Métodos y Técnicas del Atacante para Ocultar su Identidad en la Red

Guillermo Suarez de Tangil Rotaeche (Investigador Contratado), Esther Palomar (Profesor Ayudante), Arturo Ribagorda Garnacho (Catedrático de Universidad), Benjamín Ramos Álvarez (Profesor Titular de Universidad)

SeTI - Grupo de Seguridad en las T.I., Departamento de Informática, Univ. Carlos III de Madrid

Avda. Universidad 30, 28911 Leganés, Madrid

Teléfono: 0034 91 624 94 22 Fax: 0034 91 624 91 29

gtangil@pa.uc3m.es, {epalomar, Arturo, benja1}@inf.uc3m.es

Resumen. Desde los inicios del *malware*, entre los objetivos del atacante se han encontrado camuflar su identidad y localización en la red. Para ello, los atacantes hacen uso tanto de las técnicas tradicionales basadas en la manipulación de elementos de TCP/IP como de los métodos más modernos creados para proporcionar anonimato en Internet. De hecho, con la creciente investigación y mejora de los esquemas de anonimato destinados a proteger los derechos de usuarios honestos de la red, los usuarios maliciosos se ven indudablemente beneficiados. En este artículo se describen tanto los primeros métodos como las técnicas más actuales empleadas por el atacante con el fin de proteger su identidad. Se señala, además, la necesidad de proporcionar anonimato a los usuarios de la red pero sin procurar nuevas vulnerabilidades que favorezcan a objetivos maliciosos.

Palabras Clave. Identidad del Atacante, *Malware*, Anonimato, Localización del Ataque, Ocultar y Camuflar la Identidad.

1. Introducción

Desde su aparición, los objetivos de lo que hoy conocemos como *malware*, y como consecuencia el comportamiento de estas técnicas maliciosas, ha evolucionado enormemente. Véase como ejemplo uno de los primeros virus reconocido como tal, el denominado *Creeper* [1, p. 10], que fue concebido con un objetivo muy simple: llamar la atención. Su comportamiento se limitaba a imprimir por pantalla el siguiente mensaje: "*I'm a creeper... catch me if you can!*". Fue a partir de los años 80 cuando se comenzó a diseñar software con objetivos maliciosos y el momento en el cual el atacante manifiesta "el no ser detectado" como una necesidad prioritaria. La cosa cambia cuando la ley empieza a juzgar y condenar a los primeros creadores de virus (véase el caso de Robert Tappan Morris [14], condenado en 1990 a cuatro años de prisión por la creación de un virus difundido a través de *ArpaNet*).

Más tarde, el atacante trata de camuflar su identidad y su localización en la red, buscando impunidad sobre las consecuencias legales que pudieran ser derivadas de sus actos. Algunos de dichos actos deshonestos son, por ejemplo, los ataques conocidos como negación de servicio (*DoS*) y el envío masivo de correo no deseado (*Spam*), entre otros.

Con el fin de proteger su identidad, el atacante ha empleado diversos mecanismos, en general diseñados específicamente para cada ataque. Unos más efectivos que otros, algunos válidos para un determinado tipo de ataque y otros no. Se han utilizado, por tanto, mecanismos propios como la manipulación de elementos de las capas inferiores del protocolo de comunicación. Así mismo, dependiendo del impacto del ataque, los atacantes pueden determinar el nivel de anonimato necesario. Hoy en día existen mecanismos más modernos para proporcionar anonimato a usuarios legítimos de la Red y que se convierten, a su vez, en un arma potencial para el usuario deshonesto. En este artículo, se revisan tanto los primeros métodos como las técnicas más actuales de protección de la identidad del atacante.

Estructura del documento. La Sección 2 se centra en revisar las técnicas tradicionales usadas por los atacantes para ocultar su identidad. Seguidamente se detallan las técnicas modernas de anonimato disponibles para ocultar la localización ergo la identidad se describen en la Sección 3. Finalmente, se presentan las conclusiones y consideraciones más relevantes.

