Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

BULLETIN SUR LES CYBERMENACES : Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie

Canada

À PROPOS DU PRÉSENT DOCUMENT

AUDITOIRE

Le présent bulletin sur les cybermenaces est destiné à la collectivité de la cybersécurité. Tout en étant soumise aux règles standard de droit d'auteur, l'information TLP:WHITE peut être distribuée sans aucune restriction. Pour obtenir de plus amples renseignements sur le protocole TLP (*Traffic Light Protocol*), prière de consulter la page Web https://www.first.org/tlp/.

COORDONNÉES

Prière de transmettre toute question ou tout enjeu relatif au présent document au Centre canadien pour la cybersécurité à contact@cyber.gc.ca.

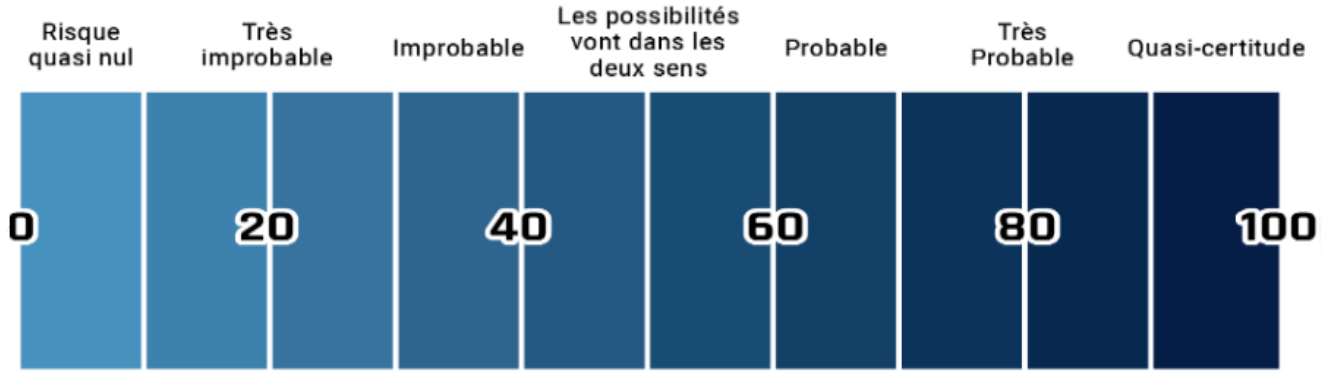
MÉTHODOLOGIE ET FONDEMENT DE L'ÉVALUATION

Les principaux avis formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) en matière de cybersécurité. En défendant les systèmes d'information du gouvernement du Canada (GC), le Centre pour la cybersécurité bénéficie d'une perspective unique lui permettant d'observer les tendances dans l'environnement de cybermenaces et d'appuyer ses évaluations. Dans le cadre du volet du mandat du Centre de la sécurité des télécommunications (CST) touchant le renseignement étranger, le Centre pour la cybersécurité tire parti d'information précieuse sur les habitudes des adversaires dans le cyberespace. Bien que le Centre pour la cybersécurité soit toujours tenu de protéger les sources et méthodes classifiées, il fournira au lecteur, dans la mesure du possible, les justifications qui ont motivé ses avis.

Les avis du Centre pour la cybersécurité sont basés sur un processus d'analyse qui comprend l'évaluation de la qualité de l'information disponible, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. On emploiera des termes tels que « nous estimons que » ou « selon nos observations » pour communiquer les évaluations analytiques. On utilisera des qualificatifs comme « possiblement », « probable » et « très probable » pour exprimer les probabilités.

Le présent document est basé sur des renseignements disponibles en date du 22 juin 2022.

Le tableau ci-dessous fait coïncider le lexique des estimations à une échelle de pourcentage approximative. Ces nombres ne proviennent pas d'analyses statistiques, mais sont plutôt basés sur la logique, les renseignements disponibles, des jugements antérieurs et des méthodes qui accroissent la précision des estimations.



