6° Coloquio de proyectos
de Becarios en Seguridad Informática

Sistema de Análisis Automatizado de Phishing y Sitios Maliciosos (SAAPM)

Gerardo Corona López
Andrea Itzel González Vargas
María Guadalupe Sarmiento Campos

UNAM CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Agenda

- Introducción
- Problemática
- Herramientas utilizadas
- SAAPM
- Conclusiones
- Lecciones aprendidas
- Estado actual-futuro del proyecto

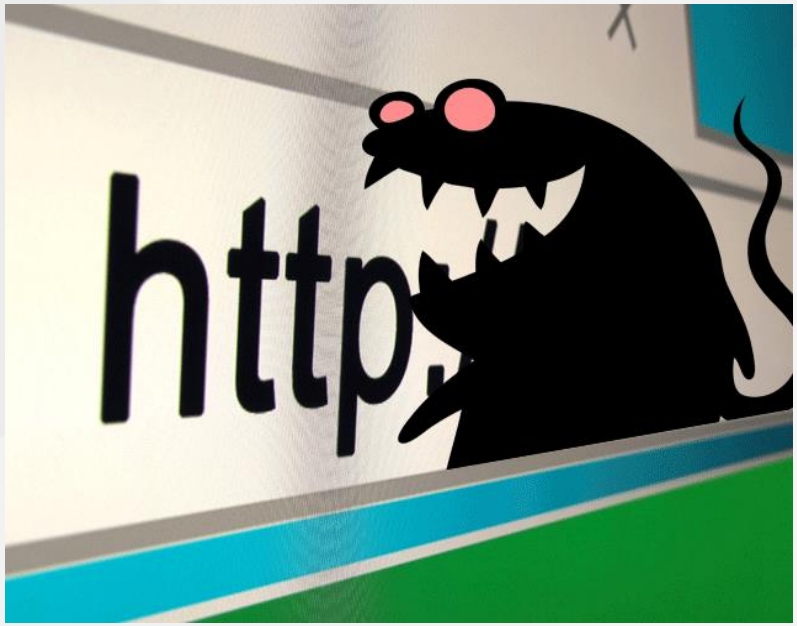
¿Qué es SAAPM?

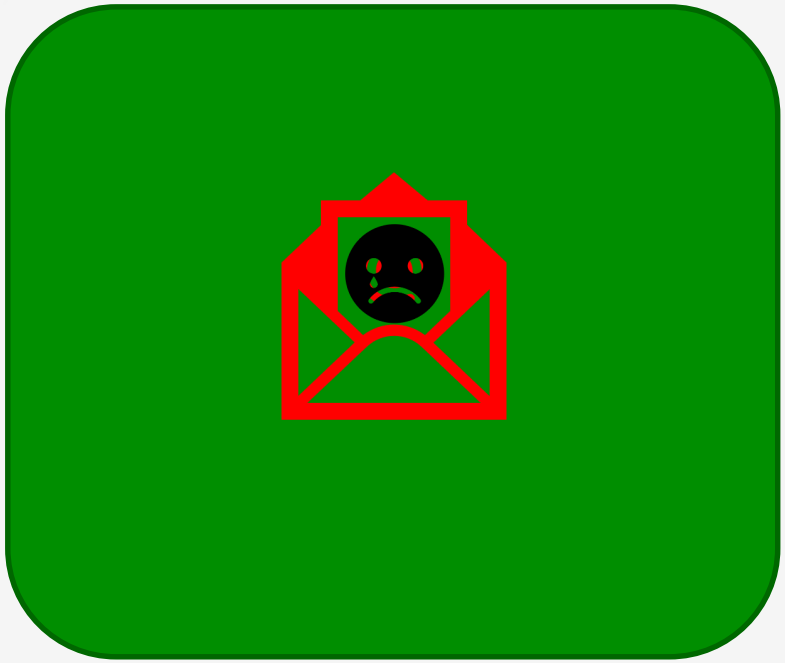
- **Clasifica direcciones URL y archivos maliciosos**
- **Automatiza**
  1. Análisis
  2. Gestión
  3. Notificación
- **Genera gráficas del comportamiento**
- **Genera reportes**

Objetivos

- Crear una herramienta que facilite al analista la gestión de sitios maliciosos
- Análisis de direcciones URL y correos de forma automatizada
- Generación de reportes
- Generación de gráficas sobre el comportamiento de los sitios maliciosos