2. Formas tradicionales del atacante para ocultar su identidad en la red

Tal y como se define en [4], el anonimato permite ocultar los elementos o atributos que pueden identificar la transacción y/o las partes que se comunican. De esta forma, si un atacante quiere permanecer en el anonimato ha de procurar bien de ocultar los elementos que sirvan para la detección del ataque o bien de ocultar el origen de la comunicación. Por ejemplo, en el caso del despliegue de una botnet, el atacante no suele preocuparse necesariamente de ocultar las acciones de los bots, sin embargo sí debe de procurar que la comunicación entre su equipo y la máquina maestra sea anónima.

2.1 Visión general

En la actualidad existen gran cantidad de herramientas de libre disposición en la Red que ayudan a rastrear la fuente de una actividad de red sin requerir un esfuerzo elevado, ni de recursos máquina ni de conocimientos técnicos; y el atacante lo sabe. En primer lugar, es necesario detectar y registrar el evento de seguridad. En términos generales, las herramientas antivirus proporcionan una interfaz amigable para dichos procesos de monitorización de eventos. Seguidamente, en algunas ocasiones se requiere involucrar a las autoridades y/o al proveedor de servicios de Internet (ISP). Éste suele ser un proceso lento, especialmente cuando es necesario involucrar a las autoridades de varios países, debido principalmente a las diferencias legales existentes en lo referente a la protección frente a delitos informáticos.

En caso de que el atacante haya lanzado el ataque a través de un *proxy* o desde una máquina *zombi* (otra máquina controlada por él y sin autorización del dueño) el proceso de localización se complica enormemente, especialmente si en la máquina controlada no se ha establecido el registro de los eventos de seguridad. En concreto, es muy común que los atacantes usen equipos infectados para hacer de pasarela entre su máquina y el destino de la comunicación, usando para ello métodos *proxy* como son [2]: redirección genérica de puertos (como por ejemplo GRE, *Generic Routing Encapsulation*, *tunneling* [3]), HTTP *proxy*, *Socks proxy*, canales IRC (*Internet Relay Chat*). La complejidad cada vez es menor debido a la proliferación de la redes inalámbricas abiertas o con una protección débil, como es el caso de las redes cifradas mediante WEP (*Wired Equivalent Privacy*) [5].

Dentro del escenario jurídico, cada vez son más las iniciativas para mejorar los marcos legales aplicables contra el uso de *malware*. A día de hoy, existen tanto leyes penales como normativas generales que castigan el uso del *malware* [1, p. 81]. Existen también varios grupos de trabajo, como los creados por la *Red Internacional de Cumplimiento Normativo y Protección de los Consumidores* (ICPEN), que tienen como objetivo el poder intercambiar información sobre delitos informáticos acometidos en otros países y poder así aplicar la ley contando con un mayor número de evidencias. Alguno de estos grupos son el Grupo de Trabajo del Fraude de Comercialización Masiva, el Grupo de Trabajo de Mejores Prácticas y el Grupo de Trabajo *ScamWatch*, entre otros.

A continuación, para poder comprender cómo un ataque puede ser rastreado desde su destino hasta su origen, así como para facilitar el entendimiento de los siguientes apartados, se presenta una visión general de los problemas de seguridad en TCP/IP. Posteriormente se presentan algunas técnicas las cuales, a partir de la manipulación de elementos de TCP/IP, proporcionan a un atacante diferentes grados de anonimato.

2.2. Problemas de seguridad en TCP/IP

Internet es una red pública basada en la familia de protocolos TCP/IP. Dichos protocolos fueron diseñados con un grado de fiabilidad muy elevado primando la interconectibilidad entre redes y sistemas heterogéneos y dejando a un lado importantes pilares de la seguridad (agujeros que tratan de ser corregidos con *IPsec, Internet Protocol Security*, de cara a la versión 6 de IP aunque aplicable a la versión más extendida, la versión 4). En concreto, muchos de estos fallos existen debido a que los equipos confían en la dirección origen del paquete IP como mecanismo para autenticar el origen de la conexión. Así mismo, los mecanismos de control de tráfico, en concreto los protocolos de encaminamiento, carecen de mecanismos fiables de autenticación.