PRINCIPAUX AVIS

- Nous évaluons que les cyberopérations liées à l'invasion de l'Ukraine par la Russie ont été certainement beaucoup plus sophistiquées et étendues que l'ont laissé entendre les sources d'information publiques.
- Selon toute vraisemblance, les cyberopérations de la Russie ont cherché jusqu'ici à détériorer, à perturber, à détruire ou à discréditer le gouvernement, les forces militaires et les fonctions économiques ukrainiens, à s'implanter dans les infrastructures essentielles et à restreindre l'accès de la population ukrainienne à l'information.[1]
- Nous estimons que les auteurs de cybermenace parrainés par la Russie poursuivront sans doute leurs activités malveillantes pour appuyer les objectifs tactiques et stratégiques des forces militaires russes en Ukraine.
- Selon notre évaluation, les auteurs de cybermenace parrainés par la Russie ont presque assurément augmenté leurs activités de cyberespionnage visant les pays membres de l'Organisation du Traité de l'Atlantique Nord (OTAN) en guide de représailles au soutien manifesté à l'endroit de l'Ukraine.
- Nous croyons que la Russie est presque inévitablement en train de développer des cybercapacités contre des cibles de l'Union européenne (UE) et de l'OTAN, y compris les États-Unis et le Canada.[2]

CYBERACTIVITÉS ATTRIBUÉES OU LIÉES À LA RUSSIE EN SOL UKRAINIEN

Selon toute vraisemblance, les cyberopérations de la Russie ont cherché jusqu'ici à détériorer, à perturber, à détruire ou à discréditer le gouvernement, les forces militaires et les fonctions économiques ukrainiens, à s'implanter dans les infrastructures essentielles et à restreindre l'accès de la population ukrainienne à l'information.[3] Les auteurs de cybermenace parrainés par la Russie poursuivront sans doute leurs activités malveillantes pour appuyer les objectifs tactiques et stratégiques des forces militaires russes en Ukraine.

Depuis l'annexion de la Crimée par la Russie en 2014, l'Ukraine a considérablement amélioré sa situation en matière de cybersécurité, notamment avec l'assistance récente de gouvernements et d'entreprises spécialisées dans la technologie de l'UE et de la collectivité des cinq (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis).[4]

À la suite de l'invasion de l'Ukraine par la Russie le 24 février 2022, des auteurs de menace présumés russes ont réalisé plusieurs attaques perturbantes et destructrices contre les réseaux informatiques de cibles ukrainiennes, y compris des attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) et le déploiement de maliciels effaceurs dans de nombreux secteurs, dont les secteurs du gouvernement, des finances et de l'énergie. Les cyberopérations ont souvent coïncidé avec des opérations militaires conventionnelles (voir la figure 1).

Pour l'instant, les auteurs de cybermenace associés à la Russie ont employé huit familles dépistées de maliciels dans le cadre de leurs activités destructrices contre l'Ukraine : WhisperGate/Whisperkill, FoxBlade (HermeticWiper), SonicVote (HermeticRansom), CaddyWiper, DesertBlade, Industroyer2, Lasainraw (IsaacWiper) et FiberLake (DoubleZero).[5]

À la mi-avril, des auteurs de cybermenace parrainés par la Russie ont lancé quatre variants différents d'un nouveau maliciel contre diverses cibles ukrainiennes. Des sociétés de cybersécurité ont attribué ces attaques au groupe Armageddon (alias Gamaredon/Shuckworm), qui a été lié au Service fédéral de sécurité (FSB) de la Russie.[6]

Cyberactivités visant les communications ukrainiennes

Au début mars, le Service de sécurité de l'Ukraine (SBU) a signalé que des auteurs de cybermenace avaient compromis des sites Web d'autorités régionales et locales afin de publier de la désinformation sur la capitulation de l'Ukraine et la signature d'un traité de paix avec la Russie.[7]

Au cours de cette même période, des auteurs de menace de connivence avec la Russie auraient brouillé la connexion qui relie le service Internet par satellite Starlink de SpaceX et les terminaux connexes, lesquels fournissaient un accès Internet supplémentaire au gouvernement ukrainien. Depuis, Starlink a apporté des modifications à son logiciel et le brouillage ne s'est pas reproduit.[8]

À la fin mars, des auteurs de menace soupçonnés d'avoir fait allégeance à la Russie ont causé une importante interruption de services touchant Ukrtelecom, un fournisseur ukrainien d'accès Internet, ce qui a occasionné l'une des pannes Internet les plus étendues dans le pays depuis le début de l'invasion.[9]

À la fin avril, l'équipe d'intervention en cas d'urgence informatique de l'Ukraine (CERT-UA) avait publié une mise en garde contre des attaques constantes par DDoS visant des sites pro-ukrainiens et le portail Web du gouvernement, qui étaient réalisées par l'entremise de sites WordPress compromis.[10]

