

DefMal : un projet de recherche français pour détecter les « variants » de ransomware

Description

Situé à Nancy, le Laboratoire de haute sécurité (LHS) du Loria (Laboratoire lorrain de recherche en informatique et ses applications) collectionne les logiciels malveillants et les ransomware depuis 2010. Il est aujourd'hui l'un des plus importants lieux de recherche de la cybersécurité en France. Il pilote aujourd'hui le projet Def Mal (Défense contre les programmes Malveillants).

Apparus pour la première fois dans les années 1990, les ransomware, transmis par courriel ou un clic sur un lien, ont pour dessein de prendre le contrôle d'un équipement informatique et de crypter les données qu'il contient avant d'obtenir une rançon en échange d'une clé de déchiffrement ([voir La rem n°41, p.54](#)). Depuis quelques années, ces ransomwares s'accompagnent parfois d'une menace de publication des données volées. Cette « double extorsion » repose ainsi sur le cryptage par ransomware, le vol de données et la humiliation publique de l'entreprise victime explique-t-on chez Mandiant, entreprise américaine de cybersécurité et filiale de Google, connue pour avoir publié en 2013 un rapport impliquant directement la Chine dans des opérations de cyberespionnage. La plus récente victime, la multinationale française Schneider Electric, s'est fait dérober, en janvier 2024, plusieurs téraoctets de données que les pirates, appartenant à un gang nommé Cactus, menacent de faire fuiter en cas de non-paiement d'une rançon qui pourrait s'élever à plusieurs millions d'euros, selon Bleeping Computer, média d'information de référence sur la sécurité informatique créée en 2004.

À partir des années 2010, ces cyberattaques se sont professionnalisées, et les commanditaires comme les cibles ont voulu. D'après Jérôme Notin, directeur du groupe d'intérêt public Acyma qui gère en France le site d'assistance aux victimes (cybermalveillance.gouv.fr), dispositif copiloté par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et le ministère de l'intérieur, il existe « une véritable chaîne d'approvisionnement du cybercrime, ce que l'on appelle le « crime as a service ». Pour les ransomware, il est possible d'acheter une attaque prête à lancer, il y a même des tutoriels en ligne et du reporting sur la rentabilité de l'attaque » ([voir La rem n°56, p.24](#)).

« Ce sont quasiment des entreprises, qui passent des annonces sur le web, revendent des données sur le marché noir, organisent des concours de recherche de vulnérabilités », explique au Monde

Jean-Yves Marion, professeur à l'université de Lorraine, directeur du Loria et responsable du programme Def Mal « Défense contre les programmes Malveillants.

Si le chercheur en sait autant, c'est que le Laboratoire de Haute Sécurité (LHS) du Loria collectionne les malwares et ransomwares depuis 2010. Dans un lieu sécurisé, deux infrastructures informatiques permettent, en partenariat avec le National Institute of Information and Communications Technology de Tokyo, de surveiller en temps réel les vagues de cyberattaques en «coutant les « bruits de fond » des données. Elles servent également à exploiter un *honeypot*, technique informatique dite du « pot de miel », qui consiste à rendre visible un ou plusieurs serveurs informatiques configurés pour piéger les pirates, afin d'étudier leurs attaques et de récupérer leurs logiciels malveillants. « Ce jour, le Laboratoire de Haute Sécurité en stocke 35 millions. Chacun de ces programmes informatiques est prudemment désassemblé pour en extraire les signatures, dont la cartographie permettra par la suite d'identifier très tôt des similitudes entre un nouveau virus et ceux déjà répertoriés. Fruit de dix ans de recherche fondamentale, cette technique d'analyse unique au monde, dite « morphologique », repose sur un système d'intelligence artificielle capable de détecter le plus tôt possible des intrusions et des « variants » de ransomwares qui échappent aux systèmes de sécurité actuels.

