**Fernando Henry Castro Gonçalves – 824210400**

**SCS (Sistemas Computacionais e segurança)**

**Campos Butantã**

**ATAQUE 1**

**Data** 08/2023

**Tipo:** Credencial Stuffing

**Descrição:** Varejista norte americana de roupas Hot Topic alerta os usuários sobre um ataque onde hackers utilizaram credenciais roubadas e acessaram a plataforma de recompensas da empresa várias vezes, potencialmente roubando os dados dos clientes

**Vulnerabilidade explorada:** Segundo a varejista, não foi possível identificar quais logins eram legítimos e quais eram não autorizados. O caso em específico não está no CVE, porém há casos semelhantes com os números: CVE-2024-45052 e CVE-2022-24044

**Impactos ou prejuízo:** Danos à imagem da empresa e exposição de informações sensíveis dos clientes.

**Tipo de Proteção que poderia ter sido aplicada para evita-lo:** Tal ataque não teria sido realizado caso os usuários usassem credenciais de login diferentes para os diversos sites que acessam na Internet. Se a empresa tivesse um sistema de segurança capaz de discernir os acessos legítimos dos acessos maliciosos o ataque também seria evitado.

Fonte: https://caveiratech.com/post/rede-de-varejo-hot-topic-revela-onda-de-ataques-de-credential-stuffing-3232562

**ATAQUE 2**

**Data:** 03/08/2023

**Tipo:** Ataque de Ransomware

**Descrição:** Centenas de unidades de saúde foram paralisadas em estados norte-americanos após um suposto ataque de ransomware. O alvo foi a rede da Prospect Medical Holdings. A empresa responsável afirmou já ter passado por situações semelhantes anteriormente.

Além do roubo de informações sensíveis de clientes, foram sequestrados dados críticos para o funcionamento da empresa. Para evitar maiores danos, a empresa decidiu manter os sistemas tecnológicos desligados.

Agentes do governo foram acionados, assim como entidades de segurança cibernética terceirizadas. Empresa garantiu que, após o incidente**,** tomou as ações preventivas para evitar casos futuros.

**Vulnerabilidade explorada:** A vulnerabilidade em específico não foi divulgada. Mas já houveram casos semelhantes envolvendo ataques cibernéticos à empresa, o que nos leva a deduzir que o sistema de segurança cibernético precisa ser aprimorado para evitar novos incidentes.

**Impactos e/ou prejuízo:** Além do prejuízo à imagem da instituição, é possível estimar que a perda esteja em torno de 800 milhões, podendo chegar a 1 bilhão de dólares. Um ataque semelhante à Change Healthcare, processadora de transações de cobrança do UnitedHealth Group,uma das maiores operadores de seguro saúde dos Estados Unidos, teve impacto de US$ 872 milhões em seu lucro do primeiro trimestre de 2024

**Tipo de proteção que poderia ter sido aplicada para evita-lo:** Caso a empresa possuísse uma prática de backup, o sequestro de dados não seria um problema tão crítico. Além disso, o ransomware pode ter sido colocado no sistema de várias formas, portanto, o ideal seria que a empresa tivesse uma boa prática de conscientização aos funcionários sobre não clicar em links suspeitos ou entrar em sites desconhecidos, além de aprimorar seu sistema de segurança com um todo.

Fonte: <https://www.cisoadvisor.com.br/ataque-a-unitedhealth-group-causa-prejuizo-de-us-872-milhoes/>

<https://www.cybersecuritydive.com/news/ransomware-hospitals/690130/>