

ESTRATEGIA DE DESPLIEGUE DE CAMPAÑAS

JaymonSecurity

Cyberintelligence & Solutions

<https://jaymonsecurity.com>

ÍNDICE

- Métodos de despliegue de campañas
- Comparativa métodos de campaña

MÉTODOS DE DESPLIEGUE DE CAMPAÑAS

Digital Dirigido: Ataques a X direcciones de correo electrónico validadas por cada entidad objetivo, para la descarga de Código en portal externo, direccionado a otra ubicación que se defina y que sea técnicamente factible la descarga.

Físico Aleatorio: Despliegue físico de unidades tipo USB (X) para cada entidad objetivo, con código sembrado en programa legítimo basado en falsa campaña (por definir).

Físico Dirigido: Mediante el uso de personal interno sembrar el código en cada entidad objetivo.

COMPARATIVA MÉTODOS DE DESPLIEGUE

Método de Despliegue	Pro	Contras	Riesgo
Digital Dirigido	<ul style="list-style-type: none"> • Despliegue sin exposición Física. • Aprovechamiento medianamente fácil y rápido. • Atención Dirigida a Contingencia actual (COVID-19) facilita las campañas. • Posibilidad y cobertura a gran cantidad de entidades objetivo. 	<ul style="list-style-type: none"> • Pudiera ser detectado por Seguridad Perimetral. • Personal Objetivo del ataque no trabajando en la oficina objetivo (Cuarentena). 	<ul style="list-style-type: none"> • Ataque detectado por Seguridad Perimetral. • Generación de Huellas en componentes y fabricantes de Ciberseguridad.
Físico Aleatorio	<ul style="list-style-type: none"> • By-pass de controles tecnológicos perimetrales. • Bajo probabilidad de sospecha inmediata. • No requiere el acceso físico. • Trazabilidad media de detección final del ejecutor. 	<ul style="list-style-type: none"> • Depende de un usuario incauto. • Dificultad de movilidad local en la ciudad (Cuarentena). • Ausencia de Personal disponible en las recepciones (Cuarentena). 	<ul style="list-style-type: none"> • La dependencia del usuario incauto pudiera provocar que nunca se materializara el ataque.
Físico Dirigido	<ul style="list-style-type: none"> • By-pass de controles tecnológicos perimetrales. • Ataque preciso contra la plataforma. • Ataque más efectivo. • Atención Dirigida a Contingencia actual (COVID-19). 	<ul style="list-style-type: none"> • Alta probabilidad de sospecha inmediata. • Requiere acceso físico. • Trazabilidad alta de detección final del ejecutor. • Requiere gran cantidad de personas para cubrir las entidades objetivo. 	<ul style="list-style-type: none"> • Identificación, detección y desaparición del atacante. • Compromiso de todo el equipo participante.

GRACIAS POR SU ATENCIÓN