Problemática



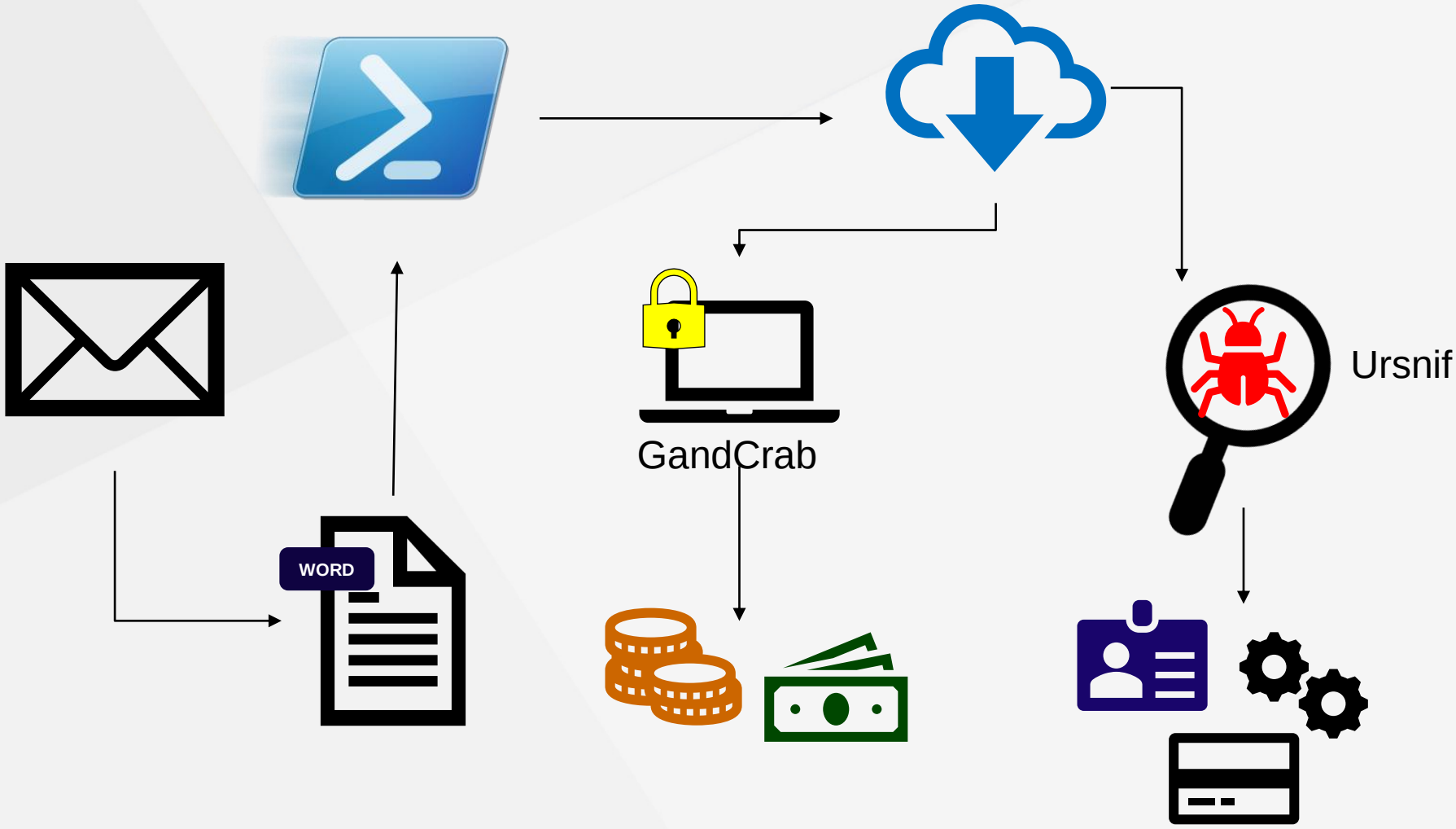


Kaspersky, 2014, Typosquatters, Recuperado de https://media.kasperskydaily.com/wp-content/uploads/sites/87/2014/03/05212421/Typosquatters.png

Problemática

UNAM, 2018, Phishing, Recuperado http://www.fundacionunam.org.mx/wp-content/uploads/2018/08/PISHING2.jpg

Carbon Black



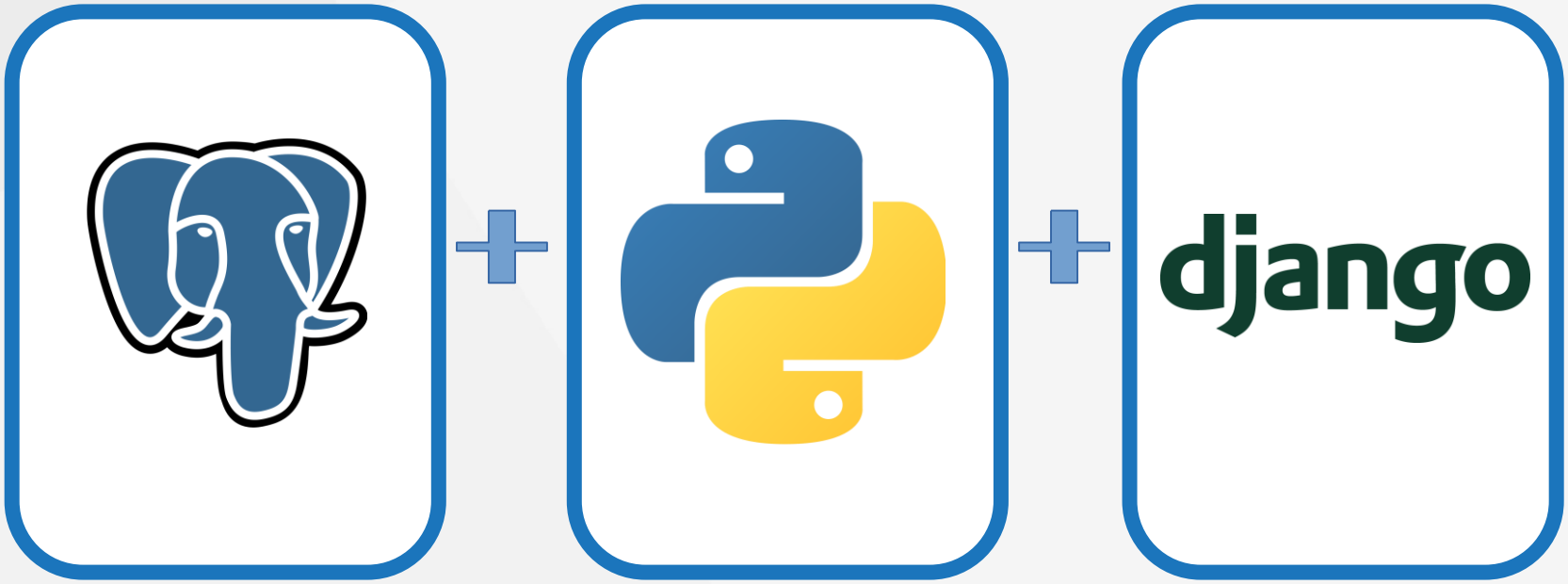
Threat post, 2019, Phishing Campaign Delivers Nasty Ransomware, Credential-Theft Two-Punch, Recuperado https://threatpost.com/phishing-gandcrab-ursnif/141182/

WeTransfer

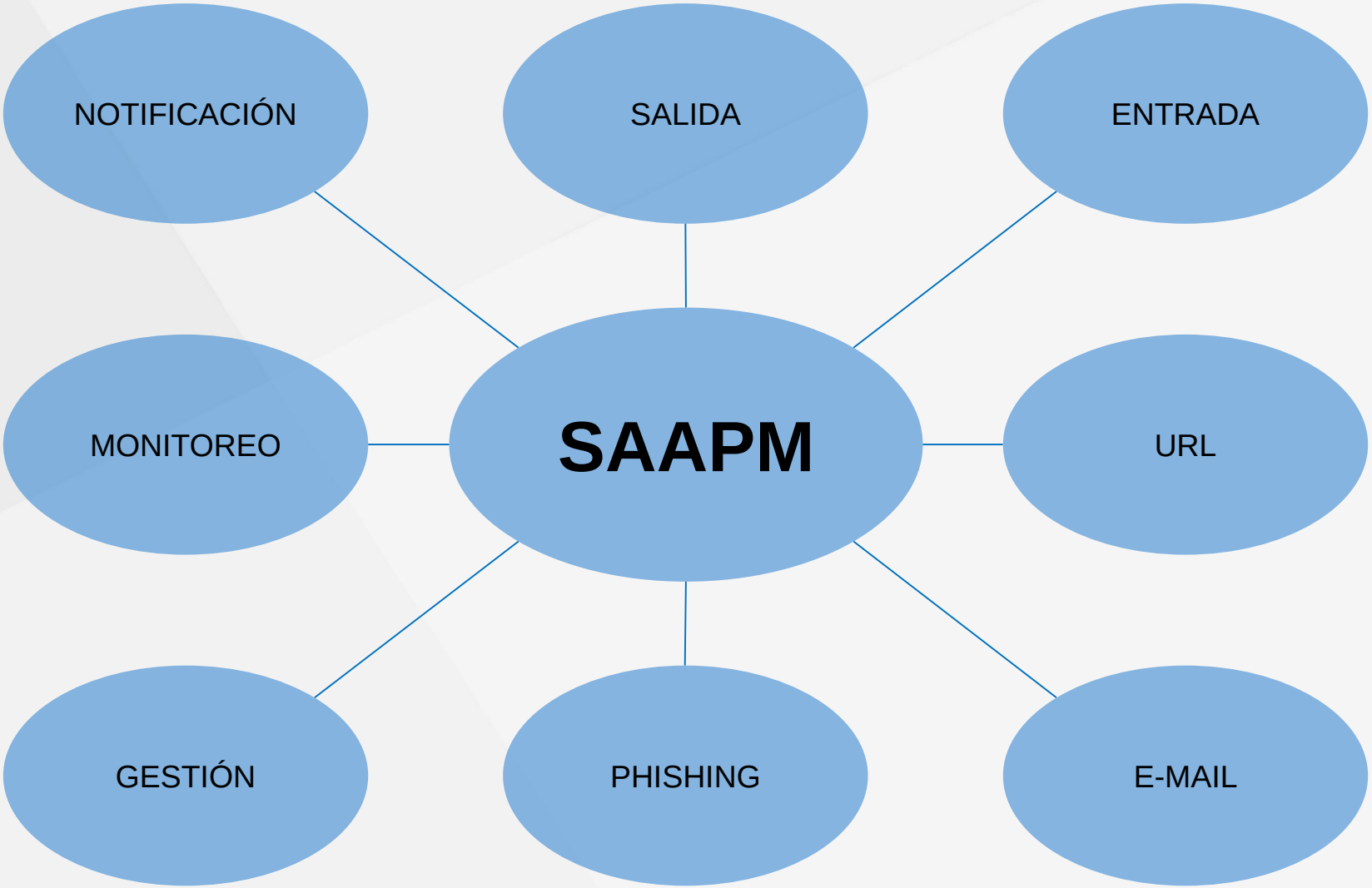
ESET, 2019, Campaña de phishing envía correo con supuestos archivos vía WeTransfer, Recuperado https://www.welivesecurity.com/la-es/2019/02/08/campana-de-phishing-envia-correo-con-supuestos-archivos-via-wetransfer/

