

Conflit Russie et Ukraine : un microcosme de la cyberguerre actuelle

Internet

Posté par : JulieM

Publié le : 20/7/2022 13:00:00

La guerre entre la Russie et l'Ukraine a provoqué des bouleversements à l'échelle mondiale, avec plus de 4 000 morts parmi les civils en l'espace de trois mois seulement, et aucune fin en vue.

Le conflit en cours continue d'avoir des répercussions économiques dans le monde entier, avec des marchés fluctuants et une inflation effrénée qui s'ajoutent à l'instabilité due à la pandémie, dicit Samuel Hassine, Directeur Stratégie et Opérations chez Tanium.

Les impacts de l'invasion russe sont incontestables : les consommateurs en sont affectés au quotidien par des hausses de prix et des pénuries mettant leurs foyers en difficulté.

Cependant, les conséquences les plus graves sont la probabilité grandissante d'une cyberguerre étendue, et susceptible d'avoir des effets sur la société en perturbant fortement les services publics, ainsi que l'économie mondiale.

Cette tactique est devenue un atout pour décupler l'impact des forces armées et accroître l'efficacité des opérations militaires. Différents éléments pointent d'ailleurs vers une intensification des cyberattaques sophistiquées. Quels enseignements devons-nous en tirer, et comment se préparer ?

Des sources d'inquiétudes bien réelles

Il est désormais monnaie courante de cibler des infrastructures critiques et de perturber des chaînes d'approvisionnement dans le cadre d'opérations militaires. Les cyberattaques soutenues par des États transposent cette approche au monde numérique, en perturbant le commerce ou l'accès à des services publics essentiels à l'aide de code malveillant.

De fait, la Russie a déjà lancé avec succès des attaques de grande ampleur contre l'Ukraine en 2015, provoquant une panne d'électricité massive dans plusieurs villes du pays. Les experts avaient alors attribué cette agression à « Sandworm », un groupe de pirates connu pour son affiliation avec les Services des renseignements militaires russes.

La réémergence du groupe de ransomware Conti en début d'année a manifesté par des attaques ciblant des organismes gouvernementaux costariciens qu'il montre que les outils et ressources utilisés avant le conflit russo-ukrainien restent d'actualité et évolutifs.

De plus, des groupes suspects comme tant liés au gouvernement russe, à l'image des collectifs REvil et Black Cat (ALPHV), que l'on croyait démantelés, ont donné des signes de vie dans le cadre d'une récente série d'attaques de ransomwares. Nous devrions également assister à une recrudescence des attaques menées par des sympathisants sans lien direct avec les États-nations concernés.

Cette hausse d'activité est en partie le résultat de la réactivation d'anciennes campagnes de ransomwares, afin de cibler les victimes originales, sans pour autant s'y limiter. Ils utilisent également des informations dérobées lors de la compromission initiale afin de s'en prendre aux contacts professionnels des victimes.

Ces événements récents sont des manifestations d'une tendance préoccupante au vu de l'intensification de l'activité et du comportement atypique de certains groupes de pirates bien établis. Il est donc probable qu'une lutte de pouvoir se joue après l'invasion de l'Ukraine par la Russie.

Ceci pourrait expliquer l'évolution des méthodes d'extorsion, qui aurait pour but d'accumuler davantage de gains par le biais d'actions criminelles. Nous pouvons donc nous attendre à voir cette activité perdurer tandis que nous cherchons à nous adapter à l'expansion de notre surface d'attaque.

Partage d'informations sur les menaces

Pour maîtriser les attaques, et en particulier en temps de cyberguerre, il est capital de faciliter l'échange rationalisé et en temps réel de renseignements sur les cybermenaces entre acteurs publics et privés. Jusqu'ici, ces différents organismes ont été réticents à procéder à un tel partage, mais nous devons poursuivre nos efforts afin de progresser dans ce domaine.

La collecte et le partage d'informations complètes issues de sources variées permettent en effet de faire une idée plus claire des menaces, afin d'élaborer des stratégies efficaces.

Ces informations décisionnelles et en temps réel serviront non seulement à assurer la sécurité des applications et systèmes critiques, mais aussi à mettre en œuvre les moyens nécessaires des mesures plus offensives, le cas échéant. Tout ceci devrait donc encourager les acteurs publics et privés à former des partenariats florissants sur le long terme face à l'évolution constante des menaces.

Anticiper

Le conflit entre Russie et Ukraine peut être perçu comme un microcosme de la cyberguerre actuelle. Les campagnes de piratage mondiales (récurrentes ou nouvelles) montrent que loin de disparaître, les attaques avancées sont en recrudescence, et de plus en plus sophistiquées et tenaces.

Ce conflit nous a également permis de mieux identifier nos forces et faiblesses en tant que pays, ainsi que les lacunes à combler. Les organisations publiques et privées restent bien trop réactives dans leurs approches en matière de sécurité, et nos angles morts sont trop nombreux.

Si notre champ de vision s'arrête devant notre porte, alors nous ne sommes pas réellement protégés. La résurgence des groupes cybercriminels montre que nous devons cesser de fonctionner de façon isolée (sur le plan politique ou autre), et introduire davantage de législations, mettre en place des financements, faciliter le partage d'informations pour unifier les ressources des secteurs publics et privés, et mettre l'accent sur la sécurité de notre pays.