



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

Agenda

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

¿Qué es SAAPM?

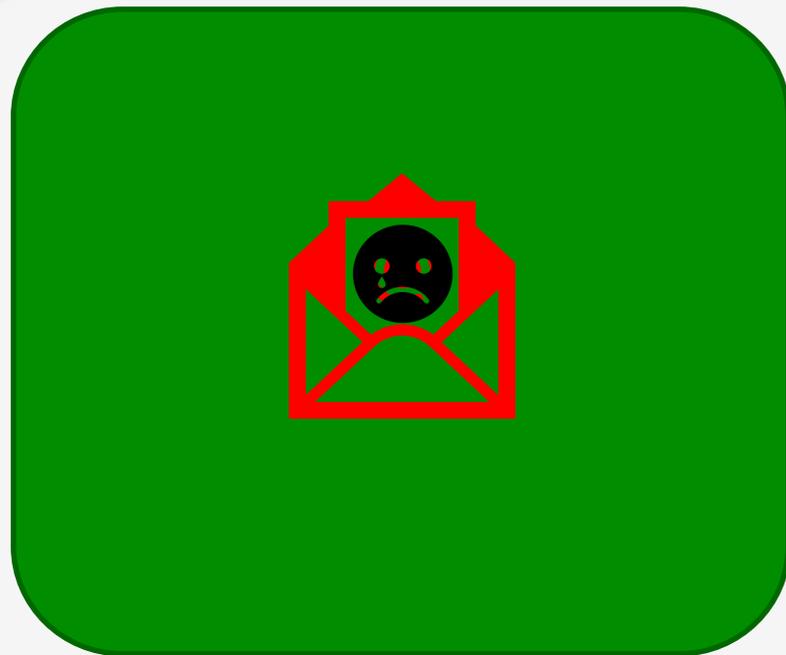
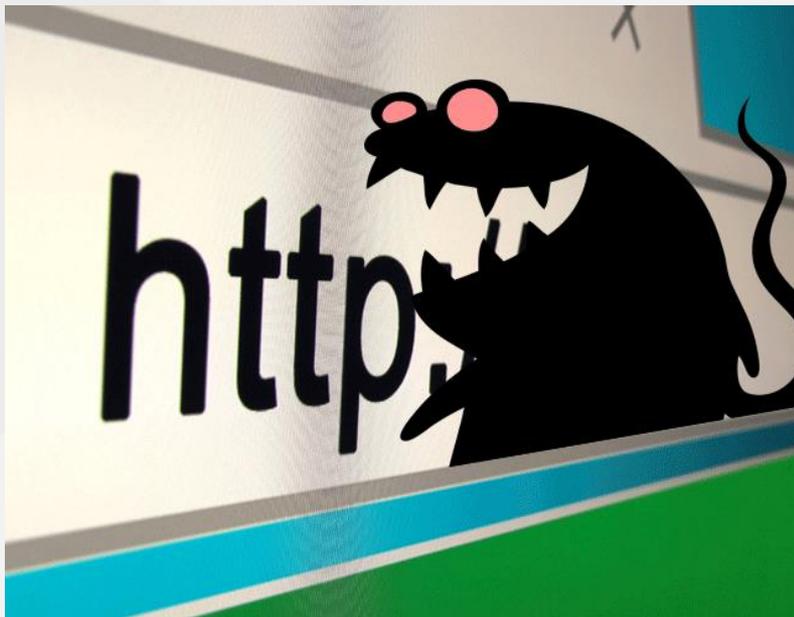
- **Clasifica direcciones URL y archivos maliciosos**
- **Automatiza**
 1. Análisis
 2. Gestión
 3. Notificación
- **Genera gráficas del comportamiento**
- **Genera reportes**

