Ataques Cibernéticos Recentes

Ataque 1 — MOVEit Transfer (Grupo Cl0p)

Data do ataque

O ataque ocorreu em maio e junho de 2023.

Tipo de ataque

Foi um ataque de exfiltração de dados, que significa que os criminosos conseguiram roubar arquivos importantes das empresas afetadas. Além disso, o ataque tinha extorsão, ou seja, os criminosos ameaçavam divulgar ou vender os dados roubados se não recebessem pagamento.

Como aconteceu

O alvo foi um programa chamado MOVEit Transfer, que serve para empresas transferirem arquivos entre computadores de forma segura. Porém, havia uma falha escondida no software que permitia que qualquer pessoa mal-intencionada enviasse comandos que o sistema aceitaria como legítimos.
Os criminosos criaram um web shell, que é como se fosse uma porta secreta dentro do software. Essa porta permitiu que eles:

1. Entrassem no sistema sem precisar de senha.
2. Visualizassem todos os arquivos armazenados.
3. Copiassem os dados para fora da empresa (exfiltração).
4. Criassem contas com privilégios de administrador para manter acesso contínuo.

Para controlar a porta secreta, eles usavam algo parecido com um código de segurança secreto dentro das mensagens enviadas ao servidor. Isso garantia que só eles conseguissem usar o web shell.

Vulnerabilidade explorada

A falha explorada se chama CVE-2023-34362. É uma SQL Injection, ou seja, uma forma de enganar o software para que ele execute comandos que não deveria.
Imagine que você tem um formulário de login, e ao invés de digitar seu usuário normalmente, alguém digita um comando secreto. Se o software não tiver proteção, ele pode executar esse comando e dar ao invasor acesso a tudo.

Impactos

- Mais de 2.700 empresas foram afetadas.
- Documentos e dados sensíveis de clientes, funcionários e parceiros foram roubados.
- As empresas ficaram em risco de terem suas informações divulgadas publicamente ou vendidas.
- Mesmo sem criptografar arquivos, os criminosos conseguiram paralisar operações, porque os dados importantes estavam comprometidos.

Proteção que poderia ter evitado o ataque

1. Atualização do software: corrigir a falha assim que a empresa forneceu a atualização.

2. Validação de entrada: o software deveria verificar cada informação recebida para garantir que não fosse um comando malicioso.
3. Monitoramento constante: sistemas que detectam atividades suspeitas, como acessos não autorizados ou movimentação de arquivos em grande quantidade.
4. Segregação de rede: separar sistemas críticos em uma rede protegida, para que mesmo que um software seja comprometido, o invasor não consiga acessar tudo.
5. Backups isolados: manter cópias de segurança em local seguro, que não possam ser acessadas diretamente pelo software comprometido.

Ataque 2 — VMware ESXi (BlackByte)

Data do ataque

O ataque aconteceu em 2024.

Tipo de ataque

Foi um ransomware direcionado a servidores de máquinas virtuais. Ransomware é um tipo de malware que bloqueia os arquivos da vítima (ou sistemas inteiros) e exige pagamento para liberar o acesso.

Como aconteceu

O alvo foi o VMware ESXi, que é usado para criar e gerenciar máquinas virtuais. Máquinas virtuais são computadores "dentro de outro computador", que permitem que várias operações rodem ao mesmo tempo no mesmo hardware físico.
O grupo BlackByte usou uma falha chamada CVE-2024-37085, que permitia burlar a autenticação do sistema. Ou seja, eles conseguiram entrar como se fossem administradores sem precisar da senha correta.

Depois de entrar, eles fizeram o seguinte:

1. Criaram um grupo de administradores falso chamado ESXi Admins. Esse grupo dá permissões máximas dentro do VMware.
2. Removeram ou desativaram ferramentas de segurança que poderiam detectar o ataque.
3. Instalaram drivers (programas que controlam hardware) vulneráveis para manter acesso contínuo.
4. Iniciaram a criptografia de todas as máquinas virtuais, tornando inacessíveis os sistemas e dados dentro delas.

Vulnerabilidade explorada

A falha, CVE-2024-37085, é um authentication bypass.
Isso significa que o sistema aceita um usuário como autorizado mesmo sem confirmar a senha ou autorização correta. Para leigos: é como se alguém entrasse numa sala trancada sem ter a chave, porque a porta tinha um defeito invisível.

Impactos

- Controle total dos hosts ESXi comprometidos, ou seja, o atacante podia bloquear e apagar máquinas virtuais inteiras.

- Impacto em sistemas críticos: bancos de dados, sistemas de produção e aplicações internas ficaram inacessíveis.
- Dificuldade de recuperação: mesmo com backups, os atacantes poderiam ter destruído ou corrompido dados de restauração.
- Alto risco financeiro e operacional, já que muitas empresas dependem dessas máquinas virtuais para funcionar.

Proteção que poderia ter evitado o ataque

1. Aplicar patches imediatamente: corrigir a vulnerabilidade assim que a atualização foi disponibilizada.
2. Controle de acesso: apenas usuários confiáveis deveriam poder criar grupos administrativos.
3. Monitoramento do Active Directory: registrar e verificar qualquer alteração em grupos críticos.
4. Segmentação de rede: isolar servidores críticos, de modo que mesmo com acesso, o atacante não consiga se mover livremente.
5. Ferramentas de segurança reforçadas: manter EDR/antivírus funcionando e monitorando alterações de drivers suspeitos.
6. Backups isolados: para restaurar máquinas virtuais sem depender de sistemas comprometidos.

Comparação simplificada

- MOVEit: foco em roubo de dados e exfiltração, via falha web.
- VMware ESXi: foco em bloqueio e destruição de sistemas críticos, via falha de autenticação e controle de máquinas virtuais.
- Ambos mostram que atualizações e monitoramento constante são fundamentais, mas cada ataque exige técnicas específicas de prevenção.

Gustavo Jaccon Franquini

RA: 825150548