ISSN 1870-4069

WannaCry: Análisis del movimiento de recursos financieros en el blockchain de bitcoin

Víctor Gabriel Reyes Macedo, Moisés Salinas Rosales

Instituto Politécnico Nacional,
México

vg.reyesmacedo@gmail.com, msalinasr@ipn.mx

Resumen. Un ransomware es un tipo de malware mediante el cual un atacante extorsiona al usuario de un equipo de cómputo para que éste le realice un pago que generalemente es operado en el sistema Bitcoin. Este estudio pretende medir el movimiento de los flujos de pago correspondientes a ataques del ransomware *WannaCry*, con el objetivo de proporcionar información sobre los métodos que utilizan los cibercriminales para mover y ocultar el rastro de los recursos financieros resultantes en el blockchain de Bitcoin.

Keywords: ransomware, bitcoin, cibercrimen, WannaCry.

WannaCry: Analysis of Financial Resources Movements for Bitcoin Blockchain

Abstract. A ransomware is a type of malware through which an attacker extorts the user of a computer system, so that he can make a payment that is generally operated in the Bitcoin system. This study aims to measure the payment flows corresponding to ransomware *WannaCry*, in order to provide information about methods used by cybercriminals to move and hide the trace of the financial resources on Bitcoin Blockchain.

Keywords: Ransomware, Bitcoin, Cybercrime, WannaCry, Networks Analysis.

1. Introducción

El 12 de mayo de 2017, miles de computadoras alrededor del mundo fueron infectadas de manera simultánea por un tipo de malware conocido como *ransomware*, cuyo objetivo consiste en cifrar la información resguardada en un equipo de cómputo y exigir un pago a cambio de la herramienta de descifrado

para recuperar los archivos comprometidos. En este caso los atacantes pidieron un pago de aproximadamente $300 USD por cada equipo infectado.

Durante este ataque se vieron afectadas empresas, instituciones educativas, hospitales y oficinas de gobierno entre otras en alrededor de 100 países, convirtiéndose así en la mayor infección por ransomware de la historia.

No obstante, no es la primera vez que algo así sucede, ya que durante los últimos 5 años este tipo de infecciones se han incrementado en 400 % [9].

En general, el pago de estos rescates es operado mediante el sistema Bitcoin[10], que entre otras cosas ofrece a los atacantes la ventaja de ser un sistema *pseudo-anónimo*[4] pues si bien los pagos no están vinculados con personas en particular, si quedan registrados en el *blockchain* del sistema, que funciona como un registro histórico de todas las transacciones que se ejecutan. Esta característica ha permitido llevar a cabo estudios sobre la verdadera capacidad de anonimato en el sistema.

Este documento presenta los avances de una propuesta de análisis de los pagos asociados a este tipo de ciberdelito tomando como caso de estudio el malware conocido como *WannaCry*, del cual se toma como objeto de estudio la forma en que distribuye los recursos captados luego del ataque global y la manera en que, a través de la red de Bitcoin, procede al blanqueo del capital obtenido, utilizando durante el proceso algunas estrategias para maximizar en la medida de lo posible su anonimato.

En la segunda sección de este artículo se abordan de manera general los antecedentes necesarios para comprender la amenaza y el modo de operación del ransomware así como la idea general del funcionamiento del sistema Bitcoin.

En la tercera sección se presenta el contexto del caso de estudio que ocupa a este documento, además discute la metodología utilizada para llevar a cabo el análisis y la recolección de los datos.

Finalmente se presentan los resultados y conclusiones del caso, con el objetivo de aportar información que coadyuve a los esfuerzos internacionales por detener esta modalidad de delito.

2. Antecedentes

Si bien las primeras amenazas de ransomware datan de 1989 [11], es a partir del año 2013 que el número de ataques de este tipo se ha incrementado más de un 500 % [5]. Dada la tasa de incremento que se ha observado, resulta importante comprender a fondo este fenómeno para lo cual se pone un breve contexto a continuación.

2.1. Ransomware: Una amenaza cibernética

El modo frecuente de infección por ransomware es mediante la descarga de archivos de procedencia desconocida. Un escenario común es en empresas en las que los empleados reciben un correo con un archivo adjunto que resulta tener el

malware oculto, o bien instalan complementos que incluyen el malware oculto. Una vez descargado, éste se ejecuta y comienza con la extorsión.

