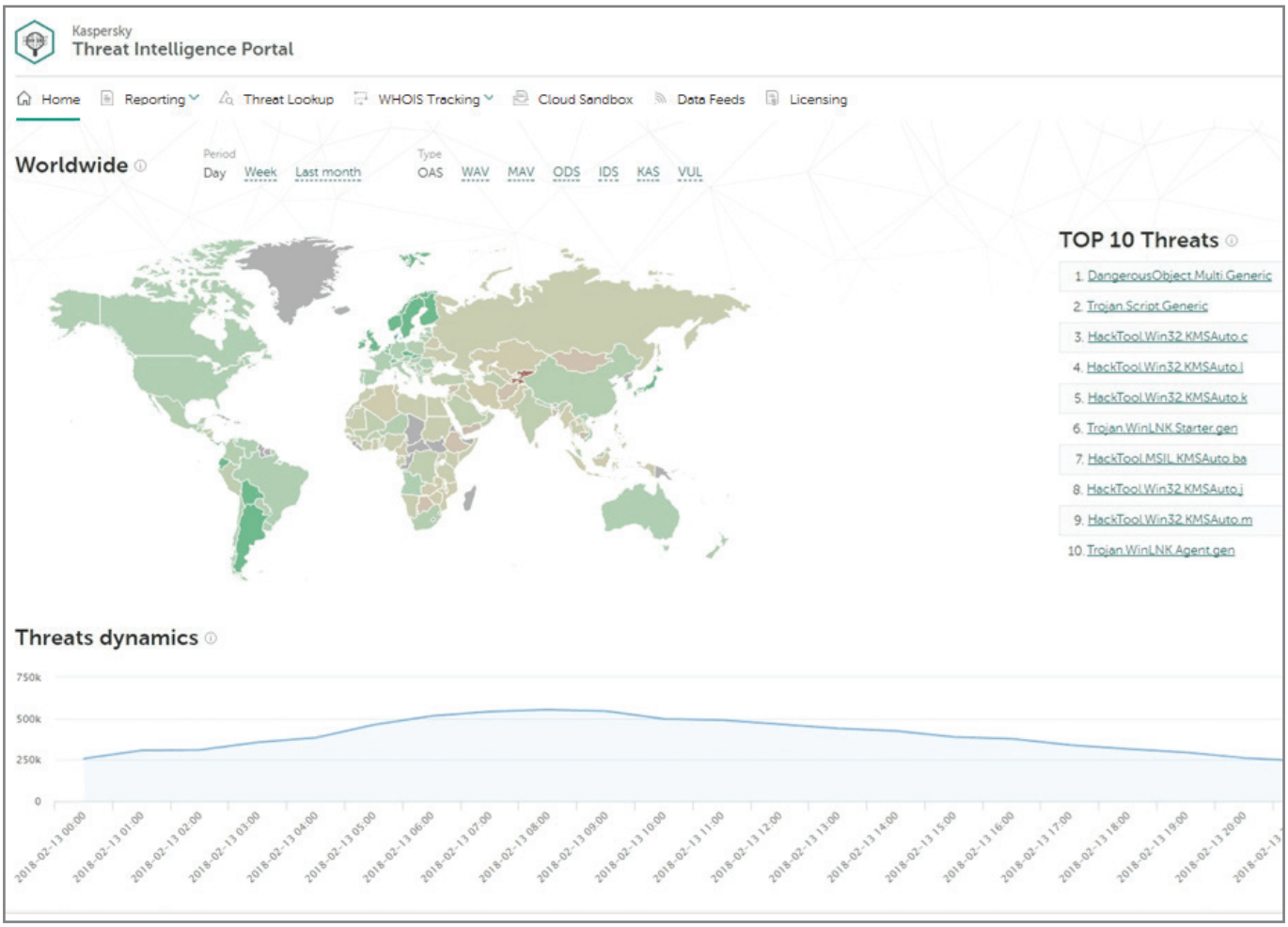
KASPERSKY lab

Portail Threat Intelligence de Kaspersky Lab : investigation des incidents et réponse adaptée

