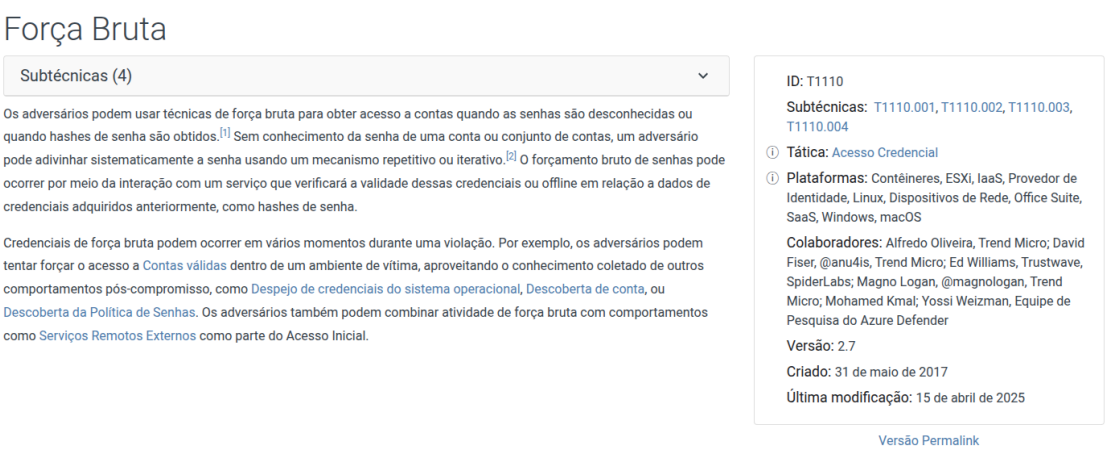
Figura 14 - Técnica T1110 (MITRE ATT&CK).



Força Bruta

Subtécnicas (4)

Os adversários podem usar técnicas de força bruta para obter acesso a contas quando as senhas são desconhecidas ou quando hashes de senha são obtidos.[1] Sem conhecimento da senha de uma conta ou conjunto de contas, um adversário pode adivinhar sistematicamente a senha usando um mecanismo repetitivo ou iterativo.[2] O forçamento bruto de senhas pode ocorrer por meio da interação com um serviço que verificará a validade dessas credenciais ou offline em relação a dados de credenciais adquiridos anteriormente, como hashes de senha.

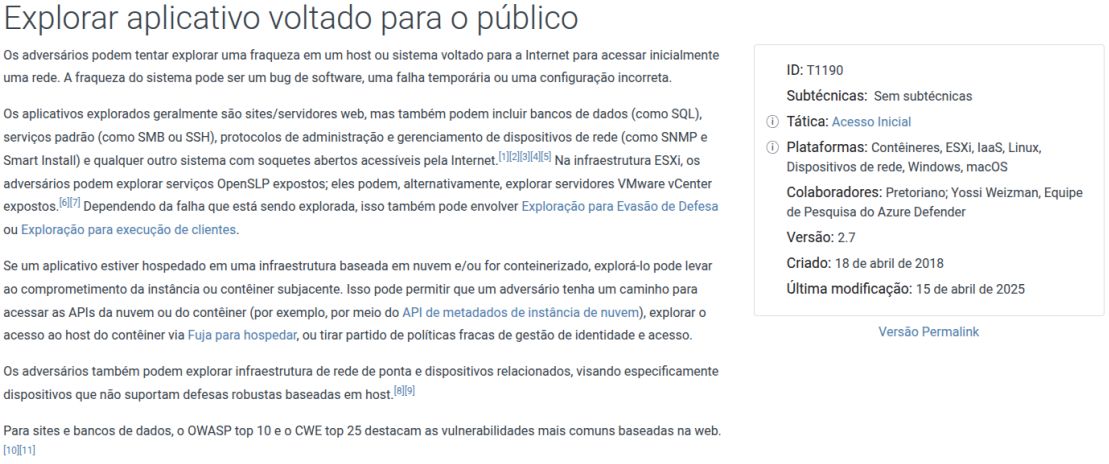
Credenciais de força bruta podem ocorrer em vários momentos durante uma violação. Por exemplo, os adversários podem tentar forçar o acesso a Contas válidas dentro de um ambiente de vítima, aproveitando o conhecimento coletado de outros comportamentos pós-compromisso, como Despejo de credenciais do sistema operacional, Descoberta de conta, ou Descoberta da Política de Senhas. Os adversários também podem combinar atividade de força bruta com comportamentos como Serviços Remotos Externos como parte do Acesso Inicial.

