
DUCATI
916

Un ataque es cuestión de tiempo.

¿Cuál es el activo más vulnerable de una organización?

Las personas.

CRYSTAL ROOT
CYBER SECURITY SOLUTIONS

Tipos de ataques

- Ataques a infraestructura Web
- Ataques a los colaboradores de la organización (Phishing)

Intenciones de un atacante

- Los atacantes usualmente tienen una meta en mente cuando toman como objetivo una organización.

- El acceso a los datos puede ser dirigido, oportunista o incluso pagado.

- Algunas metas de los atacantes:

  - Ransomware
  - Beneficios económicos
  - Interrupción de Servicio
  - Robo de propiedad intelectual

Percepciones erróneas de ciberataques

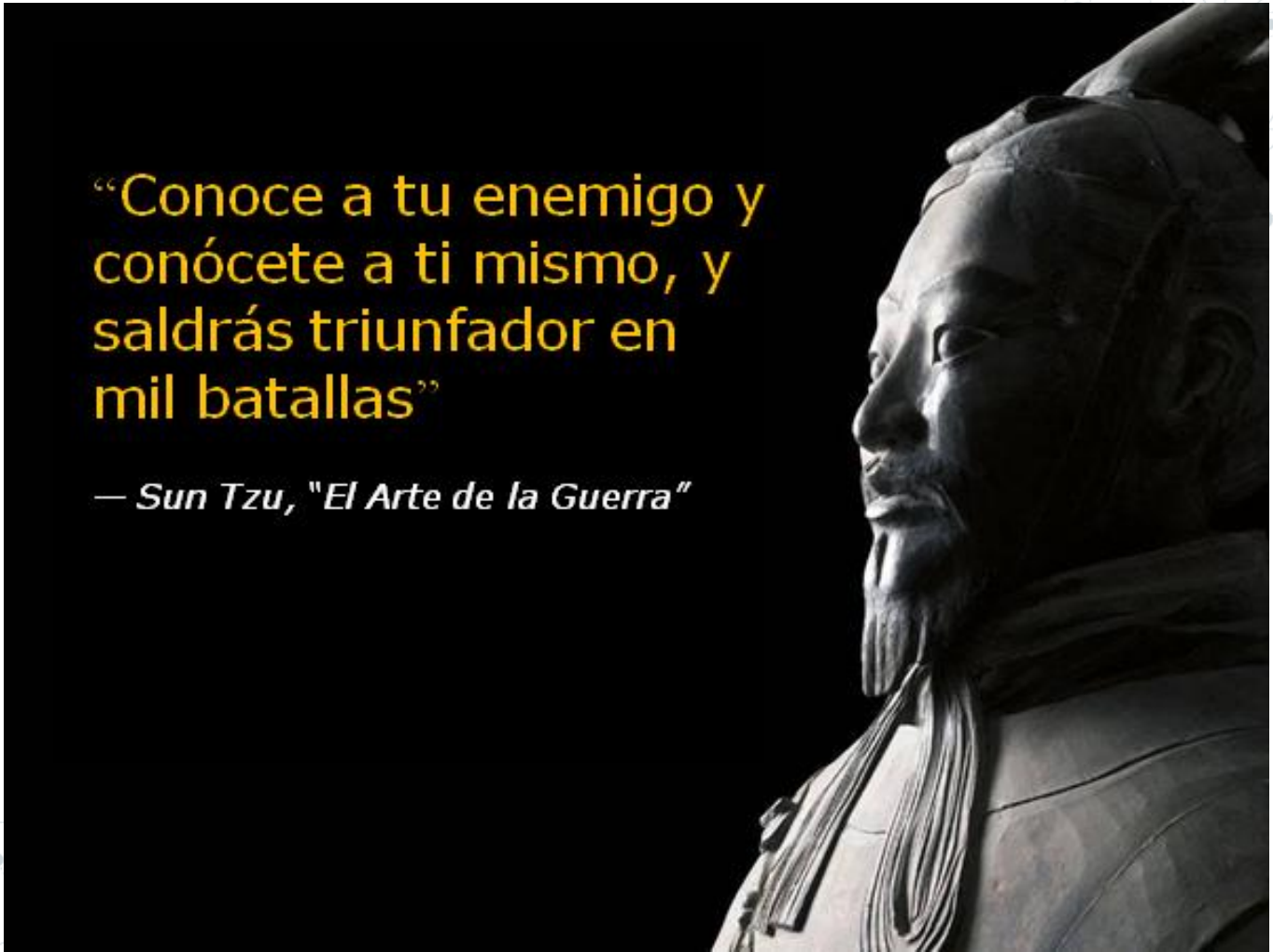
- Solo pasa en las grandes empresas.
- Esto no me pasa a mí.
- Eso no tiene consecuencias graves.
- Creemos que es un tema que le compete sólo al área de TI.
- Tengo antivirus entonces estoy protegido.

CRYSTAL ROOT
CYBER SECURITY SOLUTIONS

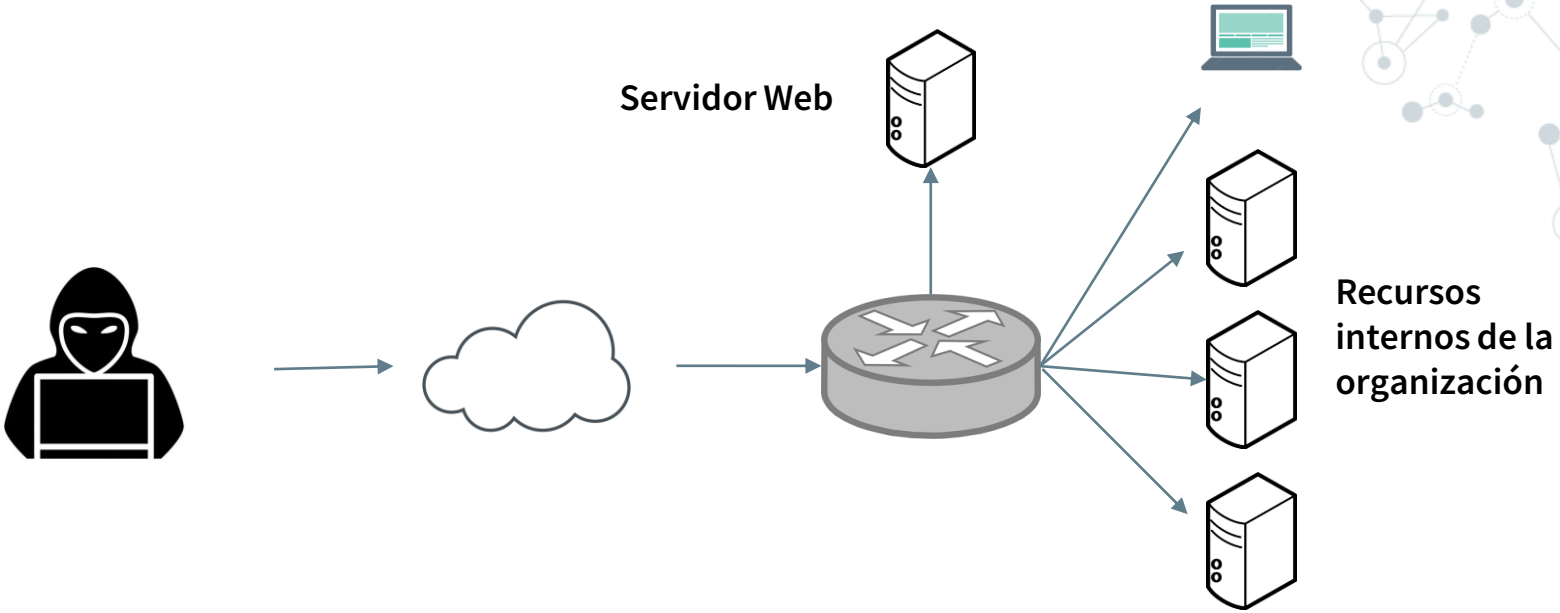
Tipo de ataques más comunes

- WEB ATTACKS
- INGENIERÍA SOCIAL
- SPAM
- DDOS
- PHISHING
- MALWARE

CRYSTAL ROOT
CYBER SECURITY SOLUTIONS


“Conoce a tu enemigo y conócete a ti mismo, y saldrás triunfador en mil batallas”
— Sun Tzu, “El Arte de la Guerra”

