FIREEYE™

FICHA TÉCNICA

Operações Red Team (Red Team Operations, RTO)

Teste sua capacidade de proteger seus ativos mais fundamentais de um ataque direcionado real

VANTAGENS

- Saiba se seus dados críticos estão correndo risco e com que facilidade eles podem ser obtidos por alguém malicioso
- Avalie a segurança do seu ambiente contra um atacante real e determinado
- Teste a capacidade da sua equipe interna de segurança de prevenir, detectar e responder a incidentes em um ambiente controlado e realista
- Identifique e corrija vulnerabilidades complexas de segurança antes que um atacante as explore
- Obtenha recomendações e análise de risco com base em fatos para melhorar a segurança

Por que escolher a Mandiant?
A Mandiant, uma empresa FireEye, tem estado na linha de frente da inteligência em segurança cibernética e ameaças cibernéticas desde 2004. Nossos responsáveis pela resposta a incidentes estiveram nas linhas de frente das violações mais complexas do mundo. Temos um profundo conhecimento de agentes de ameaça existentes e emergentes, bem como de suas ferramentas, táticas e procedimentos, sempre em constante mudança.

Visão geral do serviço
O trabalho da Operações Red Team consiste em um cenário de ataque realista e sem limites no seu ambiente. A equipe Red Team Mandiant utiliza métodos não destrutivos necessários para atingir um conjunto de objetivos definidos de comum acordo, simulando o comportamento de um atacante. A Red Team imita bem os métodos de ataque ativos e furtivos de um atacante real com o uso de TTPs vistos em episódios de resposta a incidentes recentes e reais. Isso ajuda a avaliar a capacidade da sua equipe de segurança de detectar e responder a um cenário de ataque ativo.

Exemplos de objetivos		
Roubar e-mails de executivos ou de desenvolvedores	Invadir um ambiente segmentado que contenha dados confidenciais ou críticos para os negócios	Assumir controle sobre um dispositivo automatizado, como um dispositivo IoT, um dispositivo médico ou um dispositivo de manufatura

Metodologia
As Operações Red Team começam com a determinação conjunta de se a Red Team tem ou não conhecimento do seu ambiente. A Mandiant aplica sua experiência no setor para identificar objetivos que representam riscos importantes para suas funções do core business.

As funções das Operações Red Team seguem as fases do ciclo de vida do ataque.

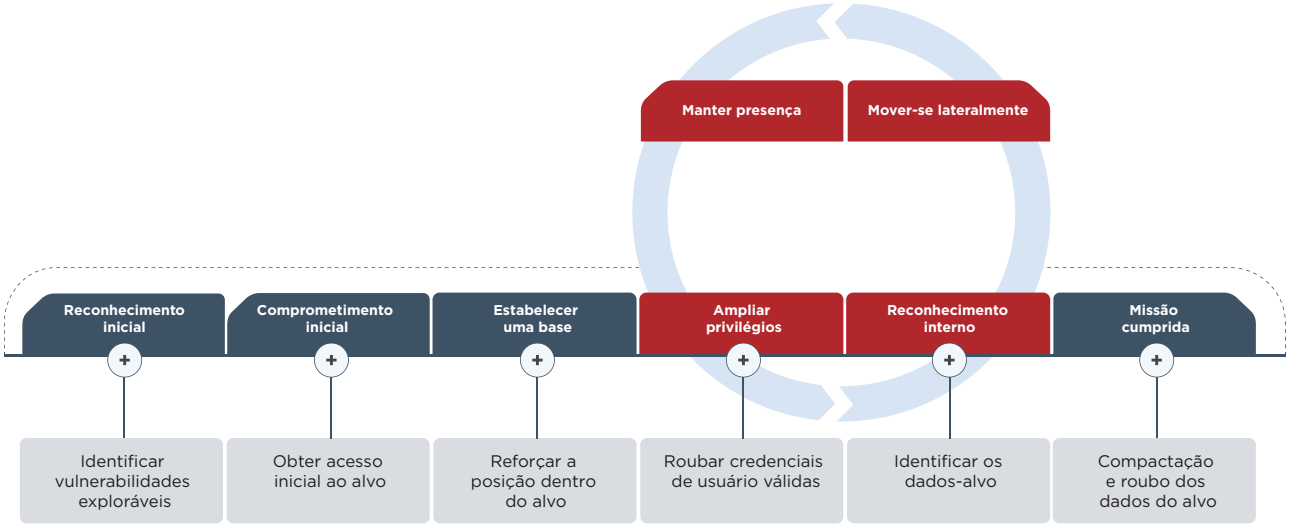

Figura 1. Ciclo de vida do ataque.

Assim que os objetivos são definidos, a Red Team começa com o reconhecimento inicial. A Mandiant utiliza uma combinação de repositórios de inteligência próprios, bem como técnicas e ferramentas de inteligência de código aberto (OSINT) para fazer o reconhecimento do ambiente alvo.

A Mandiant tenta ganhar acesso inicial ao ambiente alvo por meio da exploração de vulnerabilidades ou com a realização de um ataque de engenharia social. A Mandiant utiliza técnicas empregadas por atacantes reais para obter acesso privilegiado a esses sistemas.

Depois de obtido esse acesso, a Red Team tenta ampliar privilégios para estabelecer e manter persistência dentro do ambiente com a implementação de uma infraestrutura de comando e controle, tal como um atacante faria.

Depois que a persistência e os sistemas de controle e comando são estabelecidos dentro do ambiente, a Red Team tenta atingir seus objetivos através de quaisquer meios não disruptivos necessários.

Por que escolher as Operações Red Team

As Operações Red Team são recomendadas para organizações que desejam:

- *Testar capacidades de detecção e resposta.* As equipes de segurança se preparam para incidentes reais, mas você precisa confirmar se elas são capazes de responder corretamente — sem risco real.
- *Aumentar a conscientização e mostrar impacto.* A Red Team Mandiant comporta-se como atacantes reais que trabalham para comprometer seu ambiente na Internet com o uso de informações disponíveis apenas na Internet. As atuações bem-sucedidas da Red Team podem ajudar a justificar maiores orçamentos de segurança e identificar falhas que exigem mais investimento.

O QUE VOCÊ RECEBE

- Resumo para gerência de nível executivo e sênior
- Detalhes técnicos com informações passo a passo que permitam reproduzir nossas descobertas
- Análise de risco com base em fatos para que você se certifique de que as descobertas críticas são relevantes para o seu ambiente
- Recomendações táticas para aperfeiçoamento imediato
- Recomendações estratégicas para aperfeiçoamento a longo prazo
- Experiência inestimável na resposta a incidentes da vida real, sem a pressão de uma possível violação que apareça nas manchetes

Para saber mais sobre a FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Sobre a FireEye, Inc.

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência de ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos.