DefMal : un projet de recherche franÃ§ais pour dÃ©tecter les Â« variants Â» de ranÃ§ongiciels

Description

SituÃ© Ã Nancy, le Laboratoire de haute sÃ©curitÃ© (LHS) du Loria (Laboratoire lorrain de recherche en informatique et ses applications) collectionne les logiciels malveillants et les ranÃ§ongiciels depuis 2010. Il est aujourdâ€™hui lâ€™un des plus importants lieux de recherche dÃ©diÃ©s Ã la cybersÃ©curitÃ© en France. Il pilote aujourdâ€™hui le projet Def Mal (DÃ©fense contre les programmes Malveillants).

Apparus pour la premiÃ¨re fois dans les annÃ©es 1990, les ranÃ§ongiciels, transmis par courriel ou dâ€™un clic sur un lien, ont pour dessein de prendre le contrÃ´le dâ€™un Ã©quipement informatique et de crypter les donnÃ©es quâ€™il contient avant dâ€™obtenir une ranÃ§on en Ã©change dâ€™une clÃ© de dÃ©chiffrement (voirÂ *La remÂ* nÂ°41, p.54). Depuis quelques annÃ©es,Â ces ransomwares sâ€™accompagnent parfois dâ€™une menace de publication des donnÃ©es volÃ©es.Â Cette Â«Â *Â«Â double extorsionÂ Â»* repose ainsi sur le cryptage par ransomware, le vol de donnÃ©es et lâ€™*Â«Â humiliation publiqueÂ Â»* de lâ€™entreprise victime Â» explique-t-on chez Mandiant, entreprise amÃ©ricaine de cybersÃ©curitÃ© et filiale de Google, connue pour avoir publiÃ© en 2013 un rapport impliquant directement la Chine dans des opÃ©rations de cyberespionnage. La plus rÃ©cente victime, la multinationale franÃ§aise Schneider Electric, sâ€™est fait dÃ©rober, en janvier 2024, plusieurs tÃ©raoctets de donnÃ©es que les pirates, appartenant Ã un gang nommÃ© Cactus, menacent de faire fuiter en cas de non-paiement dâ€™une ranÃ§on qui pourrait sâ€™Ã©lever Ã plusieurs millions dâ€™euros, selon Bleeping Computer, mÃ©dia dâ€™information de rÃ©fÃ©rence sur la sÃ©curitÃ© informatique crÃ©Ã© en 2004.

Ã€ partir des annÃ©es 2010, ces cyberattaques se sont professionnalisÃ©es, et les commanditaires comme les cibles ont Ã©voluÃ©. Dâ€™aprÃ¨s JÃ©rÃ´me Notin, directeur du groupement dâ€™intÃ©rÃªt public Acyma qui gÃ¨re en France le site dâ€™assistance aux victimes (cybermalveillance.gouv.fr), dispositif copilotÃ© par lâ€™ANSSI (Agence nationale de la sÃ©curitÃ© des systÃ¨mes dâ€™information) et le ministÃ¨re de lâ€™intÃ©rieur, il existe Â«Â *une vÃ©ritable chaÃ®ne dâ€™approvisionnement du cybercrime, ce que lâ€™on appelle le Â«Â crime as a serviceÂ Â».Â Pour les ranÃ§ongiciels, il est possible dâ€™acheter une attaque prÃªte Ã lancer, il y a mÃªme des tutoriels en ligne et du reporting sur la rentabilitÃ© de lâ€™attaqueÂ* Â»Â (voirÂ *La remÂ* nÂ°56, p.24).

Â«Â *Ce sont quasiment des entreprises, qui passent des annonces sur le web, revendent des donnÃ©es sur le marchÃ© noir, organisent des concours de recherche de vulnÃ©rabilitÃ©sÂ* Â», explique auÂ *MondeÂ*

Jean-Yves Marion, professeur Ã lâ€™universitÃ© de Lorraine, directeur du Loria et responsable du programme Def Mal â€“ DÃ©fense contre les programmes Malveillants.

Si le chercheur en sait autant, câ€™est que le Laboratoire de Haute SÃ©curitÃ© (LHS) du Loria collectionne les malwares et ransomwares depuis 2010. Dans un lieu sÃ©curisÃ©, deux infrastructures informatiques permettent, en partenariat avec le National Institute of Information and Communications Technology de Tokyo, de surveiller en temps rÃ©el les vagues de cyberattaques en Ã©coutant les Â« bruits de fond Â» des donnÃ©es. Elles servent Ã©galement Ã exploiter unÂ *honeypot*, technique informatique dite du Â« pot de miel Â», qui consiste Ã rendre visible un ou plusieurs serveurs informatiques configurÃ©s pour piÃ©ger les pirates, afin dâ€™Ã©tudier leurs attaques et de rÃ©cupÃ©rer leurs logiciels malveillants. Ã€ ce jour,Â le Laboratoire de Haute SÃ©curitÃ© en stocke 35 millions. Chacun de ces programmes informatiques est prÃ©cieusement dÃ©sassemblÃ© pour en extraire les signatures, dont la cartographie permettra par la suite dâ€™identifier trÃ¨s tÃ´t des similitudes entre un nouveau virus et ceux dÃ©jÃ rÃ©pertoriÃ©s.Â Fruit de dix ans de recherche fondamentale, cette technique dâ€™analyse unique au monde, dite Â« morphologique Â», repose sur un systÃ¨me dâ€™intelligence artificielle capable de dÃ©tecter le plus tÃ´t possible des intrusions et des Â« variants Â» de ranÃ§ongiciels qui Ã©chappent aux systÃ¨mes de sÃ©curitÃ© actuels.

