gms seguridad de la información

LOS ATAQUES DE INGENIERÍA SOCIAL

Nuevos ataques en el último trimestre de 2018

Te compartimos aquí información acerca de 25 ataques que se han publicado últimamente en algunos portales de Seguridad de la Información; estos son apenas 25 casos de los muchos que siguen impactando a varias organizaciones mediante las técnicas de ingeniería social. Los cibercriminales saben que es más fácil y rentable perjudicar a una empresa a través de sus recursos humanos.

FECHA	ENLACE	RESUMEN	TIPO DE ATAQUE
02/10/2018		El *malware* bancario DanaBot se extendió a través de una campaña masiva dirigida a recipientes en los EEUU. Los cibercriminales enviaron mensajes de correo electrónico que, supuestamente, provenían de una dirección de eFax.	Varios
08/10/2018		Se han detectado nuevas operaciones cibercriminales de Cobalt Group, conocido también como Carbanak. Este grupo es responsable de más de 100 ataques a diferentes bancos en 40 países y usa técnicas de ingeniería social para lograr sus objetivos con mayor facilidad.	Varios
11/10/2018		Apareció un nuevo troyano para dispositivos móviles Android, conocido como 'GPlayed'. Usa un ícono muy similar a Google Apps, con una etiqueta de "Google Play Marketplace" para disfrazarse.	Infección
11/10/2018		Una actualización falsa de Adobe Flash ha implementado una decepción adicional: engaña a sus víctimas porque **sí** instala la actualización real de Adobe Flash… pero también instala el troyano criptominero XMRig.	Infección
15/10/2018		Un grupo cibercriminal ruso, conocido como DustSquad, se aprovechó del revuelo acerca de la posible prohibición del programa Telegram Messenger en Kazakstán. Utilizó tácticas de ingeniería social para distribuir un *malware* para Windows llamado Octopus, que se hace pasar por una alternativa en ruso de este programa de mensajería.	Infección
19/10/2018		Un grupo cibercriminal, conocido como APT-C-27, lanzó un ataque en algunos países árabes; se hizo pasar por la Agencia de las Naciones Unidas para los Refugiados de Palestina en Oriente Próximo (UNRWA) mediante el envío de mensajes de correo electrónico que contenían una carta y un formulario falsificados.	Infección
25/10/2018		En grupo de cibercriminales, llamado Cobalt Gang, usó tácticas muy simples de ingeniería social para difundir *malware:* envió un mensaje de correo electrónico a entidades bancarias en todo el mundo con el asunto: "Confirmaciones para el 16 de octubre, 2018". Este mensaje contenía un PDF como adjunto, que no tenía *malware*; sin embargo, el PDF incluía un enlace que, al hacerle clic, abría una ubicación de Google legítima, que, a su vez, redirigía el navegador a un documento malicioso.	Infección
05/11/2018		'GPlayed', el troyano para dispositivos móviles Android, tiene un predecesor llamado "GPlayed Banking." Este también usa un ícono muy similar a Google Apps, con una etiqueta de "Google Play Marketplace" para disfrazarse. A diferencia de "GPlayed", este está específicamente dirigido a los usuarios de Sberbank AutoPay, un servicio que ofrece este banco ruso.	Infección
05/11/2018		Ha sido muy difícil detectar a un grupo de cibercriminales conocido como Inception, debido a su uso de plantillas remotas, de técnicas antiforenses durante el proceso de instalación del *malware*, y de un nuevo *backdoor* básico llamado POWERSHOWER.	Infección
05/11/2018		En Irán, algunos grupos de cibercriminales usaron varias técnicas (páginas falsas de acceso, aplicaciones maliciosas disfrazadas de sus contrapartes legítimas y la toma ilegal de grupos de direcciones de IP mediante la corrupción de las tablas de enrutamiento de Internet que usan el Border Gateway Protocol (BGP) para obtener acceso remoto a las aplicaciones de medios sociales y de mensajería —como Telegram e Instagram— y robar así la información privada de los usuarios.	Varios
08/11/2018		Se descubrieron dos campañas de distribución de *malware* que buscan infectar a los clientes de las instituciones financieras en el Brasil con el troyano bancario Metamorfo.	Infección
17/10/2018		Se descubrió una campaña de ciberespionaje dirigida a la industria naval italiana, que tenía el objetivo de difundir el *malware* conocido como MartyMcFly. Este era un ataque de *phishing* a través de *emails*, en donde los cibercriminales intentaron hacerse pasar por vendedores conocidos de servicios navales para engañar a las víctimas.	Infección
12/11/2018		Se descubrió un ataque que insertaba URL maliciosos dentro de los videos embebidos en los documentos de Microsoft Office.	Infección
