Ing.USBMed, Vol. 8 (2) 48-57, 2017
DOI 10.21500/20275846.2955

Ingenierías USBMed

Armas Cibernéticas. Malware Inteligente para Ataques Dirigidos

Cyber Weapons. Intelligent Malware for Targeted Attacks

Jairo Eduardo Márquez Díaz[1]*

Resumen
En este artículo se muestra un análisis sobre el malware denominado Amenaza Persistente Avanzada o APT, el cual se es clasificado por autoridades internacionales, como una de las primeras ciberarmas que puede comprometer seriamente las infraestructuras críticas de una nación. Esto se debe en gran parte, a nuevos desarrollos de sistemas intrusivos más avanzados, que incorporan tecnologías y algoritmos dinámicos, que buscan integrar la inteligencia artificial y los algoritmos genéticos, entre otros, para hacer más complejos y completos los programas a la hora de efectuar un escaneo de los protocolos de red y/o registros, robo de información, espionaje o ataques dirigidos, donde el sigilo y la furtividad son factores clave para ello, haciéndolos indetectables, y cuya permanencia puede ser indefinida al interior de un sistema informático o red. Dicho esto, las diversas técnicas de ataque de este tipo de malware, pone entre dicho las barreras y sistemas de protección actuales, tanto lógicas como físicas. Además, con la futura incorporación de algoritmos neuro-evolutivos en su código fuente, las herramientas, protocolos y políticas de seguridad de la información van a requerir ser revaluadas prontamente.

Abstract
In this article, we present an analysis of malware known as Advanced Persistent Threat (APT), which has been classified by international authorities as one of the first cyber weapons that can seriously compromise a nation's critical infrastructures. This is due in large part to the new developments of more intrusive systems, incorporating dynamic technologies and algorithms, which seek to integrate artificial intelligence and genetic algorithms, among others, to make the programs much more complex and complete at the time to perform a scan of network protocols and/or registers, information theft, espionage or targeted attacks, where secrecy and stealth are key factors for this, making them undetectable, and whose permanence can be indefinite within a computer system or network. That said, the different techniques of attack of this type of malware, between said the current barriers and systems of protection, -logical and physical, -and also, with the future incorporation of neuroevolutionary algorithms in their source code, the tools, protocols and information security policies are going to require re-evaluation very soon.

Palabras Clave
Algoritmo genético; amenazas persistentes avanzadas; ciberarma; inteligencia artificial; malware; polimorfismo.
Key words
Artificial intelligence; advanced persistent threats; cyberweapon; genetic algorithm; malware; polymorphism.

[1] *Universidad de Cundinamarca, Cundinamarca, Colombia.*
*__Autor correspondiente__: jemarquez@unicundi.edu.co
Manuscrito recibido 10-04-2017; revisado 25-06-2017; aceptado 07-06-2017.

1. Introducción

El *malware* es un programa cuyo objetivo es infectar un sistema con el fin de tomar el control del mismo, y una vez hecho esto, modificar, sustraer, distraer, incomodar y/o dañar parcial o totalmente el software o hardware de un equipo de cómputo, una red o un sistema de comunicación. El malware se divide en varias clases, como son: virus clásicos, gusanos, troyanos, *riskware, ransonware, spyware, phishing, pharming, adware, hoax, spam, rootkits, backdoors, pop-ups, keylogger, stealer, dialer, pomware, Hijacker, Badware Alcalinos, exploit, Scam, Bomba fork, Scumware, LeapFrog, Botnet y Scareware, spearphishing, clickers,* entre muchos otros. Cada uno de estos programas es diseñado para efectuar infecciones puntuales en un sistema informático, por lo que algunos solo causan

molestias momentáneas, otros roban, bloquean, modifican, suplantan y/o destruyen información, causando pérdidas millonarias al afectado, comprometiendo en algunos casos las infraestructuras criticas de una nación.

Una línea aparte de los tipos de *malware* citados, son virus cuyo grado de letalidad es tal, que pueden bloquear o destruir grandes nodos de redes, no solo corporativas, sino de un país, incluso en la red de internet, donde su característica principal es la furtividad y sigilo a la hora de infectar, sustraer y/o atacar un sistema informático, una red de cómputo o un sistema de comunicaciones. En esta categoría entran las Amenazas Persistentes Avanzadas o APT (*Advanced Persistent Threat*)[1], cuyos rasgos de ataque se identifican por ser un malware que por sus características furtivas, puede perdurar al interior de un sistema informático por mucho tiempo sin ser detectado, aprovechando sus vulnerabilidades propias de fábrica o de la misma arquitectura de los protocolos de comunicación en el empaquetado de datos en una red. Los ataques de esta clase son planificados, y por ende, dirigidos contra blancos específicos. Por consiguiente, el objetivo de este tipo de ataque, es el espionaje corporativo, industrial, gubernamental y/o militar, en la que se busca obtener y/o manipular información crítica, comprometiendo con ello la seguridad de la información de la víctima sea este empresarial, militar o gubernamental, que por lo regular no se percatan de ello hasta que es demasiado tarde. El ataque físico con un APT está en un segundo plano, lo que se busca es persistir en la sustracción de información por un tiempo indefinido. Aunque con el nivel de acceso que se tiene a los datos de un sistema, el ataque es implacable y altamente intrusivo y destructivo si se lo desea, donde el rastro es difícil de detectar o identificar de manera puntual. Es así, que los APT detectados e identificados desde el año 2010 están evolucionando, tal como se citan algunos de manera cronológica: Stuxnet, Duqu [2], Flame [3], Miniflame, Iceforg [4], Gauss [5], Red October, Winnti, Careto [6], SyrianEA, Medre [7], Epic Turla y El Machete, entre otros más.

Basado en estas características particulares de este tipo de *malware*, el estudio que se expone en el presente artículo, se enfoca en específico a las potencialidades que podría tener un malware como el APT en cuanto a sigilo y ataque, y cómo se podría explotar al integrar algoritmos basados en inteligencia artificial y/o algoritmos genéticos, convirtiéndolo en una ciberarma inteligente que puede eventualmente comprometer las infraestructuras críticas de un país y al Internet.