Herramientas utilizadas

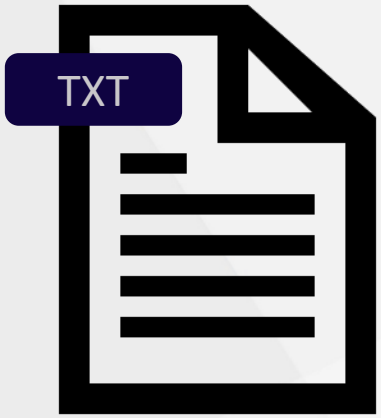
- Python 3
- Django
- PostgreSQL



Módulos


NOTIFICACIÓN
SALIDA
ENTRADA
MONITOREO
SAAPM
URL
GESTIÓN
PHISHING
E-MAIL

Módulo de Entrada



Módulo de Entrada

- URL:
  - Comas
  - Saltos de línea
- Email:
  - Cabeceras de correo

Módulo de URL

Verifica URLs Reporte

# Sitios analizados	3
# Sitios activos	1
# Sitios inactivos	0
# Redirecciones	2
# Dominios afectados	1

ENTIDADES

PayPal: 1

TÍTULOS

Log in to your PayPal account: 1

DOMINIOS

paypalgiftss.github.io: 3

PAÍSES

NL: 3

SITIOS ACTIVOS

https://paypalgiftss.github.io/paypal.com/webapps/mpp/help-pay-on-ebay/

Fecha de actualización: 27 de Febrero de 2019 a las 21:01

Módulo de URL

Dominio: paypalgiftss.github.io
IP: 185.199.111.153
Código: 200
Estado: Sitio activo
Correos: abuse@github.com
ISP: GitHub
País: Países Bajos
ASN: AS54113 Fastly
Servidor: GitHub.com
RIR: RIPE Network Coordination Centre
Servidores DNS: No identificados
Fecha de creación: 27 de Febrero de 2019 a las 21:01
Ignorado: No
Reportado: No
Detección: Sitio phishing
Entidad afectada: PayPal
Título: Log in to your PayPal account
Ofuscación: Base64

Módulo de Email

Módulo de Email

Procesamiento de Correo

CABECERAS | RAW | REPORTE DE URLS | ARCHIVOS ADJUNTOS

CAMPO	VALOR
From	= Usuario 1 <correo@dominio.com>
Subject	Apoyo para revisar archivo
X-Spam-Status	No, score=-7.396 required=4 tests=[AM.WBL=-5, ALL_TRUSTED=-1, BAYES_00=-1.9, DC_IMAGE_SPAM_HTML=0.81, DC_IMAGE_SPAM_TEXT=0.242, DC_PNG_UNO_LARGO=0.001, HTML_MESSAGE=0.001, RP_MATCHES_RCVD=-0.55] autolearn=ham autolearn_force=no
In-Reply-To	<poc@dominio.com.mx>
X-Spam-Score	-7.396
Delivered-To	correo@dominio.com

Módulo de Email

X-Spam-Flag	NO
To	correo@dominio.com
Received	from localhost (localhost [127.0.0.1]) by correo.com (Postfix) with ESMTP id 5658A2212A0 10 Oct 2018 19:06:57 -0500 (CDT)
Date	Wed, 10 Oct 2018 19:11:14 -0500
Content-Type	multipart/mixed; boundary="----------A24EB10DBACA0EBAEBF1FFC7"
X-Virus-Scanned	amavisd-new at correo.com
Return-Path	<correo@dominio.com>

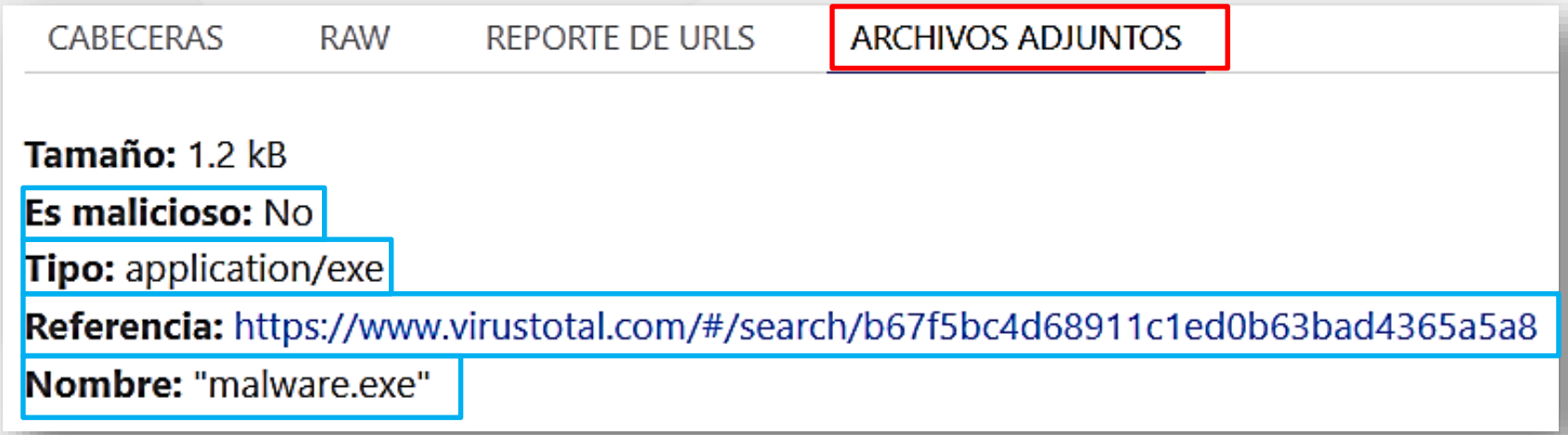
Módulo de Email

CABECERAS | RAW | REPORTE DE URLS | ARCHIVOS ADJUNTOS

```
Return-Path: <correo@dominio.com>
X-Original-To: correo@dominio.com
Delivered-To: correo@dominio.com
Received: from localhost (localhost [127.0.0.1])
    by correo.com (Postfix) with ESMTP id 5658A2212A0
    for <correo@dominio.com>; Wed, 10 Oct 2018 19:06:57 -0500 (CDT)
X-Quarantine-ID: <qOLYx1OQNK86>
X-Virus-Scanned: amavisd-new at correo.com
X-Amavis-Alert: BANNED, message contains Sat_Mexico.vbs,UNDECIPHERABLE
X-Spam-Flag: NO
```

