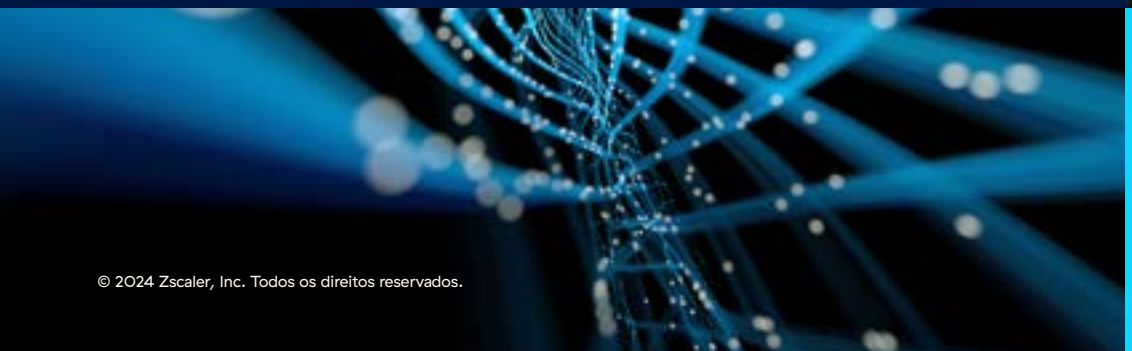
# Deception Em ação

As dez principais ameaças do mundo real capturadas pela Zscaler Deception





© 2024 Zscaler, Inc. Todos os direitos reservados.

# Defesa ativa baseada em deception contra ataques a alvos específicos

A deception é uma das estratégias mais eficazes para detectar os ataques de origem humana que geralmente conseguem ultrapassar defesas previsíveis. Seu objetivo é confundir as táticas do adversário e forçá-lo a cometer erros que acabam levando à sua detecção.

Nossa plataforma de deception é implementada com uma estratégia que prevê como o adversário pode se movimentar dentro de seu ambiente. Ela permite detectar ameaças que representam um grave perigo para as empresas em escala global.

Este documento examina alguns dos principais ataques detectados pela nossa rede global de deception.

## As dez principais detecções de criminosos do mundo real

01 APT norte-coreano

02 Táticas de ransomware operadas por seres humanos (pré-infecção)

03 Reconhecimento e escaneamento internos

04 Preenchimento de credenciais

05 Exploração do roteador MikroTik

06 Ataques de força bruta distribuídos

07 Comprometimento do controlador de máquinas de raios X

08 Disseminação do ransomware MedusaLocker

09 Alerta antecipado contra ransomware

10 RDP paralelo

© 2024 Zscaler, Inc. Todos os direitos reservados.

ESTUDO DE CASO 1

# Ataque de APT da Coreia do Norte a um grande conglomerado global

## A ocorrência

**O escaneamento da porta SMB da isca acusa uma detecção**

- Nome de usuário do NTLM capturado
- O contexto revelou que esse usuário tinha sido comprometido

**Triagem e investigação**

- Domínio C2 semelhante ao domínio legítimo
- Nossa investigação isolou duas DLLs sem assinaturas conhecidas
- As DLLs continham credenciais fixas e código loader para receber comandos adicionais
- Confirmação off-line da equipe sobre a tentativa de ataque da Coreia do Norte pelo grupo “Hidden Cobra”.

**Estratégia de deception**

- Foram identificadas as áreas críticas da infraestrutura com maior probabilidade de serem atacadas, e iscas foram plantadas nestes segmentos
- Suporte da Zscaler Threat Hunting para investigação e triagem do terminal

**Resultado**

- A Zscaler Deception foi a única solução que emitiu um alarme no ambiente

### Conclusões

Uma estratégia de deception sob medida para obter os resultados desejados dentro das limitações do ambiente é um dos fatores mais importantes para o sucesso da defesa ativa



© 2024 Zscaler, Inc. Todos os direitos reservados.



