Your IT Company

Relatório Técnico - DOM-Based Extension Clickjacking

Sumário

1. Visão Geral da Ameaça

O Clickjacking, também chamado de UI Redressing, é uma técnica conhecida desde 2008, quando pesquisadores demonstraram como usuários poderiam ser induzidos a clicar em botões invisíveis dentro de iframes. Ao longo do tempo, mecanismos de defesa como X-Frame-Options e Content-Security-Policy (CSP) foram criados e amplamente adotados, tornando o clickjacking tradicional (iframe-based) menos impactante.

Entretanto, o cenário mudou com a popularização das extensões de navegador. Hoje, elas são responsáveis por gerenciar dados extremamente sensíveis, como credenciais, senhas de uso único (TOTP), dados pessoais, informações de cartão de crédito e até passkeys. O DOM-Based Extension Clickjacking surge exatamente nesse contexto, em vez de abusar de iframes, o atacante manipula elementos injetados no DOM pelas próprias extensões, tornando-os invisíveis e sobrepondo-os a elementos comuns da interface, como banners de cookies ou captchas.

O impacto é imediato, com um único clique, o atacante pode forçar o preenchimento automático de informações e exfiltrar esses dados para sua infraestrutura. Esse ataque, revelado publicamente na DEF CON 33 em agosto de 2025, demonstrou que 10 dos 11 principais gerenciadores de senhas do mercado eram vulneráveis, afetando aproximadamente 40 milhões de usuários ativos.

Em resumo, a Clickjacking não morreu, apenas migrou para uma superfície de ataque. A gravidade aumentou, pois as extensões têm privilégios muito maiores que páginas web comuns. O risco é real para usuários finais, empresas e desenvolvedores**.**

2. Modus Operandi

O DOM-Based Extension Clickjacking funciona explorando a interface do usuário injetada por extensões. O atacante não precisa quebrar criptografia ou invadir servidores, ele apenas explora o comportamento de autofill das extensões, manipulando o DOM da página.

2.1. Passo a passo do ataque

- **Criação do site malicioso**
  - O atacante insere elementos familiares (ex: banners de cookies, captchas de verificação, newsletters).
  - Estes servem como *isca visual* para induzir o clique.
- **Injeção de formulários invisíveis**
  - Campos de login, dados pessoais ou cartões de crédito são criados em segundo plano.
  - A opacidade (opacity:0.001) ou sobreposição garante invisibilidade.
- **Forçar foco**
  - O campo recebe um focus() em loop, fazendo com que o menu de autofill da extensão apareça.

Classificação: Público

- **Captura pelo clique do usuário**
  - O clique no banner falso é redirecionado para o menu invisível da extensão.
  - Isso preenche automaticamente os campos preparados pelo atacante.
- **Exfiltração dos dados**
  - O conteúdo preenchido é coletado por console.log ou enviado via XMLHttpRequest para o servidor do atacante.

2.2. Variantes do ataque

- **Extension Element**: manipulação direta da interface da extensão.
- **Root Element**: ajuste de opacidade no elemento raiz da extensão.
- **Child Element:** manipulação de elementos filhos (com Shadow DOM aberto).
- **Parent Element (BODY/HTML)**: invisibilidade de todo o corpo da página.
- **Overlay (Parcial/Completo)**: sobreposição de elementos falsos, permitindo cliques pass-through.
- **Positioning**: posicionamento da UI sob o cursor ou em locais fixos de interação esperada

3. MITRE ATT&CK

O ataque pode ser mapeado em várias fases do framework MITRE ATT&CK:

Fase	Técnica	ID	Descrição Técnica	Aplicação no Ataque
Execução	User Execution: Malicious Click	T1204.001	Indução ao clique em elementos falsos.	Clique em banner ou captcha falso.
Defesa	UI Redressing (Clickjacking)	T1204.002	Manipulação de interface para enganar o usuário.	Uso de opacity, overlays e pointer-events:none.
Coleta	Input Capture	T1056.003	Captura de entradas do usuário ou autofill.	Dados preenchidos invisivelmente em formulários falsos.
Credenciais	Steal Web Session Cookie	T1539	Roubo de cookies de sessão.	Dados preenchidos invisivelmente em formulários falsos.

Classificação: Público

Credenciais	Use Alternate Auth Material	T1550.004	Uso de tokens ou materiais alternativos de autenticação.	Reuso de TOTP, tokens e passkeys.
Impacto	Account Manipulation	T1098	Alteração de contas ou credenciais.	Inclusão de passkeys ou sessões não autorizadas.

4. Diamond Model

Por que o Diamond Model é importante?

Criado para estruturar a compreensão de ciberataques, o Diamond Model organiza a análise em quatro vértices: **Adversary, Capability, Infrastructure, Victim**. Ele ajuda a responder perguntas cruciais: quem está atacando, com que capacidade, usando qual infraestrutura e contra quem.

