No. 31 / mayo - junio 2018

.Seguridad®

Cultura de prevención para TI

31

El valor de la privacidad

Datos personales en tiempos del panóptico

Criptomonedas y la minería no autorizada

Confidencialidad de la información

Tendencias 2018

Mitos y realidades de la red Tor

HoneyProxy: análisis de tráfico HTTP

Contenido

.Seguridad
Cultura de prevención para TI

La creación de criptomonedas y la minería no autorizada 4

Confidencialidad de la información 12

Tendencias 2018: el costo de nuestro mundo conectado 17

Mitos y realidades de la red Tor: Análisis de tráfico en un nodo de salida 23

HoneyProxy: análisis de tráfico HTTP 47

Editorial

.Seguridad
Cultura de prevención para TI

El valor de la privacidad:

Datos personales en tiempos del panóptico

Las principales ciber amenazas en la actualidad son el ransomware y el minado de criptomonedas no autorizado. Estas podrían provocar la suspensión de servicios críticos, la primera porque inhabilita los sistemas a cambio de un rescate, y la segunda porque podría secuestrar la capacidad de cómputo de una gran cantidad de máquinas para generar ganancias en moneda virtual; pero además de estas amenazas, los profesionales en ciberseguridad deben lidiar con las estafas de correos electrónicos empresariales, el uso de exploits como EternalBlue o EternalRomance y las vulnerabilidades de día cero, algunas de las cuales son aprovechadas por los cibercriminales poco tiempo después de ser descubiertas.

A pesar de que el escenario podría parecer sombrío, es necesario reconocer que en el mundo hay cada vez más conciencia sobre la ciberseguridad, gracias a los esfuerzos de los profesionales en el ramo que buscan mejorar las legislaciones para regular las actividades del mundo digital, al aumento en los programas de recompensas por vulnerabilidades o a las revelaciones de prácticas inapropiadas en la industria, que ha ampliado el debate sobre la privacidad de la información, en una sociedad en la que las empresas que prestan servicios "gratuitos" a los usuarios finales funcionan como un panóptico que registra nuestra vida digital para lucrar con ella.

En este mundo de amenazas, en el que los usuarios finales juegan un papel estelar (por ser el eslabón más débil en la cadena de seguridad), el tema del control de los datos personales ha tomado relevancia debido a la preocupación de que las personas puedan ser controladas por medio de la información que ellas mismas otorgan a las organizaciones y porque se ha destacado que los usuarios son el producto de las compañías, quienes lucran con la información personal de distintas maneras. Por lo cual, los expertos en ciberseguridad advierten de qué manera se exponen los datos personales y cómo se pueden mitigar los riesgos que ello implica.

Sin embargo, no todos corren despavoridos de las redes sociales, puesto que la cantidad de usuarios en las plataformas sigue en aumento. La privacidad de la información seguirá siendo un tema importante en los próximos meses, puesto que aún hay mucho por regular y más por concientizar, sobre todo tomando en cuenta a los usuarios finales que consideran que su privacidad carece de valor, en un mundo donde las ideas de Orwell, Huxley y Bradbury se han vuelto espeluznantemente actuales.

UNAM-CERT

.Seguridad Cultura de prevención para TI, revista bimestral, mayo-junio 2018 / Certificado de Reserva (en trámite), Certificado de Licitud de Título (en trámite), Certificado de Licitud de Contenido (en trámite), Número ISSN (en trámite), Registro de Marca 1298292 | 1298293 / Universidad Nacional Autónoma de México, Circuito Exterior s/n edificio de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Coordinación de Seguridad de la Información, Cd. Universitaria, Coyoacán Ciudad de México, México, C.P. 04510, Teléfono: 56228169

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

DIRECTOR GENERAL
Dr. Felipe Bracho Carpizo

DIRECTOR DE SISTEMAS Y SERVICIOS INSTITUCIONALES
Act. José Fabián Romo Zamudio

COORDINADOR DE SEGURIDAD DE LA INFORMACIÓN/ UNAM-CERT
M. en C. José Roberto Sánchez Soledad

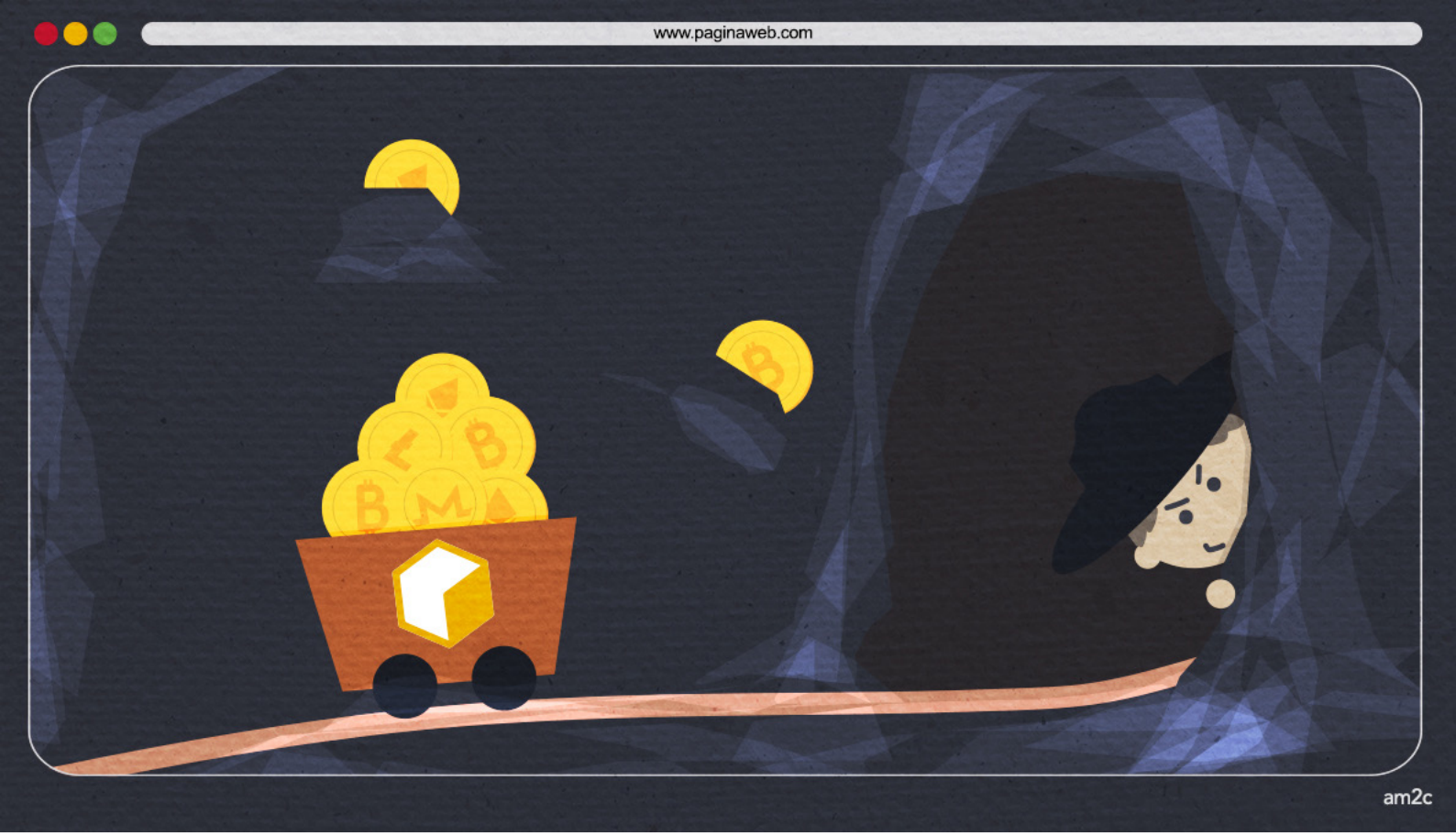
DIRECTORA EDITORIAL
L.A. Célica Martínez Aponte

EDITOR
Raúl Abraham González Ponce

ARTE Y DISEÑO
L.D.C.V. Alicia M. Manjarrez Ceron

REVISIÓN DE CONTENIDO
Demian Roberto García Velázquez
Célica Martínez Aponte
Paulo Santiago de Jesús Contreras Flores
Gonzalo Vázquez Cruz

COLABORADORES EN ESTE NÚMERO
Raúl Abraham González Ponce
Sergio Andrés Becerril
Camilo Gutiérrez Amaya
Miguel Ángel Mendoza
Virgilio Castro Rendón
Sergio Anduin Tovar Balderas



La creación de criptomonedas y la minería no autorizada

Raúl Abraham González Ponce

Desde finales del 2017, diversos analistas de ciberseguridad han advertido sobre el aumento de sitios web que contienen código JavaScript cuyo propósito es usar la capacidad de procesamiento de los visitantes para minar criptomoneda, dada la fiebre generalizada causada por el aumento en el precio de Bitcoin y divisas afines, e incluso a pesar de la depreciación a principios de 2018. ¿A qué se debe este fenómeno? ¿Por qué las criptomonedas han causado semejante furor? ¿Cómo funcionan y por qué los cibercriminales se han volcado hacia esta estrategia para obtener ganancias?

Las monedas virtuales son un sistema descentralizado para el intercambio de valores, esto significa que es posible realizar transacciones directamente con otra persona que acepte este tipo de moneda sin necesidad de un banco. Las personas pueden comprar pizzas (como sucedía cuando apareció por primera vez este sistema) o cualquier otro bien con la moneda virtual.

Este sistema es una especie de libro contable distribuido en una red en el que se lleva el registro de las transacciones realizadas, compartiendo la información de cada transacción entre todas las partes de dicha red. Esta tecnología permite que las transacciones sean transparentes y que sea difícil de alterar el contenido.

Bitcoin fue creada en 2009 por el misterioso alias de Satoshi Nakamoto, que a la fecha sigue siendo desconocido, con la intención de contar con una tecnología que llevara el registro de cómo se gasta cada unidad de moneda y prevenir cambios no autorizados. Un año después, el comercio con Bitcoin comenzó, lo cual otorgó cierto valor a

la moneda virtual. Debido a este valor, los ciberdelincuentes idearon la manera de robar bitcoins, hasta que consumaron el primer gran robo de criptomonedas en 2014, cuando fueron extraídos 850,000 bitcoins de la casa de cambio Mt. Gox (Marr, 2017).

La criptomoneda ha sido utilizada en el mercado negro de la *deep web*, debido a que es un sistema público pero anónimo y facilitaba transacciones de bienes legales e ilegales. Pronto los ataques de ransomware exigieron a los usuarios el pago en bitcoins a cambio de las llaves de cifrado. En mayo de 2017, el los responsables detrás de WannaCry exigían entre $300 y $600 dólares en esta divisa virtual, dependiendo del tiempo de respuesta del afectado. Por estos motivos, algunos relacionaron la moneda con actividades delictivas.

Un Bitcoin en 2010 valía $0.39 centavos de dólar y permaneció con una cotización menor a los diez dólares hasta la segunda mitad del 2012. El valor de la moneda no despegó sino hasta finales del 2013, cuando aumentó un 700%, de $150 dólares a más de mil (Jacobs, 2018), supuestamente con la ayuda de dos bots llamados Markus y Willy, que inflaron el precio de la moneda virtual en transacciones realizadas en la plataforma Mt. Gox. Pero la fiebre del oro virtual se diseminó hasta 2017, cuando el valor del Bitcoin aumentó exponencialmente de mil dólares en enero hasta cerca de $19,000 dólares en diciembre, lo cual llamó la atención de inversionistas que deseaban multiplicar su dinero en un plazo muy corto, aunque las criptomonedas no fueron pensadas como un instrumento de inversión, sino de intercambio.

Con el aumento en la demanda de criptomonedas aumentó su precio. Esto llevó a un escalamiento en la minería, el proceso mediante el cual un nodo o computadora que ejecuta el software de minado de la criptomoneda resuelve problemas matemáticos para crear unidades de dicha moneda.

¿Qué es la minería de criptomoneda?

La tecnología de cadena de bloques o blockchain consiste en un *ledger* o libro contable que lleva registro de las transacciones que se realizan, conocidas como bloques (de ahí el nombre). Cada vez que se realiza una transacción, se distribuye la información a cada una de las computadoras que pertenecen a la red.

Los cambios en el libro contable son cifrados y se notifica a todos los miembros que se ha llevado a cabo la transferencia de una persona a otra para que el propietario de las monedas no las vuelva a usar. De esta manera, nadie puede engañar a todos los nodos, porque la capacidad de procesamiento para hacerlo tendría que superar la capacidad de cómputo de toda la red, algo que solo podría lograr una computadora cuántica (Emerging Technology, 2017). En teoría, es probable que alguien que poseyera 51% de cómputo de la red podría "engañar" a los nodos y beneficiarse.

Los nodos mineros agrupan transacciones en bloques y los añaden a la cadena resolviendo un rompecabezas matemático complejo que es parte del programa de la moneda que atienden, e incluyen la respuesta en el bloque. Este problema consiste en encontrar un número (Number Used Once, mejor conocido como *nonce*, en el caso de Bitcoin es un número entero entre 0 y 4,294,967,296) que, combinado con la información en el bloque y transmitido a través de una función hash, produce un resultado (Acheson, 2018b; Vaidya, 2017).

Para encontrar el nonce, los nodos adivinan al azar el número, puesto que la función hash impide que se pueda predecir. Así, los mineros aplican el hash a la combinación que han adivinado y a la información en el bloque. Puede haber diferentes *nonces* que producen el resultado final. El primer minero que dé con el resultado avisa a todos los nodos de la red, detienen la búsqueda

y pasan a otro bloque. El nodo ganador se queda con una pequeña fracción de la moneda recién creada, conocida como *gas*.

Para Bitcoin, además de la recompensa por resolver el rompecabezas, el minero ganador recibe el total de las comisiones generadas por cada transacción realizada durante el bloque que el minero resuelve.

Existen granjas o *pools* dedicadas a la minería, en las que se dispone de una gran cantidad de nodos formados por procesadores o tarjetas gráficas de video que son muy potentes, gracias a la exigencia de los *gammers* que necesitan procesar información rápidamente para evitar la lentitud en su sesión de World of Warcraft (o cualquier juego de su preferencia).

La demanda de las tarjetas gráficas para minar criptomoneda ha llevado a la escasez, así que quienes tenían pensado comprar una nueva para su centro de juego debían esperar algún tiempo a que fueran resurtidas a las tiendas. El aumento del uso de estas tarjetas para minar criptomonedas y la falta de disponibilidad de estos dispositivos provocó que compañías como Nvidia y AMD decidieran fabricar modelos de GPU (Graphics Processing Unit) específicamente diseñadas para la minería (PortalTIC, 2017).

Como consecuencia del alto precio de las tarjetas y los GPU, el minado de Bitcoin dejó de ser rentable. Además, el costo del consumo de energía es muy alto. A principios de 2018, la compañía de energía HS Orka, en Islandia, advirtió que la minería de Bitcoin en el país podría superar el consumo de todas las casas en la isla, y que de seguir aumentando era probable que no tuvieran suficiente energía para alimentar la minería (Baraniuk, 2018). La población de este país es de 340,000 personas, nada comparado con los 1,379 millones en China, donde se encuentra el 70% de la minería de Bitcoin y por ende las granjas más grandes del mundo, alimentadas por energía barata proveniente del uso de combustibles fósiles y de plantas hidroeléctricas (Willie Tan, 2017).

Criptojacking

En 2014 comenzaron a surgir herramientas para minar Bitcoin dentro de un navegador web para que el visitante dedicara parte de su capacidad de cómputo a resolver el rompecabezas matemático de la minería, pero hacia finales de ese año la técnica dejó de ser usada. Sin embargo en 2017, con la aparición de otras criptomonedas como Monero, Zcash y Ethereum, era posible minar con el equipo casero de un visitante promedio (Pearson, 2017a).

En este ambiente apareció Coinhive, que en septiembre de 2017 lanzó un servicio que permitía minar la criptomoneda Monero. Coinhive es una biblioteca de JavaScript que puede ser añadida a un sitio web con el propósito de no tener que rentar una bodega industrial, ni comprar GPU, ni gastar en energía eléctrica del propio bolsillo para minar. Otras bibliotecas de script realizan la misma función, como JSEcoin y Crypto-Loot.

La idea, si se deja a un lado la malicia, es una estrategia legítima que permitiría sostener un sitio web sin la necesidad de vender espacios publicitarios, una práctica que ayudaría a organizaciones no gubernamentales, instituciones educativas y de otro tipo a no comprometer sus contenidos a la complacencia de un anunciante. Podría otorgar incluso mayor independencia para realizar proyectos que en principio parecerían poco redituables, siempre y cuando los propietarios de estos sitios solicitaran permiso a los visitantes para utilizar su capacidad de cómputo. A principios de 2018, la revista digital salon.com comenzó a pedir a los lectores ayudarlos a minar con su capacidad de procesamiento y así no depender de los anunciantes (Brodkin, 2018; Pearson, 2018).

Sin embargo, esta buena idea pronto fue aprovechada por ciberatacantes que comenzaron a inyectar el JavaScript de minado en sitios de todo tipo. Desde el 2017 se detectó que distintos sitios, como The Pirate Bay, aprovechaban la capacidad de cómputo de sus visitantes para su beneficio, sin que se solicitara permiso a los usuarios.

Pero los delincuentes no se conformaron con usar sus propios sitios para este propósito, sino que comenzaron a inyectar el script en sitios populares para aprovechar el tráfico de internautas. Diversos sitios como Showtime también llegaron a ser atacados con inyección de este código e incluso se detectó que los usuarios de algunas cafeterías de la cadena Starbucks minaban criptomonedas con solo conectarse a la red WiFi gratuita (Pearson, 2017c).

En 2018, Checkpoint advirtió que la amenaza más común en línea era Coinhive, y que los criminales comenzaban a usar este método para obtener ganancias, sobre todo en países en los que el ransomware no tenía mucho éxito debido a que los usuarios no pagaban los rescates (Howell, 2018). Más aún, a principios de febrero, se detectó que más de 4,000 sitios gubernamentales y de organizaciones independientes contenían este tipo de código, incluyendo la página de consulta de cédulas profesionales de la Secretaría de Educación Pública en México (Zorz, 2018; Martínez, 2018). Incluso se encontró script minero en publicidad de Youtube, distribuida por medio de Google Ads (Murphy, 2018).

¿En qué me afecta?

El problema de esta práctica es que el código JavaScript "secuestra" gran parte de la capacidad de cómputo de los usuarios, aprovechando al máximo su procesamiento y consumiendo hasta el máximo de energía que puede utilizar la CPU. Un usuario casero podría creer que no corre más peligro que gastar más en energía eléctrica y ver disminuida la velocidad de su computadora, pero a gran escala podría ser un problema, por ejemplo, cuando la minería afecta a sistemas corporativos. A finales de enero, investigadores de Crowdstrike advirtieron que algunas compañías habían sido afectadas al grado de no poder operar por días e incluso semanas (Zorz, 2018).

También se ha visto que algunos sistemas de control industrial han sido afectados por esta práctica, lo cual representa una amenaza para sistemas críticos, cuya

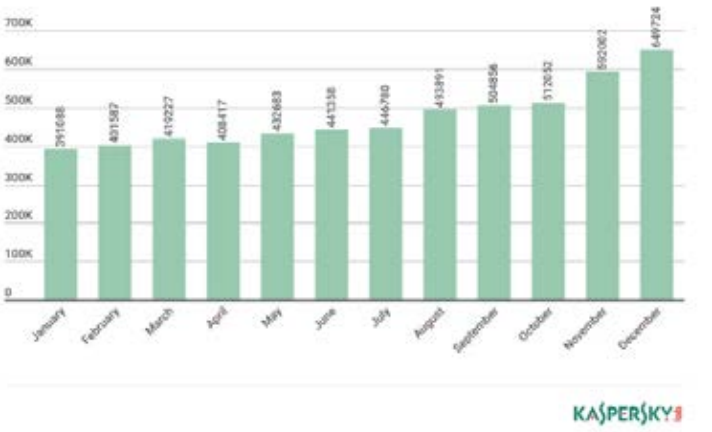
interrupción podrían afectar a la población en general (Zorz, 2018). Este tipo de afectaciones requieren de gran cantidad de procesamiento y ancho de banda de la red, lo cual es una amenaza a la estabilidad y la disponibilidad de los procesos físicos de un operador de infraestructura física, como aseguró Yehonatan Kfir, responsable técnico de sistemas de la compañía de ciberseguridad industrial Radiflow.

Los ciberdelincuentes encuentran una fuente de ingresos más lucrativa en el *criptojacking* en comparación con el ransomware, puesto que en la mayoría de las ocasiones los usuarios no saben que están minando criptomoneda, y es más sencillo que robar monederos de Monero, Zcash o Ethereum. La compañía Cisco Talos estimó que una *botnet* formada por millones de sistemas infectados podrían generar, en teoría, más de cien millones de dólares al año (Muncaster, 2018).

Según Kaspersky Lab, para finales de 2017 se encontraron 2.7 millones de usuarios afectados por mineros maliciosos, esto es 1.5 veces más que en 2016 (Ivanov y Lopatin, 2018).

