M&N14/4/COMSC/HP3/SPA/TZ0/XX/CS

International Baccalaureate®
Baccalauréat International
Bachillerato Internacional

INFORMÁTICA
ESTUDIO DE CASO: SEGURIDAD EN LAS REDES

Para usar en mayo de 2014 y noviembre de 2014

INSTRUCCIONES PARA LOS ALUMNOS

- Para la prueba 3 del nivel superior se requiere el cuadernillo del estudio de caso.

6 páginas

Introducción

La tecnología de la información ha cambiado el modo de vivir de las personas y la forma en que las empresas gestionan sus negocios. El uso de las redes no sólo ha revolucionado los negocios internamente, sino que les permite acceder globalmente a recursos y clientes a través de Internet.

Estos beneficios tienen un precio: personas y organizaciones pueden usar las redes para atacar sitios Web de compañías con un complejo arsenal de software malicioso diseñado para poner en riesgo sus operaciones cotidianas.

El panorama de las amenazas ha cambiado dramáticamente en los últimos años. En el pasado, el software malicioso era una herramienta típica de los *script kiddies*, expertos en computación no necesariamente profesionales, que intentaban hacer el mayor daño posible para crearse así una reputación en el mundo del hacking. Los virus afectaban a los sistemas informáticos, sobrecargaban los servidores y borraban datos, pero el daño solía ser temporal y los costos se debían principalmente al tiempo en que el sistema no estaba en funcionamiento. Las amenazas, no obstante, están cada vez más impulsadas por la búsqueda de un beneficio económico y ejecutadas por organizaciones delictivas, lo cual conlleva altos costos para las empresas tanto por las pérdidas directas como por las inversiones que se hacen para intentar proteger sus redes y los datos almacenados en ellas. El panorama se ha vuelto más complejo aún debido a la participación de organizaciones estatales que lanzan ataques por razones políticas o ideológicas.

Es realmente difícil encontrar cifras confiables que muestren las pérdidas ocasionadas por los delitos informáticos, ya que las empresas se muestran reacias a ofrecer estos datos, e incluso a admitir que han sido atacadas. No obstante, en un informe de 2012 sobre delitos informáticos Norton estima que el costo global de estos delitos informáticos alcanza los US$110 mil millones al año[1].

A pesar de la gran cantidad de recursos dedicados a luchar contra la delincuencia informática, la mayoría de amenazas siguen aumentando, tal como muestran las estadísticas obtenidas del informe de Symantec sobre Amenazas de seguridad en Internet correspondiente al año 2011[2].

Amenaza	**2010**	**2011**
Robots zombi	3 065 030	4 500 000
Variantes únicas de software malicioso	286 millones	403 millones
Spam global estimado por día	62 mil millones	42 mil millones
Dominios Web maliciosos	42 926	55 294
Nuevas vulnerabilidades en equipos móviles	163	315
Ataques de día cero	14 nuevas vulnerabilidades	8 nuevas vulnerabilidades

El aumento de la delincuencia informática ha ido en paralelo con el aumento en los servicios de personal de seguridad de redes, contratado directamente por las empresas o a través de consultoras. Este estudio de caso muestra la labor de Susan Woo, que trabaja para la empresa ficticia *XXXSecurity* consultora en seguridad.

---

1 http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report _Master_FINAL_050912.pdf

2 http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=2011_in_numbers

XXXSecurity

En una entrevista reciente Susan esbozó algunas de las tendencias que se presentan en la creación y detección de software malicioso y el trabajo que está realizando actualmente.

Tendencias en la creación de software malicioso

Susan habló de cómo el software malicioso suele irrumpir en un sistema a través de ataques basados en el navegador, pero a diferencia del caos instantáneo que ocasionaba hace años, hoy en día suele tener como objetivo permanecer oculto mientras recopila silenciosamente datos de la organización. Según explicó:

"Las organizaciones de delincuentes profesionales intentar usar *robots*, que son código que se puede replicar a sí mismo de forma similar a la de los *gusanos*. Pero la característica adicional que tienen es que se los puede controlar desde alguna ubicación central en cualquier parte del mundo y pueden aceptar comandos y ser activados en cualquier momento. Existe una industria clandestina en auge dedicada a producir software malicioso personalizado usando *toolkits* (conjuntos de herramientas) que se puede comprar y combinar para conseguir objetivos concretos. Un buen ejemplo de esto es *Zeus Botnet* [3].

"El éxito de ataques como *Stuxnet, Duqu* y *Flame* ha llevado a acuñar el término *Amenazas persistentes avanzadas* (*Advanced Persistent Threats* – APT) que define más un estilo de ataque que un método concreto. Estos ataques usan una serie de técnicas, entre las que se incluye la ingeniería social, para centrarse en una organización concreta."

