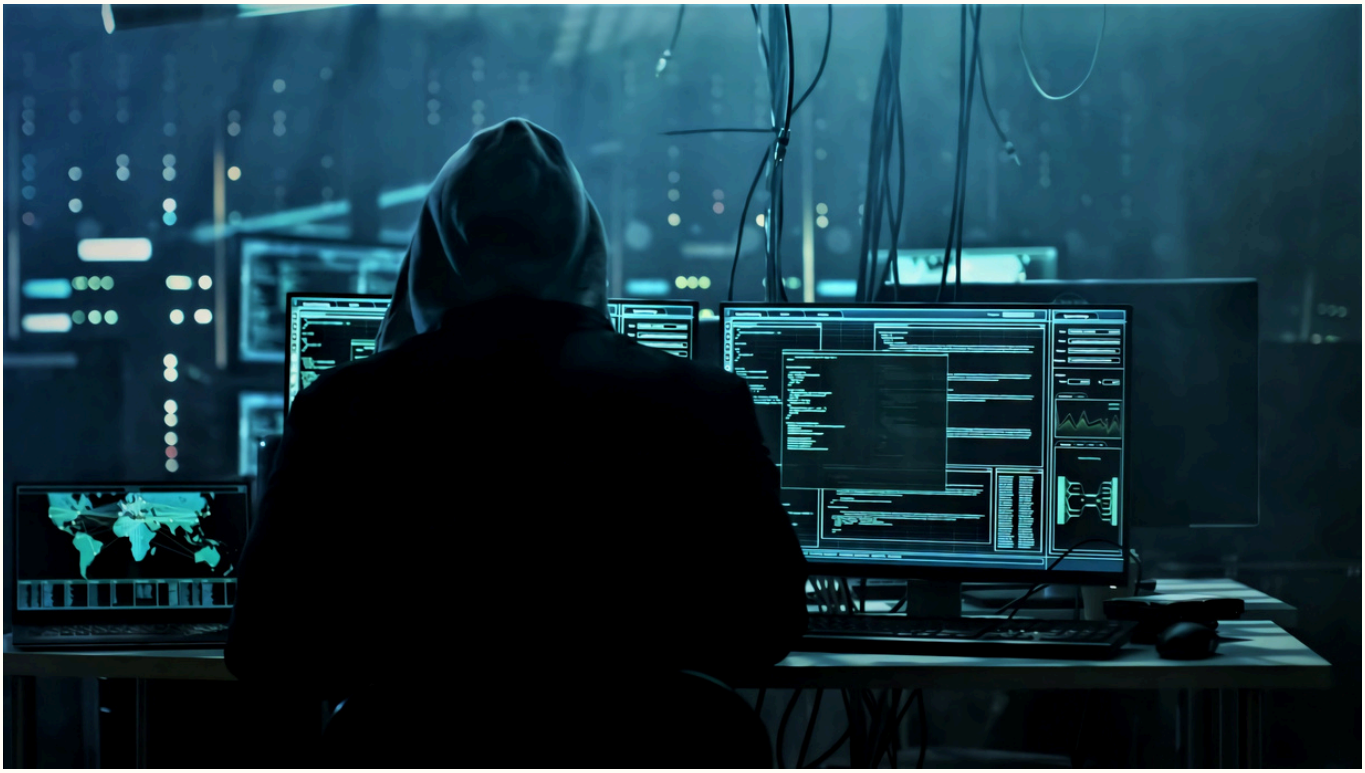


LES COURTIERS EN ACCES INITIAL (IAB)

