



# ATAQUES CIBERNÉTICOS

ARTUR ROSA CORREIA – **824135943**  
GUSTAVO SILVEIRA BENICIO – **824134160**  
LUAN BERNARDO ALVES – **824134204**



cyber attack



# ATAQUE A JBS

(31 de maio de 2021)

## RANSOMWARE

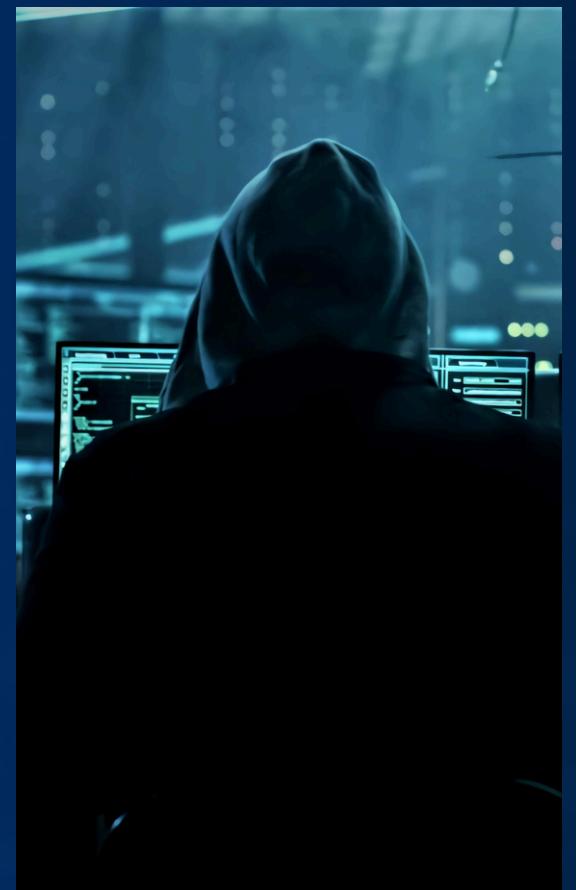
A JBS, uma das principais empresas de processamento de carne no mundo, foi vítima de um ataque de ransomware (tipo de malware que criptografa os dados da vítima e exige um resgate para desbloqueá-los.) realizado pelo grupo hacker REvil. Os envolvidos conseguiram comprometer os sistemas da empresa, que afetou suas operações em vários países, incluindo Estados Unidos e Austrália. A empresa foi forçada a interromper temporariamente suas operações para conter o ataque e proteger seus dados. Após o ataque, buscaram reforçar suas medidas de segurança para evitar futuros incidentes e melhoraram, sua defesa contra ameaças cibernéticas.





## Vulnerabilidade explorada

Embora o código CVE não tenha sido especificado, suspeita-se que a vulnerabilidade explorada tenha sido através de um phishing ou falha no controle de acesso, comum em ataques de ransomware como este. O grupo REvil é conhecido por explorar falhas em servidores vulneráveis e práticas de segurança fracas, como senhas fracas e falta de autenticação multifator (MFA).



## Prejuízos e impactos

- A JBS pagou cerca de U\$ 11 milhões em BitCoin para o resgate de dados;
- A interrupção das operações teve impacto direto no fornecimento de carne e aumentou os preços dos produtos.
- As fábricas ficaram paradas por dias, gerando perdas financeiras expressivas.
- Impacto negativo na imagem da empresa, afetando a confiança dos consumidores e parceiros comerciais.





## Tipo de Proteção que poderia ter sido aplicada para evitá-lo

- Autenticação multifator (MFA) para impedir o acesso não autorizado às redes internas.
- Backup adequado de dados e isolamento de sistemas críticos para garantir a continuidade operacional durante um ataque.
- Educação em cibersegurança para os funcionários, a fim de evitar ataques de phishing, que são uma das principais maneiras pelas quais o ransomware se infiltra nas redes corporativas

# ATAQUE A TWITCH

(6 de outubro de 2021)



## Vazamento de dados

A Twitch, plataforma de streaming, foi alvo de um ataque cibernético significativo, resultando no vazamento de uma grande quantidade de dados, cerca de 125 GB. O atacante obteve e divulgou informações confidenciais, incluindo os ganhos financeiros dos streamers e detalhes técnicos internos da plataforma. O ataque foi revelado publicamente quando os dados vazados foram publicados em um fórum online. Em resposta ao incidente, a Twitch intensificou suas medidas de segurança para proteger melhor as informações dos usuários e reforçar a integridade da plataforma.



## Vulnerabilidade explorada

A vulnerabilidade explorada foi uma configuração incorreta de um servidor da AWS que a Twitch utilizava para armazenar dados. Isso permitiu ao hacker acessar os dados críticos. A vulnerabilidade específica no CVE é CVE-2021-44228 (Log4j), uma falha de segurança que permite a execução remota de código.



## Prejuízos e impactos

- O vazamento expôs informações confidenciais de pagamento de diversos streamers famosos, causando danos à privacidade.
- Houve um prejuízo significativo à imagem da Twitch, com os usuários perdendo confiança na plataforma em relação à segurança dos seus dados.
- O projeto interno da Amazon Game Studios foi exposto, revelando planos de desenvolvimento que poderiam comprometer a vantagem competitiva da empresa.





## Tipo de Proteção que poderia ter sido aplicada para evitá-lo

- Configuração adequada de servidores e redes, Garantir que servidores na nuvem (AWS) sejam configurados corretamente para evitar acessos não autorizados.
- Monitoração contínua de segurança para detectar e corrigir falhas de configuração em tempo real.
- Implementação de testes regulares de penetração para identificar vulnerabilidades antes que sejam exploradas por atacantes.



# MUITO OBRIGADO!



cyber attack