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



Problemática

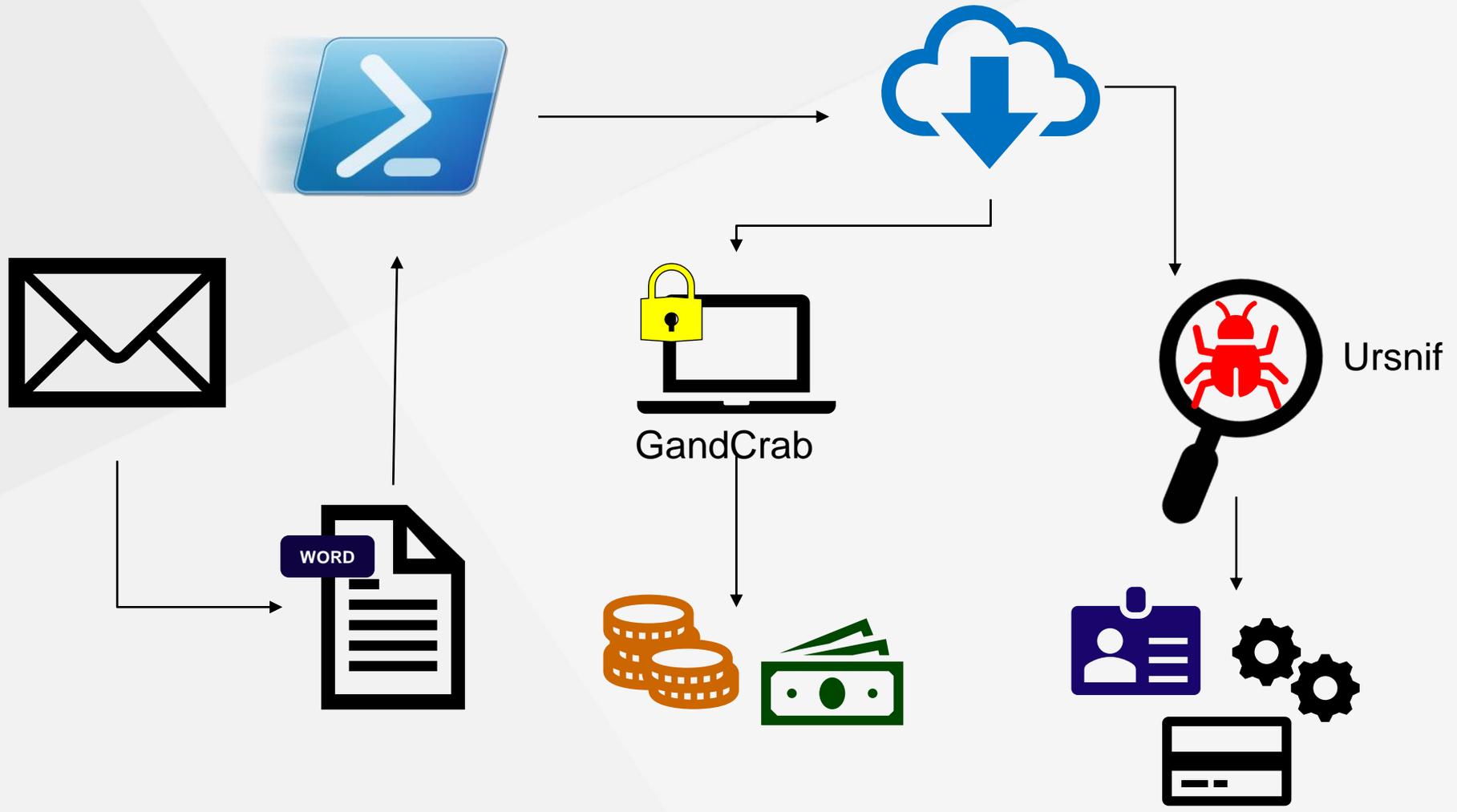
PHISHING Frases comunes

- Acceda al siguiente **enlace** para conocer sus adeudos.
- Presione **clic aquí** para **descargar** su estado de cuenta.
- Multa** por incumplimiento de obligaciones fiscales.
- Evite sanciones, revise por favor el **documento anexo**.