Une menace silencieuse pour l'Afrique Francophone

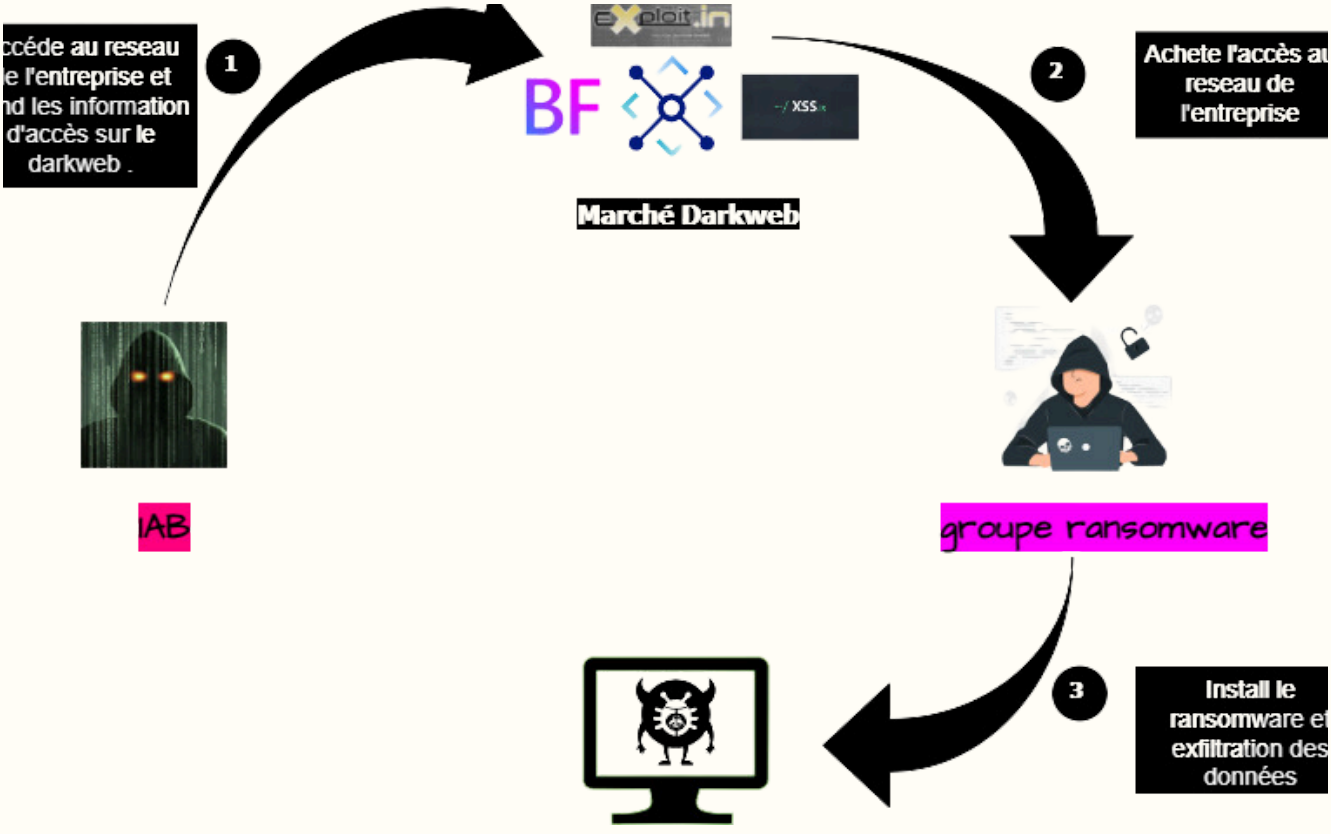
JUILLET 2024

Extrait d'une étude menée Par **Oumar Ali Mahamat,** Etudiant en 5e année de cybersécurité, stagiaire chez RHOPEN Labs.

Résumé

Dans le domaine de la cybersécurité, une menace émergente inquiète de plus en plus : les courtiers en accès initial (ou ***Initial Access Broker*** en anglais, couramment abrégé IAB). Ces cybercriminels, opérant souvent dans l'ombre du **dark web**, vendent des accès compromis à des réseaux informatiques à d'autres acteurs malveillants, facilitant ainsi des attaques destructrices, notamment par ransomware.

