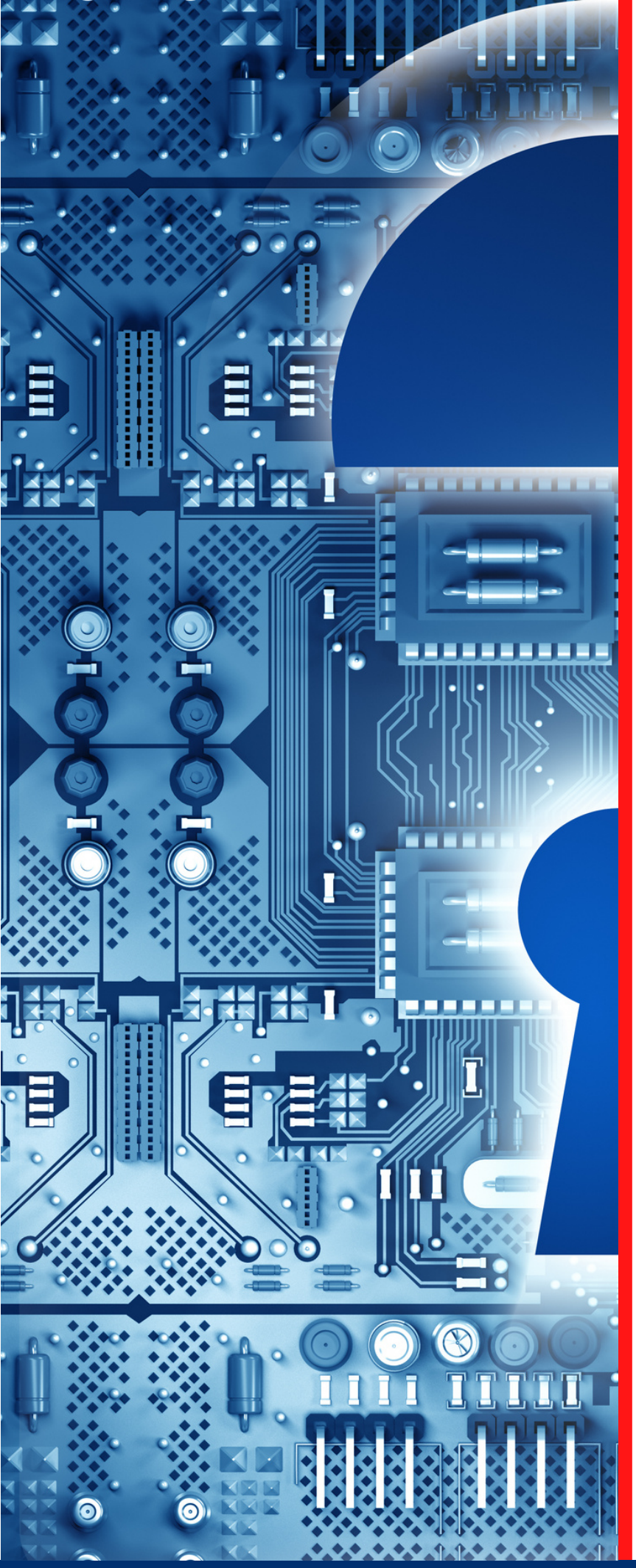


OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

07/2023

Ataques por notificações

Web Push

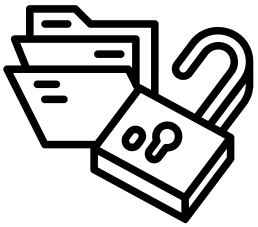
Textos: João Alberto Muniz Gaspar
Diagramação: Douglas Rocha de Oliveira
Produção: Secretaria de Segurança da Informação e Cibernética

Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.

TLP:CLEAR

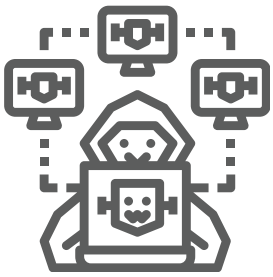
Ataques por notificações *Web Push*

O uso de notificações *Web Push* como vetor de ataque é cada vez mais comum. Essas notificações falsificam alertas legítimos normalmente para instalar *malwares* em equipamentos dos usuários a fim de coletar informações tanto do usuário como do sistema.



