# SEXY VIEW: EL INICIO DE LAS BOTNETS PARA DISPOSITIVOS MÓVILES

Castillo, Carlos
carlos-castillo@javeriana.edu.co
Pontifica Universidad Javeriana, Bogotá D.C, Colombia

***Resumen*—**El presente artículo pretende evaluar si el malware SymbOS/yxes.Alworm, como mecanismo distribuidor y generador de una Botnet, representa actualmente una amenaza real para la seguridad informática en dispositivos móviles inteligentes. Esto se podría considerar como el inicio de la era de las Botnets móviles teniendo en cuenta que, actualmente, solamente existen registros de este tipo de amenazas en los computadores tradicionales. Para lo anterior, se realiza un análisis detallado de las dos amenazas de seguridad más importantes actualmente en el mundo de las tecnologías de la información según el GTISC [3]: El malware para dispositivos móviles y las Botnets conformadas por computadores tradicionales. El análisis está orientado tanto a la parte técnica (definición, estructura, funcionamiento entre otros) como a la parte de evaluación de la situación actual y el impacto de estas amenazas. Luego de conocer los dos pilares de la presente investigación, se procede a realizar el análisis del malware Yxes, recurriendo a la informática forense aplicada a dispositivos móviles, con el fin de verificar si el comportamiento del virus se asemeja al de los Bots tradicionales. Finalmente, se exponen las conclusiones generales sobre los hallazgos encontrados y, adicionalmente, se propone una la perspectiva a futuro de la seguridad informática en dispositivos móviles.

***Abstract*—** This article aims to evaluate if the SymbOS/yxes.Alworm malware, acting as a generator of a Botnet, represents a real Information Security threat to smart mobile devices. If so, this could be considered the beginning of a new age in the mobile security field: Botnets that use mobile devices. This can be affirmed taking into account that nowadays Botnets only work on traditional computers. To probe this thesis, it realizes a detailed analysis of two of the most important security threats in TI: Malware for mobile devices and Botnets for traditional computers. The analysis is composed of two parts: A technical part (definition, structure, how it works and so on) and a real perspective of the actual situation of these threats and their real impact in TI. Afterwards that, it performs an analysis of the malware Yxes using forensic techniques to corroborate if the virus behavior matches with the behavior of the traditional Botnets. Finally, it exposes general conclusions about the analysis and it presents a future perspective about the information security field on mobile devices.

*Índice de Términos*— Malware móvil, Botnets, Banca móvil, 3G, Symbian, Ingeniería Reversa, Informática Forense, Dispositivos Móviles.

## I. INTRODUCCIÓN

Comenzaba la década de 1940 cuando el alemán Konrad Zuse finalizó la Z3, la primera computadora electromecánica digital controlada por un programa funcional [1]. La fecha exacta de tan magno evento aún está en discusión (en gran parte debido a que sucedió en medio de la segunda guerra mundial en la Alemania Nazi [1]) y tal vez por estas discrepancias es que no se le da a este hecho la importancia que merece: El inicio de la era de la computación.

Al viajar aproximadamente 40 años en el tiempo encontramos una gran variedad de computadoras portátiles (llamadas también teléfonos inteligentes o *smartphones*), pequeñas en tamaño pero con funcionalidades tan potentes como el acceso a redes corporativas en tiempo real [2] o el acceso a la conocida banca móvil (realización de transacciones financieras) [3]. Telefonía celular, agenda, correo electrónico, Internet banda ancha, multimedia (música, videos, televisión), acceso a tiendas electrónicas como *iTunes* [3] son algunas de las funcionalidades que tienen este tipo de dispositivos actualmente.

Es por esto que para muchos empleados corporativos los dispositivos móviles han reemplazado los computadores de escritorio [4]. Es tal la evolución de, por ejemplo, los sistemas operativos para teléfonos inteligentes que, recientemente, algunos miembros del equipo SCO[1] lograron ejecutar *Symbian* en un procesador *Atom* y una placa Intel sin ningún tipo de modificación [5]. Por el lado del hardware de los dispositivos móviles, grandes avances se ven a futuro. Un ejemplo de esto es el anuncio del nuevo procesador ARM *Cortex* A9, sucesor del A8, el cual usará tecnología de 45 nanómetros y sería capaz de llegar a los cuatro núcleos [6]. Teniendo en cuenta esto, se estima que en pocos años los teléfonos inteligentes representarán la mayoría de las computadoras del mundo [7].

En relación con lo anterior, la seguridad de la información en estos dispositivos debería constituir la principal preocupación en el ámbito específico de las tecnologías de la información, sin embargo, desafortunadamente esto no es así. Muy pocos ejecutivos de seguridad empresariales le han dado importancia a la posibilidad de que el *malware* descargado en los dispositivos móviles puedan infectar toda la red corporativa [4]. Una muestra de esto es que, según una encuesta realizada por Infonetics, cerca del 50% de las grandes compañías comentaron que se apoyan solamente en la seguridad que proporciona el sistema operativo de los teléfonos inteligentes [4].

La situación es preocupante teniendo en cuenta que las advertencias no son infundadas. Según Fortinet, la creciente prevalencia de las redes 3G está activando la banda ancha en los dispositivos móviles lo cual significa más contenido malicioso que está ingresando junto con el tráfico normal [2]. Adicionalmente, se conocen cientos de programas maliciosos que han sido escritos para atacar dispositivos móviles. Colocar un virus en una red móvil puede ser una manera muy efectiva de infectar una red corporativa [4].

Por otro lado, la motivación financiera incrementará los ataques a teléfonos inteligentes en los próximos años. Entre

[1] Symbian Customer Operations

más infraestructuras de pagos se implementen en estos dispositivos, estos serán cada vez más atractivos para los delincuentes informáticos [3].

Finalmente es importante aclarar que, a pesar que no se han reportado mayores incidentes en materia de seguridad en dispositivos móviles, es solo cuestión de tiempo para que un evento de serias consecuencias ocurra [4].

Cambiando de tema, encontramos la que considero la amenaza más seria actualmente en Internet: Las Botnets. Estos ejércitos de computadores *zombies,* frecuentemente utilizados por delincuentes informáticos, consiste en una colección de máquinas comprometidas controladas por una sola persona [8]. La importancia de esta amenaza radica en los usos que le dan los cibercriminales (Ataques de DDoS[2], instalación de *Keylogguers* y troyanos, envío de *spam*, monitoreo de tráfico, almacenamiento de datos ilegales entre otros [9]) y en que la implementación y arquitectura de la mayoría de las Botnets es compleja (utilizan técnicas de Ingeniería de Software como la modularidad) por lo que tienen un potencial de expansión importante [8].

Teniendo claro los dos pilares principales de la investigación (el malware móvil y las Botnets) en las siguientes secciones del documento se va a resaltar la importancia de estos dos temas en la seguridad de la información a nivel mundial, enfatizando en su situación actual y en su entendimiento detallado para, finalmente, analizar la que, según Guillaume Lovet -*Senior Manager* del equipo *Fortinet Threat Research*- podría ser la primera Botnet móvil [10]: El malware SymbOS/Yxes.A!worm (o Sexy View).

## II. IMPACTO POTENCIAL DE LAS BOTNETS MÓVILES

### *A. Teléfonos inteligentes*

La telefonía celular está reemplazando la tradicional. Una muestra de ello es que en los últimos resultados de la encuesta sobre el uso de la telefonía móvil realizada por el *National Center for Health* de Estados Unidos reveló que el 20% de todos los hogares de este país han eliminado las líneas telefónicas tradicionales y las han reemplazado por teléfonos celulares para realizar comunicación por voz. Este número aumentó un 17% con respecto al año 2008. Adicionalmente, uno de cada siete hogares recibe todas o casi todas las llamadas vía celular [11].

Por otro lado, la prestigiosa consultora Gartner anunció que las ventas de teléfonos móviles en el primer trimestre de 2009 sumaron en total 269.1 millones de unidades, lo cual representa una disminución del 8.6% con respecto al mismo periodo del 2008. Paralelamente, la venta de teléfonos inteligentes en el primer trimestre de 2009 ascendió a 36.4 millones de unidades lo cual representa un aumento del 12.7% en relación al año anterior [12]. La relación entre estas cifras muestra que la venta de teléfonos inteligentes representa el 13.5% de todos los dispositivos móviles, una cifra importante que va en constante aumento [12]. Desde luego, estos datos muestran que las personas están adquiriendo más teléfonos inteligentes debido a que cada vez incluyen más funcionalidades.

En cuanto a los fabricantes, Nokia

[2] Denegación de servicio distribuida

continua liderando el mercado de los teléfonos móviles con una participación de mercado del 36.2% seguido por Samsung con un 19.1% [12]. En el campo de los teléfonos inteligentes, Nokia continúa liderando el mercado con una participación del 45.1% seguido por RIM[3] con un 13.3% y Apple con un 5.3% [12]. Las cifras anteriores justifican el liderazgo de el sistema operativo Symbian el cual tiene una participación del 49.3% del mercado de teléfonos inteligentes seguido por RIM con el 19.9% e iPhone OS con un 10.8% (éste último prácticamente doblando su participación anterior la cual fue del 5.3%) [12].

Basándose en los datos anteriores, cabe concluir que el uso de los dispositivos móviles va en aumento debido a nuevas funcionalidades atractivas para los consumidores entre las que se encuentran unas muy críticas en materia de seguridad de la información como por ejemplo la banca móvil, la cual se analizará a continuación.

### *B. Banca Móvil*

La mayor motivación para un delincuente es el lucro financiero, y desde luego el campo digital no es la excepción. No en vano una encuesta que realizó McAfee a 30 fabricantes de dispositivos móviles a nivel mundial reveló que el área de uso que más preocupa a nivel de seguridad es la banca móvil [13]. Es por ésta motivación financiera que el aumento de infraestructuras de pago móviles propicia la delincuencia informática en los dispositivos móviles [14].

Actualmente, la mayoría de los bancos más grandes en Estados Unidos ofrecen servicios de banca móvil tales como alertas de cuenta, balances de cuenta, pagos de facturas, cobro en línea, verificación de transacciones y alertas de hipoteca [15]. El crecimiento, a futuro, de este tipo de servicios se puede ver reflejado en la siguiente gráfica [15]:

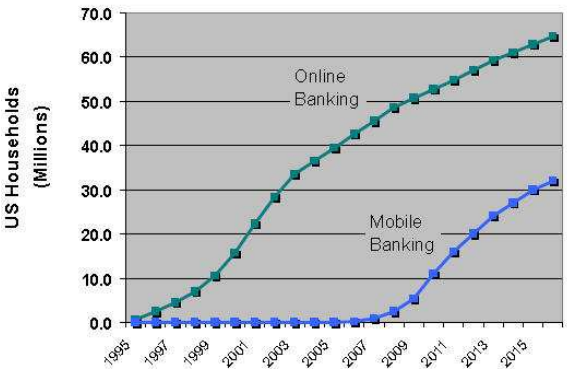


Figura 1. Banca Móvil Vs Banca en Línea [15]

La imagen anterior muestra, a manera de comparación, el crecimiento paralelo que ha tenido y que tendrá la banca móvil y la banca en línea en Estados Unidos en un periodo de 20 años (1996-2016). Un dato relevante obtenido de la gráfica es que tomó aproximadamente 10 años alcanzar los 40 millones de usuarios de la banca en línea [15]. Basados en esto, se estima que sean necesarios otros 10 años más para alcanzar una tasa de penetración similar para la banca móvil [15].

Los datos anteriores aplican únicamente a Estados Unidos, sin embargo, el mercado latinoamericano no es la excepción a esta tendencia. Un ejemplo de esto son las cifras presentadas por la compañía de soluciones tecnológicas Gemalto la cual afirma que, al cierre del primer semestre de 2009, unas 7 millones de transacciones bancarias se habrán realizado desde un teléfono móvil lo cual representa un gran crecimiento con respecto a las 3 millones de transacciones

[3] Research In Motion

registradas en el mismo periodo pero del año anterior [16].