Una propiedad característica de una APT, es su capacidad de fragmentación o descomposición en módulos, lo cual lo hace dinámico, entendido en el contexto que puede desarrollar diferentes tareas in situ, tales como leer información que circula por la red, escuchar a través de un micrófono e incluso controlar y registrar información de imágenes y video por medio de una webcam, efectuar capturas de pantalla, registro de chats e interceptación de comunicaciones vía VoIP, activar el *bluetooth* para sustraer información de dispositivos cercanos, entre otros. Hay que enfatizar, que este tipo de malware está diseñado y dirigido a grupos u organismos gubernamentales, cuyo ataque puede ser programado de manera sigilosa pasando desapercibido por mucho tiempo, e incluso hacer uso de 0 *days* [8] y *exploits* para su aparición y ataque, en la que busca infiltrarse por accesos remotos, canales encubiertos y silenciosos, haciendo casi imposible que el atacado tome cartas sobre el asunto y se pueda defender a tiempo.
Las APT son empleadas por bandas organizadas y gobiernos, estos últimos por medio de agencias de espionaje. El objetivo del uso de este tipo de malware, es básicamente espionaje corporativo, industrial, militar y gubernamental, en la que se infiltra la organización con el fin de robar información confidencial o en su defecto sabotearla. Esto implica que se requiere invertir grandes cantidades de recursos técnicos, tecnológicos y económicos, para diseñar, planificar e infiltrar una red con este *malware*, de ahí el nombre de amenaza persistente, porque este tipo de ataque puede perdurar de manera indefinida, hasta cuando su atacante esté satisfecho. En este punto se plantea preguntas como, ¿el cibercrimen patrocinado por los gobiernos es lícito?, ¿las ciberarmas podrían clasificarse como de destrucción masiva?, y de ser así, ¿entrarían a evaluarse de manera equivalente a lo que se hizo en su momento con las armas biológicas y nucleares, en cuanto al tratado de no proliferación?
¿Cuáles son los canales de propagación más comunes de este tipo de *malware*? En términos pasivos, a través de memorias flash o USB, o intrusión directa al sistemas operativo, infectado directamente los ficheros. A nivel activo, el ataque se realiza por medio de la explotación de las vulnerabilidades propias de la red o de cualquier dispositivo conectado a la misma, por correo electrónico a través de archivos adjuntos o por un *exploiting* en archivos escritos bajo el código de java, archivos comprimidos bajo el software de adobe, los browsers, entre otros. Esto da a entender que este malware aprovecha las vulnerabilidades inherentes a los protocolos de conexión como TCP/UDP, al protocolo HTTP en cuanto a sus cabeceras y credenciales de acceso, a los protocolos criptográficos de red SSL y TLS, al igual que el algoritmo de cifrado de bloques *Cipher Block Chaining* (CBC) [9, 10]; el cual define un grave problema de seguridad crítico para cualquier sistema informático o red de comunicación, porque crea certificados digitales que los valida como verdaderos. También, el ATP está relacionado con el sistema de nombres de dominio DNS, a través de la transferencia de zona o registros comprometiendo su integridad, porque puede actuar como sistema de suplantación legítimo.

2. Virus informático

Un virus informático es un programa que infecta a otros programas modificándolos para incluirse como una copia de sí mismo, la copia puede desarrollarse o evolucionar [11]. También, pueden estar latentes en el sistema (infectando discos y programas), y no presentar problemas durante largos períodos de tiempo. Además, se modifican por sí solos para evitar que sean detectados; no afectan a todos los programas

que entran en contacto con ellos [12]. Su comportamiento se acerca a un virus biológico, atacando los puntos más vulnerables de un sistema informático, tomándolo como huésped, por ejemplo, el sistema operativo, reproduciéndose, infectando otros programas, tabla de asignación de archivos, FAT, NTFS, HPFS [13], ejecutables con extensión .com, .exe, .bat, o incluso el propio hardware, como la memoria RAM y disco duro. De hecho, adquiere cualidades furtivas para evitar ser detectados por los sistemas antivirus o antimalware en general, donde guarda un periodo de latencia mientras se propaga por el medio que mejor le facilite su tránsito a otros objetivos (carpetas, archivos y registros) infectándolos sin que se presenten en la mayoría de casos síntomas que lo evidencien.

El virus informático se clasifica según su lugar de alojamiento, replicación y plataforma en la que se instala, de ahí que se hable de virus: residente, *hijackers, keylogger, zombie*, de archivos, *bat, vbs, Bug-ware, Mockinbird, Spoofing,* de sector de arranque, macro, de enlace, de encriptación, polimórfico, multipartes, boot, del mirc (combinación de virus de archivo y de arranque), parásito, sin punto de entrada, virus obj, lib y código fuente. Debido a estas variantes, hace que en muchos casos, sea difícil poder detectar el virus y erradicarlo a tiempo, antes que el daño sea irreversible.

La entrada de un virus a un sistema informático o red de comunicación es bastante simple, con solo el hecho de estar conectado a internet y el equipo de cómputo no esté protegido debidamente, por ejemplo, un antivirus desactualizado, abrir un correo electrónico y su contenido sin saber su procedencia, el ingreso a páginas web de dudosa reputación, uso de dispositivos extraíbles sin saber su procedencia o no aplicar previo escaneo de antivirus, ejecución de software malicioso sin que el usuario lo sepa, transferencia de archivos sin previo escaneo a través de conexiones tipo chat y/o similares.

A nivel técnico, una forma común que un virus ingrese a una red, es que el *firewall* esté mal configurado, o peor, no exista, sobre todo en entornos corporativos, vulnerabilidades en cuanto a la arquitectura y configuración de una red [14]. Otra anomalía, que propende al ingreso de virus, es la no existencia de un proxy, una VPN, un DNS, estas son herramientas fundamentales para minimizar el riesgo por intrusión, bien por virus informáticos como de atacantes humanos o de software tipo robots. También, es común en medianas y grandes empresas, es el no cumplimiento de las políticas de seguridad en cuanto al manejo de claves, gestión de información y navegabilidad, donde se evidencian fallos por parte de algunos empleados en no respetar las políticas, comprometiendo la información a terceros.