Cet article explore le fonctionnement des **IAB**, leurs méthodes d'accès, et les impacts significatifs sur les entreprises et organisations en Afrique francophone, tout en fournissant des recommandations pour renforcer la cybersécurité dans cette région.



Avertissement de Non-Responsabilité

L'information contenue dans cet article est destinée à des fins éducatives et de sensibilisation uniquement, en particulier pour les professionnels de la cybersécurité dans les pays d'Afrique francophone.

Les exemples et les scénarios décrits ici ne doivent en aucun cas être utilisés pour des activités illégales ou non éthiques. Les auteurs et distributeurs de cet article déclinent toute responsabilité quant à l'utilisation incorrecte ou malveillante des informations fournies.

Les entreprises et les individus doivent consulter des professionnels en cybersécurité pour obtenir des conseils spécifiques adaptés à leurs besoins et contextes uniques. Toute tentative d'exploiter les failles de sécurité décrites dans cet article pour des gains personnels ou professionnels illégitimes est fortement condamnée et peut entraîner des poursuites judiciaires.

INTRODUCTION

Très souvent ignorée lorsqu'on parle des acteurs de la menace dans le paysage complexe de la cybersécurité, distinct des groupes de cybercriminels qui revendiquent les attaquent sur leurs cibles, une autre forme de menace émerge discrètement et insidieusement : **Les courtiers en accès initial (IAB)**. Ces acteurs spécialisés, opérant souvent dans l'ombre du dark web, jouent un rôle crucial dans les cyberattaques, en particulier les attaques par **ransomware**.

Le présent article fournit un aperçu des **tactiques, techniques et procédures (TTP)** utilisées par les cybercriminels pour compromettre les réseaux et les implications des IAB dans les pays d'Afrique francophone, où la cybersécurité devient de plus en plus une préoccupation majeure.

Qui sont les courtiers en accès initial ?

Les courtiers en accès initial (IAB) sont des cybercriminels spécialisés qui se concentrent sur l'obtention d'accès non autorisé aux réseaux informatiques, sans revendication publique et sans prise de contact avec la cible compromise. Une fois cet accès obtenu, ils le vendent à d'autres cybercriminels à des coût parfois ridicules au regard des actifs en jeu. Ces acheteurs, notamment des affiliés de ransomwares, exploitent les accès ainsi reçus pour mener des attaques dévastatrices.

Le rôle des IAB dans les attaques de ransomware

Les IAB sont au cœur des attaques de ransomware. Ils fournissent aux cybercriminels les accès nécessaires pour infiltrer les réseaux, escalader les privilèges et déployer des ransomwares. Des groupes comme **Lockbit, Stormous ou encore Blackcat/APHVN**, qui ont sévi en Afrique francophone, utilisent souvent ces accès initiaux pour exfiltrer des données, compromettre les systèmes critiques et, finalement, exiger des rançons considérables.

Les marchés noirs du dark web : Où trouver les IAB ?

Les courtiers en accès initial opèrent principalement sur des forums et des marchés noirs du dark web où ils vendent des accès compromis. Voici quelques-unes des plateformes les plus notoires :

- **Exploit.in** : Un forum de premier plan utilisé par les cybercriminels pour acheter et vendre des accès à des réseaux compromis, des données volées et des logiciels malveillants.
- **XSS.is** : Connue pour être un lieu de rencontre pour les pirates informatiques, cette plateforme permet la vente de failles de sécurité et d'accès initiaux.
- **BreachForums** : Bien que fermé, ce forum est de retour et a une place de marché populaire pour les informations volées et les accès réseau.

Comment trouvent-ils l'accès ?

Les courtiers en accès initial utilisent une variété de méthodes sophistiquées pour obtenir des accès non autorisés aux réseaux. Voici quelques-unes des techniques les plus courantes :

- **Infostealer Malware** : Logiciels malveillants conçus pour voler des informations sensibles telles que les identifiants de connexion et les cookies de session.
- **Scanneurs de vulnérabilités** : Ciblage des systèmes exposés sur Internet afin d'identifier les failles de sécurité non corrigées et donc exploitables.
- **Phishing et Spearphishing** : Envoi de courriels frauduleux ciblés pour inciter les utilisateurs à divulguer leurs identifiants de connexion.
- **Botnets** : Réseaux de machines infectées utilisées pour distribuer des logiciels malveillants et collecter des données.