www.kaspersky.com/fraudprevention
#truecybersecurity

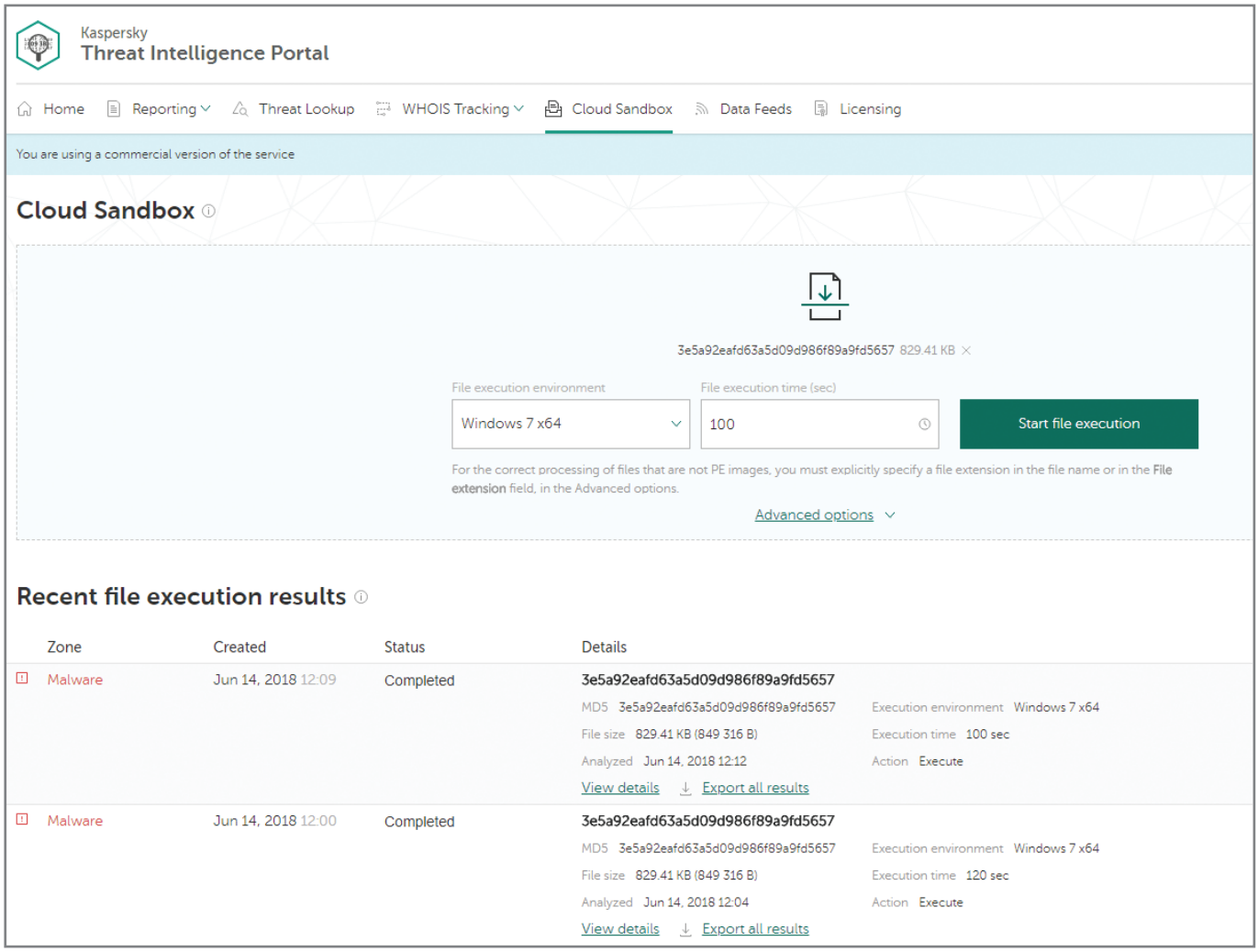
Le portail Threat Intelligence de Kaspersky Lab rassemble toutes les connaissances recueillies, raffinées et classées par Kaspersky Lab en plus de vingt ans d'existence. La plateforme récupère les dernières informations détaillées de Threat Intelligence sur les fichiers, les URL, les domaines, les adresses IP, les hachages de fichiers, les noms des menaces, les données statistiques/comportementales, les données WHOIS/DNS, etc. Grâce à ces informations, les responsables de la réponse aux incidents peuvent :

- Déterminer si un événement dans la file d'attente requiert une réponse immédiate ou un examen supplémentaire
- Utiliser la détection initiale comme point de départ pour évaluer l'ampleur d'un incident et réagir en conséquence
- Définir l'ampleur (personnes et matériel) et l'impact du problème et fournir des informations pertinentes aux autres services
- Comprendre les tactiques, les techniques et les objectifs des cybercriminels afin de déterminer la meilleure réponse possible