3. Origen y evidencias de las armas cibernéticas

Las armas cibernéticas APT se dieron a conocer en los periodos del 2010 y 2012 por medio de los virus informáticos llamados *Stuxnet, Duqu, Flame y Gauss*, descubiertos los primeros inicialmente en Irán, expandiéndose luego a toda la región de Asia Occidental. La razón, el programa atómico de Irán, que al parecer pretendía ocasionar fallos en los equipos de enriquecimiento de uranio, sumado a las crisis políticas en Siria, Egipto, Líbano, Palestina y países del Golfo Pérsico. Fue evidente que este ataque no fue interno, sino propendido por países con intereses económicos y políticos propios en la región, por lo que se puso al descubierto la aplicación de armas cibernéticas, que hasta hace algunos años solo era especulación de su existencia.

Según estudios publicados por *Kaspersky Lab, Duqu* es la continuación de la plataforma *Tilded*, que sirvió para crear otro gusano más famoso, *Stuxnet*, en la que se estableció que existían por lo menos tres programas más que usaban la misma base de *Duqu/Stuxnet*, y que hasta este momento no han sido descubiertos. Hacia finales de 2011 *Duqu* dejó de existir en el mundo real, pero a finales de febrero de 2012 los expertos de Symantec descubrieron en Irán una nueva variante de un driver similar al usado en Duqu, empleado también como vector de espionaje. Sin embargo, no se logró descubrir el módulo principal y desde entonces hasta ahora no se han encontrado nuevas modificaciones de *Duqu* [15]. Expertos en seguridad mundiales, creen que Estados Unidos e Israel son los responsables detrás de Stuxnet, aunque ambos países rehusaron oficialmente realizar comentarios sobre el tema [16]. Aunque una sospecha sobre los autores de los virus se confirmó a mediados del 2012, donde *The New York Times* informó que Stuxnet y *Flame* fueron desarrollados por dos servicios secretos en conjunto: la Agencia Central de Inteligencia (CIA) de Estados Unidos y la Unidad 8200 del servicio de inteligencia militar israelí [17]. En el mismo año en Irán aparece un troyano de nombre *Wiper*, cuyo origen se desconoce, que destruyó cientos de bases de datos de varias empresas de este país, sin posibilidad de recuperarlos. La característica principal de este virus, es que no dejó huella de ficheros del programa para poder analizar su traza algorítmica o módulo de ataque. Según un documento publicado por *Kaspersky Lab*, ellos descubrieron una campaña de espionaje cibernético estatal llamado *Flame* y Gauss, relacionados con *Wiper*.

Flame es un troyano-*backdoor* con rasgos de gusano informático, que supera a *Duqu* por su complejo desarrollo modular dinámico (que asciende a 20 módulos), empleando para ello varias herramientas algorítmicas para realizar sus ataques, que pueden ser cambiados o actualizados según la necesidad y/o requerimientos para mejorar esta arma cibernética. Kaspersky nombró a la plataforma *Flame* como *"Tilded"*, porque muchos de los archivos en *Duqu* y *Stuxnet* tienen nombres que comienzan con el símbolo tilde "(7/8)" y la letra "d" [15].

El vector de ataque común es a través de las memorias USB, difundiéndose principalmente en una LAN. Una vez instalado *flame*, empieza a realizar un análisis de tráfico de red para tomar el control de esta por medio de un ataque tipo Man in *the Midle*, lo que permite grabar conversaciones, realizar capturas por medio de pantallazos e interceptar pulsaciones del teclado, suplantar solicitudes del sistema operativo *Windows* para recibir actualizaciones y generar su propio certificado

digital. Lo interesante de este virus, es que es adaptativo, cambiando su comportamiento dependiendo del antivirus con el que se encuentre en el sistema operativo, haciendo difícil su detección, al igual que con los datos sustraídos, ya que estos se enviaban a servidores repartidos por todo el mundo. Esta estrategia está aún vigente y lo seguirá siendo por mucho tiempo, pues con ella, se dificulta el rastreo de la información robada por parte de las autoridades. Además, para minimizar el riesgo del rastreo, como los sistemas infectados actúan como una red tipo *"zombi"*, puede ser controlada por los atacantes, por ende, estos pueden a través de instrucciones desde ciertos servidores, causar la autodestrucción.

Existe una variante complementaria del APT *Flame*, demonimado *MiniFlame*, es un módulo de espionaje informático independiente y autónomo tipo *backdoor*, que, a través de su infección, permite el acceso remoto al sistema, permitiendo el robo de información de forma sutil e indetectable para los antivirus convencionales.

Otro programa asociado al concepto de armas cibernéticas APT, es el virus *Gauss*; que es un complejo sistema de espionaje modular dinámico altamente estructurado, más avanzado que *Flame*, que posee las siguientes funciones: intercepta ficheros cookie y contraseñas en el navegador, recopila y envía a los delincuentes los datos de configuración del sistema, infectan las memorias USB con un módulo dedicado al robo de datos, crean listas del contenido de los discos y carpetas del sistema, roba datos de acceso a las cuentas de diferentes sistemas bancarios que funcionan en el Oriente medio, intercepta los datos de las cuentas en las redes sociales, servicios de correo y sistemas de mensajería instantánea, entre otros [17].

Uno de los virus APT, clasificado como el más letal y avanzado *malware* de espionaje informático hasta la fecha, es el llamado *"The Mask"* o *"Careto"*. Fue descubierto a inicios del 2014, pero su operatividad se extiende hacia años atrás. La sofisticación de este virus radica por el uso combinado de complejas herramientas de malware como *exploits*, [18] *rootkit* [19, 20], *bootkit* [21] y *keyloggers*. Este virus recopila información interviniendo los canales de comunicación en una red, capturando archivos críticos (incluyendo los de tipo RDP), contraseñas, claves criptográficas (claves SSH), configuraciones VPN, grabación de conversaciones, capturas de información mediante pantallazos, claves de firma digital de Adobe, hasta el control absoluto de computadores. También, *Careto* recopilaba archivos de tipo log.txt de varios servidores, con el fin de levantar un mapa detallado de las IP, incluso de algunos ID de sus víctimas para un posterior ataque. El patrocinio y ejecución de este virus apunta a un estado que tiene un grupo dedicado para tal fin, en la que se evidenció que el ataque era selectivo, dirigido específicamente a embajadas, agencias gubernamentales, industrias energéticas, petroleras, gaseoductos e instituciones de investigación, entre otros. A esto se suma, los meticulosos procedimientos operativos para los cuales funciona el virus, que es estrictamente de inteligencia, ataca de manera furtiva, sin dejar rastros, eliminado cualquier huella en los archivos de registro de prácticamente cualquier sistema operativo, incluyendo los móviles, y salir sin ser detectado. El vector de entrada de careto es a través del *phishing*, copiando los portales de prestigiosos periódicos como *The Washington Post* y *The Guardian*, en la que redireccionaba a otros portales conocidos, donde yacían correos electrónicos falsos.

