GSA+ GROUPEMENT DE SERVICES ASSURANCE

CYBER ATTAQUE

LES BONS REFLEXES
LES PROTECTIONS
LA BONNE PRATIQUE

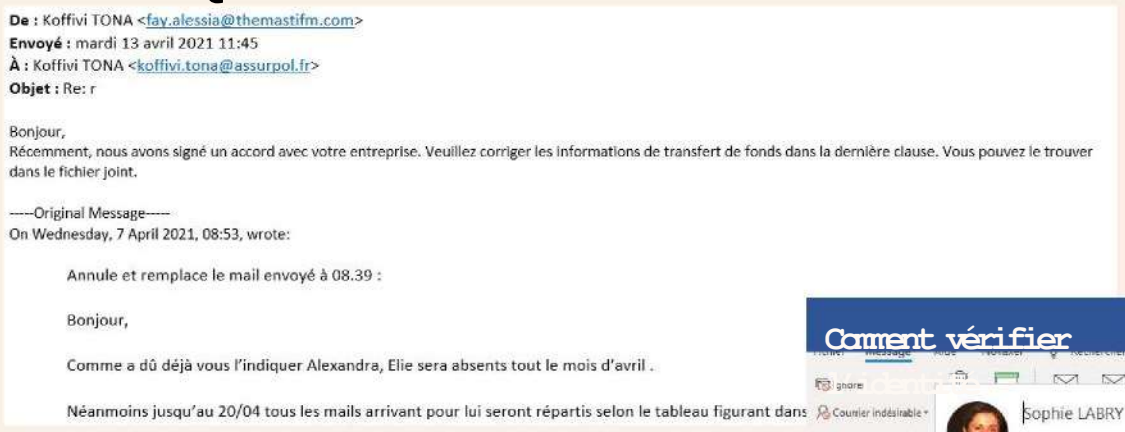
Information collaborateurs GSA+ 18 octobre 2023

SENSIBILISATION A LA CYBER ATTAQUE

- DEFINITION
- DEROULEMENT D'UNE CYBER ATTAQUE
- PROCEDURE EN CAS D'USURPATION D'IDENTITE

DEFINITION D'UNE CYBER ATTAQUE

Une cyberattaque est un acte malveillant envers un dispositif informatique.
Elle peut émaner de personnes isolées, d'un groupe de pirates ou de vastes organisations ayant des objectifs géopolitiques.



De : Koffivi TONA <fay.alessia@themastifm.com>
Envoyé : mardi 13 avril 2021 11:45
À : Koffivi TONA <koffivi.tona@assurpol.fr>
Objet : Re: r

Bonjour,
Récemment, nous avons signé un accord avec votre entreprise. Veuillez corriger les informations de transfert de fonds dans la dernière clause. Vous pouvez le trouver dans le fichier joint.

-----Original Message-----
On Wednesday, 7 April 2021, 08:53, wrote:

Annule et remplace le mail envoyé à 08.39 :

Bonjour,

Comme a dû déjà vous l'indiquer Alexandra, Elie sera absents tout le mois d'avril .

Néanmoins jusqu'au 20/04 tous les mails arrivant pour lui seront répartis selon le tableau figurant dans

De : Stephanie SOENE [mailto:fay.alessia@themastifm.com]
Envoyé : mardi 13 avril 2021 11:44
À : Emmanuelle GROSGEORGE
Objet : Re: TR: Contrat RC2003561 - GMS ENROBES // N

Bonjour!
Veuillez remplir cet accord à partir du 12/03. Des modifications doivent être apportées au deuxième paragraphe. Vous pouvez le vérifier dans le fichier joint.

-----Original Message-----
On Thursday, 8 April 2021, 15:42, wrote:

Bonjour,

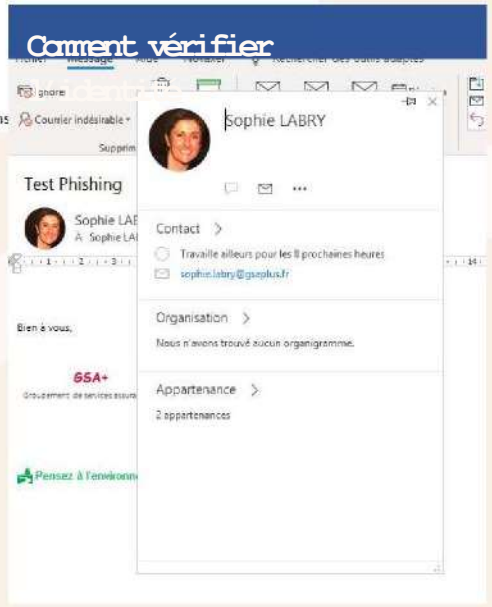
Nous accusons réception de votre demande et vous en remercions.

