SERVICIOS DE INTELIGENCIA: SEGUIMIENTO DE LAS AMENAZAS DE BOTNET

Servicios expertos de control y notificación para identificar los botnets que son una amenaza para sus clientes y su reputación.

Muchos ciberataques se realizan con botnets. Aunque este tipo de ataques pueden ir dirigidos a los usuarios normales de Internet, suelen estar destinados a los clientes de empresas específicas y sus clientes online.

La solución experta de Kaspersky Lab controla la actividad de los botnets y proporciona notificaciones rápidas (en el plazo de 20 minutos) sobre las amenazas relacionadas con los usuarios de sistemas bancarios y de pago online individuales. Esta información puede utilizarse para advertir e informar a los clientes, los proveedores de servicios de seguridad y las fuerzas del orden locales sobre las amenazas actuales. Ya puede proteger la reputación de su organización y de sus clientes con el servicio de notificación de amenazas de botnets Botnet Threats Notification Service de Kaspersky Lab.

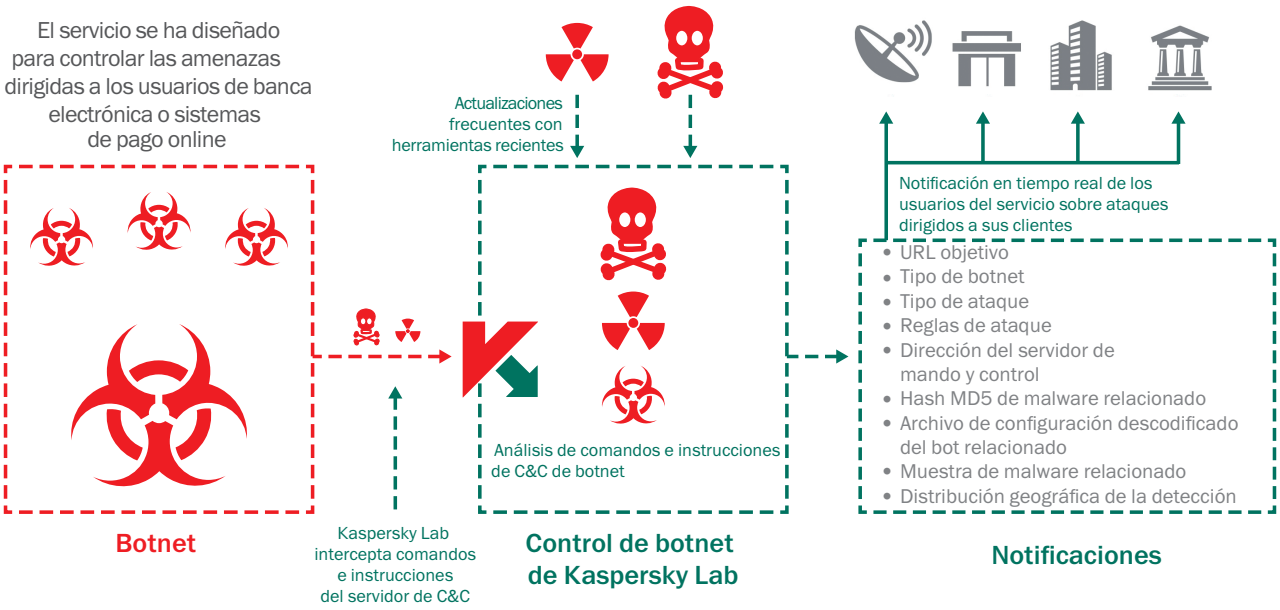
CASOS DE USO/VENTAJAS DEL SERVICIO

- **La alertas proactivas** acerca de las amenazas procedentes de botnets destinados a sus usuarios online le permiten mantenerse siempre un paso por delante del ataque
- **La identificación de una lista de URL de servidores de mando y control (C&C)** destinadas a sus usuarios online permite bloquearlas mediante el envío de solicitudes a los CERT o a la ciberpolicía.
- **Mejora de su operaciones bancarias online/ cajones de pago** gracias a la comprensión de la naturaleza del ataque.
- **Formación de los usuarios online** para reconocer y evitar que les engañen con la ingeniería social utilizada en los ataques.