ESTUDO DE CASO 2

# Detecção pré-infecção de um operador de ransomware que visava um varejista

## A ocorrência

**Conta de serviço usada como isca acionada pelo Patient Zero**

- Um Active Directory escaneado pelo sistema atua como isca de propriedade do Service Principal Name (SPN) em 8 de maio de 2021

**Movimentação lateral para uma isca no SMB do Patient Zero**

- A autenticação do NTLM revelou comprometimento da conta SYSTEM em 13 de maio de 2021

**Propagação do ransomware via WinRM**

- Isca captura procura por portas abertas na porta 5985 em 10 de junho de 2021

**Ransomware implantado via WinRM em 13 de junho**

- Infelizmente, devido à falta de resposta em tempo hábil, o ransomware infectou vários servidores da rede

**Estratégia de deception**

- O Active Directory atua como isca para detectar o comprometimento de contas
- Iscas de rede em DC e DMZ para detectar movimentação lateral

**Resultado**

- A Zscaler Deception emitiu um alerta antecipado sobre um iminente ataque de ransomware um mês antes da ocorrência

### Conclusões

As iscas do Active Directory são uma das fontes mais confiáveis de avisos de infecção iminente durante um ataque de ransomware. As equipes de segurança devem priorizá-las para fins de investigação

© 2024 Zscaler, Inc. Todos os direitos reservados

ESTUDO DE CASO 3

# Reconhecimento e escaneamento interno em um grande banco

## A ocorrência

**O invasor consegue penetrar através de um roteador comprometido**

- Um roteador comprometido é a origem de extensa interação com iscas em diversas portas, incluindo SSH

**O invasor passa mais de seis horas executando centenas de comandos em três iscas do SSH**

- Login com root/root
- Comandos de consciência situacional
- Tentativa de compilar binários personalizados de scanner de rede
- Senhas roubadas de /etc/passwd + /etc/shadow
- Tentativa de usar a isca como pivô (bloqueada)
- Tentativa de farejar a rede usando TCPDump

**Estratégia de deception**

- Iscas de alta interação na rede que não apenas detectam adversários, mas também os envolvem por um tempo suficiente para revelar sua estratégia e intenção

**Resultado**

- O impacto foi evitado enquanto o invasor estava ocupado com a isca, permitindo ao cliente localizar e acessar o roteador

### Conclusões

Ataques feitos por mãos humanas avaliam a estratégia de defesa de seu alvo e evitam completamente os tradicionais controles de detecção. Neste caso, eles visavam um roteador — um dispositivo que normalmente não tem o EDR instalado. As equipes de segurança devem plantar iscas nestes dispositivos para detectar adversários sofisticados




© 2024 Zscaler, Inc. Todos os direitos reservados.



ESTUDO DE CASO 4

# Ataque de preenchimento de credenciais a um escritório de advocacia com clientes de alto perfil

## A ocorrência

**Alerta de preenchimento emitido no chamariz Citrix aberto para a internet**

- Mais de 200 credenciais de domínio comprometidas submetidas como isca
- Ataque originado da infraestrutura de um provedor russo de serviços de nuvem

**Ações de resposta e contenção**

- Lista de bloqueio dinâmico no firewall usando a capacidade de orquestração
- Tentativa de usar a isca como pivô (bloqueada)
- Tentativa de farejar a rede usando TCPDump

**Estratégia de deception**

- Aplicativos isca abertos para a internet são comumente atacados por adversários para validação de credenciais
- Serviço gerenciado de caça a ameaças

**Resultado**

- A Zscaler Deception evitou um ataque aos ativos de produção logo no início da cadeia de destruição

### Conclusões

As iscas abertas para a internet que imitam serviços e aplicativos de acesso remoto, com vulnerabilidades de dia zero e outros pontos fracos conhecidos, desviam os ataques antes de sua execução

© 2024 Zscaler, Inc. Todos os direitos reservados.