Escenario



Phishing como vector de ataque

CRYSTAL ROOT
CYBER SECURITY SOLUTIONS

Phishing como vector de ataque

La Policía alerta de una nueva estafa: si te dicen que se ha iniciado sesión desde un nuevo dispositivo, no piques

ÁNGELA PUÉRTOLAS

Así se aprovechan los cibercriminales de la guerra entre Rusia y Ucrania: los timos más comunes para robar dinero y datos

ANA HIGUERA

Aumentan los ataques de phishing en LinkedIn: los estafadores se hacen pasar por la red social a través de correos electrónicos

RAQUEL HOLGADO

CRYSTAL ROOT
CYBER SECURITY SOLUTIONS

NOTICIA

El phishing aumenta un 70% desde el inicio de la pandemia

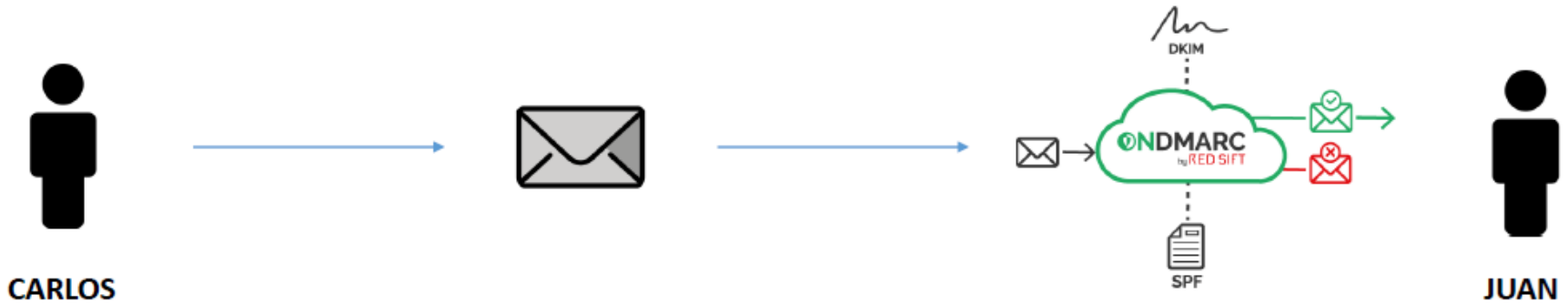
- Correos electrónicos que suplantan a una organización y se combinan con una amenaza o solicitud de información (57%).
- Ataque de correo electrónico dirigido que puede incluir *whaling* y *spear phishing* (51%).
- Un correo electrónico con un enlace malicioso (49%).
- Un correo electrónico con un archivo adjunto malicioso (46%).
- Ataque de suplantación de directivos (46%).
- Robo de credenciales por correo electrónico (40%).
- Mensaje de SMS para robar información (40%).
- Participación de los ciberdelincuentes en hilos de correo electrónico (36%)

CRYSTAL ROOT
CYBER SECURITY SOLUTIONS

Ahora cualquiera puede hacer phishing sin conocimientos de seguridad

José Antonio Lorenzo | Publicado el 15 de febrero, 2022 • 17:46

Escenario



Recomendaciones de mitigación

- Tener un enfoque proactivo y no reactivo a la seguridad.
- Implementar pruebas de penetración en la organización.
- Implementar simulaciones de campañas de phishing.
- Implementar tecnología DMARC para evitar suplantación de identidad.
- Implementar soluciones con indicadores visuales para los usuarios.

CRYSTAL ROOT
CYBER SECURITY SOLUTIONS

CRYSTAL ROOT
CYBER SECURITY SOLUTIONS

¡Gracias!

www.crystalrootsecurity.com


CrystalRootSecurity


@crystal_root_security


crystal-root-security