Diversos portales web especializados señalaron al ransomware como la amenaza más importante del año 2016 dado el incremento que este tipo de malware tuvo a nivel mundial generando situaciones que podrían poner en peligro vidas humanas, pues entre sus objetivos existen equipos de cómputo en hospitales que contienen información sensible.

Por su forma de operar se propone una clasificación en tres tipos:

1. **De Bloqueo:** Es un tipo de ransomware que impide el funcionamiento normal de un dispositivo, impidiendo al usuario hacer uso de éste. Es posible encontrar esta variación en el entorno *IoT* y uno de los más casos más comúnes ha sido el llamado *virus policía*.
2. **De Cifrado:** Es la variedad más común y tal vez la más conocida. Como ya es sabido, cifra los archivos de una amplia variedad de extensiones, cubriendo prácticamente todos aquellos relacionados con la vida personal de las víctimas o con sus actividades laborales o de negocios. Incluso ha evolucionado para cifrar discos duros.
3. **De Control:** Particularmente peligroso, toma el control de sistemas completos (que pueden ir desde la apertura electrónica de puertas en un edificio hasta plantas de potabilización de agua) hasta recibir el pago solicitado.

Uno de los casos más estudiados es el de *CryptoLocker*, el cual se dió a conocer el 5 de septiembre de 2013 siendo un tipo de malware distribuído a través de correo electrónico spam [7] y que durante su período de actividad logró recaudar cerca de $1.1 millones de dólares [12], con lo cual se convirtió en el mayor ataque en su tipo hasta ese momento, siendo superado en número de infecciones por *WannaCry* en 2017.

El beneficio financiero que representa el uso de ransomware para los ciberdelincuentes ha propiciado la aparición en la *deep web* de servicios de infección por este medio sobre pedido, de la misma forma que otros servicios ilegales pueden ser adquiridos y los cuales son pagados comúnmente mediante una comisión sobre los pagos generados por la infección.

Una propuesta de identificación de ransomware en la red de Bitcoin se muestra mediante la aplicación de BitIodine [12] en la cual el autor logra agrupar en un clúster todas las direcciones asociadas a *CryptoLocker*.

2.2. Sistema de pagos electrónicos *Bitcoin*

Bitcoin es un sistema de pagos electrónico con base en una red *peer to peer* propuesto en 2009 por Satoshi Nakamoto [10].

Su arquitectura consiste en:

- Participantes,
- Transacciones,
- Blockchain.

Los **participantes** son *los usuarios* quienes usan Bitcoin como medio de pago para comerciar y *los mineros* quienes validan las transacciones y emiten monedas.

Las **transacciones** en el sistema se llevan a cabo con la interacción de tres elementos: las *direcciones*, *las llaves* y un *wallet*. Las direcciones son identificadores compuestos por cadenas de entre 27 y 31 caracteres alfanuméricos generados mediante protocolos de criptografía asimétrica, por lo que a cada dirección le corresponde una *llave pública* y una *llave privada*. Su función es similar a la de una cuenta bancaria, en la que se pueden enviar y recibir bitcoins. Cada usuario puede tener tantas direcciones como necesite, y para administrarlas es necesario contar con un *wallet* que, de manera básica, es la colección de llaves que dan acceso a las direcciones del usuario.

Suponga que se desea hacer una transacción entre los usuarios A, que enviará 1 BTC y B quien lo recibirá. Entonces el usuario B debe indicar una dirección para recibirlo, por ejemplo `12BF3DZaoq5sCHLQGDgNqUBrKChM2tXvq9`. El usuario A accederá a su *wallet*, e ingresará el monto a enviar y la dirección de destino, y el *wallet* tomará 1 BTC de alguna de las direcciones a las que tiene acceso para poder completar la transacción.

El **blockchain** es el registro histórico de todas las transacciones que se llevan a cabo. En éste, quedan asentados los montos, las direcciones de origen de los recursos, las direcciones de destino, el momento en el cual se realiza un pago y un ID para cada transacción. Todas las transacciones se organizan por conjuntos llamados *bloques*.

El lector podrá encontrar una exposición detallada del funcionamiento del sistema Bitcoin en [2].