Le souscripteur en charge de votre dossier est Stéphanie SOENE ;Elle reviendra vers vous dans les meilleurs délais.
Toutefois, je vous remercie de noter que les mesures d'organisation prises pour faire face aux dispositions gouvernementales sur le mois d'avril risquent d'allonger nos délais de répon

Restant à votre disposition,

Cordialement,

Impossible d'afficher l'image liée. Le fichier a peut-être été déplacé, renommé ou supprimé. Vérifiez que le lien pointe vers le fichier et l'emplacement corrects.



DEROULEMENT TYPE D'UNE CYBER ATTAQUE

1. INTRODUCTION MALVEILLANTE

- Émail de spam ou de phishing avec pièce jointe malveillante, ou téléchargement via site Web ou d'un document contenant un virus
- Fonctionnalités de partage ou gestion de fichiers à distance telles que le protocole RDS

2. OBJECTIF DU MALVEILLANT

Les cybercriminels exploitent des failles du système pour obtenir des niveaux de privilèges qui leur permettent de contourner le logiciel de sécurité.
D'où le fait que votre compte d'accès ne soit **administrateur** du poste.

3. DÉSACTIVATION ET CONTOURNEMENT DE LA SÉCURITÉ

À défaut, ils tenteront de pénétrer dans la console de gestion de la sécurité et de désactiver les systèmes de sécurité (Antivirus par exemple).

4. DÉPLOIE LA CHARGE VIRALE

Déploiement méthodique en débutant par la suppression des sauvegardes stockées sur le réseau, puis exfiltrent les données sensibles de l'entreprise par des actions minimes afin de n'éveiller les outils de sécurité de transfert de flux.

5. Activation du RANSOMWARE

Chiffrement des données de l'entreprise, via encryptage sur les systèmes d'exploitation et sur la totalité des fichiers du réseau en mode partage.

6. Résultat

- Les Cybercriminels menacent de vendre sur le Dark Web les données subtilisées si la rançon n'est payée, et ainsi obtention de la clef de décryptage.
- Les échanges se passent via mail ou « Dark Web ».

LA PROCEDURE EN CAS D'ATTAQUE

1. Modifiez immédiatement votre mot de passe

- *Vous êtes sur site Tour W : En cliquant sur ctrl/Alt/suppr simultanément puis sur modifier mot de passe*
- *Vous êtes en télétravail RDS: En cliquant sur ctrl/Alt/Fin simultanément puis sur modifier mot de passe (Attention : identifiant initiale du prénom et nom tout en minuscule)*

2. Déconnectez l'appareil du réseau

Si vous êtes sur le site Tour W , débranchez votre ordinateur de la station d'accueil et du WIFI pour ne pas contaminer l'ensemble du réseau (Equivalent de la «Mise en mode avion»).
Contacter l'Informatique en cas de doute

3. Arrêt et Mise en Sécurité

- N'Eteignez pas votre appareil !

Cette action peut complètement bloquer votre matériel et impossible de le relancer en cas d'investigation ou de récupération.

- Prévenir le service Informatique ou votre référent.

4. Informez l'équipe informatique

Contactez tout de suite :

Abilio MATIAS 01 47 76 53 27
Gaëlle BONTET 01 47 76 53 55
Et votre correspondant informatique .

5. **Consignes à Suivre**

Cette procédure ne doit pas connaître de résistance ou d'hésitation. Elle doit être appliquée de façon immédiate et responsable.

L'équipe informatique (administrateurs et référents) fera le nécessaire rapidement pour vous trouver une solution de secours.

Nous pouvons tous être victimes d'une cyberattaque.

L'important est d'adopter la bonne pratique en le signalant immédiatement à l'équipe informatique pour limiter les dégâts liés à l'intrusion.

