AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Bluekit : Le nouveau service de phishing qui mise sur l'IA et 40 modèles prêts à l'emploi.

Contenu

I. Contexte

Une nouvelle menace vient d'être identifiée par les chercheurs dans le paysage de la cybercriminalité. Surnommée Bluekit, ce kit de phishing de nouvelle génération se distingue par l'intégration d'outils d'intelligence artificielle, marquant une étape supplémentaire dans l'automatisation des cyberattaques.

II. Une plateforme "tout-en-un" pour cybercriminels

Bluekit n'est pas qu'un simple outil de création de pages frauduleuses, il s'agit d'une plateforme intégrée permettant de gérer l'intégralité du cycle de vie d'une attaque. Depuis un panneau de contrôle unique, les opérateurs peuvent :

- Acheter et enregistrer des noms de domaine ;
- Déployer des pages de phishing sophistiquées ;
- Gérer leurs campagnes et surveiller les sessions des victimes en temps réel.

Cette centralisation facilite grandement la tâche des personnes malveillantes, même les moins expérimentées, en leur offrant une infrastructure clé en main.

L'IA au service de l'ingénierie sociale

L'aspect le plus notable de Bluekit est son panneau "AI Assistant". Ce module supporte plusieurs modèles de langage de pointe, tels que GPT-4.1, Llama, Claude, Gemini et DeepSeek, pour aider à la rédaction des e-mails de phishing.

Bien que cette fonctionnalité soit un atout majeur, l'analyse de cette interface par les experts montre que l'outil est encore à un stade expérimental. Les contenus générés servent actuellement de "squelettes" de campagnes, incluant des structures utiles mais nécessitant encore des ajustements manuels pour remplacer les espaces réservés (placeholders) et les blocs de codes QR génériques.

Cette tendance à l'intégration de l'IA n'est pas isolée, comme en témoigne la plateforme de voice-phishing **ATHR**, qui utilise également des agents IA pour mener des attaques d'ingénierie sociale à grande échelle.

III. Un large éventail de cibles et de fonctionnalités avancées

Pour maximiser son impact, Bluekit propose plus de 40 modèles (templates) imitant des services populaires. Les designs et logos sont particulièrement réalistes, ciblant notamment :

- Messageries : Gmail, Outlook, ProtonMail, Yahoo;
- Services Cloud : iCloud, Apple ID ;
- Plateformes techniques : GitHub, Zoho ;
- Crypto-monnaies : Ledger.

Au-delà de l'apparence, le kit offre un contrôle granulaire sur le comportement des pages. Les attaquants peuvent configurer des mécanismes anti-analyse, bloquer le trafic via VPN ou proxy, et filtrer les visiteurs selon leur empreinte numérique (fingerprinting).