Módulo de Email

Módulo de Email



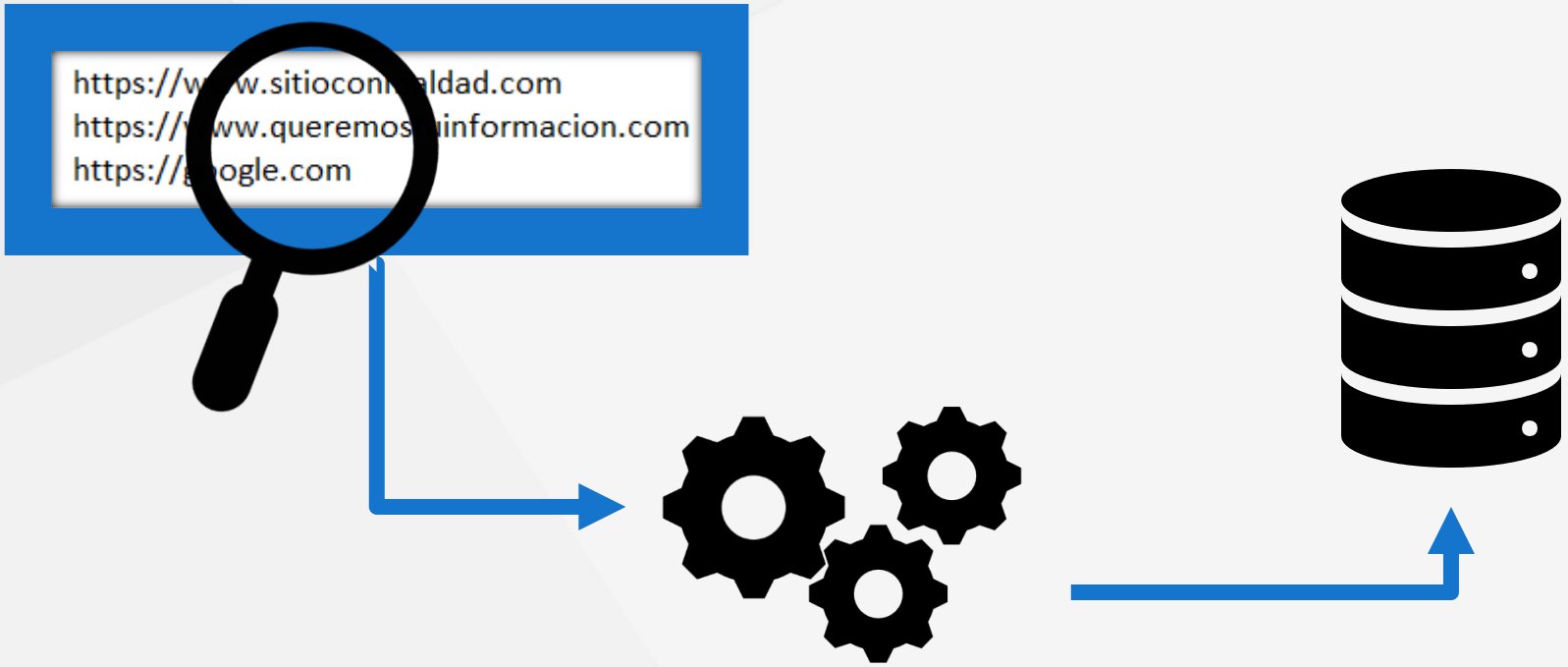
Módulo de Email

https://www.sitioconmaldad.com
https://www.queremostuinformacion.com
https://google.com