19/11/2018		Se reportaron más ataques con el troyano bancario Ursnif, que viene en los archivos de Microsoft Office Word: para poder abrir el archivo, se le pide al usuario que habilite los macros porque, supuestamente, "el documento fue creado en una versión anterior"; al habilitar los macros, se descarga el *malware*.	Infección
12 / 09 / 2018		APT28, también conocido como Fancy Bear, el famoso grupo de *hackers*, lanzó un ataque dirigido a los miembros de la OTAN y a las instituciones militares de algunos países de Europa del Este. El ataque consistía en enviar mensajes de correo electrónico de *spear-phishing* que contenían un documento malicioso adjunto llamado "NATO Simulation.doc".	Infección
01/12/2018		Se descubrió una campaña de *spear-phishing* dirigida a los usuarios en Qatar y Turquía, que intentaba engañar a las víctimas para que hagan clic en el botón de "habilitar contenido" en el documento adjunto del *email* enviado. Al hacer clic, se ejecutaba un macro malicioso. El email contenía una invitación falsa a la Conferencia de la Asociación de "Parlamentarios para Al Quds" en Estambul; sin embargo, esta conferencia nunca se realizó.	Infección
11/12/2018		Se ha identificado un nuevo *kit* de *exploits*, conocido como Novidade, que ataca a los *routers* de oficinas pequeñas al cambiar los ajustes del Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) a través de la falsificación de petición en sitios cruzados (CSRF).	Infección
11/12/2018		Se descubrieron dos nuevos *malware* para Mac: el uno es un criptominero, conocido como DarthMiner; y el otro se roba información mediante capturas de pantalla, conocido como LamePyre. La difusión de estos programas maliciosos depende de las tácticas de ingeniería social para lograr que el usuario abra un documento de Word y que se ejecute así un macro malicioso.	Infección
05/12/2018		Se ha detectado una nueva amenaza dirigida a las instituciones académicas, conocida como STOLEN PENCIL (lápiz robado). El objetivo parece ser el robo de credenciales a través de *emails* de spear *phishing*, que llevan a un sitio web que despliega un documento engañoso que solicita que el usuario instale una extensión maliciosa de Google Chrome.	Infección
13/12/2018		Se ha detectado un nuevo ataque de *phishing* conocido como el "Regreso de Charming Kitten" (el gatito encantador), que se cree que es patrocinado por el estado iraní. Es un ataque dirigido a individuos involucrados en sanciones económicas y militares en contra de la República Islámica de Irán, así como a políticos, activistas civiles y de derechos humanos y periodistas en todo el mundo.	Robo de credenciales
13/12/2018		Un grupo de cibercriminales tomó "prestado" algunos archivos del sitio web de la Embajada Británica y los usó para engañar a las víctimas y desplegar así el *malware* POWERSING.	Infección
14/12/2018		Se ha descubierto una campaña de *spam* que envía emails con un documento de Publisher (.PUB) como adjunto para engañar al usuario para que descargue un macro malicioso, que, a su vez, instala un Troyano de Acceso Remoto (RAT, por sus siglas en inglés) en la computadora de la víctima.	Varios
14/12/2018		Se ha detectado un grupo de cibercriminales que usaron una técnica conocida como esteganografía –es decir, esconder una carga útil maliciosa dentro de una imagen para evadir las soluciones de seguridad–. En este caso, los ciberdelincuentes usaron Twitter para postear tuits con memes maliciosos, que contenían un comando embebido para descargar el *malware* a la máquina de la víctima. Este *malware* tomaba capturas de pantalla de la máquina infectada, para luego enviarlas a su servidor de C&C.	Varios
18/12/2018		El grupo cibercriminal Sofacy sigue creando diferentes variantes de la carga útil Zebrocy –usando diferentes lenguajes de programación– en sus campañas de ataque.	Infección
18/12/2018		Se descubrió una campaña de *spam* que incluía una alerta falsa de tsunami para Japón. Los *emails* de *spam* contenían un enlace falso a la Agencia de Meteorología Japonesa, que, al hacerle clic, se descargaba el troyano Smoke Loader.	Infección

El servicio de Gestión de Ingeniería Social de GMS pone a tu disposición una metodología efectiva y medible de concienciación.

¡Pregunta por nuestros planes!

https://gmsseguridad.com/ingsocial.html

gestion.is@gmsseguridad.com

Av. Naciones Unidas Nº. 1014 y Amazonas,
Edif. La Previsora, Torre A, Piso 11, Of 02
Teléfono: +593 2 399-3000
Quito, Ecuador