Les fournisseurs d'hébergement « invincibles » : les fissures dans l'armure des infrastructures cybercriminelles

Les cybercriminels qui parviennent à leurs fins dépendent d'infrastructures sécurisées, indétectables et résilientes. Chaque cas de compromission de réseau, de vol d'identifiants de connexion, de rançongiciel ou de vol et vente de données sur des forums illicites repose sur une infrastructure sécurisée qui permet aux cybercriminels d'agir et de rester cachés.

Toutefois, pour les cybercriminels, il devient de plus en plus problématique de rester indétectables et difficiles à repérer. Compte tenu de la collaboration mondiale entre les gouvernements, les organismes d'application de la loi et le secteur privé, il leur est plus difficile de préserver leur anonymat en ligne. De plus, très peu de cybercriminels possèdent les compétences et l'expertise requises pour gérer et maintenir seuls une infrastructure sécurisée. Ils recherchent donc des fournisseurs d'infrastructures illicites qui peuvent assurer ce service pour leur compte, ce qui permet aux cybercriminels de se focaliser sur leurs victimes et leurs profits.

La « cybercriminalité en tant que service » désigne le marché clandestin qui s'est développé pour soutenir un éventail d'acteurs malveillants en ligne. Ce marché clandestin comprend une gamme d'outils, de services et d'informations en vente qui ne cesse de croître et d'évoluer et aide les cybercriminels à nuire à leurs cibles en ligne. Les cybercriminels potentiels peuvent acheter l'accès à des réseaux, des outils leur permettant d'échapper aux mesures de sécurité et des logiciels malveillants à déployer contre leurs victimes pour leur voler des informations à caractère personnel. Les fournisseurs d'hébergement invincibles font partie de cet écosystème et proposent des infrastructures sécurisées aux cybercriminels. Il est important de noter qu'un seul hébergeur invincible peut permettre directement à des centaines de cybercriminels de cibler des victimes dans le monde entier.

Qu'est-ce qu'un fournisseur d'hébergement « invincible » ?

En bref, les fournisseurs d'hébergement invincibles louent à des cybercriminels une infrastructure virtuelle et/ou physique depuis laquelle ils peuvent agir. Les fournisseurs d'hébergement invincibles proposent une catégorie spécifique de services d'infrastructure Internet qui permet aux acteurs malveillants (dont les cybercriminels) d'héberger du contenu illicite et de mener des opérations sur Internet.

Le terme « invincible » (bulletproof) relève purement du marketing. En réalité, ces services sont tout autant exposés aux perturbations que ceux d'autres fournisseurs d'infrastructures. Cela dit, les fournisseurs d'hébergement invincibles refusent de respecter les demandes de suppression de leur contenu émanant des organismes d'application de la loi et d'autres demandes, et ignorent les plaintes des victimes et les avis de demandes des abonnés. En d'autres termes, les cybercriminels peuvent communiquer, gérer des forums et des sites Internet illicites, déployer des logiciels malveillants et des campagnes d'hameçonnage, et se livrer au blanchiment d'argent sans craindre que l'opérateur résilie leur location si des organismes d'application de la loi ou d'autres entités le demandent.

Les fournisseurs d'hébergement invincibles participent en toute connaissance de cause à l'écosystème de la cybercriminalité et facilitent de graves délits en ligne motivés par le profit. Des incidents de cybersécurité majeurs à l'encontre d'organisations australiennes et de leurs clients ont eu lieu du fait du recours à des fournisseurs d'hébergement invincibles par des criminels. Ces incidents ont eu pour conséquences des attaques par rançongiciels aux effets perturbateurs, l'extorsion de données et le vol d'informations sensibles.

Représentation de la publicité d'un fournisseur d'hébergement invincible sur des forums clandestins :

