Ataques Cibernéticos

Disciplina: Sistemas computacionais e segurança

Aluno: João Pedro Martins Carvalho

Aluno: João Pedro Martins Carvalho

Sumário

Aluno: João Pedro Martins Carvalho

Ataque 1 — WannaCry (2017)

1. Data do ataque

12 a 15 de maio de 2017; início e pico em 12 de maio de 2017.

2. Tipo de ataque

Ransomware worm — propagação em rede explorando vulnerabilidade SMB/EternalBlue (MS17-010).

3. Descrição do ataque / como aconteceu

O ransomware WannaCry se espalhou rapidamente em maio de 2017 explorando a vulnerabilidade conhecida como EternalBlue (corrigida por MS17-010). Computadores com SMB exposto ou sem patch foram infectados, o malware criptografava arquivos e exigia resgate em Bitcoin. Um kill switch encontrado por um pesquisador de segurança interrompeu parte da propagação, mas não antes de centenas de milhares de máquinas serem afetadas.

4. Impactos e/ou prejuízo

• Mais de 200.000 computadores infectados em ~150 países; interrupções em hospitais (NHS no Reino Unido), transportes e empresas; prejuízos estimados em centenas de milhões a bilhões de dólares.

5. Tipo de proteção que poderia ter sido aplicada

• Aplicação imediata dos patches MS17-010; desativação/filtragem de SMB exposto; backups offline e planos de recuperação; segmentação de rede e defesa em camadas.

Ataque 2 — SolarWinds / Solorigate (2020)

1. Data do ataque

Código malicioso inserido em builds da SolarWinds Orion entre março e junho de 2020; descoberta pública em dezembro de 2020.

2. Tipo de ataque

Supply-chain attack (comprometimento de atualização de software) — backdoor conhecido como SUNBURST / Solorigate.

3. Descrição do ataque / como aconteceu

Operadores conseguiram inserir código malicioso no processo de build da SolarWinds Orion, fazendo com que atualizações legítimas distribuíssem a backdoor SUNBURST a clientes. Vítimas (empresas e agências governamentais) instalaram as atualizações infectadas, dando aos atacantes acesso persistente e sofisticado a redes sensíveis antes da descoberta.

4. Impactos e/ou prejuízo

• Comprometimento de múltiplas agências governamentais dos EUA e empresas privadas; acesso a e-mails e dados sensíveis; impacto geopolítico e custos de remediação elevados.

5. Tipo de proteção que poderia ter sido aplicada

• Auditoria e isolamento do processo de build; assinaturas e verificações de integridade robustas; segmentação e monitoramento avançado de comportamento; resposta coordenada entre fornecedores e clientes.

Referências

Principais fontes consultadas:

• Wikipedia — "WannaCry ransomware attack" (consulta resumida).

• Microsoft — MS17-010 (boletim de segurança sobre EternalBlue).

• Microsoft Security Blog — Solorigate deep dive (SUNBURST analysis).

• TechTarget / CSO / Time — linhas do tempo e análises do ataque SolarWinds.