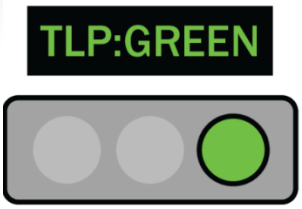
Investigation Report

Phishing Attack – Stealer

April 2024

CSIRT.TN

BY KEYSTONE GROUP



TLP: GREEN

Limited disclosure, restricted to the community.

TABLE DES MATIERES

1. CONTEXTE GENERAL

Les menaces cybernétiques sont devenues de plus en plus préoccupantes avec l'avancement de la technologie. Ces menaces incluent des attaques informatiques sophistiquées qui peuvent causer des dommages importants aux entreprises et aux particuliers. Les Stealers, qui sont une forme de malware, font partie intégrante de ces menaces.

Dans cette conjoncture mouvementée, le 24/04/2024 un courriel provenant d'une adresse valide et de confiance, incitant à l'ouverture d'un lien de stockage cloud qui héberge un fichier malicieux visant le vol des identifiants stockés dans le navigateur.

Ce travail vise à examiner cette menace cybernétique émergentes et à se concentrer sur les moyens d'en faire face en fournissant également des mesures préventives pour mieux se protéger contre ces Steelers.

1.1. CONTEXTE DES MENACES CYBERNETIQUES

Le contexte des menaces cybernétiques est caractérisé par une évolution rapide des technologies de l'information et de la communication, ce qui expose les systèmes informatiques à des risques de plus en plus grands. Les cybercriminels exploitent les vulnérabilités des réseaux et des logiciels pour infiltrer les systèmes, voler des informations sensibles, perturber les activités quotidiennes et causer des dommages financiers. Les attaques peuvent provenir de divers acteurs, notamment des États-nations, des groupes criminels organisés, des hackers indépendants et des hacktivistes. Comprendre le contexte des menaces cybernétiques est essentiel pour mettre en place des mesures de sécurité efficaces.

1.2. DEFINITION DES STEALERS

Les Stealers sont des programmes malveillants conçus pour voler des informations personnelles précieuses à partir des ordinateurs infectés. Ils peuvent collecter des données telles que les identifiants de connexion, les mots de passe, les données bancaires et les fichiers confidentiels. Les Stealers opèrent généralement de manière furtive, enregistrant les frappes au clavier, en capturant des captures d'écran ou en accédant aux fichiers de configuration des navigateurs web. Ces informations volées sont ensuite utilisées à des fins malveillantes, telles que l'usurpation d'identité, le vol d'argent ou le chantage. La définition des Stealers est donc essentielle pour comprendre leur mode de fonctionnement et pour prendre les mesures nécessaires pour s'en protéger.

2. PROPAGATION ET FONCTIONNEMENT

Les Stealers utilisent des techniques de propagation connues mais certes difficiles à contrôler, on note principalement :

- Courriers de phishing : Infecter les appareils par le biais de stratagèmes d'ingénierie sociale est une technique prisée par les hackers, et ce Stealer ne

fait pas exception. Grâce aux courriers de phishing, les acteurs malveillants peuvent envoyer des pièces jointes ou des liens malveillants à un grand nombre de destinataires d'un seul coup. Grâce aux dernières avancées en matière de technologie d'IA, comme l'introduction de ChatGPT, les courriels peuvent aisément être rendus légitimes sans beaucoup d'efforts.

- Sites web compromis : Les utilisateurs du web peuvent être redirigés vers des sites web compromis via des publicités malveillantes ou lorsque les hackers usurpent des noms de domaines (technique connus par typosquatting). Il suffit de visiter un site web infecté pour se faire berner en téléchargeant un logiciel en apparence légitime depuis un site officiel sous toutes les apparences, mais en réalité infecté un Stealer.
- Applications en apparence légitimes : Étant un cheval de Troie, le Stealer peut se déguiser en application ou logiciel en apparence légitime mais en réalité piraté et contenant un cheval de Troie. Dans les cas les plus absurdes, les victimes peuvent télécharger un malware en croyant installer un nouveau logiciel antivirus pour leur appareil ou une mise à jour de leur système d'exploitation.

2.1. QUELLES SONT LES DONNEES CIBLÉES ?

Le Stealer cible typiquement des informations sensibles, comme les identifiants de connexion, mots de passe et informations bancaires. Il vise également à collecter des données utilisateurs telles que les pseudos ou la localisation, ainsi que des informations détaillées sur le système d'exploitation de l'appareil, comme les configurations matérielles, les solutions antivirus, l'adresse IP. Certaines traces laissées par ce Stealer prouve qu'il cherche à cibler aussi les portefeuilles crypto.