Según un informe publicado por *Kaspersky lab*, [22] existe evidencia contundente, de varios países infectados por el virus en mención, donde el foco de dispersión tiene relación directa con la política exterior de España, en la que se cita que hay 31 países involucrados y víctimas de este Malware. La lista completa la componen Argelia, Argentina, Bélgica, Bolivia , Brasil , China, Colombia, Costa Rica, Cuba , Egipto, Francia , Alemania, Gibraltar, Guatemala, Irán , Irak, Libia, Malasia , Marruecos, México, Noruega, Pakistán, Polonia, Sudáfrica, España, Suiza, Túnez, Turquía, Reino Unido, Estados Unidos y Venezuela [23].

Con base en este panorama la compañía de tecnología de redes *Cisco Systems*, afirma que "para el año 2020 habrá 50.000 millones de dispositivos conectados a Internet, de los cuales una gran parte será de tipo industrial, militar o aeroespacial. Cada dispositivo conectado al ciberespacio constituye un objetivo potencial, y los ciberatacantes son muy buenos descubriendo los enlaces más vulnerables" [24]. En este sentido, tecnologías incorporadas en vehículos autónomos o semiautónomos, en televisores, consolas de video juego y sistemas de navegación inmersivos, entre otros productos, deben considerar el modelo de ciberseguridad no solo como política, sino que debe ser incorporado en sus diseños. Como dato adicional, es que, debido a los grandes avances en sistemas de RF, se puede tener acceso remoto a los marcapasos [25], e incluso a implantes electrónicos de insulina, lo que se deduce que al ser *Hackeables*, se puede modificar la frecuencia [26] o alterar las dosis respectivamente, con las correspondientes consecuencias fatales.

4. Técnicas de propagación

Los virus diseñados para la ciberguerra, presentan una gama de propiedades en su diseño para evitar su pronta detección, para el caso particular de los APT, tienen un gran impacto en infraestructuras críticas de una nación (instalaciones de energía, gas, petróleo e hidroeléctricas, organizaciones gubernamentales, corporaciones dedicadas a la investigación, etc.), destacando las técnicas furtivas o *stealth*, que busca ocultar el tamaño real de los archivos que son infectados. Otra propiedad clave es el *Tunneling*, que involucra técnicas complejas de programación, cuyo objetivo es evitar cualquier tipo de rutinas relacionadas con el servicio de interrupción del sistema operativo. El antidebugger, es otra herramienta que se emplea en el desarrollo del virus para impedir que su código sea desensamblado, esto con el fin de impedir su análisis, y con ello evitar dar información clave a los algoritmos de los antivirus.

Otra técnica refinada, es el polimorfismo o automutación;

consiste en mutar o variar las cadenas de código del virus a medida que infecta nuevos sistemas. Con estos cambios, los sistemas antivirus emplean técnicas heurísticas avanzadas para su búsqueda y detección, se centra en segmentos particulares de código inmutables, que es la parte más vulnerable. Esto significa que el polimorfismo es la forma más cercana a trabajar con algoritmos genéticos, tanto así que, la programación polimórfica empleada para el desarrollo de un virus informático, usa técnicas depuradas y refinadas en cuanto al código que porta la infección, debido a que debe insertarse en un archivo ejecutable sin que aumente el tamaño del mismo. Lo anterior, se logra al comprimir tanto el código del virus y del archivo anfitrión. Una variante de esta técnica usa métodos de encriptación dinámicos, con el fin de evitar la detección de los antivirus. Por ejemplo, una de las formas más elaboradas de polimorfismo corresponde al *Mutation Engine*, presente en código abierto, en la que cualquier virus puede hacerse polimórfico añadiendo ciertas llamadas a códigos fuente y enlazando con los módulos generadores de número aleatorio de *Mutation-Engine* [27].

Una última técnica, son los virus o programas residentes en memoria (TSR), que se alojan en ésta durante toda su ejecución, contaminando los archivos de arranque del sistema. Su objetivo, es tomar el control de todas las actividades del sistema operativo, con el fin de infectar todo lo que esté a su paso. Lo interesante de este virus, es que permanece en la memoria mientras el computador esté encendido, por lo que infectar los archivos de arranque es crucial, con ello se asegura que cada vez que se vuelva a encender el equipo el virus se carga a la memoria in situ.

De aquel tiempo donde la estructura del código de un virus era secuencial, hoy las cosas son diferentes, ahora se incorporan algoritmos modulares, en la que no es raro encontrar estructuras complejas, emulando el comportamiento de los virus biológicos en cuanto a mutación, con la diferencia que los virus informáticos pueden armarse por partes, pasando de esta manera desapercibidos ante cualquier sistema de detección de intrusos (IDS). La idea actual, es hacer que el código sea literalmente ilegible aplicando normalmente técnicas de ofuscación. Esto implica que se espera encontrar un virus con líneas de código legibles, lo que no va a suceder. La pregunta es, ¿qué sucede cuando un virus informático se desarrolla bajo los criterios de la inteligencia artificial y polimorfismos? (Algoritmos genéticos). La respuesta es el código evoluciona, por ende, sus líneas se reescriben permanentemente haciendo inservible los sistemas de antivirus para su detección.

El código de un virus polimórfico poco difiere de un código general de un programa, por ende, aplicar métodos adaptativos mediante un algoritmo genético es viable. Para ello, se asumen parámetros de código que se denominan módulos o segmentos de código que desarrollan tareas específicas en el programa, que equivale a los genes, y al agruparse en macromódulos, forman un cromosoma o fenotipo [28]; el cual contiene la información suficiente para crear un organismo viral (biológico o informático), que se refiere como un genotipo. Cuando se tiene esta estructura se procede a crear diversas combinaciones, hasta obtener los fenotipos ideales, tal como se describe a continuación.