Al mismo tiempo que el ransomware disminuye, la minería maliciosa parece tener un auge. Cada semana se reporta una nueva estrategia que permite a ciberdelincuentes maximizar sus ganancias. Por

ejemplo, la minería no autorizada echa mano de la ingeniería social para engañar a los usuarios para que instalen alguna aplicación potencialmente indeseada (potentially unwanted application, PUA) que habilita la minería.



Figrua 1. Número de usuarios de Kaspersky Lab atacados por mineros maliciosos en 2017

Otras técnicas utilizan la capacidad de cómputo de servidores poderosos en grandes compañías, como en el caso de Wannamine, que se dispersa en redes usando el exploit EternalBlue, con lo que los ciberdelincuentes generaron hasta dos millones de dólares (ídem). También se han detectado ataques dirigidos en los que se usan una PUA que contiene un instalador de minería por medio de una aplicación legítima, la cual, además, evita que el usuario pueda terminar el proceso.

En fin, los ciberdelincuentes han intentado diversas estrategias para generar ganancias con el mínimo de esfuerzo. Han infectado grandes servidores para minar millones de dólares con malware sofisticado que evita la detección y la desinstalación, han afectado a dispositivos móviles al grado de dejarlos inservibles, y han modificado páginas populares de todo tipo para aprovechar el tráfico en esos sitios. Ante este panorama, es necesario saber cómo enfrentar la amenaza.

¿Cómo protegerse contra el criptojacking?

Un escenario de este tipo nos llevaría a pensar que es fácil terminar en algún sitio que mina criptomoneda sin darnos cuenta. Por ello compartimos algunos consejos para saber si tu computadora o dispositivo móvil están siendo aprovechados por un tercero malicioso.

En primer lugar, puedes sospechar que estás infectado con algún minero si notas una ralentización de tu dispositivo. Los códigos de minería consumen muchos recursos del sistema y pueden incluso disminuir la vida útil de tu computadora o teléfono móvil.

Si notas que la computadora es más lenta de lo común, puedes utilizar el monitor de actividad o monitor de recursos de tu sistema operativo para saber qué programa ocupa demasiada capacidad de procesamiento. Si notas que alguna aplicación gasta muchos recursos del sistema, puedes sospechar de ella. Si no conoces todos los procesos, puedes investigar la función de aquellos que consideres sospechosos.

Es difícil establecer un "comportamiento normal" de un CPU, debido a que cada computadora es dedicada a distintas tareas, pero si cierras todas las aplicaciones y notas que aún se consumen más de 20% de recursos del sistema, puedes sospechar de un minero. Si notas en el monitor de actividad o administrador de tareas que al visitar una página se consumen demasiados recursos, cierra la página en la que te encuentras y verifica si todo regresa a la normalidad.

En el peor de los casos, podrías notar que la actividad de alguna aplicación sigue siendo alto aún después de haber cerrado tu navegador. Si es así, cabe la posibilidad de que hayas sido afectado por algún malware persistente. Si detectas que una aplicación utiliza grandes recursos, termina su ejecución directamente en el monitor de actividad o elimínala con ayuda de una solución antivirus.

Si la actividad de minado ocurre en tu navegador, existe otros métodos de mitigación. En Firefox es posible instalar alguna extensión que bloquee sitios con código JavaScript para minado, como NoScript, el cual también está disponible para la versión Android, además de que protege la navegación en Microsoft Edge, Tor y Safari para dispositivos de escritorio. Otra extensión que puedes instalar en Firefox con funciones similares es Mining Blocker.

Una opción más es usar la versión 50 del navegador Opera, que contiene un bloqueador de minería llamada NoCoin por defecto. También puedes bloquear JavaScript en un sitio que sabes que está minando, configurando los controles de privacidad y contenido en tu navegador.

Para hacer frente a esta epidemia, distintas compañías han tomado cartas en el asunto. Google ha planeado realizar cambios en su navegador Chrome que limitan la disponibilidad de poder de cómputo para ciertos tipos de JavaScript en segundo plano, conocidos como *service workers* (Cimpanu, 2018), una estrategia pensada antes de la epidemia de criptojacking, pero que resulta útil en este caso.

Si accedes a una página y quieres saber si se dedica al minado, puedes usar la herramienta whoismining.org para descubrirlo y después bloquear manualmente la URL, ya sea en el blocker de tu preferencia o directamente en el servidor DNS. También existe un bloqueador de script en GithHub llamado NoCoin (Pearson, 2017a).

Es importante que no bajes la guardia al navegar casualmente por la web, ya que podrías encontrar vínculos que te dirigen a sitios maliciosos para minar criptomoneda. Para ello es necesario mantener una actitud crítica y así no exponerte a los mineros o a cualquier otra amenaza.

Algunas soluciones antivirus ya ofrecen servicios para protegerte, así que toma en cuenta esta amenaza cuando evalúes si el producto que eliges es lo que necesitas.

Referencias

Acheson, N. (2018) How Bitcoin Mining Works. Coindesk. Recuperado el 22 de febrero de 2018, de https://www.coindesk.com/information/how-bitcoin-mining-works/

Ahceson, N. (2018) What Can You Buy with Bitcoin? Coindesk. Recuperado el 22 de febrero de 2018, de https://www.coindesk.com/information/what-can-you-buy-with-bitcoins/

Baraniuk, C. (2018) Bitcoin energy use in Iceland set to overtake homes, says local firm. BBC News. Recuperado el 22 de febrero de 2018, de http://www.bbc.com/news/technology-43030677

Brodkin, J. (2018) Salon to ad blockers: Can we use your browser to mine cryptocurrency? Ars technica. Recuperado el 23 de febrero de 2018, de https://arstechnica.com/information-technology/2018/02/salon-to-ad-blockers-can-we-use-your-browser-to-mine-cryptocurrency/

Cimpanu, C. (2018) Tweak to Chrome Performance Will Indirectly Stifle Cryptojacking Scripts. Recuperado el 23 de febrero de 2018, de https://www.bleepingcomputer.com/news/security/tweak-to-chrome-performance-will-indirectly-stifle-cryptojacking-scripts/

Emerging Technology. (2017) Quantum Computers Pose Imminent Threat to Bitcoin Security. MIT Technology Review. Recuperado el 22 de febrero de 2018, de https://www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security/

Estebeth, E. (2017) 2018: The Year Central Banks Begin Buying Cryptocurrency. Coindesk. Recuperado el 22 de febrero de 2018, de https://www.coindesk.com/2018-year-central-banks-begin-buying-cryptocurrency/

Howell, P. (2018) Coinhive cryptojacker is currently the most prevalent malware online. Cyberscoop. Recuperado el 23 de febrero de 2018, de https://www.cyberscoop.com/coinhive-cryptojacking-cryptocurrency-check-point/

Ivanov, A; Lopatin, E. (2018). Mining is the new black. SecureList. Recueprado el 7 de marzo de 2018, de https://securelist.com/mining-is-the-new-black/84232/

Jacobs, S. (2018) A single trader could have caused the price of bitcoin to rise over 700% in 2013. Business Insider. Recuperado el 22 de febrero de 2018, de http://www.businessinsider.com/one-or-two-traders-may-have-caused-the-price-of-bitcoin-to-rise-700-2018-1

Marr, B. (2017) A Short History Of Bitcoin And Crypto Currency Everyone Should Read. Forbes. Recuperado el 22 de febrero de 2018, de https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#1febe4d13f27

Martínez, L. (2018) La SEP confirma infiltración para minar criptomonedas en sitio web. El Economista. Recuperado el 23 de febrero de 2018, de https://www.eleconomista.com.mx/tecnologia/La-SEP-confirma-infiltracion-para-minar-criptomonedas-en-sitio-web-20180116-0109.html

Muncaster, P. (2018) Cisco: Crypto-Mining Botnets Could Make $100m Annually. Infosecurity. Recuperado el 23 de febrero de 2018, de https://www.infosecurity-magazine.com/news/cisco-cryptomining-botnets-100m/

Murphy, M. (2018) YouTube shuts down hidden cryptojacking adverts. Telegraph. Recuperado el 23 de febrero de 2018, de http://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/

O´Neil, P. (2018) Coinhive cryptojacker is currently the most prevalent malware online. CyberScoop. Recuperado el 13 de febrero de 2017, de https://www.cyberscoop.com/coinhive-cryptojacking-cryptocurrency-check-point/

Pearson, J. (2017)a Symantec: A Cryptocurrency Mining Malware 'Arms Race' Is Looming. Motherboard. Recuperado el 23 de febrero de 2018, de https://motherboard.vice.com/en_us/article/a3ngyz/symantec-a-cryptocurrency-mining-malware-arms-race-is-looming

Pearson, J. (2017)b Mining Cryptocurrency to Pay for Journalism Is Not the Worst Idea I've Ever Heard. Motherboard. Recuperado el 23 de febrero de 2018, de https://motherboard.vice.com/en_us/article/3k7avk/mining-cryptocurrency-to-pay-for-journalism-salon-coinhive-monero-not-the-worst-idea

Pearson, J. (2017)c Starbucks Wi-Fi Hijacked People's Laptops to Mine Cryptocurrency. Motherboard. Recuperado el 23 de febrero de 2018, de https://motherboard.vice.com/en_us/article/gyd5xq/starbucks-wi-fi-hijacked-peoples-laptops-to-mine-cryptocurrency-coinhive

Portaltic. (2017) ¿Qué es la minería de criptomonedas? La moneda digital dispara los precios de las tarjetas gráficas. Portaltic. Recuperado el 22 de febrero de 2018, de http://www.europapress.es/portaltic/sector/noticia-mineria-criptomonedas-moneda-digital-dispara-precios-tarjetas-graficas-20170816085943.html

Tan, W. (2017) Brief Overview of China's Cryptocurrency Mining: Capital, Costs, Earnings. Cointelegraph. Recuperado el 23 de febrero de 2018, de https://cointelegraph.com/news/brief-overview-of-chinas-cryptocurrency-mining-capital-costs-earnings

Vaidya, K. (2017) Decoding the enigma of Bitcoin Mining—Part I : Mechanism. Medium. Recuperado el 22 de febrero de 2018, de https://medium.com/all-things-ledger/decoding-the-enigma-of-bitcoin-mining-f8b2697bc4e2

Zorz, Z. (2017) Third party trackers on web shops can identify users behind Bitcoin transactions. Help Net Security Recuperado el 22 de febrero de 2018, https://www.helpnetsecurity.com/2017/08/21/identify-users-behind-bitcoin-transactions/

Zorz, Z. (2018) Thousands of government, orgs' websites found serving crypto mining script. Help Net Security. Recuperado el 23 de febrero de 2018, de https://www.helpnetsecurity.com/2018/02/12/websites-found-serving-crypto-mining-script/?platform=hootsuite

Si quieres saber más, consulta:

- WannaCry: ataque mundial y consideraciones sobre ciberseguridad
- Consejos para desarrolladores web con enfoque a comercio electrónico
- Mitos y realidades de la Internet profunda

Raúl Abraham González Ponce

Estudió Ciencias de la Comunicación en la Facultad de Ciencias Políticas y Sociales. Es editor desde hace catorce años en las áreas de interés general, literatura y educación. Ha sido editor de varios libros de texto aprobados por la Secretaría de Eduación Pública. Colaboró con artículos de opinión para la revista +Claro y literarios para Playboy. Fue colaborador en la Dirección General de Publicaciones de la UNAM por tres años, dictaminador de nuevos materiales y corrector de estilo en Editorial Patria, Larousse y Norma.

Fue responsable del área de ciencias y ciencias sociales en Oxford University Press México, donde se especializó en la edición de textos educativos científicos. Trabajó para Sistema UNO de Santillana como editor de contenidos. Además colabora con UNAM-CERT para difundir la cultura de la ciberseguridad por medio de redes sociales y a través de la Revista .Seguridad.

Confidencialidad de la información

Sergio Andrés Becerril

El 7 de septiembre se reportó un evento catastrófico para millones de personas del país vecino del Norte. Uno de los principales burós de crédito de los Estados Unidos, Equifax, informó que la información de más de 145 millones de ciudadanos (incluyendo residentes del Reino Unido y Canadá) había sido comprometida en un ataque que, según las últimas investigaciones, duró más de dos meses sin ser detectado y tardó otros dos en ser reportado al público (Gutzmer, 2017). Equifax cometió aún más errores, el más notorio al liberar un sitio donde los consumidores podrían verificar si estaban o no afectados, y entregando información aparentemente aleatoria, generando aún más dudas sobre su sistema de seguridad.

Este ataque es uno de los más notables entre decenas que se han reportado en el año, algunos de los cuales son:

- Un intento de extorsión a Bell Canada que culminó con la filtración de los registros de 1.9 millones de clientes de la compañía (Sharp, 2017).
- Ataques a dos grandes empresas en la industria de la hospitalidad, IHG (administradora de hoteles como Holiday Inn) (IHG, 2017) y Sabre (cuyo SynXis es usado por más de 32,000 hoteles) (Krebs, 2017).

Aunque a primera vista esto se trata de un año más en la seguridad informática, lo interesante es la tendencia al "gran gol-

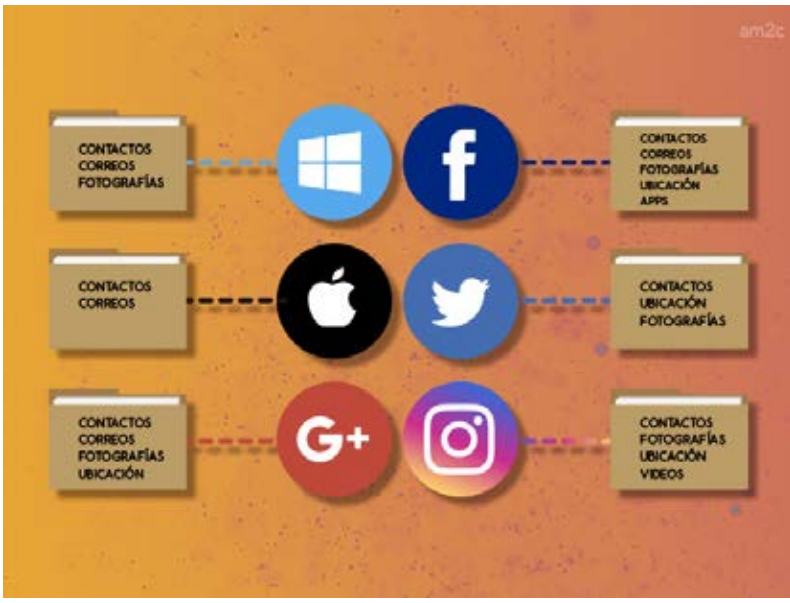
pe" que los atacantes han perseguido. El ISTR de Symantec reporta, en su edición 2017, un promedio de 1314 incidentes de divulgación de información por año en el periodo de 2014-2016 (Symantec, 2017). El número de incidentes que involucran la divulgación de más de 10 millones de identidades va al alza, de 11 en 2014 a 13 en 2015, y a 15 en 2016.

El de Equifax es uno de los más grandes incidentes, no solo por la cantidad de personas afectada (145 millones), sino también por su sensibilidad. Además de información como nombre completo, fecha de cumpleaños y dirección postal, la compañía indica la divulgación de números de Seguridad Social. En el contexto de los Estados Unidos, este número es crítico para la vida de las personas. El SSN (por las siglas en inglés de *Social Security Number*) es utilizado no solo como referencia, sino como un *token* (un secreto que solo el interesado debe conocer) para toda serie de procesos: apertura de créditos bancarios, atención médica, declaraciones de impuestos, incluso el procesamiento de sentencias criminales.

Un atacante que tiene acceso al SSN de una persona (en conjunto con su fecha de nacimiento y su nombre completo) tiene la habilidad de trastornar completamente la vida de esa persona, aprovechando todos los beneficios, financieros y demás, y al mismo tiempo arruinar su historial médico, crediticio y hasta criminal.

Ante estos acontecimientos es importante hacernos la pregunta: ¿podemos aún confiar en nuestro derecho a la privacidad? ¿O, acaso, debemos prepararnos para una vida sin confidencialidad de la información?

Ciertamente la pregunta no es nueva. Llevamos años preguntándonos esto a raíz de la cantidad de información personal y confidencial que confiamos *voluntaria* e *innecesariamente* a múltiples compañías: Google, Facebook y Apple, por mencionar algunas de las más reconocidas. Sin embargo, este es un cuestionamiento más social y cultural: ¿*Debemos* dar esta información? Y otro, uno más práctico: ¿vivimos en una era donde la privacidad, simplemente, ya no existe?



Consideremos la pregunta. Cuando entregamos nuestra información, a través de fotos, chats y videos, a una compañía como Facebook, estamos *eligiendo* entregarla al mundo. Es debatible si estamos debidamente informados del alcance de esta decisión, pero es una decisión. Cuando entregamos nuestra información a una compañía como Equifax (o, en México, al Buró de Crédito), lo hacemos como una obligación inevitable, y cuya alternativa es imposibilitarnos la vida financiera, en el contexto actual. No existe una verdadera elección. Cierto, aceptamos expresamente firmando algún formato, porque la opción es no contar con un instrumento financiero, imprescindible para la mayoría de nosotros. Cuando viajamos al extranjero, los agentes aduanales (de ida y de regreso) registran estos movimientos, preguntan detalles (que son también debidamente registrados) y están, en el caso de países como Estados Unidos, en libertad de revisar nuestro historial financiero, escolar, laboral, y hasta de redes sociales (Harrington, 2017). La opción, por supuesto, es no viajar.

Estos registros, como cualquier información digital, son prácticamente inmortales. En 2015, el Instituto Nacional de Acceso a la Información inició un proceso legal en contra de Google México (aunque es imposible atacar a Google como

empresa internacional, pues cae fuera de la jurisdicción mexicana), debido a que el empresario Carlos Sánchez de la Peña no había podido ejercer su "derecho al olvido", entrecomillado porque esto no existe en la legislación nacional. En esencia, el Sr. Sánchez quería que un reportaje que lo implicaba en presuntos actos de corrupción fuera borrado de los resultados de búsqueda de Google.

Este caso (que acabó perdiendo el INAI y el Sr. Sánchez) es una mera continuación de las demandas que se han presentado por años contra blogs, publicaciones digitales, y cualquier otro sitio web, y sufre del mismo problema: aún ganando la batalla legal, los contenidos son reproducidos en sitios web, bajo diferentes jurisdicciones, dispersándose tan rápido que es imposible detener su difusión, y en la mayoría de los casos, aumentando notablemente la exposición inicial. En el caso del Sr. Sánchez, en vez de suprimir la información, solo logró que más personas conocieran sobre sus presuntos nexos de corrupción. Como lo indica el personaje de Erica Albright en la película de *Red social*, "El Internet no se escribe a lápiz, Mark. Se escribe con tinta."

El problema, entonces, no es nuevo. El registro de actividades es tan viejo como la escritura; la digitalización de registros surge con la creación de medios digitales, y la interconexión de equipos a través de Internet tiene ya más de 30 años. Maleantes han existido desde que existe la humanidad. Entonces, ¿cuál es la diferencia?

La primera y más clara es que el alcance de estos ataques se ha expandido con el tiempo. La consolidación de empresas, y por ende, de información codiciable, la disponibilidad de mayores anchos de banda y espacios de almacenamiento, la anonimidad de transacciones financieras utilizando criptomonedas, y la amplia disponibilidad de *armamento* digital han facilitado una transición al contexto actual (Siegel; Perlroth; 2017).

La segunda es el apreciamiento del valor de la información, dado el beneficio tangible que un atacante puede obtener de una divulgación, además del severo daño que esto causa a la víctima. Una identidad robada puede utilizarse directamente para la obtención de créditos a nombre del afectado, obteniendo cualquier número de beneficios en perjuicio de la víctima; si el atacante no desea correr este riesgo, puede vender el lote de identidades robadas, obteniendo aproximadamente $1 dólar por pieza (Symantec, 2017).

Y si piensas que en México somos ajenos a este tipo de divulgaciones, te informamos que apenas hace dos años se descubrió una base con los datos de los 93.4 millones de votantes registrados ante el INE, en un servidor disponible al público, ubicado en el extranjero (Vickery, 2016).

¿Qué podemos hacer?

Ante este panorama, es pertinente preguntarse qué medidas preventivas se pueden tomar. La solución no es fácil ni rápida. Así como la transición a este contexto ha implicado a múltiples actores en un periodo extendido, también así será la respuesta social ante este cambio.

Podemos mirar el caso de Equifax y aprender de sus resultados. Los millones de afectados están conociendo herramientas que permiten el monitoreo y congelamiento de crédito para hacer frente al robo de su información, y para prevenir algún robo de identidad posterior. Informarse con anticipación de las soluciones proactivas ante alguna divulgación es buena estrategia. En México, en particular, una excelente herramienta son los reportes de crédito gratuitos (uno por año) que ofrece el Buró de Crédito, donde podemos detectar algún crédito que no haya sido solicitado por nosotros, y tomar acción. El encargado de resolver una contratación apócrifa a nuestro nombre, en México, es la Procuraduría Federal del Consumidor. Y una mala nota en el historial crediticio como resultado de un fraude de identidad puede resolverse ante las Sociedades de Información Crediticia (Círculo de Crédito y Buró de Crédito).

En el ámbito organizacional, existen soluciones que se encargan de clasificar y restringir el acceso a la información con base en dicha clasificación. Estas soluciones, conocidas como DLP (*Data Loss Prevention*) son altamente personalizadas a la institución, y suelen estar fundamentadas en la otra mejor alternativa en el ámbito organizacional: políticas de seguridad. Dentro de estas, podemos establecer controles adicionales, aunque una sólida política de clasificación de información y limitación de dispositivos personales (para evitar fugas de información) sigue siendo la mejor estrategia.

