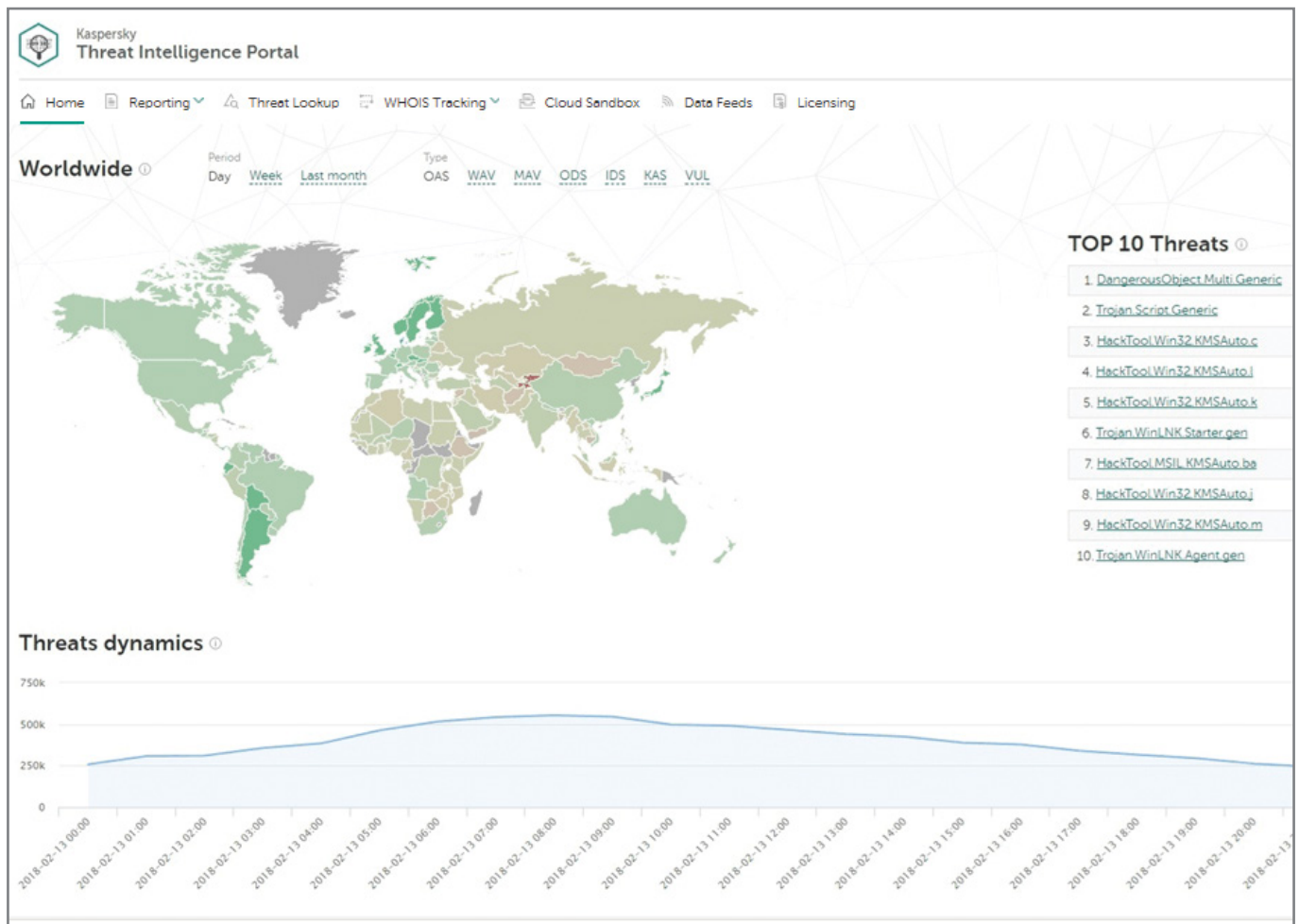


The Kaspersky Threat Intelligence Portal: Investigación y respuesta a incidentes

latam.kaspersky.com/fraudprevention
#truecybersecurity

Kaspersky Threat Intelligence Portal ofrece todos los conocimientos que Kaspersky Lab ha recopilado, perfeccionado y clasificado durante más de los 20 años de historia de la compañía. La plataforma recoge las últimas novedades de la inteligencia de amenazas sobre archivos, URL, dominios, direcciones IP, archivos hash, nombres de amenazas, datos de estadística/comportamiento, datos WHOIS/DNS, etc., que permiten a los equipos responder a incidentes:

- Determinen si uno de los eventos de la fila requiere una respuesta inmediata o una valoración adicional.
- Utilicen la primera detección como punto de partida para determinar el alcance total de un incidente y responder de acuerdo con la situación.
- Definan quién y qué se ha visto afectado y cuál ha sido el impacto y ofrezcan información significativa a otros departamentos relevantes.
- Entiendan las tácticas y técnicas utilizadas por los cibercriminales, además de sus objetivos para determinar la respuesta más efectiva.