También resaltó los peligros de los *ataques de día cero* en los que los delincuentes informáticos usan vulnerabilidades previamente desconocidas para romper controles de seguridad.

Métodos de detección

Los paquetes antivirus tradicionales que están *basados en firmas* y el uso de cortafuegos con *filtrado de paquetes* aún son importantes en la protección de los sistemas, pero a medida que el software malicioso aumenta su complejidad también lo hacen las herramientas. Susan continúa analizando los cambios en las técnicas de detección.

"La detección y la prevención ya no se basan únicamente en las firmas, sino que tienen en *cuenta las anomalías*, es decir, comparan el tráfico de la red con lo que se considera "normal". Las *listas blancas* adoptan la estrategia opuesta de los trabajos tradicionales contra el software malicioso al generar una huella local para las aplicaciones aceptables.

"Una gran cantidad de tráfico de Internet usa protocolos como HTTP, HTTPS, IM y P2P, pero mientras que los cortafuegos tradicionales son efectivos a la hora de filtrar, no son especialmente eficaces para inspeccionar los contenidos de este tipo de tráfico. En cambio, los *cortafuegos de próxima generación* (*Next Generation Firewalls* – NGFW) tienen esta capacidad y pueden realizar inspecciones en paquetes que van más allá de consultar los valores del puerto y del protocolo."

[3] http://www.fortiguard.com/analysis/zeusanalysis.html

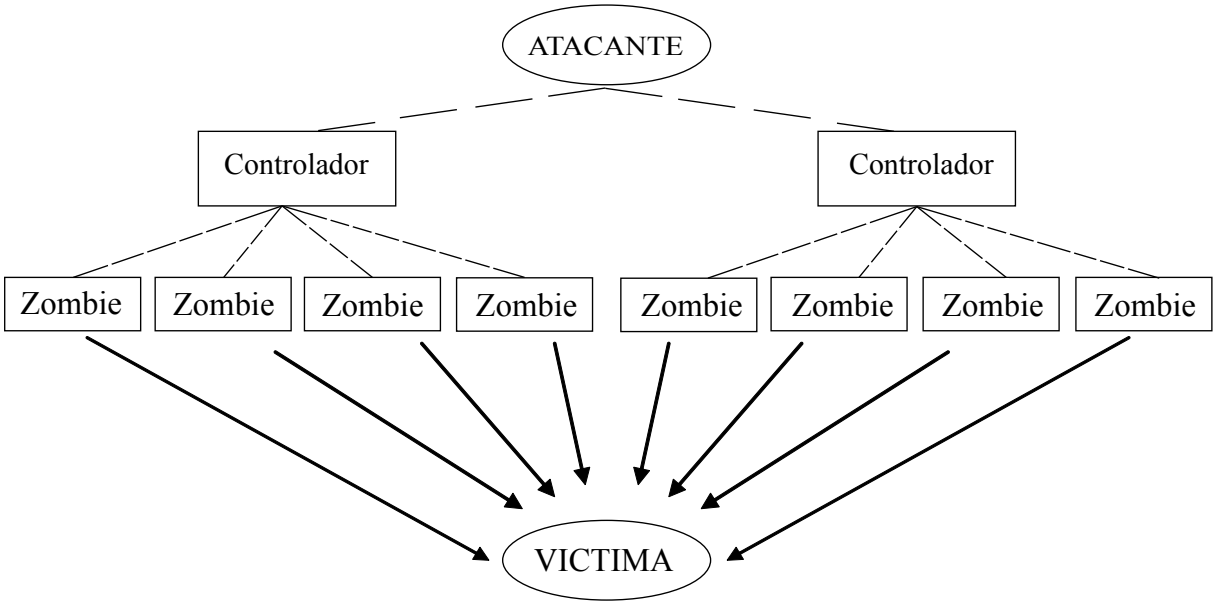
Véase al dorso

Cuando se le pregunta qué seguridad aporta el cifrado a la transferencia de datos, pide cautela y explica que incluso los protocolos *SSL/TLS* pueden verse afectados por ataques de tipo *man-in-the-middle* (intermediario).

Una de las áreas de estudio de Susan son los ataques de *Denegación de servicio* (DoS). Estos funcionan de varias formas pero con el objetivo común de sobrecargar un sitio concreto hasta el punto en que no pueda funcionar normalmente. Los autores suelen generar redes-robot que se crean a partir de computadores infectados por software malicioso que por ello se convierten en *zombis*. Posteriormente lanzan un ataque coordinado sobre un sitio concreto como, por ejemplo, el ataque que sufrió Amazon en 2008[4]. Aunque el uso de redes-robot suele tener un fin delictivo, hay ocasiones en que un movimiento popular ha llevado a organizar ataques sobre sitios Web, como el ataque masivo lanzado en Estonia en 2007[5].