Cyberactivités visant le secteur de l'énergie de l'Ukraine

Au début avril, des auteurs de cybermenace du service de renseignement militaire russe (GRU), alias l'équipe Sandworm, ont tenté de déployer le maliciel Industroyer2 ainsi que plusieurs familles de maliciels destructeurs contre des sous-stations électriques haute tension en Ukraine dans le but de causer des pannes d'électricité généralisées.[11] Ils sont parvenus à se déplacer du réseau de technologies de l'information (TI) au réseau du système de contrôle industriel (SCI) de la victime. La CERT-UA, en collaboration avec l'entreprise de sécurité Internet slovaque ESET, a réussi à remédier à l'intrusion et à protéger le réseau ciblé.[12]

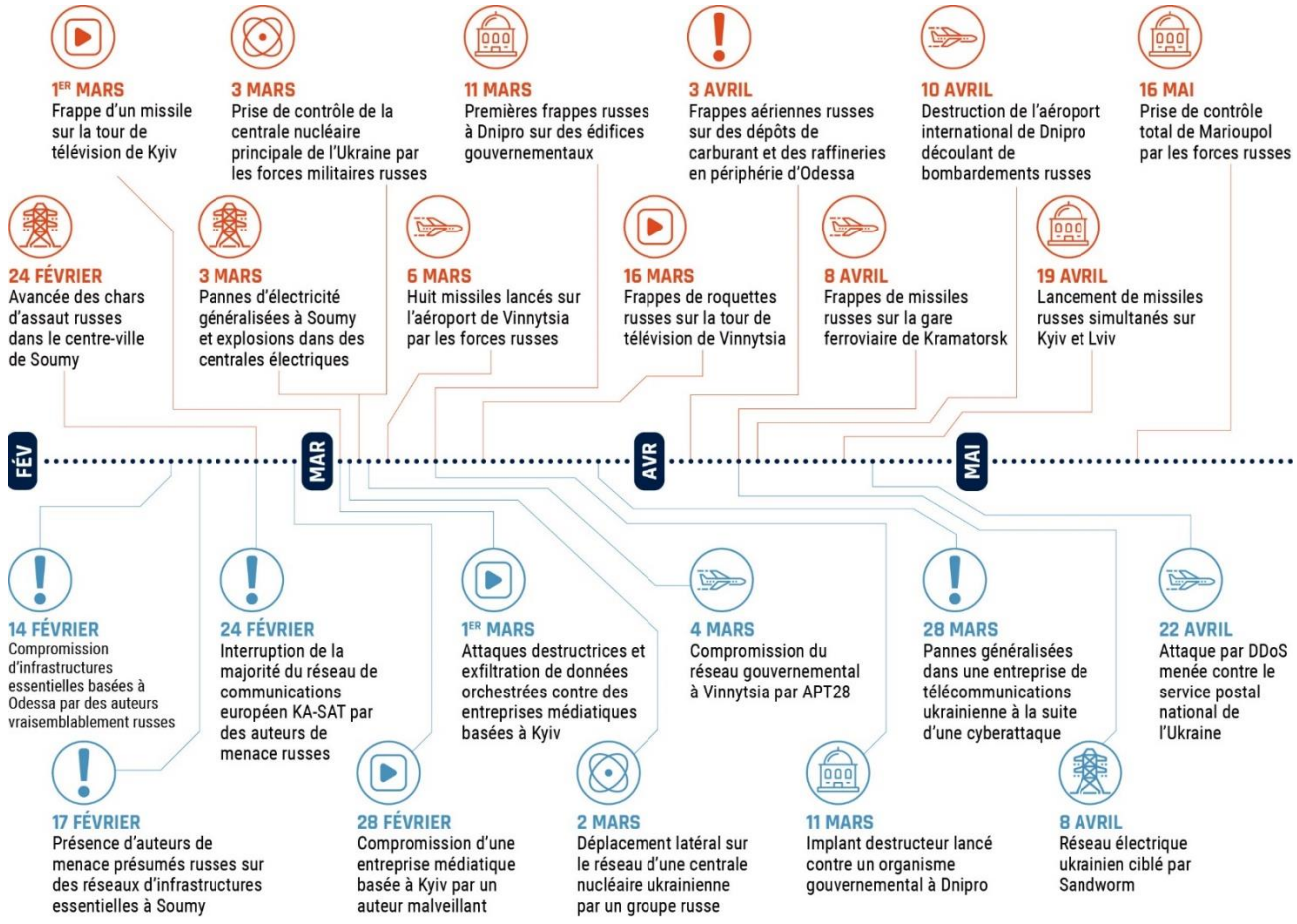
Cyberactivités visant le gouvernement ukrainien

En mai 2022, l'équipe XakNet a affirmé qu'elle s'était introduite dans le réseau du ministère des Affaires étrangères de l'Ukraine et avait exfiltré des documents qu'elle a publiés sur les médias sociaux dans le cadre d'une opération de piratage et de fuite de données.[13] L'équipe XakNet a offert une prime à ses 20 000 abonnés pour les analyses de données les plus élaborées.