Dichos resultados ubican al país como el primero en la región no solo en la implementación de aplicaciones de este tipo, sino en el aumento del número de usuarios, los cuales ascienden a cerca de 240.000 [16]. Al parecer el potencial de crecimiento del uso de la banca móvil en Colombia es inmenso teniendo en cuenta que actualmente 33 millones de líneas móviles están listas para realizar transacciones financieras debido a que la aplicación de banca móvil viene pre cargada en la SIM[4] card del usuario [16].

Volviendo a la perspectiva a futuro de la banca móvil, un hecho relevante en este aspecto es la inversión de Nokia por 70 millones de dólares en el proveedor de pagos a través del teléfono móvil Obopay en el 2009 [17], lo cual potenciaría este mercado de forma sustancial debido a que, como se vio en el apartado anterior, Nokia fabrica la mayoría de dispositivos móviles en el mundo.

Teniendo en cuenta los datos anteriores, cabe concluir que el uso de la banca móvil va en aumento, a medida que se desarrollan cada vez más las capacidades de los dispositivos y la confianza de las personas, sin embargo, la delincuencia informática también va en aumento teniendo como punta de lanza el malware móvil.

### *C. Malware Móvil*

Un estudio de la Universidad de Northeastern sugiere que no han habido grandes fallos de seguridad por parte de virus informáticos en dispositivos móviles debido que ningún sistema operativo para este tipo de equipos es suficientemente popular para que se pueda difundir efectivamente [18]. El estudio afirma que si un sistema operativo alcanza una participación en el mercado del 30%, el virus alcanzará el 85% de los dispositivos en unas pocas horas y el 99.8% en menos de una semana [18]. El candidato más opcionado para obtener la preciada posición es Symbian; sin embargo, tiene importantes rivales acercándose como por ejemplo el sistema operativo de Google, Android [19].

Otro factor que influye en la cantidad de malware móvil generado consiste en la apertura de los sistemas operativos [13] debido a que los delincuentes informáticos cuentan con más conocimiento del sistema que van a atacar.

A pesar de que las condiciones enunciadas anteriormente no se han cumplido de forma satisfactoria, el número de virus móviles conocidos va en aumento:

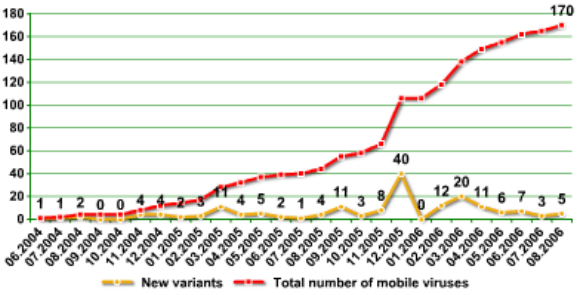



Figura 2. Nuevas variantes vs número total de virus móviles (2004-2006) [20]

Desde luego lo que impulsa la creación de nuevos virus y nuevas variantes son los usos críticos de los dispositivos (banca móvil, compra de multimedia y el uso orientado a la productividad) [14] los cuales van en aumento según los datos expuestos anteriormente.

[4] Subscriber Identity Module

El aumento del malware va ligado directamente con nuevas formas de utilizarlo y una de las más comunes, en el mundo de los PC, son las llamadas Botnet o ejércitos de computadores *zombies*,

### *D. Botnets*

En el informe de McAfee sobre amenazas del primer trimestre del 2009 se afirma que detectaron cerca de doce millones de nuevas direcciones IP que funcionan como *zombies*, es decir, computadores que están bajo el control de los delincuentes informáticos. Esto supone un incremento significativo, de casi el 50%, con respecto a los niveles del último trimestre de 2008 [21].

Por otro lado, el GTISC[5] en su encuesta anual sobre las amenazas de seguridad emergentes que afectan el mundo digital, estimó en el 2008 que el 10% de las computadoras conectadas a Internet eran parte de alguna Botnet. Este año (2009), los investigadores del GTISC estiman que este porcentaje ascenderá a un 15% [3]. Según Wenke Lee, investigador líder de las Botnet en el GTISC, "Comparado con los virus y el *spam*, las Botnets han crecido a una ritmo más acelerado" [3]. Finalmente, otro estudio afirma que el 40% de las computadoras están infectadas con Bots [22].

No menos impresionante resulta la cifra proporcionada por Panda Labs en el segundo trimestre de 2008 en donde afirma que 10 millones de computadores Bot fueron usados para distribuir *spam* y malware en Internet cada día [3].

Luego de ver la cantidad aproximada de nuevas computadoras que hacen parte de las Botnet, podemos apreciar el impacto que tiene esta amenaza a nivel mundial.

Unos investigadores de la Universidad de California se infiltraron en la Botnet Torpig (conocido como el *rootkit* activo más difícil de detectar según la empresa Prevx [23]) durante 10 días obteniendo 70 GB de información financiera entre la que se encuentra 8.310 cuentas de 410 instituciones diferentes [23].

Adicionalmente, el equipo extrajo 1.660 números únicos de tarjetas de crédito y débito de aproximadamente 180.000 Bots que observaron [23]. Usando el valor estadístico por parte de Symantec del valor de un número de tarjeta de crédito y débito actualmente, se estima que los investigadores pudieron haber obtenido aproximadamente USD$ 8.3 millones en los 10 días [23].

A pesar que es posible obtener un gran beneficio económico con la información recolectada con la Botnets, al parecer este no es el objetivo de los delincuentes informáticos. Lo que están haciendo en realidad es comerciar con dicha información vendiendo, por ejemplo, un número de tarjeta de crédito por entre 1 y 6 USD o una identidad completa (Cuenta bancaria, tarjeta de crédito, fecha de nacimiento entre otros) por entre 14 y 18 USD, según Symantec [24].

Otro ejemplo de la seriedad de esta amenaza se encuentra en el último *Cybercrime Intelligence Report* del 2009, en donde la empresa de seguridad informática Finjan describe las operaciones de la red *Golden Cash*, una plataforma de comercio electrónico en donde los criminales trafican con

[5] Georgia Tech Information Security Center

computadores Bot [25]. Lo novedoso del descubrimiento es la existencia de un sofisticado mercado en línea para comprar y vender computadores comprometidos. Por ejemplo, del lado del comprador, un conjunto de 1.000 computadores infectados con malware pueden ser adquiridos por entre $5 y $100, dependiendo del país en donde se encuentren [25].

Es evidente la importancia de esta amenaza a nivel mundial, sin embargo, ésta no sería posible trasladarla a los dispositivos móviles sin tener una conexión de banda ancha, como la que proporcionan las redes 3G[6].

*E. Redes 3G*

Las redes de tercera generación constituyen la llegada de la llamada "banda ancha" a los dispositivos móviles a través de la red celular. El diseño original de estas redes estuvo orientado a que funcionaran sobre redes que usan protocolo TCP/IP [26], es decir, una extensión de Internet. Desde luego, la principal motivación de las redes y los estándares es la velocidad, la cual se estima a que sea de 1 GB/s con baja movilidad en el 2010 (100 Mbps con alta movilidad) [26].

Existen dos estándares principales a nivel mundial en las redes 3G: WCDMA[7] (Europa) y CDMA2000 1xEV-DO[8] (Japón y Estados Unidos).

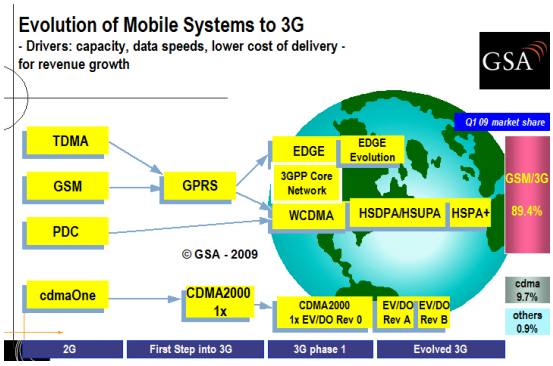


Figura 3. Evolución de los sistemas a 3G [27]

Como se aprecia en la imagen anterior, los dos estándares juntos representan el 99.1% de la telefonía celular a nivel mundial [27]. La velocidad máxima de descarga en WCDMA es de 2 Mbps [26] mientras que en CDMA2000 1xEV-DO alcanza los 3.1 Mbps [28].

En cuanto a número de usuarios, CDMA2000 continúa en alza durante el 2008 con un rápido crecimiento en India y China en el 2009, llegando a los 455 millones de usuarios alrededor del mundo [28].

Por otro lado, al primer trimestre de 2009, existen más de 3.8 billones de subscriptores GSM[9] y WCDMA-HSPA[10] (3.5G) alrededor del mundo con operadores en 120 países. Solamente WCDMA cuenta con una participación del 72% de las redes comerciales 3G [27].

Teniendo en cuenta la situación actual, es evidente que la evolución de las redes continúe siguiendo las tendencias que se nombran a continuación [26], [29]:

- Continua importancia de los servicios de voz
- Continua el crecimiento de aplicaciones IP

[6] 3 Generation
[7] Wideband Code Division Multiple Access
[8] Evolution-Data Optimized
[9] Groupe Spécial Mobile
[10] High-Speed Packet Access

- Continúan las aplicaciones que requieren alta calidad de servicio y velocidad debido a las capacidades de multimedia

- Los costos del servicio van a descender a medida que mejora la calidad con el fin de permitir el acceso a la mayoría de las personas

En este ultimo contexto, el del acceso a más personas, Nokia ha realizado el primer aporte el cual consiste en el acceso a terminales 3G más económicos como el nuevo Nokia 2730 *Classic* el cual se espera salga a la venta a un costo de 80 € [30].

Basados en la información anterior, es importante concluir que el creciente uso de los dispositivos móviles (en especial de los teléfonos inteligentes) y las aplicaciones de banca móvil generan un interés creciente por parte de los delincuentes informáticos los cuales, usando el malware móvil para crear Botnets a través de redes 3G, pueden constituir una de las amenazas más importantes para la seguridad de la información en el mundo: Las Botnets en dispositivos móviles.

Luego de entender las motivaciones del problema, es pertinente abordar los aspectos técnicos específicos de los dos pilares de la investigación: El malware móvil y las Botnets.

## III. BOTNETS: UNA AMENAZA GLOBAL

*The Honeynet Project*, una organización internacional dedicada a mejorar la seguridad de Internet, define las Botnet como "una red de máquinas comprometidas que pueden ser controladas remotamente por un atacante" [31].

El origen de esta amenaza se remonta al año 1993 cuando Jeff Fisher creo el software *Eggdrop bot* para realizar mantenimiento de red [8]. Esto demuestra que, originalmente, las Botnet no fueron pensadas para fines maliciosos, sin embargo, debido a su gran tamaño (puede llegar incluso a millones de máquinas), actualmente constituyen una de las amenazas, en términos de seguridad de la información, más importantes actualmente [31].

Para entender el funcionamiento de las Botnet, es importante conocer su estructura general, características, las principales familias, las tecnologías de comando y control y los usos de las mismas.

### *A. Estructura general*

La estructura general de una Botnet se puede apreciar en la siguiente figura:

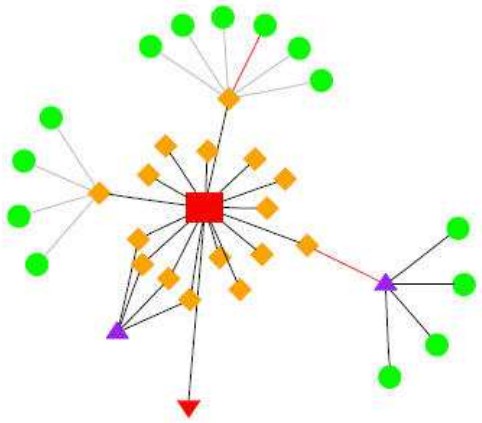


Figura 4. Estructura general de una Botnet [32]

El cuadrado rojo central representa el servidor de comando y control el cual cuenta con una serie de *zombies* o *drones* (diamantes anaranjados) que se encargan

de buscar nuevas víctimas. Una vez que un *drone* encuentra una máquina vulnerable, la infecta (círculos verdes). Finalmente, el maestro de la Botnet puede usar los *drones* infectados para atacar, por ejemplo, un servidor web (triangulo rojo invertido) realizando un ataque de DoS [32].

