João Vitor Cordeiro Lopes RA: 82429891 SCS-Butantã noturno

Ataque à LastPass (2022-2023)

Sobre a empresa:

A LastPass é uma empresa de gerenciamento de senhas amplamente utilizada por indivíduos e empresas para armazenar e proteger credenciais de login. Ela oferece ferramentas para criação de senhas fortes e para sincronização segura de senhas em diferentes dispositivos. Fundada em 2008, a LastPass foi adquirida pela LogMeIn, e sua base de usuários cresceu significativamente, tornando-se um dos alvos mais atraentes para cibercriminosos devido à quantidade de dados sensíveis que armazena.

Data: O ataque começou em agosto de 2022, e novos desdobramentos foram revelados até março de 2023.

Tipo de Ataque: Cadeia de fornecimento e execução remota de código (RCE).

Descrição: A LastPass, uma das principais empresas de gerenciamento de senhas, foi alvo de um ataque cibernético de cadeia de fornecimento, onde os invasores comprometeram um software de terceiros utilizado por um engenheiro da DevOps da empresa. Os invasores instalaram um malware de tipo keylogger no dispositivo do engenheiro, capturando suas credenciais de autenticação multifatorial (MFA). Depois de obter a senha-mestra do engenheiro, o invasor acessou cofres de senhas corporativos, o que permitiu a extração de backups e chaves de criptografia de clientes armazenados em nuvem.

Vulnerabilidade explorada: A LastPass não divulgou publicamente a vulnerabilidade específica explorada no software de terceiros. No entanto, vulnerabilidades de execução remota de código, como o **CVE-2022-30190** (vulnerabilidade do Microsoft Support Diagnostic Tool - MSDT), foram amplamente exploradas em ataques semelhantes em 2022.

Impacto: O impacto foi significativo, afetando milhões de usuários da LastPass. Dados críticos, incluindo senhas criptografadas, foram comprometidos, o que causou grande preocupação em termos de segurança e obrigou a empresa a revisar suas práticas de proteção de dados. A LastPass sofreu danos à sua reputação, enquanto os clientes temiam a exposição de suas senhas. A empresa enfrentou dificuldades para restaurar a confiança dos usuários e possíveis multas.

Proteção recomendada:

1. **Verificar fornecedores de software**: Muitas vezes, empresas usam programas de outros fornecedores que podem ter falhas de segurança. É importante avaliar e testar esses programas regularmente para garantir que eles não estão vulneráveis.
2. **Monitorar computadores de funcionários críticos**: No caso da LastPass, o computador de um engenheiro foi invadido. Monitorar o uso dos dispositivos das pessoas que têm acesso a informações sensíveis e alertar sobre atividades suspeitas pode impedir que um invasor obtenha dados valiosos.
3. **Proteger as senhas principais**: Usar senhas fortes e de preferência dispositivos de autenticação física (como chaves USB específicas para autenticação) pode proteger melhor os dados. Não confiar apenas em senhas digitadas ou em métodos básicos de segurança.

Ataque ao TruePill (2023)

Sobre a empresa:

TruePill é uma plataforma de serviços de saúde digital que facilita a telemedicina e entrega de medicamentos diretamente ao consumidor. Fundada em 2016, a empresa fornece soluções para empresas de saúde e farmacêuticas, oferecendo tanto consultas médicas online quanto uma rede de farmácias. Com o crescimento da telemedicina, o TruePill tornou-se um alvo significativo para ataques cibernéticos devido à natureza dos dados sensíveis que armazena.

Data: Ocorreu em agosto de 2023.

Tipo de Ataque: Violação de dados (data breach).

Descrição: O TruePill, uma empresa focada em soluções de telemedicina e prescrição online, foi vítima de um ataque cibernético que resultou na exposição de dados pessoais e médicos de mais de 2,3 milhões de pacientes. Os invasores conseguiram acessar arquivos contendo informações como nomes de pacientes, dados demográficos, medicamentos prescritos e os nomes dos médicos responsáveis pelas prescrições. A empresa não detalhou como o ataque ocorreu, mas enfrentou um processo coletivo por suposta falta de criptografia adequada de dados sensíveis.

Vulnerabilidade explorada: Embora o TruePill não tenha fornecido detalhes específicos sobre a vulnerabilidade explorada, é provável que o ataque tenha explorado falhas na criptografia de dados armazenados, uma vulnerabilidade comum em muitos incidentes de violação de dados. Vulnerabilidades conhecidas relacionadas à exposição

de dados incluem o **CVE-2021-26084** (Confluence), que explora falhas em sistemas de gerenciamento de conteúdo.

Impacto: A violação expôs dados altamente sensíveis de saúde, o que gerou consequências jurídicas graves para a empresa. Além disso, a TruePill enfrentou um processo coletivo de clientes afetados e danos significativos à sua reputação. O ataque destacou as vulnerabilidades no setor de saúde e a necessidade de medidas rigorosas de proteção de dados.

Proteção recomendada:

1. **Criptografar dados sensíveis**: Isso significa proteger informações como dados de pacientes ou usuários para que, se alguém conseguir acesso indevido, os dados não sejam facilmente lidos ou utilizados. Mesmo que os invasores acessem os sistemas, eles não conseguirão usar as informações de forma direta.
2. **Limitar o acesso a dados importantes**: Nem todos os funcionários ou sistemas precisam ter acesso a dados sensíveis. Controlar quem pode ver, modificar ou baixar esses dados pode reduzir o impacto de um possível ataque.
3. **Manter um monitoramento contínuo**: Usar ferramentas para observar constantemente o que está acontecendo dentro do sistema da empresa ajuda a identificar e bloquear ataques assim que eles começam, antes que causem grandes danos.