

Cibersegurança

E SEUS ATAQUES

CYBER SECURITY



Ciberinvasões

E O QUE SÃO

Ciberinvasões são ataques deliberados que visam comprometer a integridade de redes, sistemas e dados.

IMPORTÂNCIA DA CIBERSEGURANÇA

A cibersegurança ajuda a proteger informações sensíveis, infraestrutura crítica e ajuda a reduzir os riscos de roubo, espionagem e danos operacionais



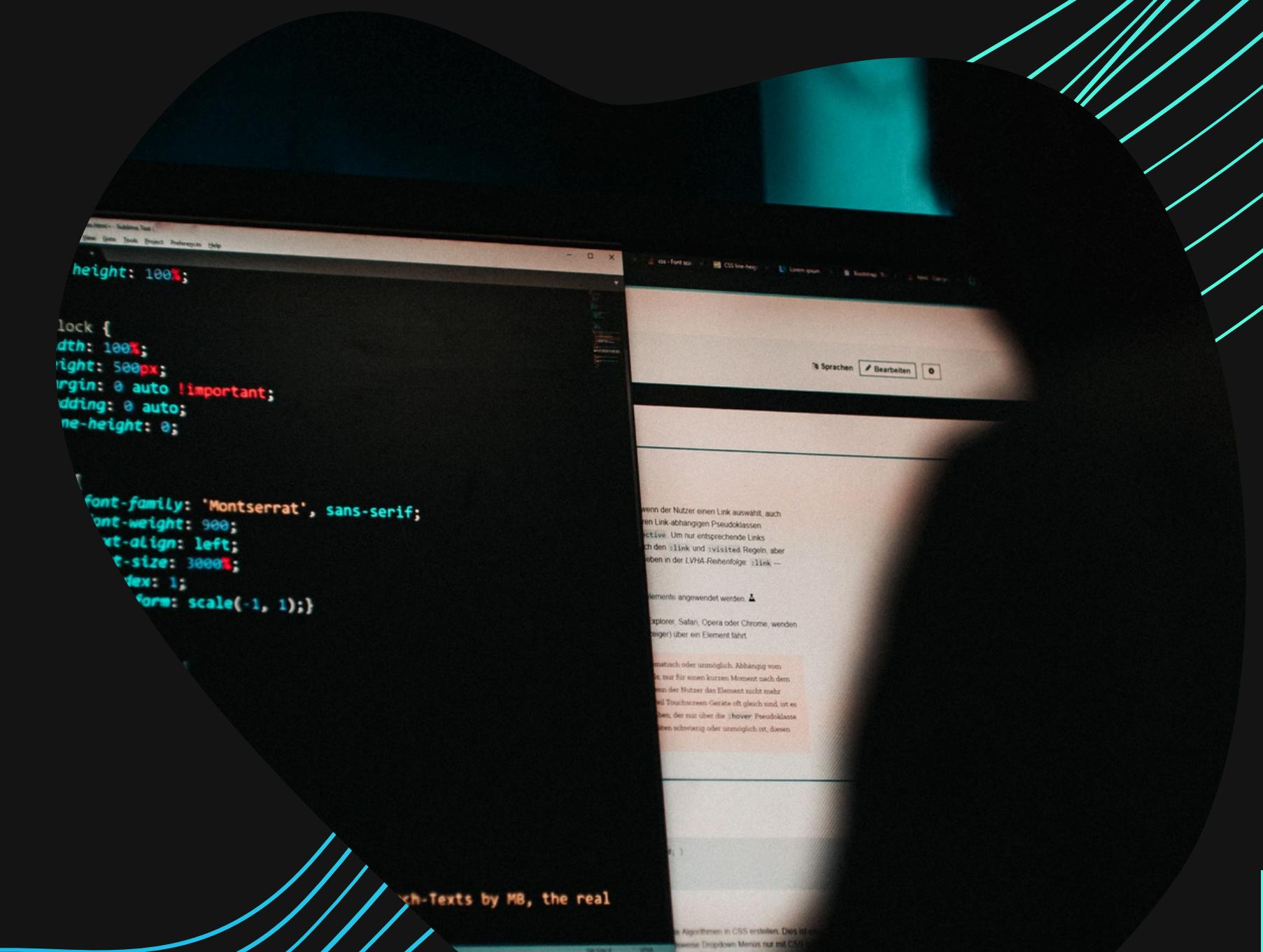
ATAQUE À EMPRESA DE ENERGIA NUCLEAR DA UCRÂNIA

Data: Agosto de 2022

Alvo: Energoatom, uma empresa de energia nuclear estatal da Ucrânia.

Tipo de Ataque: Ataque DDoS (Distributed Denial of Service)

Contexto: A Ucrânia estava em conflito com a Rússia, assim tornando suas infraestruturas críticas alvos frequentes de ataques





EXECUÇÃO:

Este foi um ataque DDoS, realizado pelo grupo pró-Rússia conhecido como "People's Cyber Army".

O objetivo foi a sobrecarga de tráfego nos servidores da Energoatom, causando falha de acessos, paralisação temporária e interrompendo serviços online da companhia

MOTIVAÇÕES POR TRÁS DO ATAQUE

Objetivo Principal: Desestabilizar o setor de energia nuclear da Ucrânia.

O ataque teve motivações geopolíticas, como enfraquecer a resiliência da Ucrânia durante a guerra contra a Rússia.

Possível roubo de dados sensíveis ou tentativas de interferir na operação de usinas nucleares, vindo provavelmente de dentro da companhia.

CONSEQUÊNCIAS DO ATAQUE:

Acesso temporário ao site e sistemas da Energoatom foi interrompido.

Não houve danos diretos às operações das usinas nucleares.

Enfatizou a vulnerabilidade de infraestruturas críticas em zonas de guerra.

Causou maior tensão entre Ucrânia e Rússia, com impacto na cibersegurança internacional.