Pero, sobre todo, conviene estar consciente de los riesgos que corremos para tomar precauciones: debemos saber quién posee nuestra información, qué datos tiene, y qué podría pasar si son divulgados. Este proceso, mitad investigación y mitad reflexión personal, es la mejor arma con la que contamos actualmente, y podría ser la diferencia entre sufrir una afectación personal o superar el incidente sin problemas, cuando la próxima noticia de un ataque informático llegue a nuestros oídos

Referencias

3D. (2016). Tribunal anula resolución del INAI sobre el falso "derecho al olvido". Recuperado el 1 de febrero de 2018, de https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/

Crowe, J. (2017, 6 de mayo). WannaCry Ransomware Statistics: The Numbers Behind the Outbreak. Recuperado 1 de febrero, 2018, de https://blog.barkly.com/wannacry-ransomware-statistics-2017

Gutzmer, I. (2017, 26 de septiembre). Equifax Announces Cybersecurity Incident Involving Consumer Information. Recuperado el 1 de febrero de 2018, de https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/

Harrington, R. (2017, 13 de septiembre). Federal agents can search your phone at the US border - here's how to protect your personal information. Recuperado el 7 de febrero de 2018, de http://www.businessinsider.com/can-us-border-agents-search-your-phone-at-the-airport-2017-2

IHG InterContinental Hotels Group. (2017, 3 de febrero). IHG® Notifies Guests of Payment Card Incident at 12 Properties in the Americas. Recuperado 1 de febrero, 2018, de https://www.prnewswire.com/news-releases/ihg-notifies-guests-of-payment-card-incident-at-12-properties-in-the-americas-300401996.html

Krebs, B. (2017, 2 de mayo). Breach at Sabre Corp.'s Hospitality Unit. Recuperado 1 de febrero, 2018, de https://krebsonsecurity.com/2017/05/breach-at-sabre-corp-s-hospitality-unit/

Sharp, A. (2017, 17 de mayo). Canada's Bell says it ignored hackers payment demands, some info leake. Recuperado 1 de febrero, 2018, de https://ca.reuters.com/article/domesticNews/idCAKCN18C1PX-OCADN.

Siegel, R., & Perlroth, N. (2017, 29 de junio). Shadow Brokers Group Leaks Stolen National Security Agency Hacking Tools. Recuperado 1 de febrero, 2018, de https://www.npr.org/2017/06/29/534916031/shadow-brokers-group-leaks-stolen-national-security-agency-hacking-tools. En agosto de 2016 un grupo puso a la venta herramientas de la NSA (National Security Agency de los Estados Unidos) para vulnerar y tomar control de equipos de cómputo.

Symantec. (2017) 2017 Internet Security Threat Report. Recuperado el 1 de febrero de 2017, de https://www.symantec.com/security-center/threat-report

Vickery, C. (2016, 22 de abril). BREAKING: Massive Breach of Mexican Voter Data. Recuperado 1 de febrero, 2018, de https://mackeeper.com/blog/post/217-breaking-massive-data-breach-of-mexican-voter-data

Si quieres saber más, consulta:

- ¿Quién te conoce?
- Sanitización de información
- DLP: tecnologías para la prevención de la fuga de información

Sergio Andrés Becerril

Es Ingeniero en computación, egresado de Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM).

Colaboró en Subdirección de Seguridad de la Información /UNAM-CERT desde el 2009 al 2012, en las áreas de detección de intrusos y el Proyecto Honeynet UNAM, el equipo de respuesta y atención a incidentes, y análisis de malware, y continúa colaborando en diversas conferencias, cursos y publicaciones.

Actualmente dirige una consultoría privada de seguridad informática y es responsable de la administración de los servidores y seguridad informática de la Escuela Nacional de Lenguas, Lingüística y Traducción (ENALLT) de la UNAM.

Tendencias 2018: el costo de nuestro mundo conectado

Camilo Gutiérrez Amaya
Miguel Ángel Mendoza

Después de los eventos relevantes de seguridad ocurridos durante 2017, son cada vez más las empresas y usuarios que se preocupan por mantener mayores niveles de protección para su información. Por ello, es recurrente escuchar la pregunta ¿qué puedo esperar en materia de ciberseguridad en estos próximos meses?

Así que sin jugar a ser adivinos ni pecar de futurólogos, vamos a responder la pregunta basados en los sucesos observados durante el año pasado y analizando el panorama de tendencias que plantea este 2018. A continuación, abordamos los aspectos en los que la seguridad de la información estará involucrada con un papel preponderante.

Privacidad e información

El derecho a la privacidad surgió con la inquietud por preservar la intimidad de las personas y la conciencia por otorgarles esa facultad. Aunque la idea de privacidad cambia con el tiempo, este derecho puede definirse como aquel que los individuos poseen para separar aspectos de su vida íntima del escrutinio público, por lo que, sin distinción todos tenemos derecho a ella. La privacidad encuentra condiciones complejas en la era digital, ya que la tecnología aparece antes de que existan legislaciones que puedan otorgar este derecho, aunado a las prácticas que como usuarios llevamos a cabo.

El paradigma de privacidad se modifica con las generaciones, las costumbres y la tecnología misma; tal como sucede con el uso de las redes sociales, incluso con prácticas de algunos fabricantes. Por ejemplo, el caso donde se lleva a cabo la monetización de la información de los usuarios, a cambio de un software de seguridad gratuito; sin duda este tipo de situaciones seguirán presentes durante este año. Aunado a lo anterior, se añade el riesgo de la recolección de datos que realizan los dispositivos del Internet de las cosas (IoT) y la escasa seguridad asociada.

La recolección de toda esta información podría contar una historia sobre cada usuario, y sumado al Aprendizaje Automático (Machine Learning) y la Inteligencia Artificial, también podría ser utilizada para influir sobre acciones y pensamientos. Por ello, la privacidad y el control sobre su información deberían ser de interés para los usuarios, sobre todo por lo que realmente podrían representar los productos y servicios que se ostentan como "gratuitos" y la manera en la que se utiliza sus datos.

Más allá de que confiamos en que los usuarios adquieran cada vez más conciencia en esta materia, también creemos que la cantidad de información que se recolectará será aún mayor. Por lo tanto, la cuestión no se enfoca en desterrar estas prácticas, pero sí en tomar decisiones conscientes y con la información suficiente para que la privacidad de cada persona pueda ser respetada.

Por otra parte, hay que considerar que durante este año entra en vigor el reglamento GDPR sobre la privacidad de datos, lo cual también alcanza a empresas de Latinoamérica que tienen alguna relación con empresas o clientes en la Unión Europea. Esto trae retos adicionales a las organizaciones para dar cumplimiento a las legislaciones y operar de manera adecuada para otorgar a sus clientes los derechos establecidos en los nuevos decretos.

Retos en seguridad informática para procesos electorales

La ciberseguridad también se encuentra involucrada en otros aspectos, tal como los procesos electorales, de distintas maneras. Por ejemplo, en el curso de las campañas políticas que pueden ser alteradas mediante "estrategias alternativas" y el uso de herramientas ilegítimas como el malware, bots o ciberespionaje. La afectación de los procesos mediante este tipo de herramientas adquiere más relevancia si consideramos que esto puede determinar el presente y futuro de una nación, y en consecuencia de los ciudadanos. Por ello, la seguridad en el ámbito electoral se convierte en un factor crítico antes, durante y después de los comicios.

Este 2018 es un año de elecciones en algunos países de la región como México, Brasil y Colombia, donde se recurre cada vez más a herramientas digitales para apoyar las elecciones, pero del mismo modo, éstas pueden ser utilizadas con otros fines. Por ejemplo, el manejo de información falsa alrededor de las campañas electorales para desprestigiar partidos políticos o candidatos, lo que se traduce en un reto importante para garantizar la objetividad durante las elecciones. El impacto de las redes sociales permite llegar a mucha gente en poco tiempo, lo que también abre la posibilidad para la manipulación de la información; pareciera que la expresión popular termina siendo la manifestación de un grupo de atacantes, que pueden sesgar la opinión pública.

Por otro lado, en los países donde se ha optado por la aplicación del voto electrónico, en busca de acabar con fraudes electorales, regularizar y acelerar el conteo, así como complementar los registros en papel, se han comenzado a presentar inconvenientes con esta tecnología. El problema se presenta cuando los métodos de

conteo no se complementan, sino que son reemplazados completamente. Hasta este momento, el modelo ha agregado nuevos puntos de falla, sin eliminar los riesgos.

Así como distintos actores han encontrado la forma de obtener triunfos de manera fraudulenta a lo largo de los años, explotando el sistema electoral físico, atacantes podrían encontrar la forma de explotar el sistema digital, sobre todo si cuentan con los recursos y algún tipo de patrocinio. Por todo lo anterior, la seguridad de la información juega un papel relevante en este tipo de jornadas, en donde su propósito primordial es contribuir a la generación de procesos electorales confiables y transparentes, que independientemente de los resultados, puedan disipar cualquier duda sobre la manera en la que se llevan a cabo los comicios, al menos, desde el aspecto tecnológico.

La revolución del ransomware

No podíamos dejar de mencionar una de las amenazas que más titulares de prensa acaparó durante el año pasado. Si bien no es el tipo de malware que afecte a la mayor cantidad de usuarios, por sus características es uno de los que más preocupación causa. Durante este año es poco probable que el ransomware retroceda en la cantidad de equipos infectados, y, por el contrario, veremos cómo los atacantes siguen usando esta amenaza para obtener algún tipo de ganancia económica.

Con respecto a los ataques a teléfonos inteligentes y otros dispositivos, vemos que este tipo de amenazas tienden a enfocarse menos en los datos y más en impedirle a la víctima el uso de su dispositivo y los servicios que facilita. Esto es un verdadero problema cuando la alternativa de pagar un rescate involucra la pérdida de configuraciones y otros datos, especialmente a medida que son más las personas que usan los dispositivos móviles en lugar de las computadoras personales o incluso las portátiles, de modo que la gama de recursos que podría verse amenazada es más amplia.

Si a lo anterior sumamos el crecimiento de la superficie de ataque debido a los dispositivos IoT y los sensores integrados en elementos cotidianos, como routers, refrigeradores, medidores inteligentes, televisores, juguetes o marcapasos; y en contextos antes inesperados, como centrales eléctricas, estaciones de servicio u hoteles, hay una mayor susceptibilidad a verse afectados por el malware (más allá de que aplique el secuestro de la información o del dispositivo mismo, y se exija un rescate).

Amenazas al Internet de las Cosas y dispositivos conectados

Hablar del IoT como una tendencia no es preciso, porque hoy en día este tipo de dispositivos ya forman parte de nuestra cotidianidad. Por lo tanto, el incremento en el uso de estos dispositivos en prácticamente todos los aspectos de nuestras vidas, sumado a la falta de enfoque en la seguridad por parte de algunos fabricantes, se abre la posibilidad para que, desde los sistemas operativos, las aplicaciones y las comunicaciones se identifiquen riesgos de seguridad que extienden la superficie de ataque por parte de los atacantes.

Prácticas deficientes de seguridad, como mantener usuarios y las contraseñas preestablecidas, tener habilitados puertos y servicios que no son utilizados, y en general configuraciones por defecto, han permitido que distintos ataques informáticos exploten estas vulnerabilidades en los equipos de usuarios.

Todo esto debe reflejar la necesidad de contar con la educación por parte de los usuarios para manejar la tecnología con mayor responsabilidad y la importancia de que los fabricantes mejoren sus diseños pensándolos desde la seguridad. En un ambiente de hiperconectividad, donde las personas se mantienen conectadas a Internet por periodos prolongados y desde distintos dispositivos, la seguridad mantiene un papel relevante.

Amenazas de alcance Mundial

En 2018 se juega el Mundial de Fútbol en Rusia y es una excusa perfecta para organizar todo tipo de estafas alrededor de este evento. Algo que ocurre con frecuencia es la aparición de distintas amenazas que emplean una temática en boga, para intentar engañar a los usuarios, tal como un suceso de la magnitud de un evento deportivo global.

Entre el abanico de trampas se identifican desde la venta de entradas falsas a partidos, hasta noticias inventadas o enlaces para, supuestamente, ver los partidos en línea y que en realidad son una puerta de entrada para los códigos maliciosos u otras amenazas. También se identifican estafas dirigidas a capturar información personal o dinero de los usuarios, mediante sitios apócrifos.

Por todo lo anterior, resulta necesario estar alerta a este tipo de amenazas, ya que un acontecimiento esperado con ansias y que ocurre cada cuatro años, podría convertirse en una amarga experiencia si no se toman las precauciones debidas.

Criptomonedas

La adopción del Bitcoin como una moneda para el intercambio de bienes y servicios abrió el camino para la aparición de otras criptomonedas, llegando a tener un crecimiento exponencial en su uso en los últimos meses. Toda la atención que ha ganado por parte de los usuarios se traduce en que los cibercriminales ya lo han tomado como un mercado que buscarán explotar.

Desde amenazas que tratan de robar billeteras virtuales hasta los ataques a servidores que alojen esta información, códigos maliciosos que usen la capacidad de cómputo de los usuarios para minar criptomonedas, así como la modificación de sitios Web para este mismo propósito, son algunas de las amenazas que estaremos viendo en esta materia durante el año.

La fiebre por la minería de criptomonedas desatará un sinnúmero de amenazas orientadas a esta actividad, intentando aprovecharse de los recursos de procesamiento de los usuarios, claro está, sin su consentimiento. Por esta razón, es necesario protegerse y estar alerta sobre campañas maliciosas orientadas al uso ilegítimo de los equipos para minar alguna moneda digital.

Infraestructuras críticas

En enero de 2017 las amenazas a infraestructuras críticas fueron noticia cuando un informe de Reuters aseguró que el corte de energía eléctrica en Ucrania "fue un ataque cibernético". Un año antes, un ataque de DDoS contra el servicio de DynDNS, causó una interrupción de Internet en varios países de la región.

Por lo tanto, es muy probable que 2018 no sea la excepción, y veamos como algo cotidiano la presentación de noticias sobre ataques a la infraestructura crítica de los países de la región. Cabe señalar que lo que se define como infraestructura crítica puede abarcar desde la red eléctrica, hasta sectores de defensa y salud, procesos de fabricación cruciales, producción de alimentos, agua o transporte, sin limitarse a ello.

Las debilidades se identifican debido a que muchas de estas redes se diseñaron y desarrollaron antes de que los ataques cibercriminales llegaran a tomar la importancia de hoy en día y por lo tanto no están preparados ni pensados para estas amenazas, y en muchas ocasiones tampoco se diseñaron con mecanismos de protección para ataques informáticos.

¿Qué nos depara el futuro?

"No hagas predicciones sobre la informática que se puedan verificar durante tu vida"; sabias palabras de Daniel Delbert McCracken. Sin embargo, vale la pena arriesgarnos a hacer una extrapolación de lo que podemos ver durante este año en materia de ciberseguridad.

Si como usuarios no somos conscientes de cuáles son las amenazas y los riesgos que podrían afectar nuestra seguridad, será mucho más sencillo para un atacante comprometer la seguridad de nuestros dispositivos personales, en cualquier lugar y en cualquier momento, desde nuestros lugares de trabajo hasta el hogar.

Así que este panorama de seguridad más allá de ponernos paranoicos y generar preocupación, tiene como propósito crear conciencia y que los usuarios comencemos a ocuparnos de la seguridad de nuestra información en distintos ámbitos, considerando las amenazas futuras que se presentan como una tendencia, para prevenir sus consecuencias y seguir disfrutando de la tecnología en un ambiente cada vez más seguro.

Referencias

Laboratorio de Investigación ESET (2018). "Tendencias en ciberseguridad 2018. El costo de nuestro mundo conectado". Recuperado el 24 de agosto de 2017, de https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf

Si quieres saber más, consulta:

- Ransomware, ¿quién secuestra nuestra información?
- Torrents: compartiendo información legítima y también amenazas
- Conpot: honeypot de sistemas de control industrial

Camilo Gutiérrez Amaya

Se desempeña actualmente como Head of Awareness & Research, liderando el equipo de investigadores de ESET Latinoamérica. Es Ingeniero Electrónico egresado de la Universidad de Antioquia e Ingeniero Administrador graduado de la Universidad Nacional de Colombia.

Cuenta con una especialización en Sistemas de la Información en la Universidad EAFIT y actualmente opta al título de Magister en Data Mining en la Universidad de Buenos Aires, Argentina.

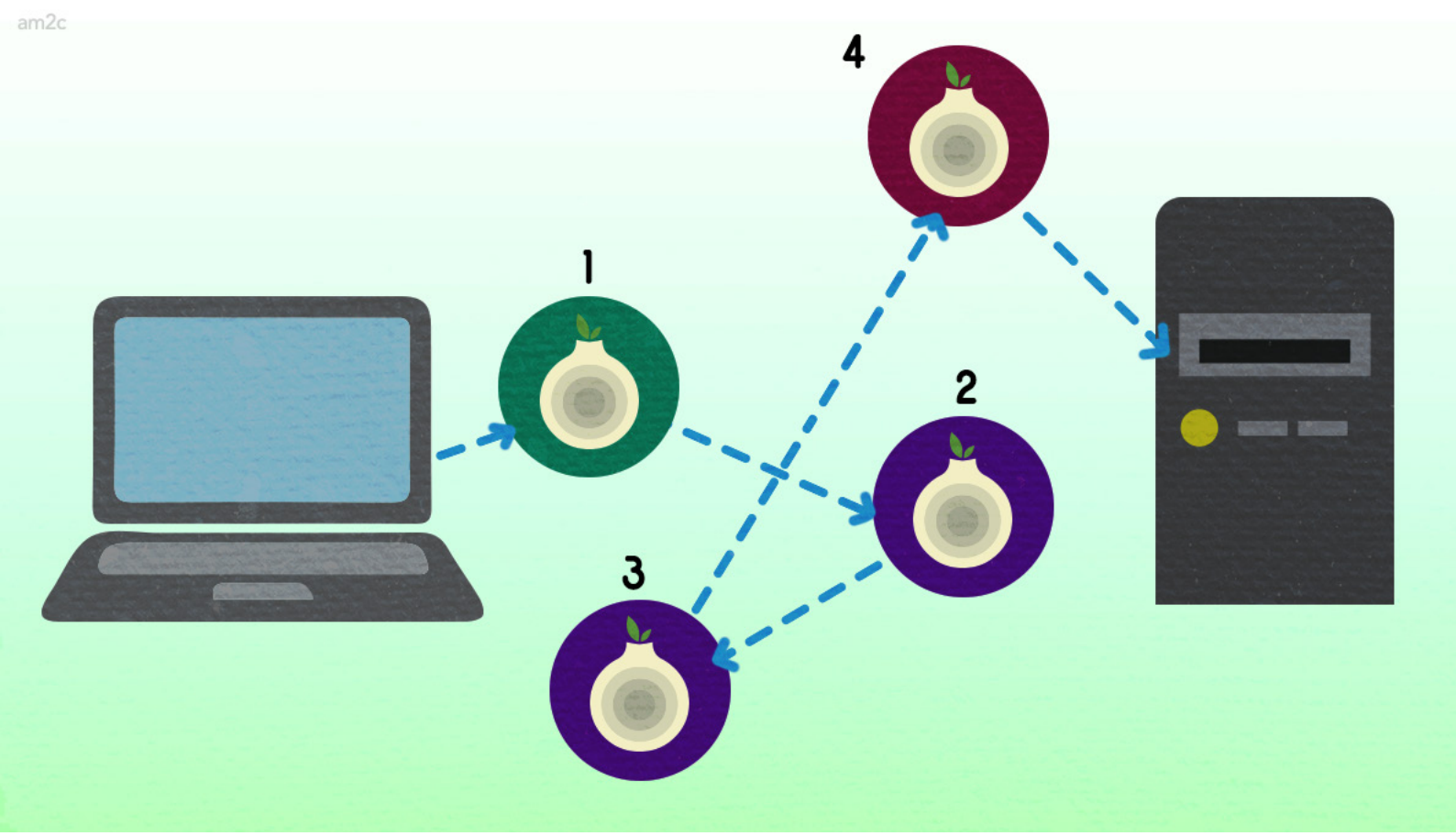
Anteriormente se desempeñó como Coordinador de Riesgo Operativo para una importante compañía de financiamiento y se ha desarrollado modelando y generando sistemas de información.

Miguel Ángel Mendoza

Ingeniero en Computación por la Facultad de Ingeniería de la UNAM, Miguel Ángel Mendoza se desempeña actualmente como Security Researcher en ESET Latinoaméri-

ca, compañía dedicada al desarrollo, investigación y comercialización de soluciones de protección antivirus y seguridad informática. Además es vocero de ESET Latinoamérica y representa a la empresa en todo tipo de actividades tales como seminarios, conferencias, capacitaciones internas y otros eventos de exposición pública.

Colaboró en la DGCCH de la UNAM, en la Facultad de Ingeniería y formó parte de la Coordinación de Seguridad de la Información/UNAM-CERT en el área de Auditoría y Nuevas Tecnologías, donde desarrolló actividades de implementación de estándares, mejores prácticas y auditorías de seguridad informática.



