# Fraud Intelligence Platform (FIP Glauco)

## Sistema de Identificación de Fraude digital

Roberto Peña Cardeña / Jose Luis Sanchez Martinez

# Fraude Digital – Situación Actual

**Soluciones Tecnológicas Actuales**

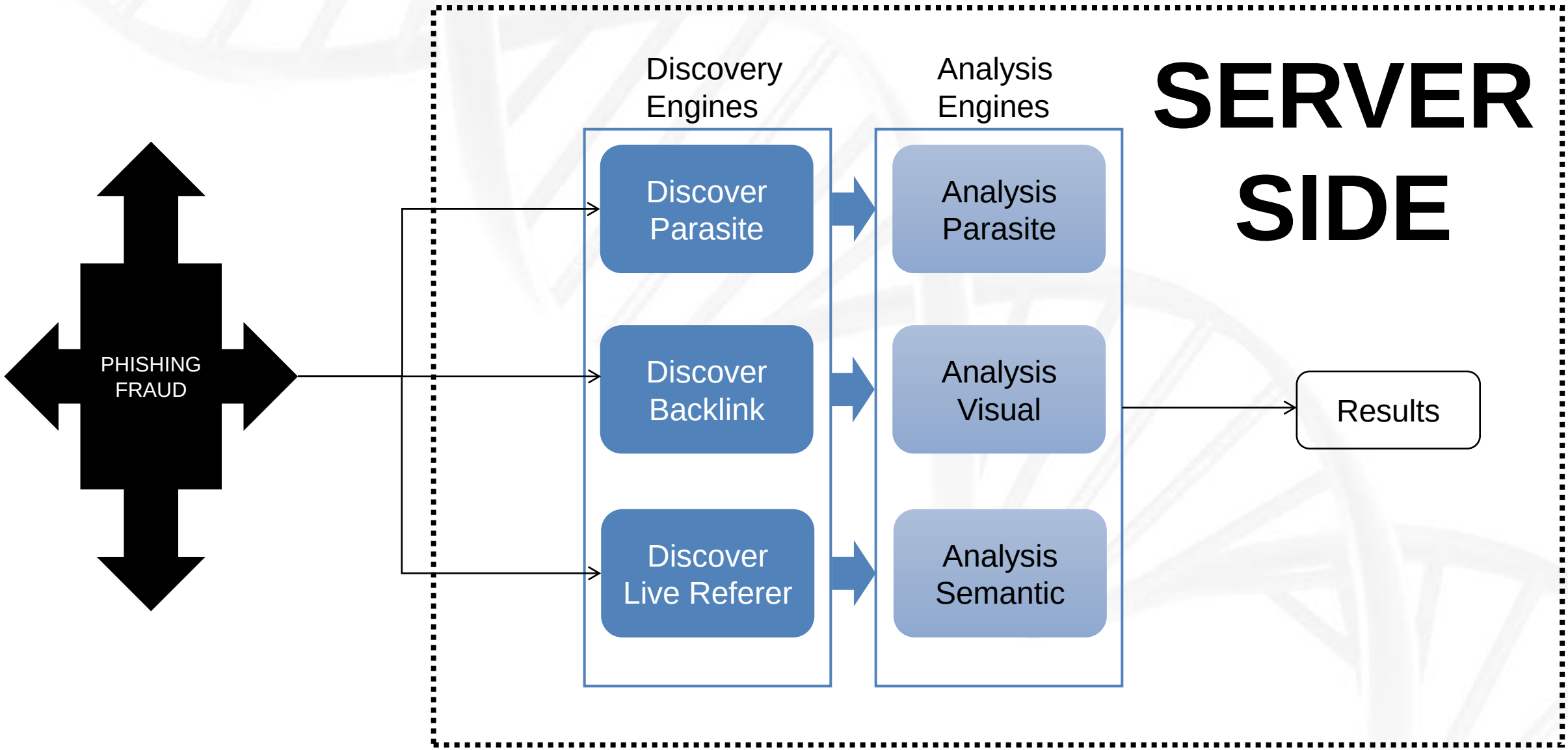
Sistemas basados en certezas de clonado y capacidades sobre código heredado de forma reactiva

**Métodos de Ataque**

Black Market de distribución de Phishing avanzado, con diseño ad-hoc, evolución a la toma de información y preparación para posibles ataques APT.