4.1 Vector de ataque

En el contexto de un arma cibernética tipo APT, el virus informático tiene como objetivo el ataque total o parcial sobre un sistema, para inutilizarlo, neutralizarlo o explotar la información sin ser detectado. El vector de propagación es diverso, bien por correo electrónico, al recibir información o publicidad engañosa a través de videos, música, imágenes, programas, archivos, donde el usuario ejecuta o acepta inocentemente su instalación. También, la infección puede ser directa, accediendo a sitios web poco confiables, en la que se consulta y/o descarga información que trae consigo virus camuflados. Otra forma, es cuando el virus es puesto sobre la red replicándose, donde los usuarios los instalan al acceder de sus redes sociales, sistemas P2P, sistemas tipo grid que comparten diversa índole de información, etc. Existe una tercera forma, que es la instalación directa del virus sobre un servidor, con la clara intención que este actúe como vector de propagación e infección sobre la red.
La dificultad para el software antivirus en cuanto a detectar y diagnosticar a tiempo un virus informático es crítico. Es por ello, que se vale de técnicas de búsqueda heurísticas que permiten localizar un virus basado en los patrones de comportamiento que este tiene en el medio, tales como ralentización del sistema, consumo de recursos computacionales, bien sea de memoria o de procesadores, bloqueos de operaciones del sistema operativo o del hardware inexplicable, por ejemplo, el disco duro o la BIOS. Actualmente la detección de un virus consume varios días antes que las compañías de antivirus proporcionen una solución real al usuario, durante los cuales los virus se propagan rápidamente, lo que causa importantes daños y pérdidas económicas en el proceso [29]. Algo interesante de un virus inteligente es emplear un byte ruidoso [30], que busca engañar al sistema consumiendo tiempo de procesamiento sin realizar algún tipo de operación real.

4.2 Virus polimórficos neuroevolutivos ofuscados

Las armas cibernéticas se definen como el conjunto de programas informáticos tipo malware, diseñados específicamente para efectuar ataques dirigidos de espionaje, sabotaje y destrucción de información crítica de una organización o nación, inhabilitando total o parcialmente sus infraestructuras de sistemas de comunicación y redes de información locales y/o globales.
Aunque la financiación para crear armas cibernéticas de tipo APT se atribuye específicamente diversos gobiernos, encabezados por China, Estados Unidos, Rusia e Israel, por citar algunos. Por ejemplo, el *Washington Post* publicó que el Pentágono tiene una lista clasificada de “armas cibernéticas” aprobadas y que se pueden utilizar, en respuesta a una serie de posibles escenarios militares [31]. También, este tipo de armas pueden ser desarrolladas por grupos organizados delincuenciales y/o terroristas. Por ende, no solo las instituciones,

Figura 1

```
main(){int
i,n[]={((((1<<1)<<(1<<1)<<(1<<1)<<(1<<(1>>1)))+((1<<1)<<(1
<<1))), (((1<<1)<<(1<<1) <<(1<<1)<<(1<<1))-
((1<<1)<<(1<<1)<<(1<<1))+((1<<1)<<(1<<(1>>1)))+(1<<(1>>
1))),((1<<1)<< (1<<1)<<(1<<1)<<(1<<1))-
((1<<1)<<(1<<1)<<(1<<(1>>1)))-
((1<<1)<<(1<<(1>>1))),(((1<<1)<<
(1<<1)<<(1<<1)<<(1<<1))-((1<<1)<<(1<<1)<<(1<<(1>>1)))-
((1<<1)<<(1<<(1>>1))),(((1<<1)<<
(1<<1)<<(1<<1)<<(1<<1))-((1<<1)<<(1<<1)<<(1<<(1>>1)))-
(1<<(1>>1))),(((1<<1)<<(1<<1)<<
(1<<1))+((1<<1)<<(1<<1)<<(1<<(1>>1)))-
((1<<1)<<(1<<(1>>1))),((1<<1)<<(1<<1)<<(1<<1)),
(((1<<1)<<(1<<1)<<(1<<1)<<(1<<1))-((1<<1)<<(1<<1))-
(1<<(1>>1))),(((1<<1)<<(1<<1)<<(1<<1) <<(1<<1))-
((1<<1)<<(1<<1)<<(1<<(1>>1)))-
(1<<(1>>1))),(((1<<1)<<(1<<1)<<(1<<1)<<(1<<1))-
((1<<1)<<(1<<1)<<(1<<(1>>1)))+(1<<1)),(((1<<1)<<(1<<1)<<
(1<<1)<<(1<<1))-((1<<1)<< (1<<1)<< (1<<(1>>1)))-
((1<<1)<<(1<<(1>>1))),(((1<<1)<<(1<<1)<<(1<<1)<<(1<<1))-
((1<<1)<<(1<<1)<<
(1<<1))+((1<<1)<<(1<<(1>>1))),(((1<<1)<<(1<<1)<<(1<<1))+
(1<<(1>>1))),(((1<<1)<<(1<<1))+((1<<1)<< (1<<(1>>1))) +
(1<< (1>>1)))}; for(i=(1>>1);j<(((1<<1) <<(1<<1))+((1 <<1)<<
(1<<(1>>1))) + (1<<1)); i++) printf("%c",n[i]); }
```

corporaciones y gobiernos son objetivo de este tipo de ataques, sino que potencialmente toda la sociedad está expuesta a ello. Ahora, los virus que se están desarrollando como ciberarma no solo amplían su espectro de ataque de un virus informático convencional, sino que además pueden infectar otros tipos de archivos y ejecutables como los .bat, .ovr, .dll, .cpl, nlm, entre otros. De igual manera, las acciones de escanear, enumerar, obtener acceso remoto, abrir una puerta trasera, circular por un sistema de detección de intrusos en una red, etc., tienen una implicación en el sistema de la víctima a gran escala: se registra cualquier evento que haya ocurrido en la máquina durante el tiempo que permanezca encendida [32]. Para el caso de las ciberarmas, se borran todos estos registros que son guardados en logs, por lo que no dejan huella de su intrusión en el sistema.