Mitos y realidades de la red Tor: Análisis de tráfico en un nodo de salida

Artículo ganador del Premio Universitario ESET edición 2017

Virgilio Castro Rendón

Resumen

Muchos utilizan la red Tor para sentirse más seguros en Internet, pues evita que los hackers y los gobiernos espíen en las comunicaciones privadas. ¿No es así? Esta investigación tratará de resolver esta pregunta, mostrando cómo es posible obtener información personal de Tor al montar y analizar un relay de salida. Durante el proceso, mostraré también cuán difícil es ayudar al proyecto Tor y para qué se usa habitualmente la red.

Objetivo

Analizar tráfico que viaja a través de la red Tor mediante la implementación de un nodo de salida y captura de tráfico y, en el proceso, mostrar a los lectores y usuarios novatos de dicha red para qué es usada, desmentir algunos mitos sobre

la red y buscar actividad maliciosa dentro de ella. En general se pretende responder a las preguntas: ¿es la red Tor sinónimo de privacidad?, ¿es la red Tor usada exclusivamente para entrar en la "dark net"? y ¿es difícil contribuir al proyecto Tor?".

Antecedentes

¿Qué es Tor?
La red Tor es un grupo de servidores administrados por voluntarios que ayuda a las personas a mejorar su privacidad y seguridad en la red.[1] Los usuarios de Tor utilizan esta red como una serie de túneles virtuales en lugar de hacer una conexión directa entre un cliente y un servidor, por lo que permite a organizaciones e individuos compartir información en redes públicas sin comprometer su privacidad. Al usar Tor, los sitios no pueden rastrear a sus usuarios, pues realmente verían en sus registros las direcciones IP correspondientes a un nodo Tor. Asimismo, Tor cifra todos los datos enviados a través de la red.

¿Quién utiliza Tor?
Tor es utilizada por periodistas, denunciantes y disidentes para que no se les pueda rastrear.[1] Asimismo es utilizada por personas en países que tienen bloqueos regionales a Internet y, de esta manera, evitar dicho bloqueo. Igualmente es usado por personas que quieren hacer uso de los "servicios cebolla" y, en general, por cualquiera que quiere mantener su privacidad.

¿Qué es un nodo Tor?
Un nodo Tor es un servidor que ayuda a la red Tor a proveer ancho de banda. Los nodos son los que forman los túneles virtuales que evitan las conexiones directas entre un cliente y un servidor. La conexión entre el cliente y la red Tor, así como todas las conexiones entre los diferentes nodos, van cifradas, por lo que no se puede analizar el tráfico en esos puntos. Un nodo puede ser usado para, simplemente, reenviar el tráfico al siguiente nodo en la conexión o, también, como un nodo de salida.

¿Qué es un nodo de salida?
Es el último nodo o servidor en el túnel virtual, por lo tanto es el que establece la comunicación directamente con los servidores finales (Por ejemplo: google.com). Este servidor se encarga de descifrar los datos que viajaron cifrados en todo el trayecto, pues tiene que ser así para que el sitio destino original sea capaz de entender la información. Es la dirección IP de este último nodo la que realmente aparecerá en los registros de los sitios visitados.

¿Qué son los servicios cebolla?
También conocidos como "hidden services" u "onion services", representan lo que comúnmente se conoce como "Dark Net" pues no pueden ser accedidos de forma convencional y se requiere de una conexión a través de Tor. Son sitios alojados en nodos Tor (por ejemplo: https://facebookcorewwwi.onion), esto implica que no es necesario salir de la red Tor para visitarlos y, por lo tanto, el tráfico entre el cliente y el servidor siempre se encuentra cifrado. Debido a esta cualidad, los servicios cebolla no son vulnerables a ser analizados en un nodo de salida y, por lo tanto, salen del alcance de este trabajo.

Preparación del ambiente

En esta sección se explica detalladamente todo lo que se hizo para poner en marcha un nodo de salida en la red Tor.[2]

El primer paso fue adquirir un servidor con una dirección IP pública, por lo que se rentó un servidor virtual. Es común que los proveedores de servidores virtuales tengan prohibido explícitamente en sus políticas el instalar y configurar un nodo de Tor. Esto se debe a que es común que la red sea utilizada por atacantes para cubrir su localización, lo que implica que todas las quejas llegarán directamente al proveedor, por lo que prefieren prohibir este tipo de aplicaciones.

Por lo tanto se investigó sobre algún proveedor que no prohibiera esto. Finalmente se decidió rentar con una empresa que promete ancho de banda ilimitado (carac-

terística especialmente útil para este trabajo) y no prohíbe explícitamente el levantar un nodo Tor.

Una vez teniendo acceso al servidor, puesto que se trata de un servidor público y queda expuesto a amenazas, se llevaron a cabo tareas básicas de configuración y seguridad.

- Se instaló y configuró en un sistema operativo Debian 9.

```
[redacted]@server:~$ cat /etc/*release
PRETTY_NAME="Debian GNU/Linux 9 (stretch)"
NAME="Debian GNU/Linux"
VERSION_ID="9"
VERSION="9 (stretch)"
ID=debian
```

Figrua 1. Versión del sistema operativo

- Se hizo una actualización de los paquetes.

```
[redacted]@server:~$ sudo apt-get update
Hit:1 http://security.debian.org/debian-security stretch/updates InRelease
Ign:2 http://ftp.de.debian.org/debian stretch InRelease
Hit:3 http://ftp.de.debian.org/debian stretch-updates InRelease
Hit:4 http://ftp.de.debian.org/debian stretch Release
Reading package lists... Done
```

Figrua 2. Actualización de los paquetes que se pueden instalar en el servidor

- Se instaló y usó chkrootkit para determinar si en el sistema estaba instalado algún rootkit por defecto. Al no encontrar ninguna amenaza de este estilo, se continúa normalmente con las configuraciones.

```
[redacted]@server:~$ sudo chkrootkit
ROOTDIR is `/'
Checking `amd'...                                           not found
Checking `basename'...                                      not infected
Checking `biff'...                                          not found
Checking `chfn'...                                          not infected
Checking `chsh'...                                          not infected
Checking `cron'...                                          not infected
Checking `crontab'...                                       not infected
```

Figrua 3. Ejecución de chkrootkit

- Se instalaron y configuraron las actualizaciones automáticas de paquetes para mantener el sistema con las últimas actualizaciones de seguridad todo el tiempo.

```
[redacted]@server:~$ sudo apt-get install unattended-upgrades apt-listchanges -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
apt-listchanges is already the newest version (3.10).
unattended-upgrades is already the newest version (0.93.1+nmu1).
```

Figrua 4. Instalación de actualizaciones automáticas

Figrua 5. Configuración de actualizaciones automáticas

- Se configuró SSH para no permitir conexiones al usuario *root*.

```
[redacted]@server:~$ sudo grep Root /etc/ssh/sshd_config
PermitRootLogin no
# the setting of "PermitRootLogin without-password".
```

Figrua 6. Usuario root no permitido

- Se instaló el programa `tor` mediante paquetes.

```
[redacted]@server:~$ sudo apt-get install tor
Reading package lists... Done
Building dependency tree
Reading state information... Done
tor is already the newest version (0.2.9.12-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figrua 7. Instalación de `tor`

- Se configuró Tor para funcionar como un nodo de salida. Esto se logra agregando la directiva "ORPort" en el archivo de configuración de Tor (/etc/tor/torrc). El ancho de banda elegido fue de 2 MB, suficiente para ser aceptado como nodo de salida. Asimismo, se estableció una política reducida que se obtuvo a partir de las políticas propuestas en la página oficial.[3] Solo se agregaron los puertos que comúnmente utilizan los chats IRC.

```
[redacted]@server:~$ sudo tail -n 35 /etc/tor/torrc
DataDirectory /var/lib/tor
ORPort 9001
Address [redacted]
OutboundBindAddress [redacted]
Nickname [redacted]
RelayBandwidthRate 2 MB
RelayBandwidthBurst 2 MB
ContactInfo [redacted]
DirPort 80
DirPortFrontPage /etc/tor/tor-exit-notice.html
ExitPolicy accept *:20-21     # FTP
ExitPolicy accept *:43        # WHOIS
ExitPolicy accept *:53        # DNS
ExitPolicy accept *:80        # HTTP
ExitPolicy accept *:110       # POP3
ExitPolicy accept *:143       # IMAP
ExitPolicy accept *:220       # IMAP3
ExitPolicy accept *:443       # HTTPS
ExitPolicy accept *:873       # rsync
ExitPolicy accept *:989-990   # FTPS
ExitPolicy accept *:991       # NAS Usenet
ExitPolicy accept *:992       # TELNETS
ExitPolicy accept *:993       # IMAPS
ExitPolicy accept *:995       # POP3S
ExitPolicy accept *:1194      # OpenVPN
ExitPolicy accept *:1293      # IPSec
ExitPolicy accept *:3690      # SVN Subversion
ExitPolicy accept *:4321      # RWHOIS
ExitPolicy accept *:6666-6668     # IRC
ExitPolicy accept *:5222-5223 # XMPP, XMPP SSL
ExitPolicy accept *:5228      # Android Market
ExitPolicy accept *:9418      # git
ExitPolicy accept *:11371     # OpenPGP hkp
ExitPolicy accept *:64738     # Mumble
ExitPolicy reject *:*
```

Figrua 8. Configuración de `tor`

- Una vez definidos los puertos permitidos, se aplicaron las correspondientes reglas en el firewall del servidor para permitir esas comunicaciones.

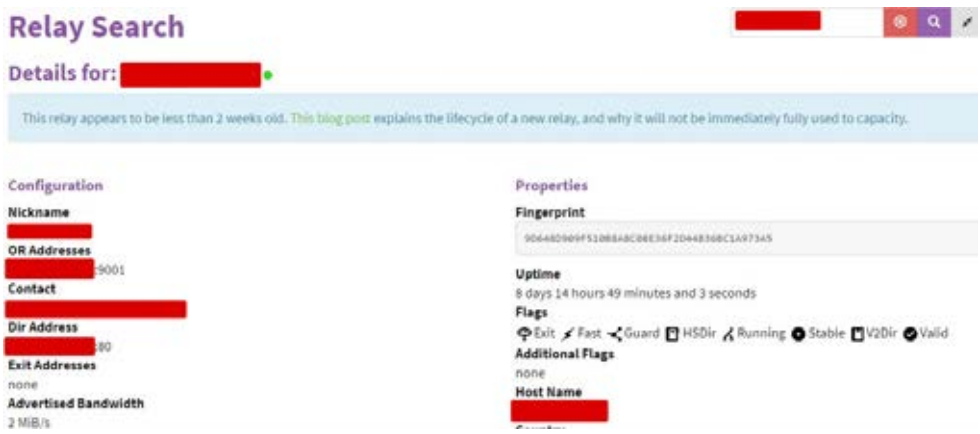
```
Chain Allow (2 references)
target     prot opt source               destination
Friend     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp any limit: avg 1/sec burst 5
DROP       icmp --  anywhere             anywhere             icmp any
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp-data
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:whois
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http-alt
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:pop3
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:imap2
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:220
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:rsync
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftps-data
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftps
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:991
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:telnets
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:imaps
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:pop3s
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:openvpn
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:1293
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:svn
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:4321
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:xmpp-client
```

Figrua 9. Reglas activas en el firewall

- Puesto que es común que los atacantes usen Tor para protegerse, se agregó una página explicativa en el servidor web sobre el funcionamiento de la red y el papel del servidor en ella. Esto debido a que se ha demostrado que, al estar enteradas las víctimas de que se trata de un nodo de salida Tor, las denuncias se reducen considerablemente. Dentro de la página se incluyó mi correo electrónico para recibir los correos de "abuse" y poderles dar una respuesta oportuna.

Figrua 10. Servicio web con descripción del nodo

- Una vez teniendo listo todo lo anterior, solo fue cuestión de tiempo para que la red nos aceptara como un nodo de salida. Automáticamente se hacen pruebas para ver si el nodo no está redirigiendo tráfico a otros sitios o cambiando las consultas DNS y si tiene ancho de banda suficiente, entre otras pruebas.
- Se puede revisar fácilmente si está aceptado como un nodo de salida en la página de búsquedas[4] de Tor, pues muestra todas las características del nodo, incluida la bandera "exit" en caso de ser aceptado como un nodo de salida.



Figrua 11. Descripción del nodo en la página oficial

- A continuación se muestra el comando utilizado para hacer la captura de tráfico. Se decidió hacer un archivo nuevo cada hora, con el fin de evitar que tuvieran tamaños excesivos. Asimismo, solo se captura lo que sale de nuestra dirección IP y se excluye nuestra conexión por SSH.

```
[redacted]@server:~$ cat capture_traffic.sh
#!/bin/bash
/usr/sbin/tcpdump -i ens18 -w /home/[redacted]/traffic/dump_%Y-%m-%d_%H:%M:%S.pcap -G 3600 -W 1 'src [redacted] and not (src port 22)'
```

Figrua 12. Comando para capturar tráfico

- Se creó una nueva tarea en `cron` para ejecutar el script de la figura 12 cada hora.

```
[redacted]@server:~$ sudo crontab -l
# m h  dom mon dow   command
#0 * * * *  /bin/bash /home/[redacted]/capture_traffic.sh
```

Figrua 13. Tarea programada para capturar tráfico

Análisis de hosts conectados

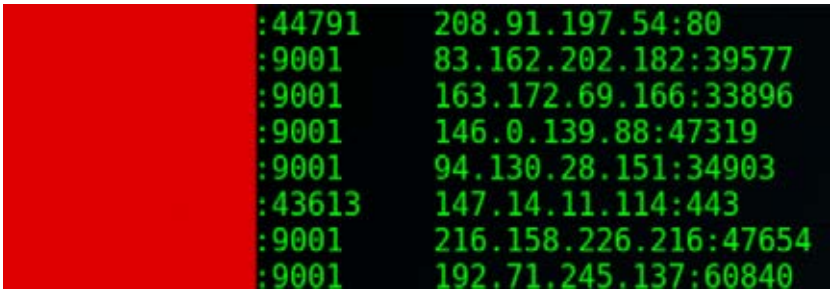
El objetivo de este análisis es obtener información de primera mano de los *hosts* con los que se está comunicando el servidor. La información de los hosts fácilmente se obtiene con el comando `netstat` y se puede hacer un filtro de las direcciones IP correspondientes a otro nodo Tor y un servidor común y corriente.

Como se determinó en el archivo de configuración de Tor, el puerto 9001 se usa para las comunicaciones con otros servidores Tor. Por lo tanto, cualquier conexión que inicie con un puerto diferente corresponde a una conexión establecida con un servidor común. Como se puede ver en la figura 14, existen más de 4,300 conexiones simultáneas.

```
4306 tcp        0      0 [redacted]:9001         91.8.18.235:55376         ESTABLISHED
4307 tcp        0      0 [redacted]:44607        95.213.209.60:80          TIME_WAIT
4308 tcp        0      0 [redacted]:9001         195.154.242.122:47602     ESTABLISHED
4309 tcp        0      0 [redacted]:9001         178.255.42.86:40110       ESTABLISHED
4310 tcp        0      0 [redacted]:9001         91.8.18.235:55376         ESTABLISHED
4311 tcp        0      0 [redacted]:9001         178.255.42.86:40110       ESTABLISHED
4312 tcp        0      0 [redacted]:9001         91.8.18.235:55376         ESTABLISHED
```

Figrua 14. Salida de netstat que muestra conexiones

Al ejecutar el comando `awk '{print $4 "\t"$5}' netstat.txt` se pueden filtrar los datos del archivo para obtener únicamente las direcciones IP y puertos de los hosts.



Figrua 15. Hosts conectados

Teniendo la información anterior, se puede crear un script como el siguiente para escribir en archivos separados los hosts que pertenecen a la red Tor (los que salen del puerto 9001 de nuestro servidor) y los hosts que son servidores comunes, es decir, los visitados por los usuarios de la red.

```
#!/usr/bin/python
with open('hosts','r') as ifile, open('tor_servers','w') as o_tor, open('common_server','w') as o_server:
    lines = set(ifile.readlines())
    for l in lines:
        hosts = l.split()
        if hosts[0].endswith(':9001'):
            o_tor.write(hosts[1].split(':')[0]+'\n')
        else:
            o_server.write(hosts[1].split(':')[0]+'\n')
```

Figrua 16. Script para filtrar hosts conectados

Una vez teniendo por separado las direcciones IP de servidores que pertenecen a la red Tor y de los que no pertenecen, podemos ejecutar comandos como `whois` de forma secuencial y obtener información de cada uno. Haciendo esto puede ser que se encuentre mucha o poca información; en este caso, podemos determinar que se están buscando páginas que se encuentran alojadas en China.

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '58.208.0.0 - 58.223.255.255'

% Abuse contact for '58.208.0.0 - 58.223.255.255' is 'anti-spam@ns.chinanet.cn.net'

inetnum:        58.208.0.0 - 58.223.255.255
netname:        CHINANET-JS
descr:          CHINANET jiangsu province network
descr:          China Telecom
descr:          A12,Xin-Jie-Kou-Wai Street
descr:          Beijing 100088
country:        CN
admin-c:        CH93-AP
tech-c:         CJ186-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-CHINANET-JS
mnt-routes:     MAINT-CHINANET-JS
remarks:        ------------------------------------------------------
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
remarks:        ------------------------------------------------------
status:         ALLOCATED PORTABLE
last-modified:  2016-05-04T00:01:43Z
source:         APNIC
mnt-irt:        IRT-CHINANET-CN

irt:            IRT-CHINANET-CN
address:        No.31 ,jingrong street,beijing
address:        100032
e-mail:         anti-spam@ns.chinanet.cn.net
```

Figrua 17. Información de un host visitado

Se puede obtener la misma información de las direcciones correspondientes a los demás nodos usando el comando `whois` y, haciendo una búsqueda un poco más profunda, se puede determinar qué tipo de organizaciones o personas son las que apoyan en mayor o menor medida el proyecto Tor. Por ejemplo, es común encontrar páginas cuyo principal tema es la seguridad informática apoyando con un nodo, como se ve en las figuras 18 y 19. Se recuerda que es posible que cualquier nodo Tor podría estar alojando un *hidden service* (sitio .onion), pero esto no se puede determinar con este tipo de análisis.

Figrua 18. Sitio web de un nodo Tor

Figrua 19. Sitio web de un nodo Tor 2

Análisis del tráfico

Se capturaron 222 GB de tráfico de red en 48 horas, repartidos en 48 archivos en formato pcap. Esto significa un promedio de 4.6 GB de tráfico por hora. Lo que demuestra que la red es aún muy utilizada y aunque esta cantidad de tráfico es poco (en comparación con los más de 100G bits/s que viajan por la red), [5] se considera como tráfico suficiente para ser analizado.

```
6.1G    traffic/dump_2017-11-19_21_00_01.pcap
5.2G    traffic/dump_2017-11-19_22_00_01.pcap
3.5G    traffic/dump_2017-11-19_23_00_01.pcap
5.5G    traffic/dump_2017-11-20_00_00_01.pcap
4.1G    traffic/dump_2017-11-20_01_00_01.pcap
222G    traffic/
```

Figrua 20. Capturas de tráfico y su tamaño

Consultas DNS

Sitios más buscados

El objetivo de este análisis es mostrar los sitios más comúnmente visitados por los usuarios de Tor. Para obtener esta información, se hace un filtro con tshark, el cual permite obtener los nombres de dominio que fueron consultados. Para automatizar la búsqueda en todos los archivos pcap, se hizo un script sencillo.

```
for dump in traffic/*; do
        tshark -r "$dump" -T fields -e dns.qry.name -Y "dns.flags.response eq 0" >> dns_queries
done
```

Figrua 21. Comando para obtener peticiones DNS

En total se hicieron 53,433 consultas DNS en aproximadamente diez horas. Se desarrolló un script en Python que permite obtener los dominios de nivel superior y segundo nivel más buscados (top 15) y mostrarlos gráficamente.