CienciaUNAM

UNAM
La Universidad de la Nación

Carbon Black



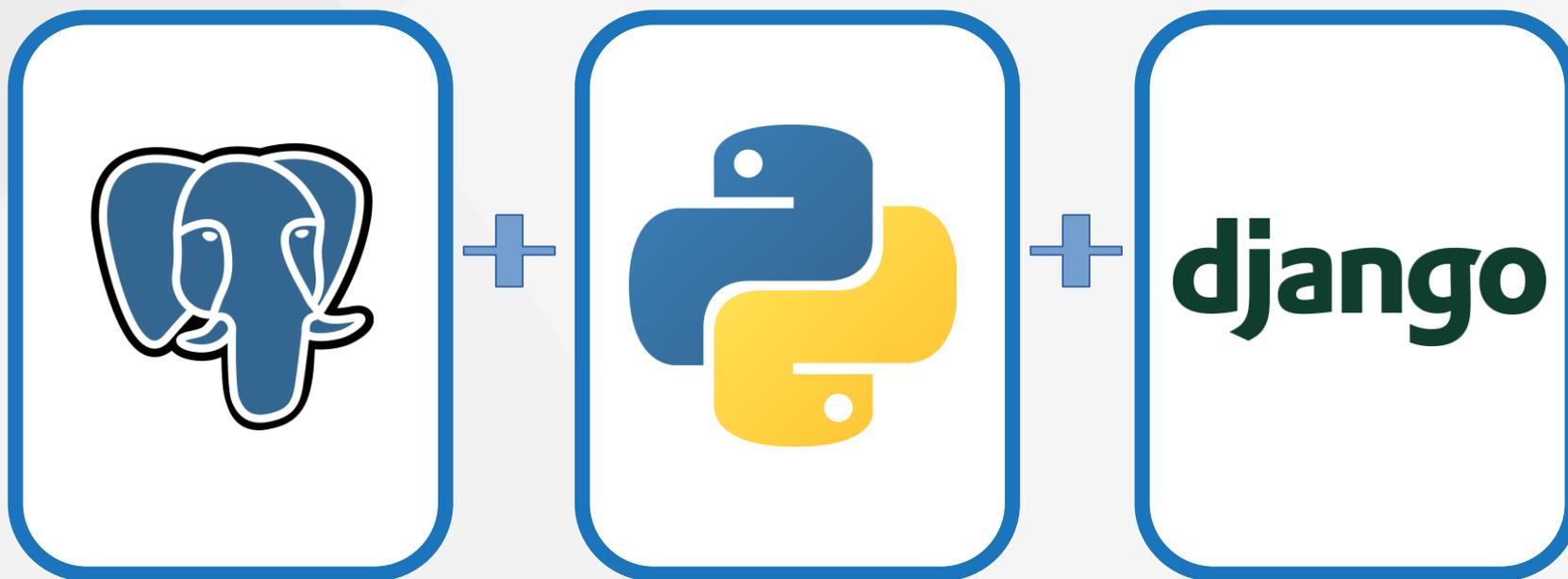
Threat post, 2019, Phishing Campaign Delivers Nasty Ransomware, Credential-Theft Two-Punch, Recuperado <https://threatpost.com/phishing-gandcrab-ursnif/141182/>

