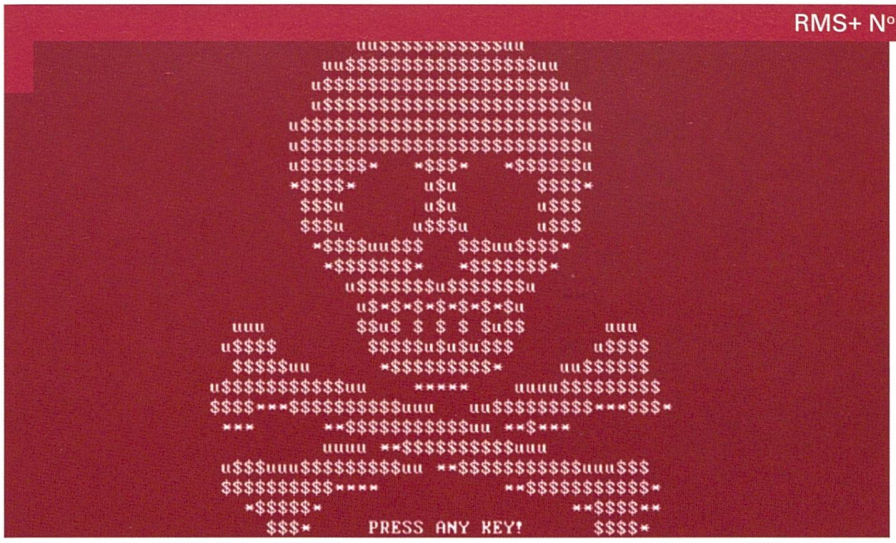
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2023)
Heft: [1]: Numéro Thématique 1

Artikel: Ukraine : cyberattaquess contre le réseau électrique
Autor: Prado, Oscar / Fontanellaz, Adrien
DOI: https://doi.org/10.5169/seals-1055347



Capture d'écran du logo apparaissant à la suite d'une infection par le virus Petya, déployé par le GRU en 2017 (Wikicommons)

Cyber

Ukraine : Cyberattaques contre le réseau électrique

Oscar Prado, Adrien Fontanellaz
Responsable sécurité systèmes d'information ; membre du comité du CHPM

Moscou peut s'appuyer sur les unités cyber relevant de ses services de renseignement, soit le GRU (renseignement militaire), le FSB (contre-espionnage) et le SVB (renseignement extérieur) mais peut aussi mobiliser les services de groupes criminels affiliés au Kremlin.

En décembre 2015, le GRU causa un black-out de plusieurs heures qui toucha 230'000 personnes après avoir accédé aux centres de conduite de la compagnie de distribution d'électricité Prykarpattyaoblenergo grâce à un cheval de Troie baptisé Black Energy. Celui-ci rendait les ordinateurs infectés inutilisables. Il s'agissait du premier black-out induit directement par une cyberattaque sur le plan global. Une nouvelle attaque intervint en décembre 2016 avec le déploiement d' Industroyer, lui aussi conçu spécifiquement pour neutraliser les infrastructures électriques, et aboutit à la mise hors service d'une station de distribution à Kiev, qui priva d'électricité le Nord de la capitale.

Le début de la guerre coïncida avec une recrudescence massive de l'activité des organes de cyberguerre russes. En novembre 2022, le président ukrainien annonçait que 1'300 attaques cyber contre le pays avaient été contrées depuis le commencement des hostilités. De fait, les services de cybersécurité ukrainiens, à commencer par l'*Ukrainian State Service of Special Communications and Information Protection of Ukraine* (SSSCIP), sont réputés pour leur compétence. En outre, ils bénéficient d'un soutien massif de leurs homologues occidentaux puisque dès février, l'Union Européenne se préparait à activer un groupe de réponse cyber incluant des experts croates, estoniens, lituaniens, néerlandais, polonais et roumains afin de soutenir Kiev. Surtout, les Etats-Unis, première puissance cyber mondiale, ont massivement intensifié leur coopération avec l'Ukraine, bientôt formalisée en juillet 2022 avec la signature d'un mémorandum de coopération avec le SSSCIP portant sur les échanges d'informations et techniques sur la sécurisation des infrastructures critiques, le partage des bonnes pratiques, la mise sur pieds de formations en cybersécurité et la tenue d'exercices conjoints. L'implication américaine alla plus loin encore ; en juin, le général Paul Nakasone, commandant de l'US Cyber Command et de la NSA, confirmait qu'une série d'opérations couvrant l'ensemble du spectre cyber avait été menée en soutien de l'Ukraine, précisant que celles-ci avaient été non seulement de nature informationnelle et défensives, mais également... offensives.

Le GRU lança pourtant une attaque d'envergure contre le réseau électrique à l'aide d'une nouvelle version du virus Industroyer le 8 avril, avec en ligne de mire une sous-station électrique à haute tension desservant deux millions de personnes. Pour ce faire, les attaquants ont infecté des terminaux de la société électrique au moyen d'un logiciel baptisé CaddyWiper capable de détruire les données, Industroyer 2 lui-même ayant été programmé pour s'activer quelques minutes après, avec comme objectif de couper le courant en s'appuyant sur des commandes envoyées par un protocole spécialisé, le IEC-104. La sophistication de l'attaque était telle qu'un autre ver était déployé simultanément afin d'infecter des machines desservant un autre réseau d'électricité, celui-ci servant de véhicule destiné à permettre l'exécution d'un logiciel de destruction des données en cas de connexion réussie. L'attaque fut pourtant neutralisée avec succès par la cyberdéfense ukrainienne.

En août, ce fut le tour du site internet d'Energoatom, opérateur des centrales nucléaires ukrainiennes, qui fut victime d'une attaque de déni d'accès impliquant plus de 7.25 millions de robots qui dura près de trois heures. Le mois suivant, les services de renseignement ukrainiens annonçaient que les Russes planifiaient une vague d'attaque massive avec une emphase sur le secteur énergétique. Début décembre, celle-ci ne s'était pas encore matérialisée.

O.P, A.F