O WannaCry é um ransomware que causou um dos maiores ciberataques da história em maio de 2017. Ele explorava uma vulnerabilidade no sistema operacional Windows chamada **EternalBlue**, que foi desenvolvida pela Agência de Segurança Nacional dos Estados Unidos (NSA) e posteriormente vazada pelo grupo de hackers Shadow Brokers.

Como o WannaCry funciona:

1. **Invasão e criptografia:**
   O WannaCry infectava computadores vulneráveis por meio de redes, utilizando a falha no protocolo SMB (Server Message Block) do Windows. Após infectar, ele criptografava os arquivos do sistema, tornando-os inacessíveis para o usuário.
2. **Pedido de resgate:**
   Exibia uma mensagem exigindo pagamento em bitcoins (uma criptomoeda difícil de rastrear) para descriptografar os arquivos. Geralmente, o valor aumentava com o tempo para pressionar as vítimas.
3. **Propagação em massa:**
   O WannaCry se espalhava rapidamente por redes inteiras, infectando computadores conectados e amplificando o impacto do ataque.

Impacto global:

- Afetou mais de **200.000 computadores** em mais de **150 países**.
- Hospitais, empresas, instituições governamentais e outros serviços essenciais foram paralisados. Um exemplo notório foi o sistema de saúde pública do Reino Unido (NHS), que teve muitos hospitais e ambulâncias comprometidos.
- Prejuízos financeiros estimados em **bilhões de dólares**.

Como foi contido:

- Um pesquisador de segurança, conhecido como **MalwareTech**, descobriu um "kill switch" no código do WannaCry. Ao registrar um domínio específico presente no ransomware, ele conseguiu desacelerar significativamente sua propagação.

Prevenção contra ransomware:

1. **Atualizações de software:**
   A Microsoft lançou um patch de segurança para corrigir a vulnerabilidade usada pelo WannaCry, incluindo versões do Windows fora de suporte, como o Windows XP.
2. **Backup regular:**
   Manter cópias dos dados em locais seguros.
3. **Antivírus e firewall:**
   Usar soluções atualizadas para detectar ameaças.
4. **Educação digital:**
   Evitar clicar em links ou abrir anexos suspeitos.

O WannaCry se tornou um exemplo marcante de como vulnerabilidades negligenciadas podem ser exploradas em larga escala, reforçando a importância de práticas de segurança cibernética.