# Glauco Sistema de Detección de Fraude Digital

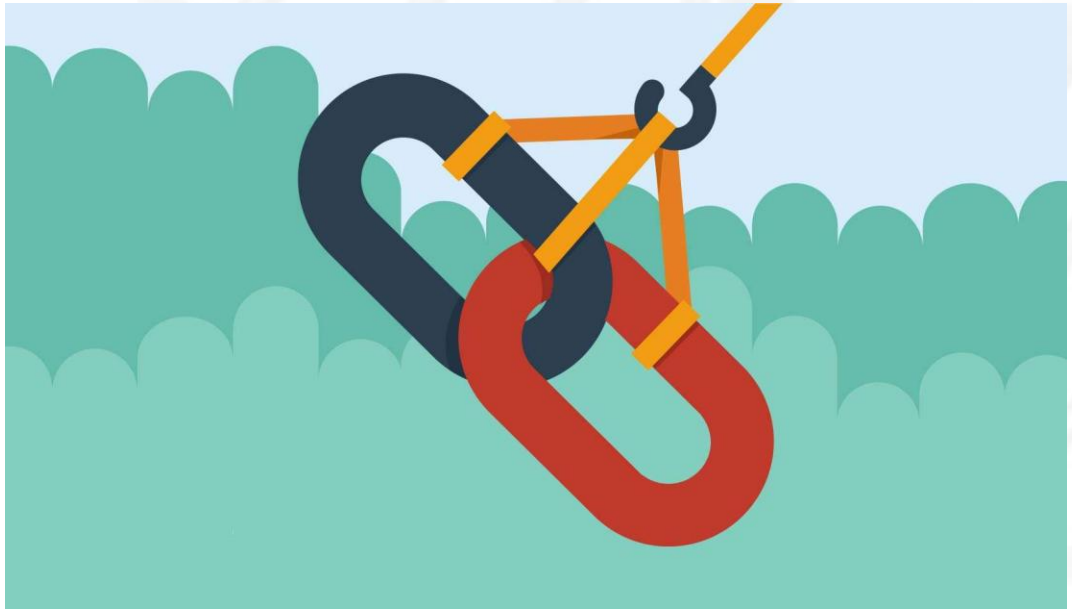
## Estructura


SERVER SIDE
Discovery Engines
Analysis Engines
PHISHING FRAUD
Discover Parasite
Discover Backlink
Discover Live Referer
Analysis Parasite
Analysis Visual
Analysis Semantic
Results

# Glauco Sistema de Detección de Fraude Digital

## Discovery Engines

# Fraude Digital – Descubrimiento Backlink & Referer



Sistema de revisión basado en la capacidad de indexación de los navegadores y de los sistemas de catalogación y registro de estructuras en internet.

Sistema de análisis basado en la revisión sobre la cabecera del origen de las peticiones a través del parámetro referer, basándonos en la conexión inicial y posteriores de comprobación del fraude.

# Fraude Digital – Parasite

Sistema de análisis basado en peticiones a través de un fichero JavaScript desde el sitio fraudulento al original para su descubrimiento y comprobación de fraude.

# Glauco Sistema de Detección de Fraude Digital

## Analysis Engines

# Fraude Digital – Semantic Engine / Problema VS Solución

```
<!DOCTYPE html PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML>
  <HEAD>
    <TITLE
    </TITLE>
  </HEAD>
<BODY>
  <P>Hello World!</P>
</BODY>
</HTML>
```

