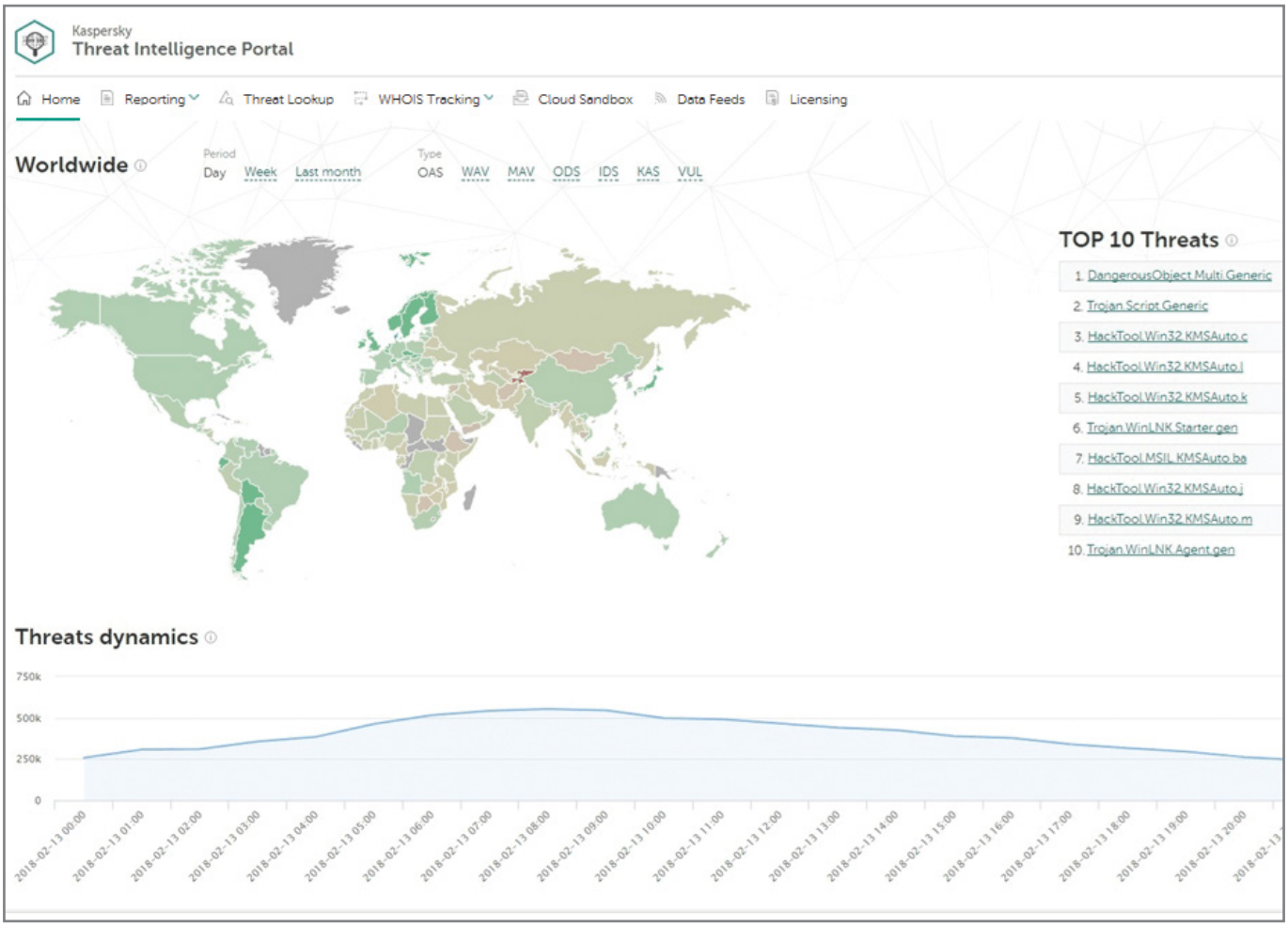
KASPERSKY lab

The Kaspersky Threat Intelligence Portal: Investigación y respuesta a incidentes

latam.kaspersky.com/fraudprevention
#truecybersecurity

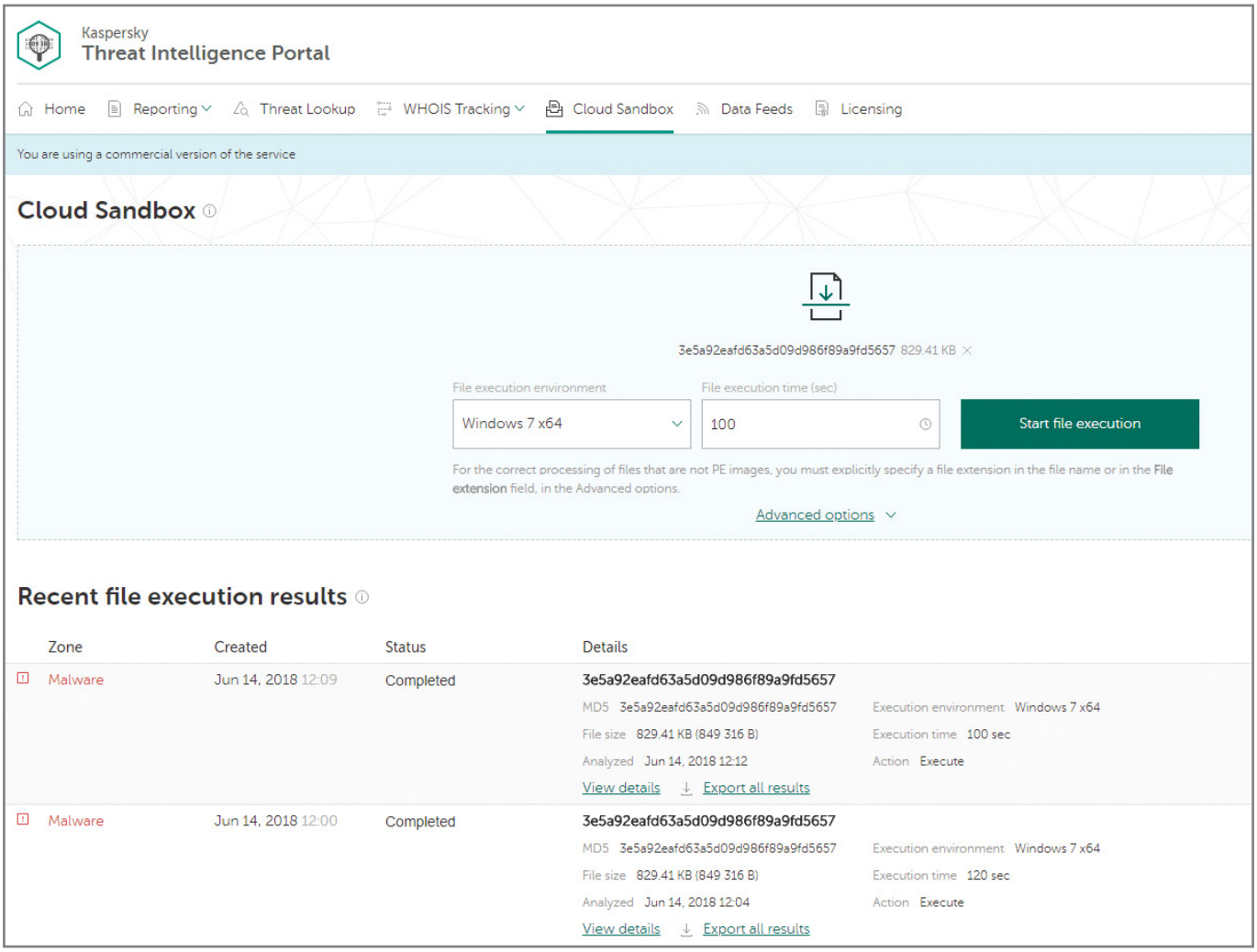
Kaspersky Threar Intelligence Portal ofrece todos los conocimientos que Kaspersky Lab ha recopilado, perfeccionado y clasificado durante más de los 20 años de historia de la compañía. La plataforma recoge las últimas novedades de la inteligencia de amenazas sobre archivos, URL, dominios, direcciones 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.

