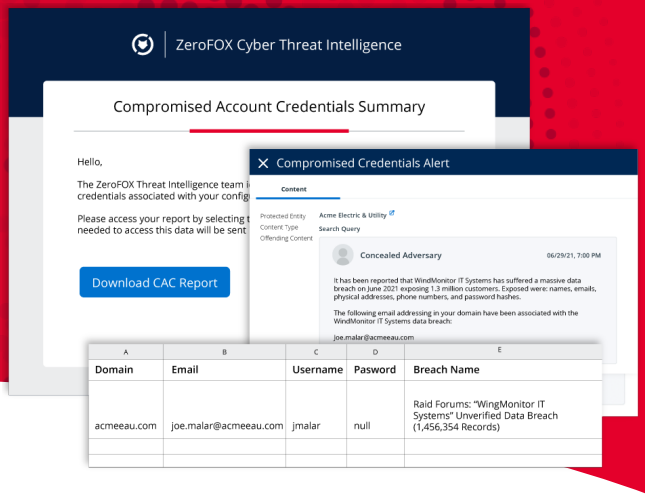
ZEROFOX

FICHA TÉCNICA

Protección e inteligencia de la web oscura

Encuentre en la web oscura indicios de violaciones de seguridad y elimine el riesgo asociado a las operaciones clandestinas



Reto

La web oscura: un mundo secreto para ellos, un riesgo para usted

Para mantener a los internautas "normales" lejos de la web oscura se crean identidades falsas, avatares, grupos cerrados y sitios secretos. Los que quieren pasarse al lado oscuro necesitan herramientas, experiencia y haberse labrado una reputación. ¿El motivo? Los ciberdelincuentes comercian con NUESTROS datos.

En estos sitios clandestinos, los ciberdelincuentes venden y compran datos de tarjetas de crédito, información de identificación personal, propiedad intelectual y credenciales comprometidas, NUESTRA información. También intercambian TTP, kits de exploits y planes de ataque. ¿Está USTED entre sus objetivos?

Solución

Agentes expertos en la web oscura para gestionar su riesgo

Nuestro equipo global de búsqueda de amenazas e inteligencia de la web oscura contacta directamente con la comunidad clandestina. Combinamos código abierto e inteligencia humana para identificar los riesgos, clasificar las amenazas y resolver los problemas mediante operaciones específicas. Nuestros agentes hablan más de 30 idiomas, como ruso, ucraniano, coreano, mandarín, cantonés y, naturalmente, inglés. Nos infiltramos en cientos de comunidades y sitios de la web oscura para localizar SU información y resolver sus problemas rápidamente y con total confidencialidad.

INVESTIGACIONES DE LA WEB OSCURA BAJO DEMANDA

Evalúe su nivel de exposición

- Nuestros analistas trabajarán con agentes de la web oscura para identificar credenciales, datos de identificación personal, propiedad intelectual, y cuentas de redes sociales y de Active Directory suyas que estén a la venta en la web oscura. Identificaremos a los ciberdelincuentes y las conversaciones, tácticas, procedimientos o estrategias de coordinación destinados a atacar su organización. Nos encargaremos de responder a cualquier solicitud de información concreta que se plantee.

MONITOREO DE LA WEB OSCURA

Monitoreo de la inteligencia en tiempo real

- Constantemente surge nueva información para vender o comprar en la web oscura. Cada revelación de datos, ataque de phishing y suplantación de identidad proporciona datos nuevos.
- La plataforma de ZeroFox monitorea continuamente los nuevos conjuntos de datos para detectar información nueva en la web oscura. Proporcionamos una amplia cobertura para canales digitales no indexados, supervisamos el compromiso de credenciales y otra información sensible, detectamos las filtraciones de datos confidenciales y arrojamos luz sobre planificaciones y conversaciones acerca de ataques.

DARK OPS

Contacto directo

- Para recuperar los recursos, negociar los precios y adquirir material específico afectado por un ataque, hay que contactar con las personas adecuadas. De nuevo, ahí está ZeroFox para ayudarle. Nuestros agentes están integrados en la comunidad clandestina, así que sabemos cómo llegar a estas personas.
- Nosotros nos encargamos de todo con discreción, desde la transferencia de fondos a los monederos de criptomoneda hasta las transacciones en la web oscura, o el contacto con los ciberdelincuentes para obtener información o pagar un rescate.

Descripción detallada de los servicios de la web oscura y Dark Ops

Suscripciones anuales "Flex RFI" de Dark Ops Acceso a los agentes y las investigaciones de Dark Ops en cualquier momento	
Búsqueda de amenazas de Dark Ops	Contrato anual renovable para el servicio de búsqueda de amenazas especial para las amenazas y alertas del cliente, basado en la actividad en la web profunda y oscura, los vectores de amenaza y los riesgos específicos para el cliente.
Investigación y contactos de Dark Ops	Contrato anual renovable para solicitudes de información dirigidas, investigaciones personalizadas e investigaciones a medida.