Exfiltration de données et surveillance en temps réel

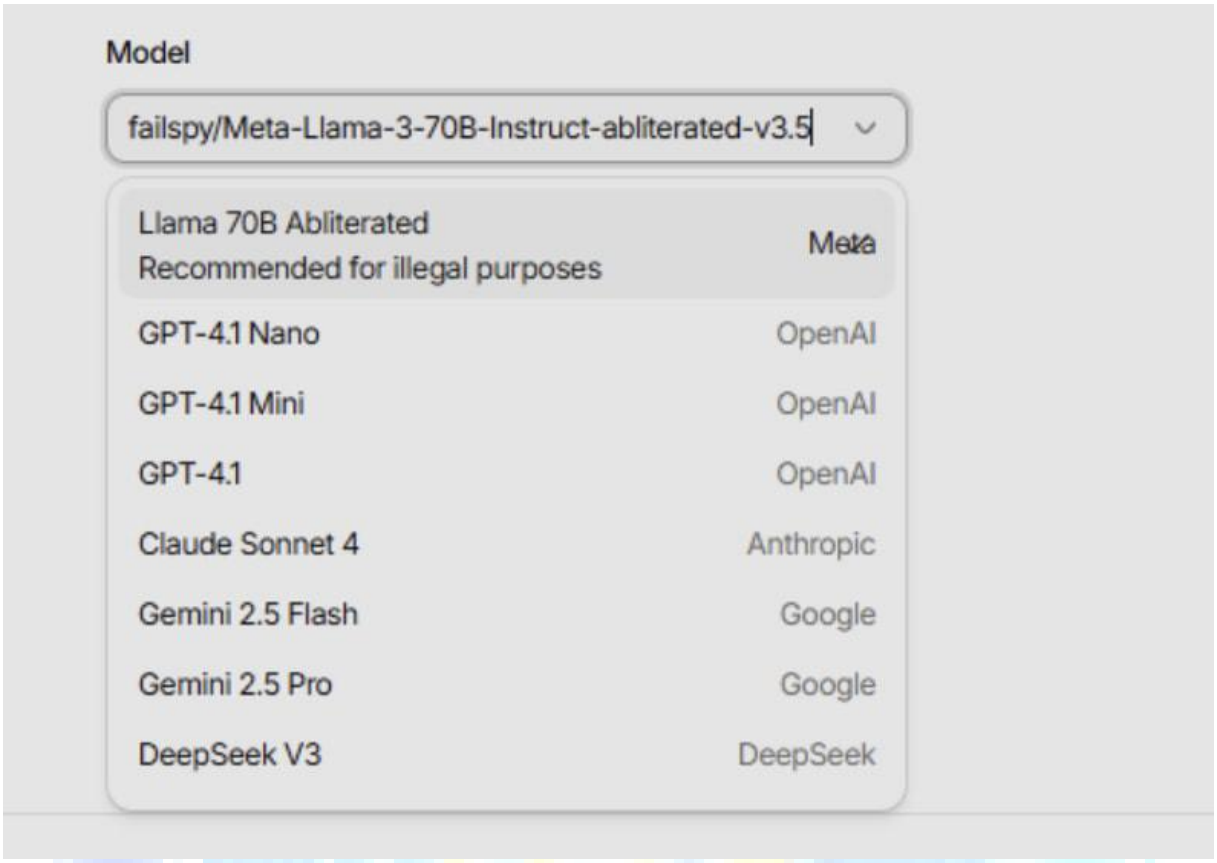
Une fois la victime infectée, les données volées (identifiants, cookies, stockage local) sont exfiltrées via des canaux privés Telegram. La plateforme permet également de suivre l'état de la session de la victime après sa connexion, offrant ainsi aux opérateurs la possibilité d'affiner leurs attaques pour une efficacité maximale.

IV. Conclusion

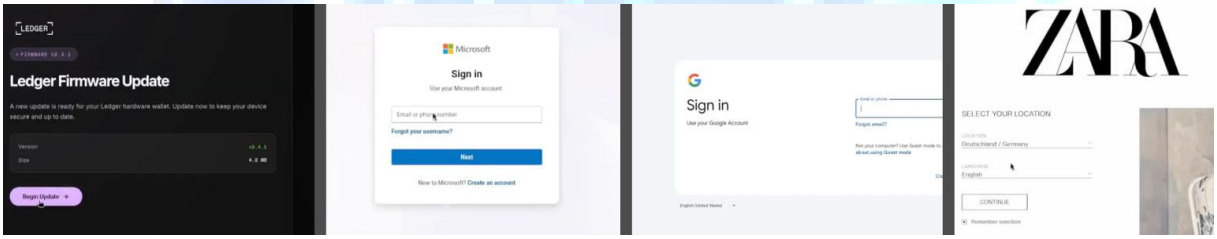
En conclusion, bien que Bluekit soit encore en phase de développement actif avec des mises à jour fréquentes, sa nature "tout-en-un" et l'utilisation de l'IA en font un candidat sérieux à une adoption massive par des cybercriminels de tous niveaux. Une vigilance accrue est recommandée face à des messages de plus en plus sophistiqués imitant les services susmentionnés.