La página principal de Kaspersky Threat Intelligence Portal tiene muchas pestañas. Por ejemplo, si el equipo de respuesta a incidentes obtiene la muestra de un archivo sospechoso que ha iniciado comunicación desde dentro del perímetro de la red con una dirección IP externa, fuera del horario laboral, podemos ir directamente a la pestaña Cloud Sandbox del menú superior.

La función de aislamiento de procesos ejecuta un objeto sospechoso, detectado tras analizar su actividad, en una máquina virtual (VM por sus siglas en inglés) con un sistema operativo completo. Las VM están aisladas de la infraestructura empresarial real, por lo que la detonación no causará daños reales. Simplemente suba el archivo, seleccione el entorno (Windows 7, en este caso), seleccione el tiempo (por ejemplo, 100 segundos) y comience la ejecución:

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

Los entornos aislados son efectivos contra el malware que evade el análisis de estadística y que, por tanto, se le podría escapar a su antivirus. Incluso si un archivo se identifica como “perjudicial”, la mayoría de los sistemas antivirus no podrán explicar su nivel de peligrosidad ni la situación. Para más información, veamos qué sucede tras la detonación en Cloud Sandbox:

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](#)

6
Detects

Malware (6)
Adware and other (0)

12
Suspicious activities

High (0)
Medium (0)
Low (12)

17
Extracted files

Malicious (3)
Adware and other (0)
Clean (4)
Not categorized (10)

0
Network activities

Dangerous (0)
Adware and other (0)
Good (0)
Not categorized (0)

Uploaded Jun 14, 2018 12:09 Analyzed Jun 14, 2018 12:12 Database update Jun 14, 2018 12:00	Execution environment Windows 7 x64 Execution time 100 sec File extension —	File size 849 316 B File type pe_exe	MD5 3e5a92eafd63a5d09d986f89a9fd5657 SHA-1 735570e1f0cae68bbb64213aa313cba301102f6 SHA-256 b82b3d9019b3e58d17d53453b8a354a25a751b370fe0088e14b31c1...
--	---	---	---

Results
System activities
Extracted files
Network activities

Tras ejecutar el objeto a analizar, un entorno aislado recopila los objetos, los analiza y emite un dictamen. Este es el resumen: detecciones (6), actividades sospechosas (12), archivos extraídos (17) y actividades de red (0). No se trata solo de un archivo “perjudicial”, sino que puede llevar a cabo muchas más acciones dañinas.

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

Download all

En la pestaña Results, la persona que interviene en un incidente puede ver capturas de pantalla durante la ejecución. En algunos casos, el malware intenta evadir los análisis automáticos esperando la interacción del usuario (introducir una contraseña, revisar un documento, mover el ratón, etc.). Kaspersky Cloud Sandbox conoce muchas técnicas de evasión y utiliza tecnologías de simulación de personas para detectarlas. Las capturas de pantalla también pueden ser útiles porque un investigador puede ver lo que sucede en el “tubo de ensayo” desde el punto de vista humano.

Cambiemos a la pestaña Extracted files para ver qué objetos se han descargado, extraído o eliminado. En este caso, se ha eliminado un archivo malicioso.

Results System activities Extracted files Network activities				
Downloaded files ⓘ				
No data found				
Dropped files ⓘ Download data				
Zone	MD5	APT ⓘ	Detection name	File name
Malware	3E5A92EAFD63A5D09D986F89A9FD5657	—	Trojan.Win32.Pincav.bgeyx	3e5a92eafd63a5d09d986f89a9fd5657.exe
Malware	84C212A2E281C8F2EC7783751FC65265	—	—	3086.exe
Malware	DE721AE292DD1EB94F1DA2A2538AAAB2	—	HEUR:Trojan.Win32.Generic	9939.exe

Las funciones clásicas dejarían de funcionar en este punto: puede abrir el archivo y obtener la lista de actividades maliciosas, y listo. Pero con Kaspersky Threat Intelligence Portal, desde la pestaña Threat Lookup puede comprobar la inteligencia detallada sobre los indicadores de compromiso y sus relaciones.

