Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

Prof. Robson Calvetti

João Luiz da Silva e Rafael Tiago Scisci Arcienega

RA: 82420546 e 824216105

Atualmente, vem aumentando muitas ocorrencias de ataques ciberneticos no mundo em geral, ataques ciberneticos são tentativas de acesso ilegal a uma rede de computadores, geralmente esses invasores podem ser indivíduos ou organizaçoes criminosas, tem objetivos bem definidos como obter dados, dinheiro, ou intenções politicas,ou simplesmente pessoal.

Um ataque que foi divulgado na data de 8 de outubro de 2022, foi na emissora de televisão Rede Record, o sistema central da Record (à época, Record TV) em São Paulo sofreu um ciberataque, onde os hackers roubaram todo o acervo de reportagens pré-gravadas e quadros dos programas de auditório da emissora, Os funcionários também ficaram sem o acesso ao Ibope pelos celulares da emissora, e foi cortado o acesso à intranet. Também, foi bloqueado o acesso aos e-mails da empresa. Por isso, os hackers talvez tenham acesso a todos os e-mails já enviados e recebidos pelos funcionários, A internet também foi derrubada, Segundo informações do jornalista do Tecmundo Felipe Payão, o ataque foi realizado pelo BransomwarelackCat, Ele é um ransomware as a service, ou seja, foi comprado pelos criminosos.

Resgate:

De acordo com o comunicado enviado à RecordTV, os hackers iriam cobrar US$ 7 milhões, mas deram um desconto válido até o dia 15, cobrando US$ 5 milhões. O valor deve ser pago em Bitcoinou Monero. Eles também disseram que caso o valor seja pago, eles vão mostrar para a empresa como a invasão ocorreu e vão ajudar na descriptografia dos dados. Caso o valor não seja pago, os hackers realizariam um ataque DdoS e já estão procurando possíveis compradores do conteúdo na dark web.

No dia 16, dados começaram a ser vazados na deep web, incluindo planilhas de faturamento e o passaporte de uma estrela da emissora.

Reação da Record:

A Record acionou o Departamento de Crimes Cibernéticos, No dia 10, o departamento de Tecnologia e Segurança restaurou o acesso aos computadores e e-mail, No dia 12, o departamento de TI conseguiu

fazer uma cópia dos dados sequestrados.

A princípio, a emissora não se pronunciou, O ataque se tornou público no dia 8 de outubro, quando a RecordTV tirou o programa alguns programas do ar.

A Record foi criticada por não ter backup da programação.

Tipo de ataque: BransomwarelackCat (O ransomware BlackCat é um tipo de malware criado por cibercriminosos russos que se tornou uma das formas mais ativas de ransomware desde a sua primeira aparição em 2021. Ele é também conhecido como ALPHV ou ALPHV-ng, e é considerado uma das operações de ransomware-as-a-service (RaaS) mais sofisticadas.)

A vulnerabilidade explorada, identificada como CVE-2024-37085, é um desvio de autenticação no VMware ESXi que permite aos atacantes obter privilégios de administrador no hipervisor ao criar um grupo "ESX Admins" e adicionar usuários a ele.28 de ago. de 2024

Tipos de proteções: Para se proteger de ransomware, é possível adotar algumas medidas, como: Atualizar o software, manter o software dos dispositivos atualizados, incluindo o software de segurança, é importante para garantir que o antimalware reconheça ameaças mais recentes, usar soluções de segurança, utilizar soluções de segurança robustas, como firewalls e antivírus, para detectar e bloquear malwares, armazenar backups separados, armazenar os backups em um disco rígido externo ou na nuvem, para que não possam ser acessados em uma rede, educar os usuários, ensinar os usuários sobre práticas de segurança cibernéticas, como evitar clicar em links suspeitos ou abrir anexos de e-mails não solicitados, usar verificadores de vírus e filtros de conteúdo Utilizar esses programas nos servidores de e-mail para reduzir o risco de spam com anexos maliciosos ou links infectados.

Em junho de 2023, o software MOVEit (ferramenta usada para transferência de arquivos usado por várias organizações e empresas) sofreu um ataque cibernético do tipo Supply chain, é um tipo de ataque cibernético que ocorre quando hackers comprometem um fornecedor ou parceiro de uma organização para obter acesso aos seus sistemas ou dados. Acabou afetando diversas empresas, como: Shell, Boots, e o o Departamento de Educação da Cidade de Nova York. Nesse ataque, o grupo explorou a vulnerabilidade CVE-2023-34362,essa falha foi categorizada como uma vulnerabilidade de injeção de SQL.

Com esse ataque, dados foram comprometidos e as atividades de diversas empresas de grande porte foram interrompidas, os prejuízos financeiros não foram divulgados, mas estima-se que foram bem significativos.

As proteções que poderiam ter sidos feitas para evitar todo esse caos são: A aplicação imediata de patches de segurança e a adoção de monitoramento contínuo de redes poderiam ter evitado que o ataque ocorresse. A manutenção de backups frequentes também teria ajudado na recuperação dos dados sem a necessidade de pagar o resgate.