# Le Bulletin Cyber - Se préparer aux implications cyber du conflit Russie-Ukraine

## Le Bulletin Cyber EY : un condensé des dernières attaques par ransomware et les différents aspects de sécurisation des actions utilisateur.

Cette nouvelle édition du cyber bulletin se concentre sur les conséquences numériques de la guerre entre la Russie et l'Ukraine.

L'intensification constante du conflit a suscité un engagement diplomatique accru de la part des États membres de l'OTAN, qui abritent certaines des économies numériques les plus robustes du monde. L'escalade des tensions géopolitiques, combinée à l'utilisation répétée par la Russie des cyber-attaques comme arme de guerre, présente un potentiel important pour que les entreprises, au-delà de l'Ukraine, soient confrontées à de graves impacts.

Cette édition revient donc sur les rivalités qui s'expriment dans l'espace numérique dans le contexte de la guerre russo-ukrainienne et sur les cyberattaques qui ont été observées jusqu'à présent.

Nos experts rappellent que le durcissement des mesures de sécurité et l'accroissement de la vigilance cyber permettent d'atténuer les risques de cyberattaques pour les organisations. A titre d'exemple, quelques mesures de sécurité seront détaillées ci-après.

---

Le collectif Anonymous s'en prend au gouvernement russe

+ 500

de sites russes et biélorusses piratés.

---

# L'implication des acteurs du cyberespace dans le conflit russo-ukrainien

La guerre en Ukraine a conduit à une recrudescence du hacktivisme et à l'implication de nouveaux acteurs du cyberespace dans le conflit. La multiplication des acteurs est susceptible de conduire à l'intensification des cyber-attaques et à leur propagation, y compris en dehors des frontières de l'Ukraine.

## 1. L'engagement du collectif Anonymous dans le conflit

Le collectif Anonymous a publiquement annoncé son soutien à l'Ukraine au travers d'un tweet publié le 24 février 2022 dans lequel il déclare qu'il est « *officiellement en guerre contre le gouvernement russe* »[1].

Depuis ce jour, Anonymous affirme avoir lancé plusieurs attaques de déni de service contre les sites internet gouvernementaux et contre Russia Today, une chaîne de télévision financée par l'Etat russe[2] ; Anonymous affirme avoir piraté plus de 2500 sites russes et biélorusses au total[3].

Au-delà des actions visant à perturber les sites internet russes, Anonymous affirme également vouloir lutter contre la désinformation et la propagande de l'état russe. Ainsi, certaines chaînes de télévision russes ont pu être piratées par le collectif pro-Ukraine, afin de diffuser des images du conflit. Le 10 mars, Anonymous a également revendiqué l'attaque de Roskomnadzor, l'organisme fédéral russe chargé de la supervision dans le domaine des médias, et a publié 820GB de données extraites à la suite de la cyberattaque.

## 2. Le groupe Conti Ransomware subit une vaste violation de données

"*La Conti Team annonce officiellement son soutien total au gouvernement russe*", a déclaré le groupe dans un post[4].

Suite à cette prise de position officielle, le groupe Conti a été victime d'une fuite de données compromettantes par un chercheur en sécurité basé en Ukraine. Ce dernier a réussi à pirater un serveur interne Jabber/XMPP et à publier des messages internes confidentiels liés au gang. Les données divulguées contiennent 339 fichiers JSON contenant un total de 60 694 messages de journal du 29 janvier 2021 au 27 février 2022 qui peuvent être lus sur le site officiel d'IntelligenceX[5].