Les accès les plus prisés par les IAB

Les courtiers en accès initial (IAB) ciblent des accès spécifiques pour compromettre les réseaux d'entreprise et faciliter les attaques par ransomware. Voici les types d'accès les plus prisés :

- **Services RDP, Anydesk**
- **VPN d'entreprise**
- **Passerelles Citrix**
- **Applications web et CMS**
- **Serveurs de messagerie d'entreprise (BEC)**
- **Accès root ESXi et Active Directory (AD)** (Plus rares mais plus recherchés)
- **Vulnérabilités Zero-Day et N-Day**
- **Points d'injection de code (HTML, SQL)**

L'Impact en Afrique Francophone

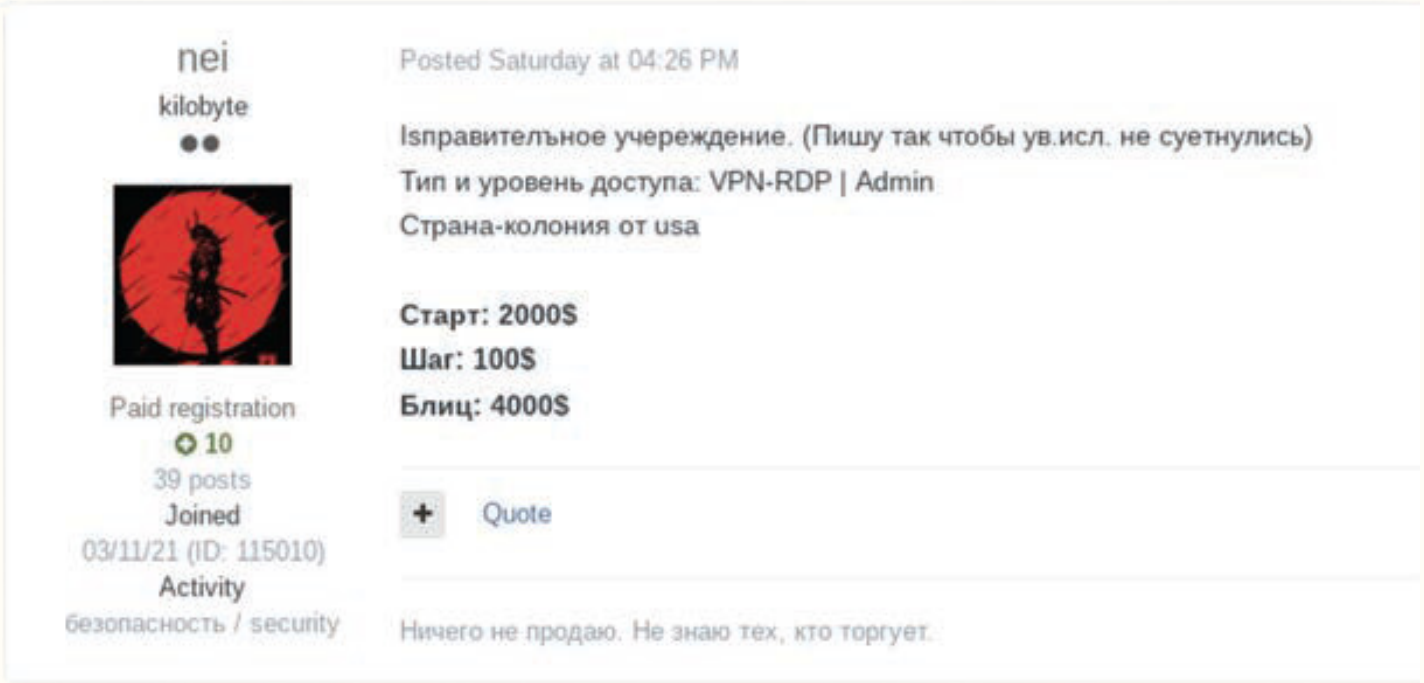
Les courtiers d'accès initial (IAB) représentent une menace croissante pour la cybersécurité des entreprises en Afrique francophone. Voici un aperçu des principaux impacts et des secteurs les plus vulnérables :