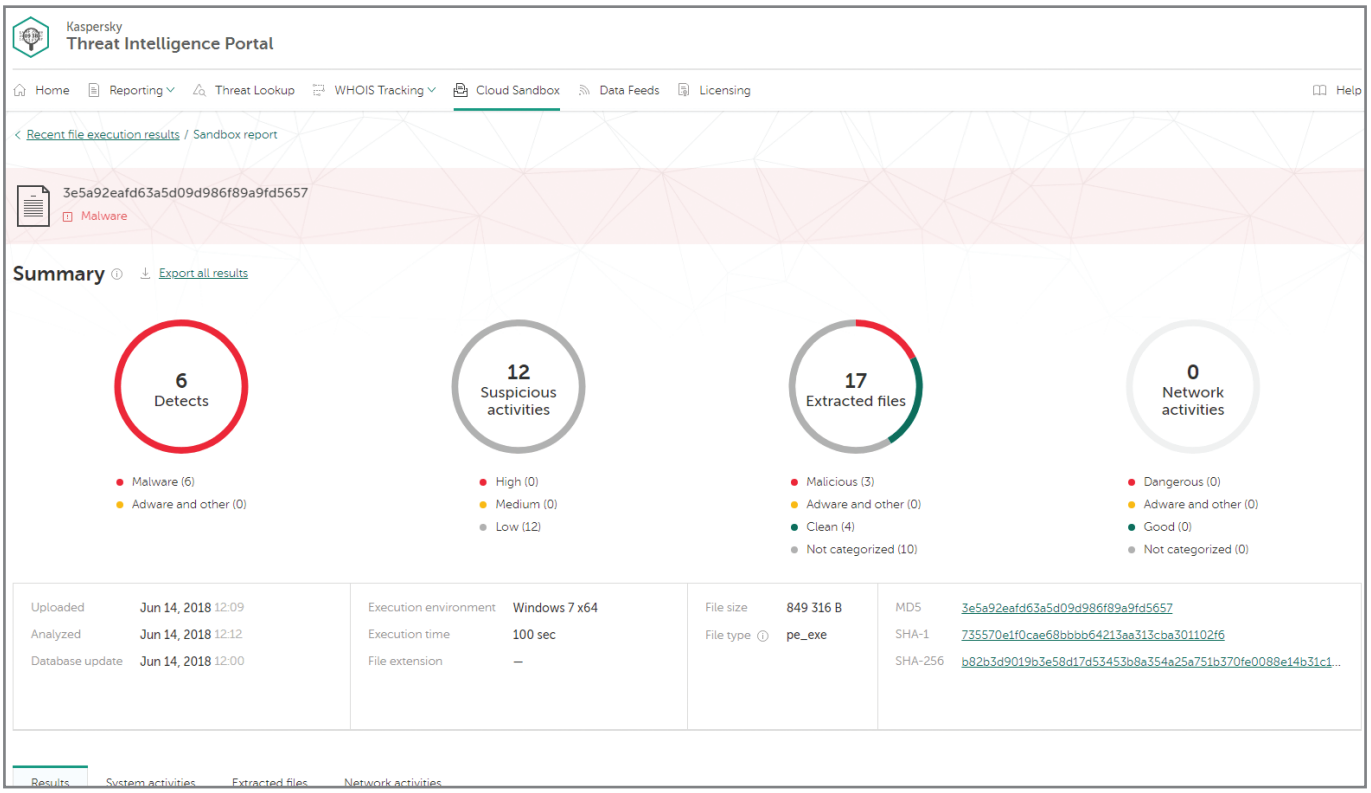


La page principale du portail Threat Intelligence propose de nombreux onglets, mais pour les besoins de notre exemple, imaginons que nous disposons d'une preuve en temps réel. L'équipe de réponse aux incidents a obtenu un échantillon de fichier suspect qui a initié une communication depuis l'intérieur du périmètre réseau avec une adresse IP externe en dehors des heures de travail normales. Nous pouvons donc passer directement à l'onglet Cloud Sandbox dans le menu supérieur.

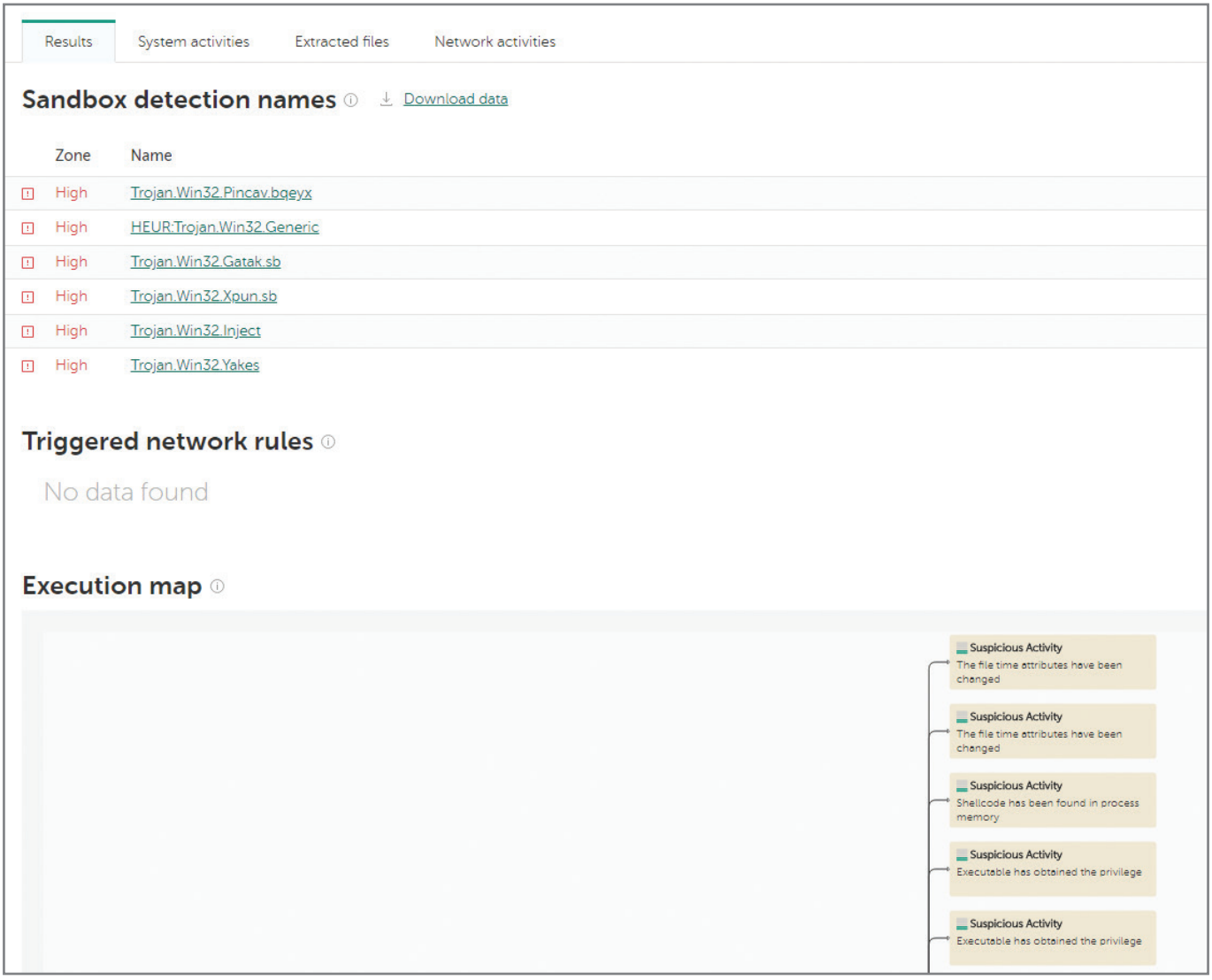
La sandbox exécute un objet suspect dans une machine virtuelle avec un système d'exploitation complet. Elle détecte l'activité malveillante d'un objet en analysant son comportement. La machine virtuelle est isolée de la véritable infrastructure d'entreprise, de sorte que la détonation ne cause aucun dommage réel. Téléchargez votre fichier, sélectionnez l'environnement (ici, Windows 7) et la durée (disons 100 secondes), puis lancez l'exécution :