### *B. Características Generales*

Paralelamente a la estructura, existen una serie de características generales que son comunes para la mayoría de las Botnet las cuales son las siguientes:

• Las Botnet incluyen una gran variedad de mecanismos sofisticados para evitar su detección una vez instalada en la máquina comprometida [8]. Uno de los mecanismos más importantes es que el de comunicación el cual está diseñado para parecer tráfico normal usando puertos aceptados por lo que incluso *firewalls* y sistemas de prevención de intrusos pueden tardar mucho tiempo en aislar los mensajes entre los Bots [3]. Otro forma de evitar su detección consiste en mantener un mecanismo de comando y control que le permite al Bot actualizarse a si mismo cuando se desee, haciéndose invisible a las firmas de los antivirus [3].

• En general, las Botnet cuentan con limitados mecanismos de propagación (siendo Agabot la que más tiene debido a su polimorfismo limitado [8]). Adicionalmente, en la mayoría de casos disponen de una reducida colección de *exploits* para infectar sistemas operativos objetivos los cuales, en su mayoría, atacan vulnerabilidades bien conocidas como las de Microsoft Windows [8], [31]. Debido a que la mayoría de usuarios no tienen su sistema operativo Windows al día en actualizaciones de seguridad, esto demuestra que, aunque son pocos los mecanismos, son efectivos.

• Todas las Botnet incluyen ataques de DoS [8].

• El mecanismo de control predominante de las Botnet es IRC [8], sin embargo, actualmente está surgiendo una nueva generación de Botnets las cuales son fácilmente administradas vía web (HTTP) como lo son AdPack y ZeuS [33]

• Los objetivos primarios (victimas) de las Botnets, en general, deben contar con una conexión a Internet de banda ancha, deben manejar alta disponibilidad, deben ser utilizados por usuarios poco experimentados y desprevenidos (sin actualizaciones de seguridad al día ni *firewall*), y, generalmente, deben encontrarse a miles de kilómetros del atacante para evitar que éste sea rastreado [9].

• Algunas Botnet están formadas por algunos cientos de Bots, sin embargo, se tiene conocimiento de otras del orden de los 50.000 Bots. El tamaño de las Botnets grandes es difícil de estimar por lo que si el Bot está ligado a más de 5 servidores IRC se da por entendido que el tamaño de la Botnet no se puede establecer. [31]

Al conocer las características principales de las Botnet, se obtiene una visión general de estas, sin embargo, para detallar más su funcionamiento es necesario especificar las Botnets más importantes en la actualidad. Para ello, a continuación se exponen las principales

familias Bot que se encuentran en Internet.

### *C. Familias de Bots [8], [9], [31] , [1]*

Una familia es una muestra nueva y distinta de código malicioso mientras que una variante es una nueva iteración de la familia con unas diferencias menores pero que aún se basa en la origina [34]. A continuación se enumeran las principales familias de Bots actualmente identificadas las cuales, según McAfee, constituyen el 92.2% de las variantes conocidas a junio de 2005 [34]:

• **Agobot:** Es probablemente el Bot más conocido debido a que su código fuente está disponible públicamente bajo la licencia GPL. Actualmente Sophos conoce más de 500 versiones diferentes de Agobot y el número sigue aumentando rápidamente. Agobot está escrito en C++, es multiplataforma y está estructurado de forma modular por lo que tiene un diseño abstracto, el cual permite de una manera sencilla añadir nuevos comandos o nuevos escáneres para las últimas vulnerabilidades. Por otro lado, ofrece características de *rootkit* al esconder procesos y archivos para evitar su detección. Finalmente, presenta dificultad para realizarle ingeniería inversa debido a que incluye funciones para detectar *debuggers* (*SoftICE* y *OllyDbg*) y máquinas virtuales (*VMWare* y *VirtualPC*)

• **SDbot:** Es la familia de malware más activa en el momento: Sophos lo tiene actualmente en la posición 7 de "las últimas alertas de virus". Está escrito en C bajo licencia GPL[11] por lo que su código fuente también está disponible en Internet. A diferencia de Agobot, el código fuente no esta bien diseñado por lo que es más difícil proporcionarle comandos o escáneres sofisticados.

• **GTBot:** GT (*Global Threat*) es el nombre común que se utiliza para los Bots que usan mIRC (un popular cliente de IRC para Windows). Estos Bots inician una instancia de chat mIRC con la ayuda de un script y algunos binarios. Uno de estos binarios se llama *HideWindow* el cual es usado para que la instancia de mIRC sea invisible para el usuario. Los otros binarios son DLL's[12] atadas a mIRC para añadirle nuevas características a los scripts que estos Bots usan. Los scripts mIRC utilizan la extensión ".mrc" y son usados para controlar el Bot.

• **DSNX:** Los *Dataspy Network* X están escritos en C++ (GPL) y tienen una conveniente interfaz de plug-ins la cual permite que un atacante puede fácilmente escribir escáneres y difusores para extender las funcionalidades del Bot. La mayor desventaja de este tipo de Botnets radica en que la versión original no trae ningún difusor, sin embargo, existen *plug-ins* actualmente en Internet para arreglar este inconveniente (ataques DDoS, escaneo de puertos, servidores HTTP etc..)

Aparte de las tradicionales familias de Bots, existen una serie de Bots que llaman la atención debido a su particular esencia:

• **Q8 Bots:** Es un Bot muy pequeño consistente en solamente 926 líneas de código C para sistemas Unix/Linux. Implementa las características comunes

[11] General Public License

[12] Dynamic Linking Library

de un Bot: Actualización dinámica vía HTTP, ataques DDoS, ejecución de comandos arbitrarios entre otros.

• **Kaiten:** No tiene difusores y esta escrito para Linux/Unix. La débil autenticación de usuario que tiene esta Botnet permite que sea secuestrada fácilmente. El Bot, consistente de solamente un archivo, ofrece una *shell* remota la cual puede ser usada para revisar por futuras vulnerabilidades, vía IRC, con el fin de obtener acceso privilegiado.

• ***Perl-based Bots:*** Estos Bots son muy pequeños y contienen, en la mayoría de casos, solamente unas pocas cientas líneas de código. Ofrecen un rudimentario conjunto de comandos (la mayoría son ataques DDoS) y son usados en sistemas UNIX.

Todas las familias descritas anteriormente utilizan IRC como tecnología de comando y control, sin embargo, existen otros mecanismos que deben ser considerados.

### *D. Tecnologías de comando y control [35], [22]*

Una de las partes fundamentales de las Botnet es el canal de comunicación con su maestro debido a que, si el Bot no recibe órdenes, permanecerá inactivo sin realizar ninguna acción. A continuación se enumeran los tipos de tecnologías de comando y control que usan actualmente las Botnets en Internet:

• **IRC:** *Internet Relay Chat* (IRC) es una forma de comunicación en tiempo real que existe en Internet. Está diseñada principalmente para permitir comunicaciones en grupos (canales) aunque también puede ser usada para realizar una comunicación uno a uno [31]. Usando esta tecnología, el Bot se conecta a un canal específico a la espera de ordenes las cuales son en realidad comandos que le comunican a la máquina comprometida las acciones que debe realizar [31]. IRC es la tecnología preferida por los delincuentes informáticos para controlar sus Botnets debido a que: Los servidores IRC están disponibles gratuitamente, son fáciles de configurar y los atacantes tienen años de experiencia con este tipo de comunicación [31]. Actualmente, dos implementaciones de servidores IRC son las más usadas para operar una Botnet: *Unreal IRCd* y *ConferenceRoom* Ejemplos: *Agabot, SDBot, SpyBot y GT bot.*

• **WEB:** Consiste en que la consola de comando y control está basada en el protocolo HTTP. Ejemplos: *BlackEnergy Bot y Clickbot.A*

• **P2P:** Las Botnet P2P[13] utilizan una arquitectura más estable la cual es descentralizada y no tiene un único punto de falla (como las tradicionales cliente-servidor). Ejemplo: *Trojan.Peacomm*

• **DNS:** Esta tecnología consiste en enmascarar tráfico en peticiones y respuestas DNS. La mayor ventaja de este método es que el tráfico DNS es siempre permitido en la mayoría de firewalls por lo que la comunicación rara vez se verá interrumpida.

• **Redes Fast-Flux:** Consiste en redes de servidores controlados por

[13] Peer to Peer

delincuentes informáticos que esconden sus IP de los intrusos. Estos servidores permiten que un usuario se conecte primero a una máquina comprometida, que sirve como proxy, para que reenvíe la petición al servidor real sirviendo, en general, de intermediario. En otras palabras, los registros DNS de un sitio real apuntan a la red de computadoras *Fast-Flux*. Esta red distribuye la petición del usuario entre todas las computadoras usando *Roud-Robin* con las direcciones IP. El éxito de esta técnica consiste en administrar servicios DNS y HTTP en las máquinas comprometidas.

A pesar que existen diferentes tecnologías de comando y control, es posible estandarizar el comportamiento de Bots, tal como se muestra a continuación.

### *E. Comportamiento general de un Bot [22]*

Un Bot típico puede ser creado y mantenido en cuatro fases: [22]

- **Infección inicial:** Consiste en comprometer la máquina para que descargue e instale el Bot. Se puede efectuar explotando una vulnerabilidad bien conocida, usando malware descargado desde la red, a través de un archivo adjunto en un correo electrónico o a través de USB entre muchos otros métodos

- **Infección secundaria:** Consiste en que la máquina infectada descarga y ejecuta el código Bot. Los métodos de descarga pueden ser: FTP, TFTP, HTTP o P2P

- **Actividades maliciosas:** El Bot se comunica con su maestro para obtener instrucciones/comandos y realizar actividades como envío de spam o ataques de denegación de servicio (DDoS)

- **Mantenimiento y actualización:** Consiste en la descarga de actualizaciones desde el servidor maestro con el fin de evitar los antivirus y mejorar las capacidades del Bot.

Teniendo claro cómo funcionan las Botnet, finalmente es importante conocer para qué las usan los delincuentes informáticos actualmente debido a que, sólo de esta manera, se entenderá el impacto real que tiene esta amenaza en Internet hoy en día.

### *F. USOS DE UNA BOTNET [3], [35], [31], [32], [34], [1]*

Los delincuentes informáticos actualmente utilizan las Botnets para:

- Robar información con el fin de realizar extorsión, ingeniería social, acceso a sistemas con credenciales legítimas entre otros.

- Realizar ataques de DoS (ICMP, UDP, SYN, HTTP)

- Efectuar envío de *spam*
- Establecer un servicio de servidores (HTTP, DNS, FTP) para diversos fines: Phising, almacenamiento de malware y software pirata, almacenamiento de spyware, almacenamiento de estados de infección entre otros.

- Adquirir capacidad tanto de cómputo como de red

• Realizar escaneo y explotación de vulnerabilidades

• Efectuar descarga e instalación de Bots (HTTP, FTP o TFTP)

• Realizar fraude de click (programación de Bots para que realicen automáticamente click en anuncios publicitarios pagos)

• Establecer Gateways - Proxys (HTTP, SOCKS, IRC): Consiste en la redirección de conexiones para esconder la ubicación real del *bot master*

• Instalar spyware (*Keylogging*, *Screenshots*, rastreo de navegación web, captura de paquetes (*sniffing*), robo de datos entre otros)

• Manipular de votación/juegos en línea: Debido a que cada Bot tiene una IP diferente, cada voto tiene la misma credibilidad que el de una persona real. Los juegos en línea pueden ser manipulados de la misma manera [31].

Al parecer, las Botnets y el malware son idénticos, sin embargo, existen unas diferencias fundamentales entre ellos [3]:

1. El malware es el responsable de convertir una computadora en un Bot
2. El malware tradicional tiene sólo un propósito de ataque

Lo anterior quiere decir que una Botnet requiere del malware para funcionar por lo tanto, una Botnet móvil requiere de malware móvil para poder existir. Esta afirmación permite entender la relación entre estos dos elementos aparentemente idénticos.

## IV. MALWARE: DEL PC A LOS DISPOSITIVOS MÓVILES

Expertos han hablado de los peligrosos malware móviles desde la aparición del primer troyano para Palm (*Liberty*), sin embargo, dichas amenazas han pasado a ser una preocupación menor. En parte es porque hay muchos menos dispositivos móviles que computadores lo cual hace de los PC un objetivo mucho más atractivo.