O *malware* instalado é capaz de exfiltrar diversas informações do sistema, como listas de processos, detalhes da unidade, números de série e outras informações da memória RAM, além de detalhes da placa gráfica. A ameaça também pode acessar dados de perfil de aplicativos, particularmente quando são acessados em navegadores da *web*, carteiras de criptomoedas, e dados pessoais do usuário, como credenciais de cartões de crédito.

O agravante das notificações *Web Push* é que elas são entregues em nível de sistema, e não em nível de navegador. A entrega em nível de sistema significa que as notificações podem ser recebidas mesmo com o navegador fechado. Além disso, as notificações também podem ser recebidas se o navegador não estiver no *site* em que o usuário aceitou as notificações.



Os ataques por notificações *Web Push* são preocupantes porque muitas vezes os usuários são induzidos a acreditar que a mensagem é legítima e, nesse caso, eles geralmente ignorarão quaisquer outros avisos de segurança, facilitando a ação maliciosa do atacante. Uma vez feito isso, os *hackers* têm acesso para executar as etapas do ataque propriamente dito, seja para implantar *ransomware* ou movimentar-se na rede da organização da vítima, visando atingir outros objetivos.

Explicando o que são notificações *Web Push*

As notificações *Web Push* são uma forma de enviar mensagens aos usuários de um *site* ou aplicativo da *web* mesmo quando eles não estão ativamente navegando no *site*. Essas notificações aparecem como pequenas caixas de diálogo *pop-up* em um dispositivo *desktop* ou móvel, geralmente no canto inferior direito ou superior esquerdo da tela, e podem conter informações como atualizações de conteúdo, promoções ou outras mensagens atraentes para o usuário.

Geralmente, para receber notificações *Web Push*, os usuários precisam optar por receber essas mensagens quando visitam um *site* pela primeira vez. Depois disso, o *site* pode enviar notificações diretamente ao navegador ou dispositivo do usuário, mesmo que ele não esteja com a janela do *site* aberta. As notificações *Web Push* são um recurso relativamente novo e foram criadas como uma alternativa aos *e-mails* de *marketing* e outras formas mais tradicionais de publicidade *online*.

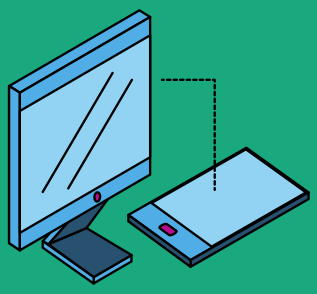
Por trás de um sistema de mensagens *push* da *web*, existem quatro componentes essenciais, que seguem abaixo.

1. ***Website*: *site* que solicita permissões adicionais para entregar notificações *push* ao usuário.**
2. **Servidor de aplicativos: entidade que envia mensagens *push* ao usuário por meio do serviço *push*.**
3. **Navegador (agente) do usuário: navegador da *web* que exibe a notificação *push* para o usuário. Em navegadores populares, a mensagem aparece com uma *tag* do tipo "XXXXXXX". Ressalte-se, novamente, que o navegador não necessita estar aberto para que a mensagem seja exibida.**
4. **Serviço *push*: componente *man-in-the-middle*[1], sempre ativo, que entrega as mensagens *push* ao navegador. Cada navegador usa um serviço *push* diferente.**

Vantagens e desvantagens de permitir notificações *Web Push*

épico

1) Vantagens



- As notificações *Web Push* são uma maneira fácil de receber mensagens pontuais e customizadas conforme os interesses definidos.
- Funcionam tanto no *smartphone* quanto em *desktop*.
- Ao contrário da mídia social ou do *marketing* por *e-mail*, não é necessário visitar um *site* específico ou abrir um aplicativo adicional para visualizar as notificações.