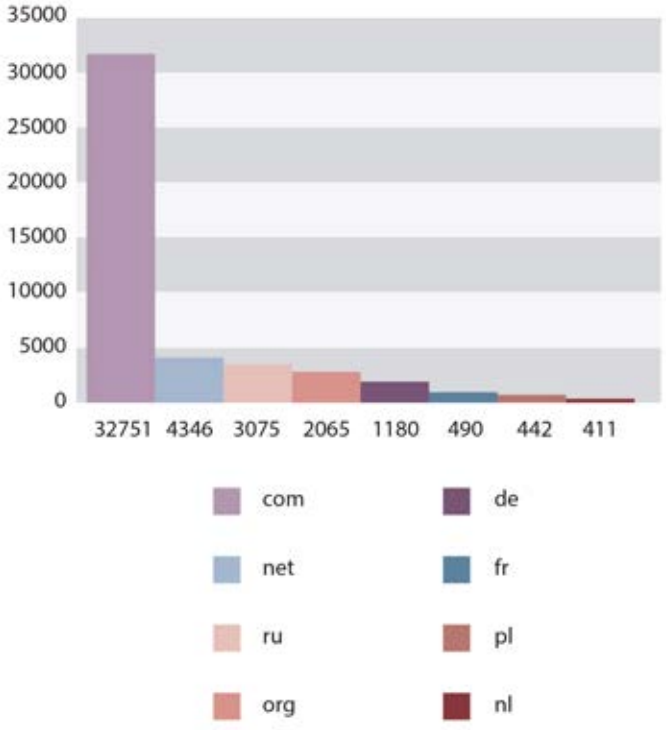
```
#!/usr/bin/python
with open('dns_queries','r') as ifile:
    domains = [d.lower() for d in ifile.readlines()]

tld = {}
sld = {}

for d in domains:
    #Agrega el dominio de orden superior al diccionario o aumenta su cuenta
    subdomains = d.split('.')
    if subdomains[-1] not in tld:
        tld[subdomains[-1]] = 1
    else:
        tld[subdomains[-1]] += 1

    #Agrega dominios de segundo nivel a su diccionario o aumenta su cuenta
    if len(subdomains) >= 2:
        dom = '%s.%s' % (subdomains[-2],subdomains[-1])
        if dom not in sld:
            sld[dom] = 1
        else:
            sld[dom] += 1
    else:
        if subdomains[-1] not in sld:
            sld[subdomains[-1]] = 1
        else:
            sld[subdomains[-1]] += 1
```

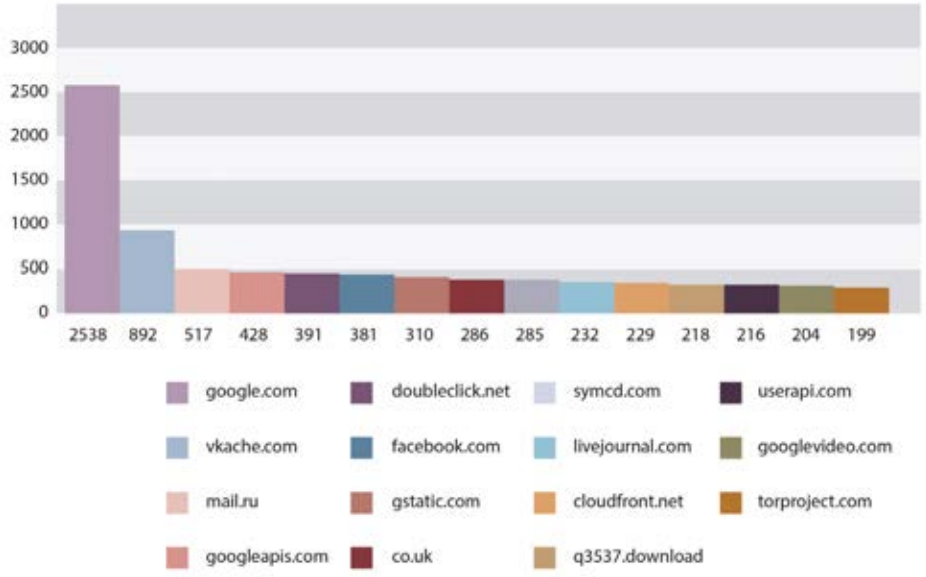
Figrua 22. Script para obtener la cuenta de dominios



Figrua 23. Top de búsquedas de dominio de nivel superior

Se observa que “com” es el TLD más buscado, sin embargo sorprende que “ru” ocupa el tercer lugar, lo que demuestra que los sitios rusos son un objetivo regular de los usuarios de la red.

En cuanto a los nombres de dominio hasta el segundo nivel, hay que destacar que se trata de dominios comunes como facebook.com y google.com. Sin embargo hay dominios extraños como q3537.download.



Figrua 24. Top de búsquedas de dominios hasta segundo nivel

Búsqueda de actividad maliciosa

Como se puede ver en las gráficas anteriores, la mayor cantidad de consultas se hace hacia sitios comunes, sin embargo, revisando los dominios se puede encontrar sitios extraños o poco comunes. En estos casos se procedió a obtener más información de dichos dominios a través del sitio Virus Total, el cual se encarga de analizar archivos y sitios en busca de malware.

El primero en analizarse llamó mi atención, pues es un dominio con una longitud muy grande, algo que es muy poco común. Sin embargo, no fue detectado como un dominio malicioso en Virus Total.

Figrua 25. Algunos dominios consultados 2

Figrua 26. Análisis en Virus Total de dominio sospechoso 2

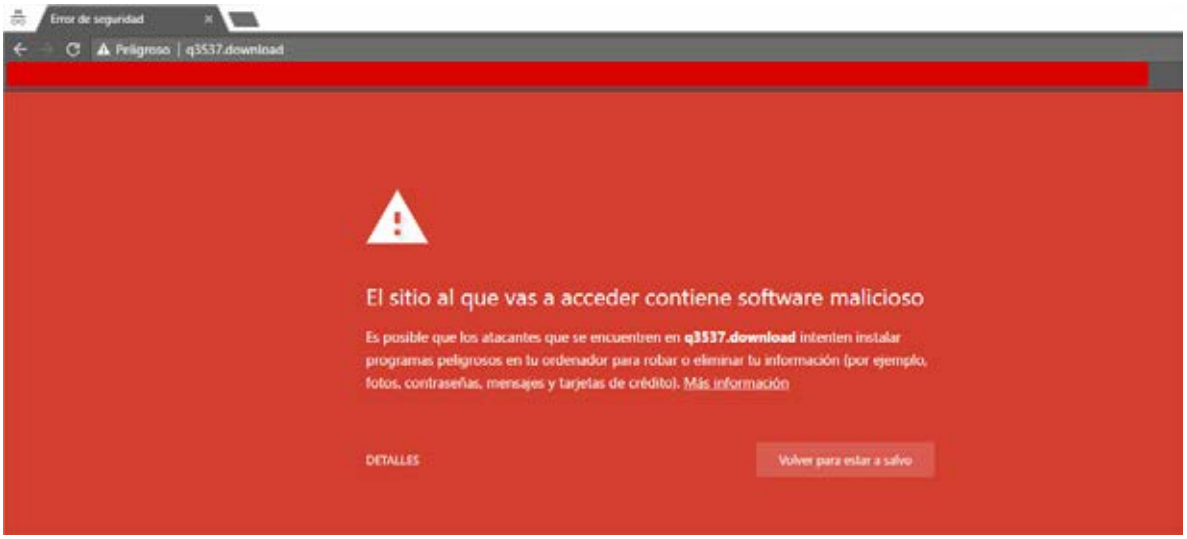
El segundo dominio analizado llamó mi atención pues, además de ser más largo que el resto de los dominios encontrados, termina en “download”, dando una referencia a que se trata de una página de descargas. En este caso sí fue determinado como un sitio malicioso por 5 escáneres.

```
spartel-marketing.com:  1
ads.realitytraffic.com: 1
momsclubofvenicefl.com: 1
adsmod.com:     1
46852.43483.wymigx.zjwpq1.kskddh.co0qvm.uul0jd.dllm3.www.q3537.download:        1
www.proprealtors.com:   1
eastchesterhousevalue.com:      1
www.teaforte.com:       1
biotecher.com:  1
jallenaluminum.com:     1
```

Figrua 27. Algunos dominios consultados

Figrua 28. Análisis en Virus Total de dominio sospechoso

Puesto que con el script de Python se determinó que q3537.download fue uno de los dominios más veces buscado, llamó mi atención aún más. Se accedió a través de un navegador y, efectivamente, es anunciado por el navegador como un sitio malicioso. Se pasó por alto la advertencia para ver el contenido del sitio y resultó ser una página en idioma chino.



Figrua 29. Advertencia en navegador sobre sitio malicioso

Figrua 30. Página principal de sitio malicioso

Se volvió a utilizar el comando `whois`, pues de esta forma se puede encontrar información que podría ser útil para advertir que el sitio está siendo utilizado para difundir malware. Sin embargo eso sale del objetivo del proyecto y se decidió terminar aquí.

```
ESET-2017 > whois q3537.download
Domain Name: q3537.download
Registry Domain ID: D446566-DOWNLOAD
Registrar WHOIS Server: whois.west263.com
Registrar URL: West263.com
Updated Date: 2017-10-20T11:17:00Z
Creation Date: 2016-10-14T07:31:58Z
Registry Expiry Date: 2018-10-13T23:59:59Z
Registrar: Chengdu West Dimension Digital Technology Co., Ltd.
Registrar IANA ID: 1556
Registrar Abuse Contact Email: westdomain@gmail.com
Registrar Abuse Contact Phone: +86.2886263960
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: C432199-DOWNLOAD
Registrant Name: wang hai rong
Registrant Organization: wang hai rong
Registrant Street: Feng Xiang Xian Fan Jia Zhai Xiang Zhang Jia Gou Cun Si Zu 047Ha
Registrant Street:
Registrant Street:
Registrant City: Bao Ji
Registrant State/Province: SN
Registrant Postal Code: 721400
Registrant Country: CN
Registrant Phone: +86.13243841569
Registrant Phone Ext:
Registrant Fax: +86.13243841569
Registrant Fax Ext:
Registrant Email: wwwymco@126.com
Registry Admin ID: C432200-DOWNLOAD
Admin Name: hairong wang
Admin Organization: hairong wang
Admin Street: Feng Xiang Xian Fan Jia Zhai Xiang Zhang Jia Gou Cun Si Zu 047Ha
```

Figrua 31. Información registrada del sitio malicioso

Dominios mexicanos

Se investigó qué tipo de sitios son los que los mexicanos buscan. Esto no es una aseveración definitiva, pues un mexicano podría buscar cualquier tipo de sitios y un extranjero podría buscar sitios mexicanos por cualquier razón. Aun así, no deja de ser un poco interesante y divertido.

Se hizo un filtro de todos los dominios usando las cadenas “.mx” y “mex”.

```
ESET-2017 > fgrep .mx dns_queries_sorted >> dominios_mex
ESET-2017 > fgrep mex dns_queries_sorted >> dominios_mex
ESET-2017 > sort dominios_mex | uniq > dominios_mex
ESET-2017 >
```

Figrua 32. Comandos para filtrar dominios mexicanos

El resultado se muestra a continuación, siendo “www.correosdemexico.gob.mx” y “www.amazon.com.mx” los dominios más consultados.

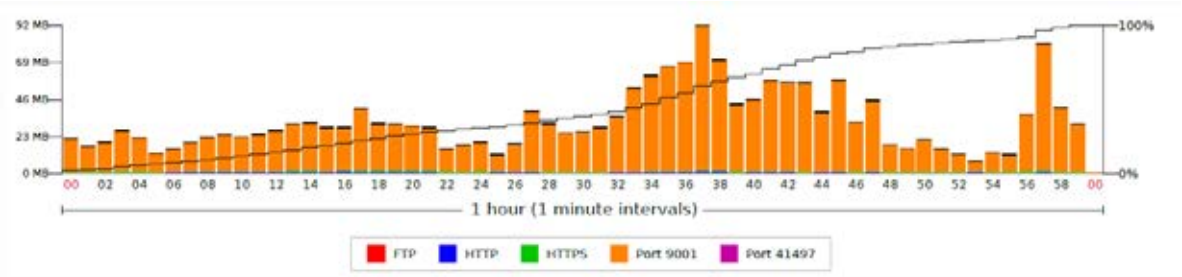
Dominio	Consultas	Dominio	Consultas
app.cfe.gob.mx	1	sevenservice.com.mx	1
arxbuysell.com.mx	1	terra.com.mx	1
bclegalconsulting.com.mx	1	themexicantaco.org	1
blogs.eluniversal.com.mx	1	transexualesmexico.net	1
cdn.mxpnl.com	6	unidep.mx	1
chorizomexicano.biz	1	vertelenovelasyseries.blogspot.mx	1
com.mx	1	whois.mx	1
folex.com.mx	1	www.actbc.mx	1
grupocyc.mx	1	www.amazon.com.mx	24
hospedame.mx	1	www.audioonline.com.mx	1
ibotana.mx	1	www.correosdemexico.gob.mx	31
jimaja.com.mx	1	www.costco.com.mx	1
jumpseller.mx	1	www.dimercom.mx	1
koolteck.com.mx	1	www.elfinanciero.com.mx	1
livinginthemexicancaribbean.com	1	www.fiestasmexicanas.net	1
mexashare.com	1	www.filosofia.mx	1
mexicolindojewelry.com	1	www.homedepot.com.mx	1
nextme.mx	1	www.i-m.mx	1
oarsa.mx	1	www.iscor.com.mx	1
paginas.seccionamarilla.com.mx	2	www.lamudi.com.mx	1
p.ato.mx	1	www.linio.com.mx	1
quicksteptelcomgimex.com	1	www.medicinatradicionalmexicana.unam.mx	1
s.ato.mx	2	www.mxdout.com	1
scientologymexico.org	1	www.sams.com.mx	1
segurodeviajero.mx	1	www.transexualesmexico.net	1

Análisis de flujos: tcpflow

Un flujo se refiere a todas las comunicaciones establecidas entre la misma dirección IP origen y la misma dirección IP destino. Esto vuelve más fácil el mostrar cuáles son las direcciones IP que más datos transmitieron, así como los protocolos más usados a través del nodo. Para lograr este objetivo, se utilizó el programa tcpflow.

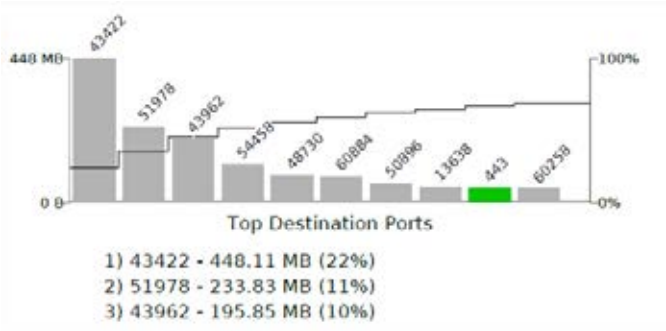
Para el primer análisis, se usó el archivo dump_2017-11-19_00_01.pcap, el cual tiene un tamaño de 1.9 GB y contiene el tráfico en esa hora en particular.

Se puede observar que la mayor parte del tráfico, por mucho, corresponde al puerto 9001. Como bien recordaremos, este es el puerto configurado para establecer las comunicaciones con otros nodos de la red. Esto nos dice que prácticamente la mayor parte del tráfico que redirigimos no va hacia hosts finales a pesar de ser un nodo de salida.

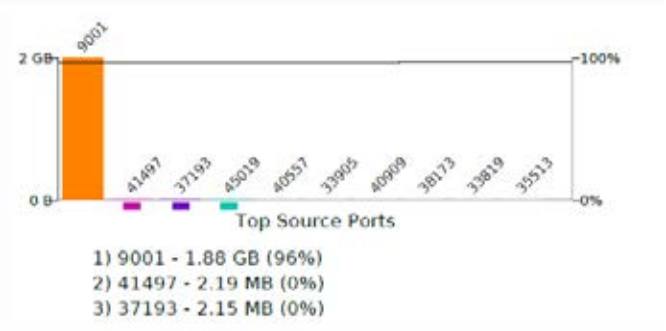


Figrua 33. Protocolos más usados por minuto

A continuación se puede ver el top de puertos origen y puertos destino. Esto corrobora la información, pues el puerto origen más usado fue el 9001 y en los puertos destino solo figura el 443 de los puertos bien conocidos.



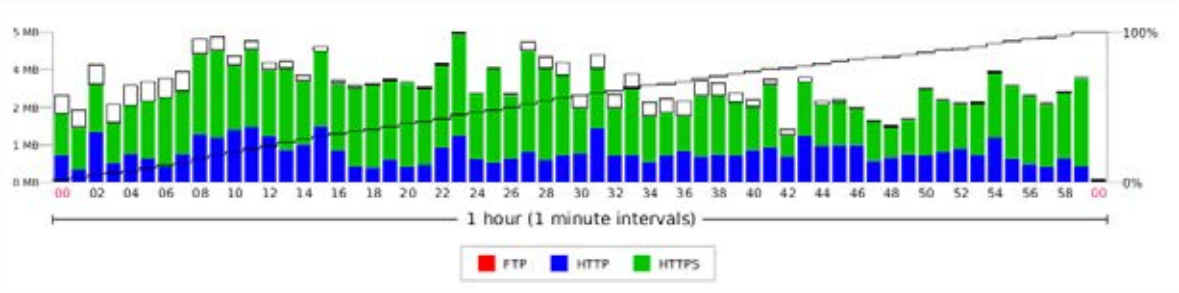
Figrua 34. Puertos destino más comunes



Figrua 35. Puertos origen más comunes

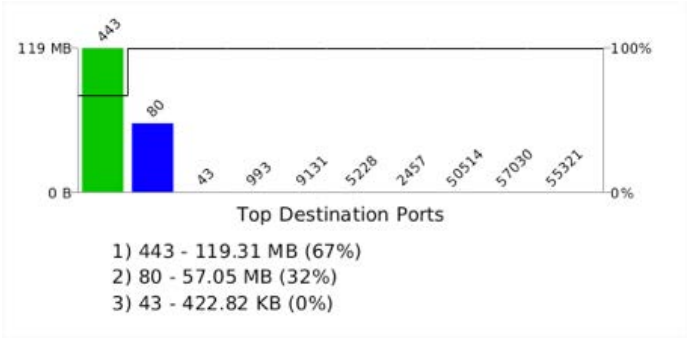
Se procedió a hacer un filtro sobre una captura diferente, en este caso se eligió el archivo dump_2017-11-20_06_00_01.pcap el cual originalmente tenía un tamaño de 4.9 GB y después de filtrar todo el tráfico correspondiente al puerto 9001, resultó un archivo de 220 MB.

Ahora es más evidente la cantidad de tráfico que viaja cifrado con respecto al que viaja no cifrado dentro de la red. Si bien sí hay una gran cantidad que viaja cifrado, es preocupante ver que sigue habiendo un porcentaje alto de tráfico que no lo hace.

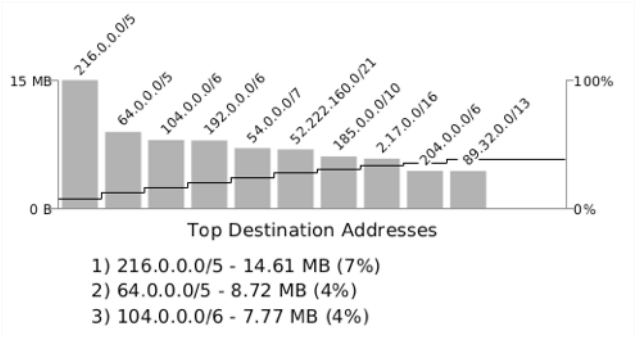


Figrua 36. Protocolos más usados por minuto 2

Puesto que se eliminó el tráfico correspondiente al enrutamiento de la red, se puede ver cuáles fueron las direcciones que más tráfico generaron durante esa hora en particular, así como una mejor vista de los protocolos mayormente usados.



Figrua 37. Puertos origen más comunes 2

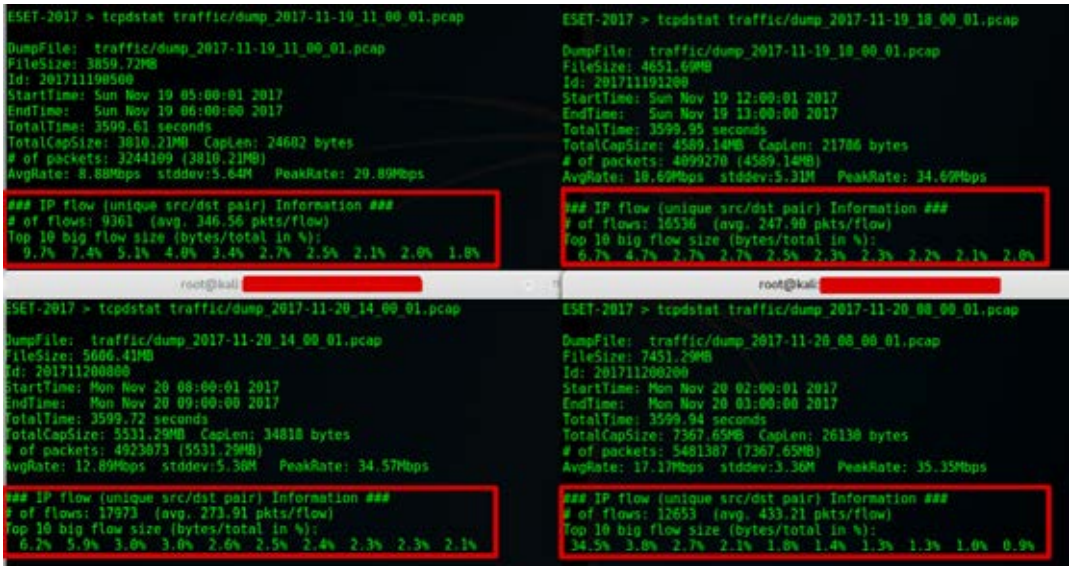


Figrua 38. Direcciones destino más comunes

Análisis de flujos: tcpdstat

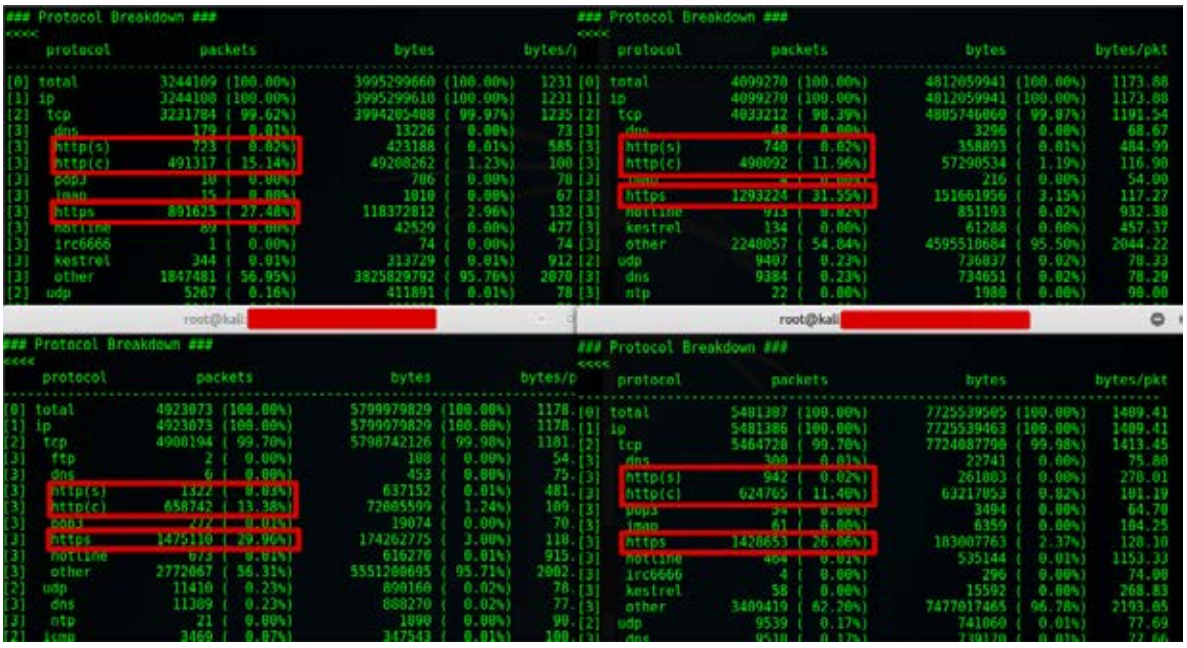
Para complementar el análisis anteriormente hecho, se decidió usar un programa un tanto antiguo pero muy útil: tcpdstat. Este programa nos ofrece de forma rápida y concisa un desglose de los protocolos más usados.