À maintes reprises, des auteurs de menace liés à la Russie ont déployé une variété de maliciels effaceurs ainsi que des attaques par DDoS contre divers ministères du gouvernement ukrainien.[14]

Figure 1 : Chronologie des attaques militaires et des cyberopérations en Ukraine – du 14 février au 16 mai[15]

Ce diagramme comprend des exemples de cyberactivités (en bleu, en dessous de la ligne de chronologie) et d'activités cinétiques (en orange, au-dessus de la ligne de chronologie) d'envergure orchestrées par la Russie.



CYBERACTIVITÉS NOTABLES ATTRIBUÉES OU LIÉES À LA RUSSIE TOUCHANT D'AUTRES PAYS

Tandis que les activités de cybermenace russes dans le contexte de la guerre en Ukraine ont visé principalement des cibles ukrainiennes, plusieurs incidents ont débordé sur d'autres pays, et les effets de ces débordements demeurent une menace préoccupante pour la communauté internationale.

À titre d'exemple, des auteurs de cybermenace russes ont amorcé une opération le 24 février 2022 qui a déstabilisé la majorité du réseau européen du service de télécommunications par satellite KA-SAT de Viasat et qui avait pour but d'interrompre les capacités de communication des forces militaires ukrainiennes.[16] Le 10 mars, des milliers de modems du réseau satellitaire KA-SAT ont été rendus inexploitables, y compris des modems situés en France, en Allemagne, en Grèce, en Hongrie, en Italie et en Pologne. Le 10 mai 2022, le Canada et ses alliés de la collectivité des cinq, de même que l'UE et l'Ukraine, ont attribué publiquement cette attaque au gouvernement russe.[17]

Entre le 15 et le 22 avril, Killnet, un groupe de piratage informatique sympathisant de la Russie, a revendiqué plus de 20 attaques par DDoS qui ont touché de nombreux secteurs des infrastructures essentielles en République tchèque, en Estonie, en Lettonie, en Pologne, au Royaume-Uni et aux États-Unis.[18]

Ciblage de l'UE et de l'OTAN

Il y a tout lieu de croire que les auteurs de cybermenace parrainés par la Russie ont redoublé d'efforts en matière de cyberespionnage contre les pays de l'OTAN qui ont exprimé leur soutien à l'Ukraine. Depuis janvier 2022, les auteurs de cybermenace russes ont ciblé des entités du gouvernement, du milieu universitaire, du secteur privé et des infrastructures essentielles au Danemark, en Lettonie, en Lituanie, en Norvège, en Pologne, aux États-Unis et en Turquie pour des motifs de cyberespionnage, de même que des entités en Finlande et en Suède, deux pays ayant soumis leur demande d'adhésion à l'OTAN à la suite de l'invasion de l'Ukraine par la Russie en février.[19]

Au début avril, les autorités ukrainiennes ont signalé publiquement que des cibles du gouvernement ukrainien et de gouvernements non précisés de l'UE avaient fait l'objet de plusieurs tentatives de harponnage attribuées à des auteurs de cybermenace du FSB.[20]

À la fin avril, le groupe de piratage informatique Hive0117, motivé par le gain financier et jusqu'alors inconnu, a mené une campagne d'hameçonnage contre divers pays de l'Europe de l'Est dans laquelle il se faisait passer pour un organisme russe et transmettait une copie du maliciel DarkWatchman.[21]

À la mi-mai, un auteur de menace inconnu a créé un site Web fictif dans le but d'inciter des utilisateurs allemands démontrant un intérêt pour la crise en Ukraine à télécharger des documents malveillants en vue de les infecter d'un cheval de Troie personnalisé autorisant l'accès à distance à PowerShell et ensuite voler des données.[22]

Nous croyons que la Russie est presque inévitablement en train de développer des cybercapacités contre des cibles de l'UE et l'OTAN, y compris les États-Unis et le Canada.[23]