Il est également important de noter que le Stealer en question a plus de chances de cibler et voler des informations sensibles sur les navigateurs web basés sur Chromium, comme Chrome et Opera, et Gecko, le plus répandu étant Mozilla Firefox. Il peut collecter les cookies d'authentification et numéros de carte via ces extensions, et accéder aux portefeuilles crypto des utilisateurs. Ce malware attaque aussi diverses applications telles que les clients de courriels, Discord, Telegram, VPN et les applications bancaires en ligne.

Il s'efforce de dérober un maximum de données confidentielles stockées sur les appareils infectés, qu'il s'agisse d'identifiants en ligne, de mots de passe, d'informations bancaires ou plus récemment de crypto-monnaies. Le cheval de Troie cible tout particulièrement les principaux navigateurs web où sont souvent enregistrées ces informations sensibles.

2.2. FONCTIONNEMENT

Un mail avec le format ci-dessous est envoyé ayant la même adresse d'immission et de réception (l'adresse de la potentielle victime/destinataire est envoyée en Cci pour Copie Carbonne Invisible).

Bonjour,

Vous trouverez en pièce jointe à cet e-mail un ensemble de documents de proposition sécurisés. Veuillez consulter ou télécharger ce document et fournir tous les commentaires nécessaires.

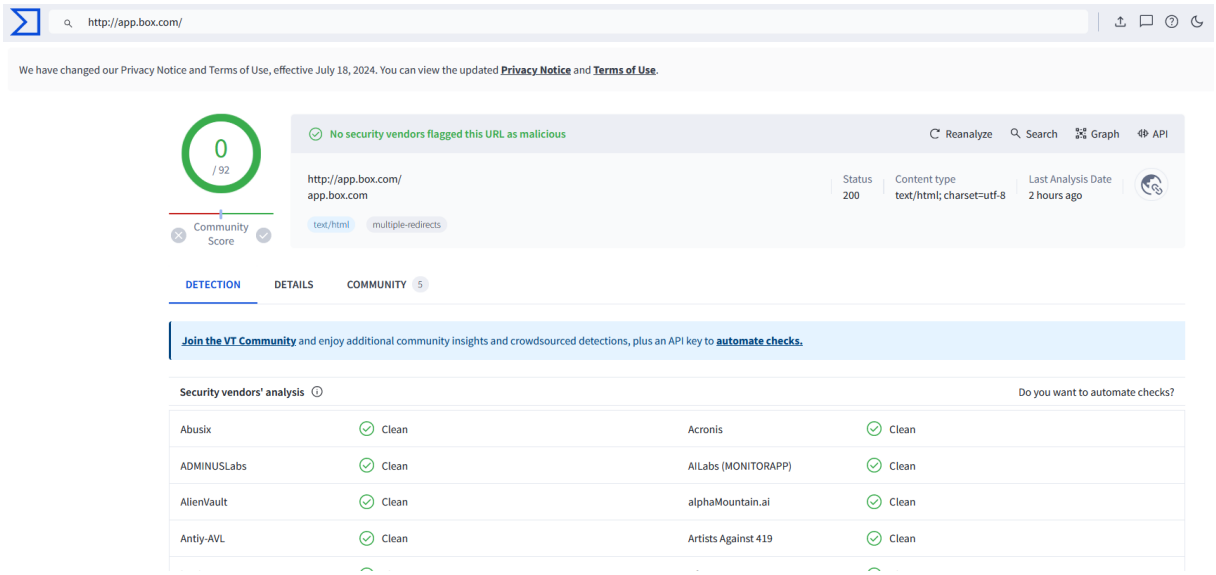
Bien Cordialements.

Assuraces-Biat2024-SecureProposal-file42185#

Cliquez ici pour consulter le document de Assurances Biat Group.

To view more details about this contract project and attachments, click here to visit Assurances Biat Group, Portal Doc Review

