Primer acercamiento al Cryptojacking basado en navegador.

J. C. Sepúlveda Serna, L. F. Muñoz Morales, L. Franco Calpa
(Universidad Icesi, Calle 18 No. 122-135 Pance, Cali - Colombia, +57 (2) 555 2334)

***Resumen*— El siguiente ensayo pretende realizar un primer acercamiento a lo que es el funcionamiento y los mecanismo de ataque (profundizando aquellos que suceden a través de un navegador) del cryptojacking. Para la realización de este documento se utilizaron dos artículos que abordan el tema, para indagar así mismo sobre las posibilidades que existen para realizar un experimento propio, que nos permita estudiar y crear propuestas de detección a la tendencia de minar criptomonedas.**
En uno de los modelos estudiados, un usuario ingresa a una página web en la cual descarga de manera inconsciente un código de JavaScript que se ejecuta en su navegador, minando -generalmente, sin su consentimiento- algún tipo de criptomoneda.
En el modelo siguiente se dan a conocer técnicas de defensa y prevención para no resultar víctima de este tipo de red que se encarga de alimentar software malicioso para obtener beneficios de manera ilegal.

***Abstract*— The following essay tries to make a first approach to what is the operation, the attack mechanism (deepening those that happen through a browser) and some defense mechanisms that are exposed during the use of cryptojacking techniques. For the realization of this document two articles were used to address the issue, to investigate itself on the possibilities that exist to conduct an own experiment, which allows us to study and create detection proposals to the tendency to undermine cryptocurrencies.**
In one of the studied models, a user enters a web page in which he unconsciously downloads a JavaScript code that runs in his browser, undermining - usually without his consent - some type of cryptocurrency.
In the following model, defense and prevention techniques are presented so as not to be a victim of this type of network that is responsible for feeding malicious software to obtain benefits illegally.

I. INTRODUCCIÓN

Las criptomonedas han sido un tema del cual se ha discutido mucho durante estos tiempos de globalización y desarrollo tecnológico, debido a su relación con el dinero real pero también a su dudosa procedencia y tratamiento. Bitcoin surgió hace unos años como un proyecto que pretendía evolucionar las divisas materiales a virtuales, transformando así las operaciones más importantes del mercado.
eventualmente, las personas comenzaron a buscar formas eficaces de adquirir "crypto-riquezas".[1] En principio, cuando el Bitcoin apenas surgía, obtener esta moneda desde un computador personal no era un proceso para nada difícil. A medida que iba avanzando la tecnología y los usuarios sentían la necesidad de obtener más monedas, empezaron a surgir estrategias como aumentar la potencia de la CPU de sus ordenadores o desplegar fragmentos de código JavaScript en las páginas web que reclutaron energía de las CPU de sus visitantes, para crear una red de minería más grande.
El objetivo de este documento es estudiar el caso en donde la minería sucede dentro del navegador cuando un usuario entra a un sitio web.

II. OBJETIVOS

General:
A partir de la información obtenida, se plantea realizar un prototipo funcional de un detector de cryptojacking. Dentro del proyecto se pretende, a través de métodos teóricos y prácticos la inspección continua de los recursos del computador que ejecuta el programa desarrollado por el equipo para comparar los patrones que suelen presentarse a la hora de ser atacado por cibercriminales y señalar un estatus.

Específicos:
- Lograr que el software recopile información del uso de CPU (Central Processing Unit) y evaluar desde qué punto puede ser candidato a ser víctima teniendo en cuenta la capacidad de procesamiento.
- Hacer que el programa obtenga información del uso de RAM (Random Access Memory) y evaluar desde qué punto puede ser candidato a ser víctima teniendo en cuenta la capacidad de la memoria temporal.
- Hacer que el software extraiga información del uso del internet y evaluar desde qué punto puede ser candidato a ser

víctima teniendo en cuenta el ancho de banda pasado por parámetro.

- Desarrollar el programa de forma que muestre el estado del computador (Está siendo minado o No está siendo minado) de manera cíclica con una frecuencia de 1 Hz

De mayor alcance:

- Permitir que el software extraiga información del tráfico de red y detecte cantidades de flujo grandes sobre direcciones ip donde no deberían haberlas.
- Lograr que el programa extraiga información de los procesos lógicos más costosos para detectar cuando se está minando y desde dónde (qué programa) se está ejecutando.

III. FUNCIONAMIENTO

La minería en el navegador se considera un abuso con excepción de que exista un consentimiento por parte del usuario. La cantidad de métodos que se utilizan para abusar de los navegadores de los usuarios a través del cryptojacking es amplia. Los resumimos a continuación:

Webmaster initiated: Los administradores de sitios web pueden agregar scripts de minería a su página web, con o sin informar a los usuarios. Esto lo hacen en la mayoría de los casos para monetizar sus sitios. [2]

Servicios de terceros: Muchos sitios web ofrecen servicios activos de JavaScript de terceros dentro de sus propias páginas. Estos podrían ser herramientas de accesibilidad, anuncios de una red de publicidad o servicios de seguimiento y análisis. Los terceros con estos privilegios pueden inyectar scripts de cryptojacking en los sitios que lo usan, ya sea intencionalmente o como resultado de una infracción.

Infracciones: Si un atacante puede violar los principales servidores, sitios web, extensiones o los servicios de scripting que utilizan, puede inyectar scripts de cryptojacking que afectarán a los usuarios del sitio sin el conocimiento o consentimiento del sitio.

IV. HIPÓTESIS

Además de la CPU existen otras variables computacionales que se ven afectadas a la hora de ser víctima de secuestro de recursos cuando un navegador es infectado por medio del cryptojacking. Se plantea que el cryptojacking ejecutado en páginas web alteran el uso de los recursos de la computadora que la está navegando. Inicialmente se dice que éstos recursos son: CPU, RAM y ancho de banda de internet.

V. EXPERIMENTO

Para lo anterior se realizaron pruebas automatizadas donde el sistema visita las páginas potencialmente mineras y calcula el uso de los núcleos de procesamiento, la memoria de acceso aleatorio y la cantidad de información que entra y sale a través de la red. En este experimento se hizo uso del lenguaje de programación Python, sistema operativo Linux y librerías tales como psutil y del sistema.

VI. RESULTADOS

Luego de que se aplicó el promedio de uso de cpu en chromium por cada página, el uso de cpu total y el de ram por instantes de tiempo un total de 100 veces por cada página, se puso en una lista las páginas que se consideran benignas y en otro las que se encontraban sospechosamente mineras. En las benignas, casi ninguna superó el 1% del uso de los procesos lógicos en el browser, mientras que en las potencialmente mineras, casi la mitad sobrepasaba el 10%. Ir a anexos

VII. ANÁLISIS

Un aspecto a tener en cuenta es que las páginas que cargan videos suelen ser las que más procesamiento utiliza, sin embargo, si se compara a youtube.com con peliculashd.site, se puede observar que la diferencia es de aproximadamente el 800% de una con respecto a la otra. En el uso total de CPU algunos promedios llegaron hasta el 60%, esto puede deberse a que el antivirus estuviera en constante chequeo de esta página maliciosa (Se puede descartar la posibilidad de ejecución de otro programa ya que el algoritmo se corrió en condiciones óptimas, es decir, ningún otro programa abierto). En el uso de ram se puede observar valores que

varían entre el 47.71% y el 51.12% para las limpias, y entre el 49.27 y 56.25 para las mineras, lo que indica una diferencia no muy relevante en términos de porcentaje.

VIII. CONCLUSIONES

Una página que no debería hacer nada más que cargar información para ser mostrada, rápidamente pasa a dejar el uso de los núcleos, lo que hace que los links limpios bajen su promedio de uso a un 0% en poco más de 1 minuto. De estos datos se puede evidenciar que la página más sospechosa de ser minera es la de peliculashd.site.

