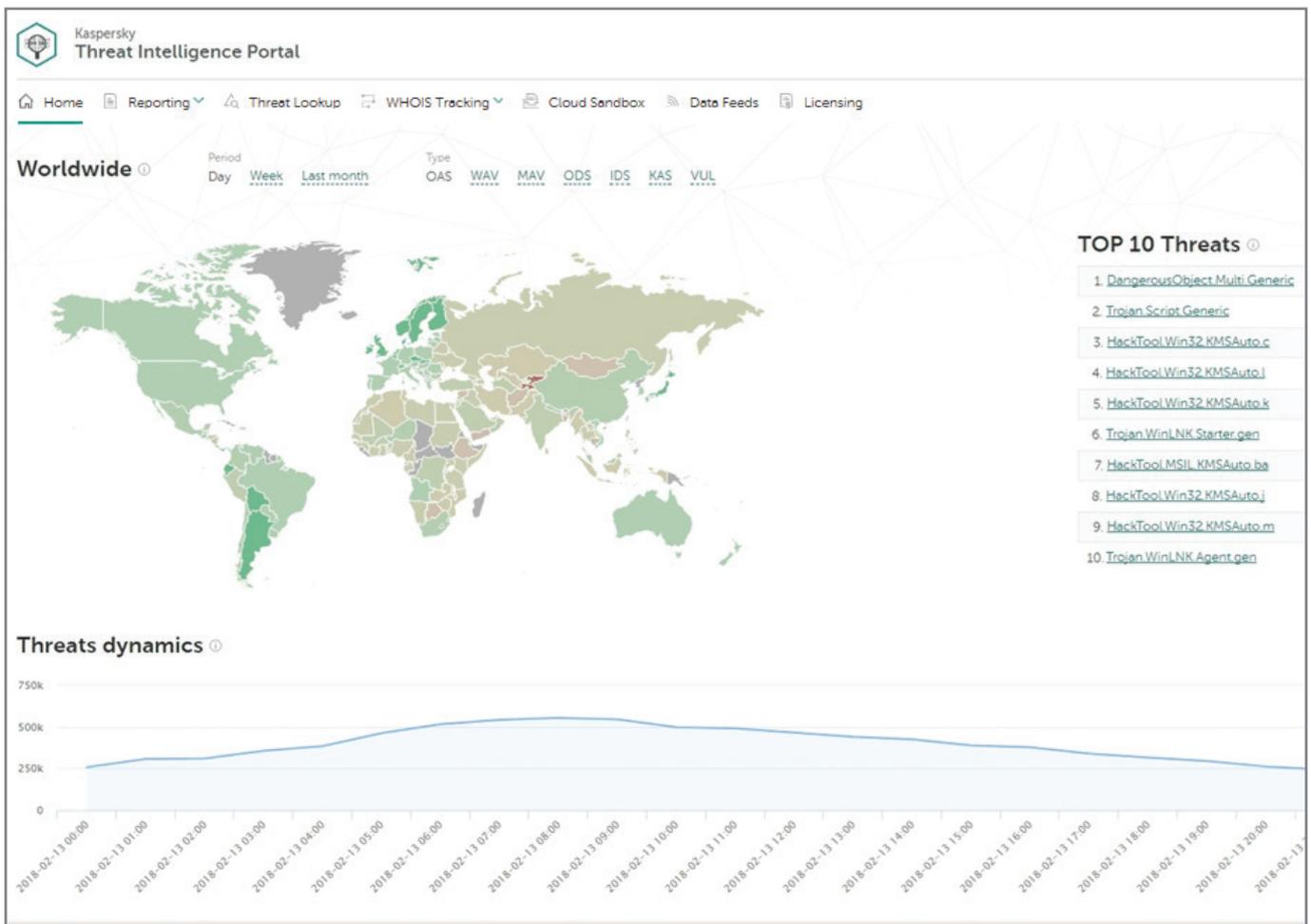


Portail Threat Intelligence de Kaspersky Lab : investigation des incidents et réponse adaptée

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 :

Kaspersky Threat Intelligence Portal

Home Reporting Threat Lookup WHOIS Tracking Cloud Sandbox Data Feeds Licensing

You are using a commercial version of the service

Cloud Sandbox

3e5a92eafd63a5d09d986f89a9fd5657 829.41 KB ×

File execution environment: Windows 7 x64 | File execution time (sec): 100

[Start file execution](#)

For the correct processing of files that are not PE images, you must explicitly specify a file extension in the file name or in the File extension field, in the Advanced options.