ID: T1110
Subtécnicas: T1110.001, T1110.002, T1110.003, T1110.004
Tática: Acesso Credencial
Plataformas: Contêineres, ESXi, IaaS, Provedor de Identidade, Linux, Dispositivos de Rede, Office Suite, SaaS, Windows, macOS
Colaboradores: Alfredo Oliveira, Trend Micro; David Fiser, @anu4is, Trend Micro; Ed Williams, Trustwave, SpiderLabs; Magno Logan, @magnologan, Trend Micro; Mohamed Kmal; Yossi Weizman, Equipe de Pesquisa do Azure Defender
Versão: 2.7
Criado: 31 de maio de 2017
Última modificação: 15 de abril de 2025

Versão Permalink

Fonte: MITRE ATT&CK, 2025.

Figura 15 - Técnica T1190 (MITRE ATT&CK).



Explorar aplicativo voltado para o público

Os adversários podem tentar explorar uma fraqueza em um host ou sistema voltado para a Internet para acessar inicialmente uma rede. A fraqueza do sistema pode ser um bug de software, uma falha temporária ou uma configuração incorreta.

Os aplicativos explorados geralmente são sites/servidores web, mas também podem incluir bancos de dados (como SQL), serviços padrão (como SMB ou SSH), protocolos de administração e gerenciamento de dispositivos de rede (como SNMP e Smart Install) e qualquer outro sistema com soquetes abertos acessíveis pela Internet.[1][2][3][4][5] Na infraestrutura ESXi, os adversários podem explorar serviços OpenSLP expostos; eles podem, alternativamente, explorar servidores VMware vCenter expostos.[6][7] Dependendo da falha que está sendo explorada, isso também pode envolver Exploração para Evasão de Defesa ou Exploração para execução de clientes.

Se um aplicativo estiver hospedado em uma infraestrutura baseada em nuvem e/ou for conteinerizado, explorá-lo pode levar ao comprometimento da instância ou contêiner subjacente. Isso pode permitir que um adversário tenha um caminho para acessar as APIs da nuvem ou do contêiner (por exemplo, por meio do API de metadados de instância de nuvem), explorar o acesso ao host do contêiner via Fuja para hospedar, ou tirar partido de políticas fracas de gestão de identidade e acesso.

Os adversários também podem explorar infraestrutura de rede de ponta e dispositivos relacionados, visando especificamente dispositivos que não suportam defesas robustas baseadas em host.[8][9]

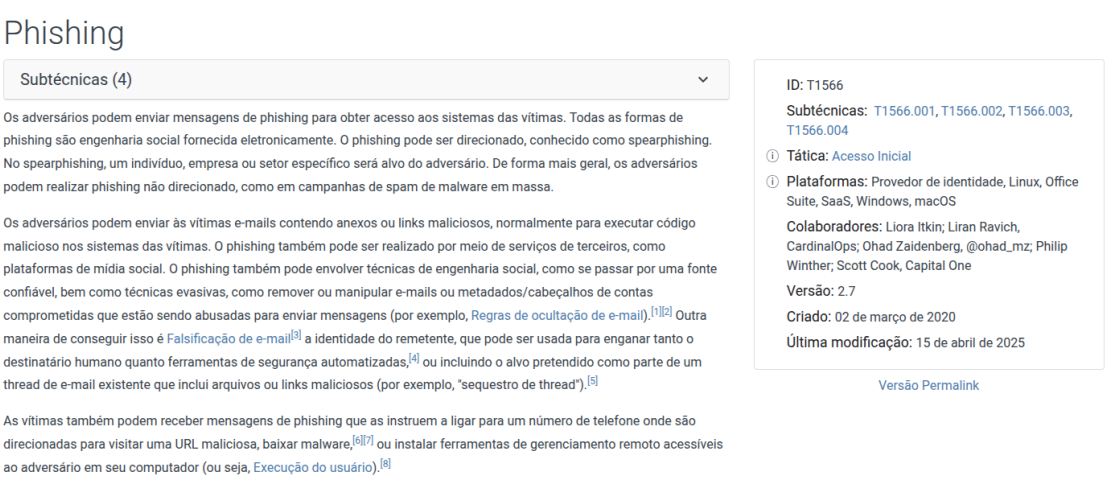
Para sites e bancos de dados, o OWASP top 10 e o CWE top 25 destacam as vulnerabilidades mais comuns baseadas na web.[10][11]

