Sistemas Computacionais e Segurança

(Prof. Calvetti)

Ataques Cibernéticos

Ataque do Ransomware WannaCry

Data: 12/05/2017

Tipo de ataque: Ransomware

Descrição do ataque: O WannaCry foi um ransomware que se espalhou rapidamente ao explorar uma vulnerabilidade no sistema Windows, conhecida como EternalBlue. Essa vulnerabilidade foi originalmente descoberta pela Agência de Segurança Nacional dos EUA (NSA) e vazou pelo grupo hacker Shadow Brokers. Uma vez que o ransomware infectava um computador, ele criptografava os arquivos e exigia um pagamento em Bitcoin para restaurá-los.

Vulnerabilidade explorada: EternalBlue - CVE-2017-0144 (vulnerabilidade no protocolo de compartilhamento de arquivos SMB no Windows).

Prejuízos e impactos: O WannaCry afetou mais de 200.000 computadores em 150 países, atingindo desde grandes corporações até instituições públicas. Um dos impactos mais significativos ocorreu no Sistema Nacional de Saúde (NHS) do Reino Unido, onde hospitais tiveram

que adiar cirurgias e consultas devido à paralisação dos sistemas. Estima-se que o ataque causou prejuízos superiores a US$ 4 bilhões em todo o mundo.

Prevenção e proteção:

Aplicação de patches de segurança: A Microsoft havia lançado uma correção para a vulnerabilidade dois meses antes do ataque, mas muitos sistemas ainda não haviam sido atualizados.

Backups regulares: Organizações poderiam ter evitado pagar o resgate ao restaurar dados criptografados a partir de backups seguros.

Soluções de endpoint: Ferramentas de detecção de comportamento anômalo poderiam ter ajudado a identificar e isolar a ameaça antes que ela se espalhasse.

Ataque SolarWinds

Data: Descoberto em dezembro de 2020, mas acredita-se que começou em março de 2020

Tipo de ataque: Ameaça persistente avançada (APT), também conhecido como ataque à cadeia de suprimentos

Descrição do ataque: Hackers, suspeitos de terem ligações com o governo russo (grupo conhecido como APT29 ou Cozy Bear), comprometeram o software de monitoramento de rede SolarWinds Orion. Os invasores conseguiram inserir um código malicioso em atualizações legítimas do software, que foram então distribuídas para milhares de clientes da SolarWinds, incluindo órgãos governamentais dos EUA e grandes empresas privadas. Uma vez instalado, o malware permitia aos atacantes acesso remoto às redes das vítimas, sem serem detectados por meses.

Vulnerabilidade explorada: A vulnerabilidade envolveu o comprometimento da cadeia de suprimentos da SolarWinds, especificamente a falta de segurança no processo de desenvolvimento de software da empresa.

Prejuízos e impactos: Este ataque comprometeu redes governamentais críticas dos EUA, incluindo os departamentos de Tesouro, Justiça e Comércio, além de grandes empresas como a Microsoft. Embora o impacto financeiro direto seja difícil de calcular, o maior prejuízo foi o comprometimento de informações sensíveis e dados confidenciais. As consequências ainda estão sendo avaliadas.

Prevenção e proteção:

Segurança na cadeia de suprimentos: A SolarWinds poderia ter implementado práticas mais rigorosas de verificação de segurança em suas atualizações de software.

Segmentação de rede: A separação de partes críticas da rede pode limitar o impacto de ataques bem-sucedidos.

Monitoramento e auditoria contínua: O uso de ferramentas para detectar comportamentos suspeitos, mesmo em software confiável, poderia ter ajudado a identificar a ameaça mais cedo.