VIV. REFERENCIAS

[1] M. E. Acer, E. Stark, A. P. Felt, S. Fahl, R. Bhargava, B. Dev,
M. Braithwaite, R. Sleevi, and P. Tabriz. Where the wild warnings
are: Root causes of chrome https certificate errors. In CCS, CCS '17,
pages 1407–1420, New York, NY, USA, 2017. ACM.

[2] BBC. Websites hacked to mint crypto-cash. https://www.bbc.com/news/technology-41518351, 2017.

[3] BleepingComputer. The internet is ride with in-browser miners and
it is getting worse each day. https://www.bleepingcomputer.com/news/security/the-internet-is-rife-with-in-browser-miners-and-its-getting-worse-each-day/, 2012. Accessed: 2017-12-08.

[4] CheckPointResearchTeam. October's most wanted
malware: Cryptocurrency mining presents new threat. https://blog.checkpoint.com/2017/11/13/octobers-wanted-malware-cryptocurrency-mining-presents-new-threat/, 2017.

[5] Coinhive. Coinhive monetize your business with your users cpu
power. https://coinhive.com/, 2017. Accessed: 2017-11-20.

X. ANEXOS

Páginas limpias

nombreArchivo	cpuChromium	cpuTotal	ramUsada	kilobytesEnviados	kilobytesRecibidos
'facebook.com'.txt	0.01	10.03	48.7	2069471.0	15134243.0
'github.com'.txt	0.0	7.1	47.79	2077355.0	15153483.0
'google.com'.txt	0.0	7.22	47.61	2071444.0	15143375.0
'mail.google.com'.txt	0.0	13.86	47.8	2085351.0	15171254.0
'twitter.com'.txt	0.0	6.57	48.37	2080263.0	15163034.0

'www.instagram.com'.txt	0.0	14.79	47.71	2083223.0	15167742.0
'youtube.com'.txt	2.21	18.34	51.12	2066103.0	15119288.0

Páginas potencialmente mineras

nombreArchivo	cpuChromium	cpuTotal	ramUsada	kilobytesEnviados	kilobytesRecibidos
'cinemametropolitan.it'.txt	15.46	24.91	56.25	2167965.0	16197850.0
'doorbin.net'.txt	7.71	37.22	49.27	2286510.0	18016781.0
'englishnews.thegoan.net'.txt	6.69	13.58	49.48	2256920.0	17218740.0
'forex-trading.hol.es'.txt	18.85	35.92	50.75	2100648.0	15232837.0
'hydraulica-ua.com'.txt	7.61	60.96	53.82	2197833.0	16681167.0
'iaijiu.com'.txt	19.89	33.11	39.63	2299583.0	18173037.0
'mymarriage.co.za'.txt	2.49	8.68	55.32	2144149.0	15726524.0
'no'.txt	2.04	10.7	55.36	2144624.0	15729358.0
'onepace.net'.txt	8.6	18.87	51.82	2278018.0	17836075.0
'peliculashd.site'.txt	17.54	37.03	50.48	2230936.0	16908993.0
'pimpmylevel.cryptdough.co.uk'.txt	5.99	17.04	49.95	2221687.0	16759572.0
'piratebayproxy247.org'.txt	0.7	11.52	49.51	2090182.0	15181647.0
'pra.open.tips'.txt	7.24	10.93	50.87	2176870.0	16313498.0

'redbitcoins.net'.txt	9.81	33.93	54.86	2241973.0	17041536.0
'sj2s.hostei.com'.txt	3.39	8.84	50.31	2172670.0	16281544.0
'studyenglishgenius.com'.txt	6.67	21.26	51.33	2215608.0	16747996.0
'tommyhulihanbasketball.com'.txt	11.16	15.99	48.9	2113771.0	15365433.0
'www.thehopepage.org'.txt	0.66	6.95	54.82	2140592.0	15670808.0
'www5.fmovie.cc'.txt	2.95	11.7	52.59	2185061.0	16413305.0