Un antivirus peut passer totalement à côté d'un fichier suspect, mais la sandbox est très efficace contre les programmes malveillants qui échappent à l'analyse statique. Même si un fichier est identifié comme « dangereux », la plupart des systèmes antivirus ne peuvent pas expliquer à quel point il est dangereux, ni ce qui se passe exactement. Pour obtenir plus de détails, voyons ce qui se passe dans la Kaspersky Cloud Sandbox après la détonation :



Après exécution de l'objet testé, la sandbox récupère les artefacts, les analyse et rend son verdict. Voici le résumé : détections (6), activités suspectes (12), fichiers extraits (17) et activités réseau (0). Cette analyse révèle qu'il ne s'agit pas seulement d'un fichier « dangereux », elle liste également les différentes actions dangereuses qu'il effectue.



Results | System activities | Extracted files | Network activities

Sandbox detection names

Download data

Zone	Name
High	Trojan.Win32.Pincav.bqeyx
High	HEUR:Trojan.Win32.Generic
High	Trojan.Win32.Gatak.sb
High	Trojan.Win32.Xpun.sb
High	Trojan.Win32.Inject
High	Trojan.Win32.Yakes

Triggered network rules

No data found

Execution map

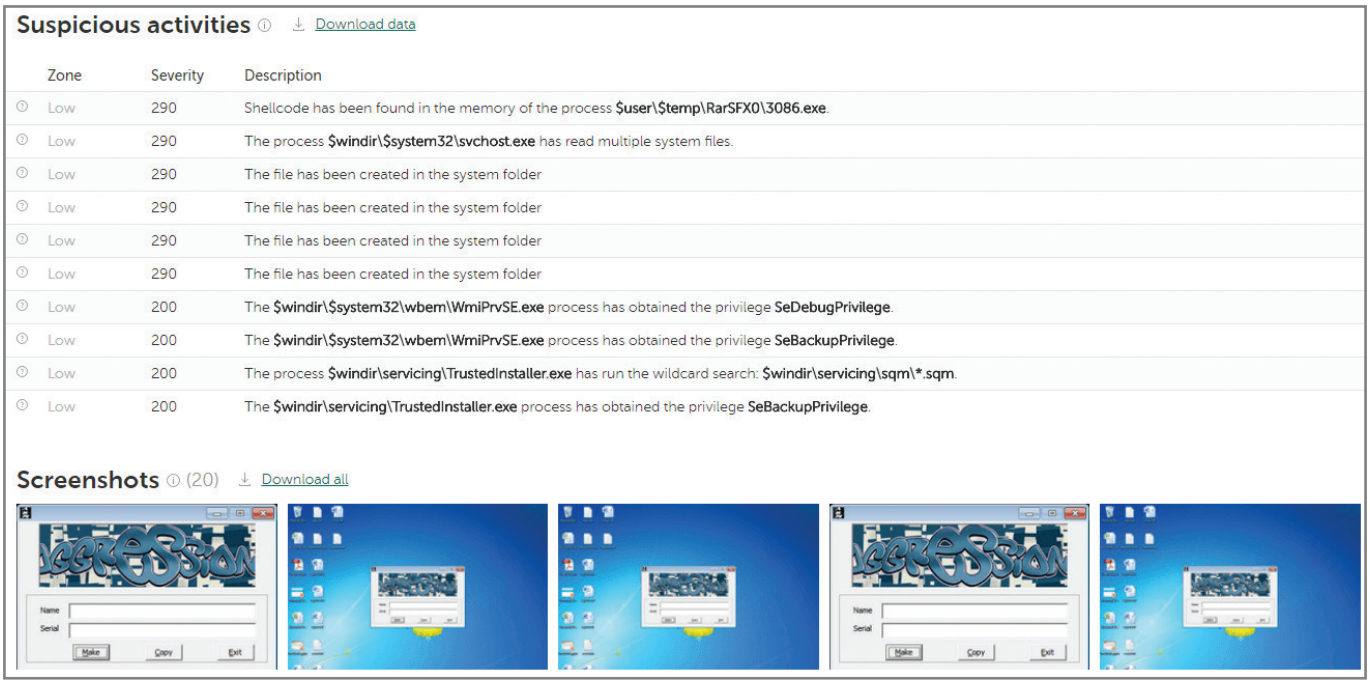
Suspicious Activity
The file time attributes have been changed

