L’Ukraine, victime d’une attaque informatique comme arme de guerre

Description

Depuis 2014, l’Ukraine est en proie à une guerre entre les forces de Kiev et les séparatistes prorusses, soutenus par le Kremlin. Dans la nuit du 13 au 14 janvier 2022, les sites web de plusieurs institutions gouvernementales ukrainiennes ont été touchés par une « attaque globale » dont l’objectif, sous les atours d’un rançongiciel, était ni plus ni moins d’effacer les données des agences visées.

Depuis la fin de l’année 2021, Moscou a envoyé une centaine de milliers de militaires et fait la démonstration de ses forces armées dans la région, notamment pour faire pression sur les Occidentaux afin que l’Ukraine ne devienne pas membre de l’Otan. Au bruit de bottes russes à la frontière s’ajoute celui du clavier des pirates informatiques, présumés russes ou biélorusses. Est qualifiée désormais d’hybride une guerre qui allie des manœuvres conventionnelles et des opérations de cyberguerre. Les attaques les plus récentes ont débuté dans la nuit du 13 au 14 janvier 2022, soit le lendemain de l’échec des négociations diplomatiques entre la Russie et l’Otan. Pour le média d’information ukrainien *Obozrevatel*, l’Ukraine subit une « attaque globale ». Plus de 70 sites web gouvernementaux ukrainiens ont ainsi été visés, parmi lesquels celui du Trésor public, des ministères des affaires étrangères, de l’éducation, de l’agriculture ou encore de l’environnement. Sur ces sites *« sont apparus des signes barrés représentant un profil de porc, un trident* [emblème national ukrainien], *la carte et le drapeau de l’Ukraine. En dessous se trouvait un message encadré de rouge, en ukrainien, russe et polonais : « toutes les données personnelles des Ukrainiens ont été rendues publiques.* […] *Ayez peur et attendez-vous au pire » »* détaille le média d’information. En effet, selon le site d’information thehackernews.com, *« les cyberattaques coordonnées visant les sites web du gouvernement ukrainien et le déploiement d’un logiciel malveillant d’effacement des données appelé WhisperGate sur certains systèmes gouvernementaux font partie d’une vague plus large d’activités malveillantes visant à saboter les infrastructures critiques du pays »*. Le 15 janvier 2022, le groupe Microsoft a annoncé avoir découvert ce logiciel malveillant (*malware*) destructeur de données, autrement plus dévastateur qu’un « simple » rançongiciel (voir *La rem* n°56, p.24).

L’attaque est dite globale car elle affecte les sites web du gouvernement, d’organisations non gouvernementales et d’associations, mais aussi les ordinateurs de personnes physiques ou des serveurs, et surtout parce qu’elle s’appuie sur une vulnérabilité informatique dite *zero-day* (voir *La rem* n°59, p.30) nommée Log4Shell, découverte le 24 novembre 2021 et publiée le 9 décembre 2021 par les équipes de sécurité cloud du géant chinois Alibaba. Cette vulnérabilité informatique concerne plus précisément Log4j, une bibliothèque pour le langage de programmation Java, utilisée par de très nombreux logiciels d’entreprises et de bureautique, par des serveurs ou même par des systèmes embarqués dans les voitures. Tous les pays du monde sont touchés, des dizaines de milliers d’entreprises sont concernées : Apple, Amazon, Cisco, Google ou encore IBM, Minecraft, Oracle, Tesla, Siemens pour ne citer que les plus connues. L’ampleur de cette

vulnérabilité informatique est telle que le gouvernement canadien a décidé, en décembre 2021, de fermer préventivement près de 4 000 sites web gouvernementaux afin de les contrôler.

Selon Nicole Perlroth, journaliste au *New York Times* spécialisée dans la cybersécurité, l'espionnage numérique et le sabotage, *« [Log4Shell] est étonnamment facile à exploiter et difficile à réparer. Il ne nécessite aucune authentification et aucune compétence. Il s'agit d'une chaîne de texte. Et avec elle, n'importe qui peut extraire des données sensibles, effacer des données, installer un* ransomware. *Il faudra des mois, voire des années, pour s'en remettre »*. Dès l'annonce de la faille Log4Shell, une recrudescence d'attaques informatiques a d'ailleurs eu lieu partout dans le monde, notamment la prolifération de rançongiciels, le vol de données ou le minage illicite de cryptomonnaies (voir *La rem* n°48, p.37). Le 14 décembre, l'entreprise américaine Cloudfare, qui exploite un réseau mondial de diffusion de contenus (CDN pour Content Delivery Network, voir *La rem* n°53, p.23) a observé 1 000 tentatives d'exploitation de la vulnérabilité par seconde dans les « fichiers journaux » (des fichiers qui contiennent des messages relatifs au système) transmis à leurs clients. Si les autorités russes ou biélorusses sont à l'origine de l'attaque contre l'Ukraine, cette dernière n'avait que peu de chance de pouvoir s'en prémunir.