Las características que hacen a este sistema atractivo a los ciber delincuentes son la cotización que ha pasado en un año de un aproximado de $800 USD a alcanzar los $4340 USD [1] y la posibilidad de generar transacciones de manera fácil, económica, rápida y global y que no están directamente vinculadas a ninguna persona. Además los pagos son irreversibles, por lo que no hay posibilidad de cancelar una transacción.

No obstante, si una dirección fue asociada de manera pública a una entidad, sí es posible señalarla como tal. Es el caso, por ejemplo, de algunas fundaciones que reciben donaciones en Bitcoin, para lo cual hacen pública la dirección y por ello se sabe a quién pertenece. Algo similar sucede con los ataques de ransomware, los cuales indican a las víctimas a qué dirección deben de realizar sus pagos, con lo que es posible asegurar que tales direcciones pertenecen a la entidad responsable del ataque.

3. Presentación del caso: WannaCry

Como se dijo anteriormente, el ataque mediante el ransomware WannaCry ha sido uno de los más agresivos de la historia, por lo que se decidió utilizar

[1] https://poloniex.com/exchange#btc_xrp al 25 de agosto de 2017 18:39 hrs GMT-5

este caso como referencia para plantear un análisis de la forma en que maneja los recursos captados en la red de Bitcoin. Este ataque en particular aprovechó una vulnerabilidad de los sistemas operativos de Microsoft, entre ellos los Microsoft Windows 7, 8.1 y 10, así como Microsoft Windows Vista SP2 y Server 2008/2012/2016 que no contaban con la actualización necesaria para corregir la vulnerabilidad que el malware aprovechó[2].

Después de captar los recursos, las direcciones permanecieron sin movimientos hasta el día 3 de agosto de 2017.

4. Recolección de datos

Para iniciar el proceso de análisis se consideraron tres direcciones abiertamente asociadas a WannaCry (sobre las cuales se pedía realizar el pago del rescate) obtenidas en `bitcointalk.com`, a las cuales llamaremos en adelante direcciones semilla[3], siendo las siguientes:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Posteriormente se recogieron datos sobre las transacciones en dichas direcciones, primero mediante el uso de la herramienta `rusty-blockparser` desarrollada por Michel Spagnuolo como una versión mejorada de `BitIodine`[12]. Con dicha herramienta se obtuvieron los datos correspondientes al TxID (ID de la transacción), fecha, hora, monto y destino de la transacción. Mediante un análisis en `blockchain.info` se obtuvieron también las direcciones de origen.

Los datos de las transacciones consideradas corresponden al período comprendido entre el 12 de mayo y el 18 de agosto de 2017, que es el mismo período comprendido entre el inicio del ataque y el momento en que se pierde el rastro de los fondos debido a que éstos entraron en servicios de exchange que entre otras cosas reciben miles de transacciones en una misma dirección y dispersan los fondos en diferentes montos a una gran velocidad.

Cabe mencionar que las transacciones que se usaron para el análisis son aquellas que se ejecutaron después de la dirección semilla. Se considera que las direcciones que alimentaron a las semillas pertenecen a las víctimas del ataque, por lo que no son relevantes para el estudio del flujo de recursos en la red. No obstante fueron útiles para conocer los montos promedio de pagos de rescate así como los horarios y fechas en que dichos pagos fueron hechos.

Para un mejor análisis, los datos obtenidos se concentraron en un archivo .csv en el cual se detallaron aspectos como la fecha y hora del pago, la dirección de origen, la dirección de destino, el ID de la transacción y el monto enviado o recibido para cada dirección.

[2] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[3] https://bitcointalk.org/index.php?topic=1916199.0

5. Medición

Como herramientas de medición se utilizó un software libre llamado *Gephi*[4]. Además se hizo un análisis con enfoque estadístico para extraer características como las medidas de centralidad y dispersión de los pagos y posibles correlaciones que puedan existir entre los flujos de bitcoins que realizan los responsables de un ransomware y la cotización de la moneda. A continuación se presentan los resultados de las mediciones con ambos enfoques.

5.1. Enfoque en redes

El estudio de las transacciones en la red de Bitcoin implica generar la **matriz de adyacencia** correspondiente, en la cual cada entrada se define con valor 1 si las direcciones se conectan al enviar o recibir recursos, o con un 0 en caso contrario.De manera formal, la matriz de adyacencia $A(G) = (a_{ij})$ de una red $G = (X, E)$ se define de la siguiente forma:

$$a_{ij} = \begin{cases} 1 \ si\{i,j\} \in E, \\ 0 \ si\{i,j\} \notin E. \end{cases} \tag{1}$$

En donde X es el conjunto de direcciones Bitcoin (que tomarán el papel de nodos en la red) y E es el conjunto de transacciones (que para efecto práctico representan los enlaces dirigidos de la red). A partir de la construcción de esta matriz, es posible medir los siguientes parámetros.