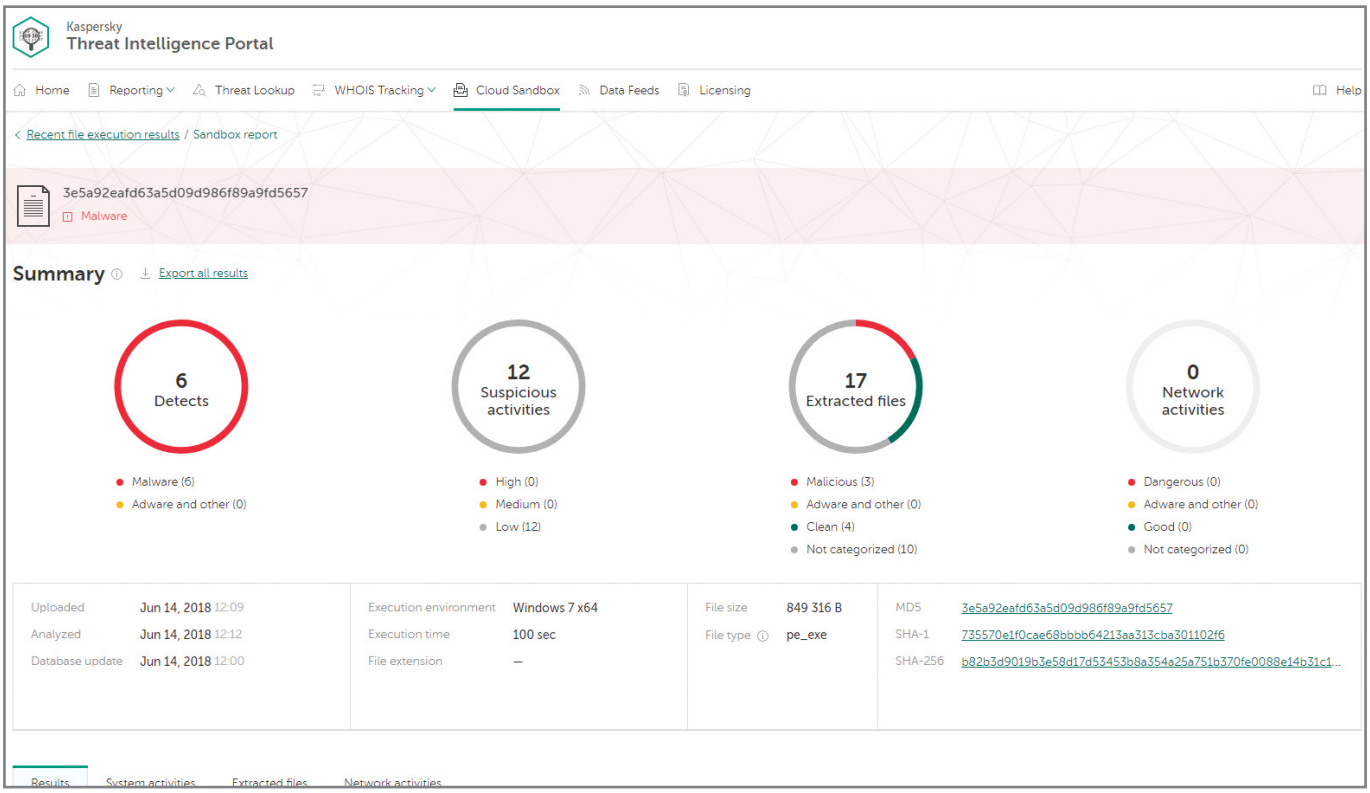


La página principal de Kaspersky Threat Intelligence Portal tiene muchas pestañas. Por ejemplo, si el equipo de respuesta a incidentes obtiene la muestra de un archivo sospechoso que ha iniciado comunicación desde dentro del perímetro de la red con una dirección IP externa, fuera del horario laboral,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