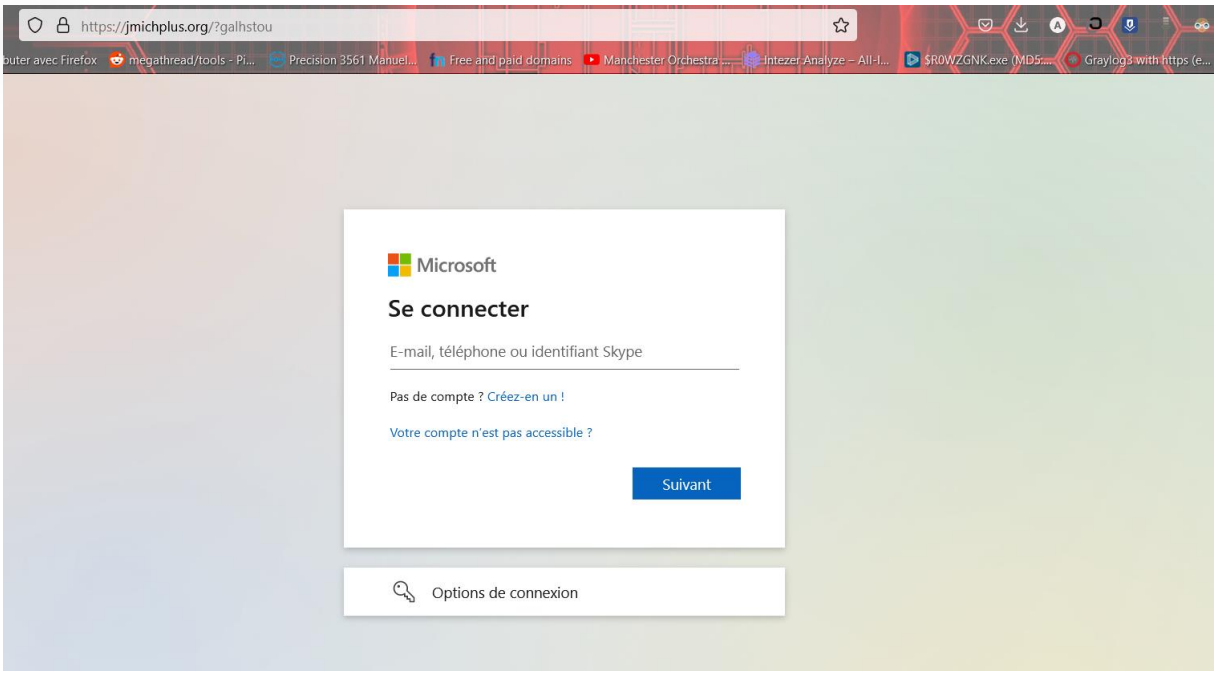
Une fois qu'une personne a cliqué sur le lien hypertexte, le navigateur par défaut ouvrera la page en question https://app.box.com/s/pfbm9mhkda6e1u3v62umb9nbtoer839s



S'agissant d'un lien d'une plateforme de stockage en ligne, similaire à Google Drive et One Drive, le lien a été autorisé et non intercepté par les IPS des solutions de filtrage ou des proxys. Toutefois, dans certains cas, les entreprises bloquent déjà les sites de stockage en ligne, ce qui a permit de bloquer cet accès.

Le fichier hébergé dans la plateforme https://app.box.com étant le fichier malicieux, une fois téléchargé et exécuté vous serez redirigés vers le lien suivant https://jmichplus.org/?galhstou.

Ce dernier est un site de phishing hébergeant une interface similaire à la page d'authentification de Outlook 365.



Il est à noter que le site en question est un site nouvellement créé (2024-04-16), donc ne jouit pas d'une mauvaise réputation et en conséquent ne sera pas bloqué par le filtre en place.

Registrar Info	
Name	HOSTINGER operations, UAB
Whois Server	https://rdapserver.net/
Referral URL	http://www.hostinger.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Important Dates	
Expires On	2025-04-16
Registered On	2024-04-16
Updated On	2024-04-21
Name Servers	
ns1.dns-parking.com	162.159.24.201
ns2.dns-parking.com	162.159.25.42

Par suite, une fois la victime potentielle a entré ses identifiant, les pirates les récupèrent et entament une nouvelle compagne en utilisant les nouveaux identifiants. Selon les cas observés aucun effort n'est réalisé pour personnaliser la nouvelle compagne, en fait il s'agit du même email envoyé en tant que simple pièce jointe.

Il est également important de considérer les faits suivants :

- Le fichier malicieux extrait les données stockées au niveau du navigateur (identifiants, cookies, …).

- Dans certaines machines ou le fichier malicieux a été exécuté il y a eu des tentatives d'extractions des identifiants enregistrés dans le système d'exploitation (aucune tentative réussie n'été observé dans les terminaux analysés).
- Les pirates ont envoyé les courriels frauduleux depuis le terminal de la victime, ce qui prouve une prise de contrôle totale sur les machines infectés.

3. RECOMMANDATIONS

Pour éliminer cette menace, on recommande vivement de :

- Bloquer l'adresse https://jmichplus.org.
- Bloquer les sites appartenant à la catégorie (Cloud Storage) à la limite du possible.
- Adopter des repos de mot de passe sécurisé autre que les repos des navigateurs.
- Identifier tous flux à destination « 93.127.163.76 » et considérer les machines sources comme infectées.
- Identifier depuis l'Active Directory ou tout autre annuaire utilisé par les machines ayant tenté plusieurs fois des actions de login ayant échoué (entre le 24 et 25 avril).
- S'assurer que la double authentification (MFA) est activée pour tous les comptes office365.
- Bloquer (dans la mesure du possible) les accès internationaux vers l'interface web office365 (spécifiquement depuis la France).