



Eduardo
Baptistella
824147595

Gabriel
Prieto
824142064

Otavio Paiva
824147017



ATAQUES

CIBERNÉTICOS



ATAQUES À HOT TOPICS

Em agosto de 2023, o varejista americano Hot Topic notificou seus clientes que haviam detectado tentativas automatizadas de terceiros não autorizados para fazer login nas contas dos clientes em seu site e aplicativo móvel. O ataque envolveu "credenciais de conta válidas (por exemplo, endereços de e-mail e senhas) obtidas de uma fonte de terceiros desconhecida".

DATA DO ATAQUE

Não há uma data específica para ataques generalizados, mas eventos significativos ocorreram ao longo dos anos, com destaque para incidentes notáveis que podem ter sido relatados em diferentes momentos.

TIPO DE ATAQUE

Os ataques a empresas como a Hot Topics podem incluir, mas não estão limitados a:

- Ransomware: Criptografia de dados para exigir um resgate.
- Phishing: Tentativas de obter credenciais e informações sensíveis por meio de e-mails fraudulentos.
- DDoS (Ataques de Negação de Serviço Distribuída): Sobrecarregar sistemas com tráfego excessivo para derrubar serviços.
- Exploração de Vulnerabilidades: Ataques que aproveitam falhas específicas em software ou hardware.

DESCRIÇÃO DO ATAQUE

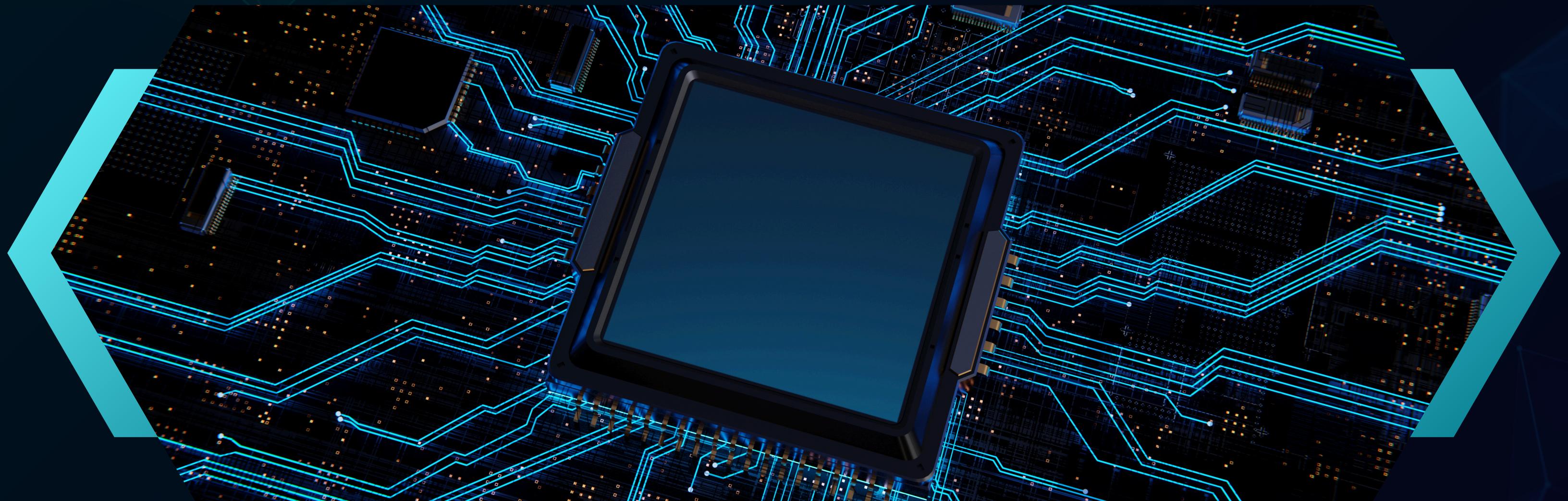
- Ransomware: Em 2022, a Hot Topics sofreu um ataque de ransomware que criptografou dados críticos, resultando na paralisação de operações e exigência de resgate.
- Phishing: Ataques de phishing direcionados a funcionários para obter acesso a sistemas internos.
- DDoS: Ataques que sobrecarregaram seus servidores, afetando a disponibilidade de seus serviços online.





VULNERABILIDADE

- CVE-2021-22986: Falha de segurança em serviços que pode ser explorada para obter acesso não autorizado.
- CVE-2022-22965: Vulnerabilidade no software utilizado para gerenciamento de dados que pode ser explorada por atacantes para comprometer sistemas.





TIPOS DE PROTEÇÃO

- Atualizações e Patches: Aplicar atualizações de segurança e patches para corrigir vulnerabilidades conhecidas.
- Segurança de Rede: Utilizar firewalls robustos, sistemas de prevenção de intrusões, e segmentação de rede para proteger contra ataques.



PREJUIZO

01

Perda de receita devido à interrupção dos serviços e custo de resgate no caso de ransomware.

02

Interrupção das operações diárias e necessidade de tempo e recursos significativos para a recuperação.





PROSPECT MEDICAL HOLDINGS



16 hospitais e mais de 160 clínicas e centros de saúde em quatro estados americanos estão com os atendimentos paralisados após um suposto ataque de ransomware. O golpe atingiu a rede da Prospect Medical Holdings e ainda causa transtornos, com direito à interrupção de serviços de emergência e suspensão de cirurgias eletivas em diferentes unidades.



Data do ataque

Agosto de 2023



Tipo de ataque

Ataque de ransomware
o ransomware bloqueia acesso ao sistema ou criptografa os dados. Os cibercriminosos exigem dinheiro de resgate de suas vítimas em troca da liberação dos dados.



Vulnerabilidades

Os ataques de ransomware também exploram vulnerabilidades para se espalharem dentro de uma rede, quando já estão dentro. Por exemplo, o ransomware Maze procura vulnerabilidades para explorar quando já esteja em uma rede, depois usa essas vulnerabilidades para infectar o maior número possível de máquinas.



PREJUIZO E COMO PROTEGER

Protecção

Fazer backup de dados, atualizar regularmente o software e usar uma abordagem de segurança Zero Trust são, todas elas, formas de evitar que as infecções por ransomware derrubem uma rede.

Prejuízo

Mais tarde, o grupo de ransomware Rhysida assumiu o crédito pelo ataque, explicando que foi capaz de roubar 500.000 números de Seguro Social, documentos corporativos e registros de pacientes. Muito provavelmente, a Prospect ainda está investigando o incidente e o impacto que teve nos pacientes.
Estimado em 69 milhões de Dólares



OBIGADO