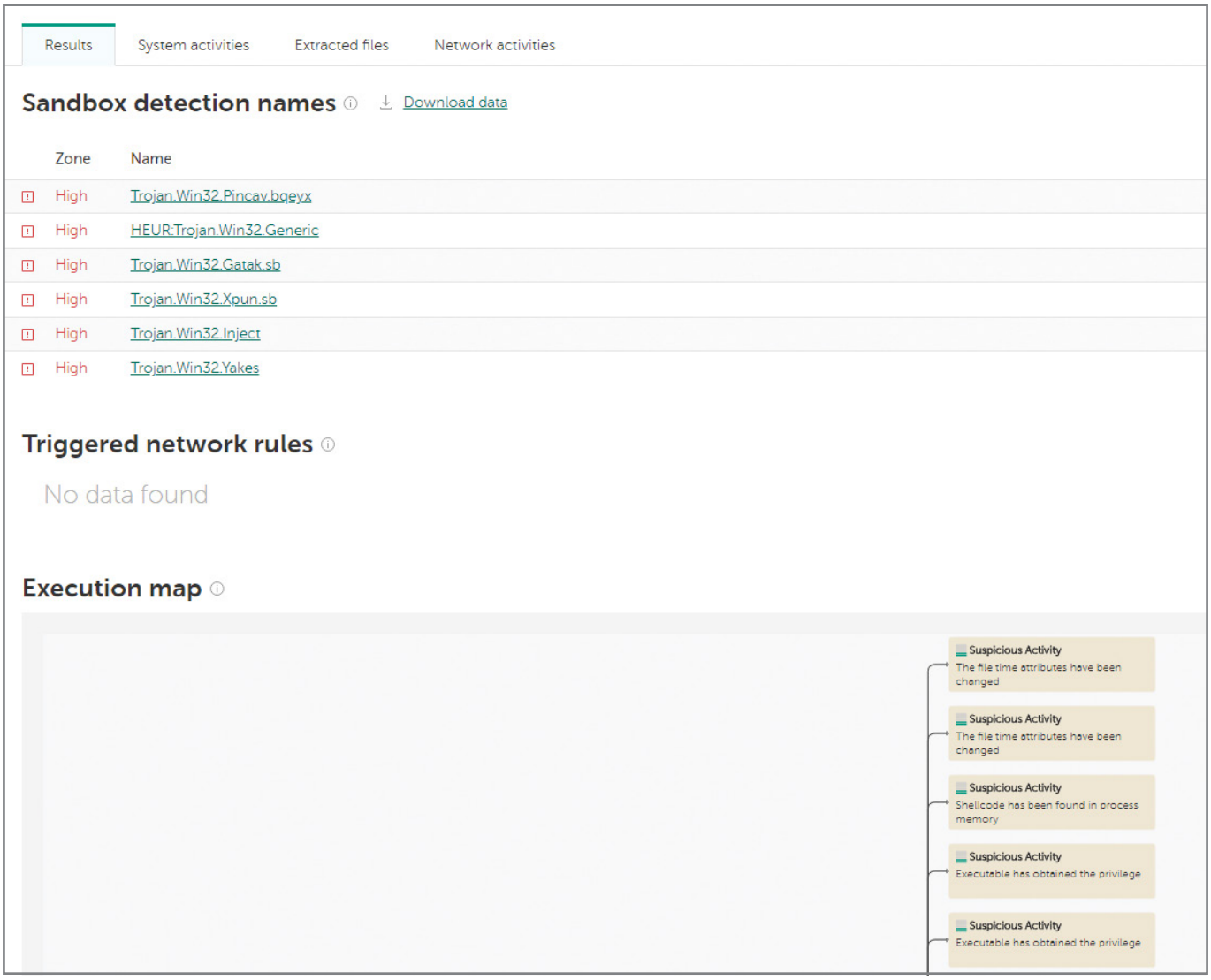
La función de aislamiento de procesos ejecuta un objeto sospechoso, detectado tras analizar su actividad, en una máquina virtual (VM por sus siglas en inglés) con un sistema operativo completo. Las VM están aisladas de la infraestructura empresarial real, por lo que la detonación no causará daños reales.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