2) Desvantagens

- Possibilidade de receber anúncios não solicitados de terceiros: diversos *sites* vendem suas informações para redes de anúncios e terceiros (normalmente com o consentimento do usuário, que clicou na caixa de diálogo "permitir o compartilhamento de suas informações com *sites* parceiros"). Os afiliados aproveitam os dados dos usuários que optam por receber notificações e começam a enviar mensagens promocionais, redirecionam usuários para *sites* de anunciantes, ganham dinheiro com promoções *pay-per-click* (PPC) ou injetam *cookies* de outros afiliados para monetizar as vendas que acontecem nos navegadores dos usuários.
- Incômodo geral: o usuário pode precisar fechar manualmente diversos *pop-ups* sobre assuntos ou temas não relevantes antes de alcançar o que realmente interessa ver *online*.

- Pressão de largura de banda: quando a quantidade de notificações *push* se torna realmente agressiva, elas podem consumir parcela significativa da largura de banda disponível para seu dispositivo.
- Vetor de *malware*: código malicioso oculto nas notificações *Web Push* pode ter como objetivo fornecer uma enxurrada de mais anúncios (*malvertising*, como a que ocorreu na campanha SundownEK[2]) ou auxiliar *hackers* a obter acesso a rede ou dispositivo para exfiltrar informações ou dados pessoais.

Abuso de notificação *Web Push* por *hackers*

Para enviar as mensagens *push*, o servidor envia dados para o serviço *push*. Esses dados podem ser de qualquer característica e seus formatos são decididos pelo servidor de aplicativos.

De maneira geral, existem dois métodos que pessoas mal-intencionadas podem utilizar para incluir mensagens de *push* maliciosas em *sites*. São eles:

01	exploração de vulnerabilidade de um *site*: uma falha de segurança pode permitir que um código malicioso seja injetado no *site* de forma a redirecionar os usuários para uma página maliciosa.
02	pagar pela inclusão do código: método mais simples e muito utilizado pelos *hackers*, pois vários *sites*, especialmente os de *download* ilegal de jogos e filmes, além dos que contém conteúdo pornográfico, cooperam com os golpistas, e voluntariamente injetam o código de redirecionamento em seus *sites* em troca do pagamento de uma taxa.

Em qualquer um dos casos acima, o servidor de aplicativos estando comprometido enviará uma mensagem *push* com o objetivo de acionar ação abusiva no navegador do usuário.

A ação a ser realizada pelo usuário quando a mensagem *push* é recebida depende do navegador utilizado pelo usuário. Em alguns casos, o navegador apenas exibe uma notificação do sistema.

Por exemplo, o navegador pode ser aproveitado para exibir notificações com conteúdo malicioso que pode, por sua vez, apresentar *links* para *sites* fraudulentos.

Sinais de que ocorreu um ataque por notificação *Web Push* maliciosa

1. Anúncios e mensagens frequentes e não autorizadas, por vezes em áreas incomuns, como na área de trabalho, mesmo com o navegador fechado.
2. Página inicial do navegador alterada sem ação do usuário.
3. Diversos *sites* que eram acessados sem problemas passam a não ser exibidos corretamente ou ocorre redirecionamento para um outro endereço.

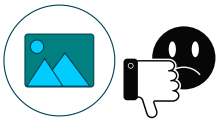
4 Recebimento de *pop-ups* que anunciam atualizações, ou *softwares* falsos, ou avisos de que o computador está infectado, seguidos de solicitações para instalar uma ferramenta de limpeza específica. Um dos ataques mais comuns têm sido uma notificação falsa que se disfarça de um alerta de segurança informando à vítima o que se supõe ser uma contaminação por vírus ou trojan e solicitando que o usuário clique em um botão para realizar um escaneamento do computador. Clicar na mensagem apresentada leva a um *site* falso, informando à vítima que foram detectadas várias ameaças em seu dispositivo e solicitando que se instale uma solução de segurança no sistema, o que pode ser feito clicando no *link* fornecido, o que acaba por instalar um *malware* no sistema da vítima.

5 Identificação de aplicativos ou programas no dispositivo, inclusive com atalhos, que não foram instalados pelo usuário.

Identificando uma notificação *Web Push* falsa

1 A mensagem tem erros, usando uma linguagem não profissional e apresentando incorreções gramaticais.

2 A mensagem tem logotipos ou imagens de má qualidade, que são bons indicadores de que o *pop-up* é falso.



3 A mensagem contém um *link* cuja URL não corresponde ao esperado. Por exemplo, instituição com domínio .com e as Mensagens propõe domínios semelhantes como .org ou .net provavelmente são falsas.