WeTransfer

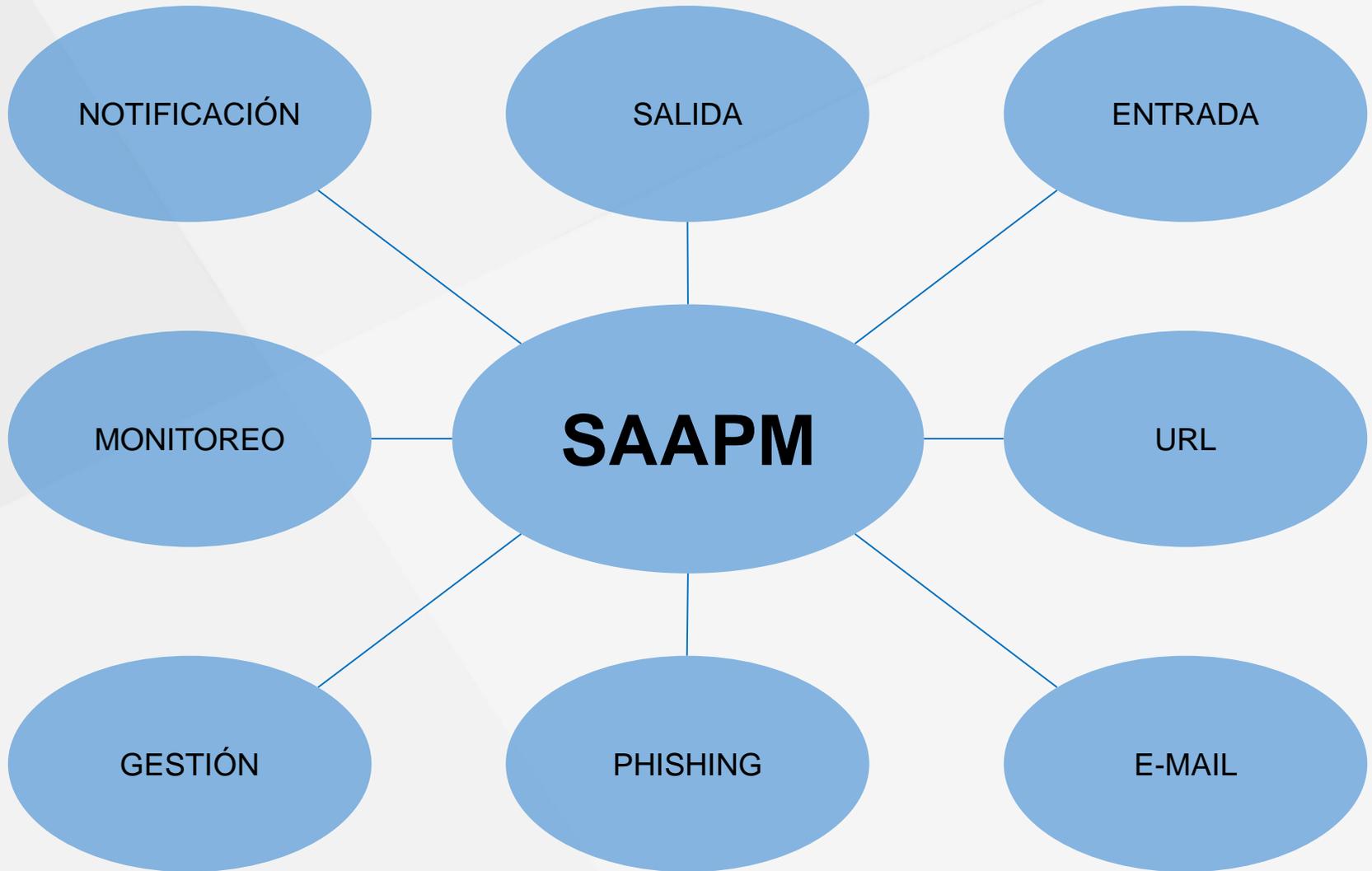


Herramientas utilizadas

- Python 3
- Django
- PostgreSQL



Módulos



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

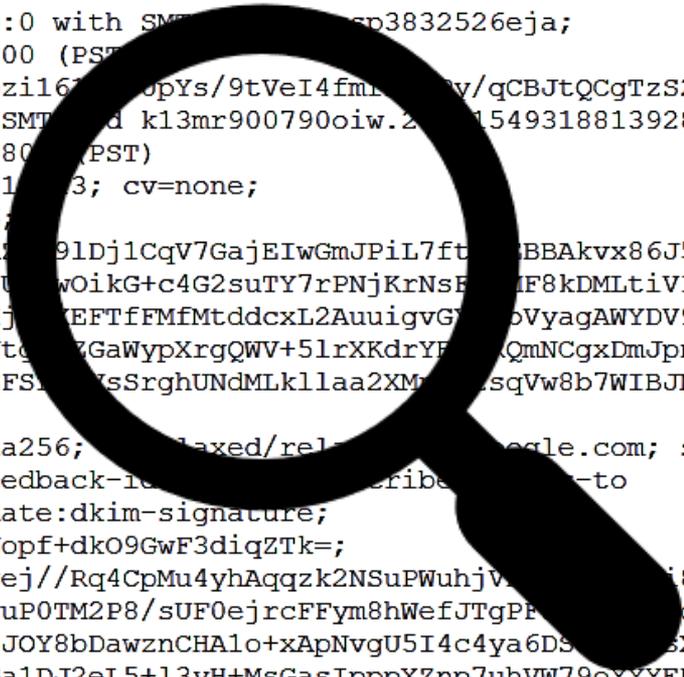
Detección: Sitio phishing

Entidad afectada: PayPal

Título: Log in to your PayPal account

Ofuscación: Base64

Módulo de Email



```
Delivered-To:
Received: by 2002:a17:906:33cc:0:0:0:0 with SMTP id sp3832526eja;
    Mon, 4 Feb 2019 14:20:14 -0800 (PST)
X-Google-Smtp-Source: AHgI3IaP2zeMBpzi167.../9tVeI4fml.../qCBJtQCgTzS27Nsn+LwEHE97aYgSot51mY
X-Received: by 2002:a54:440d:: with SMTP id k13mr900790oiw.2...1549318813928;
    Mon, 04 Feb 2019 14:20:13 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=154931...3; cv=none;
    d=google.com; s=arc-20160816;
    b=TKT6sNBvtC44r7SaXlj/S7Ca+AA...91Dj1CqV7GajEIwGmJPiL7ft...BBAkvx86J5
    Bu3ZoqxtPNxKLGa0tsImmQ7eJml...wOikG+c4G2suTY7rPNjKrNsB...F8kDMLtiV1t
    WH2eV6VbUFRBmZlrz2gamHskTmHj...EFTfFmFmTddcxL2AuuigvG...bVYagAWYDV9E
    0iIUKkFFmfm76IXNX55Mt3D2GUT...ZGaWypXrgQWV+5lrXKdrYF...QmNCgxDmJpn6
    ntNJEYjntXiMDm39bn/yKbcOVREFS...sSrghUNDMLk1laa2XM...sqVw8b7WIBJNA
    rWIw==
ARC-Message-Signature: i=1; a=rsa-sha256; relaxed/relaxed; d=google.com; s=arc-20160816;
