As extensões do navegador estão sob os holofotes no Enterprise Security News recentemente devido à onda de ataques de OAuth a desenvolvedores de extensão cromo e ataques de exfiltração de dados. No entanto, até agora, devido às limitações que os fornecedores do navegador colocam no subsistema e nas extensões de extensão, considerou -se impossível que as extensões ganhassem controle total do navegador, muito menos o dispositivo.

Os pesquisadores da Squarex Dakshitaa Babu, Arpit Gupta, Sunkugari Tejeswara Reddy e Pankaj Sharma desmascaram essa crença ao demonstrar como os atacantes podem usar extensões maliciosas para escalar privilégios para conduzir um navegador completo e a aquisição de dispositivos, todos com interação mínima do usuário. Criticamente, a extensão maliciosa requer apenas recursos de leitura/gravação presentes na maioria das extensões do navegador na loja do Chrome, incluindo ferramentas comuns de produtividade como gramática, calendly e tear, dessensibilizando os usuários de conceder essas permissões. Essa revelação sugere que praticamente qualquer extensão do navegador poderia servir como um vetor de ataque se criado ou assumido por um atacante. Para o melhor de nossa compreensão, as extensões enviadas à loja Chrome solicitando esses recursos não são colocadas através do escrutínio de segurança adicional no momento da redação deste artigo.

O ataque de sincronização do navegador pode ser dividido em três partes: como a extensão

silenciosamente adiciona um perfil gerenciado pelo atacante, seqüestra o navegador e, eventualmente, ganha controle total do dispositivo.

O que você vai ler:

- Seqüestro de perfil
- Aquisição do navegador
- Seqüestro de dispositivo
    - Contato

Seqüestro de perfil

O ataque começa com um funcionário que instala qualquer extensão do navegador – isso pode envolver a publicação de um que se disfarça de ferramenta de IA ou assumindo extensões populares existentes que podem ter até milhões de instalações agregadas. A extensão então “silenciosamente” autentica a vítima em um perfil do Chrome gerenciado pelo espaço de trabalho do Google do atacante. Tudo isso é feito de maneira automatizada em uma janela de fundo, tornando todo o processo quase imperceptível à vítima. Uma vez que essa autenticação ocorre, o invasor tem controle total sobre o perfil recém -gerenciado no navegador da vítima, permitindo que ele pressione políticas automatizadas, como desativar a navegação segura e outros recursos de segurança.

Usando um ataque de engenharia social muito inteligente que explora domínios confiáveis, o adversário pode então aumentar ainda mais o ataque de seqüestro de perfil para roubar senhas do navegador da vítima. Por exemplo, a extensão maliciosa pode abrir e modificar a página de suporte oficial do Google sobre como sincronizar as contas de usuário para solicitar à vítima que execute a sincronização com apenas alguns cliques. Depois que o perfil é sincronizado, os invasores têm acesso total a todas as credenciais e ao histórico de navegação armazenado localmente. Como esse ataque utiliza apenas sites legítimos e não tem sinal visível de que ele foi modificado pela extensão, não acionará nenhum alarme em nenhuma solução de segurança que monitore o tráfego de rede.

Aquisição do navegador

Para alcançar uma aquisição completa do navegador, o invasor precisa essencialmente converter o navegador Chrome da vítima em um navegador gerenciado. A mesma extensão monitora e intercepta um download legítimo, como uma atualização de zoom, e o substitui pelo executável do atacante, que contém um token de inscrição e entrada do registro para transformar o navegador Chrome da vítima em um navegador gerenciado. Pensando que eles baixaram um atualizador de zoom, a vítima executa o arquivo, que acaba instalando uma entrada de registro que instrui o navegador a se tornar gerenciado pelo espaço de

trabalho do Google do atacante. Isso permite que o invasor obtenha controle total sobre o navegador da vítima para desativar os recursos de segurança, instalar extensões maliciosas adicionais, exfiltrar dados e até redirecionar silenciosamente os usuários para sites de phishing. Esse ataque é extremamente potente, pois não há diferença visual entre um navegador gerenciado e não gerenciado. Para um usuário regular, não há sinal revelador de que uma escalada de privilégio tenha ocorrido, a menos que a vítima esteja altamente consciente da segurança e se esforce para inspecionar regularmente as configurações do navegador e procurar associações com uma conta de espaço de trabalho do Google desconhecida.

Seqüestro de dispositivo

Com o mesmo arquivo baixado acima, o invasor pode inserir adicionalmente as entradas de registro necessárias para a extensão maliciosa para enviar mensagens de aplicativos nativos. Isso permite que a extensão interaja diretamente com aplicativos locais sem autenticação adicional. Depois que a conexão é estabelecida, os invasores podem usar a extensão em conjunto com o shell local e outros aplicativos nativos disponíveis para ativar secretamente a câmera do dispositivo, capturar áudio, gravar telas e instalar software malicioso – essencialmente fornecendo acesso total a todos os aplicativos e dados confidenciais no dispositivo.

