Resposta a Incidente Ransomware (1)

- 1 . Fase Inicial: Ataque de Força Bruta
- 4. Execução do Ataque
- 3. Comprometimento do Servidor de Backup
- 5. Exfiltração de Dados
- 2.Escalada de Privilégios
- Conclusões e Ações Estratégicas
- Sobre

Resposta a Incidente Ransomware (1)

1. 1 . Fase Inicial: Ataque de Força Bruta

1.1. Um ataque de força bruta foi realizado contra o portal VPN.

1.2. Foram usadas listas de e-mails padrão ou vazadas, comuns na Dark Web.

1.3. O atacante obteve acesso explorando senhas antigas, sem rodízio periódico.

1.3.1. Exploração envolvida

1.3.1.1. Falta de política de senhas fortes e rotativas

1.3.1.1.1. Mitigação recomendada

1.3.1.1.1.1. Implementar autenticação multifator (MFA) no acesso ao portal VPN

1.3.1.1.1.2. Estabelecer política de rodízio e complexidade de senhas

1.3.1.1.1.3. Monitorar continuamente acessos externos e limitar a exposição de serviços sensíveis

2. 4. Execução do Ataque

2.1. Foi iniciado o processo de criptografia de arquivos e máquinas virtuais.

2.2. O malware usado escondia a execução como variável de sessão e rodava como serviço, permitindo retomada após reinicialização

2.3. Foi realizada uma varredura na rede para identificar mais alvos.

2.3.1. Exploração envolvida

2.3.1.1. Falta de proteção contra execução de código malicioso

2.3.1.2. Rede mal segmentada permitindo varredura lateral.

2.3.1.2.1. Mitigação recomendada

2.3.1.2.1.1. Usar ferramentas de segurança como EDR/XDR para detecção e resposta rápida a ameaças

2.3.1.2.1.2. Segmentar a rede para dificultar movimentações laterais do invasor

2.3.1.2.1.3. Configurar bloqueios em firewalls para evitar exploração de portas vulneráveis.

3. 3. Comprometimento do Servidor de Backup

3.1. O invasor criou uma conta disfarçada de administrador de backup.

3.2. Instalou software para recuperar credenciais e obteve acesso irrestrito ao cluster VMware

3.3. Configurou acesso remoto secundário com ferramentas como AnyDesk (Backdoor)

3.4. Instalou certificados para criptografia de arquivos e máquinas virtuais e iniciou o ataque

3.4.1. Exploração envolvida

3.4.1.1. Gestão inadequada de contas administrativas

3.4.1.2. Uso de software de recuperação de credenciais e falta de monitoramento de alterações nos certificados digitais.

3.4.1.2.1. Mitigação recomenda

3.4.1.2.1.1. Implementar controle rigoroso sobre criação e uso de contas administrativas

3.4.1.2.1.2. Configurar alertas automáticos para alterações de certificados digitais e softwares instalados

3.4.1.2.1.3. Auditar e proteger backups com autenticação adicional e isolamento físico ou lógico

4. 5. Exfiltração de Dados

4.1. Transferência de arquivos criptografados para servidores externos em diversos países

4.2. Uso de conexões SSH e protocolo SMB para mover dados sensíveis.

4.2.1. Exploração envolvida

4.2.1.1. Falta de controle e monitoramento de transferências de dados externos

4.2.1.1.1. Mitigação recomendada

4.2.1.1.1.1. Monitorar e controlar fluxos de dados externos usando firewalls e DLP (Data Loss Prevention).

4.2.1.1.1.2. Restringir o uso de protocolos como SSH e SMB apenas para aplicações autorizadas.

5. 2.Escalada de Privilégios

5.1. O atacante usou credenciais válidas para acessar o Controlador de Domínio

5.2. Explorou vulnerabilidades conhecidas em versões desatualizadas do sistema

5.3. Obteve privilégios de administrador na rede

5.3.1. Exploração envolvida

5.3.1.1. Vulnerabilidade no Controlador de Domínio não corrigida (falta de patches)

5.3.1.1.1. Mitigação recomendada

5.3.1.1.1.1. Atualizar e corrigir regularmente os sistemas críticos

5.3.1.1.1.2. Implementar segmentação de rede para minimizar impactos em caso de comprometimento

5.3.1.1.1.3. Monitorar logs de segurança para identificar atividades anômalas

6. Sobre

6.1. Alex De Boni alex@supryx.com.br supryx.com.br 51 9 9917 0222

6.2. Há 25 anos trazendo soluções em Tecnologia e Cybersegurança.

7. Conclusões e Ações Estratégicas

7.1. Segmentação da rede para limitar a superfície de ataque

7.2. Atualização regular de sistemas e dispositivos vulneráveis.

7.3. Implementação de autenticação multifator (MFA).

7.4. Adoção de ferramentas de segurança como EDR/XDR e DLP

7.5. Treinamento e conscientização dos usuários sobre segurança digital

7.6. Criação e teste de um Plano de Resposta a Incidentes (DRP).