En el diagrama siguiente se muestra la configuración básica de un ataque *de Denegación de servicio distribuido* (DDoS).

Arquitectura de un ataque DDOS



XXXSecurity está generando actualmente una serie de páginas en su sitio Web dedicadas a las distintas formas de software malicioso. La información no profundizará hasta el nivel de código, pero describirá con detalle cómo funciona cada componente del software malicioso, junto con los métodos de prevención apropiados.

Susan tiene como tarea los ataques de DoS y se centra en las tres formas de ataque siguientes, junto con las contramedidas usadas y presentando ejemplos reales:

- *Desbordamiento del búfer basado en la pila*
- *Inundación SYN*
- *Ataques smurf*

---

4 Information Week Security: http://www.informationweek.com/security/management/amazoncom-ddos-attacker-busted-in-cyprus/240004073

5 International Affairs Review: http://www.iar-gwu.org/node/65

Susan también asesora actualmente a dos organizaciones muy distintas entre sí: una es *Western Heights*, una gran compañía farmacéutica internacional, y la otra es Guanjong HS, una escuela secundaria de la ciudad. El tipo y nivel de amenazas y las medidas de seguridad deseadas son, como es de imaginarse, bastante diferentes.

"Aunque algunos elementos de seguridad podrían ser comunes a ambas, por ejemplo, el uso de servidores proxis, software de seguridad instalado, *etc.*, la ubicación de las amenazas difiere bastante entre ambas organizaciones, y esto marca el nivel de seguridad necesario. Mientras que las principales amenazas para las compañías farmacéuticas provienen del exterior, la principal amenaza para la escuela secundaria viene del interior, por la acción directa de sus propios alumnos. Aunque el colegio tiene datos que considera privados, la forma de navegar de los alumnos y sus posibles consecuencias influirá en qué medida de seguridad se elige.

"Por otra parte, las acciones de las APT serán centrales para el personal de seguridad de la compañía farmacéutica. La instalación y mantenimiento de sistemas de detección (*IDS*) y prevención (*IPS*) de intrusos, que informen a un sistema de *Gestión de eventos e información de seguridad* (*SIEM*) para la inspección del tráfico entrante y saliente de la red son prioritarios."

Cuando se le pregunta sobre el futuro y los sectores en que el software malicioso incidirá con una mayor intensidad, Susan señala el uso creciente de los dispositivos móviles y el espectacular crecimiento de las redes sociales:

"Los delincuentes informáticos siempre se centrarán en los objetivos más débiles, y ven una gran oportunidad en la proliferación de dispositivos móviles con sus vulnerabilidades de seguridad inherentes y en la adopción por parte de muchas compañías de una práctica conocida como *trae tu propio dispositivo* (*Bring Your Own Device* – BYOD). La constante amenaza de los ataques de día cero, las APT y la falibilidad inherente del personal implica que la organización no puede confiar sólo en asegurar el perímetro.

"Las redes sociales son unos de los principales objetivos debido a las grandes cantidades de datos que manejan y a que se ha extendido su uso en los lugares de trabajo."

Retos pendientes

Los retos inminentes a los que se enfrenta Susan son:

- preparar la sección sobre ataques DoS en los sitios Web de la compañía;
- analizar con el administrador de la red de la escuela secundaria Guanjong la configuración de seguridad adecuada para la red de su institución;
- aconsejar a Western Heights que medidas deberían tomar en relación con las amenazas APT;
- preparar un informe para el comité de *XXXSecurity* sobre las crecientes amenazas a la seguridad planteadas por la tendencia a implementar la práctica BYOD.

Véase al dorso

Terminología adicional para la Guía

APT
Ataques DoS / DDoS
Ataques smurf
Ataque/vulnerabilidad de día cero
BYOD
Cortafuegos
Desbordamiento del búfer basado en la pila
Filtrado de paquetes
Gestión de eventos e información de seguridad
Gusano
IDS
IM
Inclusión en listas blancas
Intermediario
Inundación SYN
IPS
Panorama de amenazas
Redes robot
Robots
Script kiddies
Servidor proxy
Software malicioso
Spam
SSL
TLS
Toolkits
Vulnerabilidad
Zombis/computadores zombis

Las empresas, productos o personas mencionados en este estudio de caso no son reales y cualquier parecido con la realidad es meramente casual.