Algo importante con respecto al desarrollo de virus polimórficos de última generación, es el uso deliberado de la ofuscación en la programación, es decir, efectuar cambios no destructivos en el código fuente con el fin de hacerlo ininteligible a terceros, complicando el proceso de ingeniería inversa aplicado sobre el mismo. Con la ofuscación se puede conseguir programas más pequeños, que es lo que se busca en un virus, y que se consiguen en aplicaciones hechas en lenguaje C, C++ y Perl, comunes para desarrollo de virus informáticos, al igual que *Python*, Java y LISP. Un ejemplo de *ofuscación*, se representa por medio de caracteres que se obtienen haciendo desplazamiento de bits. Por último, aparece un for al final que imprime los caracteres [33] (ver Figura 1).

Las técnicas comunes de ofuscación [33] de malware se encuentran a nivel de *shellCode/opcode*, en las capas de aplicación, de red y de transporte del modelo OSI. Sumado a lo anterior, se implementan nuevas áreas de la computación como son los algoritmos genéticos y la inteligencia artificial, que van a ser la próxima generación de malware diseñados a la carta, para realizar ataques selectivos (ciberataques, ciberterrorismo, ciberguerra) a sistemas computacionales y hardware [34] para sustraer, modificar o eliminar información crítica de los mismos.

4.3 Inteligencia artificial y polimorfismo

El desarrollo de virus informáticos de última generación como los APT, implica la combinación de las técnicas citadas con algoritmos polimórficos y técnicas de cifrado, que permita mutar el virus para mantener su furtividad ante los antivirus, archivos de programa y flujos de paquetes de la red. Lo interesante de estos códigos es que combinan el polimorfismo con técnicas propias de la inteligencia artificial.

Los algoritmos genéticos se basan en la teoría darwiniana de selección genética natural. Combinan la supervivencia de estructuras de cadenas compatibles, con una estructura de información aleatorizada, intercambiada para construir un algoritmo de búsqueda con algunas de capacidades de innovación de la búsqueda humana [35]. El uso de los algoritmos genéticos para el desarrollo de *malware* polimórfico, se sintetiza, en una palabra, "paralelismo", es decir, operan de manera simultánea con varias soluciones a diferencia de los algoritmos secuenciales, que emplean técnicas tradicionales. Algo importante de mencionar, es que emplean operadores probabilísticos en lugar de determinísticos, sumado a que realizan cambios aleatorios en sus soluciones candidatas y utilizan la función de aptitud para determinar esos cambios producen una mejora o no [36].

Para el desarrollo de programas usando algoritmos genéticos [37] sobre un malware de tipo APT se tiene en cuenta una serie de parámetros, como son:

- *Tamaño de la Población:* representa el número de instrucciones para efectuar N operaciones de intrusión, teniendo en cuenta que el algoritmo debe estar equilibrado, de tal manera, que se consiga una mayor velocidad en la resolución del problema. Para este caso en particular, la población inicial no se obtiene aleatoriamente, sino a través de métodos heurísticos, para generar soluciones iniciales de buena calidad. Para efectuar esta operación se toman dos fragmentos de código padre $(x_1,x_2,...,x_n)$ y $(y_1,y_2,...,y_n)$.

- *Probabilidad de Cruce o Crossover:* se entiende como la frecuencia con la que se pueden cruzar instrucciones de código con otros con miras a obtener los mejores para efectuar un ataque y/o evadir los sistemas de detección. Con los fragmentos padre definido, se procede a seleccionar un solo gen aleatorio k, con un factor de probabilidad α, por lo que se crean cruces aritméticos simples o codificados, tal como se muestra en

la ecuación:

$$(x_1, x_2, ..., x_k, \alpha y_{k+1} + (1-\alpha)x_{k+1}, ..., \alpha y_n + (1-\alpha)x_n) \quad (1)$$

Todo el cruce se resume en:

$$\alpha \bar{x} + (1-\alpha)\bar{y} \quad (2)$$

El crossover permite cruzar los mejores algoritmos padre para obtener uno nuevo que mejore las tareas de infección de los algoritmos previos. Con esto se garantiza la perpetuación del polimorfismo más dominante, la analogía biológica sería un virus tipo VIH. Para ello, se puede aplicar diferentes formas de cruce para cada codificación tales como: Crossover de un punto, dos puntos, uniforme y aritmético [38].

- *Selección:* Se toman las mejores instrucciones del código, que bajo las condiciones de estrés algorítmico sobreviven para seguir sus tareas de intrusión, detección, rastreo y copia de información de manera furtiva. Esto significa que los mejores algoritmos quedan en esta fase, y si se requiere seguirá optimizándose según las necesidades y/o condiciones del medio. Cabe mencionar, que se pueden emplear varias formas de selección como son: por rueda de ruleta, por rango, por elitismo, por estado estacionario, por torneo, escalada y jerárquica entre otros [39]

- *Mutación:* [40] Está relacionado con el polimorfismo ocurre tras un cruce, donde el código se configura o autoconfigura según requerimientos del medio (antivirus, *firewall*, protocolos, certificados, etc.), cambiando algunas instrucciones del algoritmo, efectuando nuevas tareas u optimizando las ejecutadas. La aleatoriedad se realiza parcialmente, teniendo en cuenta las tareas que ejecuta los módulos o secuencias primarias del algoritmo, expresas por la codificación binaria, que puede mutar por medio de la inversión de uno o varios bits. Hay que tener en cuenta que la idea de la mutación en esta instancia, es obtener los mejores códigos o módulos que el *malware* emplea para vulnerar las barreras lógicas en que se encuentre, por ende, aunque el cruce tiene la principal responsabilidad de buscar la solución óptima, la mutación también lo hace, y es precisamente esta capacidad que se aprovecha en las ciberarmas inteligentes, adaptarse y evolucionar, bien sea con probabilidades de mutación baja para mantener una convergencia constante, o por el contrario, con un valor alto de la probabilidad de mutación como técnica de búsqueda aleatoria.

