Universidad Nacional Abierta y a Distancia
ACREDITADA EN ALTA CALIDAD

Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo
Número **Tres**

ECBπ
Escuela de Ciencias Básicas, Tecnología e Ingeniería

VIEM
Vicerrectoría de Innovación y Emprendimiento

Semillero de Investigación
Ceros y Unos

E-boletín Informativo CIP- CSIRT Académico UNAD

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Tres
Marzo de 2022

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CIP – CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CIP – CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director CIP CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

Estado legal:
Periodicidad: Quincenal
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Boletín informativo Número 3

Marzo 22 de 2022

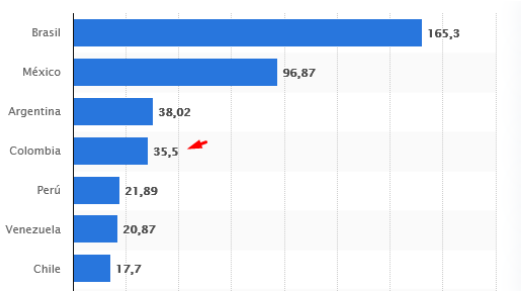
Ataques Informáticos Más Comunes Orientados a Usuarios Finales[1]

Autor: Luis Fernando Zambrano Hernández
ORCID: https://orcid.org/0000-0002-4690-3526

Introducción

El desarrollo de tecnologías de la información y la comunicación han permitido que nosotros como usuarios finales, estemos conectados cada vez mucho más tiempo en internet. Para enero de 2022, Brasil reporta el mayor número de usuarios conectados a esta red con un total de 165 millones, Colombia presenta una conexión para este mes de 35 millones de usuarios conectados[2]. Estos datos que son significativos para la región respecto a seguir conectando a sus ciudadanos en Internet son también un desafío para los usuarios. Desafío que debe girar en torno al buen uso de la información y de la identidad digital[3] y de cuáles podrían ser esas amenazas a las que estamos expuestos encontrándonos en el Ciberespacio.

Figura 1. Usuarios conectados a internet por país en el mes de enero de 2022



Fuente: https://es.statista.com/estadisticas/1073677/usuarios-internet-pais-america-latina/

[1] http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1851-31232005000100012&lng=es&nrm=iso
[2] https://es.statista.com/estadisticas/1073677/usuarios-internet-pais-america-latina/
[3] https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/identidad-digital-profesorado/que-es-la-identidad-digital/

Desarrollo

A continuación, se presentan los vectores de ataque más comunes que se enfocan en vulnerar los sistemas de seguridad para la extracción de información de los usuarios finales a través de internet[4].

Ataque a Contraseñas

Propósito:	Técnica(s) de ataque
Obtener la contraseña a través de algún tipo de técnica de ataque usada por el ciberdelincuente que permita acceder a las aplicaciones utilizadas por el usuario víctima, con el fin de obtener información que permita lograr algún tipo de utilidad económica y de satisfacción personal.	Fuerza bruta: Tiene como objetivo conseguir la contraseña del usuario a partir de un proceso de múltiples combinaciones probando técnicas como ataque por diccionario (uso de un archivo diccionario en formato .txt normalmente), el cual, mediante software automatizado logra probar combinaciones posibles hasta obtener la contraseña (esto se logra si el diccionario es extenso y efectivo).

Como reducir la exposición a este ataque:

- Haga uso de contraseñas que combinen letras en mayúscula y minúscula, números y caracteres especiales
- Use diferentes contraseñas para los sitios que consulta comúnmente y requieren de factor de autenticación
- No escriba las contraseñas en documentos físicos o en documentos digitales que no estén guardados en un espacio en el computador el cual se encuentre cifrado.
- Para navegadores web o aplicaciones que indican o sugieren guardar los usuarios y las contraseñas, no acepte esta petición o hacer caso omiso a los mensajes

Adaptado de: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

[4] https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

Ataque Por Ingeniería Social

Propósito:	Técnica(s) de ataque
Obtener a través de técnicas de ataque basadas en **engaño y manipulación**, revelación de información personal del usuario final, con el fin de generara acciones indebidas de acceso a los sistemas informáticos o de robo de información.	**Phishing, Vishing y Smishing**: Son técnicas similares que tienen como objetivo, la suplantación de organizaciones legalmente constituidas con el fin de enviar mensajes sugestivos o intimidantes logrando así obtener la confianza o el miedo de la víctima para que esta envíe la información que le están requiriendo. • **Smishing**: medio de ataque, mensajes SMS o de texto • **Phishing**: medio de ataque, Correo Electrónico • **Vishing**: medio de ataque: Llamada Telefónica. **Dumpster Diving:** Técnica usada por el ciberdelincuente donde la acción es la de buscar en la basura de la victima, con el fin de obtener información confidencial.