[Advanced options](#)

Recent file execution results

Zone	Created	Status	Details
Malware	Jun 14, 2018 12:09	Completed	3e5a92eafd63a5d09d986f89a9fd5657 MD5 3e5a92eafd63a5d09d986f89a9fd5657 Execution environment Windows 7 x64 File size 829.41 KB (849 316 B) Execution time 100 sec Analyzed Jun 14, 2018 12:12 Action Execute View details Export all results
Malware	Jun 14, 2018 12:00	Completed	3e5a92eafd63a5d09d986f89a9fd5657 MD5 3e5a92eafd63a5d09d986f89a9fd5657 Execution environment Windows 7 x64 File size 829.41 KB (849 316 B) Execution time 120 sec Analyzed Jun 14, 2018 12:04 Action Execute View details Export all results

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 :

Kaspersky Threat Intelligence Portal

Home Reporting Threat Lookup WHOIS Tracking Cloud Sandbox Data Feeds Licensing Help

< Recent file execution results / Sandbox report

3e5a92eafd63a5d09d986f89a9fd5657 Malware

Summary

[Export all results](#)

<p>6 Detects</p> <ul style="list-style-type: none"> Malware (6) Adware and other (0) 	<p>12 Suspicious activities</p> <ul style="list-style-type: none"> High (0) Medium (0) Low (12) 	<p>17 Extracted files</p> <ul style="list-style-type: none"> Malicious (3) Adware and other (0) Clean (4) Not categorized (10) 	<p>0 Network activities</p> <ul style="list-style-type: none"> Dangerous (0) Adware and other (0) Good (0) Not categorized (0)
---	---	---	---

Uploaded: Jun 14, 2018 12:09	Execution environment: Windows 7 x64	File size: 849 316 B	MD5: 3e5a92eafd63a5d09d986f89a9fd5657
Analyzed: Jun 14, 2018 12:12	Execution time: 100 sec	File type: pe_exe	SHA-1: 735570e1f0cae68bbb64213aa313cba30110246
Database update: Jun 14, 2018 12:00	File extension: -		SHA-256: b82b3d9019b3e58d17d53453b8a354a25a751b370fe0088e14b31c1...

Results | System activities | Extracted files | Network activities

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.Xpwn.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 :

Zone	MD5	APT	Detection name	File name
Malware	3E5A92EAFD63A5D09D986F89A9FD5657	—	Trojan.Win32.Pincav.bqeyx	3e5a92eafd63a5d09d986f89a9fd5657.exe
Malware	84C212A2E281C8F2EC7783751FC65265	—	—	3086.exe
Malware	DE721AE292DD1EB94F1DA2A2538AAAB2	—	HEUR:Trojan.Win32.Generic	9939.exe

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)



Hash, IP address, domain, or URL

Enter your request here

Look up

[More about request types](#)

Hash report for MD5: **Malware** [Copy request](#) [Export all results](#)

DE721AE292DD1EB94F1DA2A2538AAAB2

Hits	≈ 100	Format	PE	MD5	de721ae292dd1eb94f1da2a2538aaab2
First seen	Jun 04, 2015 16:48	Size	544 768 B	SHA-1	b6bdb2b93f6741854fbc60877b11ba0b9a080a27
Last seen	Aug 10, 2017 10:18	Signed by	None	SHA-256	d7fc75f668aa8450900e4b0995873f073af25b36a064e8b1944a76
		Packed by	None		

Detection names

Jun 05, 2015 03:45 Trojan.Win32.Yakes	Jun 05, 2015 08:44 Trojan.Win32.Yakes.kubx
--	---

File signatures and certificates

No data found

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 :

File accessed following URLs [Download data](#)

Status	URL
D Dangerous	unspoilportugal.co.uk/report_N_0027_
D Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
D Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
D Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
D Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
D Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
D Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
D Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
D Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
D Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000

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

The screenshot shows the Kaspersky Threat Intelligence Portal interface. At the top, there is a navigation bar with options like Home, Reporting, Threat Lookup, WHOIS Tracking, Cloud Sandbox, Data Feeds, and Licensing. Below this is a search bar with the placeholder text 'Enter your request here' and a 'Look up' button. The search results show a report for the domain 'unspoilportugal.co.uk' with a status of 'Dangerous'. The report includes statistics such as IPv4 count (1), Files count (-), URLs count (≈ 10 000), and Hits count (≈ 10 000). The registration organization is listed as 'None' and the registrar name is also 'None'. A yellow circle highlights the 'Category' field, which reads 'APT Related Gatak - Stealthy Actor Harvesting Data'.

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.

The screenshot shows a Kaspersky Lab report titled 'Gatak - Stealthy Actor Harvesting Data'. The report is marked as 'TLP: AMBER'. It includes the report ID '20171202' and version '1.0 (8.December.2017)'. The 'Executive summary' section describes Gatak as an elusive threat actor that engages in data theft through opportunistic watering hole attacks. It mentions that Gatak has been active since 2017 and is known for dropping old ransomware samples in false flag operations. The report also includes a section for 'Appendix I - Indicators of compromise', which lists 'Stage 0 hashes' and 'Domains and IPs'. The hashes listed are 0AE26BA127904EC354F228B316F044A1, 0B20B941D2B9372D875410FFEB53C473, and 166200F58C50EABE40B22BE200DE4724. The domains and IPs listed are 5f671ec819a7cdf6d9300f03abd83223, unspoilportugal.co[.]uk, vmx13321.hosting24.com[.]au, and ipnc.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/entreprise-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

© 2019 Kaspersky Lab. Tous droits réservés. Les marques déposées et marques de service sont la propriété de leurs détenteurs respectifs.