SAME SAME BUT DIFFERENT

```
<?php
function SGVsbG8gV29ybGQh($_ = 0) {(
            $___=__FUNCTION__
            )&&
            !$_ and list($_,$__) =
array_values(array_filter($___(42), $___)) and
            !$_($__($___)) and    $___($___); return    $_
&42         ?current(get_defined_functions()):(
            !((
            $_=md5($_))-42*2)or
            !(md5($_ = md5($_))-42/2
            *3)
);};
SGVsbG8gV29ybGQh();
```

---

```
<!DOCTYPE html PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML>
  <HEAD>
    <TITLE
    </TITLE>
  </HEAD>
<BODY>
  <P>Hello World!</P>
</BODY>
</HTML>
```

**Hello World!**

```
<?php
function SGVsbG8gV29ybGQh($_ = 0) {(
    $___=__FUNCTION__
    )&&
    !$_ and list($_,$__) = array_values(array_filter($___(42), $___)) and
    !$_($__($___)) and    $___($___); return    $_    &42       ?current(get_defined_functions()):(
    !((
    $_=md5($_))-42*2)or
    !(md5($_ = md5($_))-42/2
    *3)
);};
SGVsbG8gV29ybGQh();
?>
```

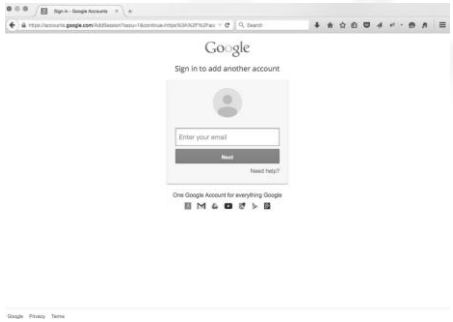
**Hello World!**

Fraud Intelligence Platform (FIP Glauco) – Sistema de identificación de fraude digital

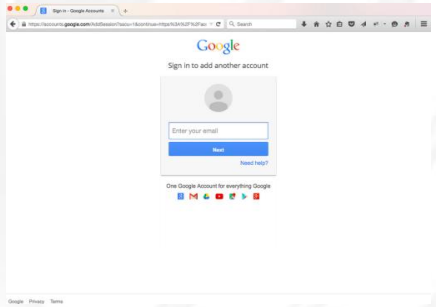
Roberto Peña Cardeña / Jose Luis Sanchez Martinez

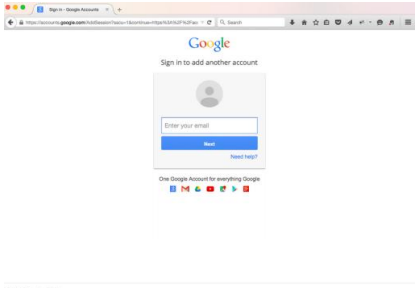
MNEMO cn-cert centro criptológico nacional

# Fraude digital – Visual Engine / Problema

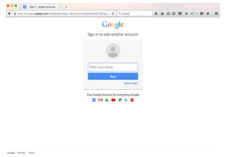


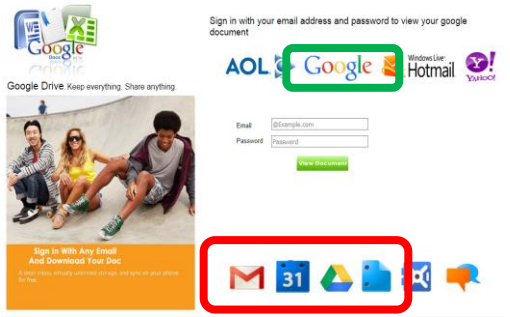




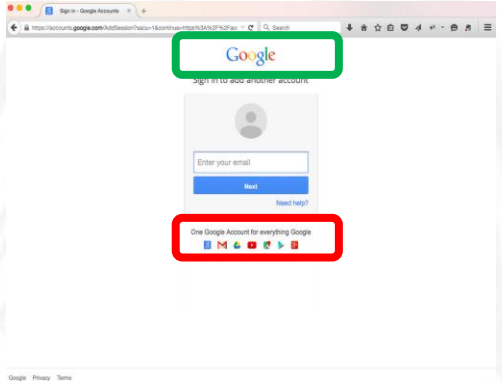












Fraud Intelligence Platform (FIP Glauco) – Sistema de identificación de fraude digital