Esto nos sirve para determinar cuánto tráfico puede recibir o enviar un solo host y ver cuáles son las costumbres de los usuarios dentro de la red. Para este análisis se usaron los archivos dump_2017-11-19_11_00_01.pcap (3.8GB), dump_2017-11-19_18_00_01.pcap (4.6 GB), dump_2017-11-20_14_00_01.pcap (5.5 GB), y dump_2017-11-20_08_00_01.pcap (7.3GB). Hay que recordar que estas capturas contienen mucho tráfico correspondiente al puerto 9001 (enrutamiento de Tor).



Figrua 39. Resultado de tcpdstat en cuatro capturas

En este análisis se puede comprobar que, si bien hay una buena parte del tráfico cifrado, aproximadamente 30% del tráfico de navegación de los usuarios corresponde a HTTP y no a HTTPS. Esto significa que sería muy sencillo para cualquiera que instale y configure un nodo de salida obtener una gran cantidad de información de los usuarios, como veremos a continuación.



Figrua 40. Resultado de tcpdstat en cuatro capturas 2

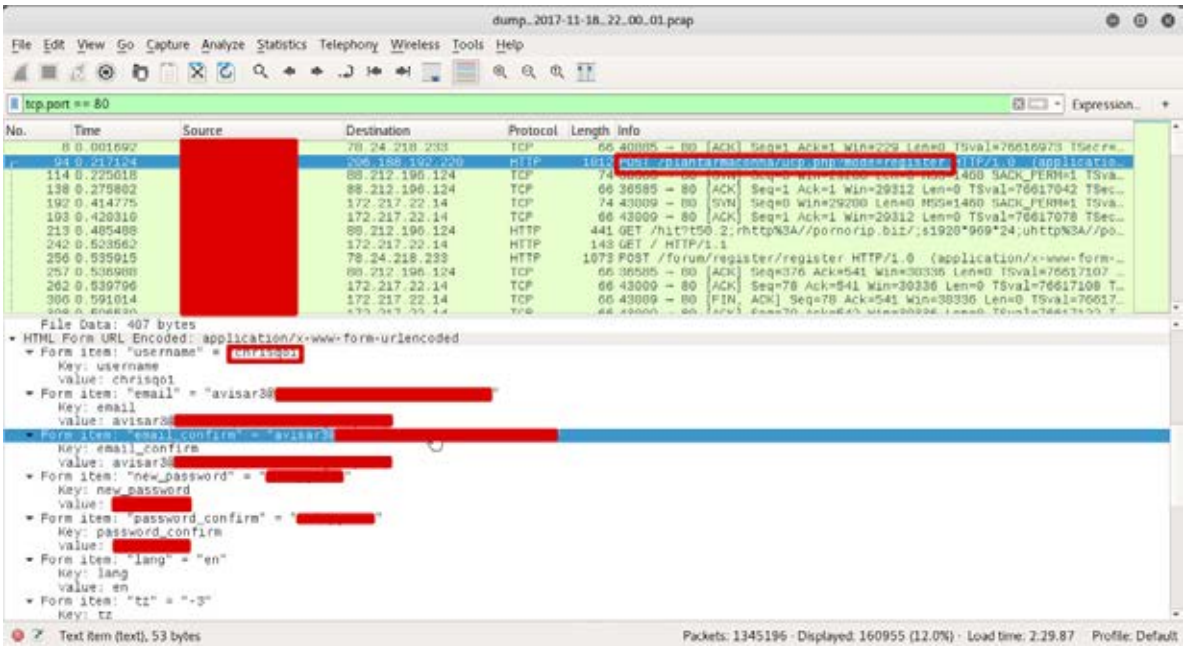
Análisis de tráfico HTTP: Wireshark

El objetivo del trabajo a partir de esta sección, es demostrar qué tan fácil podría ser para un administrador de un nodo de salida obtener información sensible de las personas que utilizan Tor.

Esta parte del análisis se comenzó usando una herramienta muy conocida: Wireshark, debido a su gran popularidad para el análisis de tramas y por todas las características que provee.

A continuación veremos que existen herramientas que automatizan la extracción de datos que, para un atacante o analista de seguridad, son mucho más útiles. Sin embargo, no está de más probar con una herramienta tan popular para demostrar claramente el análisis llevado a cabo.

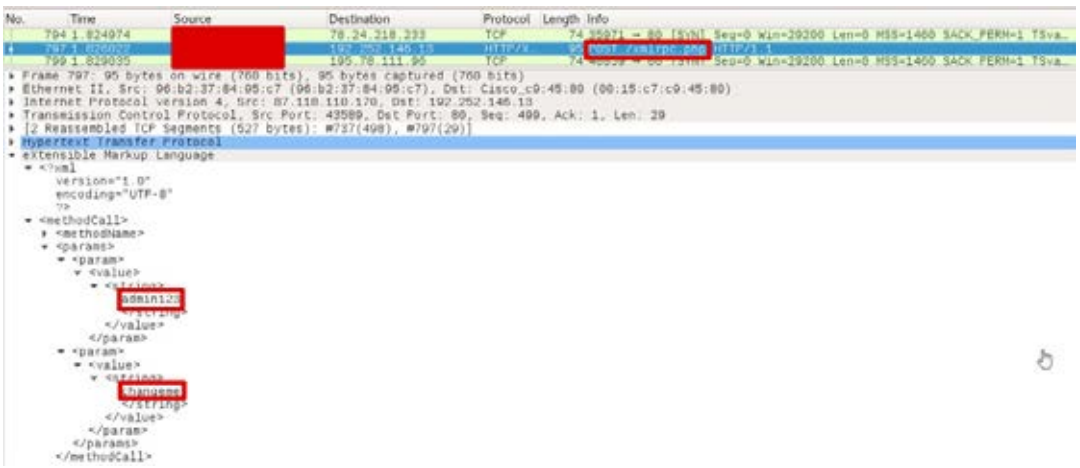
Se aplicó un filtro para mostrar únicamente el tráfico HTTP y, para mi sorpresa, una de las primeras cosas en aparecer fue un par de credenciales de un formato de registro de un sitio.



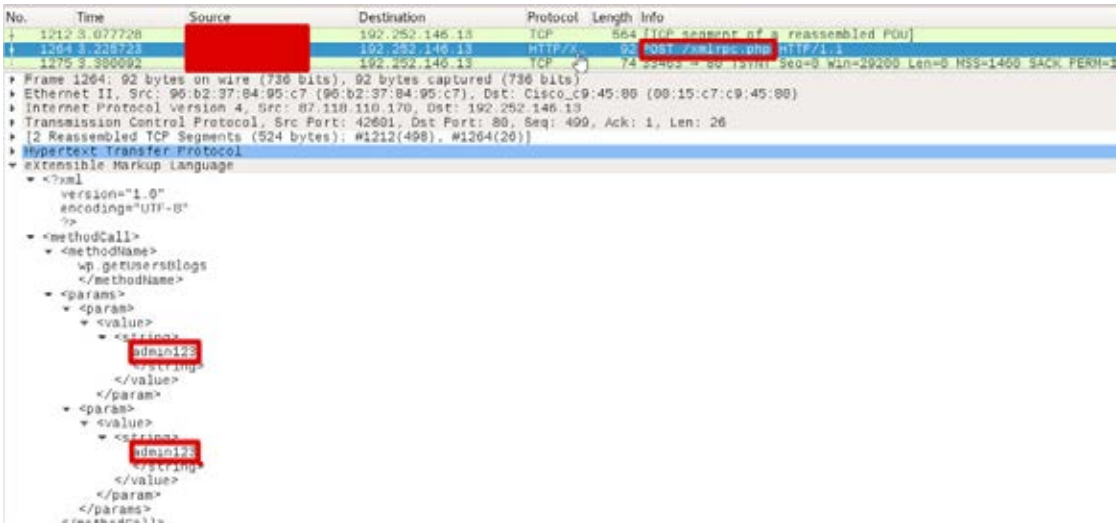
Figrua 41. Credenciales encontradas en Wireshark

En no muchos paquetes posteriores, se encontró con algo que bien podría ser considerada una situación similar. Inicios de sesión (o mejor dicho: intentos de inicio de sesión) a través del archivo xmlrpc.php que se encuentra activo por defecto en los sitios construidos con el gestor de contenidos (CMS) Wordpress.

Claramente se trata de un ataque de fuerza bruta al sitio mostrado, pues se encontraron muchos intentos para ingresar en esta captura de tráfico.



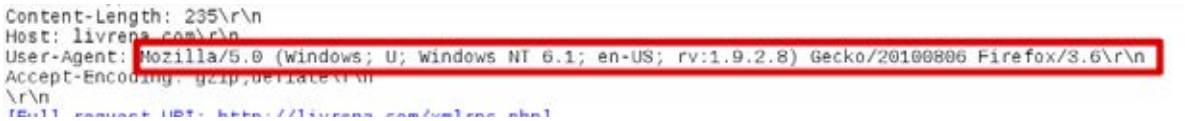
Figrua 42. Ataque de fuerza bruta en Wireshark



Figrua 43. Ataque de fuerza bruta en Wireshark 2

Además de probar repetidamente con muchas combinaciones diferentes, el atacante también suele cambiar el agente de usuario (HTTP User-Agent) en las diferentes peticiones en un esfuerzo de evitar ser bloqueado por la página atacada, lo cual solo confirma que se trata de este tipo de ataque.

Figrua 44. User-Agent en fuerza bruta

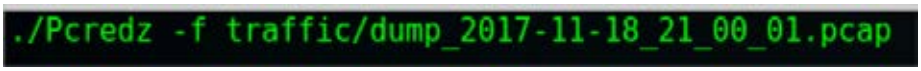


Figrua 45. User-Agent en fuerza bruta 2

Figrua 46. User-Agent en fuerza bruta 3

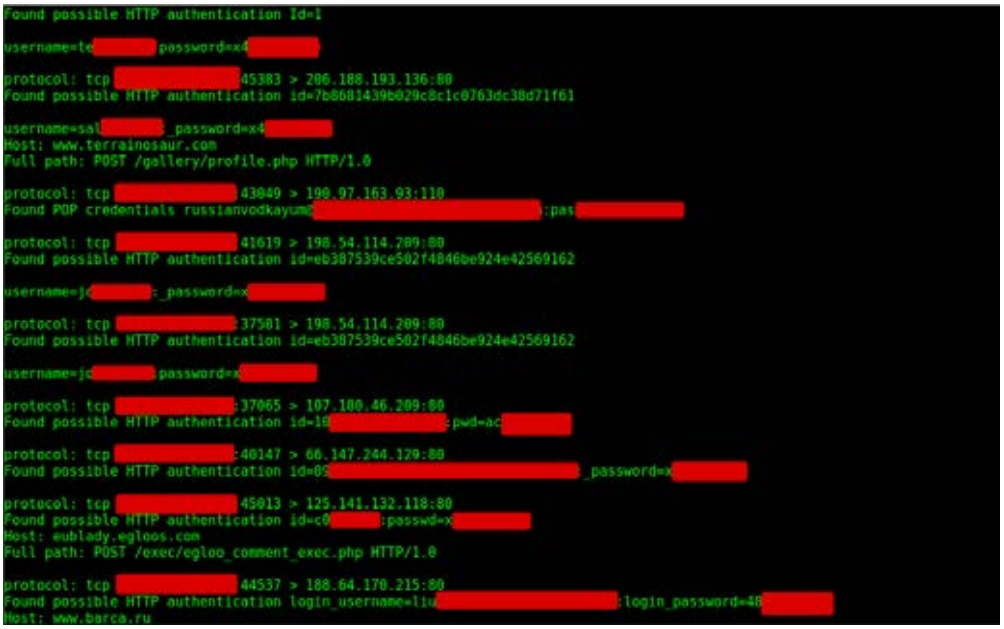
Extracción de contraseñas: Pcredz

Puesto que en general son archivos muy grandes, continuar con la búsqueda de información sensible usando Wireshark no es viable. Por lo tanto se decidió usar una herramienta que automatice la extracción de este tipo de datos[6] y así poder determinar qué tanta información importante y sensible viaja de forma insegura a través de esta red. Se ejecutó Pcredz y se seleccionó la captura dump_2017-11-18_21_00_01.pcap. Una vez que se ejecuta el programa se registran todas las posibles credenciales en un archivo de texto.



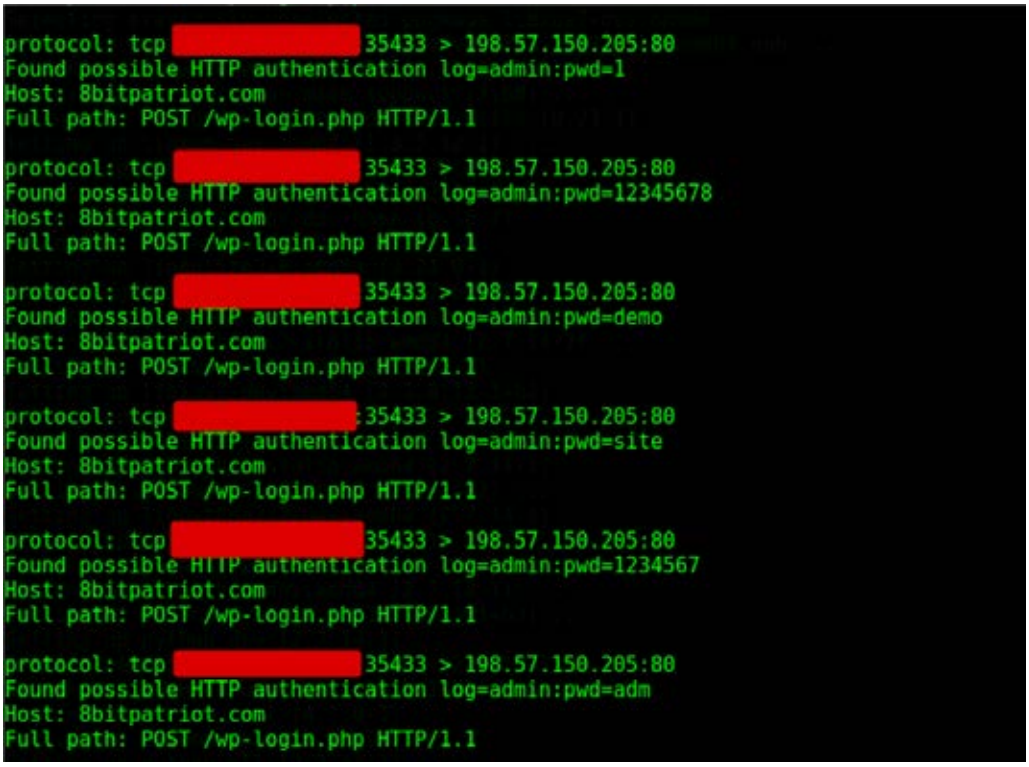
Figrua 47. Ejecución de Pcredz

Se repitió el proceso con tres capturas más y la situación en general es alarmante. No intenté determinar si eran credenciales válidas, pues eso sale completamente del alcance de este trabajo, sin embargo, se encontraron más de 300 posibles credenciales en solo cuatro horas.



Figrua 48. Credenciales obtenidas con Pcredz

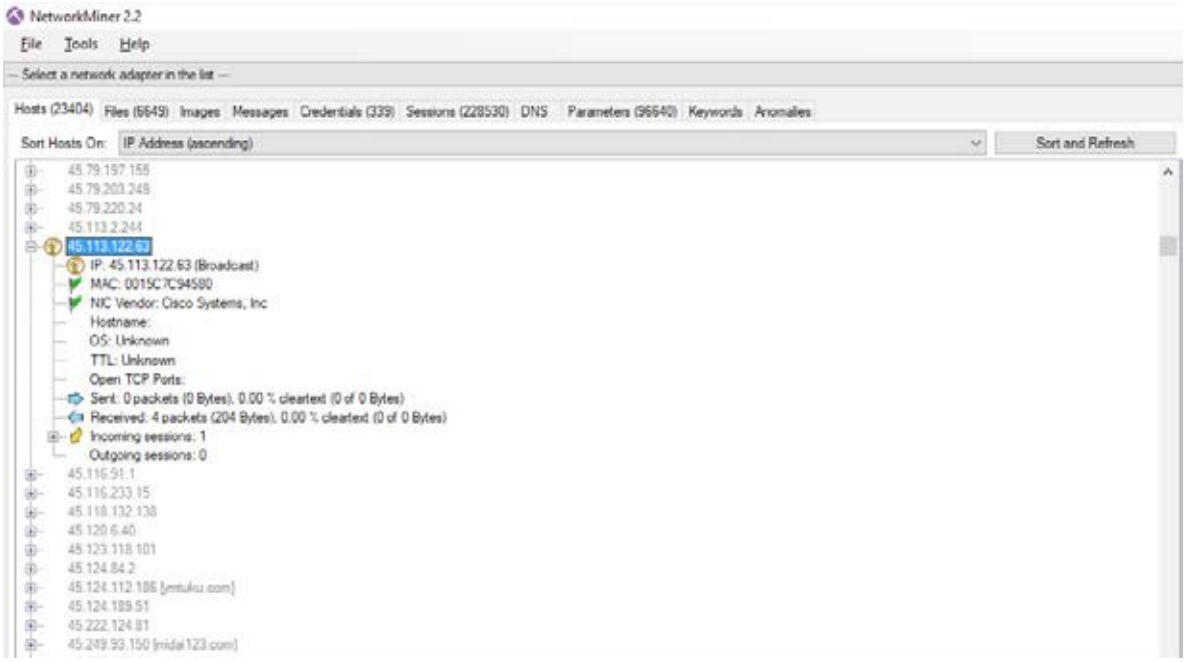
En esta herramienta también se encontraron ataques de fuerza bruta a un sitio construido con Wordpress. Si bien esto claramente modifica la cifra antes mencionada (más 300 credenciales en cuatro horas), cabe resaltar que no cambia por mucho, pues estos, ataques están lejos de ser exhaustivos. Esto debido a que se probaron únicamente contraseñas por defecto o muy débiles.



Figrua 49. Ataque de fuerza bruta encontrado con Pcredz

Extracción de información: Network Miner

Anteriormente ya se extrajo información sensible que viajó a través del nodo, sin embargo, el programa Network Miner[7] facilita la extracción de archivos y provee muchos datos en un formato fácilmente entendible. Por ejemplo, muestra todos los hosts que se encuentran en determinada captura, así como información detallada de ellos.