MEDIDAS TOMADAS E SOLUÇÕES:

A Energoatom conseguiu restaurar os sistemas afetados rapidamente.

Foram implementadas camadas adicionais de proteção contra futuros ataques DDoS.

Investimento em Cibersegurança:

A Ucrânia, com apoio de aliados internacionais, aumentou o monitoramento e a proteção de infraestruturas críticas.

ATAQUE À OMS

Data: Abril de 2020

Alvo: Organização Mundial da Saúde (OMS)

Tipo de Ataque: Phishing e tentativa de roubo de credenciais.

Contexto: A OMS estava liderando os esforços globais contra a pandemia de Covid-19



COMO O ATAQUE ACONTECEU

Método:

Hackers criaram sites falsos imitando o portal da OMS para roubar dados de login.

Ataques de engenharia social direcionados a funcionários da OMS.

Invasores:

Grupos de hackers organizados, possivelmente ligados a espionagem internacional.



MOTIVAÇÕES POR TRÁS DO ATAQUE

Exploração de vulnerabilidades durante o caos da pandemia.

Potencial tentativa de roubar informações sobre respostas à pandemia.

Hackers buscaram enfraquecer os esforços da OMS com o vazamento de dados sensíveis.





CONSEQUÊNCIAS E SOLUÇÕES

Nenhum dado crítico foi comprometido, mas o ataque aumentou a preocupação com a segurança digital.

A OMS em resposta, fortaleceu suas medidas de segurança cibernética com o apoio de parceiros como a ONU.

Esforços foram redobrados para educar funcionários sobre ameaças e melhorar sistemas de detecção de intrusões.

PARTICIPANTES

Felipe Gatti
RA: 824125546

Italo Gomes
RA: 824218750

Matheus Bovo
RA: 824138656

Rafael Cezar
RA: 82425725

Wesley Dos Santos
RA: 82422607

OBRIGADO
POR SUA ATENÇÃO