ESTUDO DE CASO 5

# Atividade de exploração do roteador MikroTik

## A ocorrência

**Alarme emitido em uma isca de MikroTik SSH personalizada**

- Iscas escaneadas nas portas conhecidas do MikroTik RouterOS, como 8291/tcp, 8728/tcp e 22/tcp (SSH)
- Interação com o serviço SSH personalizado do MikroTik usando uma ferramenta baseada em GO (SSH-2.0-Go)
- Força bruta registrada contra a credencial
- Múltiplos comandos de consciência situacional capturados
- Uma tarefa programada foi criada para procurar e executar a partir da internet

**Estratégia de deception**

- Iscas personalizadas para imitar componentes específicos usados ativamente no ambiente

**Resultado**

- Origem isolada
- Acesso antecipado a informações úteis de telemetria, como credenciais e comandos, sem ter que analisar todos os logs

### Conclusões

O bom funcionamento da deception depende de sua credibilidade. As iscas precisam parecer e ser funcionais o suficientes para incentivar a interação do invasor. Nesse caso, as iscas de SSH conseguiram confundir com sucesso o adversário, levando-o a revelar o servidor de ferramentas de comando e controle (C2)



© 2024 Zscaler, Inc. Todos os direitos reservados.



ESTUDO DE CASO 6

# Ataques de força bruta a uma grande instituição financeira

## A ocorrência

**Iscas de perímetro detectam várias tentativas de força bruta**

- Ataques provenientes de diversas origens
- Tentativas feitas contra iscas com combinações de credenciais padrão de conhecimento do público
- Abrangente exploração manual de aplicativos web identificada com base nos carimbos datadores usando BurpSuite e Nuclei Scanner

**Ações de resposta e contenção**

- Lista de bloqueio dinâmico no firewall para todas as fontes que apresentam credenciais através da função de orquestração
- As origens do ataque não tinham sido identificadas em nenhuma fonte de informações sobre ameaças — isso só aconteceu três dias depois

**Estratégia de deception**

- As iscas abertas para a internet imitam aplicativos de acesso remoto e outros serviços com vulnerabilidades de dia zero e outros pontos fracos conhecidos
- Serviço gerenciado de caça a ameaças

**Resultado**

- A capacidade de bloquear múltiplos pontos de origem com base em uma tática foi utilizada para limitar o impacto

### Conclusões

As iscas abertas para a internet da Zscaler geram valiosas informações privadas sobre ameaças que não são capturadas pelos tradicionais sistemas de informações sobre ameaças, e são uma fonte confiável de alerta antecipado sobre ataques iminentes

© 2024 Zscaler, Inc. Todos os direitos reservados.

ESTUDO DE CASO 7

# Ataque de operação humana direcionado a um hospital

## A ocorrência

**Comportamento semelhante ao PsExec, geralmente associado ao grupo APT, observado contra iscas**

- A origem era um controlador de máquina de raios X
- Acesso ao gerenciador de controle de serviços via DCE/RPC nas iscas para iniciar serviços (comportamento do PsExec)
- Varredura das portas de diversas iscas onde a movimentação lateral é mais comum (135.445.3389)
- Software comum de acesso remoto detectado (RemCom RemoteAdmin)
- A investigação revela a presença de ferramentas como Mimikatz

**Estratégia de deception**

- Colocação estratégica de iscas em segmentos que hospedam equipamentos hospitalares críticos
- Terminais chamarizes apontando para iscas

**Resultado**

- Detecção e contenção em tempo hábil de um ataque direcionado a alvos específicos

### Conclusões

A deception é eficaz para ativos como equipamentos hospitalares, dispositivos IoT, sistemas de PoS etc., onde os tradicionais controles de detecção de ameaças não podem ser implementados



© 2024 Zscaler, Inc. Todos os direitos reservados.