El **grado de un nodo** es una medida de centralidad que describe la estructura de una red en términos de la conectividad individual de los nodos, es decir, el número de enlaces con los que conecta.

Si el resultado es un valor numérico alto, se considera que el nodo está bien conectado con la red. Si el valor numérico es bajo, entonces se dice que el nodo tiene una conexión débil. Este valor indicaría, de manera práctica, las veces que se usa una dirección Bitcoin tanto para recibir pagos como para realizarlos. En este caso el valor promedio obtenido en la muestra de direcciones es de 1.053 lo cual indica que cada dirección se usa en promedio una vez, es decir, recibe un pago y realiza un pago para luego no volver a ser utilizada. Esto coincide con algunas recomendaciones de privacidad [4] que sugieren hacer uso de cada dirección una vez y durante períodos cortos para maximizar el nivel de anonimato.

La **longitud de ruta** es el número de pasos que toma llegar de un punto A a un punto B de la red.

Esta cantidad tiene un valor bajo para vértices cuya separación respecto a otros es corta, lo que significa que el flujo a través de ellos es más rápido. En [3] asocian los valores altos de este parámetro en la red de Bitcoin a actividades posiblemente ilegales, toda vez que para ocultar el rastro de información y pasar desapercibidos los ciberdelincuentes hacen pasar los pagos por varias direcciones a través de una ventana de tiempo relativamente pequeña. El valor obtenido en este parámetro durante la medición es de 3.9180, es decir, los fondos obtenidos

[4] https://gephi.org/

se trasladaron en promedio a través de aproximadamente 4 direcciones antes de llegar a su destino final. La ruta más larga encontrada fue de 11 pasos.

En ciertos casos, es posible que no existan rutas entre un par de vértices de una red. Incluso, es posible que en una red existan subconjuntos de nodos entre los cuales no existe una ruta. A una red con esta característica se le conoce como *red no conectada*. Los grupos de vértices en una red no conectada son conocidos como **componentes de la red** y se definen como un subconjunto de los vértices tales que existe al menos un enlace entre los miembros del subconjunto y ningún otro nodo pueda ser agregado si se conserva esta propiedad[6]. En términos más sencillos, son grupos de nodos aislados y son una referencia de qué tan fuertemente conectada está la red. En la medición realizada, el resultado obtenido es de 1386 componentes débilmente conectados, lo que indicaría una red sumamente débil en la que básicamente cada nodo es por sí mismo un componente.

La centralidad del eigenvector es la extensión de la medida de centralidad de los nodos. Su valor indica el nivel de conectividad de un grupo de nodos respecto al resto de la red. El valor obtenido mediante 100 iteraciones es de 0.1092 y al correr mil iteraciones fue de aproximadamente 0.05, con tendencia a ser menor mientras mayor sea el número de iteraciones. Este resultado indica que en realidad la dispersión que realizan los responsables evita que haya nodos que mantengan mayor influencia en la red, contrario a una suposición inicial en la que se consideró que habría oportunidad de identificar nodos con mayor conectividad para realizar la dispersión.

5.2. Enfoque estadístico

De los resultados estadísticos, se obtuvo que el monto promedio de los rescates fue de 0.14751963 BTC con una desviación estándar de 0.143762402 BTC, es decir un aproximado de $ 266 USD cada pago a un tipo de cambio promedio de $1,840.86468 USD/BTC con desviación estándar de $237.15 USD. El rango de los pagos fue desde 0.00000563 BTC hasta 1.999 BTC.

De las direcciones semilla aquí analizadas, los responsables del ataque obtuvieron 51.92690943 BTC que equivale aproximadamente a $95,590.4135112 USD al tipo de cambio promedio, este dato coincide con lo señalado en diferentes medios informativos en los que se ha hablado de que el monto final no fue tan grande como se habría esperado de un ataque global.