  Para evitar que el algoritmo genético tarde mucho en converger o no hacerlo en absoluto, se procese a definir parámetros o rangos asociados al tamaño de la población, número de generaciones (módulos), etc. De igual manera, para evitar una convergencia prematura se proponen muchos modelos: Estrategias como codificación Delta, algoritmos genéticos messy, CHC y bGA; Híbridos de un algoritmo genético con búsqueda local, algoritmos meméticos [41]; Algoritmos distribuidos y OPERON GA y COPdEB (usan varias poblaciones) [42]. Estos modelos buscan minimizar el tiempo de procesamiento extenso y garantizar resultados en tiempos relativamente cortos. Aunque para evitar convergencias rápidas y no óptimas se emplean algoritmos de control, basados en inteligencia artificial.

- *Inteligencia artificial:* con respecto a la inteligencia artificial, existe gran diversidad de procesos algorítmicos que permiten que un sistema sea dinámico en cuanto análisis y procesamiento de datos, debido al uso de las redes neuronales. Para el caso particular de un programa viral polimórfico, la no linealidad es un elemento esencial (Por ejemplo, Redes perceptrón multicapa, redes recurrentes y redes de funciones de base radiales); debido a que las conexiones entre las neuronas generan estructuras de datos, que se distribuyen a lo largo de la red, además se transforman, bien sea por cambios en el medio o por condiciones preconcebidas en el propio algoritmo, que hacen que la red se adapte al cambio, ajustando sus pesos w_{ij} (Matrices).

  Lo que hace cada peso sináptico es multiplicar a su entrada correspondiente x_j en la que se define la importancia relativa de cada una de ellas, donde su activación está supeditada a la entrada total supera un cierto umbral b [43]. Matemáticamente se tiene que la función de salida yi, está relacionado con una función de transferencia o activación f(.):

$$y_i = f\left(\sum x_i w_{ij} + b\right) \quad (3)$$

El uso de la función de transferencia es clave, cuando se desea una salida binaria, siendo mucho más fácil tratar con un algoritmo genético, que cuando las salidas fueran números reales. Así, en términos operativos, la red neural puede ser tolerante a fallos y responder aun cuando parte de su estructura colapsa por fallas o errores, porque la información se trata de forma distribuida y paralela, en la que existe una redundancia implícita en su interior. Este elemento es fundamental cuando se piensa en integrarlo con un algoritmo polimórfico. Además, las redes neuronales están sujetas a un factor de aprendizaje, que matemáticamente implica que se actualizan los pesos de manera secuencial [44], y por ende, puede ser ajustado conforme a las condiciones establecidas en las reglas genéticas.
Dentro del diseño de los virus más avanzados, se crean sintaxis algorítmicas que permiten circular por una red o por un sistema informático, ocultarse y cambiar su estructura lógica

dentro de un archivo, asumiendo técnicas *stealth* o furtivas, impidiendo de esta manera, que las herramientas de detección los localicen rápidamente, o peor evitan que lo hagan. Por lo tanto, con base en esta premisa, la inteligencia artificial entra a jugar un papel fundamental en la forma como se diseñan los virus informáticos, al permitir que estos asuman el rol de tomar decisiones para su supervivencia en un medio adverso, adaptarse y/o evolucionar cuando las condiciones del medio lo exigen.

5. Conclusiones

Las armas cibernéticas o ciberarmas como las APT, son desarrolladas y/o financiadas por las mayores potencias del mundo y delincuencia organizada, en la que se busca explotar las vulnerabilidades de otros para beneficio propio. El problema de este tipo de armas, es que pueden comprometer las infraestructuras críticas de una nación, poniendo en jaque su seguridad en todos los niveles (militar, salud, transporte, suministro de víveres, energía, etc.).

El cibercrimen propendido por los gobiernos generan una gran brecha en materia de seguridad de la información a nivel mundial, máxime cuando se habla de ciberarmas como las APT, cuyo nivel de sofisticación es incomparable con los malware a los que está acostumbrada la sociedad. Lo peor de esta situación, es que existe un mercado negro, donde se compran las vulnerabilidades detectadas en una organización o en una infraestructura crítica de un país, lo que propende el uso de ciberarmas a la carta para efectuar ataques dirigidos.

El desarrollo de ciberarmas con capacidad polimórfica adaptativa y furtiva, basada en la estructura de programación de algoritmos neuroevolutivos, es quizás una tendencia puesta en marcha desde hace algunos años atrás, y con el actual avance de las tecnologías emergentes, este tipo de virus evoluciona a un nivel que lo pueda llevar a la vida artificial, implicando que estos se comporten como una verdadera plaga informática, que eventualmente podría comprometer la red de Internet y sistemas de comunicación. Sobre este tema, naciones como Estados Unidos, China y Rusia, no se toman este tema a la ligera, por lo que disponen de diversos frentes de ataque y defensa contra las ciberarmas, en particular sobre sus infraestructuras críticas, previendo una posible ciberguerra.

Los ciberataques son una realidad, y en los próximos años crecen literalmente de forma exponencial. Por ejemplo, el 14 de mayo del 2017, hubo un ciberataque a nivel mundial con un virus de tipo *ransomware* denominado *"WannaCry"*, que secuestró datos corporativos de miles de equipos informáticos encriptándolos, en la que se pedía un rescate de 300 dólares en bitcoins si querían recuperar de los datos. -Las pérdidas por este ciberataque son incalculables, en la que cerca de 100 países fueron afectados-. Como se observa, el panorama en materia de seguridad de la información a nivel global está entre dicho, máxime cuando la sociedad cada vez está más conectada al ciberespacio y es cada vez más dependiente de éste, por diversos dispositivos móviles, computadores y redes públicas y privadas, y de las denominadas tecnologías emergentes relacionadas con la Internet de las cosas, la computación ubicua e inmersiva y videojuegos, entre otros. A lo anterior, se suma, que existen diversos recursos técnicos y tecnológicos que disponen ciertos gobiernos que permiten husmear ilimitadamente en la Internet, en los servidores nodo, en las cuentas en línea, en los computadores personales y corporativos, y en los dispositivos móviles, gracias al continuo avance de la computación, las telecomunicaciones y el software.

References

[1] Command Five Pty Ltd, "Advanced persistent threats: A decade in review," June 2011.