Suspicious Activity
The file time attributes have been changed

Suspicious Activity
Shellcode has been found in process memory

Suspicious Activity
Executable has obtained the privilege

Suspicious Activity
Executable has obtained the privilege



Suspicious activities

Download data

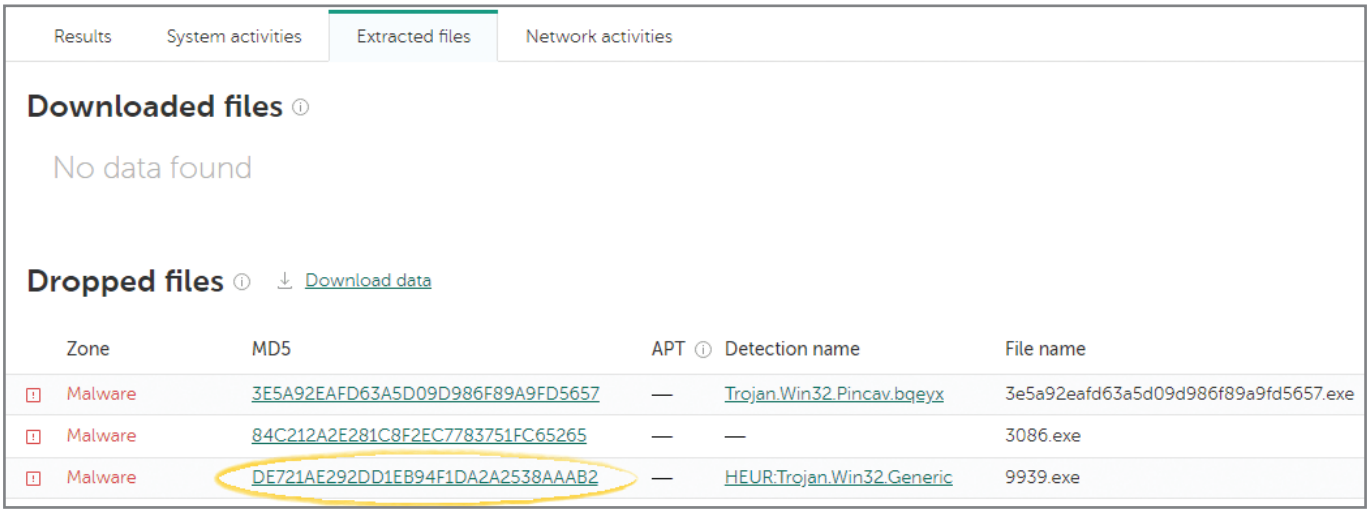
Zone	Severity	Description
Low	290	Shellcode has been found in the memory of the process **$user\$temp\RarSFX0\3086.exe**.
Low	290	The process **$windir\$system32\svchost.exe** has read multiple system files.
Low	290	The file has been created in the system folder
Low	290	The file has been created in the system folder
Low	290	The file has been created in the system folder
Low	290	The file has been created in the system folder
Low	200	The **$windir\$system32\wbem\WmiPrvSE.exe** process has obtained the privilege **SeDebugPrivilege**.
Low	200	The **$windir\$system32\wbem\WmiPrvSE.exe** process has obtained the privilege **SeBackupPrivilege**.
Low	200	The process **$windir\servicing\TrustedInstaller.exe** has run the wildcard search: **$windir\servicing\sqm*.sqm**.
Low	200	The **$windir\servicing\TrustedInstaller.exe** process has obtained the privilege **SeBackupPrivilege**.

Screenshots (20)

Download all

Dans l'onglet Résultats, le responsable de la réponse aux incidents peut voir les captures d'écran prises pendant l'exécution. Dans certains cas, le logiciel malveillant tente d'échapper à l'analyse automatique en attendant une interaction de l'utilisateur (saisie d'un mot de passe, défilement d'un document, mouvement de la souris, etc.). La Kaspersky Cloud Sandbox connaît ces techniques d'évasion et utilise des technologies simulant une interaction humaine pour les contrer. Les captures d'écran sont également très utiles : un chercheur peut voir ce qui se passe dans « l'éprouvette » depuis un point de vue humain.