Au Canada

Dès janvier 2022, du renseignement en pleine évolution indiquait que des auteurs de cybermenace de la Russie exploraient les possibilités de contre-attaques visant les États-Unis, le Canada et d'autres pays de l'OTAN et de la collectivité des cinq, y compris leurs infrastructures essentielles.[24] Les auteurs de menace cautionnés par la Russie ont déjà prouvé qu'ils étaient capables d'interrompre les systèmes de contrôle industriels (SCI) à l'aide de maliciels destructeurs. Par ailleurs, certains auteurs de cybermenace prorusses ont menacé de lancer des cyberopérations contre les pays et organisations qui fournissaient une aide matérielle à l'Ukraine.[25]

AUTEURS DE MENACE NON ÉTATIQUES CIBLANT LA RUSSIE

En riposte à un déferlement de cyberattaques d'origine russe contre l'Ukraine avant et pendant l'invasion, plusieurs auteurs de cybermenace non étatiques ont manifesté leur soutien pour l'Ukraine en répondant notamment à l'appel du gouvernement ukrainien destiné à demander l'aide de pirates informatiques volontaires pour démanteler des sites Web russes.[26]

Le pirate YourAnonSpider, affilié au collectif d'hacktivistes Anonymous, a revendiqué la cyberattaque du début mai contre RuTube, laquelle a mis la plateforme vidéo de la Russie hors service pendant au moins deux jours.[27] Au cours de cette même période, le groupe NB65, également affilié à Anonymous, s'est déclaré responsable des pannes serveur touchant plusieurs importants réseaux de télévision russes.[28]

De mars à avril, des pirates ont affirmé qu'ils avaient compromis des douzaines de sociétés et d'établissements russes, y compris l'un des principaux services de renseignement de la Russie. Anonymous et Network Battalion 65, en collaboration avec Distributed Denial of Secrets (qui se présente comme un « collectif de transparence »), ont revendiqué un grand nombre de ces opérations. À la mi-juin, Anonymous a également affirmé qu'il avait piraté les plans de véhicules aériens spatiaux sans pilote de la Russie.[29]

ACTEURS CLÉS DANS LES CYBERACTIVITÉS LIÉES À L'INVASION DE L'UKRAINE PAR LA RUSSIE

Nous évaluons que les cyberopérations liées à l'invasion de l'Ukraine par la Russie ont été certainement beaucoup plus sophistiquées et étendues que l'ont laissé entendre les sources d'information publiques. Des auteurs de menace ont réalisé des cyberopérations pour le compte de la Russie et de l'Ukraine.

Auteurs de cybermenace parrainés par la Russie

Certaines activités de cybermenace contre l'Ukraine proviennent de divers auteurs associés aux trois principaux services de renseignement russes, soit le FSB, le Service de renseignements extérieurs (SVR) et le GRU. Ces auteurs ont participé à toute une gamme d'activités malveillantes contre l'Ukraine, y compris des cyberopérations perturbantes et destructrices.[30]

Auteurs de cybermenace prorusses

GHOSTWRITER/UNC1151 est un collectif de longue date réalisant des activités d'influence étrangère en ligne et qui serait associé aux gouvernements de la Russie et de la Biélorussie. Ses activités comprennent la désinformation, la collecte de justificatifs d'identité, la conduite d'opérations de piratage et de fuite, l'espionnage et la conduite d'attaques sous faux pavillon.[31]

Cybercriminels et hacktivistes

Sympathisants de la Russie :

- Certains groupes de cybercriminels qui parlent russe ont déclaré publiquement qu'ils étaient en faveur de l'invasion de l'Ukraine par la Russie. À titre d'exemple, le **groupe d'opérateurs du rançongiciel Conti** a menacé d'exercer des représailles contre tout auteur d'attaques contre les réseaux informatiques des infrastructures essentielles russes.[32] Avant la réorganisation et le changement d'image qu'il a entrepris récemment, Conti était le groupe d'opérateurs de rançongiciel qui avait fait le plus de victimes au Canada.
- **Beregini** est un groupe de pirates prorusses basé en Ukraine qui cible constamment le gouvernement et les forces militaires ukrainiens.[33] L'**équipe XakNet**, un groupe d'hacktivistes russes, a également pris pour cible l'Ukraine.[34]
- **Killnet**, un groupe de pirates sympathisants de la Russie, a mené un grand nombre d'attaques par DDDoS contre des sites Web appartenant à des pays fournissant un soutien à l'Ukraine, plus particulièrement des sites Web liés à différents secteurs d'infrastructures essentielles, dont le secteur des transports. Récemment, le 11 mai 2022, Killnet a ciblé le ministère de la Défense, le Sénat et l'Institut national de la santé de l'Italie.[35]
- **CoomingProject** est un autre groupe d'opérateurs de rançongiciel qui a manifesté son soutien au gouvernement russe.[36]

