QU'EST-CE LE HACKING ÉTHIQUE ?

SOPHIE ILLÈS
ingénieure d'affaires
chez Sysdream

Dans le monde du hacking, les intervenants et acteurs sont en constante croissance. Leurs profils peuvent être très différents les uns des autres. Le hacking éthique (ou *ethical hacking* en anglais) est une démarche de sécurité informatique. Elle consiste pour une société à employer une personne ou une entreprise spécialisée afin de tester l'efficacité de son système de défense.

Les hackers ne sont pas forcément des personnes malveillantes. Le mot hacker ne signifie pas « criminel », il peut définir un individu qui compromet la sécurité des ordinateurs ou, à l'inverse, un individu qui teste la sécurité d'un système informatique. Dans les faits, on distingue trois types de hackers : le *black hat* ou chapeau noir, le *white hat* ou chapeau blanc et le *grey hat* ou chapeau gris. Ces termes définissent les différents groupes de pirates en se fondant sur leur comportement.

Le black hat hacker

Le *black hat hacker* est en règle générale mêlé à des actes de malveillance (création d'un réseau de PC zombies en utilisant un *botnet* pour effectuer des attaques DDoS…) ou lié à des sujets comme la violation de la sécurité des ordinateurs à des fins profitant à lui-même (vol de numéros de carte de crédit, récolte de données personnelles pour vente massive…). L'expression « chapeau noir » fait référence aux stéréotypes largement répandus qu'un hacker est un criminel qui exerce des activités illégales à des fins personnelles et qui attaque d'autres entités.
Un *black hat hacker* qui trouve une nouvelle faille de sécurité *zero-day* la vendra à des organisations criminelles sur le marché noir ou l'utilisera pour compromettre les systèmes informatiques.

Le white hat hacker

Le *white hat hacker*, souvent appelé pentesteur, ou encore *ethical hacker*, est l'opposé du *black hat hacker*. Il s'agit d'experts en sécurité informatique qui utilisent leurs capacités à des fins honnêtes, éthiques et du côté de la justice plutôt qu'à des fins malhonnêtes. Ce profil de hackers est mandaté par des entreprises pour tester par exemple la sécurité de leur réseau ou encore de leurs applications web. Le but étant de trouver des vulnérabilités qu'un attaquant pourrait exploiter et qui permettraient de compromettre leur système. Le *white hat hacker* utilise ses connaissances pour compromettre les systèmes de l'organisation, comme un *black hat hacker* l'aurait fait. Cependant, au lieu d'utiliser ses découvertes dans son propre intérêt à des fins malveillantes, il proposera un plan d'action pour remédier aux failles recensées. Pour ce faire, un mandat d'intrusion est nécessaire, autorisant ainsi le hacker à réaliser son test d'intrusion. Sans cela, le *white hat hacker* serait en infraction avec la loi et considéré comme un cyberattaquant, réalisant des activités malveillantes. Un *white hat hacker* qui trouve une faille de sécurité dans une application la rapportera à l'éditeur, lui permettant ainsi de *patcher* et d'améliorer la sécurité de celle-ci avant qu'elle ne soit exploitée par des *black hat hackers*.
Quelques *white hats* sont célèbres, comme Barnaby Jack, Kevin Mitnick, Robert Tappan Morris ou Kevin Poulsen.

Le grey hat hacker

Un hacker à chapeau gris (ou *grey hat hacker*) se situe entre un *black hat hacker* et un *white hat hacker*. Il ne fonctionne pas pour son gain personnel mais peut techniquement commettre des crimes et mener des actions contraires à la morale. Par exemple, un *black hat hacker* pourrait compromettre un système informatique sans autorisation, voler les données pour son propre gain personnel ou vandaliser un système. Un *white hat hacker* demanderait la permission avant de tester la sécurité du système et d'alerter l'organisation de ses découvertes. Un *grey hat hacker* pourrait tenter de compromettre un système informatique sans autorisation et en informer l'organisation seulement après l'avoir fait. Qu'est-ce qui le rend différent d'un *white hat hacker* ? Même s'il a permis à l'organisation de résoudre la faille trouvée, il a compromis le système de sécurité sans autorisation, ce qui est illégal. Si un *grey hat hacker* découvre une faille de sécurité dans un logiciel ou sur un site web, il peut la divulguer publiquement au lieu de la reporter en privé à l'organisation et lui donner le temps de la corriger. Il ne veut pas profiter de la faille pour son gain personnel (qui constituerait un comportement de *black hat hacker*) mais sa divulgation pourrait entraîner des conséquences graves. En effet, un *black hat hacker* pourrait en profiter avant que cette dernière ne soit corrigée. ×