

# **Investigaciones Globales**

## **Tecnología de punta en la lucha contra los cibercriminales**

- Profundo conocimiento de los esquemas cibercriminales.
- Colaboración con los organismos encargados de hacer cumplir la ley.
- Tecnologías propias para la detección de cibercriminales.
- Enfoque individual por parte del equipo de proyectos especiales.



# Índice del Brochure

Investigaciones criminales de alta tecnología

1



# Investigaciones Cibercriminales de Alta Complejidad



## Combatir los delitos informáticos, financieros y corporativos de diverso tamaño y complejidad

El objetivo principal de nuestra investigación es llevar a los autores ante la justicia. Si es necesario, seguiremos participando en el caso hasta que se ejecute la sentencia, consultando a los abogados y prestando testimonio en el tribunal.

Perfil detallado del actor de la amenaza. Exploramos la anatomía del ataque y la infraestructura del actor de la amenaza, identificamos los mecanismos y recreamos la secuencia de eventos.

Las investigaciones de crímenes de alta tecnología son el área más antigua de nuestra actividad. Llevamos a cabo una amplia variedad de investigaciones, incluyendo:

### Robo de Datos

Espionaje competitivo, phishing, violación de la propiedad intelectual, robo de secretos comerciales, credenciales y otra información sensible.

### Crímenes Financieros

Robo de criptomonedas, banca en línea, banca móvil, fraude por correo electrónico, cajeros automáticos, procesamiento de tarjetas, SWIFT, pasarelas de pago.

### Ataques Internos

Abuso de autoridad, espionaje competitivo, daño a la infraestructura crítica, fuga de datos, apropiación de cuentas.

### Flood Attacks

Sobrecarga de los canales de comunicación (correos electrónicos, llamadas telefónicas, mensajería de las redes sociales).

### Ataques de denegación de servicio DoS/DDoS

Ataques competitivos y dirigidos para sobrecargar los servicios web y la red.

### Ataques a las Infraestructuras Críticas

Ataques al suministro de agua, a la infraestructura de transporte, a los sistemas de control de las redes eléctricas.

### Ataques de Malware

Creación, proliferación y control de malware, botnets, rescates y spyware.

# QUIENES SOMOS

Un equipo de profesionales altamente calificados con:

Habilidades Avanzadas de Ethical hacking.  
Certificaciones Profesionales Reconocidas Internacionalmente.  
Mas de 10 Años de Experiencia Comprobados en Ciberseguridad.  
Habilidades de ataque avanzadas sobre diferentes aspectos de la ciberseguridad.

[www.davicyber.com](http://www.davicyber.com)