Investigaciones bajo demanda de Dark Ops Creación de informes relevantes sobre descubrimientos de sistemas, así como búsquedas anticipadas de información específica de la red operativa	
Investigación o solicitud de información de incidentes en la web oscura	ZeroFox presta servicios de analistas expertos en la investigación de eventos e incidentes en la web oscura. Estos servicios incluyen la correlación de alertas, la contextualización, y la identificación y elaboración de perfiles de los ciberdelincuentes, si procede. También plantea opciones para tomar posibles medidas.
Investigación de información confidencial en la web oscura (DWSI)	Información confidencial que incluya propiedad intelectual valiosa, datos de identificación personal u otra información, recursos corporativos o datos de clientes que estén sujetos al cumplimiento de normativas.
Investigación para búsqueda de amenazas en la web oscura (DWTH)	Credenciales comprometidas, registros de bots activos, cuentas de Active Directory, ampliación de recursos, conversaciones sobre superficie de ataque y coordinación, perfiles de delincuentes y atribución.
Informe de investigaciones de información confidencial y búsqueda de amenazas en la web oscura	Combina investigaciones de información confidencial y de búsqueda de amenazas para determinar el riesgo de la amenaza, la dimensión de la exposición, la atribución del ciberdelincuente, la actividad en el mercado, etc.
Investigación personalizada en la web oscura	Las investigaciones personalizadas se adaptan a las solicitudes de información especiales de cada cliente.
Agilización de informes	Un analista experto en TI que trabaja de 9:00 a 17:00 suele tardar entre dos y tres semanas en elaborar un informe de investigación. Por un precio adicional, este plazo puede reducirse a siete días.

Contacto directo con Dark Ops Búsqueda y comunicación directa con ciberdelincuentes concretos para interrogarles sobre adquisición de información, pagos de ransomware u otras tareas.	
Solo investigación de recursos digitales	ZeroFox identificará y contactará directamente con el ciberdelincuente para concretar el importe y las condiciones.
Investigación, transacción y recuperación de recursos digitales	ZeroFox identificará y contactará directamente con el ciberdelincuente para concretar el importe y las condiciones. El cliente puede determinar la oferta inicial, la contraoferta y el máximo, o aceptar las recomendaciones del equipo de Dark Ops de ZeroFox. El cliente también depositará la cantidad máxima, cuya divisa se convertirá a criptomoneda según el valor del mercado. Se puede contratar solo la investigación, pero no es recomendable.

Contacto directo con Dark Ops (continuación)	
Creación de monederos de criptomonedas	Creación de un monedero en la criptomoneda que desee: Bitcoin, Ethereum, XRP, Tether o Cardano. También se facturará el traspaso de fondos. Incluye formación sobre las operaciones que se pueden realizar con el monedero, incluidas las medidas de seguridad. ZeroFox no ofrece protección de monederos tras el traspaso al cliente. Este servicio no incluye el costo del traspaso de fondos al monedero, que se facturará al costo real más el 5 %.
Negociación del ransomware	ZeroFox identificará y contactará directamente con el ciberdelincuente para concretar el importe y las condiciones. El precio incluye la comunicación con la compañía de ciberseguros del cliente (si procede), dentro de unos límites razonables. NO se incluye la comunicación con las fuerzas de seguridad, pero sí la elaboración de informes de incidentes relacionados con la transacción en su caso.
Pago de ransomware	ZeroFox identificará y contactará directamente con el ciberdelincuente para concretar y negociar el importe y las condiciones. El precio incluye la comunicación con la compañía de ciberseguros del cliente (si procede), dentro de unos límites razonables. NO se incluye la comunicación con las fuerzas de seguridad, pero sí la elaboración de informes de incidentes relacionados con la transacción en su caso.
Plan secreto	Si se permite y en función de cada caso, ZeroFox se coordinará con las fuerzas de seguridad en cada país para detener a los ciberdelincuentes más destacados, incluidos los que comentan delitos especialmente atroces. Se requiere la aprobación directa de los procedimientos por parte del equipo de Dark Ops de ZeroFox para proteger la identidad de los agentes.
Contacto directo especial con Dark Ops	Las investigaciones personalizadas se adaptan a los requisitos especiales de cada cliente. Pueden incluir el contacto con ciberdelicuentes o servicios especificados por el cliente, ejercicios de simulación, etc.
Tasa de agilización del contacto directo de Dark Ops	Los contactos de Dark Ops suelen llevar entre cinco y siete días desde el inicio. Si se agilizan, este periodo puede reducirse a uno o dos días.

¿LE GUSTARÍA COMPROBARLO USTED MISMO?

Solicite una demostración
Regístrese en ZeroFox.com/request-a-demo/

Más información
Visite ZeroFox.com
Contacte con nosotros: sales@ZeroFox.com / +1 855 736 1400

ACERCA DE ZEROFOX

ZeroFox proporciona a las empresas protección e inteligencia de amenazas externa para frustrar las amenazas contra marcas, personas, recursos y datos en toda la superficie de ataque pública, mediante una sola plataforma integral. Con cobertura completa de la web de superficie, la web profunda y la web oscura, y con un motor de análisis basado en inteligencia artificial y tecnología de Intel, la plataforma de ZeroFox identifica e impide los ataques de phishing dirigidos, el robo de credenciales, la filtración de datos, el secuestro de marcas, las amenazas a directivos y ubicaciones, etc. La tecnología patentada de la plataforma de ZeroFox procesa y protege diariamente millones de publicaciones, mensajes y cuentas en todo el ámbito digital y social, que abarca las fuentes clandestinas de la web de superficie, la web profunda y la web oscura, las redes sociales, las tiendas de aplicaciones móviles, los dominios, el correo electrónico en la nube, etc.

ZEROFOX