Engaño En acción

Las diez principales amenazas reales detectadas por Zscaler Deception





©2024 Zscaler, Inc. Todos los derechos reservados.

Defensa activa basada en engaños contra ataques dirigidos

El engaño es una de las estrategias más eficaces para detectar los ataques realizados por personas que generalmente eluden las defensas predecibles. Su objetivo es alterar las tácticas de los atacantes y forzarlos a cometer errores que lleven a su detección.

Nuestra plataforma Zscaler Deception se implementa con una estrategia que tiene en cuenta cómo podría moverse un atacante en su entorno. Esto nos ha permitido detectar las amenazas graves que afectan a las organizaciones globales.

Este documento analiza algunos de los principales ataques de nuestra red global de señuelos.

Las 10 principales detecciones reales en la práctica

01 APT de Corea del Norte

02 Tácticas de ransomware por parte de seres humanos (preinfección)

03 Reconocimiento y escaneo interno

04 Rellenado de credenciales

05 Explotación del router MikroTik

06 Ataque de fuerza bruta distribuido

07 Poner en riesgo el controlador de la máquina de rayos X

08 Propagación del ransomware MedusaLocker

09 Alerta temprana contra ransomware

10 Ataque Shadow a RDP

© 2024 Zscaler, Inc. Todos los derechos reservados.

CASO PRÁCTICO 1

Ataque de APT de Corea del Norte a un gran conglomerado global

El incidente

El escaneo del puerto SMB en el señuelo desencadena una detección.

- Se capturó el nombre de usuario NTLM.
- El contexto reveló que se trataba de un usuario comprometido.

Clasificación e investigación

- Dominio C2 similar al dominio legítimo
- Nuestra investigación aisló dos DLL sin firmas conocidas.
- Los archivos DLL contenían credenciales codificadas y código cargador para recibir más comandos.
- El equipo confirmó fuera de línea que fue un intento dirigido desde Corea del Norte por parte del grupo “Hidden Cobra”.

Estrategia del engaño

- Se identificaron las partes críticas de la infraestructura con más probabilidades de recibir ataques y se colocaron señuelos en esos segmentos.
- Soporte Zscaler Threat Hunting para la investigación y clasificación de puntos finales

Resultado

- Zscaler Deception fue la única solución que dio la alerta en el entorno.

Para tener en cuenta

Una estrategia de engaño adaptada a las limitaciones del entorno y a los resultados deseados es uno de los factores más importantes que determinan el éxito de la defensa activa.



©2024 Zscaler, Inc. Todos los derechos reservados.



CASO PRÁCTICO 2

Detección de un operador de ransomware dirigido a un minorista antes de la infección

El incidente

El “paciente cero” activó la cuenta del servicio señuelo.

- Un sistema escaneó los señuelos de Active Directory para buscar la propiedad del nombre principal del servicio (SPN) el 8 de mayo de 2021.

Movimiento lateral a un señuelo sobre el SMB del paciente cero.

- La autenticación NTLM reveló el compromiso de la cuenta SYSTEM el 13 de mayo de 2021.

Propagación de ransomware a través de WinRM.

- Los señuelos detectan el escaneo del puerto 5985 el 10 de junio de 2021.

El ransomware se instala mediante WinRM el 13 de junio.

- Lamentablemente, debido a la falta de una respuesta oportuna, el ransomware infectó varios servidores en la red.

Estrategia del engaño

- Los señuelos de Active Directory detectan el compromiso de la cuenta.
- Los señuelos de red en DC y DMZ detectan el movimiento lateral.

Resultado

- Zscaler Deception avisó de un ataque inminente de ransomware con anticipación, un mes antes del incidente.

Para tener en cuenta

Los señuelos de Active Directory son una de las fuentes más confiables para advertir una infección inminente en un ataque de ransomware. Los equipos de seguridad deben priorizarlos para su investigación.

©2024 Zscaler, Inc. Todos los derechos reservados.

CASO PRÁCTICO 3

Reconocimiento y escaneo interno en un banco importante

El incidente

El atacante obtiene acceso a través de un enrutador en peligro.

- Un router en peligro es la fuente de una amplia interacción con señuelos en varios puertos, incluido SSH.

El atacante pasa más de 6 horas ejecutando cientos de comandos en 3 señuelos SSH.

- Inicio de sesión con raíz/raíz
- Comandos de conocimiento de situación
- Intento de compilar el código binario del escáner de red personalizado
- Robo de contraseñas de /etc/passwd + /etc/shadow
- Intento de utilizar el señuelo como pivote (bloqueado)
- Intento de olfatear la red con TCPDump

Estrategia del engaño

- Los señuelos de red de alta interacción no solo detectan a los atacantes, sino que también interactúan con ellos lo suficiente como para revelar su estrategia e intención.

Resultado

- Se evitó el ataque ya que el atacante estaba ocupado en el señuelo mientras el cliente intentaba localizar y acceder al enrutador.

