NOMES:
ANDREY FERREIRA PICHUTI / RA: 82414002
MOSHE ACHKIY SILVERIO MANDUJANO / RA: 824115318
JOÃO GABRIEL SILVA BARBARA DA CONCEIÇÃO / RA: 82415176
NICOLAS TRINDADE MARCIANO / RA: 824135758

ATAQUES CIBERNÉTICOS DOS ÚLTIMOS 5 ANOS

Primeiro Ataque - Invasão na Rockstar

Data do ataque: Entre os dias 17 e 18 setembro de 2022.

Tipo de ataque: O ataque foi uma invasão de rede, possivelmente usando engenharia social para acessar sistemas internos da empresa Rockstar Games.

Descrição do ataque: O cracker, intitulado como “teapotuberhacker”, invadiu os servidores de comunicação interna da Rockstar, provavelmente o Slack e Confluence, desta forma, obteve vídeos, imagens e o código-fonte do jogo GTA VI, que estava em desenvolvimento. O invasor conseguiu obter cerca de 90 vídeos mostrando algumas funcionalidades teste do jogo, ainda disponíveis no YouTube, diálogos entre personagens e dados internos.

Obs: esse cracker intitulado “teapotuberhacker” também atacou a Uber na mesma época.

Vulnerabilidade explorada: O método utilizado para invadir a empresa não foi confirmado, mas acredita-se que o cracker tenha usado engenharia social para enganar um funcionário da empresa e obter acesso aos sistemas internos de comunicação.

Impactos e prejuízos: O impacto principal foi para a imagem e a segurança da Rockstar Games. Embora a empresa tenha afirmado que o vazamento não tenha afetado o desenvolvimento do jogo, o vazamento do conteúdo de um jogo tão esperado pela comunidade causou grande repercussão nas redes sociais, gerando um alto nível de pressão pública. O incidente acabou destacando vulnerabilidades na segurança de grandes estúdios. O prejuízo financeiro exato é desconhecido, mas pode ser estimado em milhões de dólares. Além disso, foram forçados a emitir diversas notificações DMCA para remover os conteúdos das plataformas online.

Tipo de proteção que poderia ter sido aplicada para evitá-lo: Para evitar esses tipos de ataques, a empresa poderia segmentar a rede, limitando o acesso a sistemas críticos, autenticação multifator (MFA) para todos os funcionários, monitoramento mais rígido e preciso, e treinamento dos usuários contra engenharia social.

Declaração da Rockstar Games sobre o acontecimento:

"Recentemente, sofremos uma invasão de rede na qual um terceiro não autorizado acessou e baixou ilegalmente informações confidenciais de nossos sistemas, incluindo filmagens de desenvolvimento inicial para o próximo Grand Theft Auto. No momento, não prevemos nenhuma interrupção em nossos serviços de jogo ao vivo nem nenhum efeito de longo prazo no desenvolvimento de nossos projetos em andamento.

Estamos extremamente decepcionados por ter quaisquer detalhes do nosso próximo jogo compartilhados com todos vocês dessa forma. Nosso trabalho no próximo jogo Grand Theft Auto continuará conforme planejado e continuamos comprometidos como sempre em entregar uma experiência para vocês, nossos jogadores, que realmente exceda suas expectativas. Atualizaremos todos novamente em breve e, claro, apresentaremos adequadamente este próximo jogo quando estiver pronto. Queremos agradecer a todos pelo apoio contínuo durante esta situação." - Rockstar Games.

Segundo Ataque - Colonial Pipeline

Data do ataque: Dia 07 de maio de 2021.

Tipo de ataque: A empresa foi atacada por um ransomware do DarkSide, que pode ser executado tanto no Windows quanto no Linux. Detectam o malware como *Trojan-Ransom.Win32.Darkside* e *Trojan-Ransom.Linux.Darkside*. O DarkSide usa algoritmos de criptografia fortes, tornando impossível a restauração de dados sem a chave certa.

Descrição do ataque: O grupo DarkSide usou um modelo de ransomware como serviço, fornecendo software e infraestrutura relacionada aos parceiros que realizam os ataques. Um desses sócios era responsável pela segmentação da Colonial Pipeline. Operadores de ransomware não apenas criptografam dados e exigem resgate para descriptografá-los, mas também roubam informações como forma de extorsão.

Vulnerabilidade explorada: O ataque cibernético à Colonial Pipeline em 2021 explorou uma vulnerabilidade em um software de gerenciamento remoto. Especificamente, os atacantes utilizaram uma brecha em um sistema de VPN (Virtual Private Network) que não estava adequadamente protegido com autenticação multifatorial (MFA).

Impactos e prejuízos: Os funcionários tiveram de desligar alguns sistemas de informação, em parte porque alguns computadores estavam criptografados e em parte para evitar que a infecção se propagasse. Isso causou atrasos no fornecimento de combustível, gerando aumento de 4% nos contratos futuros de gasolina. os invasores desviaram cerca de 100GB de dados da rede corporativa. A empresa continua restaurando seus sistemas, mas de acordo com o blog Zero Day, o problema está mais no sistema de faturamento do que nas redes de serviço.

Tipo de proteção que poderia ter sido aplicada para evitá-lo: Para prevenir ataques como o da Colonial Pipeline, é essencial implementar autenticação multifatorial para adicionar uma camada extra de segurança, manter sistemas e softwares atualizados com os últimos patches, e garantir que as VPNs estejam configuradas de forma segura com criptografia robusta. Segmentar a rede pode limitar o impacto de uma violação, enquanto o monitoramento contínuo e um plano de resposta a incidentes ajudam a identificar e conter ataques rapidamente.

Declaração da Colonial Pipeline sobre o acontecimento:

A Colonial Pipeline divulgou uma declaração em que abordou o incidente e suas consequências. A empresa confirmou que havia sido alvo de um ataque de ransomware, que levou à paralisação de suas operações e à suspensão temporária do transporte de combustível. A declaração enfatizou que a Colonial Pipeline estava trabalhando de forma diligente para restaurar os serviços e garantir a segurança dos sistemas.

A empresa também mencionou ter acionado especialistas em segurança cibernética e autoridades governamentais para investigar o ataque e responder à situação. Além disso, a Colonial Pipeline expressou seu compromisso em tomar medidas para fortalecer a segurança de seus sistemas e evitar futuros incidentes semelhantes. A declaração refletiu a gravidade do ataque e a urgência da resposta da empresa, bem como a importância da colaboração com as autoridades para enfrentar o problema.