OUTILS DE PROTECTION GSA+

- AUTHENTIFICATION FORTE
- VADE SECURE
- CAMPAGNE DE PHISHING
- AIDE SENSIBILISATION
- SERVEUR D'ARCHIVAGE
- INTERDICTION DES CLÉS USB
- SYNTHESE DES BONS REFLEXES

L’ AUTHENTIFICATION FORTE – Mise en place 2021

L’authentification forte ou multi-facteurs (MFA) est une procédure d’identification qui fait appel à au moins deux authentifications pour vérifier l’identité de l’utilisateur qui souhaite se connecter.

Elle a pour objectif de rendre plus difficile, voire impossible, l’accès d’une personne qui aurait usurpé notre identité. Elle nous protège ainsi contre le vol d’identité, l’usurpation de compte et le phishing.

Il faut retenir que :
81% des cyberattaques seraient liées à des mots de passe insuffisamment sécurisés
99,9% de ces attaques peuvent être bloquées grâce à l’authentification Forte.

1. Accès RDS
   1.1 – Lancement du RDS
   1.2 – Entrée User / Passe

2. Accès INWEBO
   2.1 – Ouverture sur les supports souhaités
   2.2 – Entrez CODE PIN

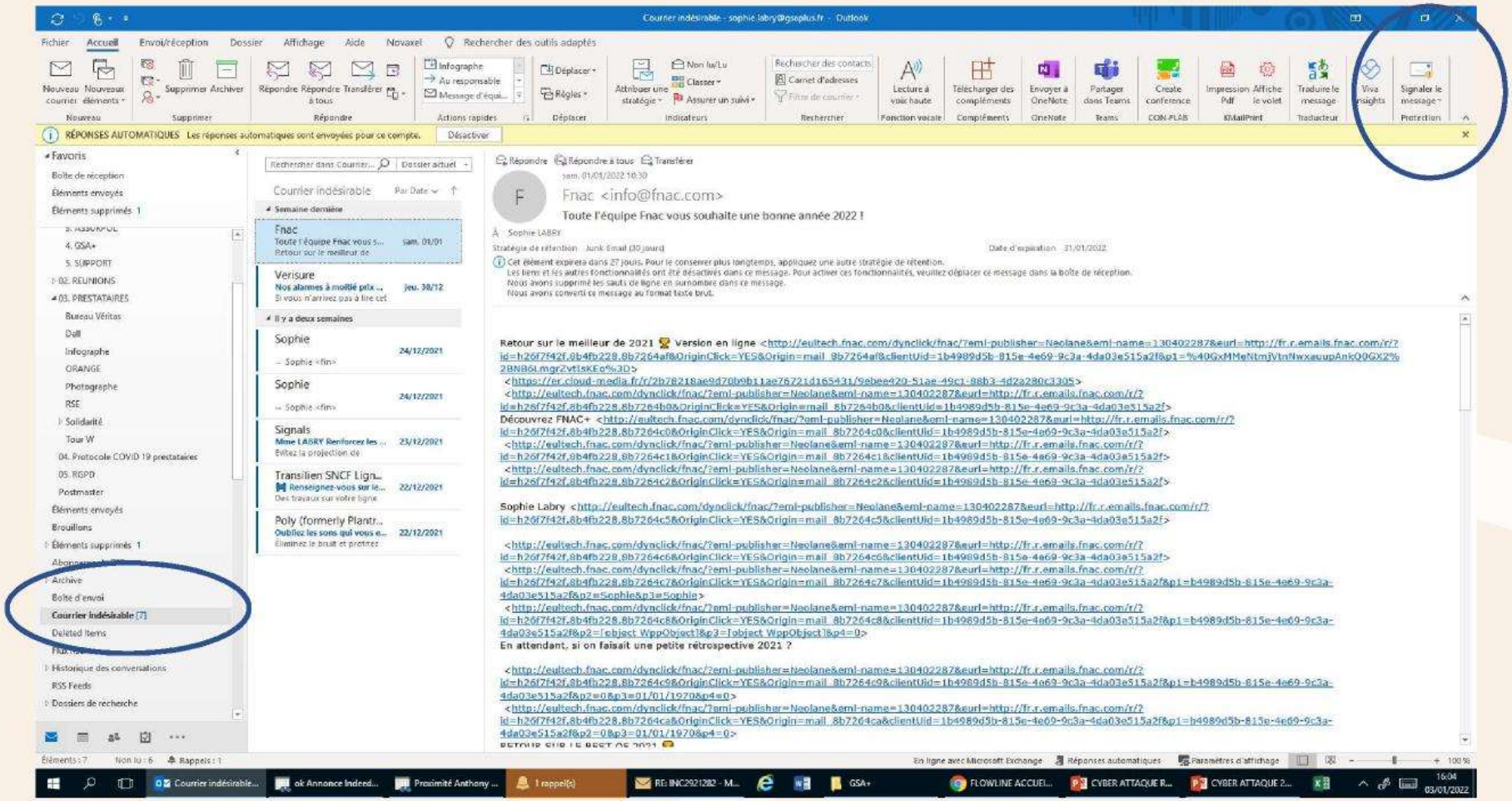
3. Résultat
   3.1 – Ouverture de RDS.