4 A mensagem se refere a um *software* que não está instalado no dispositivo.

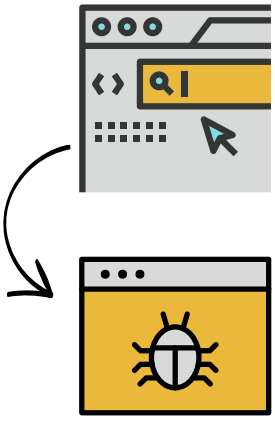
Mitigando riscos de ataques por notificação *Web Push*

A principal medida para evitar ser vítima de um ataque por notificação *Web Push* é nunca clicar em qualquer *link* fornecido em uma mensagem.

Deve-se sempre considerar que esse tipo de mensagem é uma farsa e que clicar em qualquer *link* apresentado provavelmente instalará um *malware* que permitirá que *hackers* acessem remotamente as informações em seu dispositivo e possivelmente comprometam ainda mais seu sistema.

Outra medida que pode ser adotada é impedir que uma notificação *Web push* seja enviada ao dispositivo desativando as notificações *Web push* no navegador. Pode-se bloquear todas as notificações ou apenas notificações de um *site* específico.

O método mais seguro é bloquear todas as notificações e permitir apenas os *sites* aos quais será permitido enviar notificações via navegador. Esse é um método mais proativo, em que a exceção é o recebimento de notificações.



Manter a configuração padrão, que é permitir que os *sites* solicitem autorização para enviar notificações, pode levar ao surgimento de mensagens indesejadas, o que implicará a necessidade de bloquear cada *site* ou domínio indesejado individualmente. De maneira geral, esse método é mais reativo, ou seja, somente após receber uma mensagem *push* indesejada é que o usuário saberá qual o domínio ou *site* que deve ser bloqueado.

Cabe relembrar que navegadores diferentes apresentam procedimentos distintos de configuração. Portanto, o usuário deverá verificar no suporte do seu navegador preferido, como proceder o bloqueio das notificações *Web push*.

O Departamento de Segurança da Informação e Cibernética (DSIC) recomenda aos usuários que:

- mantenham seus navegadores atualizados com as últimas versões e com todos os *patches* de segurança aplicados;
- configurem corretamente seus aplicativos, inclusive navegadores, com critérios de segurança que protejam a privacidade, a integridade e a disponibilidade; e
- ao identificar um incidente cibernético em sua organização, como um ataque de notificações *Web Push*, informe imediatamente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) de sua instituição.

O DSIC orienta aos integrantes da administração pública federal observar o previsto no Plano de Gestão de Incidentes Cibernéticos, particularmente quanto à prevenção. Ele está disponível em:

https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/plano-de-gestao-de-incidentes-ciberneticos-plangic/plangic.pdf

Por fim, o DSIC solicita, ainda, que propostas de temas, sugestões ou outras contribuições sejam encaminhadas ao e-mail educa.si@presidencia.gov.br para fomentar futuras emissões de OSICs.

TLP:CLEAR

Informações complementares

1. **Componente *man-in-the-middle*:** é uma técnica usada em cibersegurança onde um atacante se posiciona entre duas partes que estão se comunicando, interceptando e possivelmente manipulando as comunicações entre elas. são muitas vezes realizados em redes *Wi-Fi* públicas não seguras, onde o atacante pode facilmente interceptar o tráfego de rede.

2. **Campanha SundownEK:** foi uma campanha de *malware* que utilizou um *kit* de exploração de vulnerabilidades chamado *Sundown Exploit* Kit (EK). O *kit* de exploração de vulnerabilidades era usado para distribuir *malware* em computadores comprometidos através de *sites* infectados. O *Sundown* EK explorava vulnerabilidades em navegadores da *web* e em *plug-ins* populares, como o *Adobe Flash Player*, para instalar *malware* nos sistemas dos usuários. A campanha SundownEK foi uma das mais bem-sucedidas campanhas de *malware* em 2016 e 2017, tendo sido responsável por infectar milhares de computadores em todo o mundo.