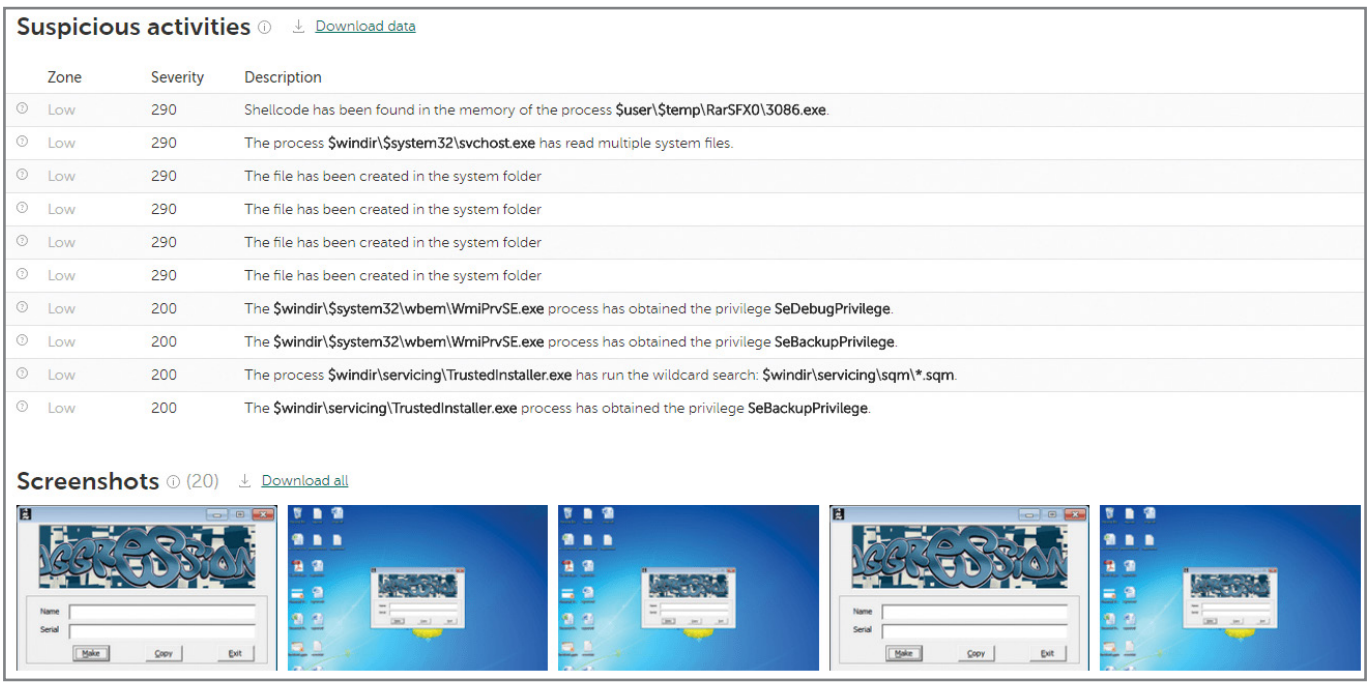


Los entornos aislados son efectivos contra el malware que evade el análisis de estadística y que, por tanto, se le podría escapar a su antivirus. Incluso si un archivo se identifica como "perjudicial", la mayoría de los sistemas antivirus no podrán explicar su nivel de peligrosidad ni la situación. Para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