VADE SECURE

L'usurpation d'identité passe le plus souvent par le phishing via nos BAL professionnelles,

Pour éviter au maximum ce vol d'identité, le GSA+ a mis en place l'outil Vade Secure qui écarte de nos BAL les mails suspects, spam, phishing...

Vous pouvez également signaler un message suspect en cliquant sur l'icône en haut à droite.



La campagne de formation / sensibilisation VADE SECURE est réalisée en début de chaque trimestre

CAMPAGNE DE PHISHING

La sensibilisation au phishing de ou hameçonnage est une priorité pour la sécurité.
Le phishing est responsable de 94% des ransomwares.
Face à ce constat, depuis 2020, le GSA+ a mis en place une campagne de phishing. Elle est résiliée une fois par an.

Son but est avant tout pédagogique, il faut s'assurer que l'utilisateur maitrise les processus pour reconnaître un phishing.

Caractéristiques du phishing

- Expéditeurs
- Liens
- Pièces jointes
- Contenu du mail ou l'objet du mail

Reconnaître l'expéditeur

- Vérifier le nom de l'expéditeur
- Vérifier l'adresse en cliquant dessus
- En général le bon format doit être utilisateur@entreprise.com

Liens

- De préférence ne pas cliquer sur un lien dans un mail
- Passer la souris dessus pour vérifier le chemin du lien
- Chercher sur un moteur de recherche pour atteindre le site en question
- Contacter l'expéditeur si vous le connaissez

Les pièces jointes

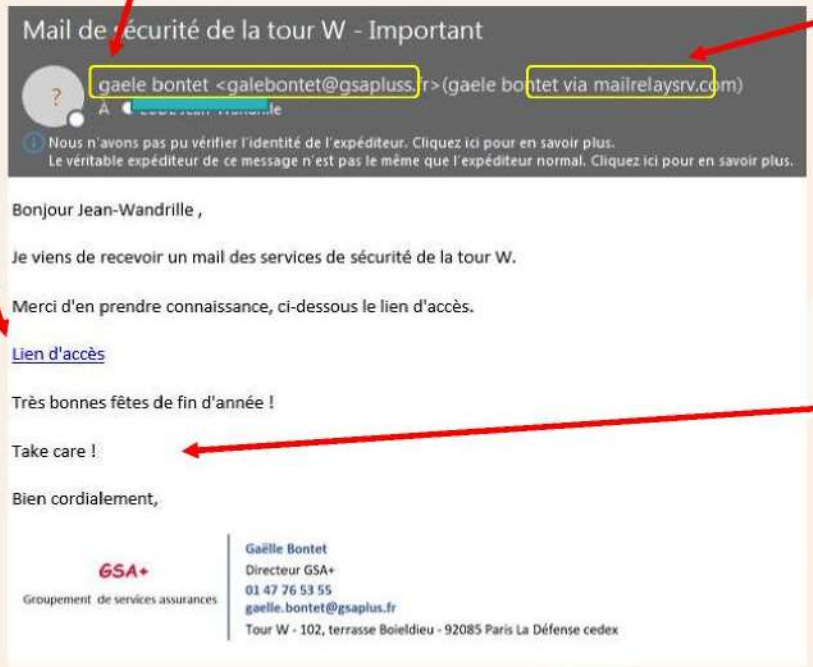
- Redoubler de vigilance lorsque la pièce jointe contient un fichier avec une fin en .zip, .rar ou .exe
- Ne pas ouvrir si vous avez un doute sur l'expéditeur
- Contacter l'expéditeur si vous le connaissez

