1.Indicadores de comprometimento

A segurança da informação exige vigilância constante para identificar sinais de invasão ou comprometimento de sistemas. Esses sinais são chamados de **Indicadores de Comprometimento** (IOC - Indicators of Compromise), **que revelam a possibilidade de um ataque cibernético em andamento ou já ocorrido**.

Algumas evidências comuns de comprometimento incluem **tráfego de rede incomum**, especialmente transferências massivas de dados para locais desconhecidos, e **modificações inesperadas em arquivos**, detectáveis pela alteração de seus valores de hash. Outro sinal de alerta é o **aumento de acessos internacionais** em uma rede normalmente restrita a um país específico, o que pode indicar a presença de um invasor remoto. Além disso, alterações nos registros DNS podem indicar uma tentativa de redirecionamento de tráfego para servidores maliciosos.

O bloqueio inesperado de contas de usuários pode ser um forte indicador de um ataque em curso. Esse bloqueio pode ocorrer devido a **múltiplas tentativas de login falhas**, sugerindo um ataque de força bruta. Em alguns casos, um invasor pode forçar o bloqueio da conta propositalmente para, em seguida, entrar em contato com o suporte técnico e solicitar a redefinição da senha, alegando ser o usuário legítimo. Essa técnica explora falhas nos processos de recuperação de credenciais.

Logins simultâneos de um mesmo usuário em locais geograficamente distantes representam um forte indicador de comprometimento. Se um funcionário acessa a rede de uma cidade e, poucos minutos depois, um segundo login ocorre de outro continente, isso sugere que credenciais foram roubadas e estão sendo utilizadas indevidamente. Essa tática é conhecida como **"impossible travel"**, pois desafia as leis da física.

Atacantes que conseguem acesso a um sistema frequentemente tentam manter sua presença por longos períodos. Para evitar a detecção, muitos **desativam atualizações de segurança e antivírus**, impedindo a aplicação de patches que corrigiram a vulnerabilidade explorada. Caso um sistema deixe de receber atualizações inesperadamente ou não consiga acessar sites de segurança, há uma forte chance de que tenha sido comprometido.

Outro indicador importante é o **consumo anormal de recursos**, como uso excessivo de CPU, memória ou largura de banda. Isso pode indicar que um invasor está extraindo grandes quantidades de dados da rede ou executando operações pesadas, como mineração de criptomoedas sem autorização.

Ransomware e vazamento de dados são consequências diretas de ataques bem-sucedidos. No caso de ransomware, os arquivos do sistema são subitamente criptografados, impedindo o acesso legítimo e exigindo um pagamento para recuperação. Além disso, muitos ataques modernos combinam ransomware com

extorsão dupla, onde os invasores copiam dados sensíveis antes de criptografá-los e ameaçam divulgá-los caso o resgate não seja pago.

Os logs do sistema são uma ferramenta essencial para detectar atividades suspeitas. Registros de acessos em horários incomuns, tentativas de login falhas e transferências de arquivos não autorizadas são sinais claros de uma possível invasão. Entretanto, atacantes experientes frequentemente **apagam ou alteram logs** para esconder suas ações, tornando essencial a configuração de alertas para detectar a exclusão ou manipulação desses registros.

O vazamento de informações confidenciais na internet é o sinal definitivo de um comprometimento grave. Se dados de uma organização aparecem em fóruns ou sites de compartilhamento, é provável que tenham sido extraídos por invasores. Esse tipo de vazamento pode resultar de ataques diretos à infraestrutura da empresa ou ser uma consequência de ransomware não pago.

A detecção precoce de indicadores de comprometimento é essencial para minimizar danos. Ferramentas de monitoramento de segurança, análise de tráfego e auditoria de logs ajudam a identificar e responder rapidamente a ameaças. Além disso, boas práticas, como autenticação multifator e monitoramento contínuo, fortalecem a defesa contra invasões e vazamentos de dados.