Para tener en cuenta

Los ataques realizados por personas tienen en cuenta la estrategia de defensa de su objetivo y evitan los controles de detección tradicionales por completo. En este caso, el objetivo era un enrutador, un dispositivo que normalmente no tiene instalado el EDR. Los equipos de seguridad deben implementar señuelos de esos dispositivos para detectar a los atacantes sofisticados.



©2024 Zscaler, Inc. Todos los derechos reservados.



CASO PRÁCTICO 4

Ataque de relleno de credenciales a un despacho de abogados con clientes de alto perfil

El incidente

Se dio alerta por el relleno de credenciales en un señuelo Citrix orientado a Internet.

- Se enviaron al señuelo más de 200 credenciales de dominio comprometidas.
- El ataque tuvo origen en la infraestructura de un proveedor ruso de servicios en la nube.

Acciones de respuesta y contención

- Lista de bloqueos dinámicos en el firewall utilizando la capacidad de orquestación
- Intento de utilizar el señuelo como pivote (bloqueado)
- Intento de olfatear la red con TCPDump

Estrategia del engaño

- Aplicaciones señuelo orientadas a Internet, a las que comúnmente apuntan los atacantes para la validación de credenciales.
- Servicio Threat Hunting gestionado

Resultado

- Zscaler Deception desvió un ataque de los activos de producción justo al principio de la cadena de eliminación.

Para tener en cuenta

Los señuelos orientados a Internet que imitan los servicios y aplicaciones de acceso remoto con días cero y vulnerabilidades conocidas desvían los ataques antes de la vulneración.

©2024 Zscaler, Inc. Todos los derechos reservados.

CASO PRÁCTICO 5

Explotación del enrutador MikroTik

El incidente

Se activó una alerta en un señuelo de SSH de MikroTik personalizado.

- Escaneo de señuelos en puertos conocidos de MikroTik RouterOS como 8291/tcp, 8728/tcp y 22/tcp (SSH)
- Interacción con el servicio SSH del señuelo de MikroTik personalizado mediante una herramienta basada en GO (SSH-2.0-Go)
- Se registró fuerza bruta de credenciales.
- Se detectaron varios comandos de conocimiento de situación.
- Se creó una tarea programada para obtener y ejecutar desde Internet.

Estrategia del engaño

- Señuelos personalizados para imitar componentes específicos que se utilizan activamente en el entorno.

Resultado

- Se aisló la fuente.
- Acceso directo a telemetría útil, como credenciales y comandos, sin tener que pasar por los registros.

Para tener en cuenta

El éxito del engaño depende de su credibilidad. Los señuelos deben tener la apariencia y ser lo suficientemente funcionales como para facilitar la interacción de los atacantes. En este caso, los señuelos SSH lograron confundir al atacante para que revelara el servidor C2 de herramientas.



©2024 Zscaler, Inc. Todos los derechos reservados.



CASO PRÁCTICO 6

Ataques de fuerza bruta a una importante institución financiera

El incidente

Los señuelos perimetrales detectan varios intentos de fuerza bruta.

- Los ataques tienen origen en varias fuentes.
- Se realizan intentos contra señuelos con combinaciones de credenciales predeterminadas conocidas públicamente.
- Se identifica la explotación manual exhaustiva de aplicaciones web basada en marcas de tiempo utilizando BurpSuite y Nuclei Scanner.

Acciones de respuesta y contención

- Lista de bloqueo dinámica en el firewall para todas las fuentes que envían credenciales a través de la función de orquestación.
- No se identificaron las fuentes del ataque en ninguna fuente de inteligencia sobre amenazas hasta tres días después.

Estrategia del engaño

- Señuelos orientados a Internet que imitan aplicaciones de acceso remoto y otros servicios con vulnerabilidades conocidas y días cero.
- Servicio Threat Hunting gestionado

Resultado

- Se aprovechó la capacidad de bloquear varias fuentes en función de una táctica para limitar las consecuencias.

Para tener en cuenta

Los señuelos orientados a Internet de Zscaler generan una valiosa inteligencia de amenazas privadas que no es detectada por las fuentes tradicionales de inteligencia sobre amenazas y es una fuente confiable de advertencias tempranas de un ataque inminente.

©2024 Zscaler, Inc. Todos los derechos reservados.

CASO PRÁCTICO 7

Ataque dirigido operado por seres humanos en un hospital

El incidente

Se ha observado un comportamiento contra los señuelos similar al de PsExec, normalmente asociado al grupo APT.

- La fuente era el controlador de una máquina de rayos X.
- Se accedió al administrador de control de servicio a través de DCE/RPC en los señuelos para iniciar los servicios (comportamiento de PsExec).
- Escaneo de puertos para detectar movimiento lateral común en varios señuelos (135.445.3389)
- Se detectó software común de acceso remoto (RemCom RemoteAdmin).
- La investigación revela la presencia de herramientas como Mimikatz.

