_swissprivacy.law

Rétrospective sur les attaques d'hacktivisme en Suisse

Pauline Meyer, le 16 novembre 2023

Le Centre national pour la cybersécurité (NCSC) publie son rapport semestriel couvrant la période de janvier à juin 2023. Il y traite principalement d'attaques relevant d'hacktivisme et parcourt les différentes annonces reçues et la situation relative aux cybermenaces.

Rapport semestriel 2023/I (janvier à juin) du 2 novembre 2023

Le thème prioritaire du rapport semestriel 2023/1 du NCSC concerne l'hacktivisme. L'hacktivisme est caractérisé par des actions illégales perpétrées dans le cyberespace par des auteurs dont l'activité est motivée par une idéologie. La guerre en Ukraine donne lieu au développement de plusieurs groupes d'hacktivistes prenant parti pour l'un ou l'autre des États belligérants. Il n'y a en revanche pas systématiquement de liens entre les groupes d'hacktivistes perpétrant des attaques et les gouvernements impliqués dans le conflit.

Les objectifs souvent poursuivis par les auteurs dans ce contexte sont le souhait d'attirer l'attention et, potentiellement, de créer de l'insécurité ou détruire la confiance dans les organisations exploitant les sites touchés.

Les attaques en déni de service distribué (*Distributed Denial of Service, DDoS*) constituent une typologie d'attaques particulièrement utilisée par les hacktivistes. Ces attaques consistent en la saturation d'un service par des requêtes simultanées émanant d'un grand nombre d'ordinateurs situés dans différents lieux pour rendre ce service indisponible. La conséquence principale est l'indisponibilité temporaire du site web de l'organisation visée par l'attaque.

Le rapport traite de différents sites web suisses ayant fait l'objet de telles attaques durant le premier semestre de 2023. Le site des Services du Parlement fait par exemple partie des cibles avec une première attaque DDoS à la suite d'une décision du Conseil des États en lien avec la loi fédérale sur le matériel de guerre. La seconde est déclenchée par l'annonce du discours du président ukrainien Volodymyr Zelensky devant l'Assemblée fédérale et surcharge non seulement le site web des Services du Parlement, mais aussi de certains offices, de cantons et de villes ainsi que de l'Association suisse des banquiers. Le NCSC décrit ces attaques en détail dans un rapport complémentaire sur les attaques DDoS de juin 2023.

Le NCSC rappelle dans son rapport que les attaques DDoS peuvent être déjouées. Il est possible de se référer aux mesures proposées par le NCSC pour prévenir et réagir à de telles attaques. Il peut être utile, surtout pour les systèmes critiques, de s'abonner préventivement à une protection DDoS commerciale.

Dans les attaques DDoS parcourues par le NCSC, les mesures prises par Swisscom sont citées, allant notamment du blocage du trafic issu des pays dont provenait la majeure partie des requêtes DDoS à la limitation de débit sur l'équilibreur de charge pour décharger durablement le serveur web. Le NCSC partage une série de mesures proactives et réactives dans son rapport complémentaire sur les attaques DDoS de juin 2023.

D'autres attaques sont susceptibles d'être perpétrées par des hacktivistes. Il en va tout d'abord de la sorte pour le défacement, à savoir l'altération par le biais d'une cyberattaque du code d'un site web, entraînant ainsi la modification de son contenu. Cela se traduit régulièrement par l'exposition des revendications des hacktivistes. Le piratage et la divulgation sont ensuite aussi réalisés dans ce contexte par la pénétration dans des systèmes informatiques, la soustraction de données et leur publication. Finalement, les hacktivistes effectuent régulièrement des tentatives de sabotage. Il est important de mettre en œuvre les recommandations existantes pour se prémunir adéquatement contre ces activités, de faire surveiller automatiquement les sites web pour être alerté lors de potentielles modifications et de réagir en cas d'alerte.

Le NCSC fait ensuite part, dans son rapport, des 19'048 annonces de cyberincidents reçues durant le premier semestre de 2023, soit 2'000 annonces de plus qu'au premier semestre de 2022. Les annonces concernent principalement des fraudes. La majorité des annonces constituent toujours de la fausse extorsion sous forme de courriels de menace émanant prétendument d'une autorité.

Une hausse de cas d'hameçonnage de 40% est identifiée par le NCSC, principalement en raison d'une vague d'hameçonnage contre les clients SwissPass. D'autres tentatives d'hameçonnage prennent la forme d'un SMS de fausses alertes de livraison de colis ou d'appels téléphoniques de prétendus collaborateurs d'entreprises de télécommunication cherchant à obtenir le code de sécurité envoyé par SMS dans le cadre d'une authentification multifactorielle.

Le NCSC termine son rapport avec des explications sur divers phénomènes à l'instar des maliciels, rançongiciels, exploitations de vulnérabilités et failles de sécurité, accompagnées de recommandations générales.

_swissprivacy.law

Proposition de citation : Pauline MEYER, Rétrospective sur les attaques d'hacktivisme en Suisse, 16 novembre 2023 *in* www.swissprivacy.law/266

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.