Adicionalmente, los dispositivos móviles carecen de sofisticación técnica lo cual le ha proporcionado limitadas formas de ataque a los delincuentes informáticos [7]. Una muestra de esto es que a marzo de 2008, F-Secure ha encontrado 401 tipos diferentes de malware móvil activos y McAfee encontró 457. Esto no es nada comparado con las 640.000 variantes para Windows en PC anunciadas por F-Secure en la misma fecha [7].

Los virus móviles descubiertos hasta ahora han causado poco daño y requieren la explicita interacción para su instalación y ejecución, sin embargo, existen varios factores que hacen que los dispositivos móviles sean especialmente vulnerables a futuros virus móviles [36]:

• La notable demanda de los consumidores por servicios celulares ricos en datos en donde los operadores de telecomunicaciones están desarrollando rápidamente redes 3G alrededor del mundo. Actualmente hay más de 130 redes 3G (WCDMA y CDMA2000 1x EVDO) alrededor del mundo. Estas redes ofrecen tasas de transferencia del orden de 1.4 Mbps (bajada) y 128 Kbps (subida). La tasa de descarga se espera que aumente a 10.2 Mbps en el 2009.

• La potencia de procesamiento (velocidad y capacidad de almacenamiento de la CPU) de los dispositivos móviles está creciendo aceleradamente.

• La existencia de sistemas operativos para dispositivos móviles (como Symbian o Windows Mobile) que permiten la descarga e instalación de una gran variedad de aplicaciones. Adicionalmente estos S.O suportan servicios como e-mail, SMS[14]/MMS[15] y aplicaciones desarrolladas en C++ y Java.

En cuanto a los que existen actualmente, al infectar un dispositivo, muestran unas señales inequívocas las cuales incluyen [14], [37]:

• Cambios en los íconos en el dispositivo móvil, como con *skulls*, puede indicar una infección

• Corrupción de funcionalidades, como las fuentes distorsionadas o la no muestra de texto ingresado, puede ser señal de infección.

• Algunos virus incluyen muestra de texto o imágenes para darle crédito al autor del malware

Desde luego resultaran extrañas estas acciones para el usuario, sin embargo, el malware móvil puede realizar muchas más acciones entre las que se encuentran [20]:

• Difundirse a través de Bluetooth, MMS
• Enviar mensajes SMS
• Infectar archivos
• Permitir control remoto del teléfono celular
• Infectar archivos
• Modificar o reemplazar iconos o aplicaciones del sistema
• Instalar fuentes y aplicaciones falsas o no operativas
• Instalar otros programas maliciosos
• Bloquear tarjetas de memoria
• Robar datos

Todas estas acciones son directas, sin embargo, existe un efecto indirecto importante el cual consiste en descargar rápidamente la batería debido a los múltiples intentos del gusano por difundirse a través de Bluetooth [14].

En cuanto a los vectores de infección, los más comunes de este tipo de virus son Bluetooth, MMS, e-mail, sincronización y tarjetas de memoria, sin embargo, Bluetooth es el vector más común hasta la fecha debido a la publicación de Cabir en el 2004, como veremos más adelante [14].

Desde el 2004, el génesis de los malware móviles, más de 30 familias de malware han aparecido [14]. Es importante en la nueva era del malware móvil analizar las familias y variantes que han salido a la luz debido a que, con este entendimiento, es posible detectar nuevas formas de contrarrestar esta amenaza, lo cual es importante para la seguridad de la información a nivel mundial.

En la evolución del código malicioso móvil, cuatro familias (*Cabir, Skuller, Doombot y Cardtrap*) dominan la escena basados en la mayor cantidad de variantes. Estas familias están consideradas las pioneras en su categoría [14]:

• **CABIR:** Es el primer malware móvil en

[14] Short Message Service
[15] Multimedia Messaging System

utilizar Bluetooth, con 35 variantes. Dichas variantes arreglaron los fallos de distribución de Bluetooth y le añadieron el método de MMS lo cual aumentó su potencial de propagación

• **SKULLER:** *Skuller* es una derivación de *Cabir* que incrementó su carga útil conteniendo otros virus y modificando las imágenes y el texto que se muestra. Una de las más grandes lecciones de la familia *Skuller* es la facilidad con la que se le pueden agregar múltiples malware móviles a un solo virus y luego copiar todo al dispositivo infectado.

• **DOOMBOT:** El primer troyano *Doomboot* apareció en el 2005 como *Trojan.SymbOS.Doomboot*. *Doomboot* añadió varios malware móviles conocidos a su carga útil. Por ejemplo, el malware móvil "*B-52 Bomber*" de Symbian tiene 25 variantes.

• **CARDTRAP:** La primera vez que apareció fue en Septiembre de 2005 infectando teléfono celulares Nokia con sistema operativo Symbian OS explotando una de las vulnerabilidades conocidas de dicho sistema operativo. *Cardtrap* fue el primer malware móvil *cross-plataform* que usa una tarjeta de memoria para propagarse debido a que en su carga útil tenia malware tanto para Symbian como para Windows. Tiene 38 variantes.

Luego de exponer las diferentes familias de malware móvil, es importante conocer la historia del malware móvil hasta la fecha debido a que esto constituye un elemento esencial para preparar a los administradores de los sistemas en su administración de la seguridad [14], sin embargo, para lograr entender cómo estas tendencias migraron de los PC a los dispositivos móviles, es necesario revisar algunos hitos de la historia del malware desde sus inicios:

• **1949:** *Von Neumann* presentaba por primera vez la posibilidad de desarrollar pequeños programas replicantes capaces de tomar el control de otros programas de similar estructura.

• **1949:** Creación de *CoreWar*, el precursor de los virus informáticos}

• **1970:** El Dr. *Gregory Benford* publica, por primera vez, la idea de un virus describiendo específicamente el término *computer virus* y dando un ejemplo de un programa denominado vacuna para eliminarlo.

• **1972:** *Creeper* creado por Robert Thomas Morris para IBM 360, el primer virus formalmente reconocido

• **1972:** *Reaper*, primera vacuna la cual estaba destinada a eliminar el virus *Creeper*

• **1975:** Animal/*Pervade*, primer troyano de la historia

• **1984:** Cohen introduce la definición formal de un virus: "Programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí mismo"

• **1988:** Adleman introduce la definición formal de un troyano: "Programa alojado dentro de otra aplicación u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene".

• **1988:** *Robert Tappan Morris* crea el primer gusano de reproducción masiva, infectando y colapsando el 10% de ARPANET

• **1995:** Nace el mítico grupo español 29A el cual cambiaría la historia del malware móvil con su creación "Cabir"

• **1998:** Virus CIH el cual borraba los primeros 2048 sectores del disco duro sobrescribiendo algunos tipos de Flash-Bios

• **2003:** Inicio de la era de las Botnet

A partir de este momento inicia la era del malware móvil con la publicación del código fuente de *Cabir* por parte del grupo 29A (primero de enero de 2005) lo cual cambió significativamente la perspectiva del desarrollo del malware móvil, tal como la conocemos hoy debido a que se propició la creación de una gran cantidad de variantes y modificaciones. El malware móvil existe desde el 2000, sin embargo, no fue sino hasta el 2005 que tomó importancia [14].

Con relación al malware móvil, los autores describen en las diferentes eras, los virus más característicos de cada una de ellas.

### *A. PRE-GÉNESIS Y GÉNESIS (2000-004) [14], [36], [37].*

Comprende el inicio del malware móvil como una amenaza seria que debe ser tenida en cuenta. Su máximo expositor es el virus *Cabir* el cual, por primera vez, utilizó la tecnología Bluetooth para lograr difundirse logrando un impacto importante a nivel mundial. A continuación los malware más representativos de esta era:

| Nombre | Infección | Acción | Novedad |
|---|---|---|---|
| **Telefonica** | E-mail | Envío de mensajes SMS en España | Usa SMS |
| **Epoc.Fake** | Bluetooth | Pretende formatear el disco duro | Usa Bluetooth |
| **Hacktool.SMSDOS** | Sitio Web Internet | Ataque de denegación de servicio (Siemens) | Realiza un DoS usando SMS |
| **Cabir** | Bluetooth | Descarga de la batería debido al envío por medio de Bluetooth | Primer malware móvil |
| **Duts** | Infección de un directorio | Archivos del directorio quedan inútiles | Afecta a Windows CE |
| **Brador** | E-mail, sitios Web, P2P | Instalación de una puerta trasera | Instala un Backdoor |
| **Skulls** | E-mail, sitios Web, P2P | Aplicaciones inútiles, íconos de calaveras en el menú. | Explota una vulnerabilidad en Symbian |

Tabla 1. PRE-GÉNESIS Y GÉNESIS [14], [36]

### *B. EDAD MEDIA (2005)*

Representa un lapso de tiempo de transición en donde la novedad más relevante consistió en el surgimiento de los malware móviles multiplataforma que intentaban infectar tanto sistemas operativos móvil (Symbian) como tradicionales (Windows). A continuación los malware más representativos de esta era:

| Nombre | Infección | Acción | Novedad |
|---|---|---|---|
| **Cardtrap** | E-mail, sitios Web, P2P entre otros | Corrupción de aplicaciones, copia malware para Win el la tarjeta de memoria | Multiplataforma (Windows y Symbian) |

| | | | |
|---|---|---|---|
| **PbStealer** | E-mail, sitios Web, P2P entre otros | Envía la lista de contactos al primer dispositivo detectado por Bluetooth. | Roba información confidencial |

Tabla 2. EDAD MEDIA [14], [36]

### C. EDAD INDUSTRIAL (2006-2007)

Constituye la evolución de la edad media en cuanto a que aparece el primer malware realizado en J2ME, es decir, el primer virus que puede ejecutarse en la máquina virtual Java para dispositivos móviles, compatible con varios modelos de procesadores . Adicionalmente, las variantes de esta era se enfocan, especialmente, en el fraude financiero realizando acciones como envíos de mensajes a números *premium* sin consentimiento del usuario. A continuación los malware más representativos de esta era:

| Nombre | Distribución | Acción | Novedad |
|---|---|---|---|
| **RedBrowser** | E-mail, sitios Web, P2P entre otros | Envío de múltiples mensajes SMS | Realizado en J2ME |
| **Worm.MSIL.Cxover** | ActiveSync | Elimina “Mis documentos” | Cross-plataform |
| **Flexispy** | E-mail, sitios Web, P2P entre otros | Recolecta información de llamadas y SMS y las publica en un sitio Web | Aplicación espía comercializada abiertamente |
| **Mobler** | Propagación a través de medios de almacenamiento | Deshabilita funciones del sistema claves | Se propaga copiándose a si mismo en cualquier medio removible |
| **Viver** | E-mail, sitios Web, P2P entre otros | Envío de SMS a números premium | Orientado a producir fraude financiero |

Tabla 3. EDAD INDUSTRIAL [14], [36]

### D. TIEMPOS MODERNOS (2008- )

Finalmente, la era de los tiempos modernos representa la actualidad del mundo del malware móvil. Se caracteriza por tener como objetivo los nuevos dispositivos móviles de gran aceptabilidad que salen al mercado, como es el caso del *iPhone*. A parte de atacar nuevos sistemas operativos, el malware de esta era no aporta ninguna novedad extraordinaria que no haya sido vista en eras anteriores. A continuación los malware más representativos de esta era:

| Nombre | Distribución | Acción | Novedad |
|---|---|---|---|
| iPhone | Descarga desde sitios Web | Sobrescribe aplicaciones legítimas. | Diseñado para iPhone |
| InfoJack | Sitio web Chino en el que se descarga un software legítimo | Recolecta información del dispositivo y la envía a un servidor Web | Afecta Windows Mobile |
| POC.MM.Stranger | Bluetooth | Instala una puerta trasera que permite escuchar conversaciones | Permite acceso total al micrófono del dispositivo |

Tabla 4. TIEMPOS MODERNOS [14]

Uno de los malware más recientes es el gusano Yxes, descubierto en el mes de febrero de 2009 por la empresa de seguridad informática Fortinet [10]. El nuevo gusano utiliza como método de propagación los mensajes SMS y acceso a Internet.

