Les pirates de Turla jouent à cache-cache grâce aux satellites

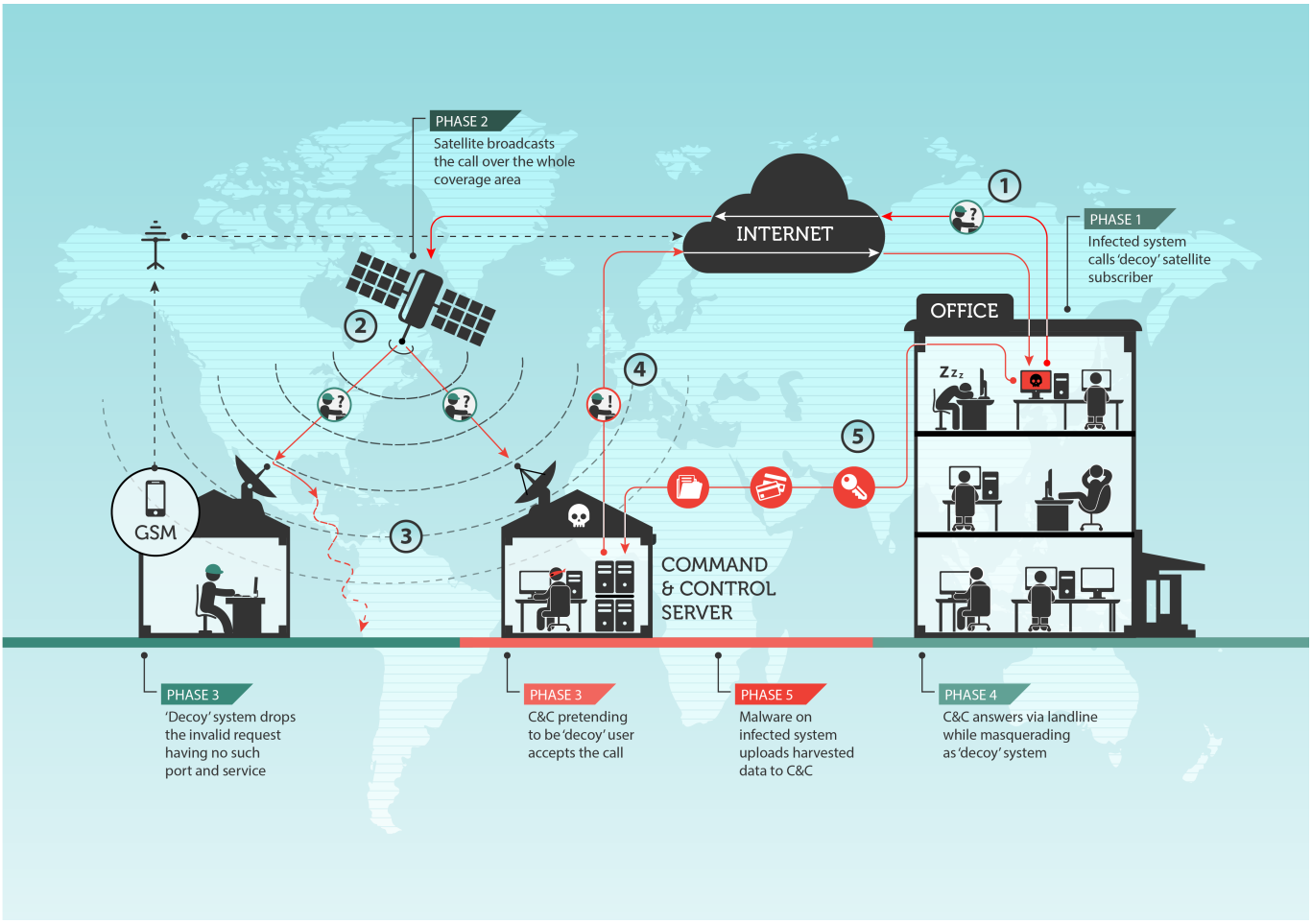
Vivons heureux, vivons cachés ! Tel est le credo des cybercriminels qui développent des APT (Advanced Persitent Threat). Et les cybercriminels du groupe Turla ont trouvé une méthode originale pour masquer leurs méfaits. Ils sont capables d'**intercepter du trafic Internet de certains satellites** et de l'utiliser pour **masquer l'emplacement de leurs serveurs de Commandes et Contrôle (C&C)**. Ils s'appuient pour cela sur des faiblesses de sécurité de la communication par satellites.

C'est ce qui ressort des travaux réalisés par Stefan Tanase, chercheur chez Kaspersky. Il a décortiqué les actions prêtées à ce groupe, qui œuvre depuis au moins 2007 et qui est à l'origine d'un rootkit sophistiqué baptisé Uburos découvert en 2014. On soupçonne cette organisation, spécialisée dans le cyberespionnage, d'être d'origine russe ou, pour le moins, russophone.

Dans ses recherches, le spécialiste constate qu'il y a plusieurs années, les satellites qui tournent en orbite autour de la terre ont été utilisés pour apporter de l'Internet dans certaines zones reculées. Or, la communication descendante, via **le protocole DVB-S**, de ces satellites **n'est pas chiffrée**. Une manne pour les cybercriminels de Turla qui en profitent pour détourner ce trafic.

Une méthode pratiquement indétectable

Concrètement, ils ont acquis une antenne parabolique et une carte d'acquisition du signal pour « snifer » le trafic dans une zone couverte par le satellite. Ils ont également pris des locaux dans cette zone pour y installer les serveurs C&C reliés à une connexion Internet fixe. Le modus operandi s'apparente alors à une attaque de type MITM (Man in The Middle). A travers le trafic descendant des satellites, il récupère une adresse IP d'un utilisateur, envoie des données depuis cette adresse à des PC pour les infecter puis pilote les malwares ainsi déployés sans que l'utilisateur s'en rende compte (cf schéma ci-dessous).



La méthode est aussi quasiment indétectable, car les satellites diffusent des données sur une large zone de couverture (plusieurs milliers de kilomètres). Il n'est pas nécessaire pour les pirates d'être proches de leur victime (jusqu'à une centaine de kilomètres).

Ce *modus operandi* permet de garder un haut degré d'anonymat. Les zones ciblées par les pirates sont l'Afrique et le Moyen-Orient. L'Amérique du Nord et l'Europe sont épargnées, car ces zones sont desservies par des satellites de conception plus modernes avec des connexions chiffrées. Pour autant, Stefan Natase constate que les liens satellites ne restent jamais actifs très longtemps, en général quelques mois. Deux raisons peuvent expliquer ce phénomène : soit il s'agit d'une auto-limitation fixée par Turla, soit les fournisseurs de services satellitaires coupent le lien face à un comportement identifié comme malveillant.

La technique des liens satellitaires n'est pas nouvelle, souligne le chercheur de Kaspersky. Au moins trois groupes l'ont déjà pratiqué : Hacking Team, Xumuxu et Rocket Kitten APT. Cependant, l'équipe de Turla l'a amélioré et à moindre coût. L'investissement de départ est sous la barre des 1 000 dollars (notamment avec l'antenne, plus une carte tuner DVB-S), la maintenance coûterait moins de 1 000 dollars par an. Un coût et une simplicité qui étonne le spécialiste, habitué à la complexité des techniques du groupe de cybercriminels.

A lire aussi :

Opération Epic Turla : les services européens de renseignement espionnés
Failles de sécurité : le double jeu des gouvernements

crédit photo © Andrey VP – shutterstock