McAfee
Together is power.

Prévisions 2019 en matière de menaces

McAfee Labs

Partenariats cybercriminels

Les cybercriminels vont renforcer leur coopération, avec des familles de services MaaS (Malware-as-a-service) moins nombreuses mais plus performantes.

Des places de marché centralisées

Les cybercriminels peuvent acheter des logiciels malveillants, des exploits, des botnets et d'autres services véreux sur le marché clandestin. Il devient facile pour les criminels de tout acabit de lancer des attaques, quel que soit leur expérience ou leur niveau de compétences.

Consolidation du marché clandestin

Les familles de services MaaS vont agir de concert. Ces alliances vont prospérer grâce à la diversité de leurs affiliés, par exemple lorsque des kits d'exploits viennent optimiser les logiciels de demande de rançon (GandCrab).

Les grands noms élargissent le champ d'action

Des produits toujours plus puissants conduiront à un minage de cryptomonnaies plus sophistiqué, à un essor des malwares sur mobiles et à une augmentation des vols d'identifiants et d'informations de cartes de crédit.

Exploitation plus rapide

Les cybercriminels vont gagner en agilité. En 2019, ils exploiteront des vulnérabilités éphémères, raccourcissant le délai entre la détection d'une vulnérabilité et sa conversion en vecteur d'attaque.

Techniques de contournement

L'externalisation croissante des attaques va entraîner l'utilisation de l'intelligence artificielle dans les tactiques de contournement.

Outils de contournement

Les outils de compression, de chiffrement et autres font souvent partie de l'arsenal permettant d'échapper à la détection. Les techniques de contournement gagnent en agilité grâce à l'intégration de l'intelligence artificielle.

Agilité de contournement

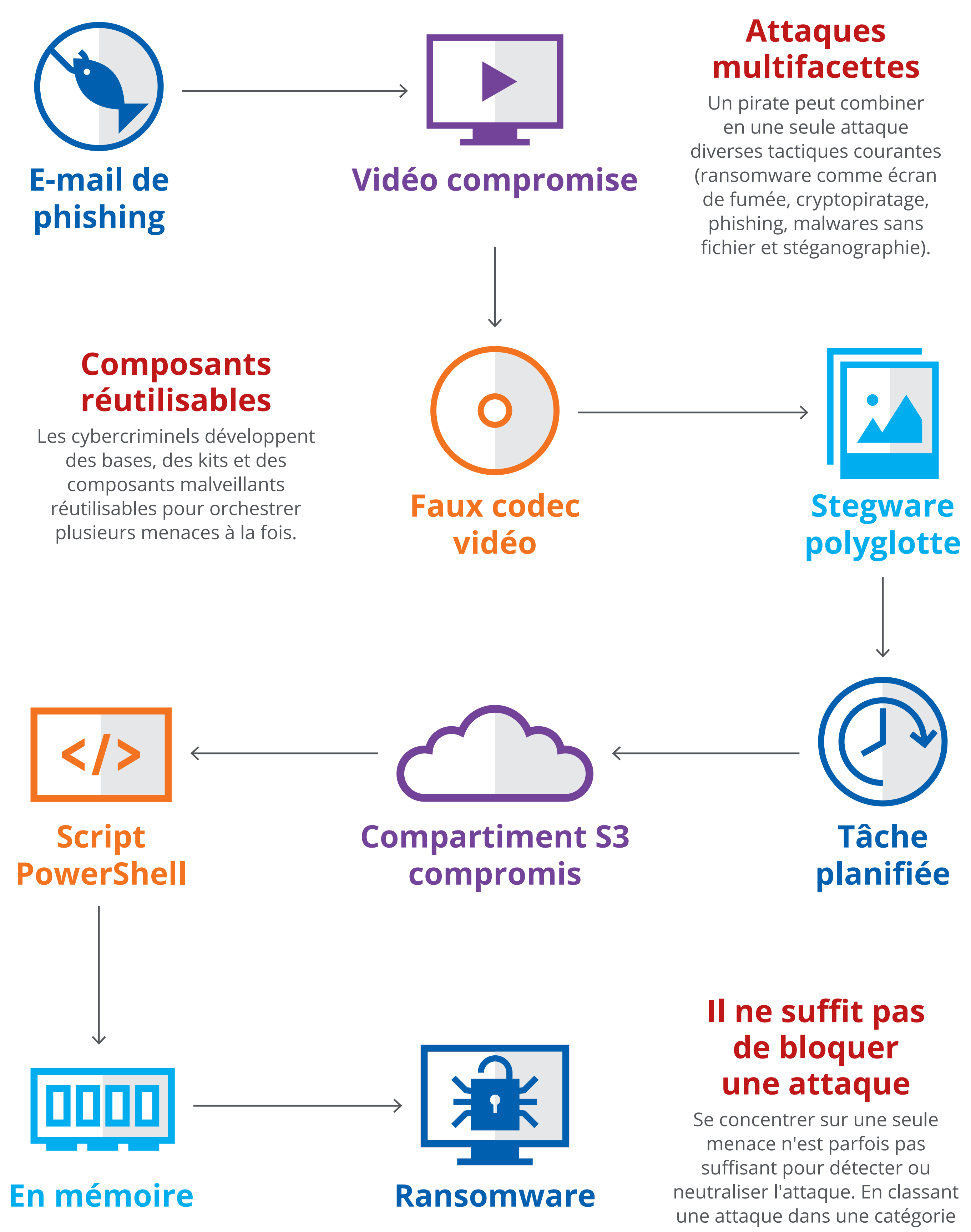
Au nombre des techniques employées : un mineur de cryptomonnaie qui s'arrête lorsque le Gestionnaire des tâches ou une analyse sont exécutés ; des kits d'exploits qui utilisent l'injection de processus ou la manipulation de l'espace mémoire pour insérer du code ; des botnets qui ajoutent du code dissimulé pour ralentir la rétroconception, ou encore des APT qui utilisent des certificats volés pour échapper à la détection.

