USJT – UC Sistemas Computacionais e Segurança – Prof. Calvetti - Atividade

NOME: Daniel Silva

ATIVIDADE:

Escolher 2 (dois) ataques cibernéticos de tipos diferentes ocorridos nos últimos 5 anos e fazer um texto com: Data do ataque (pode ser aproximada); Tipo de ataque; Descrição do ataque ou de como aconteceu; Vulnerabilidade explorada (verificar se está no CVE e qual o seu código); Impactos e/ou prejuízo (pode ser estimado); Tipo de Proteção que poderia ter sido aplicada para evitá-lo.

PESQUISA:

O golpe de bitcoin no Twitter de 2020

O Twitter foi crackeado em 15 de julho de 2020. Os invasores usaram engenharia social, confirmada pelo Twitter como phishing por telefone, para sequestrar diversas contas de alto perfil. Essas contas incluíam a do CEO da Tesla, Elon Musk, do CEO da Amazon, Jeff Bezos, e do ex-presidente dos Estados Unidos, Barack Obama. Os invasores conseguiram roubar credenciais de funcionários e obtiveram acesso ao sistema de gerenciamento interno da empresa.

O golpe consistia em usar essas contas e criar tweets fraudulentos que pediam para que as pessoas enviassem uma moeda bitcoin para uma carteira específica de criptomoedas, com a promessa de que o dinheiro enviado seria retornado em dobro como um gesto de gratidão. Poucos minutos após os tweets iniciais, mais de 320 transações já haviam sido realizadas e mais de US$118.000, equivalentes em bitcoins, foram depositados nessa conta antes que as mensagens de fraude fossem removidas pelo Twitter.

Exploits da Microsoft afetam a Acer

Uma onda global de ataques cibernéticos e violações de dados começou em janeiro de 2021, após quatro exploits de 0-days terem sido descobertos em servidores Microsoft Exchange locais, dando aos invasores acesso total aos e-mails e senhas dos usuários em servidores afetados, privilégios de administrador no servidor e acesso a dispositivos conectados na mesma rede. Os invasores normalmente instalam um backdoor que permite ao invasor acesso total aos servidores impactados, mesmo que o servidor seja atualizado posteriormente para não ser mais vulnerável aos exploits originais.

Em 18 de março de 2021, uma afiliada da gangue cibernética de ransomware Revil, alegou ter roubado dados não criptografados da fabricante taiwanesa de computadores Acer, incluindo um número não divulgado de dispositivos criptografados, com a empresa de segurança cibernética Advanced Intel vinculando essa violação de dados e o ataque de ransomware aos exploits do Microsoft Exchange. A REvil exigiu um

resgate de US$50 milhões, alegando que, se o resgate fosse pago, eles "forneceriam um descriptografador, um relatório de vulnerabilidade e a exclusão dos arquivos roubados", e afirmando que o resgate dobraria para US$100 milhões se não fosse pago em 28 de março de 2021. O vazamento de dados incluía planilhas financeiras, saldos bancários, comunicações com o banco, etc. O REvil também conseguiu o número de contas de clientes, e publicou tudo como uma lista de leilões em seu site.

- CVE mais próximo da data do ocorrido: **CVE-2021-27065 "Vulnerabilidade de execução remota de código do Microsoft Exchange Server"**

DICAS PARA EVITAR OS ATAQUES MENCIONADOS:

- Faça as atualizações de segurança, pois os fornecedores lançam regularmente atualizações para corrigir as vulnerabilidades que foram descobertas e que podem ser exploradas por ataques 0-day.

- Utilize programas de segurança que usem análise heurística e aprendizado de máquina para detectar atividades suspeitas e ameaças novas e desconhecidas; Firewalls para permitir apenas transações essenciais e utilize sistemas de detecção e prevenção de intrusões (IDS/IPS) para monitorar o tráfego de rede e bloquear comportamentos suspeitos em tempo real.

- Faça backup de seus dados importantes regularmente, pois os invasores que usam ransomware gostam de se aproveitar de usuários que dependem de determinados dados para gerir suas organizações.

- Evite clicar em links suspeitos ou baixar anexos de fontes desconhecidas, pois ataques de phishing frequentemente exploram vulnerabilidades 0-day. Pesquise pelo link digitando-o no campo do URL do navegador para verificar sua veracidade.

- Realize formações para ensinar os seus colaboradores e utilizadores sobre boas práticas de segurança online e como identificar e evitar táticas de engenharia social. Fique calmo e não se deixe cair no senso de urgência que os golpistas criam, pois é assim que eles atuam para que a vítima não pense criticamente e execute a ação fraudulenta.

- Divida a sua rede em segmentos menores e isolados para impedir que um ataque 0-day se espalhe por todo o sistema.

- Utilize uma lista branca de aplicações para permitir que apenas programas aprovados sejam executados, tornando mais difícil para os ataques 0-day correrem com sucesso.

- Não conecte dispositivos USB desconhecidos, porque eles podem ser usados para armazenar arquivos maliciosos.

BIBLIOGRAFIAS

UNIVERSITY, EC-Council. **Top Ten Cyberattacks of 2020-2021**. Disponível em: <https://www.eccu.edu/blog/cybersecurity/top-ten-cyberattacks/>. Acesso em: 15 set. 2025.

WIKIPEDIA. **2021 Microsoft Exchange Server data breach**. Disponível em: <https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach>. Acesso em: 15 set. 2025.

WIKIPEDIA. **Golpe de julho de 2020 de várias contas verificadas do Twitter para postar tweets fraudulentos**. Disponível em: <https://pt.wikipedia.org/wiki/Golpe_de_bitcoin_no_Twitter_de_2020>. Acesso em: 15 set. 2025.

KASPERSKY. **Dicas para a prevenção de phishing**. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/phishing-prevention-tips>. Acesso em: 15 set. 2025.

FORTNET. **Como evitar ransomware | 9 dicas | Fortinet**. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/how-to-prevent-ransomware>. Acesso em: 15 set. 2025.

KASPERSKY. **O que é um ataque de dia zero? – Definição e explicação**. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/zero-day-exploit>. Acesso em: 15 set. 2025.