Conflit Russie et Ukraine : un microcosme de la cyberguerre actuelle
Internet
PostÃ© par : JulieM
PubliÃ©e le : 20/7/2022 13:00:00

La guerre entre la Russie et l'Ukraine a provoquÃ© des bouleversements Ã l'Ã©chelle 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 rÃ©percussions Ã©conomiques dans le monde entier, avec des marchÃ©s fluctuants et une inflation effrÃ©nÃ©e qui s'ajoutent Ã l'instabilitÃ© due Ã la pandÃ©mie, dixit Samuel Hassine, Directeur StratÃ©gie et OpÃ©rations chez Tanium.

Les impacts de lâ□□invasion russe sont incontestables : les consommateurs en sont affectÃ©s au quotidien par des hausses de prix et des pÃ©nuries mettant leurs foyers en difficultÃ©.

Cependant, les consÃ©quences les plus graves sont la probabilitÃ© grandissante dâ□□une cyberguerre Ã©tendue, et susceptible dâ□□avoir des effets sur la sociÃ©tÃ© en perturbant fortement les services publics, ainsi que lâ□□Ã©conomie mondiale.

Cette tactique est devenue un atout pour dÃ©cupler lâ□□impact des forces armÃ©es et accroÃ®tre lâ□□efficacitÃ© des opÃ©rations militaires. DiffÃ©rents Ã©lÃ©ments pointent dâ□□ailleurs vers une intensification des cyberattaques sophistiquÃ©es. Quels enseignements devons-nous en tirer, et comment se prÃ©parer ?

Des sources dâ□□inquiÃ©tudes bien rÃ©elles

Il est dÃ©sormais monnaie courante de cibler des infrastructures critiques et de perturber des chaÃ®nes dâ□□approvisionnement dans le cadre dâ□□opÃ©rations militaires. Les cyberattaques soutenues par des Etats transposent cette approche au monde numÃ©rique, en perturbant le commerce ou lâ□□accÃ¨s Ã des services publics essentiels Ã lâ□□aide de code malveillant.

De fait, la Russie a dÃ©jÃ lancÃ© avec succÃ¨s des attaques de grande ampleur contre lâ□□Ukraine en 2015, provoquant une panne dâ□□Ã©lectricitÃ© massive dans plusieurs villes du pays. Les experts avaient alors attribuÃ© cette agression Ã Â« Sandworm Â», un groupe de pirates connu pour son affiliation avec les Services des renseignements militaires russes.

La rÃ©Ã©mergence du groupe de ransomware Conti en dÃ©but dâ□□annÃ©e â□□ manifestÃ©e par des attaques ciblant des organismes gouvernementaux costariciens â□□ montre que les outils et ressources utilisÃ©s avant le conflit russo-ukrainien restent dâ□□actualitÃ© et Ã©voluent.

De plus, des groupes suspectÃ©s comme Ã©tant liÃ©s au gouvernement russe, Ã lâ□□image des collectifs REvil et Black Cat (ALPHV), que lâ□□on croyait dÃ©mantelÃ©s, ont donnÃ© des signes de vie dans le cadre dâ□□une rÃ©cente sÃ©rie dâ□□attaques de ransomwares. Nous devrions Ã©galement assister Ã une recrudescence des attaques menÃ©es par des sympathisants sans lien direct avec les Ã□tats-nations concernÃ©s.

Cette hausse dâ□□activitÃ© est en partie le rÃ©sultat de la rÃ©activation dâ□□anciennes campagnes de ransomwares, afin de cibler les victimes originales, sans pour autant sâ□□y limiter. Ils utilisent Ã©galement des informations dÃ©robÃ©es lors de la compromission initiale afin de sâ□□en prendre aux contacts professionnels des victimes.

Ces Ã©vÃ©nements rÃ©cents sont des manifestations dâ□□une tendance prÃ©occupante au vu de lâ□□intensification de lâ□□activitÃ© et du comportement atypique de certains groupes de pirates bien Ã©tablis. Il est donc probable quâ□□une lutte de pouvoir se joue aprÃ¨s lâ□□invasion de lâ□□Ukraine par la Russie.

Ceci pourrait expliquer lâ□□Ã©volution des mÃ©thodes dâ□□extorsion, qui aurait pour but dâ□□accumuler davantage de gains par le biais dâ□□actions criminelles. Nous pouvons donc nous attendre Ã voir cette activitÃ© perdurer tandis que nous cherchons Ã nous adapter Ã lâ□□expansion de notre surface dâ□□attaque.

Partage dâ□□informations sur les menaces

Pour maÃ®triser les attaques, et en particulier en temps de cyberguerre, il est capital de faciliter lâ□□Ã©change rationalisÃ© et en temps rÃ©el de renseignements sur les cybermenaces entre acteurs publics et privÃ©s. Jusquâ□□ici, ces diffÃ©rents organismes ont Ã©tÃ© rÃ©ticents Ã procÃ©der Ã un tel partage, mais nous devons poursuivre nos efforts afin de progresser dans ce domaine.

La collecte et le partage dâ□□informations complÃ¨tes issues de sources variÃ©es permettent en effet de faire une idÃ©e plus claire des menaces, afin dâ□□Ã©laborer des stratÃ©gies efficaces.

Ces informations dÃ©cisionnelles et en temps rÃ©el serviront non seulement Ã assurer la sÃ©curitÃ© des applications et systÃ¨mes critiques, mais aussi Ã mettre en Å□uvre les moyens nÃ©cessaires Ã des mesures plus offensives, le cas Ã©chÃ©ant. Tout ceci devrait donc encourager les acteurs publics et privÃ©s Ã former des partenariats florissants sur le long terme face Ã lâ□□Ã©volution constante des menaces.

Anticiper

Le conflit entre Russie et Ukraine peut Ãªtre perÃ§u comme un microcosme de la cyberguerre actuelle. Les campagnes de piratage mondiales (rÃ©surgentes ou nouvelles) montrent que loin de disparaÃ®tre, les attaques avancÃ©es sont en recrudescence, et de plus en plus sophistiquÃ©es et tenaces.

Ce conflit nous a Ã©galement permis de mieux identifier nos forces et faiblesses en tant que pays, ainsi que les lacunes Ã combler. Les organisations publiques et privÃ©es restent bien trop rÃ©actives dans leurs approches en matiÃ¨re de sÃ©curitÃ©, et nos angles morts sont trop nombreux.

Si notre champ de vision sâ□□arrÃªte devant notre porte, alors nous ne sommes pas rÃ©ellement protÃ©gÃ©s. La rÃ©surgence des groupes cybercriminels montre que nous devons cesser de fonctionner de faÃ§on isolÃ©e (sur le plan politique ou autre), et introduire davantage de lÃ©gislations, mettre en place des financements, faciliter le partage dâ□□informations pour unifier les ressources des secteurs publics et privÃ©s, et mettre lâ□□accent sur la sÃ©curitÃ© de notre pays.