Intelligence artificielle

Les criminels vont tirer parti de l'intelligence artificielle pour automatiser la sélection des cibles et vérifier les environnements infectés avant le déploiement des phases ultérieures afin d'éviter la détection.

Identification des attaques

Des attaques associant plusieurs menaces synergiques créent un écran de fumée et empêchent les professionnels de la sécurité d'identifier le but ultime de l'entité malveillante.



Attaques multifacettes

Un pirate peut combiner en une seule attaque diverses tactiques courantes (ransomware comme écran de fumée, cryptopiratage, phishing, malwares sans fichier et stéganographie).

Composants réutilisables

Les cybercriminels développent des bases, des kits et des composants malveillants réutilisables pour orchestrer plusieurs menaces à la fois.

Il ne suffit pas de bloquer une attaque

Se concentrer sur une seule menace n'est parfois pas suffisant pour détecter ou neutraliser l'attaque. En classant une attaque dans une catégorie donnée, on risque de ne pas la percevoir dans sa globalité et d'être moins efficace pour la neutraliser.

Attaques d'exfiltration des données dans le cloud

Davantage de données à voler

Les entreprises poursuivent leur adoption massive du cloud sous diverses formes (SaaS, PaaS, IaaS). Conséquence : le volume de données stockées dans le cloud augmente. Les attaques vont suivre la même tendance et cibler de plus en plus souvent ces services de cloud.

Informations sensibles

Dans son Rapport sur l'adoption du cloud et les risques associés, McAfee révèle que **21 % des données** dans le cloud sont de nature sensible, notamment la propriété intellectuelle, les informations clients et les données à caractère personnel.

Attaques MITM

GhostWriter : utilise le cloud comme tremplin pour les attaques natives au cloud de type man-in-the-middle, **pour lancer des attaques de cryptopiratage ou par ransomware**.