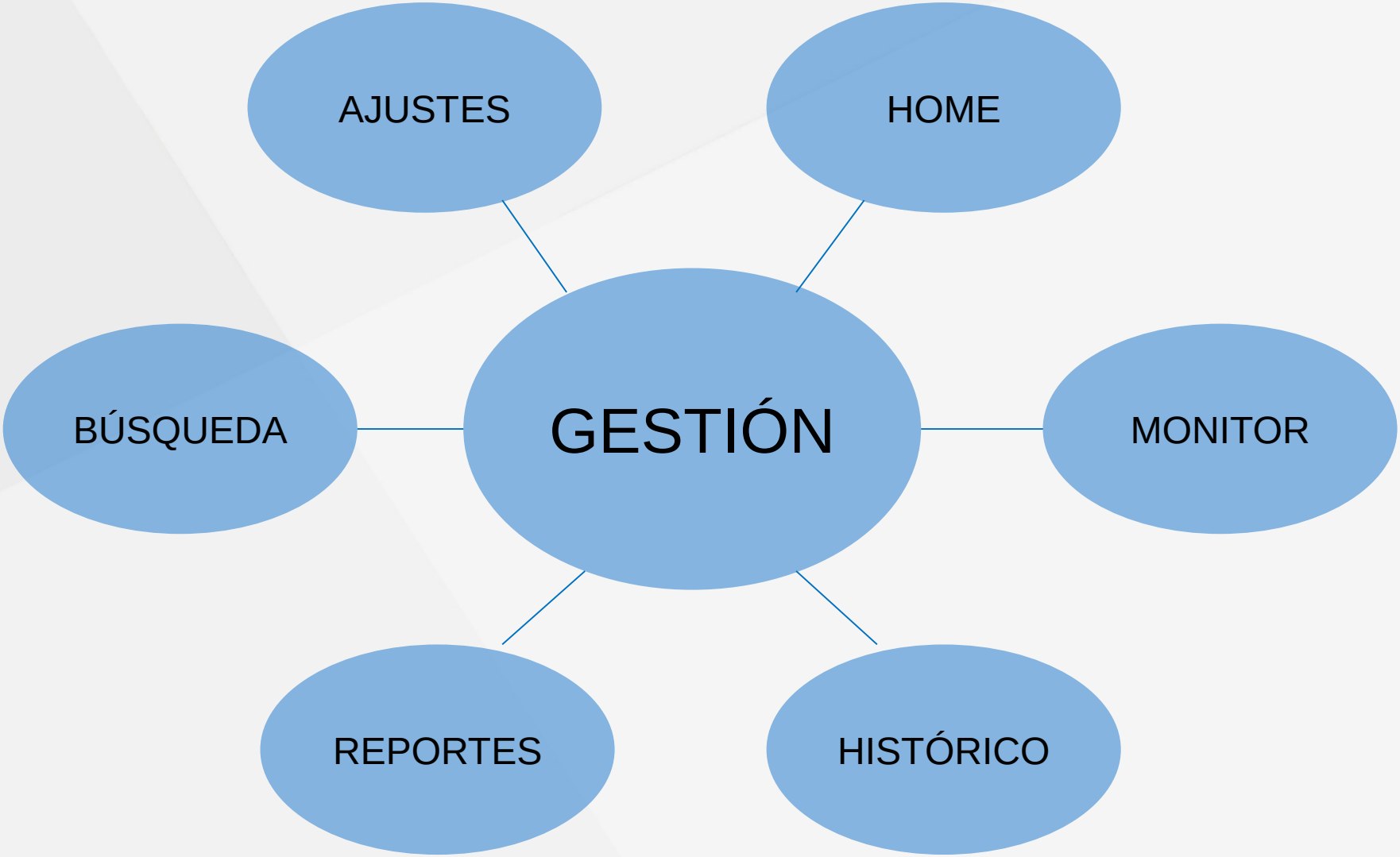
Módulo Phishing

Módulo de Phishing

- Análisis, procesamiento y clasificación de información relacionada de cada sitio Phishing.



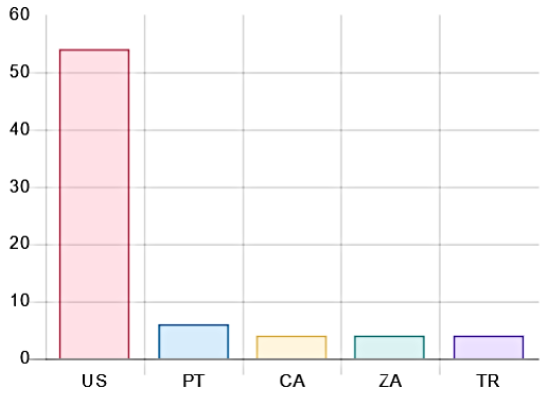
Módulo de Gestión



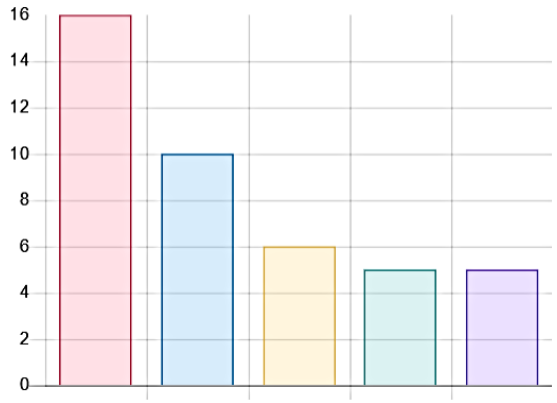
Submódulo Home (Dashboard)

Sistema de Análisis Automatizado de Phishing y Sitios Maliciosos

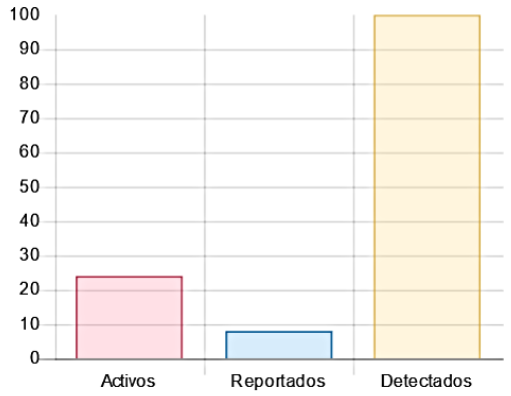
TOP 5 PAÍSES
Top 5 países que hospedan sitios phishing



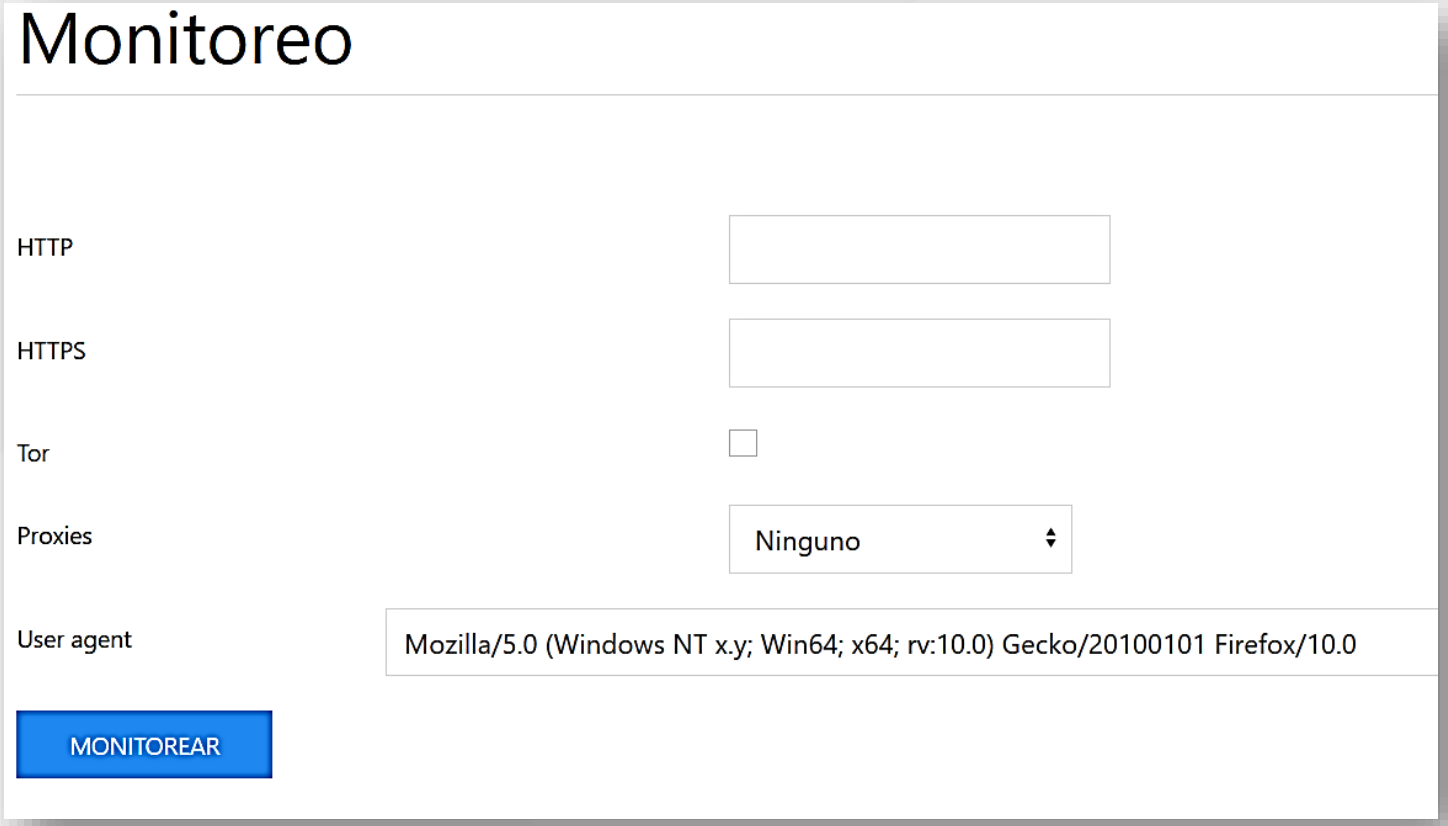
TOP 5 HOSTING
Top 5 servicios de hosting que hospedan sitios phishing