V. Annexes

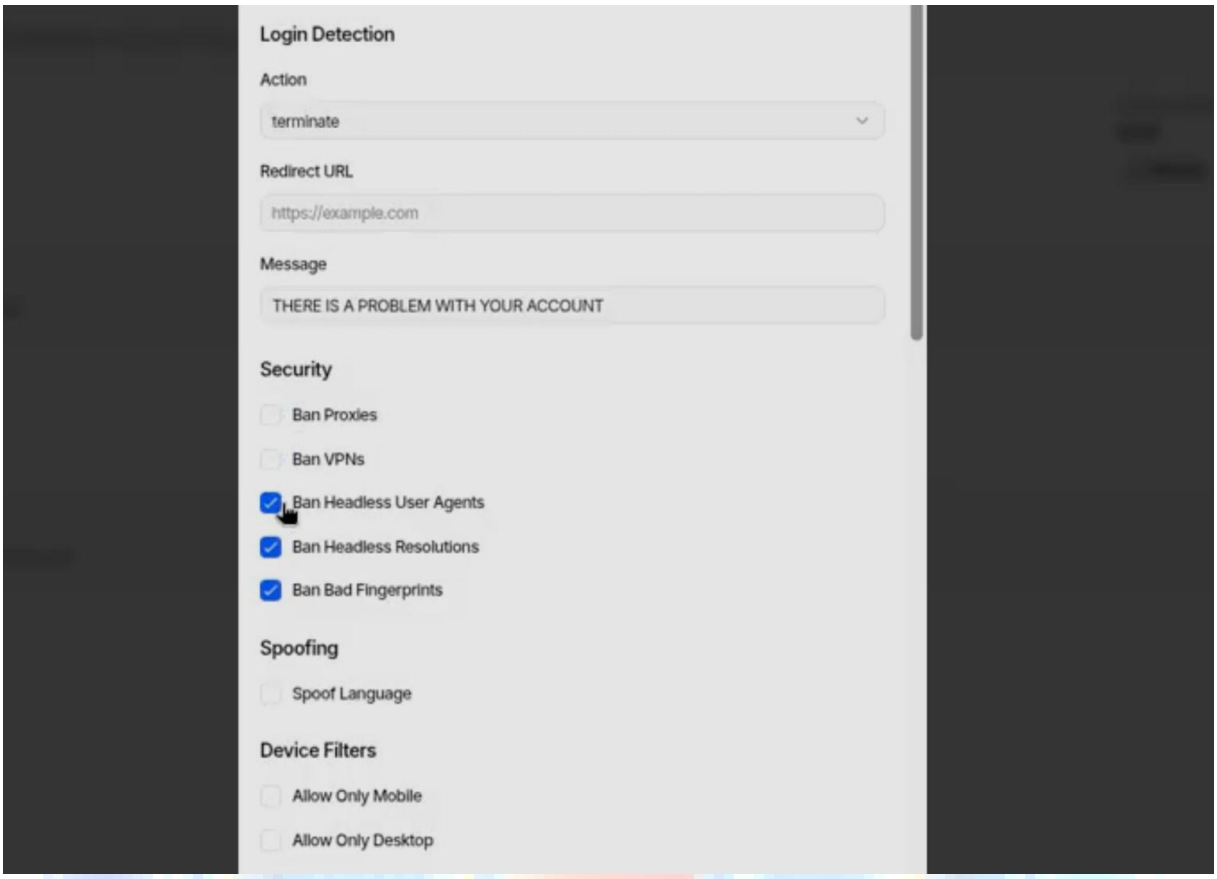
Les modèles IA disponibles sur Bluekit



Les templates offerts par Bluekit



Les options de sécurité



Dashboard de monitoring post infection