Depuis 2017, l'outil est commercialisé par la start-up Cyber-Detect, issue des travaux de recherche du Loria, qui compte une quinzaine de clients, dont la moitié dans le secteur public. Pour Régis Lhoste, son président, « tous les antivirus que l'on a aujourd'hui sur nos ordinateurs sont défectueux, car ils sont conçus pour identifier les virus déjà connus. Dès qu'un programme sort de ce périmètre, par exemple s'il a été construit spécifiquement pour vous attaquer, ils ne le repèrent plus ». Les pirates déploient ainsi des variants dont le code source est également dissimulé afin de rendre leurs attaques les plus indétectables possibles. Ces variants sont « polymorphes et packés, c'est-à-dire que le fichier malveillant est caché, compressé jusqu'au moment de l'exécution », ajoute Jean-Yves Marion.

Def Mal est un projet ciblé du Programme et équipement prioritaire de recherche (PEPR) en cybersécurité du plan d'investissement France 2030. Lancé en 2022, il vise à soutenir l'expertise du Laboratoire de Haute Sécurité du Loria et à renforcer l'activité des logiciels et des programmes malveillants et, plus précisément, l'analyse et la défense contre les malwares et les ransomwares.

Piloté par l'université de Lorraine, le projet mobilise une communauté de scientifiques ainsi que douze doctorants issus notamment de Centrale Supélec, du Commissariat à l'énergie atomique et aux énergies alternatives (CEA), du Centre national de la recherche scientifique (CNRS), de l'École d'ingénieur Eurecom, de l'Institut national de recherche en sciences et technologies du numérique (Inria) et de l'Institut de recherche en informatique et systèmes informatiques (Irisa). Un budget de 5 millions d'euros, échelonné sur six ans, va permettre, outre d'embaucher des chercheurs, d'accroître des collaborations, dont certaines sont déjà

engagées, à l'échelle européenne et internationale, comme avec le centre de cybersécurité CISP, en Allemagne, ou encore le Japan Advanced Institute of Science and Technology (JAIST) et le National Institute of Information and Communications Technology (NICT), lui aussi au Japon.

L'objectif du programme est de développer des outils d'analyse et de détection de pointe en s'attaquant aux malwares par le biais d'une approche interdisciplinaire, afin d'anticiper les cyberattaques de demain qui viseront les objets connectés au réseau internet, les drones, les véhicules autonomes, les systèmes industriels, les smartphones et tous les équipements et produits électroniques autour desquels la société tout entière est en train de s'organiser. « Une plateforme d'échange doit être mise en place pour partager nos données avec les services de l'état et des partenaires industriels » précise Jean-Yves Marion. « In fine, le but est de multiplier les ponts entre public et privé pour couvrir les multiples facettes de l'écosystème cybercriminel en entretenant des relations avec les forces de l'ordre, des juristes ou des sociologues. »

Sources :

- Ilascu Ionut, « New Cactus ransomware encrypts itself to evade antivirus », bleepingcomputer.com, May 7, 2023.
- Attigui Abdessamad, « Cybersécurité : comment le Laboratoire de Haute Sécurité de Nancy analyse la morphologie des malwares pour mieux les détecter », usinenouvelle.com, 27 octobre 2023.
- « Informatique : un labo pour détecter les pirates avant intrusion », AFP, france24.com, 29 octobre 2023.
- Marchand Leïla, « Les antivirus sont tous défaillants » : les chercheurs contre-attaquent face aux malwares », lesechos.fr, 25 novembre 2023.
- « Accélération pour le projet du PEPR en cybersécurité Def Mal », Factuel, factuel.univ-lorraine.fr, 11 décembre 2023.
- Rapport Mandiant, « Double extorsion : l'évolution du ransomware », mandiant.fr, consulté le 19 janvier 2024.
- Bourgin Yoann, « Schneider Electric touché par le ransomware Cactus, plusieurs téraoctets de données volés », usine-digitale.fr, 30 janvier 2024.

Categorie

1. Techniques

date création

3 avril 2024

Auteur

jacquesandrefines