Outre la diffusion du logiciel malveillant WhisperGate, rendue possible par la vulnérabilité *zero-day* Log4Shell, les sites web du gouvernement et des administrations ukrainiennes ont été compromis par le biais d'une attaque dite *« supply chain »*, qui consiste à viser un sous-traitant, peu sécurisé, pour démultiplier la portée de l'attaque. Selon le département de cyberpolice ukrainien, pour atteindre autant de sites web simultanément, l'attaque a visé Kitsoft, le prestataire ukrainien à l'origine de leur développement. Ce dernier a utilisé un logiciel open source de gestion de contenus, similaire à WordPress, nommé OctoberCMS, dont une faille de vulnérabilité, publiée le 26 août 2021 et corrigée un mois plus tard, n'avait jamais été mise à jour, ni par les administrateurs systèmes des sites web attaqués, ni par le sous-traitant.

Ce qui fait en outre la spécificité de cette attaque globale, c'est que l'objectif n'était pas tant de bloquer les sites web du gouvernement que d'effacer des données de serveurs et ordinateurs infectés par le logiciel malveillant. Dans un billet de blog dédié à la sécurité informatique, Microsoft explique que le virus, se présentant sous la forme d'un rançongiciel, *« est en fait une ruse qui a pour objet, lorsque le périphérique est mis hors tension, d'écraser le contenu sans mécanisme de récupération »*.

Ce n'est pas la première fois que l'Ukraine est victime d'une attaque informatique complexe. En décembre 2015, le virus Black Energy mettait à mal le réseau électrique du pays. En septembre 2017, une attaque informatique mondiale avec le virus Petya/NotPetya a révélé par la suite que la cible originelle était l'Ukraine, ainsi que les groupes étrangers ayant établi des relations commerciales avec ce pays (voir *La rem* n°44, p.50).

Comme toujours, les Russes ont nié être à l'origine de ces attaques. *« Les Ukrainiens nous accusent de tous les maux, même de la mauvaise météo qu'ils subissent actuellement »*, a ironisé Dmitri Peskov, le porte-parole de Vladimir Poutine dans des propos rapportés par France 24. Le secrétaire adjoint du Conseil national de sécurité et de défense ukrainien, Serhiy Demedyuk, a déclaré à Reuters que l'Ukraine attribuait

désormais l'attaque à un groupe de pirates informatiques connu sous le nom d'UNC1151, qui, de Minsk, agit depuis 2016 et serait directement lié au gouvernement biélorusse. Interrogé à ce propos, le président des États-Unis, Joe Biden, a déclaré que, *« s'ils continuent à utiliser des attaques informatiques, nous pourrons répondre de la même manière »*. Le 26 janvier 2022, le ministère ukrainien des affaires étrangères constatait que le site officiel Ukraine.ua avait de nouveau fait l'objet d'une cyberattaque.

Sources :

- « La campagne de Ghostwriter soutenue par UNC1151, alignée avec les intérêts du gouvernement biélorusse », Mandiant Threat Intelligence, globalsecuritymag.fr, décembre 2021.
- « The race is on to patch Log4Shell, the bug that's breaking the internet », Carly Page, techcrunch.com, December 13, 2021.
- « Hard to overstate the severity of the Apache Log4j vulnerability being exploited across critical and industry systems as we speak », Nicole Perlroth, twitter.com, December 14, 2021.
- « Assainissement des fichiers journaux Cloudflare pour protéger les clients contre la vulnérabilité Log4j », Jon Levine, Sohei Okamoto, blog.cloudflare.com/fr-fr/, 14 décembre 2021.
- « Incident. Les institutions ukrainiennes visées par une cyberattaque d'envergure », *Courrier International* – Paris, courrierinternational.com, 14 janvier 2022.
- « Ukrainian government websites attacked : How could it happen ? », Olha Karpenko, ain.ua/en, January 14, 2022.
- « Malware attacks targeting Ukraine government », Tom Burt, blogs.microsoft.com, January 15, 2022.
- « Ukraine suspects group linked to Belarus intelligence over cyberattack », Pavel Polityuk, reuters.com, January 16, 2022.
- « Cyber-guerre : l'Ukraine frappée par les hackers, la Russie principale suspecte », Bastien L., lebigdata.fr, 17 janvier 2022.
- « La Cyber Police, les communications spéciales de l'État et le Service de sécurité d'Ukraine, en collaboration avec des experts internationaux, établissent les sources des cyberattaques sur les sites Web de l'État », département de la Cyber Police de la police nationale d'Ukraine, traduction, cyberpolice.gov.ua, 17 janvier 2022.
- « Ukraine : recent cyber attacks part of wider plot to sabotage critical infrastructure », Ravie Lakshmanan, thehackernews.com, January 18, 2022.
- « Ukraine : la faille Log4shell exploitée pour « déstabiliser le pays » », Alexandre Horn, numerama.com, 19 janvier 2022.
- « Ukraine : Les États-Unis menacent d'une réponse cyber », Jonathan Greig, zdnet.fr, 20 janvier 2022.
- « Suspected Belarus ties to Ukrainian hacks complicate Biden's quandary », Maggie Miller, politico.com, January 22, 2022.
- « Ukraine.ua website faced a cyberattack », Ukraine's Ministry of Foreign Affairs (MFA), mfa.gov.ua, January 26, 2022.

Categorie

1. Ailleurs

date créée
12 mai 2022
Auteur
jacquesandrefines