Hackers abusam de truques de texto RTL/LTR e falhas do navegador para

Data: 2025-09-18 06:49:52

Autor: Inteligência Against Invaders

Pesquisadores de segurança cibernética dos laboratórios de ameaças de Varonis descobriram uma vulnerabilidade persistente que permaneceu sem tratamento por mais de uma década, permitindo que os invasores explorem o manuseio do navegador de escrúpulos de texto da direita para a esquerda (RTL) e da esquerda (LTR) para criar URLs deceptivos.

Essa técnica, conhecida como BIDI Swap, permite que os atores de ameaças criem links maliciosos que parecem legítimos a usuários inocentes, tornando -a uma ferramenta eficaz para campanhas de phishing.

Infográfico mostrando diferentes tipos de ataques de falsificação, incluindo site, email, IP, GPS e falsificação de man-in-the-middle

Compreendendo o método de ataque de troca de bidi

A técnica de troca BIDI explora as fraquezas em como os navegadores implementam o algoritmo bidirecional, parte do padrão Unicode projetado para exibir os scripts LTR e RTL mistos corretamente.

Embora esse algoritmo geralmente lida com os nomes de domínio corretamente, ele luta com subdomínios e parâmetros de URL contendo instruções de texto misto.

Os invasores aproveitam essa limitação para criar URLs onde o texto exibido não corresponde ao destino real, mascarando efetivamente Links maliciosos por trás de endereços aparentemente confiáveis.

A vulnerabilidade se torna particularmente perigosa quando combinada com estruturas inteligentes de domínio.

Por exemplo, os atacantes podem construir URLs usando caracteres hebraicos ou árabes ao lado de subdomínios ingleses, fazendo com que os navegadores exibam endereços confusos ou enganosos que parecem levar a sites legítimos como “Varonis.com” quando realmente redirecionam para domínios maliciosos.

Exemplo de domínios de ataque de homografia de punycode e detalhes correspondentes do certificado SSL ilustrando técnicas de falsificação de domínio

A BIDI Swap se baseia nas técnicas anteriores de exploração Unicode que atormentam a segurança

da Web há anos.

Os ataques de homografia de Punycode representam um desses antecessores, onde os invasores usam nomes de domínio internacionalizados contendo caracteres visualmente semelhantes de diferentes alfabetos.

Por exemplo, domínios como “Aprpple.com” usando caracteres cirílicos em vez de letras latinas podem enganar os usuários a acreditar que estão visitando sites legítimos.

As explorações de substituição do RTL apresentam outro vetor de ataque histórico, onde os caracteres Unicode especiais deslizam a direção do texto no meio da corda.

Esses ataques podem disfarçar extensões de arquivos, fazendo com que os executáveis ??maliciosos apareçam como PDFs inofensivos, transformando o “malware.exe” no que parece ser “malware.pdf” através da colocação estratégica de caracteres.

Esforços de resposta e mitigação do navegador

As implementações atuais do navegador mostram níveis variados de proteção contra ataques de troca de bidi.

O recurso de “sugestão de navegação para os URLs de navegação do Chrome fornece proteção limitada, sinalizando principalmente domínios conhecidos como” google.com “, permitindo que muitos endereços falsificados passem sem detectar.

O Firefox adota uma abordagem diferente, destacando os principais componentes do domínio na barra de endereços, facilitando a identificação de links suspeitos.

O Microsoft Edge reconheceu o problema, mas não implementou alterações significativas na representação da URL.

Curiosamente, o agora descontinuado Navegador de arco Proteção efetiva demonstrada distinguindo claramente entre domínios legítimos e potencialmente falsificados por meio de indicadores visuais aprimorados.

Organizações e indivíduos podem implementar várias medidas defensivas contra esses sofisticados ataques de falsificação de URL.

A educação do usuário permanece crucial, enfatizando a importância de examinar cuidadosamente os URLs antes de clicar, especialmente aqueles que contêm scripts mistos ou combinações incomuns de caracteres.

Os usuários devem passar os links para revelar destinos reais e verificar a consistência do domínio.

As soluções técnicas incluem incentivar os desenvolvedores do navegador a aprimorar as proteções existentes, como destaque de domínio aprimorado e sistemas de detecção de aparência mais abrangente.

Equipes de segurança deve implementar camadas adicionais de proteção, incluindo sistemas de filtragem de email que podem detectar tentativas de falsificação baseadas em Unicode e programas

de treinamento do usuário que abordam especificamente essas ameaças emergentes.

A persistência das vulnerabilidades de troca de bidi nos principais navegadores destaca o desafio contínuo de equilibrar o apoio à internacionalização com os requisitos de segurança.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.