THALES
Building a future we can all trust

COMMUNIQUE DE PRESSE
29 mars 2023
Paris

De l'Ukraine à l'Europe entière:

un tournant dans la cyberguerre

- **La Direction d'Analyse de la menace cyber de Thales présente son rapport de février 2023 revenant sur un an d'attaques cyber à l'échelle du continent européen.**
- **Le troisième trimestre 2022 marque un tournant dans la cyberguerre liée au conflit en Ukraine avec une transition très nette d'une cyberguerre centrée sur l'Ukraine et la Russie vers une cyberguerre hybride de haute intensité s'étendant à l'Europe. Celle-ci cible en particulier la Pologne, les pays baltes et les pays nordiques, de manière croissante dans les secteurs des infrastructures nationales critiques, notamment dans les domaines de l'aviation, l'énergie, la santé, les banques et l'administration publique.**
- **De la cyber-destruction ciblée au cyber-harcèlement tous azimuts, les méthodes des hacktivistes pro-russes prennent la forme d'attaques massives en déni de service ou DDoS[1]. Ces attaques visent à rendre temporairement inaccessible un serveur et à provoquer un dysfonctionnement du service. Elles contribuent aux procédés russes de guerre informationnelle ayant pour but d'épuiser les organisations privées comme publiques.**

[1] *Une attaque par déni de service vise à rendre indisponible un ou plusieurs services, visant par exemple à exploiter une vulnérabilité logicielle ou matérielle. L'interruption de service peut également s'effectuer en empêchant l'accès à ce service, par exemple en saturant la bande passante du réseau*

L'Europe de l'Est et l'Europe du Nord en première ligne de la cyberguerre

Une nouvelle géographie des attaques se dessine en douze mois de conflit. Si la majorité des incidents dans le monde était concentrée sur l'Ukraine au moment de l'invasion (50,4% au premier trimestre 2022 contre 28,6% au troisième trimestre), les pays membres de l'Union européenne ont vu le nombre d'incidents liés au conflit augmenter de façon spectaculaire sur les 6 derniers mois, passant de 9,8% à 46,5% des attaques mondiales.

A l'été, on dénombrait autant d'incidents liés au conflit dans les pays de l'UE qu'en Ukraine (85 contre 86). Le début de l'année 2023 confirme cette tendance avec une écrasante majorité des incidents concentrée dans les pays européens (80,9%).

Les pays candidats à l'intégration européenne tels que le Monténégro et la Moldavie sont de plus en plus ciblés (de 0,7% des attaques au premier trimestre 2022 à 2,7% en fin d'année 2022), la Pologne est constamment harcelée avec le nombre record de 114 incidents liés au conflit en un an et les hacktivistes de guerre se concentrent particulièrement sur les pays baltes (157 incidents en Estonie, Lettonie, Lituanie) et les pays du Nord (95 incidents en Suède, Norvège, Danemark, Finlande). Hormis l'Allemagne avec 58 incidents en un an, en comparaison, les pays comme la France (14), le Royaume-Uni (18), l'Italie (14) ou encore l'Espagne (4) sont davantage préservés.

« L'Europe est entrée malgré elle dans une cyberguerre hybride de haute intensité au tournant du conflit, au troisième trimestre 2022 avec une vague massive d'attaques par déni de service, en particulier dans les pays nordiques, les pays baltes et les pays de l'Est de l'Europe. La cyber fait dorénavant partie de l'arsenal indispensable aux nouvelles techniques de guerre, c'est-à-dire la désinformation, la manipulation de l'opinion publique, la guerre économique, le sabotage, ou encore la guérilla. A la lumière de cette latéralisation du conflit de l'Ukraine à l'Europe dans sa globalité, les attaques à court terme contre les infrastructures critiques doivent être considérées avec attention en Europe occidentale dans l'hypothèse d'une nouvelle accélération du conflit. » précise**, Pierre-Yves Jolivet, VP Cyber Solutions, Thales.**

Des hacktivistes de guerre aux techniques de cyberharcèlement

Sur l'ensemble des cyberattaques enregistrées dans le monde sur la période du conflit, 61% sont issues de groupes d'hacktivistes pro-russes, aux premiers rang desquels Anonymous Russia, KillNet et Russian Hackers Teams. Ces groupes apparus au cours du conflit se sont organisés en miroir des efforts des hacktivistes ukrainiens de l'IT Army au début du conflit. Plus structurés, utilisant des ressources de la cybercriminalité organisée de type *botnet-as-a-service*[2] comme Passion Botnet, ils ont pour objectif de cyberharceler les pays occidentaux apportant leur soutien à l'Ukraine. Les hacktivistes sont donc la nouvelle composante du conflit. Ce sont des groupes civils indépendants, pouvant être assimilés à un groupe cybercriminel agissant selon des objectifs et des intérêts politiques précis, sans être directement sponsorisés par un Etat mais agissant en soutien par conviction. De toutes origines et de tous niveaux techniques, ils proviennent également d'horizons très variés.

