TENDANCES 2019

CYBER THREAT INTELLIGENCE

INTRINSEC
Innovative by design

SECTEURS LES PLUS CIBLÉS

Finance

Secteur historiquement ciblé pour le profit financier

Distribution

La transformation digitale du secteur entraîne un intérêt croissant pour les données clients et leur revente

Énergie

La présence plus importante d'IoT et l'automatisation des processus industriels augmentent les possibilités d'attaques

LOGICIELS MALVEILLANTS

30% de nos investigations en réponse aux incidents identifiant un malware à l'origine de la compromission d'un serveur avec en majorité :

- Ransomware
- Mineurs de cryptomonnaies
- Trojan

RÉSEAUX UNDERGROUND : QUELQUES TENDANCES À SUIVRE

- **Diversification des espaces d'échanges** : l'arrestation des administrateurs de sites malveillants sur le réseau Tor a amené les membres de cet écosystème à se déplacer sur d'autres réseaux tels que les réseaux sociaux et applications de messagerie (Telegram, WhatsApp, Discord, etc.)
- **Intérêt constant pour la revente d'identifiants clients** obtenus de manière illégitime via le piratage de base de données ou via des attaques de type credentials stuffing menées à l'aide d'outils comme Sentry MBA, SNIPR ou STORM
- **Revente d'identifiants techniques** : accès à des serveurs RDP, à des interfaces de contrôle SCADA

TENDANCES 2019

CYBER THREAT INTELLIGENCE

INTRINSEC
Innovative by design

FUITE DE DONNÉES

Fuite de données internes et sensibles d'entreprises (patrimoine informationnel)

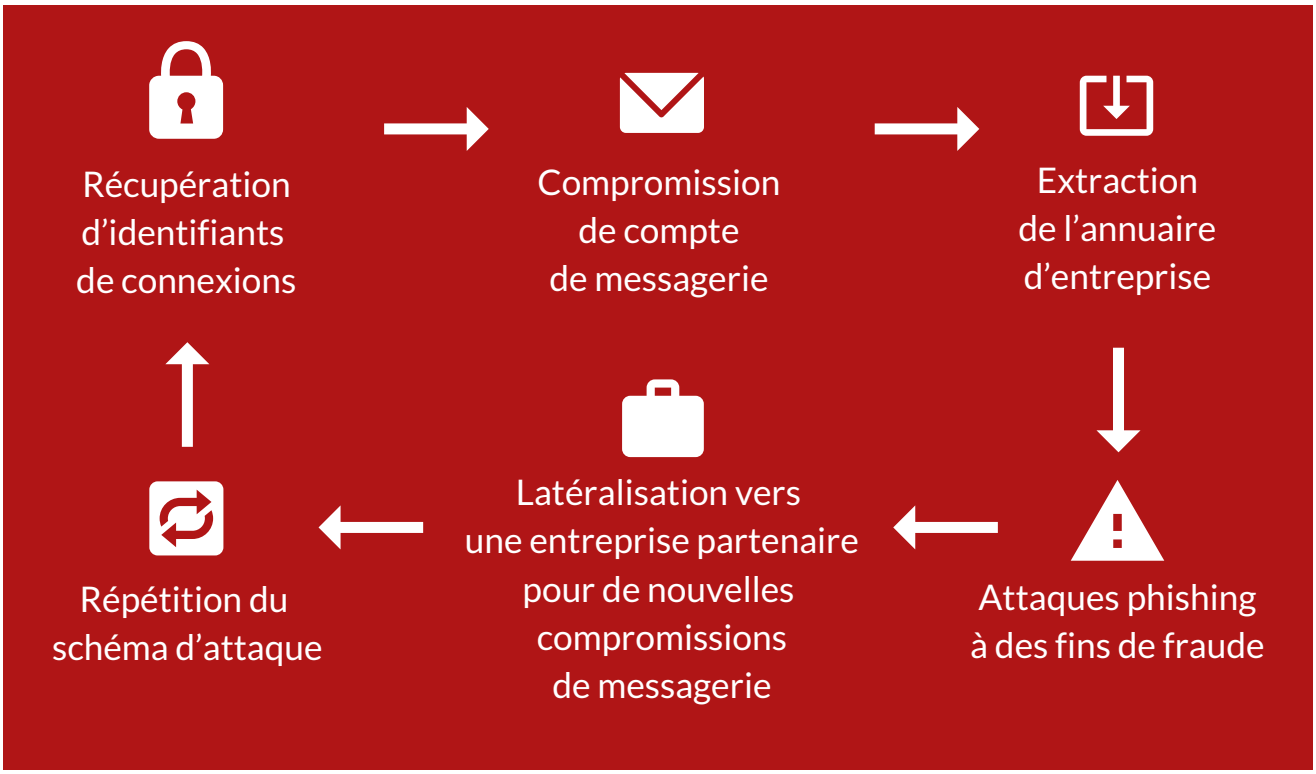
Base de données utilisateur exposées / Exfiltration de données personnelles.

Insider threat (fuite involontaire provenant d'un collaborateur) : partage réseau, usage Dropbox...

PHISHING

Menace encore et toujours d'actualité (manque de sensibilisation, facilité de mise en œuvre…), le risque de phishing et la sophistication des campagnes pèseront en 2019

Augmentation en fréquence d'un scénario s'alimentant lui-même



TENDANCES 2019

CYBER THREAT INTELLIGENCE

INTRINSEC
Innovative by design

ATTAQUE IOT

L'exploitation des objets connectés à des fins malveillantes devrait s'intensifier en 2019

Cette intensification amplifierait le **risque pour les utilisateurs finaux** (e.g. exploitation de vulnérabilité sur des véhicules connectés) ou bien encore **pour des infrastructures critiques** : exploitation d'objets connectés ou développement de malware visant des IoT présents au sein d'installations industrielles pour sabotage, panne...

ATTAQUE SUPPLY CHAIN

Attaque d'un fournisseur de confiance pour compromettre une cible finale

Compromission d'applications tierces installées sur des sites (e.g. cas du plugin Wordpress RGPD) pour compromettre un maximum de cibles. Beaucoup de ces modules manquent de transparence dans leur gestion des failles et demandent une surveillance spécifique.

NOS RECOMMANDATIONS

Pour réduire les risques face à ces menaces, de nombreuses approches complémentaires existent :

- La lutte contre le phishing via l'identification des acteurs malveillants essayant d'usurper votre marque
- La vérification de votre empreinte sur Internet afin de détecter votre Shadow IT
- La sensibilisation spécifique et adaptée à votre secteur/vos activités
- La réalisation de scans de vulnérabilités afin d'identifier les plugins tiers installés sur vos serveurs
- La mise en place d'une surveillance cyber complétant le dispositif de protection des données
- L'anticipation des moyens de réponses aux incidents afin de disposer des capacités de hunting et d'une organisation prête à réagir rapidement.