DATASHEET

FORXITE

LEAKS & EXPOSURE HUB

Detección y notificación temprana de filtraciones y exposición de datos en ecosistemas digitales

El Desafío

Las filtraciones de datos y exposiciones de información sensible se originan en múltiples entornos digitales donde actores maliciosos publican, validan y distribuyen información comprometida.

Foros especializados, sitios de ransomware y canales de mensajería se han convertido en puntos clave donde estas exposiciones se hacen visibles antes de impactar directamente en las organizaciones. Sin visibilidad sobre estos espacios, los equipos de seguridad dependen de eventos internos o reportes externos tardíos, perdiendo capacidad de reacción temprana.

Esto permite no solo detectar exposición propia, sino también identificar eventos relevantes a nivel sectorial y regional, aportando visibilidad operativa para equipos SOC y CSIRT.

Monitoreo del ecosistema criminal

Forxite realiza monitoreo continuo sobre fuentes relevantes donde se originan y difunden filtraciones:

- Foros de filtración de datos
- Sitios de publicación de ransomware
- Canales públicos y cerrados en plataformas de mensajería
- Espacios de intercambio de accesos y credenciales

Cada hallazgo es validado y estructurado antes de su notificación, permitiendo reducir ruido.

Nuestra cobertura

Foros y comunidades

Monitoreo de espacios donde se publican y distribuyen bases de datos, accesos y credenciales.

Canales de mensajería

Monitoreo de Telegram y otros entornos donde se comparten datos comprometidos o accesos iniciales.

Sitios de ransomware

Seguimiento de publicaciones de grupos de ransomware y detección de organizaciones listadas como víctimas.

Exposición de credenciales y accesos

Identificación de publicaciones relacionadas con usuarios, contraseñas, claves API y accesos comprometidos.

MODELO DE INVESTIGACIÓN

Este servicio se enfoca en la detección, validación y notificación estructurada de eventos de exposición. En caso de requerir:

- Análisis en profundidad
- Perfilado de actores
- Correlación con otras amenazas
- Investigación ampliada sobre el incidente

Las organizaciones pueden activar investigaciones especializadas mediante el servicio CFI Request, utilizando el modelo de créditos. Esto permite escalar desde la detección temprana hacia inteligencia profunda de forma controlada y trazable.

ENTREGABLES

- Alertas estructuradas en tiempo cercano a la detección
- Evidencia asociada (capturas, samples cuando aplica)
- Consolidación de eventos relevantes
- Soporte básico para interpretación del hallazgo

IMPACTO OPERATIVO

Detección temprana de filtraciones y publicaciones relevantes
Reducción del tiempo de exposición ante eventos de leak
Visibilidad sobre menciones en sitios de ransomware
Acceso a evidencia para análisis interno
Contexto operativo para equipos SOC y CSIRT sobre eventos relevantes por sector y país

CASOS DE USO

- Identificación de publicaciones que involucren a la organización
- Detección de inclusión en sitios de ransomware
- Monitoreo de filtraciones en la industria o país
- Obtención de evidencia para análisis interno
- Activación de investigaciones ante eventos críticos

Acerca de FORXITE

Forxite es una compañía especializada en inteligencia aplicada a riesgos digitales, ciberamenazas y ciberfraudes. Combinamos analistas especializados con el desarrollo de una plataforma tecnológica propia, orientada a estructurar, escalar y dar trazabilidad a las capacidades de inteligencia.

Póngase en contacto con nosotros: info@for7ress.com