Además, contrario a una suposición inicial, no se observó correlación entre los pagos de rescate a WannaCry y la cotización del bitcoin. Tampoco hay signos de correlación entre la cotización de la moneda y los movimientos de recursos encontrados en la red, por lo que se puede descartar la posibilidad de que los responsables hayan comenzado a mover el dinero de los rescates desde las semillas hasta sus destinos finales orientados por un alza en precios, o visto desde otra perspectiva, es posible descartar que el movimiento de flujos y el mismo ataque tuvieran influencia en el precio de la moneda.

6. Conclusiones

Estas direcciones presentaron indicios del proceso conocido como *peeling chain* descrito por Sarah Meiklejohn en 2013 [8], mediante el cual se lleva a cabo la dispersión de fondos a través de pagos por montos pequeños. El propósito de esto es dificultar el rastreo de los recursos. Es frecuente encontrar esta característica en flujos de bitcoins asociados con actividades sospechosas, y una forma de medirlo es mediante la longitud de ruta, que es una medida de la eficiencia en el transporte de la información. Para el caso que nos ocupa, este valor resultó en un valor promedio de 3.98, que debe verificarse contra los valores de muestras adicionales de ransomware.

Se observa además que el grado de los nodos (las direcciones bitcoin) utilizados por WannaCry tiene un valor promedio de 1.084, que indicaría que las direcciones usadas permanecen activas por períodos cortos y son poco reutilizadas. Esta característica es un indicativo de posible actividad sospechosa debido a que la actividad breve es difícil de rastrear[4].

También se concluye que la red formada por las direcciones involucradas en este estudio es una red débilmente conectada, en la que la mayoría de los nodos se mantienen aislados.

El rastreo arrojó además que para el caso de WannaCry los fondos entraron a servicios de *exchange* y *trading* ofrecidos por las operadoras más importantes del mundo, entre las identificadas se encuentran *Poloniex*, *HitBTC.com*, *BitStamp*, *Huobi*, *WhaleClub*, *Mercado Bitcoin* y *ShapeShift*. Este resultado es importante debido a que con el apoyo de autoridades y empresas, se pueden dar pasos en la dirección de prevenir este tipo de actividades. La identificación se hizo mediante la plataforma `https://www.blockseer.com/`.

Por último cabe señalar que, según los resultados de esta muestra, el ataque de WannaCry no influyó de manera significativa en la cotización de la moneda de Bitcoin, y que las variaciones de dicha cotización tampoco parecen haber afectado o influído en la dispersión de los fondos obtenidos.

7. Trabajo futuro

Para finalizar con esta investigación debe tomarse una muestra aleatoria de direcciones bitcoin que correspondan al mismo período analizado para WannaCry, con la finalidad de comparar comportamientos sospechosos con usuales. También se requiere someter los datos a un análisis estadístico con la finalidad de detectar patrones de comportamientos en cuanto al proceso de *peeling chain* y a los timestamps, con la finalidad de detectar las zonas horarias en la que se realizan los pagos y establecer con ello un marco de referencia.

Referencias

1. Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. International Conference on Financial Cryptography and Data Security, pp. 34–51 (2013)

2. Antonopoulos, A. M.: Mastering Bitcoin: unlocking digital cryptocurrencies. (2014)
3. Baumann, A., Fabian, B., Lischke, M.: Exploring the Bitcoin Network. WEBIST (1), pp. 369–374 (2014)
4. Herrera-Joancomartí, J.: Research and challenges on bitcoin anonymity. In: Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, pp. 3-16 (2015)
5. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E.: Cutting the Gordian knot: A look under the hood of ransomware attacks. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 3–24 (2015)
6. Lewis, T. G.: Network science: Theory and applications. (2011)
7. Liao, K., Zhao, Z., Doupé, A., Ahn, G. J.: Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin. In: Electronic Crime Research (eCrime) APWG Symposium, pp. 1–13 (2016)
8. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 conference on Internet measurement conference, pp. 127–140 (2013)
9. Nieuwenhuizen, D.: A behavioural-based approach to ransomware detection. pp. 1–3 (2017)
10. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. (2008)
11. Smith, J.: Ransomware Incident Response for Law Enforcement. Doctoral dissertation, Utica College (2017).
12. Spagnuolo, M., Maggi, F., Zanero, S.: Bitiodine: Extracting intelligence from the bitcoin network. In: International Conference on Financial Cryptography and Data Security, pp. 457–468 (2014)