



NEW
TIPS

ATAQUES CIBERNÉTICOS

PROTECT YOUR COMPUTER NOW

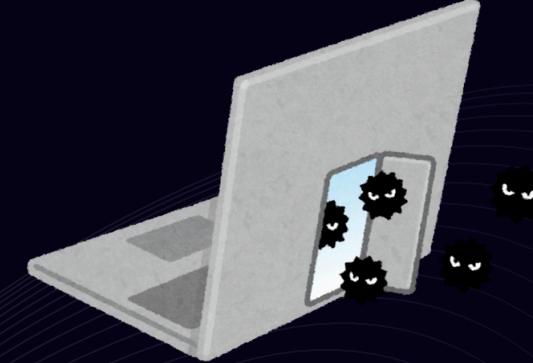
EQUIFAX

DESCRIÇÃO DO ATAQUE

O ATAQUE À EQUIFAX, UMA DAS MAIORES AGÊNCIAS DE CRÉDITO DOS EUA, RESULTOU NA VIOLAÇÃO DE DADOS PESSOAIS DE APROXIMADAMENTE 147 MILHÕES DE CONSUMIDORES. OS HACKERS EXPLORARAM UMA VULNERABILIDADE EM UM SOFTWARE DE CÓDIGO ABERTO CHAMADO APACHE STRUTS, QUE A EQUIFAX USAVA EM SEUS SISTEMAS. A FALHA PERMITIU QUE OS ATACANTES ACESSASSEM DADOS SENSÍVEIS, COMO NÚMEROS DE SEGURIDADE SOCIAL, DATAS DE NASCIMENTO E ENDEREÇOS.



VULNERABILIDADE EXPLORADAS:



O ATAQUE EXPLOROU UMA FALHA CONHECIDA NO APACHE STRUTS, QUE NÃO HAVIA SIDO CORRIGIDA PELA EQUIFAX APESAR DE UM PATCH DE SEGURANÇA ESTAR DISPONÍVEL. A FALTA DE ATUALIZAÇÃO DO SOFTWARE E A DEFICIÊNCIA NA IMPLEMENTAÇÃO DAS MEDIDAS DE SEGURANÇA PERMITIRAM O ACESSO NÃO AUTORIZADO AOS SISTEMAS DA EMPRESA.

IMPACTOS E PREJUÍZOS:

A VIOLAÇÃO RESULTOU EM UM GRANDE CUSTO FINANCEIRO PARA A EQUIFAX, INCLUINDO MULTAS REGULATÓRIAS, AÇÕES JUDICIAIS E DESPESAS COM MITIGAÇÃO. A REPUTAÇÃO DA EMPRESA FOI SEVERAMENTE PREJUDICADA, E MUITOS CONSUMIDORES TIVERAM SUAS INFORMAÇÕES PESSOAIS COMPROMETIDAS, AUMENTANDO O RISCO DE ROUBO DE IDENTIDADE E FRAUDE



TIPO DE PROTEÇÃO QUE PODERIA TER SIDO APLICADA:

A EQUIFAX PODERIA TER EVITADO O ATAQUE MANTENDO SEUS SISTEMAS ATUALIZADOS COM OS PATCHES DE SEGURANÇA MAIS RECENTES, ALÉM DE TER IMPLEMENTADO MELHORES PRÁTICAS DE SEGURANÇA, COMO A SEGMENTAÇÃO DE REDES E A PROTEÇÃO DE DADOS SENSÍVEIS. ALÉM DISSO, UMA REVISÃO E REFORÇO DOS PROCESSOS DE SEGURANÇA CIBERNÉTICA E AUDITORIAS REGULARES TERIAM AJUDADO A IDENTIFICAR E CORRIGIR VULNERABILIDADES DE FORMA MAIS EFICAZ.



NOTPETYA

DESCRIÇÃO DO ATAQUE:

O NOTPETYA FOI UM RANSOMWARE QUE SE ESPALHOU RAPIDAMENTE ATRAVÉS DE UMA VULNERABILIDADE NO PROTOCOLO SMBV1, SEMELHANTE AO WANNACRY, MAS COM CARACTERÍSTICAS MAIS DESTRUTIVAS. O ATAQUE SE DISFARÇOU COMO UM RANSOMWARE, MAS, NA VERDADE, TINHA COMO OBJETIVO PRINCIPAL DESTRUIR DADOS E SISTEMAS. ELE COMEÇOU NA UCRÂNIA E SE ESPALHOU GLOBALMENTE, AFETANDO GRANDES EMPRESAS E ORGANIZAÇÕES.

VULNERABILIDADE EXPLORADAS

O NOTPETYA EXPLOROU A MESMA VULNERABILIDADE SMBV1 QUE O WANNACRY, ALÉM DE USAR TÉCNICAS DE PROPAGAÇÃO LATERAL PARA SE ESPALHAR PELA REDE, COMO A FERRAMENTA ETERNALBLUE. O ATAQUE TAMBÉM UTILIZOU UM MECANISMO DE ATUALIZAÇÃO Falsa PARA SE INFILTRAR NOS SISTEMAS.

IMPACTOS E PREJUÍZOS

O ATAQUE CAUSOU DANOS SIGNIFICATIVOS A VÁRIAS EMPRESAS E ORGANIZAÇÕES AO REDOR DO MUNDO. EMPRESAS COMO MAERSK E FEDEX FORAM SEVERAMENTE AFETADAS, RESULTANDO EM PREJUÍZOS FINANCEIROS SIGNIFICATIVOS. A NATUREZA DESTRUTIVA DO RANSOMWARE LEVOU À PERDA PERMANENTE DE DADOS PARA MUITAS ORGANIZAÇÕES, ALÉM DE GRANDES CUSTOS ASSOCIADOS À RECUPERAÇÃO E RESTAURAÇÃO DOS SISTEMAS AFETADOS.



TIPO DE PROTEÇÃO QUE PODERIA TER SIDO APLICADA

PARA PREVENIR UM ATAQUE COMO O NOTPETYA, AS ORGANIZAÇÕES PODERIAM TER DESATIVADO O SMBV1, APlicado patches de segurança de forma proativa e implementado uma abordagem de segurança em camadas, incluindo a segmentação da rede, a utilização de soluções antivírus atualizadas e a realização de backups regulares e seguros. A educação contínua sobre segurança cibernética e a realização de simulações de resposta a incidentes também ajudariam a preparar as organizações para enfrentar tais ameaças.

