PLATEFORME DE
SENSIBLISATION SUR
LA SECURITE NUMERIQUE

CYBER ATTAQUES

DES MODES OPERATOIRES DE PLUS EN PLUS REPANDUS

CENTRE D'INFORMATIQUE ET DE RECHERCHE
DE L'ARMEE ET DE LA SECURITE
(CIRAS)

Adresse: 36 rue Lamothe, Plateau centre ville
Brazzaville, B.P: 15422
Tel: 00 242 22 281 58 71
Email: contact@pssn.cg
Site web: www.pssn.cg

CYBER ATTAQUES
DES MODES OPERATOIRES DE PLUS EN PLUS REPANDUS

Botnets

Le principe du botnet est de pouvoir lancer des attaques de grande envergure en utilisant frauduleusement de nombreux ordinateurs répartis géographiquement. Une fois infectés, les ordinateurs obéissent à distance aux instructions d'une unité de commande et de contrôle (appelée C&C), et n'ont plus qu'à attendre des instructions pour lancer des attaques. Certains botnets sont ainsi composés de dizaines, voire centaines de milliers, d'ordinateurs localisés dans plusieurs pays.

Le « use case » le plus classique du botnet réside dans le lancement d'attaques par déni de service distribué (DDOS) dont l'objectif est de paralyser ou rendre indisponibles des réseaux ou serveurs de tiers (sites web de banques, institutions gouvernementales, etc.). Si le continent Africain n'est pas aujourd'hui à l'origine de botnets, il y participe à travers les nombreuses machines infectées (dites machines « zombie ») qu'il abrite. Ses infrastructures peuvent également être la cible de botnets, à l'image de l'attaque du botnet Mirai contre le Libéria en novembre 2016.

L'Afrique en général, et l'Afrique de l'Ouest en particulier, sont donc une victime collatérale des botnets du fait de la faible protection des infrastructures numériques. Et plus les pays sont connectés, plus ils sont infectés, ce qui démontre que l'usage du numérique ne vas pas forcément de pair avec la mise en place de mesures d'hygiène numérique….

Défiguration de sites web (ou « défacement »)

Lors d'une défiguration, le cybercriminel va afficher un message, une image ou sa signature en exploitant les vulnérabilités d'un site web. Les « défacements » ciblant l'Afrique sont aujourd'hui relativement anodins car rarement menés pour des raisons idéologiques. Les pirates agissent plus par goût du défi et volonté de laisser une « trace », en général une simple signature sur le site internet piraté.

Hameçonnage (ou « phishing »)

L'hameçonnage est une pratique qui consiste pour le cybercriminel à usurper une identité pour obtenir des renseignements personnels (mot de passe, numéro de carte de crédit...). Le pirate fait croire à sa victime qu'elle a à faire à un tiers de confiance (administration, banque, sécurité sociale…) pour appuyer sa demande de renseignements. Cette technique est un grand classique de la cybercriminalité africaine, le gain financier pouvant être immédiat et très important dans le cas de la récupération de données bancaires.

Les black markets

De la même manière que se sont progressivement constitués des forums et marchés noirs russophones, anglophones ou francophones, on assiste depuis près de 18 mois à l'émergence de forums cybercriminels africains, en particulier nigérians. Ces derniers proposent des outils ou des fraudes spécifiquement adaptés aux infrastructures et services d'Afrique de l'Ouest et draine une véritable communauté spécialisée de cybercriminels.

Sources et citations

CEIS