ID: T1190
Subtécnicas: Sem subtécnicas
Tática: Acesso Inicial
Plataformas: Contêineres, ESXi, IaaS, Linux, Dispositivos de rede, Windows, macOS
Colaboradores: Pretoriano; Yossi Weizman, Equipe de Pesquisa do Azure Defender
Versão: 2.7
Criado: 18 de abril de 2018
Última modificação: 15 de abril de 2025

Versão Permalink

Fonte: MITRE ATT&CK, 2025.

Figura 16 -Técnica T1566 (MITRE ATT&CK).



Phishing

Subtécnicas (4)

Os adversários podem enviar mensagens de phishing para obter acesso aos sistemas das vítimas. Todas as formas de phishing são engenharia social fornecida eletronicamente. O phishing pode ser direcionado, conhecido como spearphishing. No spearphishing, um indivíduo, empresa ou setor específico será alvo do adversário. De forma mais geral, os adversários podem realizar phishing não direcionado, como em campanhas de spam de malware em massa.

Os adversários podem enviar às vítimas e-mails contendo anexos ou links maliciosos, normalmente para executar código malicioso nos sistemas das vítimas. O phishing também pode ser realizado por meio de serviços de terceiros, como plataformas de mídia social. O phishing também pode envolver técnicas de engenharia social, como se passar por uma fonte confiável, bem como técnicas evasivas, como remover ou manipular e-mails ou metadados/cabeçalhos de contas comprometidas que estão sendo abusadas para enviar mensagens (por exemplo, Regras de ocultação de e-mail).[1][2] Outra maneira de conseguir isso é Falsificação de e-mail[3] a identidade do remetente, que pode ser usada para enganar tanto o destinatário humano quanto ferramentas de segurança automatizadas,[4] ou incluindo o alvo pretendido como parte de um thread de e-mail existente que inclui arquivos ou links maliciosos (por exemplo, "sequestro de thread").[5]

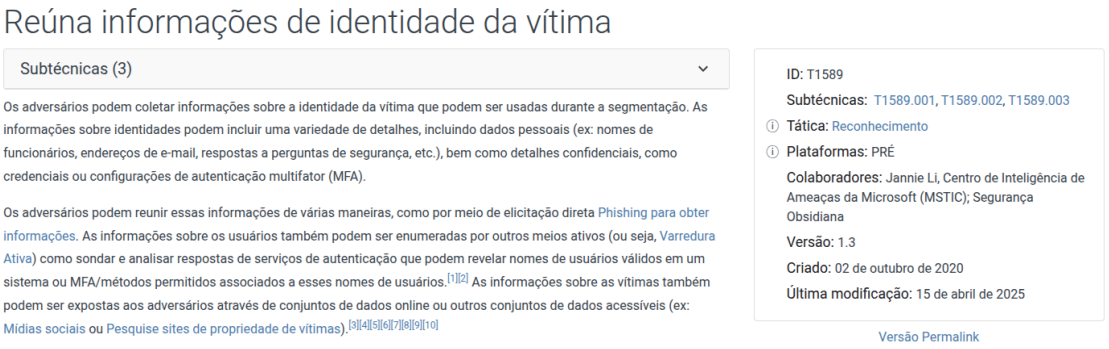
As vítimas também podem receber mensagens de phishing que as instruem a ligar para um número de telefone onde são direcionadas para visitar uma URL maliciosa, baixar malware,[6][7] ou instalar ferramentas de gerenciamento remoto acessíveis ao adversário em seu computador (ou seja, Execução do usuário).[8]

ID: T1566
Subtécnicas: T1566.001, T1566.002, T1566.003, T1566.004
Tática: Acesso Inicial
Plataformas: Provedor de identidade, Linux, Office Suite, SaaS, Windows, macOS
Colaboradores: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad_mz; Philip Winther; Scott Cook, Capital One
Versão: 2.7
Criado: 02 de março de 2020
Última modificação: 15 de abril de 2025

Versão Permalink

Fonte: MITRE ATT&CK, 2025.

Figura 17 - Técnica T1589 (MITRE ATT&CK).