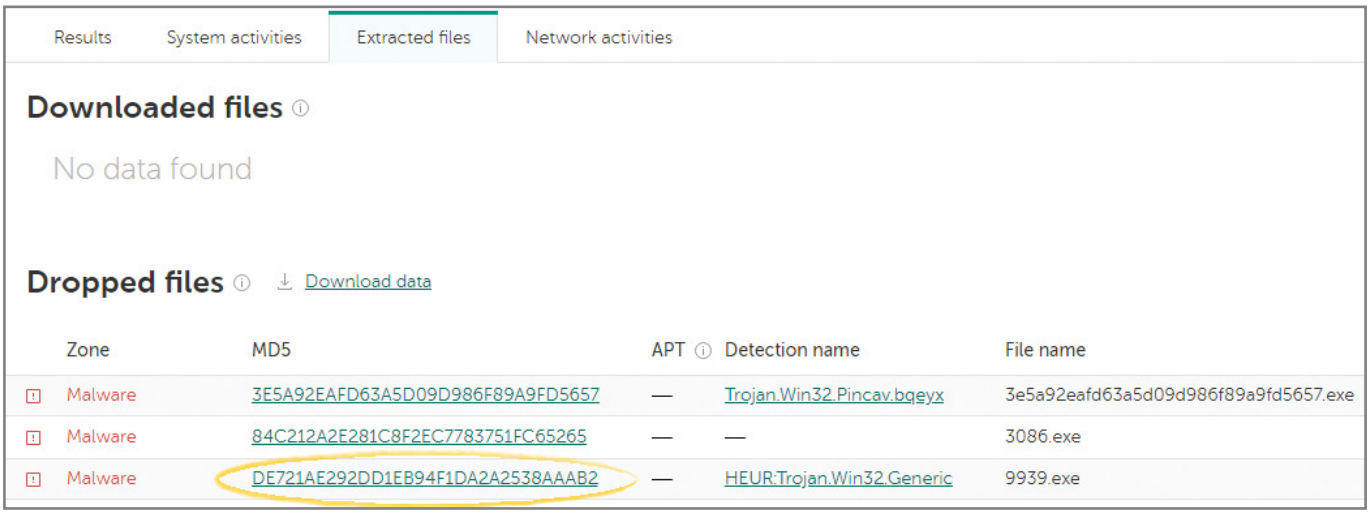
Tras ejecutar el objeto a analizar, un entorno aislado recopila los objetos, los analiza y emite un dictamen. Este es el resumen: detecciones (6), actividades sospechosas (12), archivos extraídos (17) y actividades de red (0). No se trata solo de un archivo "perjudicial", sino que puede llevar a cabo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





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.