ACTÚE EN TIEMPO REAL:

El servicio incluye una suscripción de notificaciones personalizadas que contienen información de inteligencia sobre las marcas afectadas obtenida mediante el seguimiento de las palabras clave de los botnets que vigila Kaspersky Lab. Las notificaciones se pueden enviar por correo electrónico o RSS en formato HTML o JSON. Las notificaciones incluyen lo siguiente:

- **URL objetivo:** el malware de bots está diseñado para esperar hasta que el usuario acceda a las URL de la organización objetivo y, en ese momento, ejecuta el ataque.
- **Tipo de botnet**: comprenda exactamente la amenaza de malware que el cibercriminal utiliza para poner en peligro las transacciones de sus clientes. Algunos ejemplos son Zeus, SpyEye y Citadel.
- **Tipo de ataque**: identifique con qué finalidad se utiliza el malware. Por ejemplo, para insertar datos web, borrar el contenido de la pantalla, hacer capturas de vídeo o reenviar al usuario a URL de phishing.
- **Reglas de ataque:** conozca las reglas de inserción de códigos web que se utilizan, como por ejemplo solicitudes HTML (OBTENCIÓN/PUBLICACIÓN) o los datos de la página web antes y después de la inserción.
- **Dirección del servidor de mando y control (C&C)**: permite notificar el proveedor de servicios de Internet del servidor atacante para agilizar el desbaratamiento de la amenaza.
- **Hash MD5 de malware relacionado**: Kaspersky proporciona la suma de verificación, que se utiliza para comprobar el malware.
- **Archivo de configuración descodificado del bot relacionado:** para identificar todas las URL objetivo.
- **Muestra de malware relacionada:** para el análisis inverso y de ciencia forense digital del ataque del botnet.
- **Distribución geográfica de la detección (10 países principales):** con datos estadísticos de las muestras de malware relacionadas de todo el mundo.



La solución de Kaspersky Lab está disponible en las versiones Standard o Premium, y ofrece una gran variedad de condiciones de servicio y URL supervisadas. Consulte con Kaspersky Lab o con su partner distribuidor para determinar qué paquete es el adecuado para su empresa.

NIVELES DE SUSCRIPCIÓN Y ENTREGAS

Premium

Notificación por correo electrónico o formato JSON — 10 URL supervisadas

- Archivo de configuración descodificado del bot relacionado
- Muestra de malware relacionada (a petición)
- Distribución geográfica de las detecciones de muestras de malware relacionadas

Standard

Notificación en formato de correo electrónico — 5 URL supervisadas

- URL de destino (identificación de las URL desde las que los programas bot se destinan a los usuarios)
- Tipo de botnet (por ejemplo, Zeus, SpyEye, Citadel, Kins, etc.)
- Tipo de ataque
- Reglas de ataque, incluidas las siguientes: insertar datos web; URL, pantalla, captura de vídeo, etc.
- Dirección de mando y control
- Hash MD5 de malware relacionado

¿POR QUÉ KASPERSKY LAB?

- Fundada y dirigida por el experto en seguridad más prominente del mundo, Eugene Kaspersky
- Relaciones de colaboración con organismos encargados de hacer cumplir las leyes, como Interpol y CERTS
- Herramientas en la nube que supervisan millones de ciberamenazas en todo el mundo en tiempo real
- Equipos globales que analizan y comprenden todos los tipos de amenazas de Internet
- La mayor empresa de software de seguridad independiente del mundo centrada en la inteligencia sobre amenazas y el liderazgo en tecnología
- Líder indiscutible en más pruebas independientes de detección de malware que cualquier otro proveedor
- Identificado como líder por Gartner, Forrester e IDC

Para obtener más información sobre Kaspersky Intelligence Services, póngase en contacto con nosotros a través de intelligence@kaspersky.com.
PARA OBTENER MÁS INFORMACIÓN, VISITE www.kaspersky.es.

KASPERSKY lab