ESTUDO DE CASO 8

# Disseminação do ransomware MedusaLocker em um conglomerado

## A ocorrência

**Alarme acusa criptografia de compartilhamentos de arquivos na isca**

- Mais de 50 pontos de origem acessam compartilhamentos de SMB usados como isca
- Os arquivos isca foram renomeados com a extensão “.ReadInstructions”.
- O nome de usuário capturado era uma credencial privilegiada

**Estratégia de deception**

- Implementação estratégica de iscas de SMB Share em segmentos-chave especificamente para casos de uso de ransomware

**Resultado**

- O rápido isolamento de segmentos do servidor limitou a disseminação do ransomware

### Conclusões

Uma isca é melhor do que nenhuma. Mesmo que você não esteja pronto para uma implementação em larga escala, uma implementação limitada e estratégica vale seu peso em ouro quando chega a hora

© 2024 Zscaler, Inc. Todos os direitos reservados.

ESTUDO DE CASO 9

# Alerta antecipado de um comprometimento iminente

## A ocorrência

**O uso de credenciais privilegiadas em uma isca soou o alarme em uma organização manufatureira global**

- O ponto de origem acessou vários compartilhamentos na isca
- O nome de usuário do NTLM capturado aciona a regra ThreatParse para identificar contas potencialmente privilegiadas com base em palavras-chave como *adm*, *svc*, *bkp*
- A conta comprometida foi confirmada como sendo do administrador de domínio

### Estratégia de deception

- Deception acionada com muitas restrições. Active Directory e terminais chamarizes utilizados para conduzir o adversário até as iscas
- Regras personalizadas e alertas telefônicos para sinalizar interações com iscas específicas

### Resultado

- Ameaça detectada uma semana antes do FBI alertar o cliente sobre um iminente ataque de ransomware com base em informações obtidas na dark web

### Conclusões

Às vezes as empresas têm que contornar certas restrições do ambiente. Ao contrário dos controles de detecção tradicionais, que precisam ser difundidos para serem eficazes, você pode ser muito específico com a deception e ainda assim atingir o objetivo



© 2024 Zscaler, Inc. Todos os direitos reservados.



ESTUDO DE CASO 10

# Detecção de Sombra RDP na empresa FMCG

## A ocorrência

**Falhas no logon de um usuário isca observadas**

- Múltiplas falhas de logon com contas isca
- Os logs do Windows capturados não revelaram a fonte
- Extenso trabalho com o cliente no RCA, que envolveu o rastreamento do fluxo de autenticação
- Sistema Azure descoberto com RDP aberto para a internet

**Estratégia de deception**

- Um dos usuários da isca AD foi criado com um nome disponível em um dicionário comum

**Resultado**

- Um inédito caso de uso de detecção foi revelado
- Foi identificado um erro de configuração que poderia ter causado sérios prejuízos para a empresa
- Esse aprendizado serviu para estender o caso de uso a outros clientes de serviços gerenciados, e acabou ajudando a identificar proativamente três ocorrências similares

### Conclusões

Como o deception detecta ataques com base na intenção do adversário, em vez de assinaturas e heurísticas, ele resulta na detecção eficaz de ameaças desconhecidas de tempos em tempos

© 2024 Zscaler, Inc. Todos os direitos reservados.

Na guerra, as iscas e armadilhas não são novidade. Mas no mundo digital de hoje, elas assumem uma forma diferente. Dinâmicas, estratégicas e secretas, as armadilhas para capturar ataques não são apenas uma forma de bloquear ameaças, mas também um meio de obter inteligência — que é imediatamente acrescentada à nuvem de segurança da Zscaler.

Quer saber mais sobre iscas como tática de segurança? Explore alguns dos nossos recursos aqui: zscaler.com/br/products/deception-technology

**Sobre a Zscaler**
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que os clientes tenham mais agilidade, eficiência, resiliência e proteção. A Zscaler Zero Trust Exchange™ protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SASE é a maior plataforma de segurança integrada na nuvem do mundo. Para saber mais, visite www.zscaler.com/br.

©2024 Zscaler, Inc. Todos os direitos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ e outras marcas registradas listadas em **zscaler.com/br/legal/trademarks** são (i) marcas registradas ou marcas de serviço ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Quaisquer outras marcas registradas são de propriedade de seus respectivos detentores.

+1 408.533.0288 Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134 zscaler.com/br