Sympathisants de l'Ukraine :

- Tel qu'il a été mentionné ci-dessus, des membres du collectif d'hacktivistes Anonymous ont lancé diverses cyberopérations contre le gouvernement et des entreprises industrielles russes. Ils ont notamment effacé des fichiers, piraté la télévision d'État russe ainsi que réalisé des fuites de données et des opérations de DDoS.[37] Un autre groupe de piratage, les **Cyberpartisans biélorusses**, a également concentré ses activités sur la compromission de cibles russes, bien que son impact jusqu'ici soit limité.[38]
- Selon des représentants ukrainiens, plus de 400 000 personnes se sont portées volontaires pour contribuer à une initiative participative du gouvernement ukrainien (« l'armée TI ») visant à protéger les réseaux de l'Ukraine.[39]

PRINCIPAUX INDICATEURS LIÉS À DES SCÉNARIOS DE CYBERMENACE

Le CST surveille des sources d'information classifiées et non classifiées afin de déterminer l'intention stratégique des auteurs de cybermenace. Puisque les cyberactivités russes sont issues des objectifs en matière de politiques énoncés par le gouvernement russe, le CST est également à l'affût des rapports classifiés et de source ouverte sur l'évolution de la situation nationale en Russie.

Bien qu'il soit difficile de prédire les cyberactivités futures, nous avons l'œil notamment sur les indicateurs suivants :

Indicateurs contextuels :

- une intensification du conflit en Ukraine, ou des revers russes constants;
- un soutien continu ou accentué de l'OTAN dans le conflit;
- des sanctions économiques persistantes ou durcies, ou de nouvelles mesures contre la Russie;

- une rhétorique de plus en plus agressive de la part du gouvernement russe;
- des déclarations relatives aux lignes rouges;
- un déclin radical de l'appui intérieur russe;
- des déclarations de soutien précis à la Russie par d'autres acteurs étatiques ou non étatiques.

Indicateurs de cyberactivités :

- Une intensification des activités malveillantes en ligne visant les alliés du Canada, surtout les États-Unis
- Une augmentation des activités de balayage et de reconnaissance contre des cibles gouvernementales, militaires et civiles du Canada et de ses alliés
- Une augmentation des compromissions ou des tentatives de compromission contre des cibles gouvernementales, militaires et civiles du Canada et de ses alliés
- Un intérêt marqué pour l'utilisation et la mise à l'essai de capacités contre des technologies utilisées dans les secteurs des infrastructures essentielles (p. ex. des dispositifs de SCI, des unités d'alimentation sans interruption [ASI] et des systèmes d'interface homme-machine [IHM])
- Un nombre accru de prépositionnements dans des réseaux d'infrastructures essentielles (notamment dans les secteurs des finances, de l'énergie et des services publics)
- Le ciblage précis de personnes ou d'entités participant ou associées aux sanctions

ATTÉNUATION DES RISQUES, SENSIBILISATION ET RENFORCEMENT DE LA CYBERSÉCURITÉ

Depuis la mi-janvier, le Centre a communiqué à tous les secteurs des infrastructures essentielles canadiennes la nécessité de redoubler de vigilance et de suivre les avis du Centre pour la cybersécurité concernant les tactiques, les techniques et les procédures des auteurs de cybermenace russes. L'information du Centre a été diffusée publiquement dans la mesure du possible et par l'intermédiaire de canaux de confiance pour les avis et les indicateurs techniques plus sensibles liés à la crise actuelle.

Publication de divers produits d'avertissement par le Centre pour la cybersécurité et ses alliés

Depuis 2021, durant le renforcement de la présence militaire russe le long de la frontière ukrainienne et à la suite de l'invasion russe en sol ukrainien sans justification ni provocation, le Centre pour la cybersécurité a surveillé de près l'évolution des menaces ainsi que leurs effets, intentionnels et indirects, sur les organisations et la population canadiennes. Au cours de cette période, le Centre pour la cybersécurité a publié huit produits visant à conseiller, à alerter et à informer les destinataires sur les menaces et les effets possibles de l'invasion de l'Ukraine par la Russie :

Alertes

- AL22-002 – Activités perturbatrices contre des organisations ukrainiennes – Mise à jour 1 (24 février 2022)
- AL22-001 – Maliciel Wiper ciblant des organisations ukrainiennes (17 janvier 2022)