    h=mime-version:message-id:feedback-id:reply-to:reply-to:reply-to:from:subject:to:date:dkim-signature;
    bh=Va4kIg0PFZO/LwbHWSgB99C0Nopf+dk09GwF3diqZTk=;
    b=RL7WrYNb8wwD+Edyb49pZf4Gfgej//Rq4CpMu4yhAqqzk2NSuPWuhjv...i8
    4qt7/FaeOnCfAiT5KHo7OrLDttvuP0TM2P8/sUF0ejrcFFym8hWefJTgPP...qT
    J/LTlxJUVJqsoObp6+irBSjWen/JOY8bDawznCHAl0+xApNvgU5I4c4ya6DS...SXM
    IL27fPoJATgiGSBupypX4xnoIHGa1DJ2eL5+13yH+MsGasIpppXZnp7uhVW79oYYERE
    3fmv1HLOHJBG739YIix0rejxDGuVjI/RlUS5zdg6vxyYZeuerLytUB5LtlTWxrn1x3oH
    u4Uw==
```

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 ESMTTP id 5658A2212A0

for <correo@dominio.com>; Wed, 10 Oct 2018 19:06:57 -0500 (CDT)

X-Quarantine-ID: <qOLYx10QNK86>

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

CABECERAS	RAW	REPORTE DE URLS	ARCHIVOS ADJUNTOS
# Sitios analizados		0	
# Sitios activos		0	
# Sitios inactivos		0	
# Redirecciones		0	
# Dominios afectados		0	
ENTIDADES			
TÍTULOS			
DOMINIOS			
PAÍSES			

Módulo de Email

CABECERAS

RAW

REPORTE DE URLS

ARCHIVOS ADJUNTOS

Tamaño: 1.2 kB

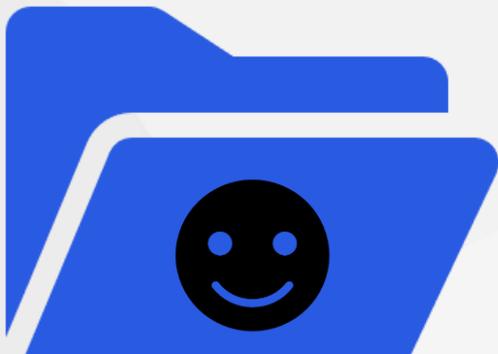
Es malicioso: No

Tipo: application/exe

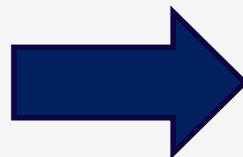
Referencia: <https://www.virustotal.com/#/search/b67f5bc4d68911c1ed0b63bad4365a5a8>

Nombre: "malware.exe"