El malware, denominado SymbOS/Yxes.A!worm (también conocido como “Sexy View”), afecta dispositivos móviles que tienen como sistema operativo SymbianOS S60 tercera edición (Por ejemplo: Nokia 3250), sin embargo, se ha reportado que el malware también funciona en teléfonos con SymbianOS S60 tercera edición FP1 (como por ejemplo: Nokia N73) [10].

El gusano contiene un certificado firmado por Symbian por lo que se instala como una aplicación válida de fábrica en dispositivos móviles que utilizan Symbian S60 tercera edición. Adicionalmente, obtiene los números de la lista de contactos y se intenta enviar automáticamente a través de mensajes SMS que contienen una URL maliciosa la cual contiene una copia del gusano (siempre y cuando el teléfono tenga habilitada la navegación a través de Internet) [10].

Por otro lado, Yxes intenta obtener información del dispositivo (tal como número serial o número de subscripción) e intenta copiarlo en un servidor remoto controlado por delincuentes informáticos. Lo que se realiza con dicha información después es algo desconocido al momento de escribir el reporte [10].

Debido a la estrategia de propagación del gusano, la cual consiste en dejar una copia del gusano en un servidor web, el virus puede mutar fácilmente. De acuerdo con Guillaume Lovet, *Senior Manager* del equipo *Fortinet Threat Research*, "Tal como va nuestro análisis, el gusano actualmente no recibe comandos del servidor remoto que contacta, sin embargo, debido a que las copias del virus se encuentran alojadas en los servidores maliciosos controlados por delincuentes informáticos, estos pueden actualizarse en cualquier momento, por lo tanto el gusano está mutando, añadiendo o removiendo funcionalidades. Estamos realmente en la era de las Botnet móviles." [10].

La siguiente sección del documento es clave debido a que responderá a la siguiente pregunta: ¿Es Sexy View la primera Botnet de dispositivos móviles?

## V. ANÁLISIS DEL MALWARE

La presente sección del documento se enfocará, básicamente, en el análisis del malware Yxes/Sexy View para determinar si se puede clasificar como una Botnet móvil. Para ello es primordial entender la plataforma de software sobre la cual funciona: Symbian

### A. SYMBIAN OS

El sistema operativo para teléfonos inteligentes Symbian consta principalmente de dos variantes:[37]:

• S60: Consiste en una suite de librerías y aplicaciones estándar. Intenta proveer poderosas características a teléfonos modernos con grandes pantallas a color, conocidos formalmente como *smart phones*. Soporta aplicaciones desarrolladas en Java MIDP[16], C++ y Python.

• UIQ: Esencialmente es una interfaz gráfica para el usuario que provee componentes adicionales al núcleo del sistema operativo. Soporta aplicaciones desarrolladas en C++ y Java

[16] Mobile Information Device profile

Debido a que Yxes está disponible para dispositivos S60, nos centraremos únicamente en esa plataforma. Dejándolo a un lado la parte de interfaz de usuario, Symbian cuenta con cuatro unidades de almacenamiento lógicas las cuales son [38]:

- C: FLASH RAM: Aplicaciones instaladas y datos del usuario
- D: TEM RAM: Almacenamiento temporal de archivos de aplicaciones
- E: MMC CARD: Tarjeta de almacenamiento masivo
- Z: OS ROM: Contiene la mayoría de los archivos del sistema operativo

Paralelamente, cuenta con una arquitectura de archivos en donde se encuentra una gran variedad de carpetas, sin embargo, las más importantes se enuncian a continuación [38]:

- *System/Apps:* Aplicaciones que son visibles para el usuario
- *System/Recogs:* Reconocimiento de componentes
- *System/Install:* Datos necesarios para desinstalar aplicaciones del usuario
- *System/libs:* Librerías del sistema y de aplicaciones de terceros

En estos espacios de almacenamiento se guardan los archivos más importantes del sistema operativo. Es tal la importancia de estas carpetas que si cualquiera de las aplicaciones que se encuentran almacenadas en *Apps* es deshabilitada, el usuario no podrá volver a usarla y será necesario realizar un *hard reset* [38].

Aparte de los directorios, Symbian cuenta con una serie de aplicaciones claves que se deben tener en cuenta al analizar malware [38]:

- System/Apps/Menu/Menu.app: Menú principal del teléfono celular
- System/Apps/AppInst/Appinst.app: Servicio de instalación
- System/Apps/AppMngr/AppMngr.app: Servicio de desintalación
- System/Apps/MMM/Mmm.app: Provee el servicio de envío y recepción de mensajes SMS, MMS, BT etc..
- System/Apps/Phonebook/ Phonebook.app: Servicio que provee la lista de contactos

Continuando con las aplicaciones, es importante comentar que cada una de ellas tiene un identificador llamado UID el cual tiene una longitud de 32 bits [38]. En caso de que cualquier otro ejecutable tenga el mismo UID, se asume como una copia de la misma aplicación [38]. Por ejemplo, si una aplicación en C: o en E: tiene exactamente el mismo nombre y ruta que una en Z:, ésta será ejecutada en lugar de la aplicación legítima en la ROM [38]. Este dato es muy importante tenerlo en cuenta la analizar el malware debido a que con esta técnica se puede realizar suplantación de procesos en los dispositivos.

Las aplicaciones no son más que ejecutables y en Symbian actualmente existen tres tipos de ejecutables nativos [38]:

- Foo.APP: Aplicaciones del usuario final, accesible desde el menú. Cada

aplicación debe tener su propio directorio en System/apps

• Foo.MDL: Reconocimiento de componentes. Provee asociación entre servicios para el resto del sistema operativo. Se ejecuta automáticamente al iniciar el dispositivo. Debe ser colocado en el directorio System/recogs

• Foo.EXE: Aplicaciones de línea de comando y servidores. No pueden ser accedidas por un usuario normal y consisten en servicios o utilidades usadas por las aplicaciones con interfaz gráfica

Los ejecutables, así como en Windows y Linux, tienen un formato definido el cual, en el caso de Symbian, es llamado E32Image [39]. Desde la versión 9 de Symbian, E32Image utiliza ABI (*Application Binary Interface*) el cual es un estándar desarrollado por ARM [17] y sus socios el cual define cómo los compiladores (RVCT -propietario- y GCEE -GNU-) deben generar los archivos ejecutables. El estándar le permite a los ejecutables de diferentes compiladores interactuar [39].

Teniendo en cuenta lo anterior, El formato de salida del compilador EABI es ELF (*Executable and Linking Format*), sin embargo, Symbian no utiliza este formato debido a que es muy grande y la ROM[18] de los dispositivos móviles es limitada por lo que Symbian convierte este ELF en una imagen E32 [39].

La forma de reducir esto consiste en reemplazar, por ejemplo, MyFunction() a un número y guardando el registro del mapeo en un archivo de definición con extensión .def [39]. La herramienta para realizar esto es elf2e32.exe la cual está localizada en la ruta \epoc32\tools del SDK de Symbian [39]. Básicamente es por esta razón que realizar ingeniería reversa en ejecutables ARM es mucho más complicado que realizarlo en ejecutables Intel.

El proceso de compilación se muestra de una manera más gráfica en la siguiente imagen [39]:

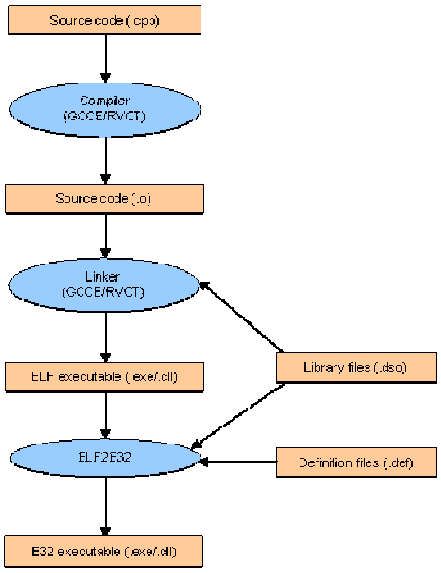



Figura 5. Proceso de generación de una E32Image [39]

El ejecutable E32 que se observa a final del proceso tiene la siguiente estructura [39]:

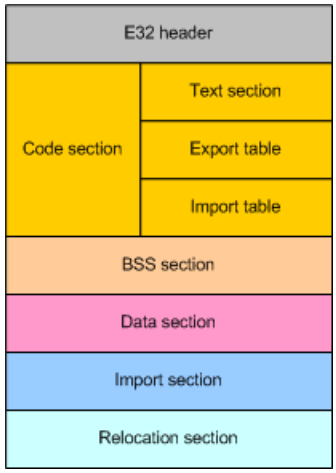



Figura 6. Estructura de un archivo E32 [39]

[17] Advanced RISC Machines
[18] Read Only Memory

A continuación una explicación de cada una de las secciones del archivo [39]:

• **Sección del encabezado:** Contiene una gran variedad de información sobre el archivo ejecutable (UID, fecha de creación, lenguaje, versión, número de DLL's importadas entre otros).La declaración de este archivo se puede encontrar en la ruta \epoc32\include\f32image.h

• **Sección del código:** Contiene todos los archivos objeto (.o) del código fuente así como la la tabla de exportación de direcciones que contiene todas las funciones exportadas

• **Sección BBS:** Contienen los datos no utilizados

• **Sección de datos:** Contiene los datos inicializados

• **Sección de importación:** Contienen la información referente a todas las funciones importadas que usa el programa

• **Sección de relocalización:** Contiene la tabla de relocalización que necesita Symbian OS para cargar el programa

Todos los ejecutables E32, junto con los recursos como imágenes, sonidos entre otros, son empaquetados en un archivo SIS (*SymbianOS Installation System*) el cual es el único método usado por el usuario normal para importar código ejecutable a un dispositivo [38]. En particular, un archivo SIS contiene [40], [41]:

**1.** Lenguajes usados
**2.** UID de la aplicación
**3.** Información de las versiones S60 soportadas
**4.** Archivos a instalar: Aplicaciones APP GUI, componentes de reconocimiento MDL, MBM (*Multi BitMap Image*), archivos AIF (*Application Information Files*) y archivos de recursos (RSC, RSS, RSP, Rxx)
**5.** Archivos que se ejecutarán mientras se instala
**6.** Certificados

Luego de conocer el sistema operativo donde funciona el malware, es pertinente conocer los hallazgos generales conocidos hasta ahora sobre el gusano Yxes debido a que son éstas características las que se vana c comprobar mediante un análisis forense para determinar si Yxes se comporta como una Botnet móvil.

## B. YXES O SEXY VIEW

A manera de introducción, se exponen algunos datos generales del gusano [43]:

• Alias conocidos: Worm:SymbOS/Yxe, Worm:SymbOS/Yxe.gen

• Clase: Symbian Worm

• Primera detección. 18 de febrero de 2009

• Síntomas visibles: Anormal aumento en el valor de las facturas de telefonía, rápida pérdida de batería, imposibilidad de ejecutar las siguientes aplicaciones: *AppMgr, TaskSpy, Y-Tasks, ActiveFile, TaskMan*

• Una vez instalado, no existe un icono o información relacionada que se pueda encontrar en el menú del sistema.

• Si la verificación en línea no está activada en el dispositivo móvil, el

gusano se instala como una aplicación normal bajo el nombre Sexy View

• La instalación del virus se realiza solamente si el usuario lo autoriza

Además de los síntomas visibles, el malware realiza las siguientes acciones [43]:

• Se ejecuta como el proceso "EConServer.exe" el cual se puede camuflar debido a un proceso de nombre parecido: "EComServer.exe" Este proceso se iniciará automáticamente cada vez que se reinicie el dispositivo.