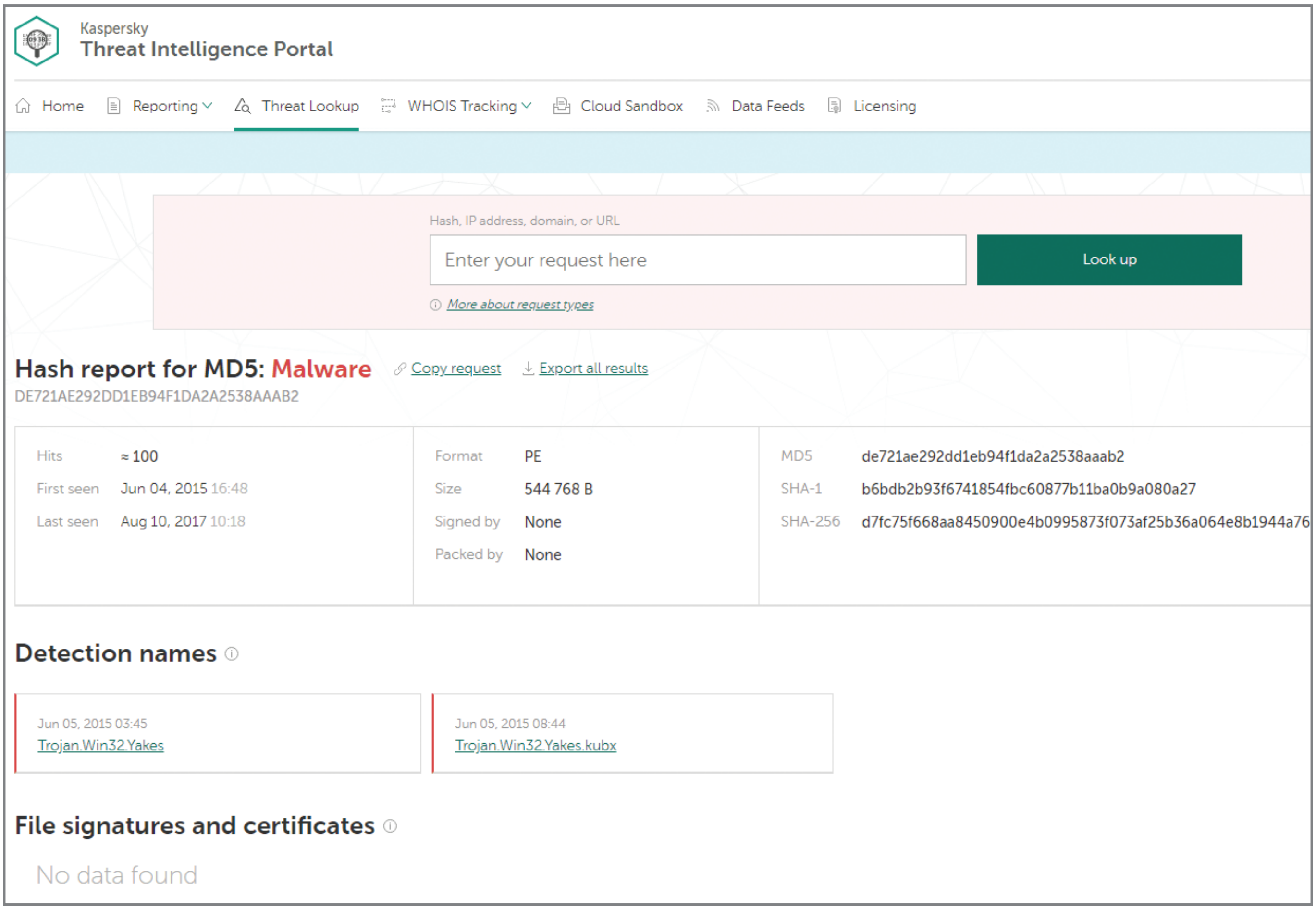
Passons à l'onglet Fichiers extraits pour voir les objets téléchargés, extraits ou déposés. Dans notre exemple, un fichier malveillant a été déposé :



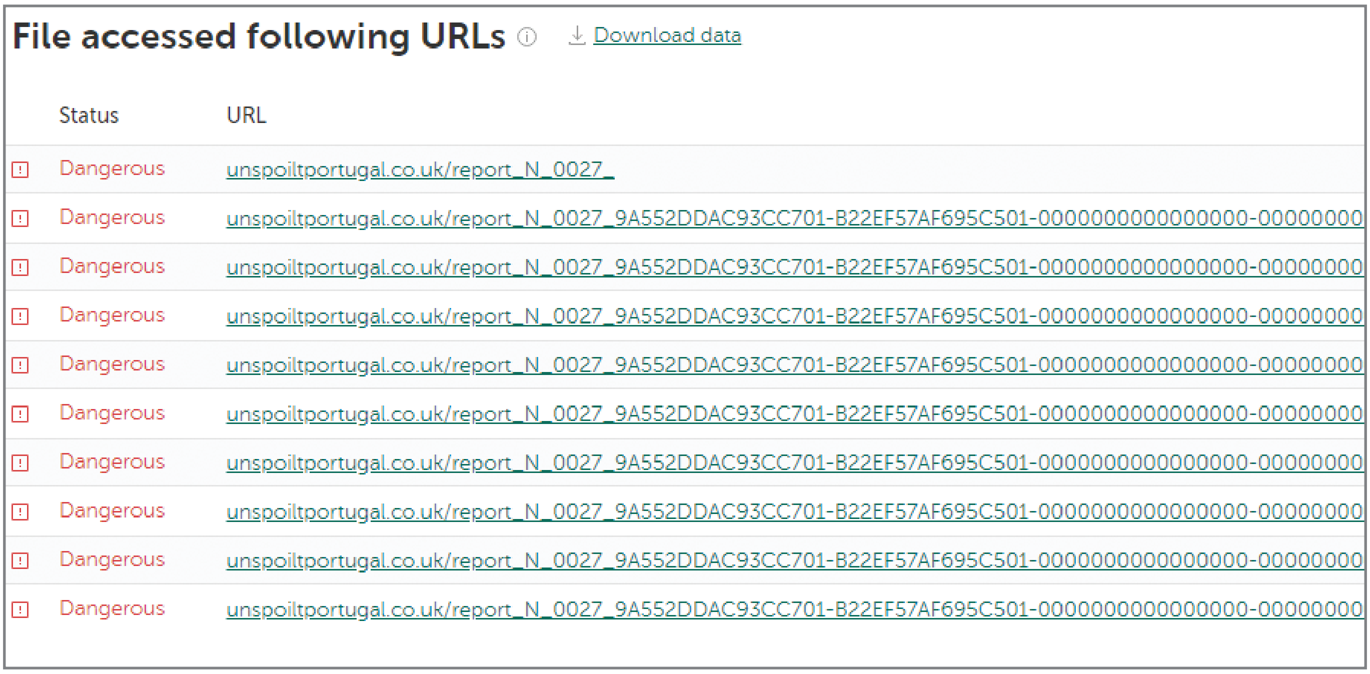
Les fonctionnalités d'une sandbox classique s'arrêteraient là : vous avez exécuté le fichier, obtenu une liste des activités malveillantes... et c'est tout. Cependant, grâce au portail Threat Intelligence de Kaspersky Lab, vous pouvez basculer directement vers Threat Lookup pour obtenir des informations plus détaillées sur les indicateurs de compromission et leurs relations.