Por otro lado, tanto los equipos de una red como los propios encaminadores establecidos entre el inicio y el final de la comunicación, pueden ver tanto el origen como el destino. De hecho, pueden incluso modificarla, dando lugar al conocido ataque denominado *IP Spoofing* [19]. En definitiva, la familia de protocolos TCP/IP presenta un conjunto de problemas de seguridad intrínsecos al diseño del protocolo, que facilitan a los atacantes mecanismos para ocultar su identidad, entre otros. El lector interesado

podrá encontrar en [6] un análisis exhaustivo de los problemas de seguridad asociados a la familia de protocolos TCP/IP.

2.3 Manipulación de los elementos TCP/IP

Se identifican dos tipos de comportamientos comunes en los atacantes. En primer lugar, se distinguen aquellos ataques que tratan de ocultar las evidencias que genera el ataque o camuflar sus acciones de tal forma que la víctima no se percate de que se está llevando a cabo el ataque. En esta categoría se enmarcan todos aquellos que tratan de ocultar el ataque para no ser detectado. De esta manera, la identidad del atacante permanecerá en el anonimato [7]. Un ejemplo es el trabajo presentado en [8] basado en el uso de mecanismos tipo *FIN Scanning* para evitar que sean registradas las sesiones TCP.

En segundo lugar, se consideran aquellos ataques que tratan de modificar algún elemento del paquete IP para que el atacante no pueda ser identificado. En esta categoría se encuentra el clásico ataque por falsificación de la IP (*IP Spoofing*) en el que el atacante falsifica el campo origen del paquete IP antes de ser enviado a su destinatario (véase la Ilustración 1). De esta forma el atacante puede enviar paquetes de red sin dejar evidencia del origen. Las limitaciones de esta técnica son obvias, si el atacante cambia el campo origen del paquete, en principio no va a recibir ningún paquete de vuelta, haciendo únicamente posible un ataque del tipo *DoS* o, en algunos casos, una prospección de puertos [9, p. 195].

3. Métodos modernos de anonimato usados por los atacantes

Consecuencia de la creciente necesidad impuesta por los usuarios de las tecnologías de la información, la investigación en el área de procurar anonimato en Internet ha seguido un ritmo creciente en los últimos años. Indudablemente los creadores de *malware* se han beneficiado de los avances producidos en esta línea. A continuación, se presenta una visión general de dichas tecnologías, así como una muestra de ataques conocidos basados en las mismas.

