# Apparition de failles dans l'écosystème des ransomwares

Selon le Centre national de cybersÃ©curitÃ© (NCSC) du Royaume-Uni, les ransomwares reprÃ©sentent la menace qui pÃ¨se le plus actuellement sur les entreprises du monde entier. L'Ã©poque oÃ¹ ils ciblaient une seule machine et tentaient d'extorquer un utilisateur en lui volant ses donnÃ©es est rÃ©volue. La menace est organisÃ©e et sophistiquÃ©e, grÃ¢ce Ã  une technologie qui s'est dÃ©mocratisÃ©e au point que le ransomware est devenu une vÃ©ritable industrie.

Certains opÃ©rateurs de ransomware ciblent les MSP (fournisseurs de services managÃ©s) avec des attaques de la chaÃ®ne d'approvisionnement qui ont un impact sur des milliers d'entreprises. D'autres, tels que les groupes APT (advanced persistent threat), s'attaqueront Ã  des cibles spÃ©cifiques pour dÃ©stabiliser des gouvernements ou exploiter des donnÃ©es Ã  forte valeur ajoutÃ©e pour extorquer de grandes sommes dâ€™argent. L'annÃ©e derniÃ¨re aux Ã‰tats-Unis, l'agence de cybersÃ©curitÃ© et de sÃ©curitÃ© des infrastructures (CISA) a observÃ© des incidents de ransomware qui ont touchÃ© 14 des 16 secteurs d'infrastructures essentielles des Ã‰tats-Unis, notamment la dÃ©fense, l'alimentation et l'agriculture, les services gouvernementaux et mÃªme les services d'urgence. Le centre Australien de cybersÃ©curitÃ© (ACSC) a rÃ©cemment signalÃ© que ses infrastructures clÃ©s Ã©taient continuellement ciblÃ©es par des opÃ©rateurs de ransomware, allant jusqu'Ã  publier une mise en garde commune avec les Ã‰tats-Unis et le Royaume-Uni pour avertir de la menace croissante sur les entitÃ©s gouvernementales et les entreprises privÃ©es.

Dans le rapport 2022 sur la Cyber sÃ©curitÃ©, il est rÃ©vÃ©lÃ© une augmentation de 50 % des cyberattaques d'une annÃ©e sur l'autre en 2021, soit 1 organisation sur 61, dans le monde, impactÃ©e par un ransomware chaque semaine. C'est le secteur de l'Ã©ducation et de la recherche qui a subi la plus forte augmentation (75%), avec une moyenne de 1 605 cyberattaques par semaine au cours de l'annÃ©e. Cette forte hausse pourrait, du moins en partie, Ãªtre attribuÃ©e au fait que les entreprises soient plus vulnÃ©rables en raison de leur passage Ã  des modÃ¨les de travail hybrides en rÃ©ponse Ã  la pandÃ©mie. Mais la cause la plus probable reste l'Ã©conomie croissante du Â« Ransomware-as-a-Service Â» (RaaS), oÃ¹ les groupes de ransomware et leurs partenaires proposent et commercialisent des ransomwares prÃªts Ã  l'emploi Ã  des clients qui lancent ensuite les attaques. Ces grands opÃ©rateurs de ransomware ne se contentent pas de proposer le ransomware, mais offrent souvent des services de blanchiment d'argent, des spÃ©cialistes de la nÃ©gociation et mÃªme des instructions dÃ©taillÃ©es, comme le prouve le Â« guide Â» de Conti qui a rÃ©cemment Ã©tÃ© divulguÃ©. Cette dÃ©mocratisation de la cybercriminalitÃ© a crÃ©Ã© une vÃ©ritable filiÃ¨re des ransomwares, oÃ¹ la concurrence stimule l'innovation comme dans tout secteur lÃ©gal.

Cependant, grÃ¢ce aux efforts des chercheurs et des spÃ©cialistes de la sÃ©curitÃ©, ainsi qu'aux gouvernements du monde entier qui renforcent dÃ©sormais leurs dispositifs de cybersÃ©curitÃ© et adoptent une approche plus proactive, on commence Ã  voir apparaÃ®tre des fissures dans l'Ã©cosystÃ¨me des ransomwares.