Módulo de Email



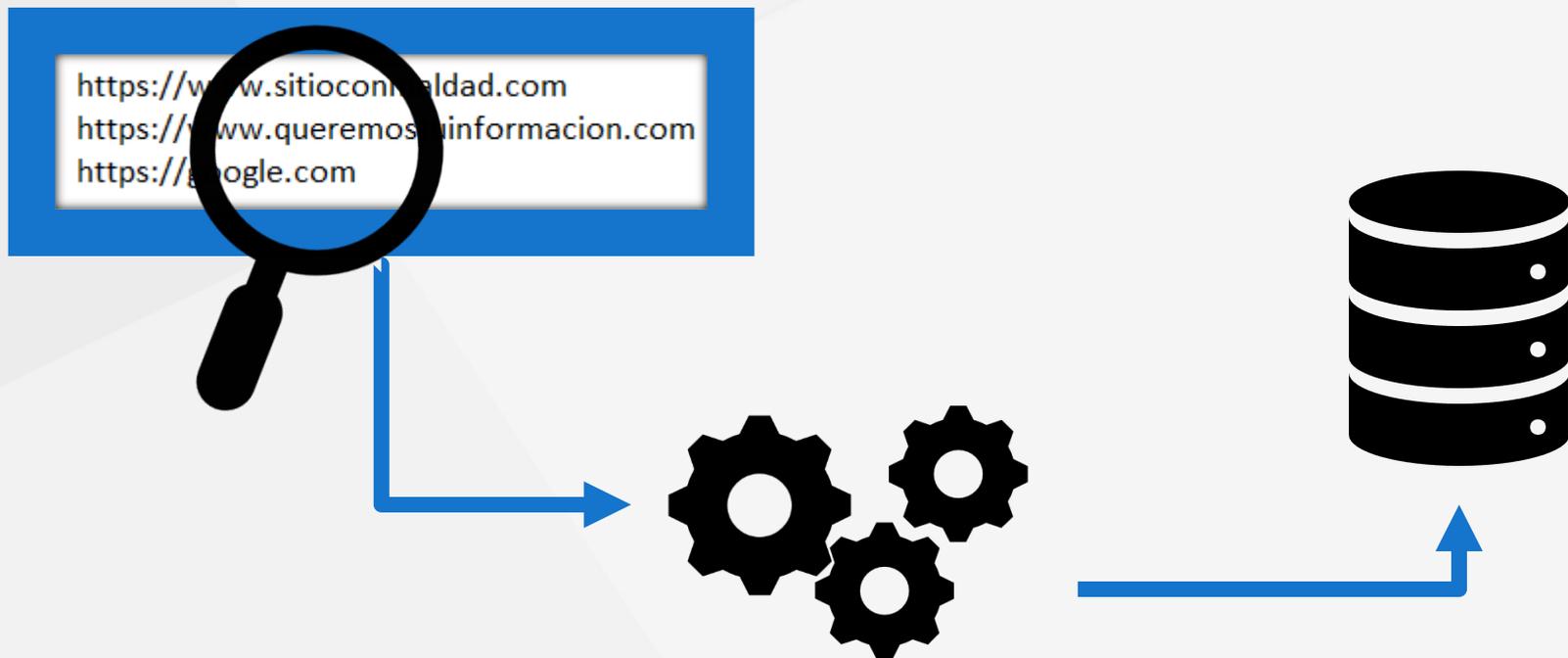
<https://www.sitioconmaldad.com>
<https://www.queremostuinformacion.com>
<https://google.com>



Módulo
Phishing

Módulo de Phishing

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



Módulo de Gestión

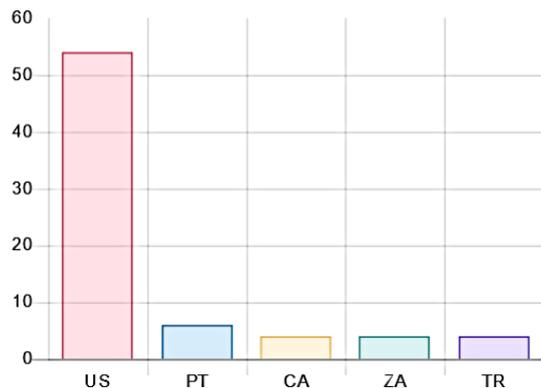


Submódulo Home (Dashboard)