Plusieurs autres fuites de données concernant le gang Conti ont suivi : ces données contiennent des échanges de conversation qui poussent à croire que le groupe de ransomware fonctionne comme une entreprise. Elles nous ont permis d'établir le business plan du groupe, le fonctionnement de leur processus de recrutement, et de comprendre d'un point de vue organisationnel son fonctionnement interne (par exemple le choix de la cible détermine la méthodologie adaptée à mettre en place par l'équipe en charge de la mission). Différents profils au sein des équipes Conti ont pu être identifiés :

- Les développeurs développent les malwares et le backend des serveurs

- Les administrateurs système sont en charge de l'infrastructure interne
- Les testeurs
- Les Reverser analysent les outils commerciaux afin de comprendre leur fonctionnement et d'identifier des moyens de contournement
- Une équipe de pentest
- Une équipe d'OSINT chargée de recenser les informations pertinentes sur une entreprise (telle que les individus représentant une cible facile pour Conti et une menace interne pour leur entreprise)
- Les « Crypters » en charge d'obfusquer au maximum les payloads

Selon Dmitry Smilyanets[6], un analyste du renseignement russophone, les données volées sont authentiques. Une analyse approfondie de ces données a permis à nos équipes CSIRT d'extraire plusieurs informations pertinentes : IOCs, modes opératoires de certaines équipes Conti, ainsi que les éventuels rapprochements entre certains groupes et/ou organisations.

À la suite de cette exposition médiatique imprévue, le groupe de ransomware Conti a annoncé dans une communication interne à ses employés, le 21 mars 2022 dernier, l'arrêt de leurs activités pour une durée de 2 à 3 mois, dans l'attente d'une « résolution de la situation ».

## L'accroissement des cyberattaques dans le cadre du conflit Russie-Ukraine

## 1. Un ransomware utilisé comme leurre dans les cyberattaques contre l'Ukraine

Selon un récent rapport de Symantec[7], le ransomware déployé a servi de diversion aux attaques destructrices d'effacement de données visant l'Ukraine.

Le wiper, surnommé HermeticWiper[8], est un malware conçu uniquement pour endommager le *Master Boot Record* (MBR) du système ciblé. Le malware a été déposé lors de cyberattaques récentes visant principalement des entrepreneurs ukrainiens des secteurs de la finance et du gouvernement.

Une note de rançon sur les machines compromises était accompagnée d'un message politique indiquant que "*La seule chose que nous apprenons des nouvelles élections est que nous n'avons rien appris des anciennes !*".

Selon Symantec, les attaquants ont eu accès aux réseaux cibles après avoir exploité des vulnérabilités de Microsoft Exchange dès novembre 2021 et installé des *web shells* pour déployer le malware wiper.

Il s'agit du deuxième malware d'effacement de données utilisé contre des réseaux ukrainiens depuis le début de l'année. En janvier, Microsoft a fait état d'un malware d'effacement de données, nommé WhisperGate, déguisé en ransomware et ciblant des organisations ukrainiennes et des organismes gouvernementaux[9]. Ce dernier écrasait le *Master Boot Record* (MBR) et affichait un message menaçant en ukrainien, russe et polonais au redémarrage, rendant les systèmes incapables de démarrer. WhisperGate téléchargeait et exécutait un corrupteur de fichiers qui écrasait les types de fichiers ciblés (contrairement aux ransomwares qui chiffrent les fichiers), les rendant irrécupérables.

Dans ce contexte, IBM prévient que la situation actuelle en Ukraine devrait devenir plus critique avec des cyberattaques de plus en plus sophistiquées[10].

S'il est encore peu probable que les entreprises non-Ukrainiennes soient intentionnellement visées, il est possible qu'elles fassent partie des dommages collatéraux.

## 2. Le CISA et le FBI mettent en garde contre les attaques par effacement de données

Le *Cybersecurity and Infrastructure Security Agency* (CISA) et le *Federal Bureau of Investigation* (FBI) ont publié un avertissement sous la forme d'un avis de cybersécurité conjoint[11].

Cet avertissement a été émis suite à la révélation de cyberattaques ciblant l'Ukraine, utilisant le logiciel malveillant HermeticWiper[12] et le faux ransomware, WhisperGate, dans le but de compromettre les appareils des organisations affectées.