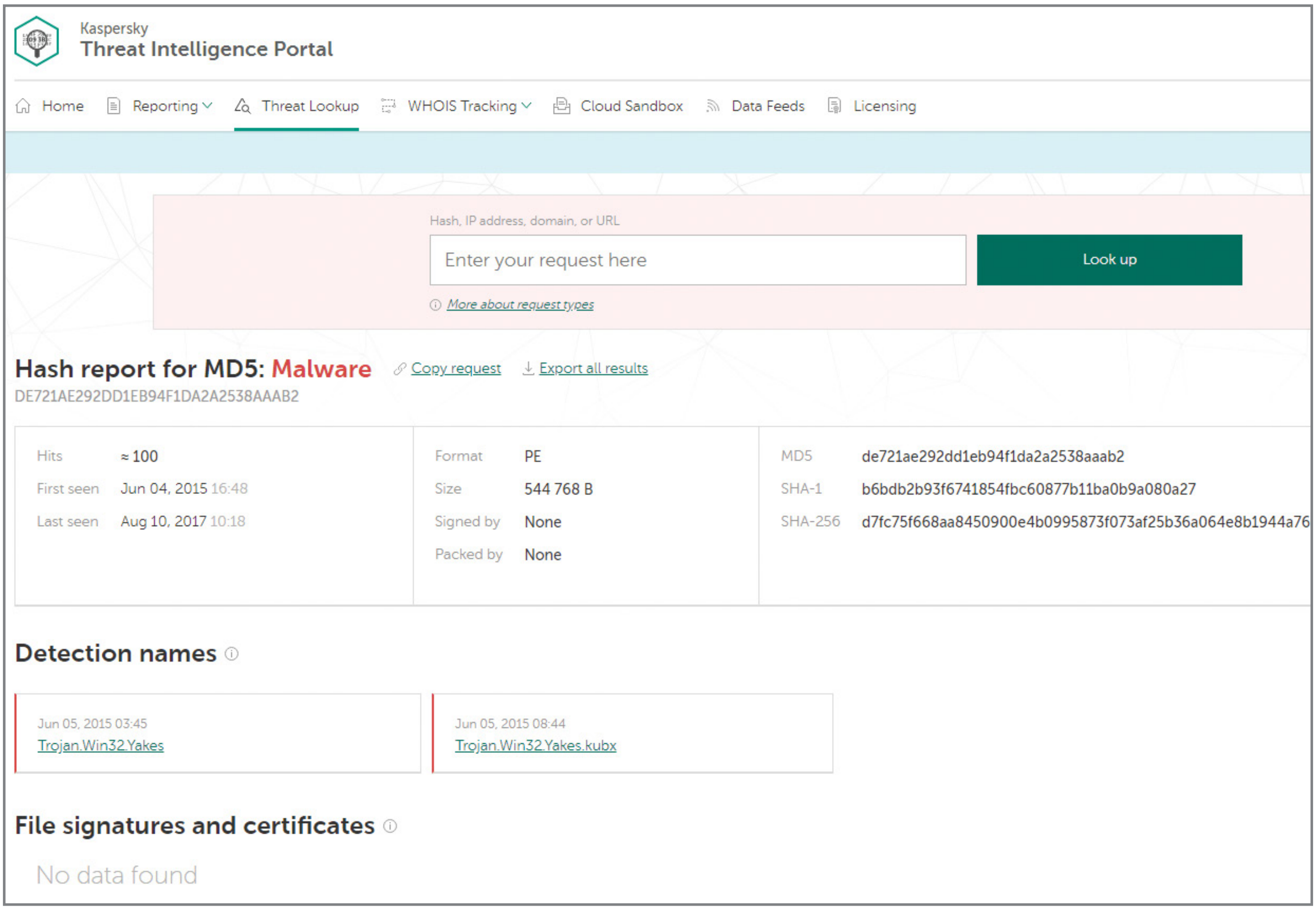
Cambiemos a la pestaña Extracted files para ver qué objetos se han descargado, extraído o eliminado. En este caso, se ha eliminado un archivo malicioso.



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).