L'attaque du Colonial Pipeline a-t-elle Ã©tÃ© le point de bascule ?

Les attaques modernes de ransomware se caractÃ©risent notamment par l'ampleur des dÃ©gÃ¢ts qu'elles peuvent provoquer dans le monde rÃ©el, qu'il s'agisse de paralyser le service national de

santÃ© britannique ou de semer le Erreur ! RÃ©fÃ©rence de lien hypertexte non valide. au sein du ministÃ¨re amÃ©ricain de la sÃ©curitÃ© intÃ©rieure. Le succÃ¨s d'une attaque par ransomware n'a jamais Ã©tÃ© aussi bien compris que celui de l'attaque contre Colonial Pipeline en 2021. L'un des plus grands exploitants de pipelines aux Ã‰tats-Unis, Colonial Pipeline fournit prÃ¨s de 45 % du carburant de toute la cÃ´te Est. Qu'il s'agisse de chauffer des habitations et des entreprises ou d'alimenter les voitures, les avions et mÃªme les forces armÃ©es. Les opÃ©rateurs de ransomware DarkSide ont profitÃ© d'une vulnÃ©rabilitÃ© apparemment non corrigÃ©e dans le systÃ¨me de Colonial Pipeline, obligeant la sociÃ©tÃ© Ã  dÃ©sactiver certains systÃ¨mes afin de contenir la menace. Le coÃ»t du carburant a explosÃ©, il y a eu des achats de panique et les secteurs de l'aviation et de l'armÃ©e auraient pu Ãªtre gravement touchÃ©s si la situation n'avait pas Ã©tÃ© corrigÃ©e une semaine plus tard.

Cette attaque a semblÃ© Ãªtre la goutte d'eau qui a fait dÃ©border le vase pour l'administration Biden, qui a annoncÃ© peu aprÃ¨s l'incident que les bourses de crypto-monnaies telles que SUEX, basÃ©e en Russie, seraient sanctionnÃ©es, empÃªchant ainsi les acteurs du ransomware de rentabiliser leurs attaques. Cela semble Ãªtre le dÃ©but d'une sÃ©rie d'Ã©vÃ©nements qui ont finalement conduit Ã  la formation de fissures dans l'Ã©cosystÃ¨me des ransomwares, et la preuve - s'il en fallait une - qu'adopter une approche proactive plutÃ´t que corrective est le moyen le plus efficace de lutter contre la cybercriminalitÃ©.

Aux Ã‰tats-Unis, les ransomwares sont dÃ©sormais considÃ©rÃ©s par le ministÃ¨re de la Justice comme une menace de sÃ©curitÃ© nationale. L'Union europÃ©enne et 31 autres pays dans le monde les ont rejoints pour sanctionner les Ã©changes de crypto-monnaies et perturber ainsi les activitÃ©s des opÃ©rateurs de ransomware. En Australie, un nouveau Â« Ransomware Action Plan Â» a Ã©tÃ© Ã©tabli, confÃ©rant aux organisations et aux institutions gouvernementales plus de pouvoir et de capacitÃ©s pour s'attaquer directement aux ransomwares. Ces mesures montrent Ã  quel point la position des gouvernements du monde entier en matiÃ¨re de sÃ©curitÃ© a changÃ©, de la rÃ©activitÃ© Ã  la proactivitÃ©, et les entreprises feraient bien de faire de mÃªme.

Tourmente dans l'Ã©cosystÃ¨me des ransomwares

Comme pour tout fournisseur de services, la rÃ©putation est essentielle.  Les groupes RaaS ont besoin de sÃ©duire des partenaires ou des clients pour dÃ©velopper leur rÃ©seau et multiplier leurs revenus. Toute perturbation infligÃ©e Ã  ces groupes peut donc entraÃ®ner des consÃ©quences majeures et mÃªme retourner le secteur contre lui.