Jusqu'à présent, les deux souches de logiciels malveillants n'ont été utilisées que contre des réseaux ukrainiens. Toutefois, selon les deux agences fédérales, "*elles pourraient également toucher accidentellement d'autres cibles*".

Afin de se protéger des attaques par effacement de données, nous recommandons les mesures suivantes :

- Configurer les programmes antivirus et antimalware pour effectuer des analyses régulières.
- Activer des filtres anti-spam puissants pour empêcher les courriels de phishing d'atteindre les utilisateurs finaux.
- Filtrer le trafic réseau.
- Mettre à jour les logiciels.

- Exiger une authentification multifactorielle (MFA).

## 3. Attaque du réseau satellitaire ViaSat

Les cyber-attaques russes font également des victimes en dehors de l'Ukraine. En ciblant le réseau de satellites "ViaSat", qui couvre l'Europe, dont l'Ukraine, elles ont coupé des centaines de milliers de personnes d'Internet[13].

Le 17 mars, le gouvernement américain a mis en garde contre les menaces qui pèsent sur les réseaux de communication par satellite, par crainte que les récentes attaques contre les réseaux de satellites en Europe ne se propagent bientôt aux États-Unis. Dans un avis conjoint, le *CISA* et le *FBI* invitent les fournisseurs de réseaux de communication par satellite (SATCOM) et les organisations d'infrastructures critiques qui dépendent des réseaux satellitaires à renforcer leurs défenses de cybersécurité en raison d'une probabilité accrue de cyberattaque, avertissant qu'une intrusion réussie pourrait créer un risque dans les environnements de leurs clients[14].

## La Russie crée une nouvelle autorité étatique de certification TLS pour faire face aux sanctions

Le gouvernement russe a poussé sa propre autorité de certification TLS à résoudre les problèmes d'accès aux sites web qui se sont accumulés à la suite des sanctions imposées par l'Occident.

Le ministère russe du développement numérique devrait fournir un substitut national pour gérer l'émission et le renouvellement des certificats TLS en cas de révocation ou d'expiration[15].

Toutes les entités juridiques opérant en Russie pourraient bénéficier de ce service, les certificats étant délivrés aux propriétaires de sites sur demande dans un délai de 5 jours ouvrables.

Cette proposition intervient alors que les entreprises et les gouvernements occidentaux ont imposé des sanctions qui empêchent les organisations comme DigiCert d'opérer en Russie[16].

Les certificats TLS sont utilisés pour lier numériquement une clé cryptographique aux coordonnées d'une organisation, ce qui permet aux navigateurs web de confirmer l'authenticité du domaine et de garantir que la communication entre un ordinateur client et le site web cible est sécurisée.

Cependant, les navigateurs web tels que Google Chrome, Microsoft Edge, Mozilla Firefox et Apple Safari, n'ont pas clairement indiqué l'intention d'accepter les certificats délivrés par la nouvelle autorité de certification russe afin que les connexions sécurisées aux serveurs certifiés puissent fonctionner comme prévu[17].

## Conclusion

Le conflit, combiné à l'utilisation des cyber-attaques comme arme de guerre, présente des risques importants pour que les entreprises, au-delà de l'Ukraine, soient confrontées à de graves impacts, notamment lorsqu'elles sont établies dans des pays ayant imposé des sanctions à la Russie. En effet, d'autres attaques russes sont à prévoir, bien qu'il y ait un haut degré d'incertitude quant au moment et à la portée de ces actions.

- La Russie pourrait exécuter des attaques via des compromissions de la chaîne d'approvisionnement, comme avec NotPetya en 2017 et SolarWinds en 2020, ou en exploitant des vulnérabilités connues (par exemple, Log4j) ou encore inconnues.
- Comme l'a montré l'attaque contre ViaSat, des impacts directs ou indirects peuvent être ressentis par des organisations hors de l'Ukraine, conduisant à la perturbation des services publics, de la logistique, des télécommunications ou d'autres fournisseurs de services.
- Les groupes criminels basés en Russie pourraient également multiplier les attaques par *ransomware* contre les organisations occidentales dans tous les secteurs, y compris contre des infrastructures critiques (par exemple, les hôpitaux, le pétrole et le gaz, etc.).