• Intenta terminar ciertos procesos como el administrador de aplicaciones (*AppMgr*). La siguiente es una lista de los procesos que intenta destruir: *AppMgr, TaskSpy, Y-Tasks, ActiveFile* y *TaskMan*

• Copia los siguientes archivos siguientes archivos:

c:\sys\bin\EConServer.exe, c:\private\101f875a\import\[2001EB45].rsc

• Crea un semáforo llamado EConServerSemaphore_0x2001EB45 el cual asegura que una sola copia del gusano sea instalada en el dispositivo

• Revisa los mensajes SMS en la bandeja de entrada del dispositivo (sin borrarlos) y, en particular, busca la cadena de caracteres "olpx" posiblemente seguida por una D o una K

• Recolecta la siguiente información: IMEI, IMSI (*subscription number*), fabricante del dispositivo, modelo del dispositivo. Si el modelo no se puede obtener, el gusano coloca como nombre por defecto Nokia 3250

• Intenta silenciosamente conectarse a Internet enviando un HTTP *request* con el modelo del teléfono y la versión del gusano y obtiene respuestas HTTP, en particular las respuestas que contienen el string "olpx"

• Crea un log llamado mr.log en el cual escribe varios estados de información tales como *"SetConnectionfailed", "SetConnectionSucceeded", "TimeUptoRoot"*

• Crea un archivo .SISX (archivo de instalación de Symbian firmado) llamado root.sisx en la carpeta C:\Data

• Modifica el archivo C:\system\data\System.ini

• Accede y desbloquea, si es necesario, y almacena información en la tarjeta de memoria extraíble.

Todas estas acciones son las que se van a tratar de comprobar al realizarle análisis forense al malware, a partir de un procedimiento específico de malware móvil.

## C. PROCEDIMIENTO DE ANÁLISIS DE MALWARE MÓVIL

El NIST[19] define la informática forense en dispositivos móviles como la ciencia que se encarga de recuperar y recolectar evidencia digital de un teléfono móvil bajo una serie de condiciones forenses usando unos métodos aceptados [42]. Para realizar esto, la informática forense es soportada por herramientas tecnológicas de extracción y análisis de datos debido a

[19] National Institute of Standards

la gran cantidad de información que puede obtener de un dispositivo vulnerado [42].

En el presente análisis se va a basar en una guía metodológica para realizar análisis forenses en dispositivos móviles orientada a incidentes, con el fin de obtener evidencia digital del comportamiento del malware Yxes. Dicha evidencia servirá para establecer si el comportamiento del gusano tiene alguna relación con el funcionamiento de las Botnets típicas actuales.

La guía fue simplificada obviando los temas estrictamente forenses debido a que el ataque se realiza de forma controlada y no simula una situación real en donde la evidencia digital debe ser admisible ante la corte. Teniendo en cuenta lo anterior, el procedimiento de análisis del malware es el siguiente:

• **FASE PREPARATORIA:** Principalmente trata de la preparación de todos los elementos necesarios para efectuar con éxito el procedimiento. En esta fase solamente se va a realizar una actividad la cual es determinar las herramientas forenses a utilizar. En este caso, y teniendo en cuenta la gran variedad de herramientas que existen actualmente [42], se escogió *Device Seizure* para realizar el procedimiento.

• **FASE DE RECOLECCIÓN DE INFORMACIÓN:** Consiste en la recolección de la evidencia digital [42]. Esta fase se realiza la actividad de adquisición de la imagen de datos, la cual se realiza automáticamente usando la herramienta seleccionada.

• **FASE DE ANÁLISIS:** Consiste en el análisis de los datos recolectados [42]. Esta fase es efectuada por los investigadores forenses y, en general, se identifican los datos tanto físicos como lógicos para construir una línea de tiempo en donde se correlacionen todos los hechos y se pueda obtener la mayor cantidad de detalles del incidente ocurrido. En este caso, las actividades que se van a realizar son: Recuperar datos borrados, obtener información oculta y realizar análisis de datos lógicos (Identificadores del dispositivo, Información de la lista de contactos, Información del calendario, Mensajes de texto, Registro de llamadas (recibidas, perdidas, marcadas), Correo electrónico, Fotos /Videos / Audio, Mensajes multimedia, mensajería instantánea y navegación web, Documentos electrónicos, Identificación procesos en ejecución, Revisar los logs del sistema e Identificar rastros de conexiones (Bluetooth, Irda, cable, HTTP). Se realizará énfasis especial en los logs de conexión HTTP debido a que esta comunicación podría representar comunicación con el Bot Master de la Botnet.

• **FASE DE REPORTE:** Consiste en documentar todas las acciones, eventos y hallazgos obtenidos durante el proceso [42]. Esta fase se enfocará en relacionar los hallazgos de Fortinet sobre Yxes y los hallazgos resultados del análisis forense.

Luego de definir el procedimiento, se procede a aplicarlo primero instalando y ejecutando el malware para luego realizar el análisis forense orientado a incidentes.

## D. INSTALACIÓN DE YXES

El primer paso para realizar el análisis consiste en obtener una muestra del malware. Para ello, se recurrió a la base de datos de malware pública *Offensive Computing* como se muestra a continuación [48]:

Figura 7. Información general de Yxes.B [48]

Como se aprecia en la imagen anterior, el malware fue detectado por el antivirus AVG como SymbOS/Yxes, con fecha de adición el 6 de marzo de 2009 y formato SISX (equivalente al SIS presente en las versiones de Symbian anteriores a la 9).

El archivo ejecutable viene comprimido en un .ZIP por lo que, al extraerlo, se obtiene un EXE. Este archivo es el que se va a instalar en el dispositivo (cambiándole la extensión a SISX) el cual es un Nokia N73 con sistema operativo Symbian OS S60 3rd edición.

Antes de iniciar, se realizaron las siguientes acciones por motivos de seguridad:

• Remover la tarjeta de memoria extraíble: Debido a que el análisis forense se va a realizar solamente en la memoria del teléfono (para detectar principalmente conexiones con un Bot maestro), la tarjeta extraíble no es necesaria.

• *Hard Reset:* Se realiza con el fin de eliminar información residual anterior que puede complicar la información obtenida a través del análisis forense. Este procedimiento se deberá realizar varias veces debido a que las herramientas forenses actuales son capaces de recuperar información eliminada anteriormente. Para el Nokia N73 el *Hard Reset* se realiza encendiendo el dispositivo manteniendo presionado *, 3, SEND y POWER.

• Eliminación de la lista de contactos: El malware intentará enviar un SMS a toda la lista de contactos por lo que se eliminará y se dejará solamente un número conocido con el fin de obtener la URL desde la cual se descarga el malware. Por precaución, también se elimina la que se encuentra en la SIM.

Figura 8. Verificación de la existencia de un solo contacto de prueba

Desde luego es necesario realizar una copia de respaldo de esta lista de contactos, la cual se almacena en la tarjeta de memoria extraíble.

A continuación, se procede a probar la conexión a Internet en el dispositivo. Debido a que el N73 de Nokia (tipo RM-132 y modelo N73-5) no soporta conexión 3G, se realizará a través de GPRS:

Figura 9. Verificación de la conexión a Internet utilizando el protocolo HTTP

En cuanto a las capturas de pantalla, se va a utilizar el programa *freeware* "*Screenshot*" proporcionado por *Antony*

*Pranata* [44]. Para poder observar los archivos del sistema, fue necesario realizar un procedimiento especial y novedoso [45] el cual permite desbloquear directorios originalmente no accesibles por seguridad y, de paso, permite instalar cualquier aplicación sin necesidad de firmarla lo cual anula por completo el exitoso mecanismo de seguridad que tiene la plataforma Symbian. Este paso es necesario debido a que, a pesar que el certificado es válido, la muestra obtenida presentó problemas en el momento de la instalación:

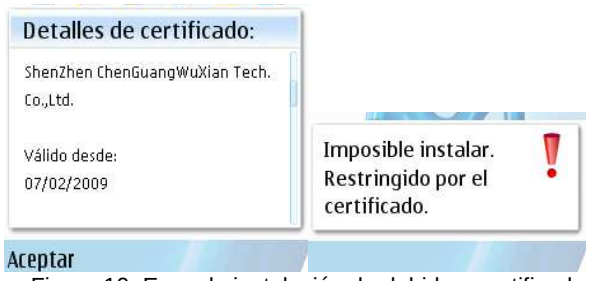



Figura 10. Error de instalación de debido a certificado corrupto

El procedimiento consiste en instalar una aplicación llamada X-plore (versión de prueba) [46] la cual es un explorador de archivos que permite realizar acciones que normalmente la interfaz de Symbian no permite (copiar, pegar, renombrar entre otros ). En la siguiente imagen se muestra los directorios bloqueados por Symbian (ubicaciones que contienen archivos ocultos, y los módulos de la RAM y la ROM):

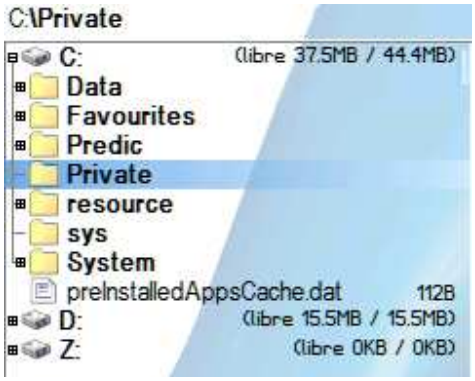



Figura 11. Carpetas Private y sys bloqueadas

Luego de esto, se instala la aplicación *HelloCarbide* la cual explota una vulnerabilidad de Symbian y desbloquea los directorios del sistema C:\SYS y C:\PRIVATE. Para ello, sin cerrar el X-plore, se ejecuta la aplicación *HelloCarbide* seleccionando la opción que se muestra a continuación:


Figura 12. Aplicación *HelloCarbide*

A continuación, se vuelve al X-plore (manteniendo la tecla menú al lado izquierdo del 1) para verificar que los directorios han sido desbloqueados:


Figura 13. Desbloqueo de las carpetas prohibidas

Seguidamente, se coloca el archivo installserver.exe en el directorio C:\sys\bin:

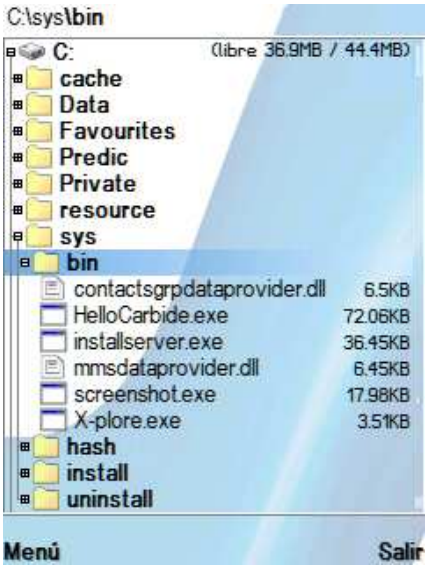



Figura 14. Colocación del archivo installserver.exe

Se reinicia el dispositivo debido a que *HelloCarbide* no permite ejecutar ninguna aplicación y desde que reinicia es posible instalar aplicaciones sin firmar. Como se expuso anteriormente, el certificado de la aplicación está corrupto por lo que fue necesario eliminarlo. Para esto se utilizó la herramienta *Freesigned* [47] la cual deja la aplicación sin firma. Finalmente, se procede a instalar el malware:


Figura 15. Instalación del malware Yxes (Sexy View)

Verificando que se encuentra correctamente instalado, comprobando una de las señales de la presencia de Yxes en el dispositivo, el archivo EConServer.exe en el directorio C\sys\bin:

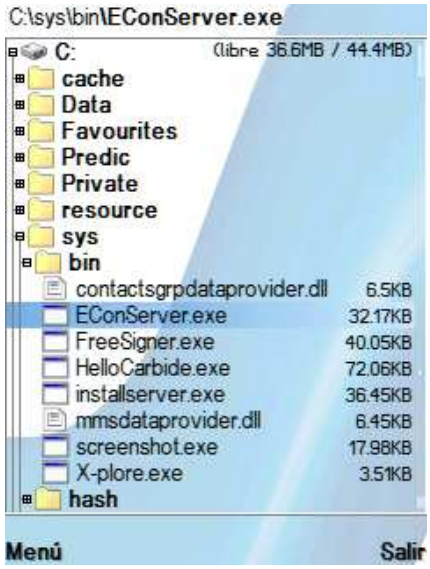



Figura 16. Verificación de la existencia del ejecutable EConServer.exe especificado por Fortinet

Luego de instalar el malware y de dejarlo actuar por un tiempo prudente, se procede a realizar el análisis forense orientado a incidentes

## E. ANÁLISIS FORENSE DEL DISPOSITIVO

### FASE PREPARATORIA

En la fase preparatoria se escoge la herramienta la cual tiene como versión 3.1.3345.32887. Luego de instalar el programa con los drivers respectivos, se inicia el seguimiento de los pasos de la guía metodológica.

