Adtech abusado por atores de ameaças para espalhar anúncios malicioso

Data: 2025-09-17 11:25:56

Autor: Inteligência Against Invaders

Campanhas publicitárias maliciosas aumentaram a sofisticação, com os cibercriminosos explorando

e até operando empresas da Adtech para fornecer malware, ladrões de credenciais e esquemas de

phishing diretamente através de redes de anúncios convencionais.

Um aglomerado de empresas interconectadas – atravessando as empresas de shell, hospedadas em infraestrutura comprometida e registrada em massa por meio de um registrador notório – permitiu um ator prolífico de ameaça, apelidado de “Vane Viper”, para canalizar anúncios maliciosos em escala global.

Com negação plausível incorporada em todas as camadas, essas operações se tornaram um perigo persistente para empresas e consumidores.

A campanha de Vane Viper começa no topo corporativo: Adtech Holding, uma empresa de Chipre, controla subsidiárias, incluindo Propellerads, Propushme, Zeydoo, Notix e Adex.

Essas plataformas se apresentam como redes de anúncios do lado da oferta e da demanda legítimas, mas na prática o tráfego agregado de sites comprometidos e cliques de rota através de um sistema de distribuição de tráfego (TDS) para páginas de destino maliciosas.

Os registros corporativos rastreiam hélices para entidades de conchas em Chipre, a Ilha de Man e Londres, enquanto seu Registrador, URL Solutions (também conhecido como Pananames), está entre os registradores mais arriscados para registros de domínio em massa.

Por trás do brilho de banners brilhantes e pop-ups, encontra-se uma teia emaranhada de empresas de concha. As subsidiárias de hélices ocultam a propriedade por meio de empresas aninhadas, e sua infraestrutura se sobrepõe às redes de hospedagem da Webzilla-infamous para hospedar sites de pirataria e fazendas de fraude.

Os executivos vinculados a oligarcas russos e fraudadores condenados obscurecem ainda mais a responsabilidade legal, permitindo que as campanhas de malvertismo florescessem sob o disfarce de um modelo de publicidade convencional.

Táticas dinâmicas de cobertura

Em vez de confiar apenas em anúncios de banner, van endereçado Notificações de push do navegador e roteiros de trabalho de serviço para alcançar persistência e escapar de quedas.

Igor Limbakh aparece como diretor da empresa para Propellerads e Adtech Holding, e detém diretos

na Samoukale Enterprises (Adex), ITPUB, Finplat Technologies, Fourup e outros.

Quando os usuários visitam domínios comprometidos ou parecidos, eles são solicitados a aceitar notificações.

Uma vez concedidos, esses alertas no navegador oferecem um fluxo ininterrupto de anúncios maliciosos, gotículas de malware e iscas de phishing.

A Vane Viper é responsável por quase metade de todos os eventos de registro em massa feitos através da Atração de Soluções, desde janeiro de 2023.

Os domínios de push-notificação observados incluem na página-push.com e pushimg.com-alguns ativos por anos, enquanto milhares de domínios novos são registrados mensalmente para substituí-los desligados.

As técnicas dinâmicas de capno de captura garantem que os pesquisadores de segurança vejam conteúdo benigno, enquanto as vítimas reais são roteadas por meio de várias camadas de redirecionamento, scripts de envenenamento por história e filtros de geofencismo.

Os fluxos de tráfego originários de um bit.ly link podem cadear através de comandos TDS, proxies de parceiros e finalmente soltar um Trojan Apk bancário em Dispositivos Android. Ao adaptar as cargas úteis com base na região do usuário, tipo de dispositivo e fuso horário, essas campanhas maximizam as taxas de infecção e monetizam a cada clique.

Implicações para os usuários

A operação de Vane Viper ressalta falhas fundamentais no ecossistema de publicidade digital, que prioriza a escala e a lucratividade em relação à responsabilidade.

Aumento da contagem mensal de registro dos domínios desde janeiro de 2023, até a contagem mensal máxima de 3.500 domínios em outubro de 2024.

As empresas enfrentam riscos quando redes de anúncios legítimas, involuntariamente, fornecem páginas de colheita de malware ou colheita de credenciais aos funcionários, enquanto os consumidores encontram sites carregados de armadilhas que se disfarçam de videoclipes, portais de compras ou downloads de software.

As ferramentas de segurança tradicionais lutam contra a infraestrutura TDS encoberta e a persistência de notificação de push, dificultando a detecção e a remediação.

Para mitigar essas ameaças, as organizações devem adotar uma estratégia de defesa de várias camadas:

- Aplicar as políticas de segurança de conteúdo para restringir a execução de trabalhadores de serviço.
- Monitore a telemetria DNS para volumes de consultas anômalas indicativas de atividade maliciosa de TDS.
- Implementar controles mais rígidos do navegador em torno de notificações push e scripts de terceiros.
- Vet Adtech Partners para propriedade transparente, processos de relatórios de abuso e

procedimentos rápidos de remoção.

Por fim, a ascensão do Vane Viper ilustra como cibercriminosos reaproventaram a cadeia de suprimentos da Adtech em uma arma. Sem reformas sistêmicas-como requisitos padronizados de transparência, responsabilidade mais forte do registrador e protocolos de manipulação de abuso em todo o setor-o ciclo de malvertismo persistirá.

Para defensores e usuários da Internet, o desafio é claro: para recuperar a confiança na publicidade digital, o ecossistema da Adtech deve ser reengenhado para favorecer a responsabilidade sobre o alcance.

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