S'il est encore peu probable que les entreprises non-Ukrainiennes soient intentionnellement visées, il est possible qu'elles fassent partie des dommages collatéraux suite à des cyberattaques disruptives massives (comme ce fut le cas avec CrashOverride en 2016 par exemple) visant à appuyer les actions militaires en perturbant la société civile (perturbation des services gouvernementaux, des transports publics, des services financiers etc.)

## Recommandations

Dans ce contexte, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) recommande de mettre en œuvre les mesures de sécurité suivantes[18] :

- Renforcer l'authentification sur les systèmes d'information.
- Sauvegarder les données et applications critiques hors ligne.
- Etablir une liste hiérarchisée des services numériques critiques de l'entité.
- S'assurer de l'existence d'un système de gestion de crise adapté à une potentielle cyberattaque.

Pour compléter, nous recommandons aux organisations de renforcer de manière proactive leurs défenses et de se préparer à des attaques potentiellement perturbatrices et destructrices, en se concentrant sur les points suivants :

- Restrictions des accès à distance aux systèmes d'information de l'organisation.
- Renforcement de la sécurité et surveillance des comptes, notamment des comptes à privilèges.
- Renforcement de la sécurité des méthodes d'authentification (identifiants et mot de passe).
- Restriction des mouvements latéraux.
- Durcissement de la configuration des terminaux.

- Protection de l'infrastructure de virtualisation.
- Restrictions du trafic de sortie.
- Segmentation des réseaux IT et OT.
- Définition d'un plan de continuité d'activité et d'un plan de reprise d'activité.
- Réalisation d'exercices de crise et *threat hunting*.

Pour les utilisateurs, il est recommandé de :

- Vérifier les paramètres de sécurité de ses comptes (e-mail et réseaux sociaux).
- Vérifier les informations publiées sur les réseaux sociaux, surtout celles encourageant un passage à l'action.
- Effectuer des copies de ses données importantes et les sauvegarder sur différents supports.
- Se renseigner régulièrement sur les cyberattaques en cours et appliquer les recommandations correspondantes.

---

## Sources

---

## Pour aller plus loin

Les dirigeants, les conseils d'administration et les responsables de la cybersécurité ne sont pas toujours informés des menaces que suscitent les nouvelles formes émergentes de cybercriminalité. Ce bulletin propose une vision claire de ces menaces, qu'elles soient sectorielles, informatiques ou mobiles. Il présente les dernières tendances ainsi qu'une version synthétique des rapports proposés chaque semaine à nos clients. N'hésitez pas à nous contacter pour plus d'informations

Nos atouts

- **Le Lab** : 600m2 dédiés à la recherche et au développement à l'innovation et à la transformation numérique.
- **War Room** : Un environnement hautement sécurisé exploitant des solutions collaboratives et des technologies propriétaires innovantes.

- **Cyber Teams** : L'équipe EY France cybersécurité est composée d'experts pluridisciplinaires, proposant des solutions nouvelles pour résoudre des problématiques stratégiques pour nos clients.

- **CyberEye** : Une solution leader de Cyber Threat Intelligence solution, apportant une connaissance précise des cybermenaces pouvant toucher les entreprises.

- **ASC and CTI** : Nos 63 Advanced Security Centers, situés dans de nombreux pays, partagent des renseignements opérationnels et centrés vers les entreprises pour notre Cyber Threat Intelligence.

EY | Assurance | Consulting | Strategy and Transactions | Tax

**About EY**

EY is a global leader in assurance, consulting, strategy and transactions, and tax services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.



EYG/OC/FEA no.

ED MMYY