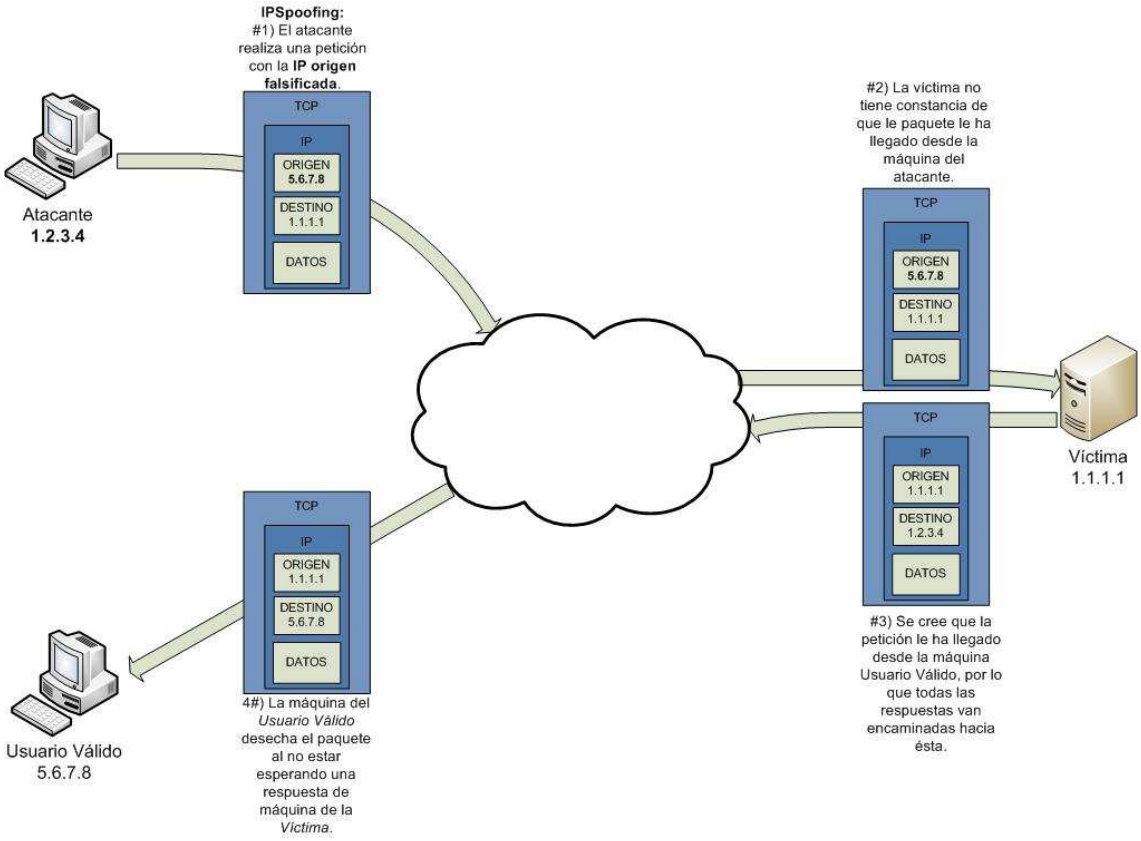

Ilustración 1: IP Spoofing. En la figura se muestra cómo el atacante falsifica el campo Origen de la trama IP para que no conste como origen de la comunicación.

3.1 Visión General: Tecnologías de anonimato

Existen varios tipos de anonimato, según quién o qué permanece anónimo durante la comunicación. Puede ocultarse al identidad del emisor, el receptor o la vinculación existente entre ambos. Identificamos dos tecnologías de anonimato [4]: los *sistemas basados en retransmisores* y los *sistemas basados en encaminamiento aleatorio*.

En el primer grupo, el retransmisor es una entidad centralizada con funciones de *proxy*, como por ejemplo el conocido *Anonymizer* para tráfico http [18]. Quizás los sistemas más populares de este grupo son los basados en las *redes Mix* introducidas por David Chaum en [10]. Una red *Mix* establece la comunicación con el destinatario a través de un conjunto de encaminadores (servidores *proxies*) cifrando el mensaje en varios tiempos, con cada una de las claves de estos encaminadores. El mensaje queda "envuelto" por varias capas como si de una cebolla se tratase. La red ***Tor*** (*TCP based*

Onion Routing) es una de las más populares, en la que cada salto negocia una clave simétrica con el siguiente encaminador. La ilustración 2 muestra el esquema de una red TOR y la construcción de los mensajes transmitidos entre los nodos TOR. ***Mixmaster***, **Buses**, ***Mixonion***, ***MorphMix***, ***Pipenet***, ***Babel*** y ***Tarzan*** son otros ejemplos.

Por otro lado, ***Crowds***, ***Freenet*** y ***Onion Routing*** son sistemas basados en encaminamiento aleatorio cuyo objetivo es ocultar el origen de la transmisión enviando los fragmentos del paquete IP por distintos caminos elegidos aleatoriamente.

3.2 Ataques Conocidos

Presentamos a continuación los ataques más conocidos basados en los métodos de anonimato descritos en el apartado anterior:

- Basados en **Tor**: Los autores en [11] aseguran que operadores de IRC (mecanismo usado por la mayoría de las *botnets* para comunicar la máquina maestra con los *bots*) han informado de *botnets* cuyos zombis han recibido conexiones provenientes de nodos **TOR**. De hecho, muchos operadores IRC han decidido bloquear el acceso desde redes TOR mientras que otros han decidido facilitar el acceso [12].