Figrua 50. Hosts encontrados en una captura

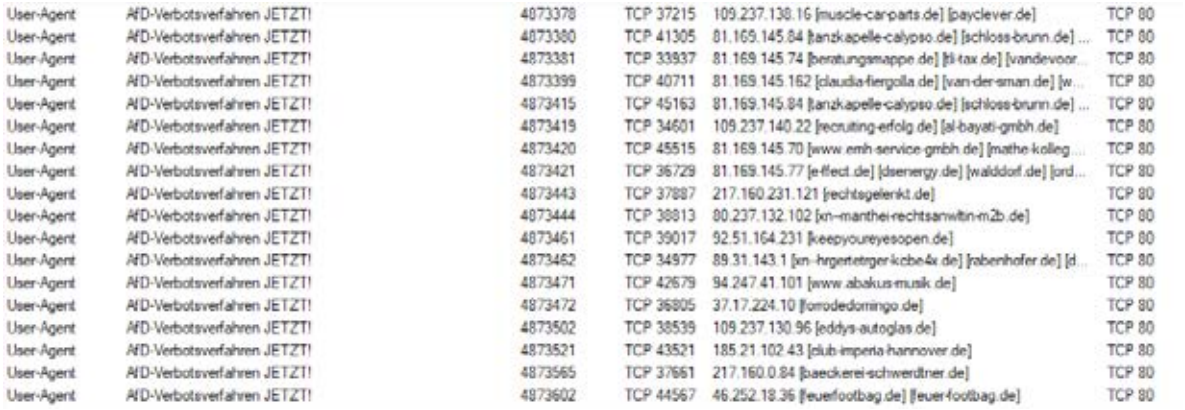
Una de las características que implementa este programa es la extracción de credenciales. No lo hace tan bien como PCredz, pero obtiene mucha información que fácilmente podría utilizar un atacante, como los identificadores de sesión y de esta manera hacer un secuestro de sesión.

Server	Protocol	Username	Password	Valid login	Login timestamp
78.140.137.93 [rawpost.com]	HTTP Cookie	__mcja=172068000.1.2073218301.1510992660.0.151099...	N/A	Unknown	2017-11-18 02:
78.140.137.93 [rawpost.com]	HTTP Cookie	__mcja=172068000.1.2073218301.1510992660.0.151099...	N/A	Unknown	2017-11-18 02:
172.82.228.19 [adobetp.chegg.com]	HTTP Cookie	check=true; AMCVS_3FE7CBC1556605A77F000101%40A...	N/A	Unknown	2017-11-18 02:
172.82.228.19 [adobetp.chegg.com]	HTTP Cookie	check=true; AMCVS_3FE7CBC1556605A77F000101%40A...	N/A	Unknown	2017-11-18 02:
172.82.228.19 [adobetp.chegg.com]	HTTP Cookie	PHPSESSID=90561p66f221f6v2b1md1b8t6; C=0; O=0; U...	N/A	Unknown	2017-11-18 02:
172.82.228.19 [adobetp.chegg.com]	HTTP Cookie	PHPSESSID=041hueoeudehbsd6ok.cuf4sv61; C=0; O=0; ...	N/A	Unknown	2017-11-18 02:
172.82.228.19 [adobetp.chegg.com]	HTTP Cookie	PHPSESSID=p5vb2q3t2pl2oc2k8cg7gjm0; C=0; O=0; U=...	N/A	Unknown	2017-11-18 02:
216.137.61.57 [promo.webpayments.closeby.internet.apps....	HTTP Cookie	Set-Cookie: Path=/; Secure; HttpOnly; CloudFront-Key-Pair...	N/A	Unknown	2017-11-18 02:
94.142.139.248 [skyback.ru]	HTTP Cookie	h3Pdxw7bFm=1; PHPSESSID=69eaade64da43e4254b1d...	N/A	Unknown	2017-11-18 02:
104.28.8.154 [en.mytubes.xyz]	HTTP Cookie	100640546P=2-1510994328-1510994372-1510994328-1...	N/A	Unknown	2017-11-18 02:
185.68.16.181 [napor.com.ua]	HTTP Cookie	da517e9f69575c62c3bd405786d712f6=3uuu2p5pb98obkt...	N/A	Unknown	2017-11-18 02:
84.200.32.149 [k183.clanzilla.de]	HTTP Cookie	PHPSESSID=mcmdt7015tr11r67gj99h1jbb3	N/A	Unknown	2017-11-18 02:
84.200.32.149 [k183.clanzilla.de]	HTTP Cookie	PHPSESSID=mcmdt7015tr11r67gj99h1jbb3; wordpress_te...	N/A	Unknown	2017-11-18 02:
84.200.32.149 [k183.clanzilla.de]	HTTP POST	mu[redacted]	9[redacted]	Unknown	2017-11-18 02:
84.200.32.149 [k183.clanzilla.de]	HTTP Cookie	PHPSESSID=mcmdt7015tr11r67gj99h1jbb3; wordpress_te...	N/A	Unknown	2017-11-18 02:
104.28.9.154 [en.mytubes.xyz]	HTTP Cookie	100640546P=5-1510994328-1510995177-1510994328-1...	N/A	Unknown	2017-11-18 02:
5.35.172.152 [www.24video.in]	HTTP Cookie	raw_ref=https%3A%2F%2Fduckduckgo.com%2F; J5ES5IO...	N/A	Unknown	2017-11-18 02:

Figrua 51. Información sensible de una captura

Se hizo una extracción de todas las cabeceras HTTP y en particular de los agentes de usuario (HTTP User-Agent), con el fin de encontrar actividad maliciosa. Esto en razón de que pueden encontrarse campañas de atacantes que se diferencian mediante esta cabecera. Asimismo, es posible encontrar actividad de malware que tenga un agente de usuario muy particular.

En general los agentes de usuario encontrados son bastante comunes (sin que esto signifique que sea tráfico no malicioso). Por otro lado, fue común encontrar el agente "AfD-Verbotsverfahren JETZT!", que no corresponde a una campaña de ataques o de malware, sino a una campaña para enviar un mensaje político.[8]

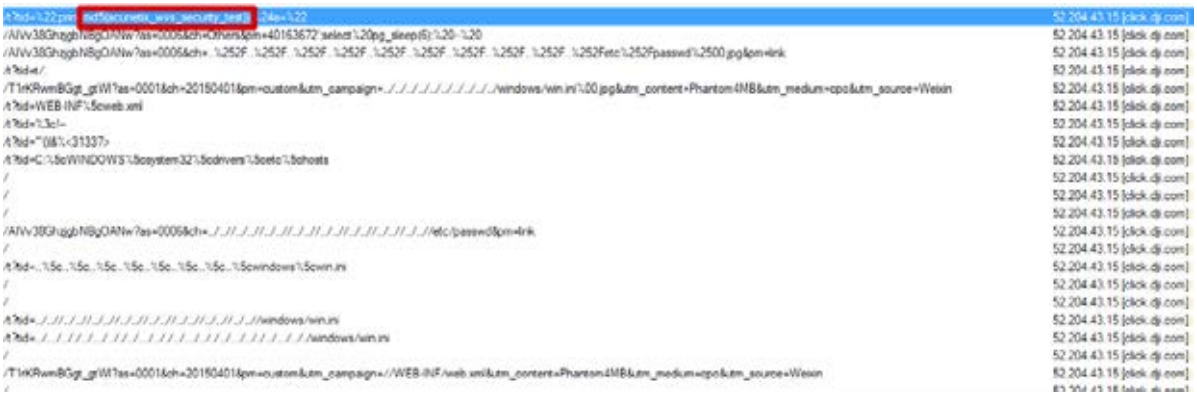


User-Agent	AfD-Verbotsverfahren JETZT!	4873378	TCP 37215	109.237.138.16 [muscle-car-parts.de] [payclever.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873380	TCP 41305	81.169.145.84 [tanzkapelle-calypso.de] [schloss-brunn.de] ...	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873381	TCP 33937	81.169.145.74 [beratungsmappe.de] [tli-tax.de] [vandevoor...	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873399	TCP 40711	81.169.145.162 [claudia-fiergolla.de] [van-der-sman.de] [w...	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873415	TCP 45163	81.169.145.84 [tanzkapelle-calypso.de] [schloss-brunn.de] ...	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873419	TCP 34601	109.237.140.22 [recruiting-erfolg.de] [al-bayati-gmbh.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873420	TCP 45515	81.169.145.70 [www.emh-service-gmbh.de] [mathe-kolleg....	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873421	TCP 36729	81.169.145.77 [e-flect.de] [dsenergy.de] [walddorf.de] [prd...	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873443	TCP 37887	217.160.231.121 [rechtsgelenkt.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873444	TCP 38813	80.237.132.102 [xn--manthei-rechtsanwltin-m2b.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873461	TCP 39017	92.51.164.231 [keepyoureyesopen.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873462	TCP 34977	89.31.143.1 [xn--hrgertetrger-kcbe4x.de] [rabenhofer.de] [d...	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873471	TCP 42679	94.247.41.101 [www.abakus-musik.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873472	TCP 36805	37.17.224.10 [torodedomingo.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873502	TCP 38539	109.237.130.96 [eddys-autoglas.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873521	TCP 43521	185.21.102.43 [club-imperia-hannover.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873565	TCP 37661	217.160.0.84 [baeckerei-schwerdtner.de]	TCP 80
User-Agent	AfD-Verbotsverfahren JETZT!	4873602	TCP 44567	46.252.18.36 [feuerfootbag.de] [feuer-footbag.de]	TCP 80

Figrua 52. Agente de usuario de una campaña política

Del mismo modo se extrajeron las peticiones GET hechas en diferentes capturas. Fue relativamente rápido encontrar un escaneo de vulnerabilidades hecho con Acunetix, que intenta ver si un servidor es vulnerable a SQL injection y a *local file inclusion*, entre otras vulnerabilidades.

Figrua 53. Escaneo de vulnerabilidades



Figrua 54. Escaneo de vulnerabilidades 2

Conclusiones

La red Tor es una red ampliamente usada que ayuda a muchas personas en diferentes situaciones que necesitan mantener su privacidad un poco mejor protegida. Se demostró que no es difícil instalar y configurar un nodo Tor y que, si alguien quisiera apoyar con un poco de ancho de banda para ayudar a estas personas, fácilmente puede lograrlo. Además, podría ser útil implementarlo para los investigadores de seguridad, ya que es un buen método para hallar actividad maliciosa en la red, así como campañas de ataques y, con algo de suerte, nuevas familias de malware.

En cuanto al uso que se le da a la red, si bien no se puede determinar el tráfico dirigido a los hidden services, está claro que la red está lejos de ser exclusiva para eso. Se encuentra todo tipo de sitios que pueden ser visitados en cualquier navegador, en cualquier lugar. Eso sí, las visitas a estos sitios son de todo tipo: escaneos de vulnerabilidades, ataques de fuerza bruta, campañas políticas, descargas de malware y navegación común.

El punto más importante de toda la investigación trata sobre la privacidad en esta red. Usar Tor está muy lejos de ser sinónimo de privacidad si no se hace con el cuidado adecuado. Quedó demostrado que en un nodo de salida administrado por un atacante o un gobierno, fácilmente se pueden extraer todo tipo de archivos, contraseñas, cookies y cualquier tráfico que no se encuentre cifrado. Esto debe convencer al lector que, si planea usar Tor para mantenerse privado, debería tener cuidado y asegurarse de viajar solo a sitios seguros usando las versiones seguras de los protocolos, como por ejemplo HTTPS, SSH o IMAPS.

Referencias

[1] Tor (s/f). Tor: Overview. Recuperado el 10 de noviembre de 2017, de https://www.torproject.org/about/overview.html.en

[2] Antonios A. Chariton (2016). Running a Tor Exit Node for fun and e-mails. Recuperado el 10 de noviembre de 2017, de https://blog.daknob.net/running-a-tor-exit-node-for-fun-and-e-mails/

[3] Tor (s/f). Reduced Exit Policy. Recuperado el 14 de noviembre de 2017, de https://trac.torproject.org/projects/tor/wiki/doc/ReducedExitPolicy

[4] Tor (s/f). Traffic. Recuperado el 14 de noviembre de 2017, de https://metrics.torproject.org/bandwidth.html

[5] Tor (s/f). Relay Search. Recuperado el 16 de noviembre de 2017, de https://metrics.torproject.org/rs.html

[6] Igandx (s/f). PCredz. Recuperado el 20 de noviembre de 2017, de https://github.com/Igandx/PCredz

[7] Netresec (s/f) NetworkMiner. Recuperado el 20 de noviembre de 2017, de http://www.netresec.com/?page=NetworkMiner

[8] Marius, (2017) TOR VS. AFD - NSA STYLE. Recuperado el 22 de noviembre de 2017, de https://marius.bloggt-in-braunschweig.de/2017/10/09/politische-kampagnen-aus-dem-tor-netz/

Si quieres saber más:

- La red Tor como elemento de privacidad en nuestras vidas
- Mitos y realidades de la Internet profunda
- WannaCry: ataque mundial y consideraciones sobre ciberseguridad

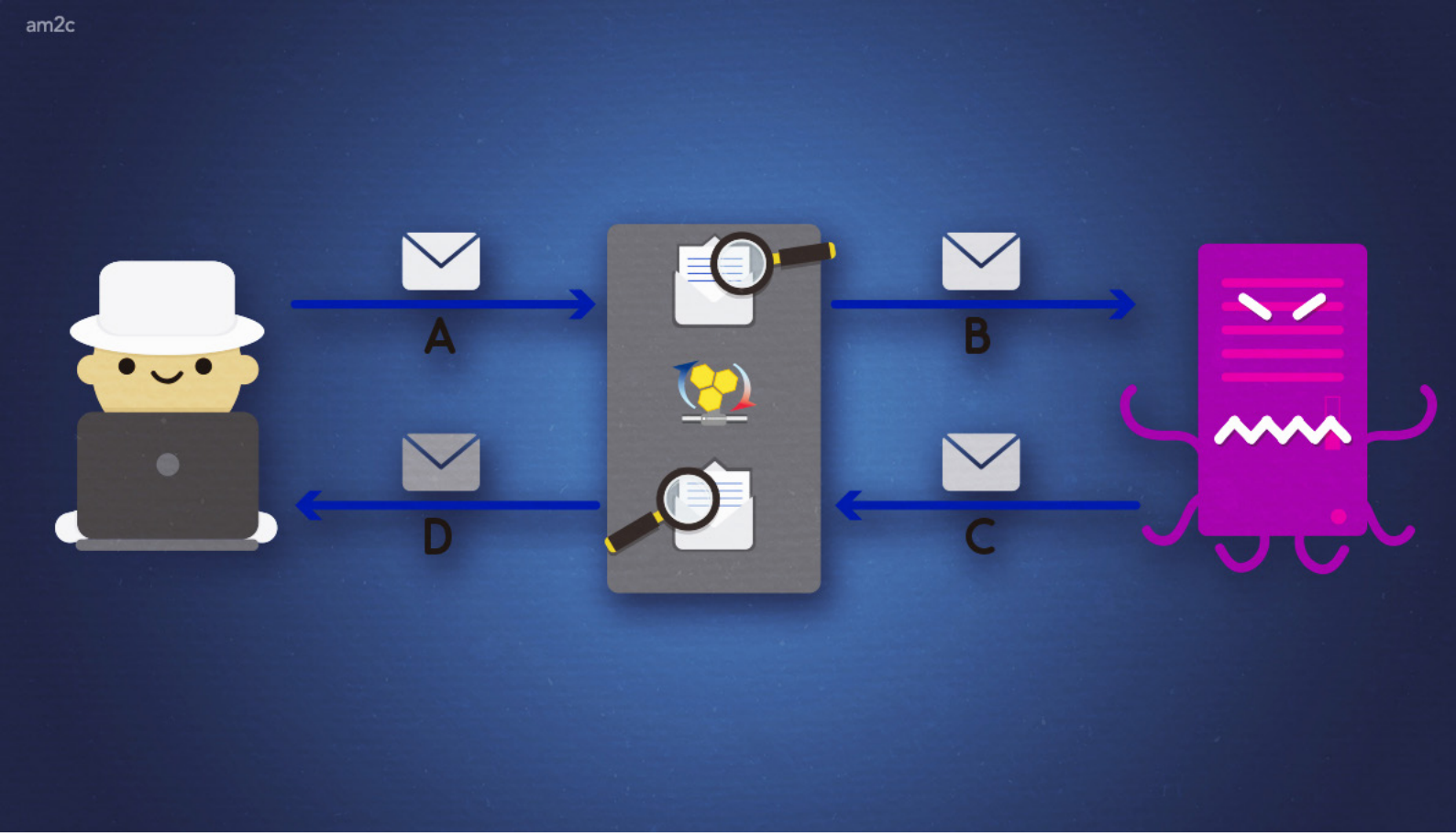
---

Virgilio Castro Rendón

Especialista en análisis de vulnerabilidades y pruebas de penetración, estudiante de la carrera de Ingeniería en Computación por la Facultad de Ingeniería de la UNAM.

Formó parte de la decimoprimera generación del Plan de Becarios en Seguridad Informática de UNAM-CERT, donde actualmente labora en el departamento de Auditoria y Nuevas Tecnologías como Especialista en Pruebas de Penetración a Sistemas Informáticos.

Sus principales áreas de interés son la programación, la criptografía y las pruebas de penetración.



HoneyProxy: análisis de tráfico HTTP

Sergio Anduin Tovar Balderas

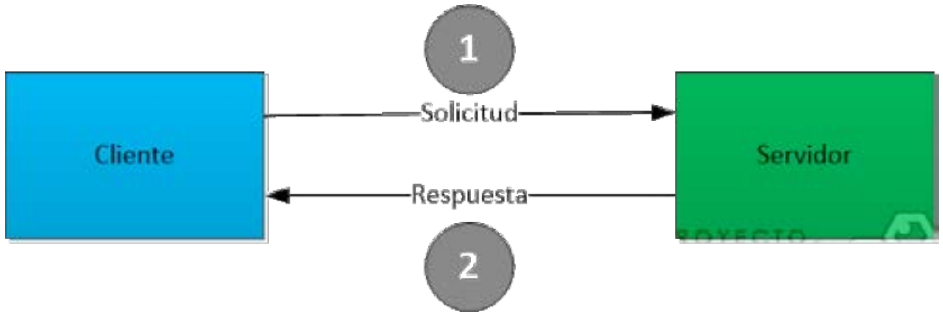
Muchas organizaciones cuentan con dispositivos de seguridad para filtrar URL o sitios que ayudan a prevenir y proteger que sus usuarios se expongan a páginas maliciosas con paquetes de exploits y para cumplir con las políticas de la organización.

En este artículo presentaré una prueba de concepto (PoC, Proof of Concept) de HoneyProxy para mostrar la modificación de peticiones y respuestas tanto del cliente y servidor, así como su ejecución con diferentes opciones que permiten a los investigadores de seguridad poder analizar el tráfico e interactuar con sitios maliciosos o malware. Además, de forma particular mostraré en la PoC cómo observar el tráfico, modificar la URL en la solicitud del cliente, el encabezado de respuesta del servidor y respuestas del servidor para mostrar imágenes en el mismo servidor o en uno remoto. Esto puede ser utilizado para analizar el tráfico de red, identificar equipos infectados con malware o interactuar con el malware durante un análisis dinámico.

A continuación se muestra el proceso y flujo al visitar una página web:

1. Solicitud: el usuario abre el navegador y teclea la dirección URL del sitio. Se resuelve el nombre de dominio y el navegador web del cliente genera una solicitud empleando el método GET del protocolo HTTP. Durante este proceso se envían otros campos dentro de la solicitud como el equipo y agente de usuario.
2. Respuesta: el servidor procesa la solicitud del cliente y responde con un código de estado 200 (Ok), indicando

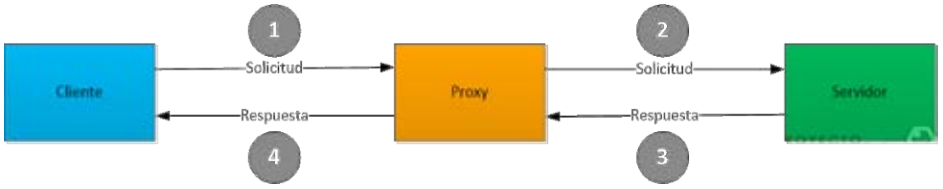
que la solicitud del cliente se completó con éxito. Además, se envía la fecha y hora, servidor y longitud del contenido, por mencionar algunos.



Figrua 1. Visita a página web (de Sergio Anduin Tovar Balderas)

Un proxy es intermediario entre un cliente y un servidor, su funcionamiento es el siguiente:

1. El cliente envía una solicitud al servidor
2. El Proxy recibe la solicitud del cliente, la procesa y envía la solicitud al servidor
3. El servidor procesa la solicitud y responde
4. El Proxy recibe la respuesta del servidor, la procesa y envía la repuesta al cliente



Figrua 2. Proxy (de Sergio Anduin Tovar Balderas)

El proxy, al interceptar las conexiones que hace un cliente a un servidor, permite mejorar el rendimiento de sitios web (caché) o proporcionar control de acceso al permitir o bloquear cierto tipo de tráfico de red por mencionar ejemplos. Principalmente existen los proxy de envío (forward), inverso (reverse) y transparente (transparent), y pueden tener otras características como autenticación, filtrado por dirección IP o contenido, listas negras, entre otras, y diversas aplicaciones en su uso.

HoneyProxy

HoneyProxy es un proxy de hombre en el medio (mitm, man-in-the-middle) ligero que permite la inspección y análisis de tráfico HTTP(S) en tiempo real. HoneyProxy cuenta con diferentes opciones que son útiles durante una revisión de seguridad a una aplicación web o de un dispositivo móvil. También posibilitan modificar las solicitudes o respuestas para examinar el tráfico de red durante el análisis dinámico de malware. En la publicación Implementación de HoneyProxy del Proyecto Honeynet UNAM se presentaron las características, el funcionamiento e implementación de HoneyProxy.

