Aluno: João Victor de Souza Moreira

RA:825135230

ATAQUES CIBERNÉTICOS

- **Ataque 1 – Microsoft Exchange Server / Hafnium**

Data aproximada: janeiro a março de 2021

Tipo de ataque: exploração de vulnerabilidades zero-day em servidores locais do Microsoft Exchange. O ataque permitia execução remota de código e inserção de webshells para manter acesso.

o grupo Hafnium, junto com outros agentes maliciosos, explorou quatro falhas graves (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 e CVE-2021-27065). Com isso, conseguiam acesso sem autenticação, executavam código malicioso, instalavam backdoors e extraíam dados sensíveis como e-mails e credenciais.

Vulnerabilidades exploradas: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 e CVE-2021-27065.

Impactos: aproximadamente 250 mil servidores no mundo foram afetados. Entre as vítimas estavam órgãos governamentais, ONGs, empresas privadas e instituições de pesquisa. Houve comprometimento de dados, vazamento de informações e custos elevados com resposta e limpeza dos sistemas.

Prevenção possível: aplicação rápida de patches de segurança, monitoramento de logs e acessos, uso de firewalls e autenticação multifator, além de limitar a exposição direta dos servidores Exchange à internet.

- **Ataque 2 – SharePoint “ToolShell” / CVE-2025-53770 e CVE-2025-53771**

Data aproximada: julho de 2025 (atividade identificada entre os dias 17 e 22 do mês).

Tipo de ataque: exploração zero-day em servidores on-premises do Microsoft SharePoint. O ataque envolveu execução remota de código e bypass de autenticação por path traversal.

O exploit apelidado de “ToolShell” utilizou a falha de deserialização (CVE-2025-53770) para executar código sem autenticação e a vulnerabilidade CVE-2025-53771 para contornar mecanismos de autenticação. Além disso, os atacantes roubaram chaves de criptografia (MachineKey), o que permitia manter acesso mesmo após medidas de correção.

Vulnerabilidades exploradas: CVE-2025-53770 e CVE-2025-53771.

Impactos: dezenas a centenas de servidores comprometidos. Setores como governo, telecomunicações, saúde e educação foram impactados. Houve risco de roubo de dados e persistência prolongada dos atacantes, exigindo medidas emergenciais.

Prevenção possível: atualização constante com patches, restrição de exposição do SharePoint à internet, monitoramento contínuo, rotação de chaves criptográficas após incidentes e uso de soluções de segurança como antivírus, firewalls, AMSI e autenticação forte.