Ataque SolarWinds

Data do ataque: Setembro de 2019

Tipo de ataque: proliferação de malware

Descrição: O ataque à SolarWinds se compreendeu ao longo de 6 meses, durante esse tempo os hackers executaram pacientemente e sistematicamente seu ataque. A seguir, um resumo de como aconteceu:

- Em Setembro de 2019, hackers foram capazes de acessar a rede da Solar Winds
- Eles começaram testando a inserção do seu código no sistema Orion em Outubro de 2019
- Depois de 4 meses, eles inseriram código um malicioso chamado ‘Sunburst’ dentro Orion.
- Em 26 de Março de 2020, a SolarWinds começou a distribuir as atualizações do Orion contendo o código malicioso.

O malware foi disperso em centendas de clientes da SolarWinds assim que o código malicioso foi instalado na atualização hackeada. Uma vez no sistema da vítima, o malware deu acesso aos hackers aos sistemas de TI do clientes. A partir de então, os agressores podiam instalar ainda mais malwares, que permitiriam eles espionarem mais organizações.

Vulnerabilidade explorada: Hackers comprometeram o componente de monitoramento de rede Orion SolarWinds assinado digitalmente, abrindo uma backdoor nas redes de centenas de clientes da SolarWinds; empresas públicas e privadas.

Impactos e/ou prejuízo: Como resultado do ataque, cerca de 18.000 clientes da SolarWinds acabaram sendo prejudicados, incluindo o governo dos EUA.

Tipo de proteção: Implementar gerenciamento de log e informação de segurança e gerenciamento de eventos (SIEM).

Auditar diretórios ativos por mudanças.

Performar testes de penetração regularmente.

Incrementar seu sistema de prevenção de perda de dados.

Ataque WannaCry

Data do ataque: 12/05/2017

Tipo de ataque: ransomware de criptografia

Descrição do ataque: Em 12 de maio de 2017, o worm do ransomware WannaCry se espalhou para mais de 200 mil computadores em mais de 150 países. Vítimas ilustres incluem FedEx, Honda, Nissan e o Serviço Nacional de Saúde (NHS) do Reino Unido, que foi forçado a desviar algumas de suas ambulâncias para hospitais alternativos.

Vulnerabilidade explorada: O WannaCry se espalhou usando uma exploração de vulnerabilidade chamada "EternalBlue". A Agência de Segurança Nacional dos Estados Unidos (NSA) desenvolveu essa exploração, presumivelmente para uso próprio, mas ela foi roubada e lançada ao público por um grupo chamado Shadow Brokers depois que a própria NSA foi comprometida. O EternalBlue só funcionava em versões mais antigas e sem patch do Microsoft Windows, mas havia um número de máquinas mais do que o suficiente executando tais versões para permitir a rápida disseminação do WannaCry.

Impactos e/ou prejuízo: O ataque do ransomware WannaCry atingiu cerca de 230 mil computadores em todo o mundo.

Tipo de proteção: Atualizar com frequência os patches de segurança.

Não utilizar sistemas operacionais defasados.

Utilizar plataformas Zero Trust.

Referências:

SolarWinds attack:

https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack

https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

https://www.techtarget.com/searchsecurity/news/252493987/SolarWinds-backdoor-infected-tech-giants-impact-unclear

WannaCry ransomware:

https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry

https://www.cloudflare.com/pt-br/learning/security/ransomware/wannacry-ransomware/