Estrategia del engaño

- Colocación estratégica de señuelos en segmentos que alojan equipos hospitalarios esenciales.
- Los señuelos de los extremos apuntan a otros señuelos.

Resultado

- Detección y contención oportunas de un ataque dirigido.

Para tener en cuenta

El engaño es eficaz para activos tales como equipos hospitalarios, dispositivos de IoT, sistemas de punto de venta, etc., donde no se pueden implementar controles tradicionales de detección de amenazas.



©2024 Zscaler, Inc. Todos los derechos reservados.



CASO PRÁCTICO 8

Propagación del ransomware MedusaLocker en un conglomerado empresarial

El incidente

Se activó una alerta sobre el cifrado de archivos señuelo compartidos.

- Más de 50 fuentes tuvieron acceso a archivos señuelo compartidos SMB.
- Los archivos señuelo fueron renombrados con la extensión “.ReadInstructions”.
- El nombre de usuario detectado era una credencial con privilegio.

Estrategia del engaño

- Implementación estratégica de archivos señuelo compartidos SMB en segmentos clave específicamente para uso en casos de ransomware.

Resultado

- El aislamiento rápido de los segmentos del servidor limitó la propagación de ransomware.

Para tener en cuenta

Un señuelo es mejor que ningún señuelo. Aunque no esté listo para una implementación a gran escala, una implementación limitada y estratégica será suficiente cuando sea importante.

©2024 Zscaler, Inc. Todos los derechos reservados.

CASO PRÁCTICO 9

Alerta temprana de un peligro inminente

El incidente

El uso de credenciales con privilegios en un señuelo activó una alerta en una organización de fabricación global.

- La fuente accedió a múltiples contenidos señuelo compartidos.
- El nombre de usuario de NTLM detectado activó la regla ThreatParse para identificar posibles cuentas con privilegios basadas en palabras clave como *adm*, *svc*, *bkp*.
- Se confirma que la cuenta en peligro es de un administrador de dominio.

Estrategia del engaño

- Implementación del engaño con muchas limitaciones. Se confió en Active Directory y los señuelos de los puntos finales para dirigir a los atacantes hacia los señuelos.
- Reglas personalizadas y alertas telefónicas para las interacciones con determinados señuelos.

Resultado

- Se detectó la amenaza una semana antes de que el FBI alertara al cliente sobre un inminente ataque de ransomware basándose en la información que recogieron de la “dark web”.

Para tener en cuenta

En ocasiones, las organizaciones deben trabajar dejando de lado ciertas limitaciones del entorno. A diferencia de los controles de detección tradicionales, que deben ser omnipresentes para ser eficaces, se puede usar un engaño muy limitado y aun así lograr el objetivo.



©2024 Zscaler, Inc. Todos los derechos reservados.



CASO PRÁCTICO 10

Detección de Shadow RDP en la empresa FMCG

El incidente

Se observaron errores de inicio de sesión de usuario señuelo.

- Varios errores de inicio de sesión de cuentas señuelo.
- Los registros de Windows capturados no revelaron la fuente.
- Se trabajó extensivamente con el cliente en RCA, lo que implicó el seguimiento del flujo de autenticación.
- Se descubrió que el sistema Azure tenía RDP abierto a Internet.

Estrategia del engaño

- Se creó uno de los usuarios señuelo de AD con un nombre disponible en un diccionario común.

Resultado

- Se reveló el primer caso de uso de la detección en su clase.
- Se identificó un error de configuración que podría tener consecuencias comerciales graves.
- Se aprovechó el aprendizaje para ampliar el caso de uso a otros clientes de servicios gestionados e identificar proactivamente 3 casos similares.

Para tener en cuenta

Dado que el engaño detecta ataques en función de la intención del atacante, en lugar de basarse en las firmas y la heurística, de vez en cuando se obtiene una detección eficaz de ataques totalmente desconocidos.

©2024 Zscaler, Inc. Todos los derechos reservados.

Cuando se trata de cazar, los señuelos no son nada nuevo. Pero en el mundo digital de hoy, los señuelos adquieren otra forma. Los ataques de trampas dinámicos, estratégicos y clandestinos no son solo una manera de mitigar las amenazas, sino también un medio para obtener inteligencia, que se agrega inmediatamente a la nube de seguridad de Zscaler.

¿Le interesa saber más sobre los señuelos como táctica de seguridad? Explore algunos de nuestros recursos aquí:
zscaler.com/mx/products/deception-technology

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zero Trust Exchange™ protege a miles de clientes contra ciberataques y pérdida de datos al conectar usuarios, dispositivos y aplicaciones de manera segura en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange, basado en SASE, es la plataforma de seguridad en la nube en línea más grande del mundo. Para obtener más información, visite www.zscaler.com/mx.

© 2024 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ y otras marcas registradas listadas en **zscaler.com/mx/legal/trademarks** son (i) marcas comerciales o marcas de servicio registradas o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y otros países. Cualquier otra marca comercial pertenece a sus respectivos propietarios.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San José, CA 95134 zscaler.com/mx