Sistema de Análisis Automatizado de Phishing y Sitios Maliciosos

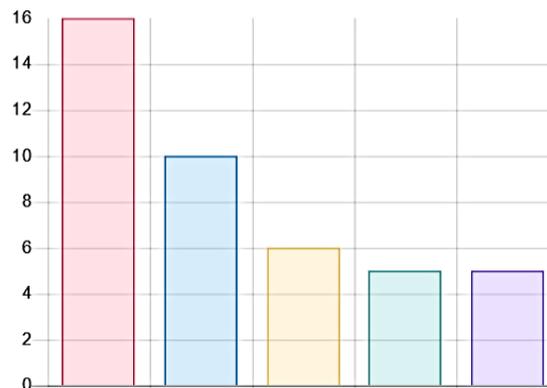
TOP 5 PAÍSES

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

Monitoreo

HTTP

HTTPS

Tor

Proxies

User agent

Mozilla/5.0 (Windows NT x.y; Win64; x64; rv:10.0) Gecko/20100101 Firefox/10.0

MONITOREAR

Submódulo de Histórico

Histórico

1 de Enero de 2019 a las 00:00 - 28 de Febrero de 2019 a las 23:59

Fecha inicio

Fecha fin

ACEPTAR

# Sitios analizados	418
# Sitios activos	32
# Sitios inactivos	323
# Redirecciones	44
# Dominios afectados	124

January 2019

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Time

Hour

Minute

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

Generación de Reporte

Fecha inicio

2019-02-20 10:30

Fecha fin

2019-02-28 10:30

Nombre de archivo

Reporte

Gráfica "Sitios de phishing"



Descripción

Número de sitios phishing detectados, activos y reportados

Gráfica "Top 5 sitios phishing vs tiempo de vida"



Descripción

Top 5 sitios phishing con mayor tiempo de vida desde su registro en el sistema

Submódulo de Reporte



LibreOffice
The Document Foundation

Reporte

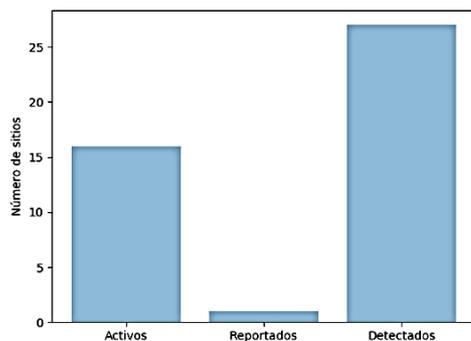
Reporte elaborado por la herramienta SAAPM

Periodo

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

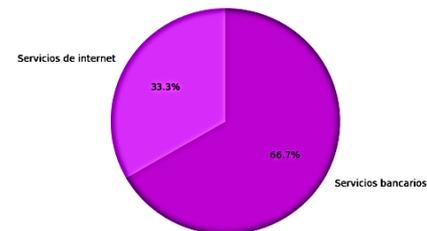
ESTADOS DE SITIOS PHISHING

Número de sitios phishing detectados, activos y reportados



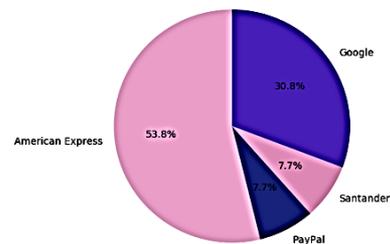
SECTORES AFECTADOS

Sectores que han sido afectados por sitios phishing



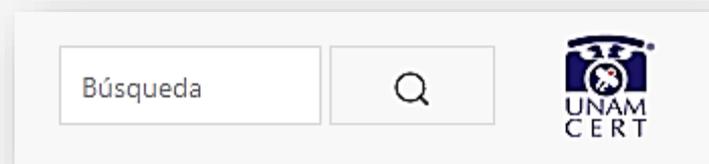
ENTIDADES AFECTADAS

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

5



Módulo de Notificación

De	phishing@pocs.seguridad.unam.mx
Para	abuse@github.com
CC	
CCO	
Asunto	UNAM-CERT Report [20190227DC1C833] - Illegitimate webpage in your network (Phishing scam)

Módulo de Notificación

Mensaje

Dear Sir or Madam:

UNAM-CERT has received and confirmed reports about an illegitimate webpage hosted in a server linked to your network:

URLs:

hxxp://paypalgiftss[.]github.io/paypal.com/webapps/mpp/help-pay-on-ebay/

hxxps://paypalgiftss[.]github.io/paypal.com/webapps/mpp/help-pay-on-ebay

hxxps://paypalgiftss[.]github.io/paypal.com/webapps/mpp/help-pay-on-ebay/

IP: 185.199.111.153

Country: NI

Selecciona las capturas a enviar en el mensaje



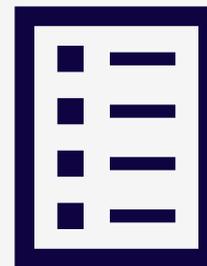
REPORTAR

IGNORAR

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 víctimas 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