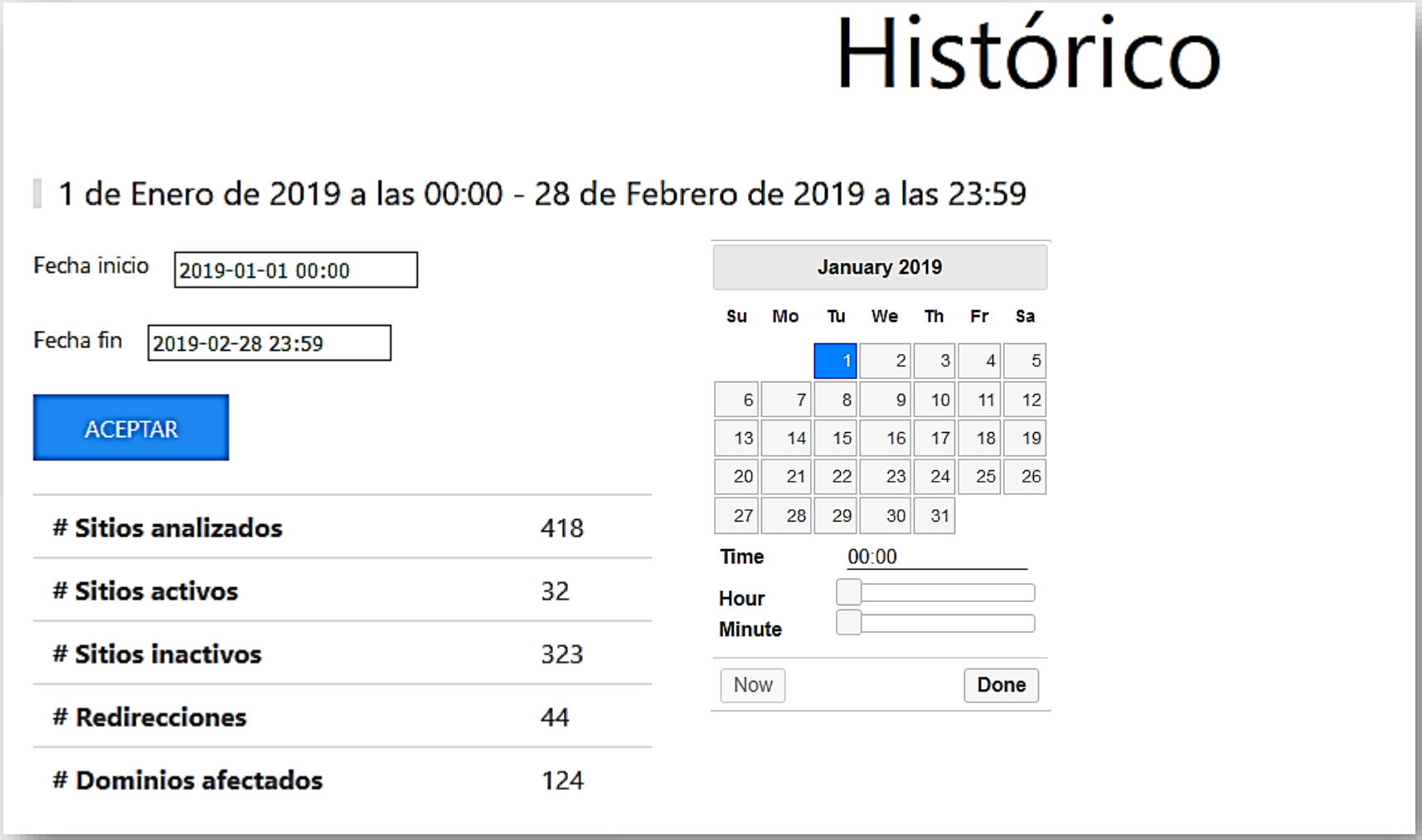
SITIOS PHISHING
Número de sitios phishing detectados, activos y reportados



Submódulo de Monitoreo



Submódulo de Histórico



Submódulo de Histórico

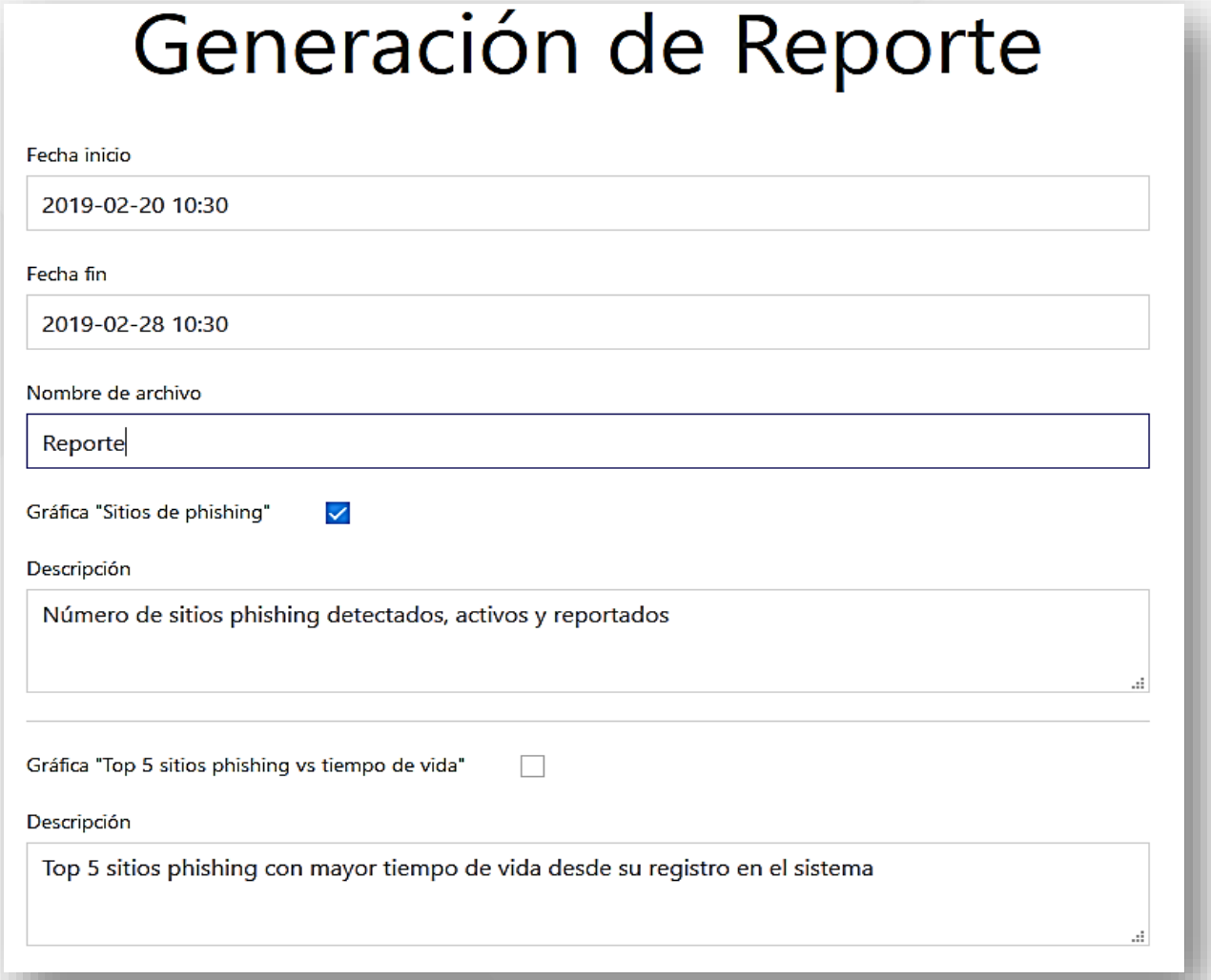
ENTIDADES
- Facebook: 2
- AliExpress: 2
- Santander: 2
- Outlook: 1
- Google: 13
- PayPal: 2
- American Express: 44

