Novo clickfix ataque implanta página de notícias BBC falsa e verificação fa

Data: 2025-08-19 19:18:48

Autor: Inteligência Against Invaders

Os pesquisadores de segurança cibernética descobriram uma nova variante de ataque de clickfix

que personifica o conteúdo de notícias da BBC confiável e, ao mesmo tempo, alavancando

interfaces de verificação de gornilha falsificadas Cloudflare para coagir os usuários a executar PowerShell comandos.

Esta campanha, detalhada em análises recentes de fontes como News de segurança cibernética e ESET, explora a familiaridade do usuário com protocolos legítimos de segurança na web para fornecer uma variedade de cargas úteis de malware, incluindo InfoStealers, Ransomware e Trojans de acesso remoto.

O design do ataque ignora a detecção convencional de endpoint, contando com a execução de comando iniciada pela vítima, destacando uma mudança em direção aos vetores de exploração centrados no homem que evitam as defesas baseadas em assinatura.

A mecânica operacional dessa ameaça começa com pontos de entrada enganosos, como resultados de mecanismos de pesquisa manipulados ou anúncios on -line que redirecionam as vítimas para um portal de notícias da BBC meticulosamente clonado.

Este site fabricado incorpora artigos de furto de fontes autênticas, criando uma ilusão de credibilidade que reduz os usuários à interação prolongada.

Após a navegação, o site desencadeia um desafio de segurança simulado, imitando o processo de verificação humana da Cloudflare, completa com réplicas precisas de logotipos, IDs de raio e marketing verborrage, retirados diretamente da documentação oficial da Cloudflare.

Os usuários são solicitados a se envolver com uma caixa de seleção “Verifique se você é humano”, que cupra um script de PowerShell codificado de base64 para a área de transferência do sistema.

As instruções subsequentes orientam as vítimas a invocar a caixa de diálogo Executar do Windows via Windows + R, cole o conteúdo da área de transferência com Ctrl + V e execute via Enter, instalando involuntariamente malware como ladrão de lumma, escuro, assíncrono ou ntsupport.

Esse método capitaliza o comportamento reflexivo do usuário para resolver obstáculos técnicos aparentes, tornando -o altamente eficaz contra indivíduos tecnicamente experientes.

Proliferação rápida

Ao longo de 2024 e em 2025, os ataques de clickfix proliferaram dramaticamente, com o ESET

relatando um aumento de 517% no primeiro semestre de 2025, posicionando-o como o segundo vetor mais prevalente após o phishing e compreendendo quase 8% dos incidentes bloqueados.

O sucesso da técnica deriva de sua manipulação psicológica, atacando a urgência de acessar conteúdo de entidades autoritárias, como meios de comunicação ou serviços de segurança.

As variantes se estendem além da representação da BBC para imitar o software Microsoft, Google Chrome e do setor, diversificando mecanismos de entrega e segmentando setores vulneráveis a iscas personalizadas.

A diversidade de malware amplia ainda mais a ameaça, abrangendo criptominos e ameaças persistentes avançadas atribuídas a atores-estatais-nação, frequentemente implantados por medidas anti-forenses que detectam e abortam em ambientes virtualizados para obter detecções de antivírus zero.

A sofisticação de evasão é evidente na construção das cargas úteis, que freqüentemente recupera o código ofuscado de serviços de nuvem aparentemente benignos, incorporando verificações de tempo de execução para indicadores de sandbox.

Inovações recentes, como a variante FileFix identificadas pelo pesquisador Mr.D0X, adaptar a abordagem direcionando os usuários a colar comandos no Windows File Explorer Barra de endereço, contornando as mitigações de diálogo tradicionais de execução.

De acordo com o relatórioessas adaptações enfatizam a agilidade dos atacantes em resposta à crescente conscientização, com campanhas rastreadas pela Microsoft sob designações como o Storm-1865.

A integração de barras de progresso falsas e diálogos de confirmação aumenta o engano, tornando a diferenciação dos desafios genuínos da CloudFlare, extremamente desafiadores, sem escrutínio forense.

Medidas defensivas

Para combater esse cenário de ameaças em evolução, os especialistas em segurança defendem uma estratégia de defesa de várias camadas, enfatizando a educação e o endurecimento do sistema.

As principais recomendações incluem desativar a caixa de diálogo Executar do Windows por meio de objetos de política de grupo ou edições de registro para bloquear a invocação de comando não autorizada, juntamente com as ferramentas de análise comportamental que sinalizam execuções anômalas de PowerShell ou manipulações de quadro de transferência.

As organizações devem priorizar os programas de treinamento que destacam as bandeiras vermelhas, como interações não solicitadas no nível do sistema operacional durante a verificação da Web, uma prática nunca empregada por fornecedores legítimos como o CloudFlare.

As soluções avançadas de detecção e resposta de endpoint (EDR) com detecção de anomalias baseadas em aprendizado de máquina são essenciais para identificar indicadores pós-execução, mantendo os sistemas remendados contra vulnerabilidades relacionadas em ferramentas como o Windows File Explorer.

A resposta do setor de segurança cibernética tem sido proativa, com empresas como ProofPoint e ESET para melhorar os feeds de inteligência de ameaças e desenvolver regras heurísticas para o reconhecimento de padrões de clickfix.

Iniciativas mais amplas de conscientização sublinham que esses ataques exploram vulnerabilidades psicológicas em vez de falhas de software, necessitando de um foco em fatores humanos nas posturas de segurança.

À medida que as variantes continuam a surgir, misturando a representação com o engano interativo, a vigilância contínua através da caça de ameaças e compartilhamento de inteligência permanece primordial.

Esta campanha híbrida BBC-cloudflare exemplifica a crescente convergência de desinformação e entrega de malware, pedindo uma reavaliação de modelos de confiança nos ecossistemas digitais para mitigar os riscos de tais paradigmas insidiosos de engenharia social.

Encontre esta notícia interessante! Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas!**