Essa metodologia é essencial em **Threat Intelligence** porque permite correlacionar campanhas, prever possíveis alvos e priorizar medidas de defesa. Ao invés de analisar apenas o **"como"** do ataque, o Diamond Model conecta o **quem, o como, o onde e o alvo**, fortalecendo o entendimento estratégico.

Adversário: Pesquisadores maliciosos, atores de crime cibernético ou APTs interessados em credenciais sensíveis.

Capacidade: Técnicas avançadas de manipulação do DOM, sobreposição de UI, automação de exfiltração.

Infraestrutura: Sites maliciosos preparados com overlays, exploração de vulnerabilidades XSS em domínios legítimos, demo sites públicos de PoC.

Vítimas: Usuários de gerenciadores de senhas, estimados em ~40 milhões de instalações ativas.

5. IoCs e Artefatos

Indicadores conhecidos (PoCs / Demo Sites)

- https://websecurity.dev/password-managers/dom-based-extension-clickjacking/
- https://websecurity.dev/overlay/login.html
- https://websecurity.dev/overlay/index2.html

Classificação: Público

- **Artefatos técnicos**
  - Uso de document.querySelector().style.opacity = 0
  - Configuração de pointer-events:none em elementos de sobreposição.
  - Criação de formulários invisíveis (<form style="opacity:0.001">) para capturar dados.
  - Exfiltração via XMLHttpRequest ou console.log para coleta local.

Esses indicadores são mais úteis como exemplos técnicos para caçadores de ameaças do que como bloqueios diretos, já que podem ser facilmente modificados.

6. Extensões e Versões Afetadas

- **Vulneráveis:**
  1. **1Password:** <= 8.11.7.2
  2. **Bitwarden:** <= 2025.8.0
  3. **iCloud Passwords:** <= 3.1.25
  4. **Enpass:** <= 6.11.5
  5. **LastPass:** <= 4.146.3
  6. **LogMeOnce:** <= 7.12.4
  7. **KeePassXC-Browser:** <= 1.9.9.2
- **Corrigidas:**
  - **Dashlane:** v6.2531.1 (corrigido em agosto de 2025)
  - **Enpass:** 6.11.6 (corrigido em agosto de 2025)
  - **Keeper:** 17.2.0 (corrigido em julho de 2025)
  - **NordPass:** 5.13.24 (corrigido em fevereiro de 2024)
  - **ProtonPass:** 1.31.6 (corrigido em dezembro de 2023)
  - **RoboForm**: 9.7.6 (corrigido em julho de 2024)

Essa listagem mostra que, mesmo após 4 meses da notificação inicial (abril de 2025), diversos fornecedores ainda não corrigiram suas extensões.

Classificação: Público

7. Recomendações de Mitigação e Detecção

- **Usuários**
  - Mantenha extensões atualizadas: habilitar atualizações automáticas.
  - Desative o autofill manual e use copiar/colar quando possível.
  - Configure “on click” em navegadores Chromium para limitar acesso de extensões por site.
  - Evite armazenar TOTP junto com credenciais no mesmo gerenciador.
- **Desenvolvedores de extensões**
  - Implementar Closed Shadow DOM para impedir manipulação.
  - Monitorar via MutationObservers alterações suspeitas em estilos.
  - Detectar overlays/z-index anômalos antes de exibir menus de autofill.
  - Avaliar uso de pop-ups dedicados para preenchimento sensível (mesmo que menos conveniente).
  - **Ambientes corporativos**
  - Aplicar MDM/GPO para restringir extensões instaladas.
  - Monitorar tráfego em busca de padrões suspeitos de exfiltração (XMLHttpRequest anômalos).
  - Auditar extensões críticas regularmente e considerar soluções independentes (desktop/mobile) em vez de dependência total de extensões de navegador.

8. Considerações Finais

O **DOM-Based Extension Clickjacking** demonstra como técnicas aparentemente antigas podem ganhar nova relevância em superfícies modernas. Enquanto o clickjacking tradicional foi praticamente neutralizado com políticas de segurança em cabeçalhos, sua versão voltada para extensões é significativamente mais perigosa, pois atua sobre componentes com privilégios elevados e dados críticos. O caso reforça que:

- A segurança deve ser pensada desde o design da extensão.
- Clickjacking ainda é relevante e deve voltar a ser tratado como risco crítico.
- O problema não se limita somente a gerenciadores de senhas, mas também a carteiras de criptomoedas, extensões de notas seguras e outras que manipulam dados sensíveis também estão em risco.

Classificação: Público

9. Referências Técnicas

1. https://marektoth.com/blog/dom-based-extension-clickjacking/
2. https://websecurity.dev/password-managers/dom-based-extension-clickjacking/
3. https://www.thehackernews.com/2025/08/dom-based-extension-clickjacking.html
4. https://www.securityweek.com/password-managers-vulnerable-to-data-theft-via-clickjacking/
5. https://www.nudgesecurity.com/post/dom-based-extension-clickjacking-vulnerabilities-in-popular-password-managers

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

Produzido por: Equipe de Threat Intelligence

Classificação: Público