TÍTULOS
- Amex Express - Identity Verification: 2
- Apple Pay: 2
- Suspected phishing site | Cloudflare: 1
- Step 2 : Enter Payment info: 1
- Facebook: 1
- American Express - Activation of One Time Password: 4
- Sign In: 2
- American Express Login: 2

DOMINIOS
- www.pybm.com.mx: 6
- vixenly-scissors.000webhostapp.com: 1
- prolightsounds.com: 3
- www.velashapeiii-movil.com.mx: 6
- mexlunacoin.com: 6

PAÍSES
- US: 153
- FR: 1
- RU: 1
- ES: 1
- CA: 19
- CH: 4

Submódulo de Reporte



Submódulo de Reporte

Reporte

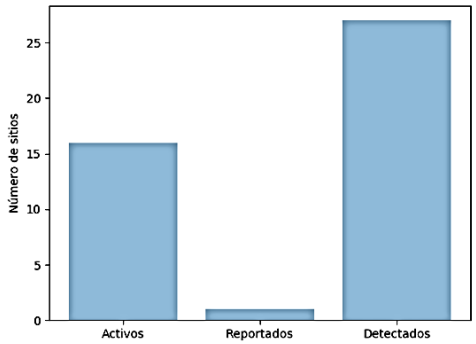
Reporte elaborado por la herramienta **SAAPM**

Periodo

De: **2019-02-20 10:30:00-06:00** A : **2019-02-28 10:30:00-06:00**

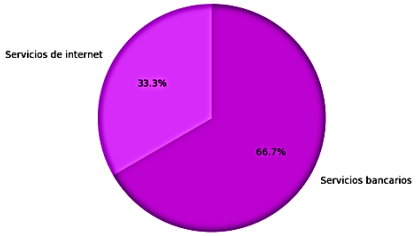
ESTADOS DE SITIOS PHISHING

Número de sitios phishing detectados, activos y reportados



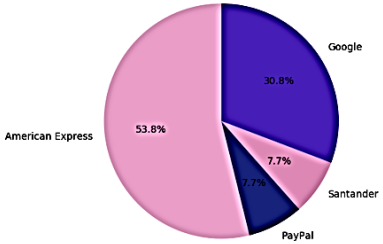
SECTORES AFECTADOS

Sectores que han sido afectados por sitios phishing



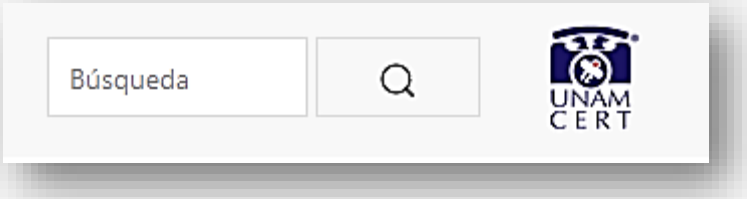
ENTIDADES AFECTADAS

Entidades que han sido afectadas por sitios phishing



Submódulo de Búsqueda

- URL
- Dominio
- Dirección IP
- Correo
- Hash (MD5)



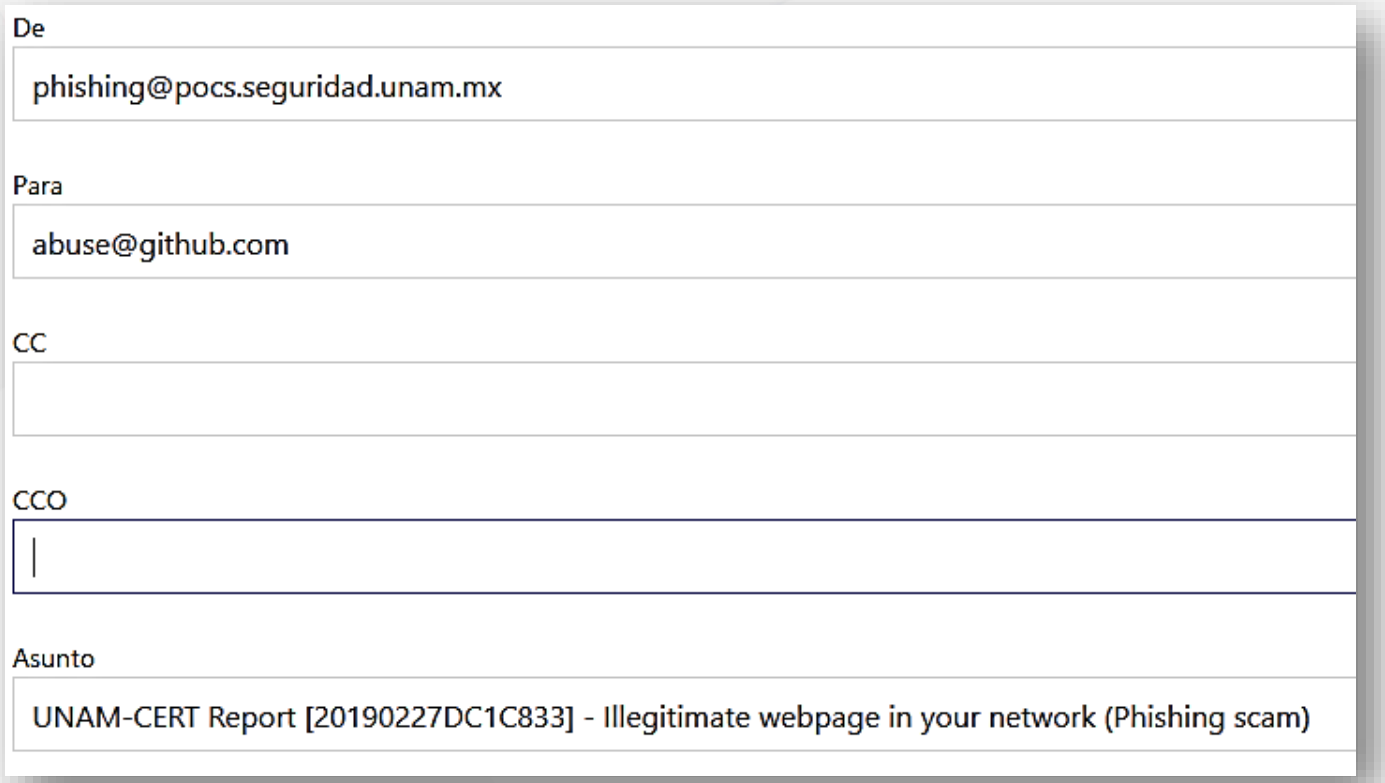
Submódulo de Ajustes

- Plantillas para el reporte por medio de Email
- Configuración de Proxy
- Listas blancas
- Configuración en general de interés para el analista