[2] N. Falliere, L. OMurchu, and E. Chien, "W32. duqu: The precursor to the next stuxnet," *Symantec Security Response*, vol. 4, Nov. 2011.

[3] sKyWIper Analysis Team , "A complex malware for targeted attacks," 2012.

[4] "The icefog apt: A tale of cloak and three daggers."

[5] B. Bencsáth, G. Pék, L. Buttyán, and M. Felegyhazi, "The cousins of stuxnet: Duqu, flame, and gauss," *Future Internet*, vol. 4, no. 4, pp. 971–1003, 2012.

[6] "Unveiling "careto" - the masked apt."

[7] Inteco, "¿que son las amenzas persistentes avanzadas (apts)?."

[8] L. Ablon and A. Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Santa Monica, California: RAND Corporation, 2017.

[9] M. Bellare, J. Kilian, and P. Rogaway, "The security of the cipher block chaining message authentication code," *Journal of Computer and System Sciences*, vol. 61, no. 3, pp. 362–399, 2000.

[10] A. K. Yau, *Side Channel Analyses of CBC Mode Encryption*. PhD thesis, University of London, 2009.

[11] F. B. Cohen and D. F. Cohen, *A short course on computer viruses*. John Wiley & Sons, Inc., 1994.

[12] M. G. Benedetto, C. Navarro, C. M. Alvez, C. E. S. Baena, J. J. Etchart, G. R. Leal, C. R. Loggio, S. René, and G. L. Berón, "Las acciones de los virus informáticos y sus daños sobre los sistemas," *Ciencia, Docencia y Tecnología Suplemento*, vol. 1, no. 1, 2011.

[13] M. Support, "Introducción a los sistemas de archivos fat, hpfs y ntfs."

[14] S. M. Bonilla and J. A. González, "Modelo de seguridad de la información," *Ingenierías USBmed*, vol. 3, no. 1, pp. 6–14, 2012.

[15] Reuters, "Descubren armas cibernéticas similares a la creada contra irán," Dec. 2011.

[16] Opinión & análisis, "La carrera de armas cibernéticas puede cambiar el mundo," June 2012.

[17] G. Alexander, "Armas cibernéticas. descubren armas cibernéticas similares a la creada contra irán." Boletín de Seguridad.

[18] J. C. Foster, *Writing security tools and exploits*. Syngress, 2006.

[19] B. Blunden, *The Rootkit arsenal: Escape and evasion in the dark corners of the system*. Jones & Bartlett Publishers, 2012.

[20] N. Altholz, *Rootkits for Dummies*. Wiley, 2007.

[21] K. Peter, "Stoned bootkit," 2016.

[22] Unveiling "Careto", "The masked apt. kaspersky lab. version 1.0," Feb.

[23] Diario Turing/Vigilancia y privacidad, "¿puede estar españa detrás del malware careto/the mask?," Sept. 2016.

[24] E. Keren, "Ciberguerra. primera regla: deja de pensar que otros te van a proteger," *Rev. Investigación y Ciencia*, pp. 38–41, 2015.

[25] L. D. Rodríguez, D. Conde, and A. Baranchuk, "Síndrome de marcapasos: una causa subestimada de insuficiencia cardíaca," *Insuficiencia cardíaca*, vol. 9, no. 1, pp. 31–35, 2014.

[26] A. Martínez, "Hackear un corazón humano es posible." ABC Tecnología- Redes.

[27] "Proyecto malware," 2009.

[28] M. Mitchell, "Genetic algorithms: An overview in an introduction to genetic algorithms, chapter 1," 1995.

[29] J. C. Sarmiento Tovilla, *Un modelo del sistema inmune para prevenir y eliminar los virus informáticos*. PhD thesis, Instituto Politécnico Nacional. Centro de Investigación en Computación, 2003.

[30] D. Harley and L. Andrew, "Análisis heurístico: detectando malware desconocido."

[31] E. Nakashima, "List of cyber-weapons developed by pentagon to streamline computer warfare," 2011.

[32] M. García, H. Fernández., Y. Martínez, S. Rubén, M. Ochoa, A. Ramos, and A. Antonio, "Hacking y seguridad en internet 2da edición," 2013.

[33] R. C. de la Fuente, S. G. Erena, and A. V. González, "Sistema de ofuscación de malware para la evasión de nids," 2013.

[34] M. J. B. Zuluaga and D. F. J. Mendoza, "Propuesta de gestión de riesgos para scada en sistemas eléctricos," *Ingenierías USBmed*, vol. 3, no. 2, pp. 12–21, 2012.

[35] A. Verdejo, "Algoritmos genéticos."

[36] A. de la Peña and J. P. Truyol, "Algoritmos genéticos."

[37] B. Ulrich, "Genetic algorithms: Theory and applications. lecture notes. third edition."

[38] S. Orozco, "Optimización de herramientas multiobjetivo para la toma de decisiones de inversión en sistemas aislados sostenibles de energía," *Universidad de Antioquia, ISA, COLCIENCIAS*, 2007.

[39] M. Gestal, D. Rivero, J. R. Rabuñal, J. Dorado, and A. Pazos, "Introducción a los algoritmos genéticos y la programación genética," *A Coruña*, vol. 2010, pp. 30–68, 2010.

[40] M. B. Melián, J. A. Moreno, and J. M. Moreno, "algoritmos genéticos. una visión práctica," *Números. Revista de Didáctica de las Matemáticas*, vol. 71, pp. 29–47, 2009.

[41] P. Moscato and C. Cotta, "A gentle introduction to memetic algorithms," in *Handbook of metaheuristics*, pp. 105–144, Springer, 2003.

[42] A. Parisi, F. Parisi, and D. Díaz, "Modelos de algoritmos genéticos y redes neuronales en la predicción de índices bursátiles asiáticos," *Cuadernos de economía*, vol. 43, no. 128, pp. 251–284, 2006.

[43] F. Izaurieta and C. Saavedra, "Redes neuronales artificiales," *Departamento de Física, Universidad de Concepción Chile*, 2000.

[44] P. P. Cruz and A. Herrera, *Inteligencia artificial con aplicaciones a la ingeniería*. Marcombo, 2011.