CySec News

2019 OCTUBRE

PHISHING & RANSOMWARE

ESTADISTICAS

Ransomware	Phishing
1. Ocurren más de 4,000 ataques de Ransomware por día. (FBI) 2. 75% de las organizaciones infectadas con Ransomware tenían protección activa. (Sophos) 3. Los daños globales relacionados a ataques de Ransomware llegarán a $11.5 billones en el 2019. (Cybersecurity Ventures) 4. Se estima que habrá un ataque de Ransomware cada 14 segundos para el fin del 2019. Esto no incluye ataques a individuos, que ocurren con mayor frecuencia. (Cybersecurity Ventures) 5. 91% de los ataques comienzan con la técnica de spear phishing, que apunta a vulnerar correos e infectar organizaciones. (KnowBe4)	1. En una encuesta realizada a más de 1300 profesionales de TI se descubrió que 56% de las organizaciones identificaron al phishing como su mayor riesgo de seguridad informática. (CyberArk) 2. 76% de las negocios reportaron ser víctimas de ataques phishing en el último año. (Wombat Security) 3. Verizon reporta que usuarios estadounidenses abren un 30% de todos los correos maliciosos y un 12% de ellos dan clic al enlace peligroso. (Verizon) 4. Kaspersky's ha detectado 246,231,645 intentos de phishing en el 2017, y evidenció un crecimiento de 91 millones con respecto al 2016. (Kaspersky)

Fuente: https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

TÉCNICAS DE PHISHING

Se habla de que los ciberdelincuentes se encuentran un paso adelante innovando sus técnicas de ataque, combinando diferentes tipos de ciberamenazas, es cierto que, entre los ataques más usados por los ladrones cibernéticos está el phishing y el Ransomware, en el reporte de seguridad de ESET mencionan que en el 2018 el Ransomware ocupo el primer lugar de la amenaza más utilizada para los ataques cibernéticos, sin embargo, el phishing no se queda atrás ya que este vector de ataque está en constante evolución volviéndose más inteligente para lograr su objetivo.

Pero ¿qué es lo que hace tan atractivo el uso de campañas de phishing? Como sabemos este tipo de ciberataque tiene la finalidad de engañar a los usuarios para robar información personal, contraseñas, información financiera o suplantar identidad.

A continuación, mencionare los tipos de phishing para poder reconocerlo:

Phishing tradicional: este tipo de ataque opera por medio del correo electrónico el ciberdelincuente se hace pasar por alguna empresa o marca reconocida, para poder ganar la confianza de los usuarios y así obtener información personal o credenciales de acceso a un determinado sitio, otro método de operación es recibir un correo electrónico el cual incluya links que lo dirijan a un sitio web malicioso.

Malware-Based Phishing: este tipo de ataque se caracteriza por el envío de correos electrónicos en los que se introduce una pieza de malware como archivo adjunto o como un descargable en el sitio web al que apunta el hipervínculo enviado por email y así poder aprovechar las vulnerabilidades del dispositivo del usuario. Este tipo de ataque es especialmente común en las pequeñas y medianas empresas.

Vishing: en esta modalidad de ataque el ciberdelincuente realiza llamadas haciéndose pasar por algún proveedor, operadora, un centro de soporte, un banco, etc. Con el objetivo de recabar información personal.

Smishing: a diferencia los demás, este tipo de ataque se ejerce a través de los teléfonos móviles. El hacker suele hacerse pasar por una empresa de confianza y envía un sms informando al usuario de que ha ganado un premio, en donde debe participar en un sorteo o para ofrecerle algún tipo de servicio.

Spear Phishing: este tipo de ciberataque ya tiene identificada a la víctima, su finalidad es acceder a cierto tipo de información confidencial.

Pharming: los ciberdelincuentes pueden envenenar un servidor DNS para que los usuarios visiten el sitio falso sin darse cuenta. Los sitios web falsos se pueden utilizar para instalar virus o troyanos en la computadora del usuario, o pueden ser un intento de recopilar información personal y financiera para usarla en el robo de identidad.

SEO Phishing: los cibercriminales logran clonar alguna página de algún sitio web ya sea una tienda online o bancaria.

TÉCNICAS DE RANSOMWARE

Por el contario el Ransomware es una amenaza que busca infectar nuestros dispositivos, 60% de los ataques de Ransomware en América Latina son originados en México, este tipo de software malicioso puede instalarse por medio de enlaces, correo electrónico, publicidad emergente o un sitio web poco seguro, la popularidad del Ransomware se debe a que, es muy sutil a la hora de ingresar en nuestros sistemas operativos. México enfrenta un promedio de 57 intentos de Ransomware por día, todos los días.

Sin embargo, también existen diferentes tipos de Ransomware y cada uno funciona de diferente manera:

Filecoder: cifra archivos del equipo y pide un rescate generalmente en bitcoins para darle al usuario la clave de descifrado.

Lockscreen: cifra archivos y bloquea el acceso al equipo.

Virus de la policía: se trata de un troyano que bloquea las máquinas al iniciarse y muestra un falso mensaje de la policía con la excusa de haber detectado accesos a páginas ilegales como pornografía infantil y para el desbloqueo solicita el pago de una multa.

Wiper: nunca devuelve el acceso a los archivos y los elimina directamente.

Hoax Ransomware: es similar al filecoder, sólo que no cifra ningún archivo, lo que busca es asustar al usuario para que pague un rescate.

FUENTE DE REFERENCIA

Randed	US-CERT	ESET	SearchDataCenter
Kaspersky	WeLiveSecurity	AVAST	Proofpoint
Securelist	Godaddy	Panda Security	Revista Mas Seguridad

Contribuidor

Nancy Martinez: Egresada como estudiante de comunicación y periodismo de la FES Aragón (UNAM, MÉXICO), actualmente trabaja en una consultora de seguridad informática, en donde se encarga de administrar las redes sociales, compartiendo las noticias más recientes sobre ciberseguridad.

LinkedIn: https://www.linkedin.com/in/nancy-martínez-lucio-a4a93a179/

Recursos LCW

LinkedIn	https://www.linkedin.com/company/cysecbywomen/
Facebook	https://www.facebook.com/CySecByWomen/
Twitter	@cysecbywomen