I**nstitutions Financières** : Les banques et les institutions financières sont des cibles privilégiées en raison des transactions monétaires qu'elles gèrent. Les IAB exploitent souvent les failles de sécurité pour accéder à des informations sensibles et facilitent ainsi les attaques de ransomware.

Infrastructures Critiques : Les infrastructures essentielles, comme l'énergie, les transports et les télécommunications, sont également à risque. Les IAB peuvent compromettre ces systèmes pour provoquer des perturbations majeures ou exiger des rançons élevées.

PME et Startups : De nombreuses petites et moyennes entreprises n'ont pas les ressources nécessaires pour investir dans des systèmes de sécurité avancés. Cela les rend particulièrement vulnérables aux attaques facilitées par les IAB.

Secteur Public : Les institutions publiques sont souvent ciblées par des ransomware, notamment en raison de leur manque de fonds pour des solutions de cybersécurité robustes. Les courtiers d'accès initial peuvent vendre des accès à ces réseaux pour des sommes modiques, créant des opportunités pour les affiliés de ransomware.



Recommandations pour renforcer la cybersécurité

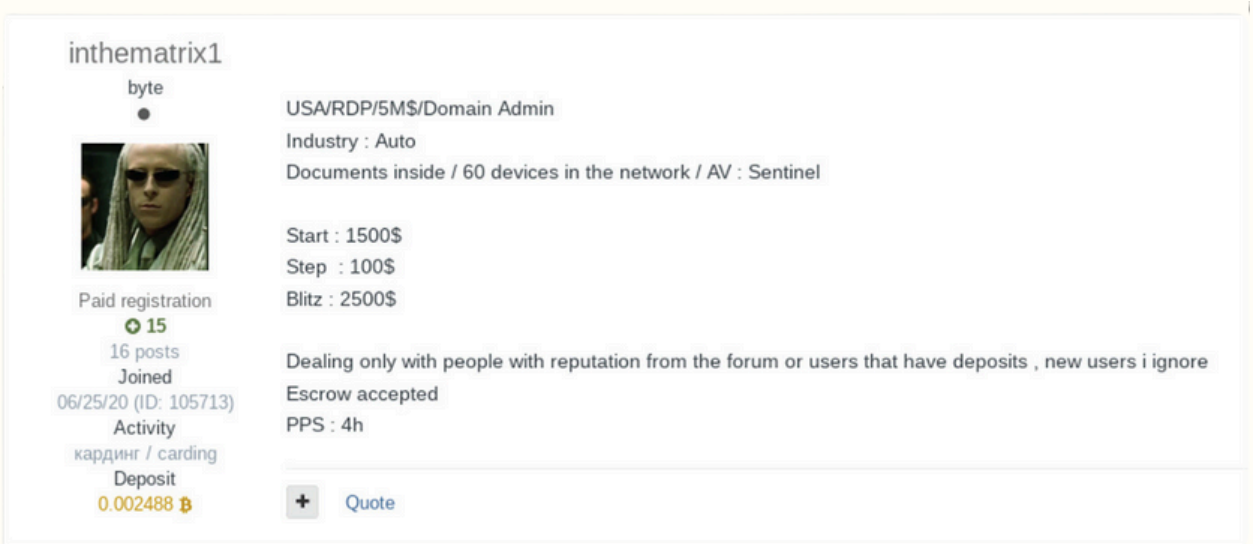
Pour contrer la menace des IAB et des ransomwares, les entreprises en Afrique francophone doivent adopter des mesures proactives de cybersécurité. Voici quelques recommandations essentielles :

Mise en place d'un SOC : La mise en place d'un Centre des Opérations de sécurité (SOC), avec un EDR efficace et une solution SIEM bien configurée, peut permettre aux entreprises de repousser la plupart des cyberattaques par ransomware. Face à une entreprise bien protégée, un cybercriminel peut abandonner sa cible.