Comme le rÃ©vÃ¨le le rapport 2022 sur la SÃ©curitÃ©, un mois aprÃ¨s l'attaque de Colonial Pipeline, le groupe DarkSide responsable a annoncÃ© qu'il mettait fin Ã  ses activitÃ©s aprÃ¨s la saisie de ses serveurs et le vol de ses fonds cryptographiques. Cela a eu un impact sur leur capacitÃ© Ã  payer leurs partenaires RaaS. Le groupe REvil, responsable de la faille Kaseya MSP en juillet 2021, a Ã©galement disparu plus tard dans l'annÃ©e aprÃ¨s qu'une intervention des autoritÃ©s de police ait rÃ©ussi Ã  contrÃ´ler son infrastructure et son blog, rendant au groupe la monnaie de sa piÃ¨ce. Le ministÃ¨re de la Justice est allÃ© encore plus loin, a arrÃªtÃ© des membres du groupe REvil et a saisi plus de 6 millions de dollars de ranÃ§ons.

Mais que signifie cette Ã©volution pour l'Ã©cosystÃ¨me des ransomwares ?

Certains des groupes responsables de ces attaques exercent dÃ©sormais une pression supplÃ©mentaire sur leurs victimes pour que les autoritÃ©s soient tenues Ã  l'Ã©cart lors des attaques. Le groupe de ransomware Grief, par exemple, a menacÃ© de supprimer complÃ¨tement les clÃ©s de dÃ©cryptage de ses victimes si elles engageaient des nÃ©gociateurs professionnels. Par ailleurs, ce ciblage proactif des opÃ©rateurs de ransomware a conduit une multitude d'opÃ©rateurs et de partenaires Ã  quitter l'arÃ¨ne ou Ã  se sÃ©parer les uns des autres et Ã  Â«

changer de marque Â» pour Ã©viter toute inculpation ou saisie. AprÃ¨s la fermeture de DarkSide, par exemple, plusieurs membres ont formÃ© un groupe dissident appelÃ© BlackMatter, qui a lui aussi subi la pression des autoritÃ©s et a fermÃ© ses portes avant la fin de l'annÃ©e.

Cette perturbation de l'Ã©cosystÃ¨me des ransomwares n'est pas un cas isolÃ©, mais le rÃ©sultat d'une pression croissante des agences gouvernementales mondiales pour endiguer ce qui est en train de devenir rapidement une menace globale. NÃ©anmoins, les organisations ne devraient pas trop baisser la garde.

Pas encore sortis d'affaire

Bien que 2021 ait portÃ© un coup significatif Ã  l'Ã©cosystÃ¨me des ransomwares, nous risquons encore de voir des millions d'attaques de ransomwares tout au long de l'annÃ©e 2022, avec des nouveaux opÃ©rateurs et des partenaires affiliÃ©s qui existent dÃ©jÃ  et intensifient leurs efforts. Emotet, l'un des botnets les plus dangereux de l'histoire, a fait son retour fin 2021, malgrÃ© un effort coordonnÃ© des gouvernements du monde entier pour le faire disparaÃ®tre. Ce trojan bancaire issu d'un botnet modulaire a infectÃ© 1,5 million d'ordinateurs dans le monde sur des milliers de rÃ©seaux d'entreprise, souvent utilisÃ©s comme vecteur de diffusion pour des attaques de ransomware Ã  l'Ã©chelle du rÃ©seau.

Les organisations doivent donc rester vigilantes et, Ã  l'instar des gouvernements de tous les pays, adopter une attitude plus proactive et prÃ©ventive face Ã  la menace croissante des ransomwares. Cela implique d'exploiter les renseignements sur les menaces mondiales en temps rÃ©el, et de les utiliser pour protÃ©ger les entreprises non seulement des menaces visibles, mais aussi de celles que lâ€™on ne voit pas. Les vulnÃ©rabilitÃ©s Zero-day et les attaques de derniÃ¨re gÃ©nÃ©ration sont des menaces complexes qui nÃ©cessitent une rÃ©ponse complexe, ainsi qu'une sensibilisation des employÃ©s, des sauvegardes continues, une authentification multifactorielle et le recours au principe du moindre privilÃ¨ge.

Les fissures dans l'Ã©cosystÃ¨me des ransomwares commencent peut-Ãªtre Ã  se faire sentir, mais bien que les coups rÃ©cemment portÃ©s indiquent que les acteurs des ransomwares pourraient Ãªtre en train de perdre la bataille, la cyberguerre est loin d'Ãªtre terminÃ©e.