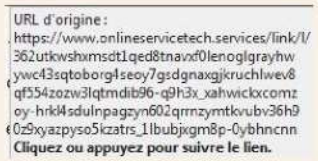
CAMPAGNE DE PHISHING

Le prénom est mal orthographié
La partie de l'adresse avant le @ ne correspond pas à l'identité.
Le nom de l'entreprise (après le @ - domaine) n'est pas correct

Via indique un relais, l'expéditeur n'envoi donc pas du serveur GSA+
L'adresse après le via est suspecte car inconnue

En plaçant la souris sur le lien, le chemin apparait.
Ce lien m'est inconnu, il est donc suspect je ne clique pas.





Si vous connaissez bien l'expéditeur, demandez-vous s'il s'exprime souvent ainsi.
En cas de doute n'hésitez pas à l'appeler

SERVEUR D'ARCHIVAGE - S3 SUR SITE HERBERGEMENT DE LYON

Notre infrastructure est active depuis fin mars 2021 additionnée d'un serveur d'archivage :

GSA+

Deux sites d'hébergement en cluster :

Deux sites actifs dédiés au GSA+ permettant un plan de continuité d'activité (PCA).

En cas de coupure d'un site, la bascule se fait automatiquement. Aucun impact sur l'utilisateur.

Depuis mars 2021, pour se protéger des cyberattaques, le GSA+ a décidé la mise en place d'un troisième stockage d'archivage inactif de nos données. Ce serveur est dédié au Plan de Reprise d'activité.

Les données sont glissantes sur un mois. En cas d'attaque, le virus ne peut évoluer sur ce serveur, ce qui facilite la reprise d'activité dans les meilleures conditions.

INTERDICTION DES CLES USB OU PERIPHERIQUES EXTERNES SUR TOUS LES PC INFORMATIQUES

Les périphériques et clés USB sont rapidement devenus un des principaux vecteurs d'attaque, au 2ème rang du classement des Cybermenaces. Utiliser une clé USB n'est donc pas sans risque et peut causer de graves préjudices :

- **prise de contrôle** de votre appareil,
- **espionnage** à distance,
- **blocage** ou même destruction totale grâce à la " Killer Key " qui détruit instantanément le système informatique du dispositif (tour, écran, etc.) grâce à une surcharge électrique.
- récupérer en quelques secondes, **les mots de passe enregistrés** en clair et de les faire transiter par la messagerie de la victime.

Le Comité de Direction a donc décidé d'interdire les clés USB sur l'ensemble des postes des collaborateurs du GSA+.
Seuls les correspondants informatiques pourront dans un cadre très exceptionnel, en avoir l'usage.

Les outils de remplacement :
SharePoint ou WeTransfert peuvent remplacer la clé USB et permettre l'échange de documents avec son correspondant.

SYNTHESE DES BONS REFLEXES

	Les bons réflexes des collaborateurs	Les protections infrastructure GSA+
L'hameçonnage	Au moindre doute ou interrogation sur le mail reçu (objet du mail, pertinence des propos...): • vérifier la provenance **avant** l'ouverture des pièces jointes ou le clic sur le lien. • Vérifier par appel téléphonique du correspondant en cas de doute	L'organisation de campagnes de phishing La mise en place de l'outil VADE SECUR, pour maximiser nos BAL. La relecture régulière des procédures pour une meilleure application en temps réel des bons réflexes.
Le programme malveillant	Il est important de s'assurer de la bonne provenance des installations de logiciels lorsqu'ils sont autorisés sur nos postes.	Nous sommes très limités dans l'installation de logiciels ou d'applications. Le service informatique limite fortement les risques en mettant en place des protections d'installations.
L'usurpation d'identité	Ne jamais renseigner son identifiant / Mot de passe suite à un clic sur un lien en provenance d'un mail avant d'avoir vérifier sa provenance réelle. (vérifier par appel téléphonique si doute)	L'outil INWEBO est installé sur tous les postes La double authentification empêchera l'accès à notre réseau en cas d'usurpation d'identité.