### FASE DE RECOLECCIÓN DE INFORMACIÓN

En la fase de recolección de información, se realiza la adquisición de la imagen de la memoria, la cual consiste todos los datos lógicos del dispositivo por lo que se escoge el *plug-in* Nokia Symbian OS 9.x (*logical*). En cuanto al tipo de datos, se escoge *Backup and Private Data* debido a que en la aplicación de la guía original se muestra que esta adquisición

es la que tiene más probabilidades de adquirir evidencia digital de un malware.

## FASE DE ANÁLISIS

En la fase de análisis se empieza a evaluar la información obtenida como por ejemplo las propiedades generales de la adquisición:

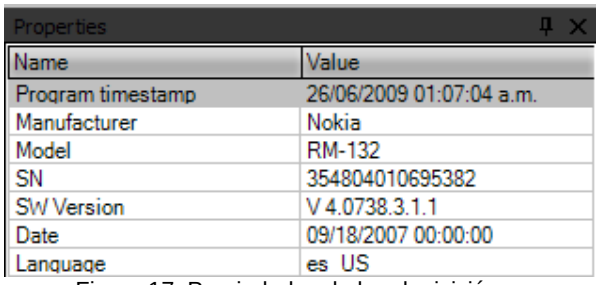



Figura 17. Propiedades de la adquisición

En la figura anterior se puede comprobar que el dispositivo es un Nokia RM-132 (N73) con el último firmware que corresponde al 18 de septiembre de 2007. En la adquisición se obtuvieron 471 registros con la siguiente estructura:

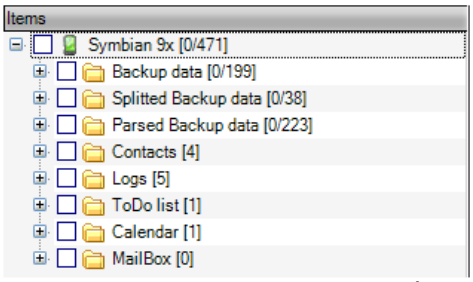



Figura 18. Estructura de la adquisición

Cada una de estas carpetas es explicada en la aplicación de la guía metodológica original [42]. Para encontrar la comprobación de los hallazgos de Fortinet, hacemos uso de una de las herramientas más útiles de *Device Seizure*: La funcionalidad "*Find*".

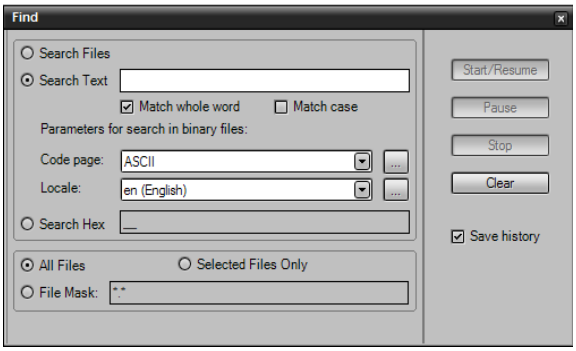



Figura 19. Funcionalidad de buscar cadena de caracteres

Esta es la característica que se va a utilizar para buscar las siguientes cadenas proporcionadas por Fortinet:

1. [2001EB45].rsc

```
....dc:\sys\bin\EConServer.exe
```

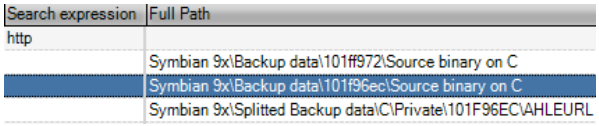

Figura 20. Evidencia de la instalación del *malware*

Corrobora que el archivo que acompaña a EConServer.exe permite que la aplicación se ejecute cada vez que el dispositivo inicia (*startup*).

2. EconServerSemaphore_0x2001EB45: No se encontró ningún registro de esta cadena

3. "olpx" seguido de una D o una K: No se encontró ningún registro de esta cadena.

4. HTTP request "olpx"



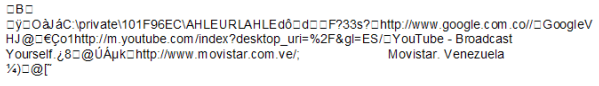



Figura 21. Evidencia de navegación más no de comunicación con un *Bot Master*

5. “mr.log” – “Set Connection Failed” – “Set Connection Succeded” – “TimeUptoRoot”: No se encontró ningún registro de esta cadena.

6. “root.six”: No se encontró ningún registro de esta cadena.

A continuación se analizan unos archivos que potencialmente puedan contener la evidencia que relaciones a Yxes con una Botnet:

C:\Private\100012a5\DBS_10207216_SWinsLog.db - Instalation log of Softwares

| time | uid | name | vendor | version | action | startup |
|---|---|---|---|---|---|---|
| 788455139 14764766 | 536872277 | Screenshot | Antony Pranata | 3.01(0) | 0 | 1 |
| 1598767639 14764766 | -1610609715 | X-plore | Lonely Cat Games | 1.32(0) | 0 | 0 |
| -348417254 14757423 | -397690606 | HelloCarbide | Vendor-EN | 1.00(0) | 0 | 0 |
| 1654747621 14757424 | 270512361 | MMSSync | Nokia | 1.00(0) | 0 | 1 |
| 1662460746 14757424 | 270530930 | Contacts Group DS Plugin | Nokia | 1.11(0) | 0 | 1 |
| 1908818968 14764767 | -289773696 | FreeSigner | junnikokuki | 1.00(0) | 0 | 1 |
| 2021470968 14764767 | 536996677 | Sexy View | Play Boy | 1.06(0) | 0 | 1 |

Figura 22. Evidencia la fecha de instalación del malware SexyView

En este archivo se muestra el UID de las aplicaciones instaladas por el usuario, la fecha y hora de instalación, la versión y si se ejecutan al iniciar. Claramente se puede apreciar que Sexy View inicia automáticamente cada vez que se enciende el dispositivo.

\101f401d\Logdbu.dat is the log file.

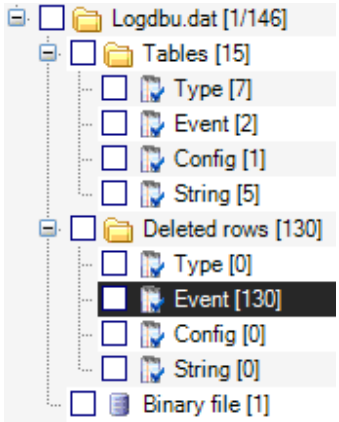



Figura 23. Estructura del Logdbu.dat

Este archivo contiene el log general de eventos del dispositivo, entre los que se encuentran el tráfico GPRS. En Deleted Rows, Event se pueden apreciar las diferentes sesiones de tráfico GPRS:

| | | | | | |
|---|---|---|---|---|---|
| 2 | Tigo web | 0 | 10 | 1 | Data |
| 2 | Tigo web | 0 | 155 | 1 | Data |
| 2 | Tigo web | 0 | 316 | 1 | Data |
| 2 | Tigo web | 0 | 319 | 1 | Data |
| 2 | Tigo web | 0 | 329 | 1 | Data |
| 2 | Tigo web | 0 | 339 | 1 | Data |
| 2 | Tigo web | 0 | 349 | 1 | Data |

Figura 24. Log tráfico GPRS

A pesar que se encuentra el registro, si entramos al link de Dara encontramos lo siguiente:

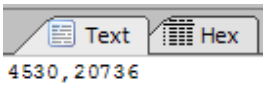



Figura 25. Data de las sesiones de conexión a Internet

Es evidente que no se puede obtener información sobre el tráfico que se envió o se recibió por lo que no es posible determinar si eran comandos del *Bot Master*.

Finalmente, se intentó realizar adquisición física del dispositivo para obtener el volcado de los procesos que se ejecutan en el teléfono de prueba, sin embargo, no fue posible realizarlo debido

a que ocurrió lo mismo que sucedió cuando se intentó probar la guía metodológica para realizar análisis forense en dispositivos móviles: El procedimiento no fue posible efectuarlo debido a que el soporte de Paraben no proporcionó una forma de realizarlo [42].

FASE DE REPORTE

Los hallazgos encontrados no fueron los esperados. El comportamiento del malware anunciado por Fortinet no se manifestó en el momento de análisis. Por ejemplo, no hubo un aumento en el valor de las facturas debido a que en ningún momento el malware intentó enviar mensajes SMS con la dirección web para descargar el gusano. Por otro lado, se puedo ejecutar las aplicaciones que supuestamente iban a estar deshabilitadas. Finalmente, no se encontró registro de la cadena “olpx” presente en el funcionamiento del malware según Fortinet ni hubo evidencia de la existencia del archivo mr.log ni del archivo root.sisx en C:\Data.

En cuanto al análisis forense, la herramienta para dispositivos móviles no proporcionó el detalle requerido en la información obtenida como por ejemplo en el archivo Logdbu.dat en donde posiblemente se encuentre el registro de las conexiones HTTP que realiza el malware.

Lo único que se pudo comprobar con la herramienta forense fue la instalación del malware verificando la existencia del archivo EConServer.EXE y su respectivo rsc. Adicionalmente se verificó que el malware queda configurado para que inicie automáticamente cuando se enciende el dispositivo.

## VI. CONCLUSIONES

- El malware yxes no puede ser considerado como el inicio de la era de las Botnets en dispositivos móviles debido a que, mediante el análisis forense realizado, no se pudo obtener evidencia de comunicación entre el malware y un atacante remoto.

- El malware no presentó el comportamiento especificado por la fuente que lo descubrió por lo que no se puede afirmar que, por lo menos la muestra obtenida, sea una copia real del original.

- La informática forense para dispositivos móviles aún no cuenta con una herramienta capaz de proporcionar evidencias digitales de incidentes de seguridad como por ejemplo infección de malware.

- El comportamiento del malware yxes se puede comprobar utilizando la técnica de ingeniería reversa [37], sin embargo, la única herramienta que permite realizar este procedimiento en dispositivos móviles es IDAPro la cual es costosa para fines académicos (USD 257).

- Los sistemas operativos móviles no son inmunes a vulnerabilidades clásicas de los pc como los buffer overflow. Ejemplos de estas son las descubiertas en symbian [41] y en J2ME [49]. Si a esto se le añade la posibilidad de obtener una Shell en Symbian [41] estamos hablando de un nuevo tipo de malware que no necesitará de la interacción con el usuario para instalarse por lo que la expansión de un gusano de este tipo en la red celular sería de grandes dimensiones. Esto representa un

ambiente propicio para la expansión de las Botnets móviles.

- Actualmente existe muy poca conciencia respecto al riesgo informático que representan los dispositivos móviles.

- El aumento del uso de aplicaciones críticas (como la banca móvil o las compras en línea) en los dispositivos móviles llamará cada vez más la atención de los delincuentes informáticos por lo que se espera que en los próximos años las amenazas en términos de seguridad de la información aumenten en este tipo de dispositivos.

## RECONOCIMIENTO

Quiero agradecer a mis padres por el apoyo y la motivación que me proporcionaron para realizar el presente trabajo de investigación. A Maximiliano y a María Camila por ayudarme a revisar la redacción en inglés. Especial agradecimiento para Andrés Ramírez quien realizó una extensiva revisión de la redacción de todo el artículo. Finalmente, y no menos importante, agradecer a mi hermana Cindy Castillo por ayudarme con las referencias y con la unificación de toda la información. Gracias a todos.