Threat Lookup es nuestro motor de seguridad. Contiene 5 petabytes de inteligencia de amenazas recopilados y clasificados por Kaspersky Lab durante los últimos 20 años: hashes de archivo, datos estadísticos/de comportamiento, datos WHOIS/DNS, etc.

Así, tras ejecutar nuestra muestra en el entorno aislado, usamos los resultados al instante como consultas de búsqueda en Threat Lookup con solo hacer clic en el objeto (en este caso, un hash MD5).

Kaspersky
Threat Intelligence Portal

[Home](#)
[Reporting](#)
[Threat Lookup](#)
[WHOIS Tracking](#)
[Cloud Sandbox](#)
[Data Feeds](#)
[Licensing](#)

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

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

Ahora contamos con un informe más detallado sobre el malware. Veamos los resultados de Threat Lookup para comprobar cuáles son las URL a las que accedió el malware que estamos explorando:

File accessed following URLs		
Status	URL	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000	

Aquí tenemos una URL marcada como "Peligrosa". Ahora, examinémosla para comprobar lo que Threat Lookup tiene sobre ella:

The screenshot shows the Kaspersky Threat Intelligence Portal interface. At the top, there's a navigation bar with links like Home, Reporting, Threat Lookup, WHOIS Tracking, Cloud Sandbox, Data Feeds, and Licensing. Below this is a search bar with the placeholder text "Hash, IP address, domain, or URL" and a "Look up" button. The main content area displays a "Report for Domain: Dangerous" for the domain "unspoiltportugal.co.uk". The report includes statistics: IPv4 count (1), Files count (—), URLs count (≈ 10 000), and Hits count (≈ 10 000). It also shows registration details: Registration organization (None), Registrar name (None), and a category "APT Related" with a link to "Gatak - Stealthy Actor Harvest".

¡Resulta que la URL maliciosa en cuestión pertenece a un ataque APT! Kaspersky Threat Intelligence Portal ofrece la descarga de un informe APT. Este PDF incluye un documento de síntesis, detalles técnicos exhaustivos y una lista de indicadores de compromiso relacionados que vale la pena verificar para ver si a su organización le ha sucedido algo similar y para desarrollar con tiempo casos de uso específicos para detectar los ataques descritos.

The screenshot shows a PDF report from Kaspersky Threat Intelligence Portal. The report is titled "Gatak - Stealthy Actor Harvesting Data" and has a Report ID of 20171202 and Version 1.0 (8.December.2017). The report is categorized as "TLP: AMBER". The executive summary describes Gatak (also known as Stegoloader and GOLD) as an elusive threat actor which engages in data theft through opportunistic watering hole attacks. The report also includes a section titled "Appendix I - Indicators of compromise" which lists Stage 0 hashes and Domains and IPs.

Stage 0 hashes

0AE26BA127904EC354F228B316F044A1
0B20B941D2B9372D875410FFEB53C473
166200558C505A8540B33B5200D54724
5f671ec819a7cdf6d9300f03abd83223

Domains and IPs

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

Con Kaspersky Threat Intelligence Portal podrá:

- Mejorar y acelerar su capacidad de análisis y respuesta a incidentes gracias a la información significativa que reciben los equipos de seguridad/SOC sobre las amenazas y los ataques dirigidos. Realice diagnósticos y analice incidentes de seguridad en hosts y en la red de una forma más eficiente y eficaz y dé prioridad a los indicios de los sistemas internos contra las amenazas desconocidas, minimizando el tiempo de respuesta a incidentes e interrumpiendo el kill chain antes de que los datos y los sistemas críticos acaben comprometidos.
- Investigar en profundidad los indicadores de amenazas como direcciones IP, URL, dominios o archivos hash, con un contexto de amenazas altamente validado que le permite dar prioridad a los ataques, mejorar la selección de personal y recursos y centrarse en mitigar las amenazas que suponen más riesgos para su negocio.
- Mitigar los ataques dirigidos. Mejore la seguridad de su infraestructura con una inteligencia de amenazas táctica que pone a su disposición una serie de estrategias defensivas para contrarrestar las amenazas específicas a las que se enfrenta su organización.

Kaspersky Lab
Ciberseguridad empresarial: www.kaspersky.com/enterprise
Noticias sobre ciberamenazas: www.securelist.lat
Noticias sobre seguridad de TI: business.kaspersky.com/

#truecybersecurity
#HuMachine

latam.kaspersky.com

© 2019 AO Kaspersky Lab. Todos los derechos reservados. Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