Bulletins de cybersécurité

- Bulletin de cybersécurité conjoint sur les contrôles de sécurité faibles et les pratiques couramment exploitées pour obtenir un accès initial (17 mai 2022)
- Bulletin de cybersécurité conjoint sur la protection contre les cybermenaces ciblant les fournisseurs de services gérés et leurs clients (11 mai 2022)
- Bulletin de cybersécurité conjoint sur les vulnérabilités les plus couramment exploitées en 2021 (27 avril 2022)
- Bulletin de cybersécurité conjoint sur les cybermenaces criminelles et parrainées par la Russie qui planent sur les infrastructures essentielles (20 avril 2022)

Bulletin sur les cybermenaces

- Le CCC rappelle aux exploitants des infrastructures essentielles du Canada de prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et de prendre des mesures d'atténuation contre celles-ci (13e février 2022)

- Le CCC exhorte les exploitants des infrastructures essentielles du Canada à prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et à prendre des mesures d'atténuation contre celles-ci (1er janvier 2022)

Le CST alerte les Canadiens sur les activités de désinformation de la Russie

Outre les efforts de cyberespionnage et les cyberattaques destructrices, des auteurs de cybermenace affiliés à la Russie et parrainés par celle-ci ont déployé des opérations de cyberinfluence conçues pour appuyer les objectifs de guerre de la Russie. Le 1er avril 2022, le CST a commencé à déclassifier du renseignement et à le publier sur l'un de ses comptes de médias sociaux en vue d'exposer des éléments de désinformation que la Russie propage au sujet du conflit en Ukraine :

- Le 6 avril, le CST a signalé que la Russie prétendait que les États-Unis avaient établi des laboratoires biologiques dans des pays de l'ex-URSS et qu'ils se servaient de l'Ukraine comme terrain d'expérimentation biologique.[40]
- Le 13 avril, le CST a révélé que la Russie propageait de fausses allégations au sujet de membres des Forces armées canadiennes qui commettaient des crimes de guerre en Ukraine et qu'elle utilisait des images altérées pour renforcer ses faussetés au sujet de l'implication du Canada dans le conflit.[41]
- Le 25 avril, le CST a indiqué que la Russie rejetait intentionnellement le blâme concernant les atrocités commises par les forces russes et qu'elle répandait de fausses allégations selon lesquelles l'Ukraine avait violé la Convention de Genève et que cette violation avait mené à des dissensions au sein de l'armée ukrainienne.[42]

Le manque de signalement des incidents demeure un défi : nous encourageons fortement les entités canadiennes de tous les secteurs essentiels à signaler les compromissions réelles ou potentielles au Centre pour la cybersécurité, qui se fonde sur cette information pour brosser un tableau complet des cybermenaces pesant sur le Canada, de même que pour parfaire ses avis et ses conseils destinés à la défense contre les tactiques en constante évolution.

Le CST se tient prêt à intervenir en cas de compromission majeure du Gouvernement du Canada (GC) ou des systèmes d'importance pour le GC. À cet égard, le Centre pour la cybersécurité peut fournir une assistance sous forme :

- de notifications, ainsi que d'avis et de conseils initiaux;
- de soutien visant à contenir et à atténuer les menaces;
- d'analyses des journaux et des maliciels; et
- d'analyses de criminalistique numérique.

Pour signaler une compromission ou obtenir des conseils, prière de communiquer avec le Centre pour la cybersécurité au 1-833-CYBER88 ou à contact@cyber.gc.ca.

