gms seguridad de la información

LOS CIBERATAQUES CON INGENIERÍA SOCIAL

20 ataques entre enero y marzo de 2018

Te compartimos ataques que se han publicado en portales de empresas de Seguridad de la Información, 20 de ellos siguen impactando a organizaciones y que parten con técnicas de ingeniería social. Los cibercriminales saben que es más fácil y rentable atacar a una empresa a través de sus recursos humanos.

FECHA	ENLACE	RESUMEN	TIPO DE ATAQUE
1-ENE-18		Israel: Se engaña a las personas con remitentes y asuntos falsos, mediante el uso del nombre de un conocido instituto de investigación.	INFECCIÓN
1-ENE-18		Con asuntos llamados "boleto", se engaña a los usuarios para descargar *malware* o para desviar a sitios falsos y robar sus credenciales.	VARIOS
1-ENE-18		Se distribuye *malware* con mensajes que dicen en el asunto: "Orden de Compra".	INFECCIÓN
3-ENE-18		Los cibercriminales utilizan técnicas de engaño con asuntos de monedas virtuales para que las víctimas descarguen *malware* que toma control de su equipo y hasta de la red de las empresas.	INFECCIÓN
11-ENE-18		Se ataca a los equipos MacOS a través del engaño a los usuarios para tomar control de sus equipos y sus dispositivos.	INFECCIÓN
18-ENE-18		Los cibercriminales distribuyen troyanos bancarios por medio de correos falsos.	INFECCIÓN
18-ENE-18		Mediante aplicaciones que contienen un código malicioso, se roban las credenciales desde las redes sociales.	INFECCIÓN
24-ENE-18		Los ciberdelincuentes suplantan contactos gubernamentales para realizar espionaje a personas.	ESPIONAJE
30-ENE-18		Se realizan operaciones de espionaje a comunidades tibetanas a través de mensajes falsos y accesos falsos a cuentas de correo electrónico.	ESPIONAJE
1-FEB-18		Un adolescente se hace pasar por el director de la CIA y del FBI para robar información secreta.	ROBO DE INFORMACIÓN CONFIDENCIAL
13-FEB-18		Se detectan aplicaciones falsas de mensajería instantánea a través de las cuales se engaña a los usuarios para obtener toda su información.	ESPIONAJE
13-FEB-18		Los atacantes envían mensajes falsos con adjuntos maliciosos que explotan las vulnerabilidades en la pagina web telegram para tomar el control de los teléfonos de los usuarios.	INFECCIÓN
26-FEB-18		Los atacantes envían mensajes falsos entre ellos, y suplantan así la identidad de DHL con adjuntos que tienen un formato RTF, que camufla varios tipos de *malware*.	VARIOS
2-MAR-18		Se ejecutan ataques dirigidos de *phishing* para aprovechar las vulnerabilidades en los sistemas.	INFECCIÓN
7-MAR-18		Se registran víctimas de espionaje en la India, que fueron engañados para abrir documentos maliciosos que estaban adjuntos en mensajes falsos.	ESPIONAJE
13-MAR-18		Descubren ataques de espionaje en Irán, que se ejecutan con mayor efectividad gracias a los engaños a los usuarios.	ESPIONAJE
22-MAR-18		Engañan a los usuarios que visitan las páginas web mediante mensajes en ventanas emergentes (*pop-ups*) y una vez que dan clic, sin notarlo, los usuarios instalan varias amenazas, entre ellas, *ransomware*.	VARIOS
23-MAR-18		Se utilizan aplicaciones falsas para Android para espiar a protestantes en Irán.	ESPIONAJE
25-MAR-18		Se descubrió otro documento que es utilizado para infectar a los equipos de las víctimas engañadas con *malware* multipropósito, entre ellos, *software* para controlar de forma remota las máquinas.	VARIOS
28-MAR-18		se engaña a los usuarios con asuntos como "Propuestas de Inversión", para que descarguen un archivo que, una vez abierto, infecta a los equipos con *malwares*, entre ellos, el *ransomware*.	INFECCIÓN

Transforma al equipo humano de tu organización del eslabón más débil en cuanto a la Seguridad de la Información a agentes de prevención y detección contra ataques que pueden impactar de forma negativa a tu empresa.

www.gmsseguridad.com/is.html
info@gmsseguridad.com

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