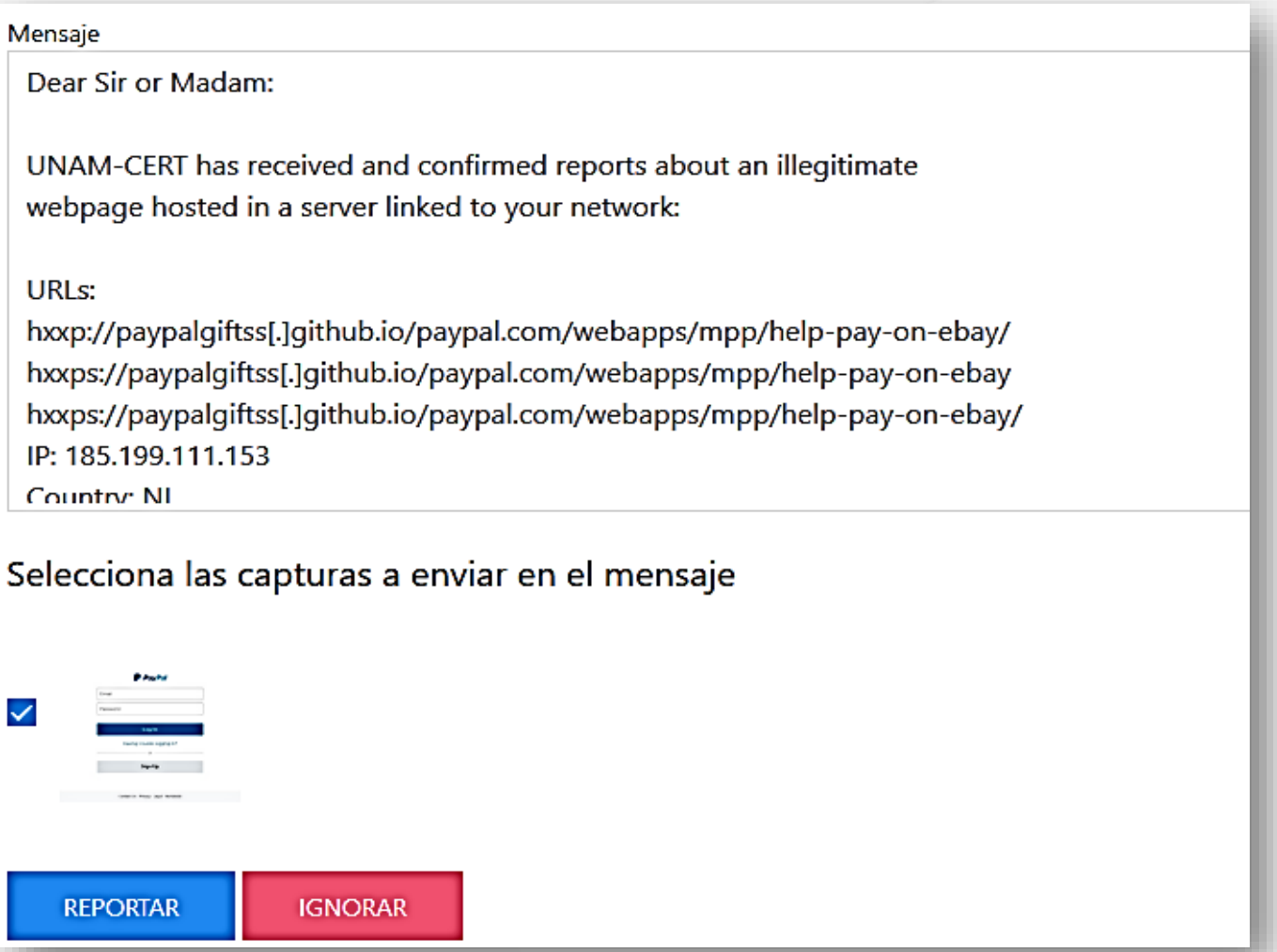
Módulo de Monitoreo

- Automatización de tareas
- Análisis de correos: **phishing@pocs.seguridad.unam.mx**
- Monitoreo de las URL
- Notificaciones

Módulo de Notificación



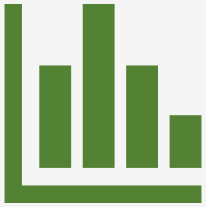
Módulo de Notificación

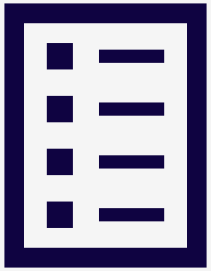


Módulo de Salida

Genera archivos con información de interés para el analista:

- Compilación de direcciones IP, dominios y URL
- Reglas de firewall





Demostración del Sistema

Conclusiones

- Automatización
  1. Ahorro de tiempo.
  2. Notificación oportuna a los responsables.

- Análisis de gráficas
  1. Identificación de campañas phishing.
  2. Tendencias

- Análisis de correos y URL
  1. Identificación de nuevos modos de engaño al usuario

Lecciones aprendidas

- Al reportar a tiempo un sitio malicioso logramos que menos usuarios sean victimas de robo, estafa, etc.

- Para reducir el número de usuarios afectados por sitios maliciosos, es necesario capacitarlos para identificar sitios y correos maliciosos.

Estado actual-futuro del proyecto

ALCANCE

- **Actual:** CSI/UNAM-CERT
- **Futuro:** Comunidad UNAM y sitio público

BITACORAS

- **Actual:** CSI/UNAM-CERT
- **Futuro:** Entidades de seguridad de terceros para generar inteligencia

TIEMPO

- **Actual:** Tareas aún ejecutadas manualmente
- **Futuro:** Automatizar tareas para mejorar tiempo de reporte y cierre de sitios phishing.

GRACIAS

Andrea Itzel González Vargas
Facultad de Ciencias-UNAM
andrea.gonzalez@bec.seguridad.unam.mx

Gerardo Corona López
Facultad de Ingenieria-UNAM
gerardo.corona@bec.seguridad.unam.mx

María Guadalupe Sarmiento Campos
UPIITA-IPN
maria.sarmiento@bec.seguridad.unam.mx