Depuis 2017, lâ€™outil est commercialisÃ© par la start-up Cyber-Detect, issue des travaux de recherche du Loria, qui compte une quinzaine de clients, dont la moitiÃ© dans le secteur public. Pour RÃ©gis Lhoste, son prÃ©sident,Â Â«Â *tous les antivirus que lâ€™on a aujourdâ€™hui sur nos ordinateurs sont dÃ©faillants, car ils sont conÃ§us pour identifier les virus dÃ©jÃ connus.Â DÃ¨s quâ€™un programme sort de ce pÃ©rimÃ¨tre, par exemple sâ€™il a Ã©tÃ© construit spÃ©cifiquement pour vous attaquer, ils ne le repÃ¨rent plus*Â Â». Les pirates dÃ©ploient ainsi des variants dont le code source est Ã©galement dissimulÃ© afin de rendre leurs attaques les plus indÃ©tectables possibles. Ces variants sont Â«Â *polymorphes et packÃ©s, câ€™est-Ã -dire que le fichier malveillant est cachÃ©, compressÃ© jusquâ€™au moment de lâ€™exÃ©cution*Â Â», ajoute Jean-Yves Marion.

Def Mal est un projet ciblÃ© du Programme et Ã©quipement prioritaire de recherche (PEPR) en cybersÃ©curitÃ© du plan dâ€™investissement France 2030. LancÃ© en 2022, il vise Ã soutenir lâ€™expertise du Laboratoire de Haute SÃ©curitÃ© du Loria et Ã renforcer lâ€™Ã©tude des logiciels et des programmes malveillants et, plus prÃ©cisÃ©ment, lâ€™analyse et la dÃ©fense contre les malwares et les ransomwares.

PilotÃ© par lâ€™universitÃ© de Lorraine,Â le projet mobilise une communautÃ© de scientifiques ainsi que douze doctorantsÂ issus notamment de Centrale Supelec, du Commissariat Ã lâ€™Ã©nergie atomique et aux Ã©nergies alternatives (CEA), du Centre national de la recherche scientifique (CNRS), de lâ€™Ã©cole dâ€™ingÃ©nieur Eurecom, de lâ€™Institut national de recherche en sciences et technologies du numÃ©rique (Inria) et de lâ€™Institut de recherche en informatique et systÃ¨mes alÃ©atoires (Irisa).Â Un budget de 5 millions dâ€™euros, Ã©chelonnÃ© sur six ans, va permettre, outre dâ€™embaucher des chercheurs, dâ€™accÃ©lÃ©rer des collaborations,Â dont certaines sont dÃ©jÃ

engagÃ©es, Ã lâ€™Ã©chelle europÃ©enne et internationale, comme avec le centre de cybersÃ©curitÃ© CISPA, 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.

Lâ€™objectif du programme est de dÃ©velopper des outils dâ€™analyse et de dÃ©tection de pointe en sâ€™attaquant aux malwares par le biais dâ€™une approche interdisciplinaire, afin dâ€™anticiper les cyberattaques de demain qui viseront les objets connectÃ©s au rÃ©seau internet, les drones, les vÃ©hicules autonomes, les systÃ¨mes industriels, les smartphones et tous les Ã©quipements et produits Ã©lectroniques autour desquels la sociÃ©tÃ© tout entiÃ¨re est en train de sâ€™organiser. Â«Â *Une plateforme dâ€™Ã©change doit Ãªtre mise en place pour partager nos donnÃ©es avec les services de lâ€™Ã‰tat et des partenaires industrielsÂ* Â» prÃ©cise Jean-Yves Marion. Â« In fine, *le but est deÂ multiplier les ponts entre public et privÃ© pour couvrir les multiples facettes de lâ€™Ã©cosystÃ¨me cybercriminel en entretenant des relations avec les forces de lâ€™ordre, des juristes ou des sociologues.Â* Â»

Sources :

- Ilascu Ionut, Â« New Cactus ransomware encrypts itself to evade antivirus Â», bleepingcomputer.com, May 7, 2023.
- Attigui Abdessamad, Â« CybersÃ©curitÃ© : comment le Laboratoire de Haute SÃ©curitÃ© de Nancy analyse la morphologie des malwares pour mieux les dÃ©tecter Â», usinenouvelle.com, 27 octobre 2023.
- Â« Informatique : un labo pour dÃ©tecter les pirates avant intrusion Â», AFP, france24.com, 29 octobre 2023.
- Marchand LeÃ¯la, Â« Â«Â Les antivirus sont tous dÃ©faillantsÂ Â» : les chercheurs contre-attaquent face aux malwares Â», lesechos.fr, 25 novembre 2023.
- Â« AccÃ©lÃ©ration pour le projet du PEPR en cybersÃ©curitÃ© Def Mal Â», Factuel, factuel.univ-lorraine.fr, 11 dÃ©cembre 2023.
- Rapport Mandiant, Â« Double extorsion : lâ€™Ã©volution du ransomware Â», mandiant.fr, consultÃ© le 19 janvier 2024.
- Bourgin Yoann, Â« Schneider Electric touchÃ© par le ransomware Cactus, plusieurs tÃ©raoctets de donnÃ©es volÃ©s Â», usine-digitale.fr, 30 janvier 2024.

Categorie

1. Techniques

date crÃ©Ã©e
3 avril 2024
Auteur
jacquesandrefines