Como reducir la exposición a este ataque:

- Verifique que la dirección de correo electrónico en el dominio[5] (cuentaempsarial@empresa.com), corresponda a la de la organización.
- De lectura de forma detallada al mensaje, con el fin de detectar errores ortográficos o fallas en la redacción. Por lo general las organizaciones legales cuidan su reputación hasta en el más mínimo de talle
- Para el caso de ataques tipo Phising, busque comprobar el número telefónico en el sitio oficial de la organización
- No descargue los archivos adjuntos en este tipo de correos. Si lo llegara a hacer, analícelo a través del antivirus. (de una mirada a nuestro **Boletín Nro° 2**)
- En el caso de la técnica de ataque Dumpster Diving, Elimine la información que va a desechar haciendo uso de una trituradora de papel o de un objeto similar.

Adaptado de: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

[5] https://www.hostinger.co/tutoriales/que-es-un-dominio-web

Ataque a las Conexiones

Propósito:	Técnica(s) de ataque
Obtener a través de técnicas de ataque basadas en interceptar los medios de comunicación o saltar las medidas de seguridad, el control de los sistemas de información o de infectarlos para su manipulación remora.	**Ataques a Cookies**: Técnica de ataque que tiene como propósito extraer información que se almacenan en las cookies. *"Las cookies son pequeños ficheros que se guardan en el dispositivo del usuario y contienen información de las páginas web que ha visitado"*[6] **Web Spoofing:** Técnica que tiene como objetivo suplantar una pagina web real por una falsa, construyendo un dominio con caracteres que hacen pensar a la víctima que están en el sitio original. Eje www.arnazon.com | www.amazon.com ¿Cuál es el real? **Redes Trampa:** Técnica de ataque que consiste en la creación de redes wifi duplicadas, suplantando a redes legitimas. Por lo general cuentan con un nombre de red similar o igual que el original, con el fin de acceder a la información de acceso que la victima genere en el momento de buscar una reconexión en el punto falso.

Como reducir la exposición a este ataque:

- No se conecte en redes inalámbricas que se encuentren libres y que no cuenten con un nivel de autenticación mínima
- Digite el dominio de la página a la que quiere acceder, siempre poniendo de forma previa el protocolo de comunicación https[7]
- Compruebe de forma detallada la dirección de la pagina web a la cual quiere acceder y ubíquese sin hacer clic encima de esta para comprobar el enlace hacia donde será direccionado.
- Actualice de forma constante le navegador web que utiliza
- No almacene las contraseñas haciendo uso de las opciones que brinda el navegador web
- Haga uso de la opción de modo incognito cuando vaya a intercambiar información sensible a través de navegador

Adaptado de: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

[6] https://www.osi.es/es/actualidad/blog/2018/07/18/entre-cookies-y-privacidad
[7] https://developers.google.com/search/docs/advanced/security/https?hl=es

Si ha presentado algún evento de este orden, notifique al correo seguridad.informacion@unad.edu.co

Canales de comunicación

El CIP CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- Correo: csirt@unad.edu.co
- Twitter: @csirtunad

https://csirt.unad.edu.co

Recursos bibliográficos consultados

[1] Juan Carlos Brocca y René Casamiquela. [en línea] Las licencias de software desde la perspectiva del usuario final. Universidad Nacional de Comahue. Disponible en: http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1851-31232005000100012&lng=es&nrm=iso

[2] Número de usuarios de internet por país en América Latina en enero de 2022 [en línea]. STATISTA. Disponible en: https://es.statista.com/estadisticas/1073677/usuarios-internet-pais-america-latina/

[3] ¿Qué es la Identidad digital? [en línea]. Consejería de Educación, Universidades, Cultura y Deportes, Gobierno de Canarias. Disponible en: https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/identidad-digital-profesorado/que-es-la-identidad-digital/

[4] Guía de Ciberataques. [en línea] Oficina de Seguridad del Internauta. Disponible en: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

[5] ¿Qué es un dominio web? Dominios explicados para principiantes [en línea] HOSTINGER. Disponible en: https://www.hostinger.co/tutoriales/que-es-un-dominio-web

[6] Entre cookies y privacidad [en línea]. Oficina de Seguridad del Internauta. Disponible en: https://www.osi.es/es/actualidad/blog/2018/07/18/entre-cookies-y-privacidad

[7] Proteger sitios con el protocolo HTTPS [en línea]. GOOGLE. Disponible en: https://developers.google.com/search/docs/advanced/security/https?hl=es