---

[1] KAPELLMANN ZAFRA, Daniel, Raymond LEONG, Chris SISTRUNK, Ken PROSKA, Corey HILDEBRANDT, Keith LUNDEN et Nathan BRUBAKER. *Industroyer.V2: Old Malware Learns New Tricks*, Mandiant, 25 avril 2022.
[2] CISA. *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 20 avril 2022.
[3] KAPELLMANN ZAFRA, Daniel, Raymond LEONG, Chris SISTRUNK, Ken PROSKA, Corey HILDEBRANDT, Keith LUNDEN et Nathan BRUBAKER. *Industroyer.V2: Old Malware Learns New Tricks*, Mandiant, 25 avril 2022.
[4] PIPIKAITE, Algirde et Lukas BESTER. *How the cyber world can support Ukraine,* World Economic Forum, 19 mars 2022.
[5] Microsoft. *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*.
[6] BURT, Jeff. *Russian-linked Shuckworm crew ramps up Ukraine attacks*, The Register, 20 avril 2022.
[7] LAPIENYTE, Jurgita. *Ukrainians seize five bot farms used to spread fake news and panic,* Cybernews, 29 mars 2022.
[8] DUFFY, Kate. *A top Pentagon official said SpaceX Starlink rapidly fought off a Russian jamming attack in Ukraine*, Business Insider, 22 avril 2022.
[9] COKER, James. *Attack on Ukraine Telecoms Provider Caused by Compromised Employee Credentials*, Infosecurity, 6 avril 2022.
[10] TOULAS, Bill. *Ukraine targeted by DDoS attacks from compromised WordPress sites*, BleepingComputer, 28 avril 2022.
[11] KAPELLMANN ZAFRA, Daniel, et coll. *Industroyer.V2: Old Malware Learns New Tricks*.
[12] GREENBERG, Andy. *Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine*, Wired, 12 avril 2022.
[13] CISA, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*.
[14] Microsoft. *Special Report: Ukraine*.
[15] Figure adaptée du contenu de : Microsoft. *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*.
[16] BURGESS, Matt. *A Mysterious Satellite Hack Has Victims Far Beyond Ukraine*, Wired, 23 mars 2022.

[17] Affaires mondiales Canada. *Déclaration sur les cyberactivités malveillantes de la Russie qui touchent l'Europe et l'Ukraine*, 10 mai 2022.
[18] GREIG, Jonathan. *Italy stops wide-ranging Russian attack of websites of parliament, military, health agency*, The Record, 12 mai 2022.
[19] Microsoft. *Defending Ukraine: Early Lessons from the Cyber War*, 22 juin 2022.
[20] CERT-UA. #4378, 4 avril 2022.
[21] TOULAS, Bill. *Russian govt impersonators target telcos in phishing attacks*, Bleepingcomputer, 27 avril 2022.
[22] MalwareBytes. *Custom PowerShell RAT targets Germans seeking information about the Ukraine crisis*, 16 mai 2022.
[23] CISA, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 20 avril 2022.
[24] CISA, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*.
[25] CISA, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*.
[26] SHORE, Jennifer. *Don't Underestimate Ukraine's Volunteer Hackers*, Foreign Policy, 11 avril 2022.
[27] COLLIER, Kevin. *A Cyberattack Took Down One of Russia's Largest Video Platforms for Days*, NBC News, 11 mai 2022.
[28] Hackread. *Anonymous Affiliate NB65 Breach State-Run Russian Broadcaster; Leak 786B of Data*, 6 avril 2022.
[29] YourAnonSpider. *Russian UAV drones plans and tactics hacked*, 10 juin 2022.
[30] Microsoft. *Special Report: Ukraine*.
[31] RONCONE, Gabriella, Alden WAHLSTROM, Alice REVELLI, David MAINOR, Sam RIDDELL et Ben READ. *UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests*, Mandiant, 16 novembre 2021.
[32] REICHERT, Corinne. *Conti Ransomware Group Warns Retaliation if West Launches Cyberattack on Russia*, CNET, 25 février 2022. https://www.cnet.com/news/politics/conti-ransomware-group-warns-retaliation-if-west-launches-cyberattack-on-russia
[33] WAHLSTOM, Alden, Alice REVELLI, Sam RIDDELL, David MAINOR et Ryan SERABIAN. *The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine*, Mandiant, 19 mai 2022.
[34] CISA, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*.
[35] PETKAUSKAS, Vilius. *Hacker wars heat up as the pro-Russian Killnet attacks Italy*, Cybernews, 23 mai 2022.
[36] CISA, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*.
[37] DAVID, Benjamin. *Russian Ministry Website Reportedly Hacked*, InfoSecurity, 6 juin 2022.
[38] ROTH, Andrew. "Cyberpartisans" hack Belarusian railway to disrupt Russian buildup, The Guardian, 25 janvier 2022.
[39] STOKEL-WALKER, Chris et Dan MILMO. *'It's the right thing to do': the 300,000 volunteer hackers coming together to fight Russia*, The Guardian, 15 mars 2022.; SHORE, Jennifer. *Don't Underestimate Ukraine's Volunteer Hackers*, Foreign Policy, 11 avril 2022.
[40] Compte Twitter officiel du CST @cst_cse, 6 avril 2022.
[41] Compte Twitter officiel du CST @cst_cse, 13 avril 2022.
[42] Compte Twitter officiel du CST @cst_cse, 25 avril 2022.

CAT. D96-88/2022F-PDF
ISBN 978-0-660-44579-3