Cependant, mettre en place un SOC peut être coûteux et complexe pour beaucoup. Heureusement, **RHOPEN Labs**, basée au Cameroun, propose une **solution SOC as a Service**, offrant surveillance continue, détection des menaces et réponse aux incidents sans nécessiter d'investissements massifs en infrastructure et personnel.

Renforcement des Politiques de Sécurité : Les entreprises doivent mettre en œuvre des politiques de sécurité rigoureuses, y compris des contrôles d'accès stricts, l'utilisation de VPN sécurisés et la mise en place de l'authentification multi-facteurs (MFA).

Sensibilisation et Formation : Il est crucial de sensibiliser les employés aux menaces de phishing et aux pratiques de cybersécurité de base. Des programmes de formation réguliers peuvent aider à réduire les erreurs humaines qui conduisent souvent à des compromissions initiales.



CONCLUSION

En conclusion, les menaces de **ransomware** représentent un défi majeur pour les entreprises de toutes tailles. Les courtiers d'accès initial jouent un rôle clé en facilitant l'accès aux réseaux compromis à des coûts relativement bas. Par exemple, environ 1 000 000 d'accès à des VPN mal configurés peuvent être vendus pour 1 500 $.

Plusieurs entreprises et organisations d'Afrique francophone, que nous avons fait le choix de ne pas mentionner ici, ont été récemment victimes de ces acteurs malveillants.

Pour lutter efficacement contre cette menace, il est crucial que les entreprises investissent dans des mesures de sécurité robustes telles que des EDR bien configurés, une surveillance proactive par des SOC et une gestion rigoureuse des politiques et des actifs.

De plus, la collaboration entre les experts en cybersécurité est essentielle. Le partage d'indicateurs de compromission (IoC) et d'autres informations pertinentes peut renforcer la résilience collective contre les attaques de ransomware.

En comprenant les limitations financières et en adoptant des stratégies de cybersécurité adaptées, les organisations peuvent se prémunir contre les attaques de ransomware et protéger leurs ressources précieuses.

PS: Cet article n'est qu'un aperçu du travail fouillé de recherches menées par son auteur, certaines informations ont été censurées pour des raisons évidentes de sécurité. En l'occurrence, nous disposons d'une liste d'outils et de courtiers en accès initial les plus redoutés dans le monde, dont ceux ayant compromis et vendu les accès de certaines entreprises et organisations d'Afrique francophone.

Lien LinkedIn

A propos du réacteur de l'article :

Oumar Ali Mahamat est un étudiant en 5e année de cybersécurité, actuellement en stage chez RHOPEN Labs. Passionné par la protection des systèmes informatiques et la veille sur les cybermenaces, il se concentre sur la collecte et l'analyse des indicateurs de compromission pour enrichir les solutions de threat intelligence.

Actif dans le domaine de la sécurité informatique, Oumar travaille sur la mise en place d'une base de données de renseignement sur les menaces ciblant les pays d'Afrique francophone, sous la supervision de **François-Xavier DJIMGOU NGAMENI**, Président de RHOPEN Labs et Expert en cybersécurité.

À propos de RHOPEN Labs

Filiale de l'entreprise technologique française RHOPEN, RHOPEN Labs est une société de droit camerounais au capital de 20.000.000 de Fcfa, entreprise innovante dans le domaine de la Cybersécurité et du Cloud/DevOps et dédiée à la protection des organisations africaines contre les menaces numériques. Avec une équipe d'experts et des solutions endogènes de pointe, RHOPEN Labs s'engage à fournir des services de sécurité de premier ordre.