[2] *Service de vente ou de location d'un réseau proxy pour donner la possibilité à d'autres acteurs malveillants de l'utiliser et lancer des attaques.*

Ici encore, le troisième trimestre 2022 marque un tournant avec une vague de DDoS alors que le premier trimestre faisait état d'un panorama des modes d'attaques très varié, à part quasi égale entre vols et fuites de données, DDoS, espionnage, influence, intrusion, rançongiciel, phishing, wiper et infostealer[3]. Les cyberattaquants agissent à travers des attaques massives par déni de service (à 75%) à l'encontre des entreprises et des administrations, déployant ainsi des techniques de harcèlement systématique, souvent à faible impact opérationnel, mais mettant sous tension les équipes de sécurité et les décideurs. L'objectif n'est pas d'appliquer des impacts significatifs, mais de harceler et décourager tout soutien à l'Ukraine.

A l'inverse, les attaques par wipers peuvent détruire les systèmes de l'adversaire et l'espionnage à long terme peut compromettre l'intégrité de sa sécurité mais elles doivent faire l'objet d'une préparation beaucoup plus longue dans le temps, nécessitant plus de ressources. Les opérations cyber-militaires destructrices ne représentent que 2% du volume total des incidents tout comme les techniques d'espionnage et sont principalement concentrées sur les organisations publiques ukrainiennes.

L'intervention dans le domaine cyber est une pratique habituelle du pouvoir russe, faisant partie de son arsenal dans l'objectif de harceler l'adversaire sans entrer en confrontation directe avec lui.

Si les actes de cyberguerre ont encore lieu en Ukraine comme nous l'avons vu avec l'attaque ATK256 contre plusieurs organismes publics ukrainiens à l'occasion de l'anniversaire du conflit (23 février 2023), ils sont noyés, aux yeux des Occidentaux, par un cyberharcèlement constant.

La contribution de Thales à la protection des infrastructures critiques

Thales assure la cybersécurité de 9 des 10 géants mondiaux de l'internet et intervient sur les systèmes d'information critiques de plus de 130 clients, Etats et opérateurs de services essentiels ou vitaux. Doté de plus de 3500 experts en cybersécurité, le groupe met à la disposition des gouvernements et des opérateurs d'infrastructures critiques des systèmes de détection et de réponse à incident intégrés, comprenant des capacités de renseignements d'intérêt cyber (*Cyber Threat Intelligence*), des sondes souveraines, des plateformes de supervision - centres opérationnels de cybersécurité- ainsi que des systèmes de chiffrement pour éviter le vol de données.

L'offre du Groupe s'articule autour de trois gammes de produits et services : les produits souverains, les plateformes de protection des données et les services de cybersécurité, qui ont généré plus de 1,5 milliard d'euros de chiffres d'affaires en 2022.

Lire le résumé - Téléchargement du rapport

[3] Le phishing est une technique d'hameçonnage destinée à leurrer l'utilisateur pour l'inciter à communiquer des données. Un wiper est un type de malware dont l'objectif est d'effacer les données du système infecté. Un infostealer est un logiciel espion utilisé pour récupérer des informations dans un système.

A propos de Thales

Thales (Euronext Paris : HO) est un leader mondial des hautes technologies spécialisé dans trois secteurs d'activité : Défense & Sécurité, Aéronautique & Spatial, et Identité & Sécurité numériques. Il développe des produits et solutions qui contribuent à un monde plus sûr, plus respectueux de l'environnement et plus inclusif.

Le Groupe investit près de 4 milliards d'euros par an en Recherche & Développement, notamment dans des domaines clés de l'innovation tels que le quantique, l'Edge computing, la 6G et la cybersécurité.

Thales compte 77 000 collaborateurs répartis dans 68 pays. En 2022, le Groupe a réalisé un chiffre d'affaires de 17,6 milliards d'euros.

_____

CONTACTS PRESSE

Relations médias Thales
Marion Bonnet
+33 (0)6 60 38 48 92
marion.bonnet@thalesgroup.com

Pour en savoir plus :
Solutions de cybersécurité | Thales Group
Cyberthreat Hitmap (thalesgroup.com)