## REFERENCIAS

[1] BORGHELLO Cristian. "Cronología de los virus informáticos: La historia del malware". ESET para Latinoamérica http://www.eset-la.com/press/informe/cronologia_virus_informaticos.pdf

[2] Fortinet. “Overcoming mobile insecurities”. FORTIGUARD BLOG. 12/05/09. http://blog.fortinet.com/overcoming-mobile-insecurities/

[3] GTISC. "Emerging Cyber Threats Report for 2009". Georgia Tech Information Security Center. 15/10/08. http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

[4] ADAMS John. "Neutralizing the Smartphone Security Threat". EXPERT ADVICE. Tech News World. 17/06/09. http://www.technewsworld.com/rsstory/67354.html

[5] MATURANA Jesús. "Ultraportátiles: Linux, Windows, Android y ¿Symbian?". THE INQUIRER. 17/04/09. http://www.theinquirer.es/2009/04/17/ultraportatiles-linux-windows-android-y-%c2%bfsymbian.html

[6] PENALVA Javier. "ARM prepara procesadores de doble núcleo para supermóviles". XATAKA. http://www.xataka.com/moviles/arm-prepara-procesadores-de-doble-nucleo-para-supermoviles

[7] LAWTON George. "Is It Finally Time to Worry about Mobile Malware?", INDUSTRY TRENDS. 2008. http://doi.ieeecomputersociety.org/10.1109/MC.2008.159

[8] BARFORF Paul. YEGNESWARAN Vinod. "An Inside Look at Botnets". Advances in Information Security. Malware Detection. Springer US. 2007. http://pages.cs.wisc.edu/~pb/botnets_final.pdf

[9] GOVIL J. “Examining the criminology of bot zoo”. Maharshi Dayanand Univiversity. Information, Communications & Signal Processing. 6th International Conference, Singapore. 2007. http://ieeexplore.ieee.org/Xplore/login.jsp?url=http://ieeexplore.ieee.org/iel5/4446227/4449533/04449633.pdf%3Farnumber%3D4449633&authDecision=-203

[10] Fortinet. “Fortinet Investigates a New SMS Mobile Worm: Yxes.A”. FORTIGUARD ADVISORY (FGA-

2009-07). FortiGuard Center. Threat Research and Response. 18/02/09. http://www.fortiguardcenter.com/advisory/FGA-2009-07.html

[11] FORESMAN Chris. “Survey: one in five US households are cellphone only”. ARS Technica. 10/05/09. http://arstechnica.com/telecom/news/2009/05/survey-one-in-five-us-households-are-cellphone-only.ars

[12] Press Release. “Gartner Says Worldwide Mobile Phone Sales Declined 8.6 Per Cent and Smartphones Grew 12.7 Per Cent in First Quarter of 2009”. GARTNER. 20/05/09. http://www.gartner.com/it/page.jsp?id=985912

[13] McAfee. "Mobile Security Report 2009". McAfee e informa telecoms & media. 2009. http://www.mcafee.com/us/local_content/reports/mobile_security_report_2009.pdf

[14] DUNHAM Ken, ABU-NIMEH Saeed, BECHER Michael, FOGIE Seth, HERNACKI Brian, MORALES Jose Andrés, WRIGHT Craig. "Mobile Malware Attacks and Defense", Syngress Publishing Inc - Elsevier Inc, Burlington Unites States Of America, Tech News World, http://books.google.com.co/books?id=Nd1RcGWMKnEC&pg=PT28&dq=mobile+malware&ei=bPw6SunLE4i0zASb68C6BQ

[15] MMA. "Mobile Banking Overview". Mobile marketing association. 2009. http://www.mmaglobal.com/mbankingoverview.pdf

[16] SANDOVAL, Álvaro. "Banca móvil gana terreno en Colombia; cinco de los principales bancos empiezan a recoger frutos", PORTAFOLIO. 15/04/09. http://www.portafolio.com.co/economia/economiahoy/2009-04-15/ARTICULO-WEB-NOTA_INTERIOR_PORTA-4978089.html

[17] NUTTALL, Chris. "Nokia sends $70m mobile payment to Obopay". FINANCIAL TIMES TECH BLOG. 25/03/09. http://blogs.ft.com/techblog/2009/03/nokia-sends-70m-mobile-payment-to-obopay/

[18] CBC News. “Smartphone viruses can't spread well — yet: study”. CBC News. 02/04/09. http://www.cbc.ca/technology/story/2009/04/02/tech-090302-smartphone-virus.html

[19] Press Release. “Programa Android de Google gana apoyo, según analistas”. REUTERS. Helsinki Finlandia. 11/05/09. http://lta.reuters.com/article/internetNews/idLTASIE54A1QQ20090511

[20] GOSTEV Alexander. "Mobile Malware Evolution: An Overview, Part 1". Viruslist. 2006. http://www.viruslist.com/en/analysis?pubid=200119916

[21] McAfee® Avert® Labs. "Informe de McAfee sobre amenazas: Primer trimestre de 2009". McAfee. http://img.en25.com/Web/McAfee/5395rpt_avert_quarterly-threat_0409es_s_fnl.pdf

[22] ZHAOSHENG Zhu, GUOHAN Lu, YAN Chen, FU Z.J, ROBERTS P, KEESOOK Han. " Botnet Research Survey", Northwestern Univ., Evanston, IL, Computer Software and Applications, 2008. COMPSAC '08. 32nd Annual IEEE International, 2008. http://ieeexplore.ieee.org/Xplore/login.jsp?url=http://ieeexplore.ieee.org/iel5/4591502/4591503/04591703.pdf%3Farnumber%3D4591703&authDecision=-203

[23] PRINCE Brian. “Security Researchers Uncover 70GB of Financial Data Stolen by Botnet”. eWEEK. 04/05/09. http://www.eweek.com/c/a/Security/Security-Researchers-Uncover-70-GB-of-

Financial-Data-Stolen-by-Botnet-501015/?kc=rss

[24] KREBS Brian. "Stolen Identities Sold Cheap on the Black Market". THE WASHINGTON POST. 19/03/09. http://voices.washingtonpost.com/securityfix/2007/03/stolen_identities_two_dollars.html

[25] PRINCE, Brian. "Finjan Researchers Uncover Marketplace for Botnets". eWEEK Network Security & Hardware. 17/06/09. http://www.eweek.com/c/a/Security/Finjan-Researchers-Uncover-Marketplace-for-Botnets-595200/?kc=rss

[26] HONKASALO H, PEHKONEN K, NIEMI, M.T, LEINO, A.T. "WCDMA and WLAN for 3G and beyond". Wireless Communications. IEEE. 2002. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=998520

[27] GSA. "GSM/3G Stats". Global Mobile Suppliers Association. http://www.gsacom.com/news/statistics.php4

[28] CDMA Development Group. "4Q 2008 Subscribers Statistics". CDMA Worldwide. http://www.cdg.org/worldwide/report/084Q_cdma_subscriber_report.pdf

[29] MOHR Werner. "Mobile Communications Beyond 3G in the Global Context". SIEMENS Mobile. http://www.cu.ipv6tf.org/pdf/werner_mohr.pdf

[30] Press Release. “Nokia presenta su teléfono 3G más barato”. REUTERS. Paris Francia. 18/05/09. http://es.reuters.com/article/esEuroRpt/idESMAE54H0JG20090518

[31] BÄCHER Paul, HOLZ Thorsten, KÖTTER Markus, WICHERSKI Georg. "Know your Enemy: Tracking Botnets". THE HONEYNET PROJECT. http://www.honeynet.org/book/export/html/50

[32] MIELKE Clinton, CHEN Hsinchun. "Botnets, and the cybercriminal underground". Department ShadowServer Found., Univ. of Arizona Tucson, Tucson, AZ, Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference, 2008, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4565058

[33] Jorge. “Reporte de amenazas de mayo”. Blog ESET Latinoamérica. 31/05/09. http://blogs.eset-la.com/laboratorio/2009/05/31/reporte-amenazas-mayo-2009/

[34] STINSON Elizabeth, MITCHELL John. "Characterizing Bots’ Remote Control Behavior", Department of Computer Science, Stanford University, Stanford, CA 943052007, Lecture Notes in Computer Science, Detection of Intrusions and Malware, and Vulnerability Assessment, 2007, http://www.stanford.edu/~stinson/pub/botswat_long.pdf

[35] IANELLI Nicholas, HACKWORTH Aaron. “Botnets as a Vehicle for Online Crime”. CERT Coordination Center, United States, 2005. http:// www.cert.org/archive/pdf/Botnets.pdf

[36] BOSE Abhijit, SHIN Kang. " On Mobile Viruses Exploiting Messaging and Bluetooth Services", Securecomm and Workshops, Dept. of Electr. Eng. & Comput. Sci., Michigan Univ., Ann Arbor, MI, 2006, http ece.wpi.edu/~wjlou/htmls/teaching/ECE579S/files/11-3.pdf

[37] ZHANG Jie. "Finding the “Bad guys” on the Symbian”. Fortinet Information Technology, Tianjin, China, 2007, http://www.fortiguardcenter.com/papers/AVAR2007_Find_Out_the_Bad_guys_on_the_Symbian.pdf

[38] NIEMELA Jarno. “What Makes Symbian Malware Tick”. F-Secure Corporation. Virus Bulletin. 2005. http://www.virusbtn.com/pdf/conference_slides/2005/JNiemela_VB2005_sanitized.pdf

[39] PRANATA Antony. "New Symbian OS 9 Executable File Format (E32Image)". http://www.antonypranata.com/articles/new-symbian-os-9-executable-file-format-e32image

[40] SHUB-NIGURRATH. "Primer on Reversing Symbian S60 Applications". ARTEAM. 2007. http://news.nopcode.org/pdf/Primer_on_Reversing_Symbian_S60_Applications_by_Shub-Nigurrath_v14.pdf

[41] MULLINER Collin. "Symbian Exploitation and Shellcode Development", Fraunhofer-Institut for Secure Information Technology (SIT), Darmstadt, Germany, Blackhat Japan ,2008. http://events.ccc.de/congress/2008/Fahrplan/attachments/1171_CollinMulliner_ExploitingSymbian_BHJapan.pdf

[42] CASTILLO Carlos, ROMERO Andrés. "GUÍA METODOLÓGICA PARA EL ANÁLISIS FORENSE ORIENTADO A INCIDENTES EN DISPOSITIVOS MÓVILES GSM". Trabajo de Grado, Pontifica Universidad Javeriana, Bogotá Colombia, 2008. http://www.criptored.upm.es/guiateoria/gt_m142h1.htm

[43] Fortinet, "SymbOS/Yxes.A!worm", FORTIGUARD CENTER Virus Definition, FortiGuard Center, 09/06/09; http://www.fortiguardcenter.com/viruscency/SymbOS/Yxes.A!worm

[44] PRANATA Antony. "Screenshot". http://www.antonypranata.com/screenshot/download-screenshot-symbian-os-s60

[45] Cento. Hack para S60 3ªEdicion (HELLO CARBIDE). 2008. http://goponygo.com/blog/aplicaciones-symbian/hack-para-s60-3ªedicion-hello-carbide/

[46] Lonely Cat Games. X-Plore. http://www.lonelycatgames.com/?app=xplore&page=download&platform=symbian

[47] El rincon de symbian. "FreeSigned". http://www.elrincondelsymbian.com/Foro/programas-5-edicion/55240-freesigner-v1-00-s60v3-symbianos9-1-selfsigned-junnikokuki-freeware-valido-5800-a.html

[48] Offensive Computing. Http://www.offensivecomputing.net/

**Autores**

Carlos Castillo nació en Bogotá, Colombia, el 9 de Enero de 1987. Se graduó en el Colegio Santo Tomás de Aquino en el año 2003 y se encuentra estudiando actualmente en la Pontifica Universidad Javeriana de Bogotá D.C.

En el año 2007 publicó, junto con José Luis Gómez y Edgar Torres un artículo llamado "Blue MAC Spoofing: El backdoor de Bluetooth". Entre sus campos de interés se encuentra la seguridad informática, la informática forense y las aplicaciones web.

En el año 2008, junto con Andrés Romero, finalizó su trabajo de grado "Guía metodológica para realizar análisis forenses en dispositivos móviles GSM" obteniendo como logro más significativo la publicación de un artículo en el CLEI2008 realizado en Santa Fé Argentina.

Actualmente se encuentra realizando su práctica profesional en el área de seguridad informática de Belcorp, empresa líder en productos de belleza en América Latina.

Entre sus campos de interés se encuentra la seguridad informática, la informática forense y los dispositivos móviles.