6 ataques baseados em navegador para os quais todas as equipes de segu

Data: 2025-09-04 17:02:23

Autor: Inteligência Against Invaders

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]ataques de downgrade).

[IMAGEM REMOVIDA]a.fl_button {
cor de fundo: #5177b6;
borda: 1px sólido #3b59aa;
Cor: #FFF;
alinhamento de texto: centro;
decoração de texto: nenhum;
raio da borda: 8px;
exibição: bloco embutido;
tamanho da fonte: 16px;
peso da fonte: negrito;
margem: 4px 2px;
cursor: ponteiro;
preenchimento: 12px 28px;
}

.fl_ad {
cor de fundo: #f0f6ff;
largura: 95%;
margem: 15px auto 15px auto;
raio da borda: 8px;
borda: 1px sólido #d6ddee;
sombra da caixa: 2px 2px #728cb8;
altura mínima: 200px;
Display: Flex;
alinhar itens: centro;
}

.fl_lef>a>img {
margem superior: 0px !importante;
}

.fl_rig>p {
tamanho da fonte: 16px;
}

.grad-text {
imagem de fundo: gradiente linear (45 graus, var (–amanhecer-vermelho), var (–íris) 54%, var (–aqua));

```
-webkit-text-fill-color: transparente;
-webkit-background-clip: texto;
clipe de fundo: texto;
}

.fl_rig h2 {
tamanho da fonte: 18px!importante;
peso da fonte: 700;
Cor: #333;
altura da linha: 24px;
família de fontes: Geórgia, times new roman, Times, serif;
exibição: bloco;
alinhamento de texto: esquerda;
margem superior: 0;
}

.fl_lef {
exibição: bloco embutido;
altura mínima: 150px;
largura: 25%;
preenchimento: 10px 0 10px 10px;
}

.fl_rig {
preenchimento: 10px;
exibição: bloco embutido;
altura mínima: 150px;
largura: 100%;
alinhamento vertical: superior;
}

.fl_lef>a>img {
raio da borda: 8px;
}

.cz-news-title-right-area ul {
preenchimento à esquerda: 0px;
}

@media tela e (largura máxima: 1200px) {
.fl_ad {
altura mínima: 184px;
}

.fl_rig>p {
margem: 10px 0;
}
}

@media tela e (largura máxima: 1100px) {
```

```
.fl_lef {
largura: 27%;
}
}

@media tela e (largura máxima: 990px) {
.fl_lef>a>img {
largura: 100%;
}
}

@media tela e (largura máxima: 600px) {
.fl_lef>a>img {
Largura: Auto;
}

.fl_ad {
exibição: bloco;
}

.fl_lef {
largura: 100%;
preenchimento: 10px;
}

.fl_rig {
preenchimento: 0 10px 10px 10px;
largura: 100%;
}
}

@media tela e (largura máxima: 400px) {
.cz-story-navigation ul li:first-child {
preenchimento à esquerda: 6px;
}

.cz-story-navigation ul li:último-filho {
preenchimento à direita: 6px;
}
}
```

2. Entrega de código malicioso (também conhecido como. ClickFix, FileFix, etc.)

Uma das maiores tendências de segurança no ano passado foi o surgimento da técnica de ataque conhecida como ClickFix.

Originalmente conhecidos como “CAPTCHA falso”, esses ataques tentam induzir os usuários a executar comandos maliciosos em seus dispositivos – normalmente resolvendo alguma forma de desafio de verificação no navegador.

Na realidade, ao resolver o desafio, a vítima está copiando código malicioso da área de transferência da página e executando-o em seu dispositivo. Normalmente, ele fornece à vítima instruções que envolvem clicar em prompts e copiar, colar e executar comandos diretamente na caixa de diálogo Executar do Windows, Terminal ou PowerShell.

Variantes como Correção de arquivo também surgiram que, em vez disso, usam a barra de endereços do Explorador de Arquivos para executar comandos do sistema operacional, enquanto exemplos recentes viram esse ataque se ramificar para Mac através do terminal macOS.

Mais comumente, esses ataques são usados para entregar infostealer malware, usando cookies e credenciais de sessão roubada para acessar aplicativos e serviços de negócios.

Assim como o phishing moderno de credenciais e sessões, os links para páginas maliciosas são distribuídos em vários canais de entrega e usando uma variedade de iscas, incluindo a representação de CAPTCHA, o Cloudflare Turnstile, a simulação de um erro ao carregar uma página da Web e muito mais.

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]É muito fácil para os invasores comprarem e adicionarem atualizações maliciosas às extensões existentes, passando facilmente pelas verificações de segurança da loja virtual de extensão).

As notícias sobre compromissos baseados em extensões têm aumentado desde o Extensão Cyberhaven foi hackeado em dezembro de 2024, junto com pelo menos 35 outras extensões. Desde então, tem havido relatórios regulares sobre extensões de roubo de dados Personificar marcas legítimase impactando milhões de usuários.