Office 365 devient une cible

KnockKnock : l'adoption en masse d'Office 365 a entraîné une multiplication des attaques, surtout les tentatives de compromission de la messagerie électronique. À titre d'exemple, le **botnet KnockKnock qui cible les comptes système non soumis à l'authentification multifacteur**.

Assistants numériques à commande vocale

Nouveau point d'entrée dans les foyers

De plus en plus d'assistants numériques à commande vocale sont utilisés par les particuliers pour gérer les appareils IoT. Cette tendance va fournir aux cybercriminels un nouveau point d'accès aux réseaux domestiques.

Connexion par téléphone

Les auteurs de logiciels malveillants vont exploiter les téléphones et les tablettes pour prendre le contrôle des appareils IoT en craquant leurs mots de passe et en exploitant leurs vulnérabilités.

Appareil approuvé

Comme le trafic proviendra d'un appareil de confiance, il ne déclenchera pas de signal d'alarme, ce qui rendra les vecteurs d'attaque plus difficiles à identifier.

Commandes vocales

Des activités malveillantes comme l'ouverture de portes et la connexion à des serveurs de contrôle pourraient être déclenchées par des commandes vocales de l'utilisateur (« Lire ma musique » et « Quelle sera la météo aujourd'hui ? »).

Recrutement dans des botnets

Les appareils IoT infectés viendront grossir les rangs des botnets qui pourront lancer des attaques DDoS et voler des données à caractère personnel.

Plates-formes de gestion des identités et périphériques de périmètre

Les plates-formes de gestion des identités à grande échelle assurent des fonctions sécurisées d'authentification et d'autorisation des utilisateurs, des équipements et des services. Elles constituent une cible de choix pour les cybercriminels.

Réseaux sociaux

En dépit des efforts de sécurité déployés par les fournisseurs d'infrastructure, leurs environnements restent une cible lucrative pour les cybercriminels en raison des données qu'ils hébergent. Ce sera le prochain champ de bataille.

Périphériques de périmètre

En exploitant les mots de passe statiques et la sécurité limitée, les cybercriminels vont continuer à lancer des attaques à distance contre des périphériques de périmètre (protocole ou matériel système permettant la mise en réseau et embarqué dans un produit IoT).

Fragilité des modèles d'approbation

Le modèle d'approbation de l'IoT repose sur une confiance présumée et une sécurité basée sur le périmètre. Comme la plupart des périphériques de périmètre IoT n'ont aucun système de défense intégré par défaut, un exploit qui aboutit prend le contrôle total de l'équipement.

Sécurisation de nos systèmes

L'authentification multifacteur et la cyberveille sur les identités deviendront les méthodes les plus efficaces pour garantir la sécurité dans cette lutte sans merci.

Multiplication des campagnes de désinformation contre les entreprises

Les fausses informations et les campagnes d'extorsion via les réseaux sociaux vont cibler des marques et ne seront plus le fait d'États mais de groupes criminels.

Contenu mensonger

Les comptes de botnet transmettent et diffusent des messages, qui souvent mettent en avant deux opinions opposées sur un même thème afin de susciter la polémique. Les messages les plus performants sont amplifiés pour harceler les sociétés et leur soutirer de l'argent en menaçant leurs marques.

Diffusion rapide

Un compte robot avec 279 abonnés, dont la plupart étaient d'autres robots, a lancé une campagne de harcèlement contre une entreprise. Par amplification, le compte a généré 1 500 abonnés supplémentaires en seulement quatre semaines, simplement en envoyant des tweets malveillants à propos de leur cible.

Lisez le rapport *Prévisions 2019 en matière de menaces* de McAfee Labs.
Consultez la page www.mcafee.com/2019Predictions pour obtenir le rapport complet.

McAfee
Together is power.

Décembre 2018