FRAUDWATCH
Digital Brand Protection

VIGILANCIA MEJORADA DE LA DEEP Y DARK WEB

FraudWatch ofrece ahora un servicio mejorado de supervisión de la Deep y Dark web. Proporcionamos una herramienta de inteligencia exhaustiva y profunda, que permite a su organización obtener una visión detallada de las amenazas cibernéticas pasadas, actuales y futuras que se dirigen a su organización.

Se puede acceder a los datos resultantes a través de un panel de control activo, con la capacidad de ver, descargar, ordenar y eliminar registros. El tablero también presentará al usuario los resultados de los datos visualizados, lo que permite una presentación rápida de los mismos.

Los actores de las amenazas utilizan varios métodos y plataformas para comunicarse y compartir información a través de la web superficial, deep y dark, para evitar ser detectados y permanecer en el anonimato. La deep webincluye todos los sitios web habituales que requieren autenticación mediante credenciales de cuenta, y contiene información que no recogen los motores de búsqueda. Hemos desarrollado herramientas propias que pueden infiltrarse en estas fuentes para proporcionar la información más relevante y actualizada diariamente.

Nuestro servicio mejorado de vigilancia de la deep y dark webes una herramienta automatizada que recopila datos de varias fuentes de interés, donde se sabe que los actores de las amenazas intercambian información y se comunican. En el actual panorama de las ciberamenazas, en constante evolución, las grandes organizaciones son regularmente objeto de ataques. Con las frecuentes violaciones de datos que se producen, es vital estar al tanto de las conversaciones entre adversarios. Nuestra plataforma realiza escaneos diarios en busca de cualquier mención relevante de una marca o individuo y notifica a nuestros clientes cualquier dato relevante que pueda haber sido filtrado, permitiéndoles mitigar inmediatamente el problema.

Ofrecemos un acceso seguro a los registros de la Deep y dark web y la posibilidad de descargar información sensible a través de canales cifrados. Podemos proporcionar a usuarios seleccionados acceso a los datos de la Deep weby dark web para permitir un control más fácil sobre qué empleados pueden acceder a los resultados, para minimizar los riesgos a nivel interno.

Nuestras fuentes de alta amenaza incluyen las diversas redes anónimas descentralizadas entre pares, incluyendo los mercados y foros ToR así como I2P y ZeroNet. Nuestras otras fuentes incluyen una serie de fuentes de la deep web, como foros de hackers autentificados, fuentes de la web superficial de alto riesgo, salas de chat cifradas, grupos de Telegram, redes de Internet Relay Chat, datos de servidores FTP, Server Data, registros de fugas de datos y sitios de Paste.

LO QUE MONITORIZAMOS

Nuestra plataforma puede escanear varias menciones de marcas objetivo, propiedad intelectual, dominios e información de identificación personal (PII, por sus siglas en inglés) de ejecutivos o empleados, como direcciones de correo electrónico, credenciales de cuentas y documentos de identificación. También buscamos en las bases de datos de fugas de datos actualizadas periódicamente la PII relacionada con su organización.

MONITORIZACIÓN DE NÚMEROS DE IDENTIFICACIÓN BANCARIA

La supervisión de los números de identificación bancaria (BIN, por sus siglas en inglés) en la Deep y Dark webes un servicio adicional que ofrecemos a las instituciones financieras. Las páginas de phishing son hoy más prominentes que nunca, y eso hace que el robo de números de tarjetas de crédito e información personal de los individuos sea imposible de detener.

Los datos de las tarjetas de crédito robadas pueden comprarse en los mercados de la dark webpor tan sólo $15 USD y las credenciales de las cuentas de PayPal se venden por unos míseros $10. Algunos mercados de la dark webincluso regalan un gran número de datos de tarjetas de crédito como parte de una promoción. Por ejemplo, en octubre de 2022, un mercado de tarjetas de la dark webllamado 'Biden Cash' liberó más de 1,2 millones de tarjetas de crédito de forma gratuita para promocionar su mercado, permitiendo que cualquiera con acceso a ToR las descargara de forma gratuita y realizara fraudes financieros. Creemos que nuestra herramienta de monitorización puede aportar un valor inmenso, ya que conocer una tarjeta de crédito filtrada permite evitar que los delincuentes la utilicen.

EJEMPLO DE LA PROMOCIÓN FALSA 'BIDEN CASH'

sales@fraudwatch.com www.fraudwatch.com security@fraudwatch.com

FRAUDWATCH
Digital Brand Protection

TIPOS DE DATOS QUE MONITORIZAMOS

Palabras clave/dominios de marca:

- Marca, empresa, institución financiera
- Dominios
- Propiedad intelectual
- Indicadores de violación de datos

Seguimiento de ejecutivos/PII:

- Nombre
- Dirección de correo electrónico
- Credenciales de la cuenta
- Información de identificación personal (como números de carné de conducir o de pasaporte)
- Datos violados que contienen PII de un individuo/ejecutivo

Monitoreo de BIN/Tarjetas de Crédito:

- Supervisión de los números de identificación bancaria para identificar las tarjetas de crédito robadas

CANALES/FUENTES VIGILADAS

Web de superficie de alto riesgo Dark Web:

- ToR
- I2P
- ZeroNet

Deep Web:

- Datos del servidor FTP
- Fugas de datos
- Foros de hackers autentificados
- Plataformas de chat encriptadas
- Grupos de Telegram
- Salas de chat de retransmisión por Internet (IRC, por sus siglas en inglés)
- Grupos de Discord
- Sitios Paste

Qué incluye el servicio:

- Opción de búsqueda histórica con posibilidad de retroceder hasta 8 años
- Acceso a miles de millones de registros
- Nuevos escaneos diarios automatizados en busca de información relevante en nuestro amplio conjunto de datos
- Notificaciones de nuevos resultados
- Acceso a los registros a través de un panel de control activo con datos visualizados
- Posibilidad de acceder, descargar, ver, ordenar y eliminar registros de forma segura

Qué datos se descubren:

- Credenciales de acceso comprometidas de los usuarios internos (ejecutivos/empleados)
- Información personal comprometida de usuarios internos (ejecutivos/empleados)
- Credenciales de inicio de sesión comprometidas de los clientes
- Información comprometida de tarjetas de crédito de clientes
- Extractos bancarios legítimos o falsificados
- Credenciales de inicio de sesión de aplicaciones de pago
- Menciones de un BIN en una campaña dirigida
- Indicadores de compromiso (como registros de datos)
- Indicadores de compromiso a través de dominios
- Información sobre un ataque próximo o en curso
- Datos filtrados de empleados o clientes de una brecha
- Credenciales de criptocarteras comprometidas
- Cuentas bancarias comprometidas
- Cuentas bancarias utilizadas para el blanqueo de dinero
- Propiedad intelectual
- Métodos utilizados por los delincuentes para eludir las medidas de seguridad
- Métodos utilizados por los delincuentes para cometer fraudes
- Acceso a activos/artefactos digitales (como kit de phishing, tutoriales, archivos de configuración)

GLOBAL SERVICE COVERAGE

Asia Pacific Head Office
+61 3 9887 6777

EMEA
+44 20 3974 1444

North America
+1 415 449 8800

sales@fraudwatch.com

www.fraudwatch.com

security@fraudwatch.com