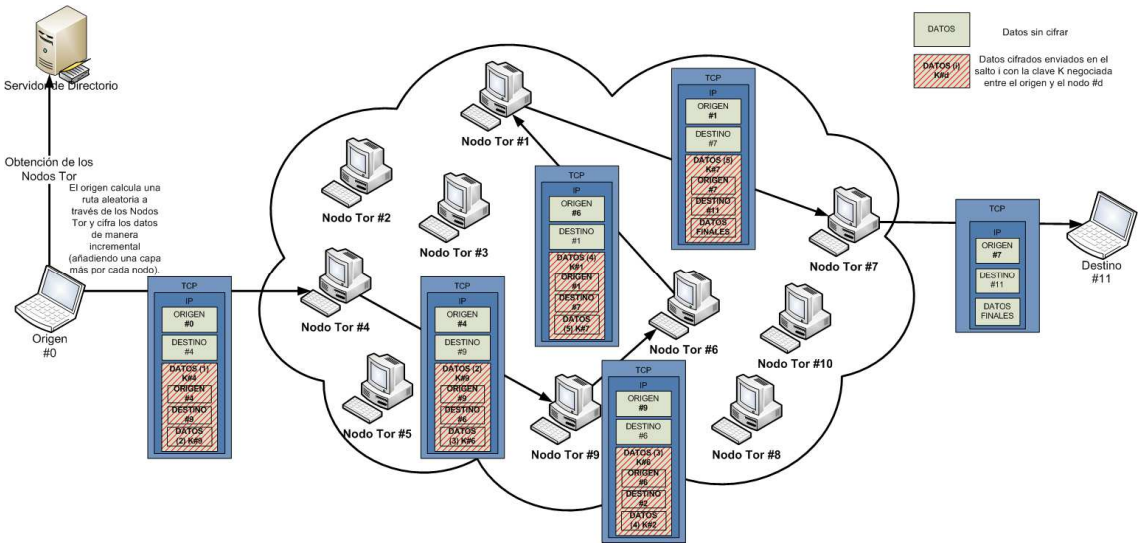

Ilustración 2: Red Tor. Esquema de una red Tor en la que el origen establece una comunicación anónima con el destino pasando por un conjunto de nodos elegidos aleatoriamente y cifrando la ruta de manera incremental (añadiendo una capa por cada salto).

- Basados en **Anonymizer** y similares: Troyanos como el *Bobax Trojan* [13], ponen a disposición de los atacantes un servicio web, el cual, según la orden enviada por parámetro, es capaz de enviar *Spam*, actualizarse, y propagarse. Dicho servicio permite a los atacantes usar herramientas diseñadas para http tipo *Anonymizer*. En estos casos, el anonimato se ve supeditado a las políticas de seguridad del *proxy.* Si el servidor registra las sesiones de los clientes, y las autoridades obligan al administrador a proporcionar dicha información, entonces la localización del atacante podría ser trazada, por lo que ocasionalmente su identidad podría ser desvelada.

- Basados en **Buses**: Buses es parecido a las redes Tor en cuanto a que los mensajes se van cifrando de manera incremental. Sin embargo, a diferencia de las redes Tor, el camino no se establece de manera aleatoria, sino que se reenvía al siguiente en una lista: El funcionamiento es parecido al de una línea (de autobús) circular y cada envío pasa por la siguiente ‘estación' hasta llegar a su destino. El trabajo presentado en [17] propone una implementación de *malware* basado en este tipo de redes anónimas. Los resultados mostrados presentan mayor eficacia que en redes basadas en encaminamiento aleatorio, además de un anonimato equivalente a las técnicas basadas en *mixes*, y con una latencia menor.

4. Consideraciones Finales

En los últimos años ha empezado a crecer la necesidad de otorgar anonimato a usuarios legítimos de Internet y como tal, las herramientas y tecnologías para ello también han evolucionado. En este artículo se han revisado tanto las técnicas tradicionales como las más recientes, concebidas para proporcionar anonimato a usuarios en Internet. A medida que estas técnicas proliferan y se consolidan en la Red, indirectamente se descubren nuevas vulnerabilidades, especialmente en las aplicaciones de ámbito social.