Roberto Peña Cardeña / Jose Luis Sanchez Martinez

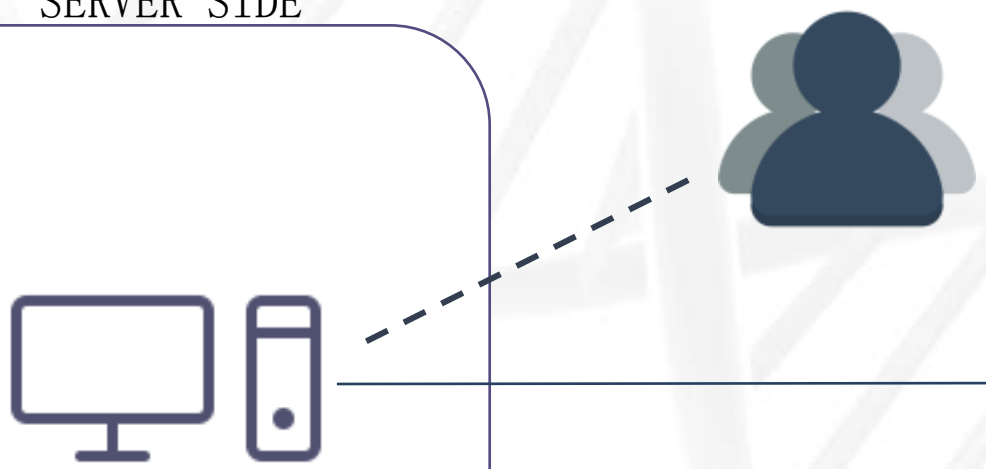
MNEMO ccn-cert centro criptológico nacional

# Fraude Digital – Visual Engine / Solución

# Glauco Sistema de Detección de Fraude Digital

## Funcionamiento y Demos

SERVER SIDE



Live Referer

Backlink

Parasite

DISCOVER

Visual

Semantic

Parasite

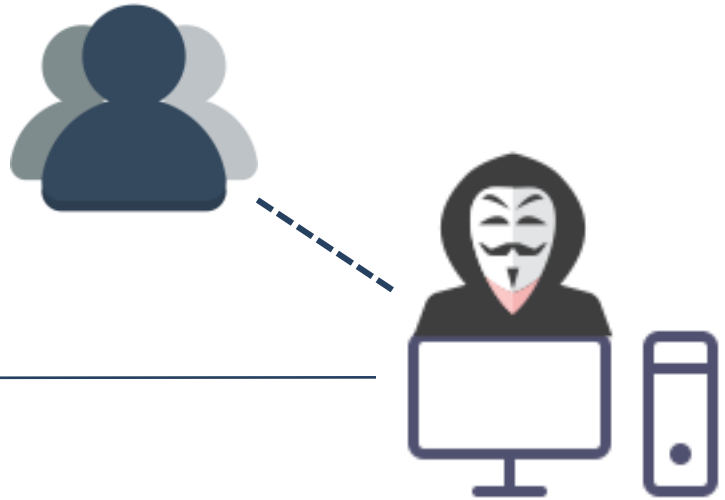
ENGINES

- Limpiar el body
- Redireccionar al sitio legítimo
- Mostrar mensaje al cliente
- Enviar e-mail
- Alertar al CERT-SOC

MNEMO

ccn-cert
centro criptológico nacional

SERVER SIDE



Live Referer

Backlink

Parasite

DISCOVER

Visual

Semantic

Parasite

ENGINES

- Detección semántica de caracteres representativos
- Detección visual completa
- Detección visual parcial multipixel
- Generación de defensas

MNEMO

cn-cert centro criptológico nacional

# Glauco Sistema de Detección de Fraude Digital

## Video demo y Real demo

MNEMO


## CONTACTOS

**Roberto Peña:**
r.peca@mnemo.com

**José Luis Sánchez:**
jl.sanchezmartinez@mnemo.com