[Estado de Internet] / Seguridad

Phishing en servicios financieros

Colaboramos con la empresa de inteligencia frente a las amenazas WMC Global para obtener una imagen más completa de cómo afectaron las amenazas al sector financiero en 2020. A continuación se recogen los resultados.

ATAQUES CONTRA EL SECTOR DE LOS SERVICIOS FINANCIEROS

736 071 428
ataques web
+ 62 % frente a 2019

3400 millones
ataques de Credential Stuffing
+ 45 % frente a 2019

Aumento del 110 %
de los ataques DDoS
frente a 2019

---

63 millones: Número de ataques máximo de Credential Stuffing en un día

LAS HERRAMIENTAS COMPLEJAS FACILITAN LOS ATAQUES

En algunos casos, los kits de phishing complejos son réplicas casi perfectas de la marca objetivo. Incluyen asistencia operativa y funcionalidad de back-end. Así, los criminales menos habilidosos solo tienen que comprar estos kits y utilizarlos contra el público. Dispone de más información en el informe completo.

EL SURGIMIENTO DEL PHISHING COMO UN SERVICIO

8344
Dominios en los que se han encontrado kits de phishing Kr3pto desde 2020. Solo en el Reino Unido, 11 bancos como objetivo

220 000
Interacciones con API atribuidas a kits de phishing Ex-Robotos, del 1 de enero al 12 de febrero de 2021

Ahora el objetivo de los delincuentes son las protecciones 2FA y MFA: se engaña a las víctimas para que introduzcan su OTP o para que la revelen al atacante durante una conversación.

¿CÓMO PUEDE GARANTIZAR LA SEGURIDAD?

Tal y como se explica en nuestro nuevo informe, debe "limitar y controlar el acceso, utilizar varias capas de autenticación y estratificar las defensas para agilizar al máximo la detección de incidentes. Cuanto antes detecte el problema, antes se podrá resolver".

Estado de Internet / Seguridad
Descargue el informe para conocer las últimas tendencias y los ataques que se usan contra el sector de los servicios financieros, así como para saber cómo defenderse ante ellos.

Descargar ahora

@2021 Akamai Technologies | Asistencia | Publicado en mayo de 2021 septiembre de 2020.