Reúna informações de identidade da vítima

Subtécnicas (3)

Os adversários podem coletar informações sobre a identidade da vítima que podem ser usadas durante a segmentação. As informações sobre identidades podem incluir uma variedade de detalhes, incluindo dados pessoais (ex: nomes de funcionários, endereços de e-mail, respostas a perguntas de segurança, etc.), bem como detalhes confidenciais, como credenciais ou configurações de autenticação multifator (MFA).

Os adversários podem reunir essas informações de várias maneiras, como por meio de elicitação direta Phishing para obter informações. As informações sobre os usuários também podem ser enumeradas por outros meios ativos (ou seja, Varredura Ativa) como sondar e analisar respostas de serviços de autenticação que podem revelar nomes de usuários válidos em um sistema ou MFA/métodos permitidos associados a esses nomes de usuários.[1][2] As informações sobre as vítimas também podem ser expostas aos adversários através de conjuntos de dados online ou outros conjuntos de dados acessíveis (ex: Mídias sociais ou Pesquise sites de propriedade de vítimas).[3][4][5][6][7][8][9][10]

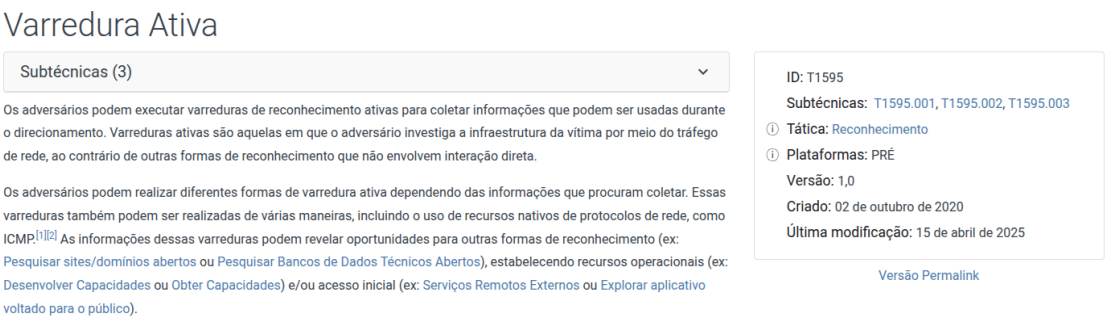
A recolha desta informação pode revelar oportunidades para outras formas de reconhecimento (ex: Pesquisar sites/domínios abertos ou Phishing para obter informações), estabelecendo recursos operacionais (ex: Contas de compromisso) e/ou acesso inicial (ex: Phishing ou Contas válidas).

ID: T1589
Subtécnicas: T1589.001, T1589.002, T1589.003
Tática: Reconhecimento
Plataformas: PRÉ
Colaboradores: Jannie Li, Centro de Inteligência de Ameaças da Microsoft (MSTIC); Segurança Obsidiana
Versão: 1.3
Criado: 02 de outubro de 2020
Última modificação: 15 de abril de 2025

Versão Permalink

Fonte: MITRE ATT&CK, 2025.

Figura 18 - Técnica T1595 (MITRE ATT&CK).



Varredura Ativa

Subtécnicas (3)

Os adversários podem executar varreduras de reconhecimento ativas para coletar informações que podem ser usadas durante o direcionamento. Varreduras ativas são aquelas em que o adversário investiga a infraestrutura da vítima por meio do tráfego de rede, ao contrário de outras formas de reconhecimento que não envolvem interação direta.

Os adversários podem realizar diferentes formas de varredura ativa dependendo das informações que procuram coletar. Essas varreduras também podem ser realizadas de várias maneiras, incluindo o uso de recursos nativos de protocolos de rede, como ICMP.[1][2] As informações dessas varreduras podem revelar oportunidades para outras formas de reconhecimento (ex: Pesquisar sites/domínios abertos ou Pesquisar Bancos de Dados Técnicos Abertos), estabelecendo recursos operacionais (ex: Desenvolver Capacidades ou Obter Capacidades) e/ou acesso inicial (ex: Serviços Remotos Externos ou Explorar aplicativo voltado para o público).

ID: T1595
Subtécnicas: T1595.001, T1595.002, T1595.003
Tática: Reconhecimento
Plataformas: PRÉ
Versão: 1,0
Criado: 02 de outubro de 2020
Última modificação: 15 de abril de 2025

Versão Permalink

Fonte: MITRE ATT&CK, 2025.