Threat Lookup est notre moteur de recherche pour la sécurité. Il contient environ 5 pétaoctets de données de Threat Intelligence, recueillies et classées par Kaspersky Lab au cours des 20 dernières années : hachages de fichiers, données statistiques/comportementales, données WHOIS/DNS, URL, adresses IP, etc.

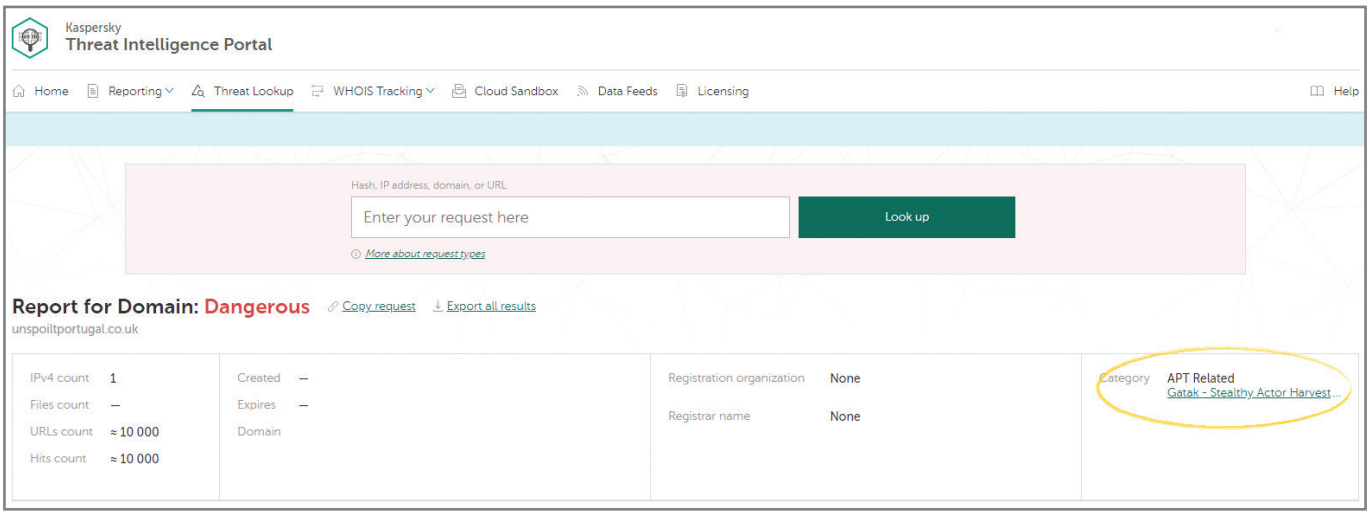
Ainsi, après avoir exécuté notre échantillon dans la sandbox, nous pouvons immédiatement utiliser les résultats pour des requêtes de recherche dans Threat Lookup, en cliquant simplement sur l'objet (ici, un hachage MD5)



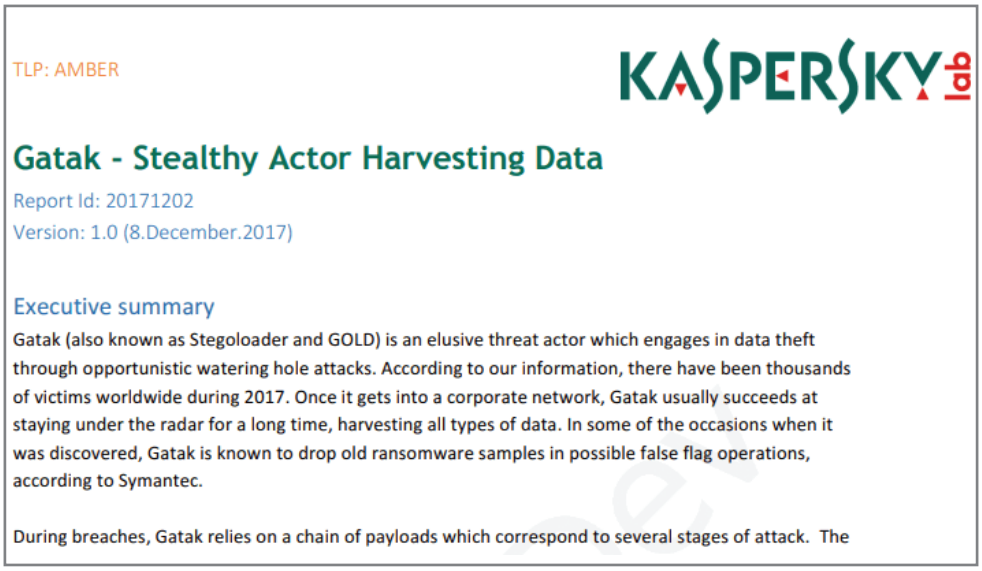
Nous disposons maintenant d'un rapport plus détaillé sur le programme malveillant. Consultons les résultats de Threat Lookup pour identifier les URL auxquelles le programme malveillant a accédé :



Voici une URL marquée comme « dangereuse ». Une fois encore, faisons une recherche sur cette URL malveillante dans Threat Lookup :



Il s'avère que cette URL malveillante est associée à une attaque APT ! Le portail Threat Intelligence de Kaspersky Lab vous propose de télécharger un rapport APT. Ce fichier PDF inclut un sommaire, des données techniques détaillées et une liste des indicateurs de compromission associés. Il peut être intéressant de vérifier si votre organisation a déjà rencontré un cas similaire et de développer rapidement des cas d'utilisation spécifiques pour la détection de l'attaque décrite.


TLP: AMBER

KASPERSKY lab

Gatak - Stealthy Actor Harvesting Data

Report Id: 20171202
Version: 1.0 (8.December.2017)

Executive summary

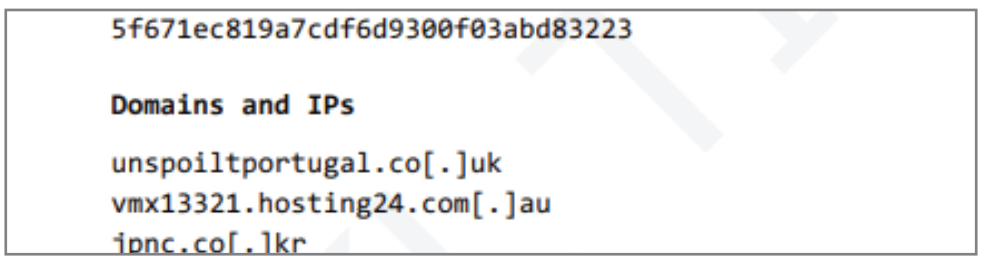
Gatak (also known as Stegoloader and GOLD) is an elusive threat actor which engages in data theft through opportunistic watering hole attacks. According to our information, there have been thousands of victims worldwide during 2017. Once it gets into a corporate network, Gatak usually succeeds at staying under the radar for a long time, harvesting all types of data. In some of the occasions when it was discovered, Gatak is known to drop old ransomware samples in possible false flag operations, according to Symantec.

During breaches, Gatak relies on a chain of payloads which correspond to several stages of attack. The


Appendix I - Indicators of compromise

Stage 0 hashes

0AE26BA127904EC354F228B316F044A1
0B20B941D2B9372D875410FFEB53C473


5f671ec819a7cdf6d9300f03abd83223

Domains and IPs

unspoiltportugal.co[.]uk
vmx13321.hosting24.com[.]au
jpnc.co[.]kr

Le portail Threat Intelligence de Kaspersky Lab vous offre de nombreux avantages :

- Améliorez et accélérez votre processus de réponse aux incidents et vos capacités de diagnostic en fournissant aux équipes de sécurité/SOC des informations utiles sur les menaces et un aperçu global de la logique qui sous-tend les attaques ciblées. Diagnostiquez et analysez plus efficacement les incidents de sécurité qui frappent les hébergeurs et le réseau, et hiérarchisez les signaux émis par les systèmes internes face à des menaces inconnues afin de réduire le délai d'intervention et de perturber la chaîne de frappe avant que des données et des systèmes critiques ne soient compromis.

- Examinez de manière approfondie les indicateurs de menace (adresses IP, URL, domaines, hachages de fichiers) dotés d'un contexte hautement validé afin de hiérarchiser les attaques, de prendre de meilleures décisions concernant la dotation en personnel et l'affectation des ressources, et de mettre l'accent sur l'atténuation des menaces les plus dangereuses pour votre entreprise.

- Limitez les attaques ciblées. Optimisez vos infrastructures de sécurité grâce à une veille tactique et stratégique, ainsi qu'à des stratégies de défense et de lutte adaptées contre les menaces qui pèsent sur votre entreprise.

Kaspersky Lab
Solutions de cybersécurité pour les entreprises :
www.kaspersky.fr/enterprise-security
Actualités dédiées aux cybermenaces :
http://www.viruslist.com/fr/
Actualités dédiées à la sécurité informatique :
https://www.kaspersky.fr/blog/b2b/

#truecybersecurity
#HuMachine

www.kaspersky.fr