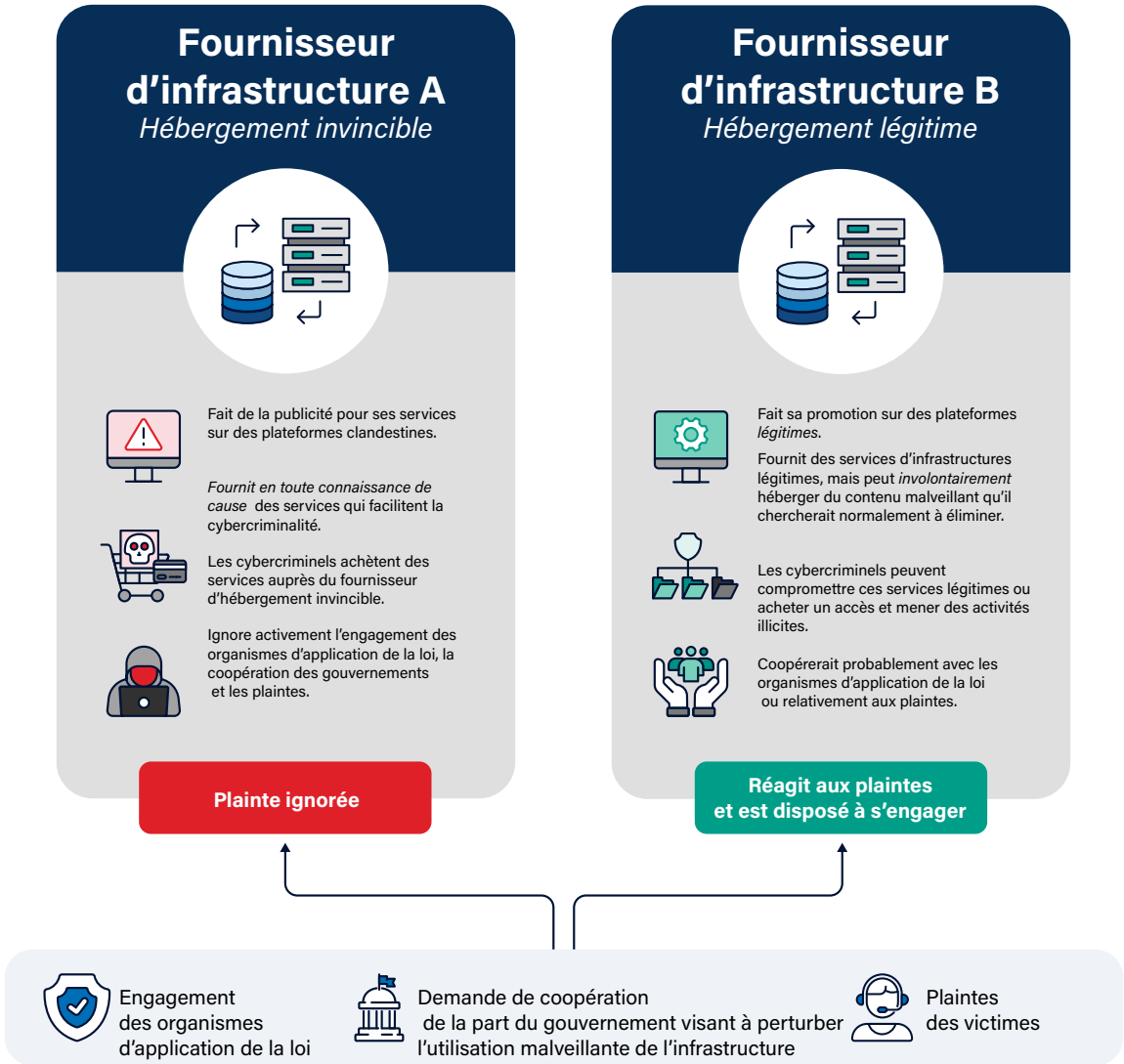
Quel est le mode opératoire des fournisseurs d'hébergement invincibles ?

Le modèle d'entreprise diffère selon le fournisseur d'hébergement invincible. La méthode la plus courante implique la location d'adresses IP à des clients cybercriminels et l'utilisation de procédures complexes de commutation de réseau pour contribuer à dissimuler leurs emplacements, leur identité et leurs activités. Dans de nombreux cas, les fournisseurs d'hébergement invincibles revendent ou louent des adresses IP et des serveurs provenant de fournisseurs d'hébergement, de centres de données ou de fournisseurs d'accès Internet

légitimes. Ces prestataires « en amont » ne savent pas nécessairement qu'ils permettent à des fournisseurs d'hébergement invincibles de bénéficier d'une infrastructure et que ceux-ci fournissent ensuite des services « en aval » à des cybercriminels.

Les fournisseurs d'hébergement invincibles configurent leurs réseaux et leur architecture système de manière à ce qu'il soit plus difficile d'identifier leurs clients. Par exemple, ils changent fréquemment les identifiants Internet associés à l'activité de leurs clients – comme les adresses IP qui leur ont été assignées et leur nom de domaine. De telles techniques sont problématiques pour les défenseurs et les enquêteurs, car il est plus difficile de relier un incident et une adresse IP utilisée par un acteur ou un client à un moment donné. En outre, les fournisseurs d'hébergement invincibles utilisent souvent des infrastructures dans des pays aux approches permissives en matière d'Internet et où les mesures formelles d'enquête et de prévention des activités malveillantes en ligne sont clémentes, voire inexistantes.

Qu'est-ce qui distingue les fournisseurs d'hébergement invincibles des fournisseurs d'infrastructures légitimes ?



L'impact du ciblage des fournisseurs d'hébergement invincibles sur les menaces de la cybercriminalité

Les fournisseurs d'hébergement invincibles offrent une précieuse opportunité de perturber simultanément des centaines, voire des milliers de cybercriminels. Un certain nombre de cybercriminels et d'autres acteurs malveillants en ligne recourent à ces services pour faciliter leurs délits – comptant sur le fait que leurs activités resteront dissimulées et opérationnelles malgré les demandes de suppression ou les plaintes.

Toutefois, les organismes d'application de la loi, les agences gouvernementales et le secteur privé collaborent en vue de cibler et de perturber ces fournisseurs d'infrastructures illicites, notamment dans le cadre de mesures défensives, par exemple en bloquant proactivement le trafic Internet qui provient de fournisseurs d'hébergement invincibles connus. Ces activités contribuent à réduire l'ampleur de la cybercriminalité sur les réseaux australiens et alliés, et comprennent des fournisseurs légitimes d'infrastructures et de services Internet « en amont » qui ne savent pas nécessairement qu'ils facilitent l'accès Internet à des fournisseurs d'hébergement invincibles et fournissent des infrastructures sécurisées à des cybercriminels.

Les fournisseurs d'hébergement invincibles ne sont pas l'unique catégorie de fournisseurs d'infrastructures dans l'écosystème de la cybercriminalité en tant que service. Ces services perpétuent la menace de la cybercriminalité en Australie et la facilitent en soutenant activement les campagnes de cybercriminels et en entravant délibérément les enquêtes et les interventions légales. Les actions menées contre les fournisseurs d'hébergement invincibles permettent d'exposer la vulnérabilité de ces services et les types d'acteurs malveillants en ligne qui les utilisent.