O ataque de sincronização do navegador expõe uma falha fundamental na maneira como os perfis e navegadores gerenciados remotos são gerenciados. Hoje, qualquer pessoa pode criar uma conta de espaço de trabalho gerenciada vinculada a um novo domínio e uma extensão do navegador sem nenhuma forma de verificação de identidade, tornando impossível atribuir esses ataques. Infelizmente, a maioria das empresas atualmente tem visibilidade zero no navegador – a maioria não possui navegadores ou perfis gerenciados, nem qualquer visibilidade das extensões que os funcionários estão instalando frequentemente com base em ferramentas de tendência e recomendações de mídia social.

O que torna esse ataque particularmente perigoso é que ele opera com permissões mínimas e quase nenhuma interação do usuário, exigindo apenas uma etapa sutil de engenharia social usando sites confiáveis - tornando quase impossível para os funcionários detectarem. Embora incidentes recentes como a violação de Cyberhaven já tenham comprometido centenas, se não milhares de organizações, esses ataques exigiam engenharia social relativamente complexa para operar. A natureza devastadoramente sutil desse ataque – com um limiar extremamente baixo de interação do usuário – não apenas torna esse ataque extremamente potente, mas também lança luz sobre a possibilidade aterrorizante de que os adversários já estão usando essa técnica para comprometer as empresas hoje.

A menos que uma organização opte por bloquear completamente as extensões do navegador por meio de navegadores gerenciados, o ataque de sincronização do navegador ignorará completamente as listas negras existentes e as políticas baseadas em permissões. O fundador da Squarex, Vivek Ramachandran, diz: “Esta pesquisa expõe um ponto cego crítico

em segurança corporativa. As ferramentas de segurança tradicionais simplesmente não podem ver ou interromper esses ataques sofisticados baseados em navegador. O que torna essa descoberta particularmente alarmante é como ela arma, aparentemente inocente, extensões de navegador em ferramentas completas de aquisição de dispositivos, enquanto voam sob o radar de medidas de segurança convencionais como EDRs e SASE/SSE Secure Web Gateways. Uma solução de resposta à detecção de navegador não é mais apenas uma opção-é uma necessidade. Sem visibilidade e controle no nível do navegador, as organizações estão essencialmente deixando a porta da frente aberta aos atacantes. Essa técnica de ataque demonstra por que a segurança precisa "mudar" para onde as ameaças estão realmente acontecendo: no próprio navegador ".

A Squarex tem conduzido pesquisas de segurança pioneiras sobre extensões de navegador, incluindo as extensões sorrateiras de def 32 conversas: os artistas de fuga do MV3 que revelaram várias extensões maliciosas compatíveis com MV3. Esta equipe de pesquisa também foi a primeira a descobrir e divulgar o ataque de Oauth aos desenvolvedores de extensão do Chrome uma semana antes da violação de Cyberhaven. A Squarex também foi responsável pela descoberta dos ataques de remontagem de Mile, uma nova classe de ataques do lado do cliente que explora falhas arquitetônicas e ignora completamente todas as soluções seguras do Web Gateway. Com base nesta pesquisa, a solução de detecção e resposta do navegador da Squarex protege as empresas contra ataques avançados baseados em extensão, incluindo tentativas de seqüestro de dispositivos, realizando análises dinâmicas em todas as atividades de extensão do navegador em tempo de execução, fornecendo uma pontuação de risco a todas as extensões ativas em toda a empresa e identificar ainda mais os ataques aos quais eles podem ser vulneráveis.

Para obter mais informações sobre o ataque de sincronização do navegador, descobertas adicionais desta pesquisa estão disponíveis em **sqrx.com/research**.

Sobre Squarex

A Squarex ajuda as organizações a detectar, mitigar e caçar ameaças ao lado dos ataques da web que acontecem contra seus usuários em tempo real.

A solução de detecção e resposta do navegador da Squarex (BDR), adota uma abordagem focada no ataque à segurança do navegador, garantindo que os usuários da empresa sejam protegidos contra ameaças avançadas, como códigos QR maliciosos, phishing de navegador no navegador, malware macro baseado em macro e malware e macro e malwares e malware macro e macro e malware e macro e macro e malwares e malwares e malwares e malwares e malwares e mal-estar e mal-estar, " Outros ataques da Web que abrangem arquivos, sites, scripts e redes comprometidas.

Além disso, com a SquareX, as empresas podem fornecer aos contratados e trabalhadores remotos acesso seguro a pedidos internos, SaaS da empresa e converter os navegadores em dispositivos BYOD / não gerenciados em sessões de navegação confiáveis.

Contato

Chefe de PR

June Liew

Squarex

junice@sqrx.com