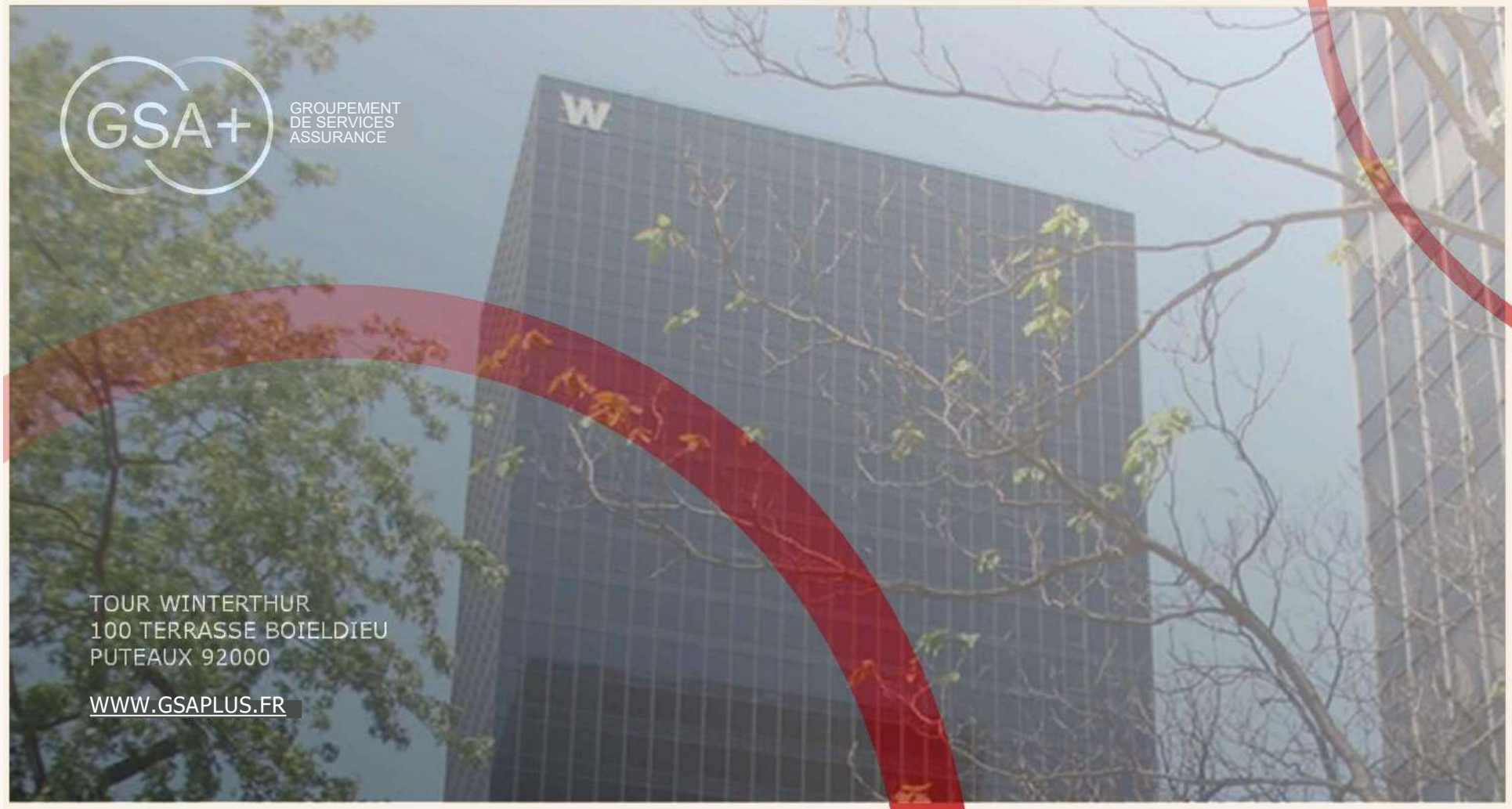
VOS REFERENTS INFORMATIQUES

GSA+

Abilio MATIAS	01 47 76 53 27
Ou en son absence	
Gaëlle BONTET	01 47 76 52 50

Référents

ASSUROL - Delphine Guay	01 47 76 53 24
ASSURATOME – Philippe RENAUT	01 47 76 53 50
AMSRE – Céline MAISON	01 47 76 89 52


GSA+
GROUPEMENT
DE SERVICES
ASSURANCE
TOUR WINTERTHUR
100 TERRASSE BOIELDIEU
PUTEAUX 92000
WWW.GSAPLUS.FR