HoneyProxy tiene diferentes modos de operación (regular, transparente, etcétera), el modo determinará si el cliente necesita realizar alguna configuración. Cuando se ejecuta HoneyProxy utiliza las opciones preestablecidas o las que se encuentran en el archivo de configuración (default.conf). Cuando el cliente realiza una solicitud a un sitio

web, la solicitud es recibida por HoneyProxy y procesada para enviarla al servidor. En este punto, la solicitud puede ser modificada antes de su envío (solicitud modificada). Posteriormente el servidor recibe, procesa y genera una respuesta ante la solicitud del cliente. HoneyProxy recibe la respuesta y también puede ser modificada antes de su envío al cliente (respuesta modificada). Durante este proceso HoneyProxy emplea las bibliotecas para su funcionamiento, utiliza los programas (scripts), registra el tráfico y los sitios en las bitácoras, inicia la interfaz web de HoneyProxy para observar las solicitudes y respuestas y generar reportes.

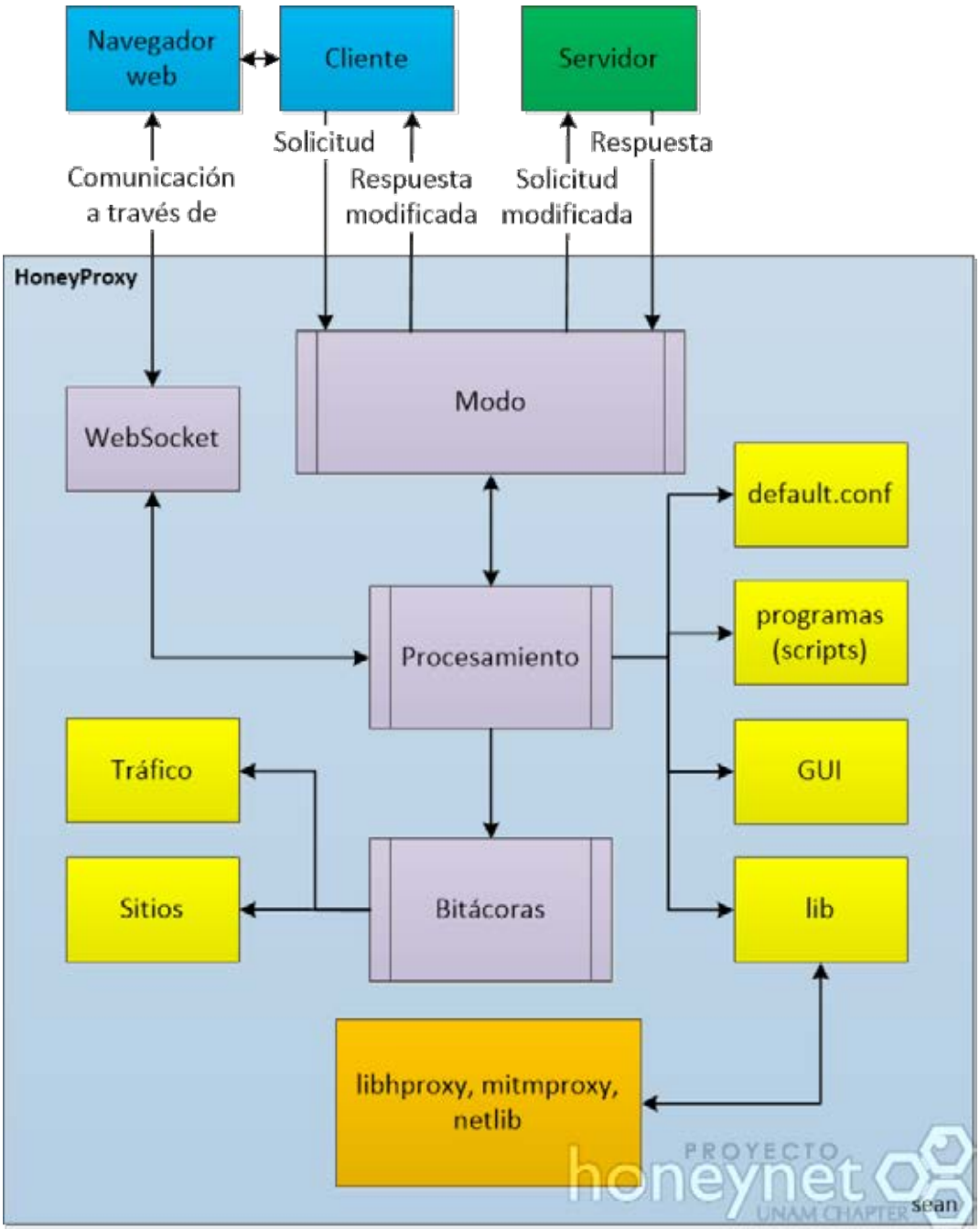


Figura 3. Panorama general de funcionalidad (de Sergio Anduin Tovar Balderas)

Prueba de concepto de HoneyProxy

En esta PoC se muestra la ejecución de HoneyProxy empleando diferentes opciones. Se presentará desde la forma básica para iniciar el proxy, el uso de diferentes tipos de autenticación y cómo modificar las solicitudes y respuestas.

Para presentar la capacidad para manipular las solicitudes del cliente y las respuestas del servidor que tiene HoneyProxy, se utilizarán las siguientes URL:

- Principal del servidor (http://lucas.honeynet.unam.mx): muestra el contenido de la página principal
- Ruta ip (http://lucas.honeynet.unam.mx/ip): muestra la dirección IP pública del cliente

Las siguientes figuras muestran las páginas que se utilizarán en la prueba de concepto.

Figura 4. Página principal

Al visitar la URL http://lucas.honeynet.unam.mx/ip se muestra la dirección IP pública del cliente.

Figura 5. Página para conocer la dirección IP pública del cliente

En la prueba de concepto se utilizará el puerto 8080 para el proxy, el 8081 para la interfaz web de HoneyProxy y se configurará manualmente el proxy en el navegador web. La configuración del proxy depende del navegador web (Chrome, Explorer, Edge, Opera, Safari, Firefox) que utilicemos. Es posible configurar HoneyProxy en modo transparente para que los usuarios no configuren su navegador.

Para configurar el proxy en Firefox se siguen los siguientes pasos: ingresar al menú, preferencias, avanzado, red, conexión, configurar, seleccionar la configuración manual del proxy, ingresar el nombre de dominio (honeyproxy.honeynet.unam.mx) o dirección IP (172.16.16.108) y puerto (8080).

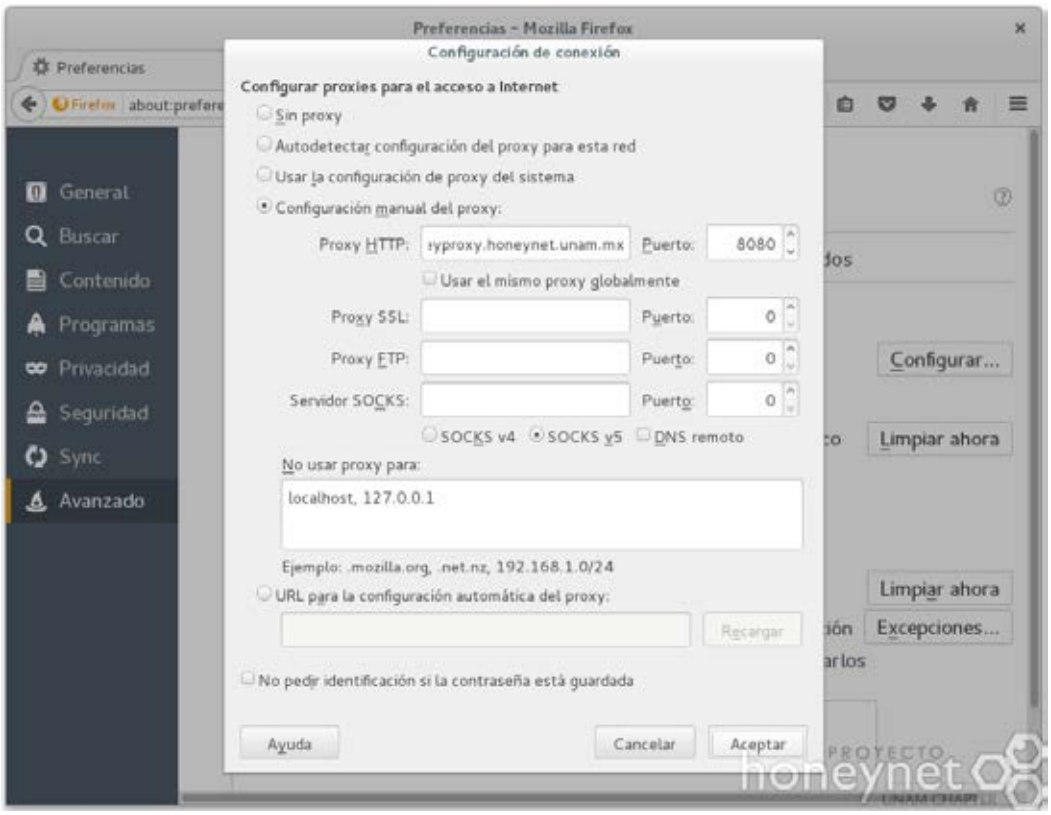


Figura 6. Configuración de un proxy en Firefox

Para iniciar HoneyProxy es necesario ejecutarlo a través de Python, si no se especifican opciones a través de la línea de comandos, emplea los valores preestablecidos. El proxy se encuentra en el puerto 8080 y la interfaz web en el puerto 8081, ambos sin autenticación (autenticación anónima).

Figura 7. Ejecución básica de HoneyProxy (autenticación anónima)

Esta forma de ejecución activa la autenticación en la interfaz web de HoneyProxy y en el proxy. Los datos de acceso para la interfaz web se muestran cuando inicia y para el proxy se permite autenticar con cualquier usuario y contraseña (autenticación no anónima).

Figura 8. HoneyProxy con autenticación no anónima

Se puede especificar el usuario (sean) y contraseña (lucas) en el proxy a través de la opción *singleuser*.

Figura 9. Autenticación para un usuario

La herramienta *htpasswd* sirve para crear y manipular un archivo de contraseñas, los archivos de autenticación básica del servidor HTTP Apache. Se crea un archivo de contraseñas con dos usuarios.

Figura 10. Creación de archivo de contraseñas

Es posible utilizar un archivo de contraseñas (autenticacionHoneyProxy) para especificar los múltiples usuarios que se podrán autenticar en el proxy.

Figura 11. Autenticación a través de un archivo de contraseñas

Como se mencionó anteriormente es posible emplear un archivo de configuración con nuestras configuraciones, en la siguiente figura se muestra cómo utilizar el archivo de configuración sean.conf.

Figura 12. Uso de archivo de configuración (sean.conf) personalizado

A continuación, se muestra cómo modificar la solicitud del cliente. En específico, se cambiará la URL http://lucas.honeynet.unam.mx/ip por http://lucas.honeynet.unam.mx. El proceso es el siguiente:

1. El cliente envía una solicitud (paso 1) HTTP para obtener (método GET) la página web con URL http://lucas.honeynet.unam.mx/ip.
2. HoneyProxy recibe la solicitud, la procesa y modifica (paso 2, solicitud modificada) para enviarla al servidor web y pueda atenderla (respuesta).
3. En los pasos 3 y 4 la respuesta del servidor viaja sin ser modificada, contiene la página principal.

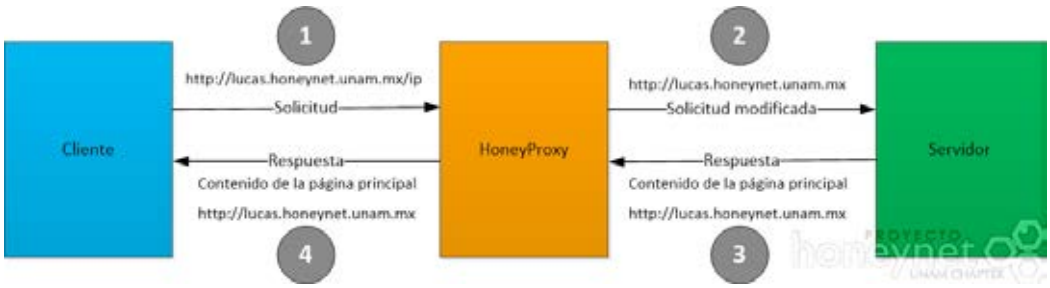


Figura 13. Proceso de modificación de la solicitud (de Sergio Anduin Tovar Balderas)

La opción *replace* permite reemplazar el patrón especificado y el argumento ~q sirve para que el patrón que se busca remplazar concuerde con la solicitud, se remplaza ip por una cadena vacía (quita la palabra ip de la URL).

Figura 14. Ejecución de HoneyProxy para remplazar la URL

Se puede observar que la URL contiene la ruta /ip pero el contenido muestra la página principal.

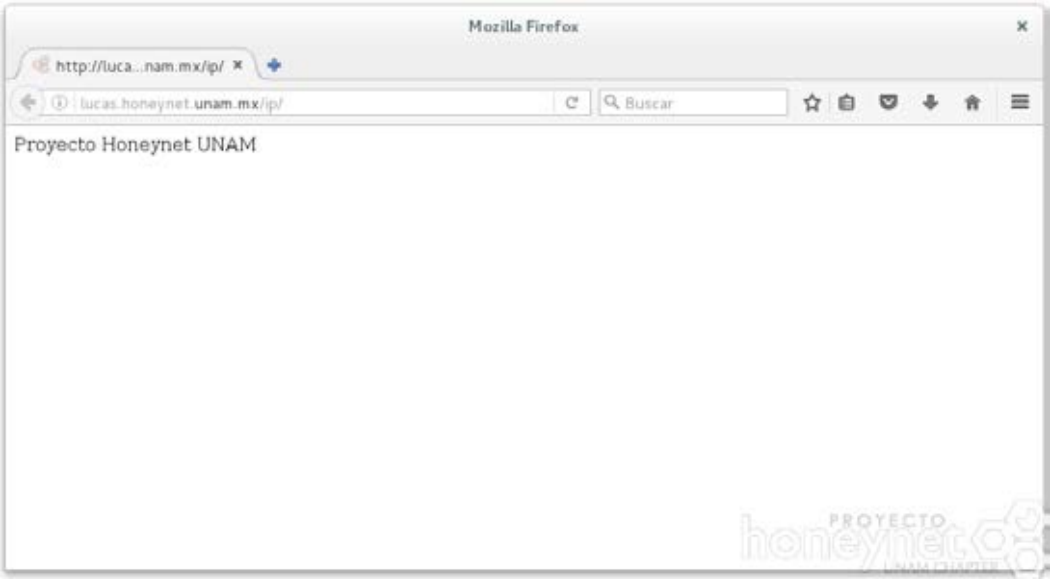


Figura 15. Navegador web del cliente con ruta /ip y contenido de la página principal

Las siguientes tres pruebas utilizan la opción *replace* en conjunto con el argumento ~s que permite remplazar el patrón que concuerde con la respuesta (respuesta modificada).

El campo Server del encabezado de respuesta del servidor web contiene información sobre el programa utilizado por el servidor como una descripción del tipo de sistema operativo e información de los módulos instalados.

Figura 16. Encabezado de respuesta del servidor

En esta primera prueba se sustituirá parte del encabezado de respuesta del servidor, en particular “Apache” por “Lucas Server”.

Figura 17. HoneyProxy modifica la respuesta del servidor (superior) y la solicitud del cliente y respuesta del servidor (inferior)

Siguiendo con las pruebas, esta modifica la respuesta del servidor (respuesta modificada) remplazando la imagen phu.png por unam.png.

Figura 18. HoneyProxy remplaza la respuesta del servidor por otra la imagen

Se puede apreciar la imagen original de la página http://lucas.honeynet.unam.mx/ip al inicio de la prueba de concepto.

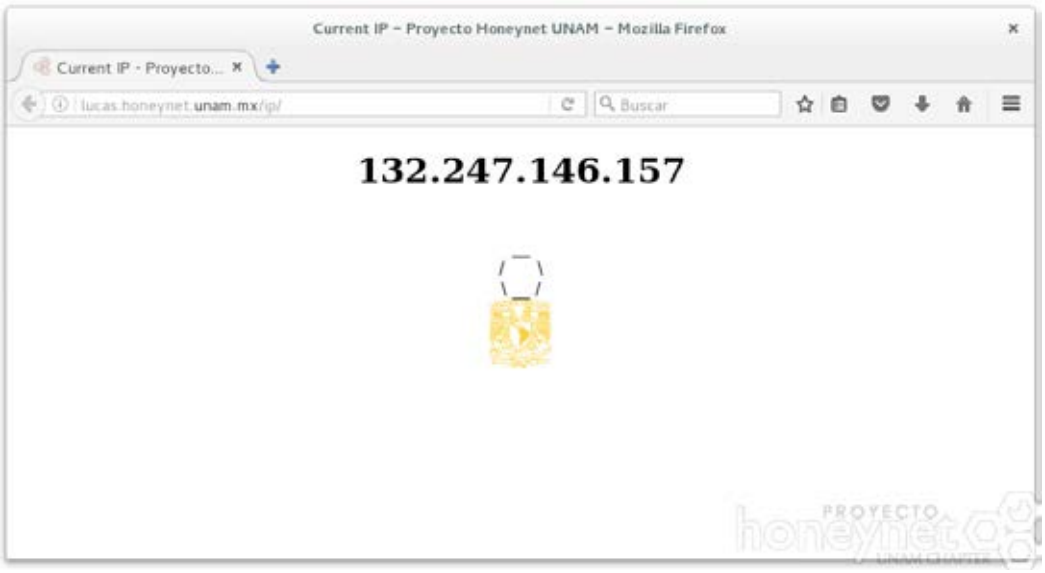


Figura 19. Navegador web del cliente con respuesta modificada (imagen del mismo servidor)

La última prueba remplaza la imagen phu.png por una URL que apunta a la imagen h-cert-logo.png que se encuentra en un servidor remoto, este remplazo es una respuesta modificada.

Figura 20. HoneyProxy remplaza la respuesta del servidor por otra imagen

Se puede observar que la imagen cambia y se encuentra alojada en otro servidor web.

Figura 21. Navegador web del cliente con respuesta modificada (URL externa)

Conclusiones

HoneyProxy es una herramienta que asiste a los investigadores de seguridad en el análisis de tráfico HTTP(S). Además, permite modificar las solicitudes y respuestas HTTP justo en el momento en el que son recibidas, para enviarlas al servidor durante el estudio de algún malware o aplicación web, mejorando la interacción al hacer más fluida la comunicación. Es posible utilizar programas (scripts) para tareas específicas que requiera el analista, así como especificar las opciones que requiera y guardar los eventos del análisis para mostrarlos como evidencia.

Conoce otras herramientas en nuestra página del Proyecto Honeynet UNAM.

Referencias

Hils, Maximilian. (2013). HoneyProxy. GitHub. Recuperado el 14 de diciembre de https://github.com/mhils/HoneyProxy

Tovar Balderas, Sergio Anduin. (diciembre 2017). Implementación de HoneyProxy. Proyecto Honeynet UNAM Chapter. Recuperado el 8 de enero de 2018. http://www.honeynet.unam.mx/es/content/implementacion-de-honeyproxy

Mozilla. (2018). Recursos y especificaciones de HTTP. Recuperado el 18 de enero de 2018 de https://developer.mozilla.org/es/docs/Web/HTTP/recursos_y_especificaciones

Si quieres saber más, consulta:

- Proyecto Honeynet UNAM
- Glastopf: Honeypot de aplicaciones web – I
- Glastopf: Honeypot de aplicaciones web – II
- Cowrie Honeypot: Ataques de fuerza bruta
- Conpot: Honeypot de Sistemas de Control Industrial
- Implementación del honeyclient Thug
- PoC: Captura de malware con el honeypot dionaea - parte i
- PoC: Captura de malware con el honeypot dionaea - ii
- Implementación de un spampot para la captura de correo electrónico no deseado
- Spampot para captura de correo electrónico no deseado - ii

- Ghost: honeypot para malware que se propaga a través de dispositivos usb - parte i
- Ghost: honeypot para malware que se propaga a través de dispositivos usb - parte ii
- Frameworks para monitoreo, forense y auditoría de tráfico de red – i
- Frameworks para monitoreo, forense y auditoría de tráfico de red-ii (PoC)

Sergio Anduin Tovar Balderas

Es egresado de la carrera de Ingeniería en Computación con módulo de salida en Redes y Seguridad por la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM).

Labora desde 2014 en la Coordinación de Seguridad de la Información (CSI/UNAM-CERT) en el área de Detección de Intrusos y Tecnologías Honeypot, donde lleva a cabo actividades de desarrollo, instalación y pruebas de tecnologías honeypot para análisis y detección de actividad maliciosa. Fue instructor de la línea de especialización Detección de Intrusos y Tecnologías Honeypot en el Congreso Seguridad en Cómputo UNAM 2014.

Egresado de la octava generación del Plan de Becas en Seguridad Informática de UNAM-CERT. Ha participado como instructor de nuevas generaciones en este mismo plan de capacitación. Laboró en el proyecto Seguridad en UNIX de la misma organización, además ha impartido cursos y participado en proyectos con dependencias de la UNAM y entidades externas del sector público.

Cuenta con la certificación IPS-ESE (*IPS Express Security for Engineers*) de Cisco.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNAM CERT®

Revista .Seguridad *Cultura de prevención para* TI
No.31 /mayo-junio 2018