As permissões de extensão de navegador arriscadas incluem amplo acesso a dados, a capacidade de modificar o conteúdo do site, rastrear a atividade do usuário, capturar capturas de tela e gerenciar guias ou solicitações de rede. Permissões como “ler e alterar todos os dados em todos os sites” ou acesso a cookies e histórico de navegação são particularmente perigosas, pois podem ser exploradas para sequestro de sessão, roubo de dados, injeção de malware ou phishing.

Geralmente, seus funcionários não devem instalar extensões de navegador aleatoriamente, a menos que sejam pré-aprovadas por sua equipe de segurança. A realidade, no entanto, é que muitas organizações têm muito pouca visibilidade das extensões que seus funcionários estão usando e do risco potencial ao qual estão expostos como resultado.

Para lidar com extensões maliciosas, as ferramentas de segurança que operam no navegador podem rastrear as extensões do navegador implantadas, destacar permissões arriscadas, comparar com extensões maliciosas conhecidas, identificar versões fraudulentas/não oficiais de uma extensão legítima e destacar outras propriedades arriscadas comumente associadas a extensões maliciosas (por exemplo, extensões “Desenvolvedor”).

5. Entrega de arquivos maliciosos

Arquivos maliciosos têm sido uma parte essencial da entrega de malware e roubo de credenciais por

muitos anos. Assim como canais que não são de e-mail, como malvertising e ataques drive-by, são usados para fornecer phishing e iscas do ClickFix, os arquivos maliciosos também são distribuídos por meios semelhantes, deixando a detecção de arquivos maliciosos para verificações básicas de erros conhecidos, análise de sandbox usando um proxy (não tão útil no contexto de malware com reconhecimento de sandbox) ou análise de tempo de execução no endpoint.

Isso não precisa ser apenas executáveis maliciosos que lançam malware diretamente no dispositivo. Os downloads de arquivos também podem conter links adicionais que levam o usuário a conteúdo malicioso. Na verdade, um dos tipos mais comuns de conteúdo para download são os aplicativos HTML (HTAs), comumente usados para gerar páginas de phishing locais para capturar credenciais furtivamente. Mais recentemente, os invasores têm armado arquivos SVG para uma finalidade semelhante, executando como páginas de phishing independentes que renderizam portais de login falsos inteiramente do lado do cliente.

Mesmo que o conteúdo mal-intencionado nem sempre possa ser sinalizado na inspeção superficial de um arquivo, a gravação de downloads de arquivos no navegador é uma adição útil à proteção contra malware baseada em endpoint e fornece outra camada de defesa contra downloads de arquivos que executam ataques do lado do cliente ou redirecionam o usuário para conteúdo mal-intencionado baseado na Web.

6. Credenciais roubadas e lacunas de MFA

Este último não é tanto um ataque baseado em navegador, mas é um produto deles. Quando as credenciais são roubadas por meio de phishing ou malware infostealer, elas podem ser usadas para assumir contas sem MFA.

Este não é o ataque mais sofisticado, mas é muito eficaz. Você só precisa olhar para o ano passado Floco de neve comprometimentos de conta ou o Jira ataques no início deste ano para ver como os invasores aproveitam as credenciais roubadas em escala.

Com a empresa moderna usando centenas de aplicativos, a probabilidade de um aplicativo não ter sido configurado para MFA obrigatória (se possível) é alta. E mesmo quando um aplicativo foi configurado para SSO e conectado à sua identidade corporativa principal, “Logins fantasmas” locais podem continuar a existir, aceitando senhas sem necessidade de MFA.

Os logins também podem ser observados no navegador – na verdade, é o mais próximo de uma fonte universal de verdade quanto você saberá como seus funcionários estão realmente fazendo login, quais aplicativos estão usando e se a MFA está presente, permitindo que as equipes de segurança encontrem e corrijam logins vulneráveis antes que possam ser explorados por invasores.

Conclusão

Os ataques estão acontecendo cada vez mais no navegador. Isso o torna o lugar perfeito para detectar e responder a esses ataques. Mas, no momento, o navegador é um ponto cego para a maioria das equipes de segurança.

A plataforma de segurança baseada em navegador da Push Security fornece recursos abrangentes de detecção e resposta contra a principal causa de violações. O push bloqueia ataques baseados em navegador, como phishing AiTM, preenchimento de credenciais, pulverização de senha e

sequestro de sessão usando tokens de sessão roubados.

Você também pode usar o Push para encontrar e corrigir vulnerabilidades nos aplicativos que seus funcionários usam, como logins fantasmas, lacunas de cobertura de SSO, lacunas de MFA, senhas vulneráveis, integrações OAuth arriscadas e muito mais para fortalecer sua superfície de ataque de identidade.

Se você quiser saber mais sobre como o Push ajuda você a detectar e interromper ataques no navegador, Reserve algum tempo com um membro da nossa equipe para uma demonstração ao vivo.

Patrocinado e escrito por Segurança Push*.*