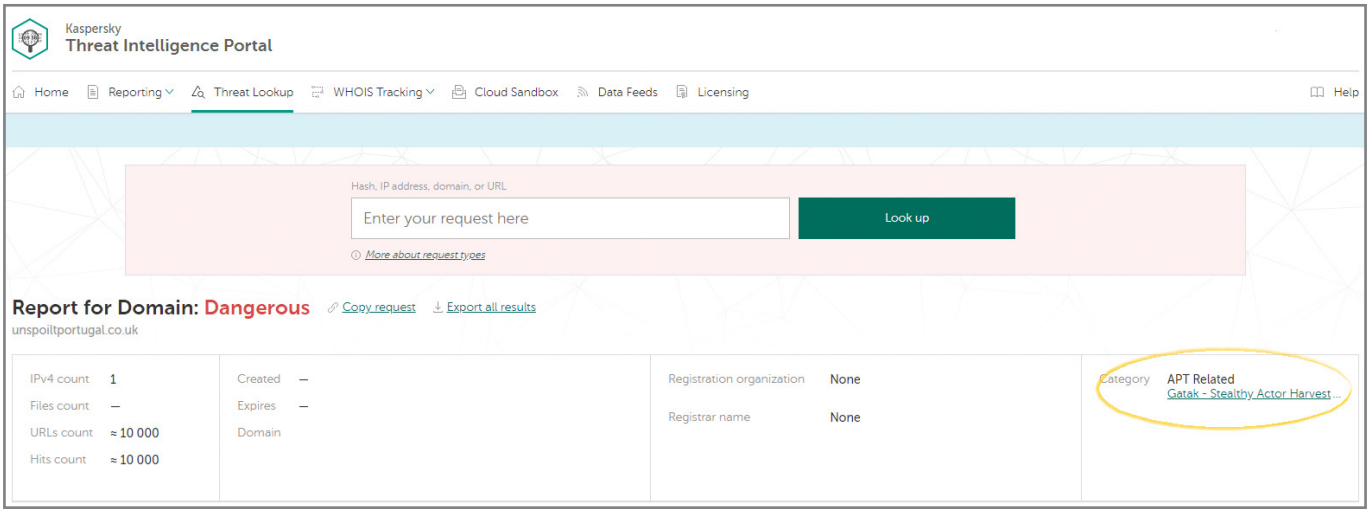
Ahora contamos con un informe más detallado sobre el malware. Veamos los resultados de Threat Lookup para comprobar cuáles son las URL a las que accedió el malware que estamos explorando:

File accessed following URLs

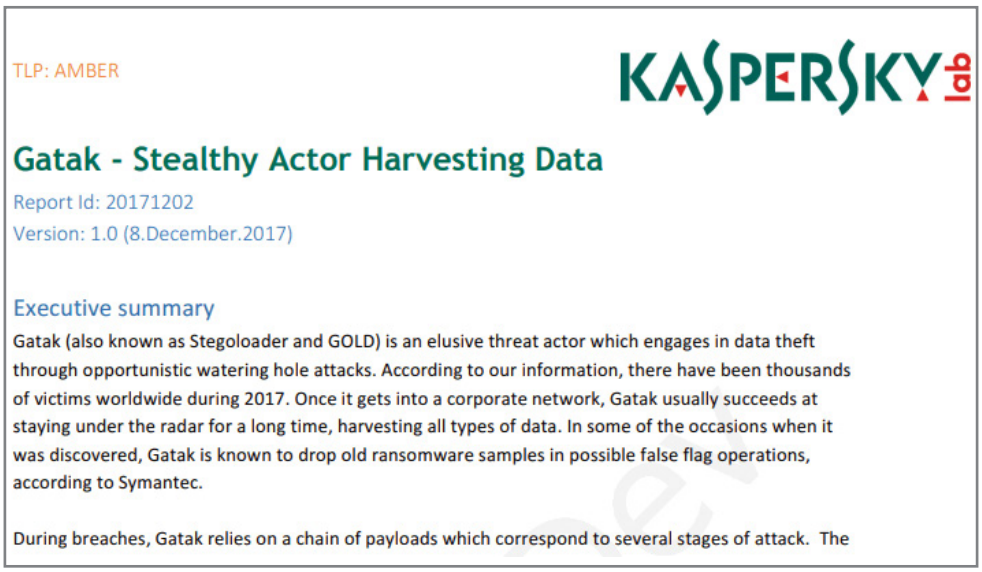
Download data

Status	URL
Dangerous	unspoiltportugal.co.uk/report_N_0027_
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoiltportugal.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:



¡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.


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

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