Algunos autores [15,16] restan importancia a este hecho, argumentando que los atacantes ya disponen de herramientas que les proporcionan anonimato (véase Sección

2). Sin embargo, y pese a que ciertamente no hemos encontrado en la literatura muchos indicios de que los atacantes se estén beneficiando de las tecnologías descritas en la Sección 3, no significa que no se estén empleando en la actualidad, ni que no se vayan a utilizar. De hecho, parece realista suponer que los criminales que deseen poner en marcha cualquier tipo de fraude y que no cuenten con su propia infraestructura (o ésta se haya quedado obsoleta) van a ser potenciales usuarios de dichas herramientas, como en los casos referenciados en la Sección 3.2. De hecho, en [17] se propone una implementación de un programa malicioso (*malware*) basado en redes de anonimato.

Por este motivo, identificamos la necesidad de una solución que proporcione anonimato en beneficio de los usuarios honestos y que cuente con mecanismos que impidan a usuarios maliciosos aprovecharse de este anonimato. En este contexto, la propuesta anteriormente citada [17] define, además, una solución basada en la identificación de los mensajes cifrados, tanto enviados como recibidos, involucrando en ocasiones al usuario.

Referencias

1. Plonk, A., Carblanc, A., et Grupo de Trabajo de Seguridad de la Información y Protección de la Privacidad: Software malicioso (*malware*) una amenaza de seguridad para la economía de internet. CERT. Report No.: DSTI/ICCP/REG(2007)5/FINAL (2008)

2. Ianelli, N., Hackworth, A.: Botnets as a vehicle for online crime. The International Journal of FORENSIC COMPUTER SCIENCE, Vol. 2, No. 1 (2007) 19-39

3. Hanks, S., Li, T., Farinacci, D., Traina, P.: Generic routing encapsulation (GRE). RFC Editor United States (2000) RFC2784

4. Bertolín, J.A., Bertolín, G.A.: Identificación y análisis del anonimato en comunicaciones electrónicas. Revista Española de Electrónica Nº 627 (2007) 32-45

5. Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of rc4. Lecture Notes in Computer Science (2001) 1-24 Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography.

6. Bellovin, S.: Security problems in the TCP/IP protocol suite. ACM SIGCOMM Computer Communication Review, Vol. 19, No. 2 (1989) 32-48

7. Tan, K.M.C., McHugh, J., Killourhy, K.S.: Hiding intrusions: From the abnormal to the normal and beyond. In proceedings of the 5th International Workshop on Information Hiding, London, UK, Springer-Verlag (2003) 1-17

8. Mahoney, M.V., Chan, P.K.: An analysis of the 1999 darpa/lincoln laboratory evaluation data for network anomaly detection. In proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Florida, USA, Springer-Verlag (2003) 220-237

9. Zalewski, M.: Silence on the wire: a field guide to passive reconnaissance and indirect attacks. William Pollock (2005)

10. Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, Vol. 24, No. 2 (1981) 84-88

11. Dagon, D., Gu, G., Zou, C., Grizzard, J., Dwivedi, S.J., Lee, W., Lipton, R.: A taxonomy of botnets. Unpublished paper (2005)

12. Torproject: List of irc/chat networks that block or support tor (2009) https://wiki.torproject.org/noreply/TheOnionRouter/BlockingIrc

13. Stewart, J.: Judgment in u.s. v. Robert Tappan Morris (2002) http://www.rbs2.com/morris.htm

15. Shue, C., Gupta, M.: Hiding in Plain Sight: Exploiting Broadcast for Practical Host Anonymity. In proceedings of Hawaii International Conference on System Sciences (HICSS) (2010)

16. Torproject: Abuse faq (2009) http://www.torproject.org/faq-abuse.html.en#WhatAboutCriminals

17. Hirt, A., Aycock, J.: Anonymous and malicious. Berlin. In: 15th Virus Bulletin International Conference. Vol. 2, Citeseer (2005)

18. Boyan, J., The Anonymizer: Protecting User Privacy on the Web. In: Computer-Mediated Communication Magazine, Vol. 4, No. 9 (1997)

19. Tanase, M.,: IP spoofing: an introduction. In: Security Focus (2003) http://www.securityfocus.com/infocus/1674