Rançongiciel, une plongée dans le monde de la cybercriminalité

Jean-Yves Marion

THE CONVERSATION
Academic rigour, journalistic flair

Rançongiciel, une plongée dans le monde de la cybercriminalité

Published: November 28, 2023 6.18pm CET

Jean-Yves Marion
Professeur d'informatique et directeur du Loria, CNRS, Inria, Université de Lorraine

Les cybercriminels agissent en bandes très organisées, et surtout très modulables.
Dan Asaki, Unsplash, CC BY

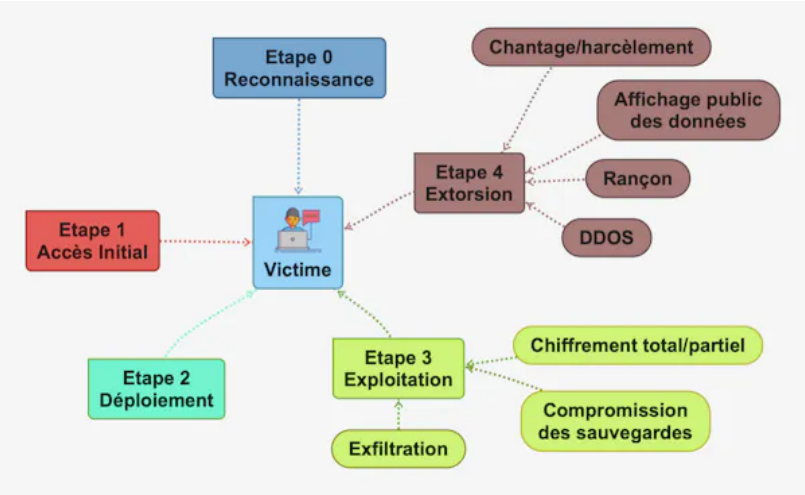
Europol vient d'annoncer le démantèlement d'un groupe de rançongiciels en Ukraine. Dans leur forme la plus basique, ces cyberattaques bloquent les systèmes informatiques et exfiltrent les données de la victime, promettant de les restituer contre rançon.

Ainsi, en août 2022, une cyberattaque attribuée au rançongiciel LockBit a paralysé le centre hospitalier sud-francilien en exfiltrant 11 Gigaoctets de données de patients et d'employés. L'hôpital a dû fonctionner en « mode dégradé » pendant plusieurs mois, avec les dossiers médicaux inaccessibles et des appareils de soin inutilisables. En juillet 2023, c'est le port de Nagoya, l'un des plus importants du Japon, qui a été obligé de s'arrêter pendant deux jours à cause d'un rançongiciel.

De l'exfiltration des données à leur revente sur des marchés illicites et aux menaces de rendre publiques les informations volées, jusqu'au fonctionnement très altéré des organisations victimes des attaques, la réalité du terrain est brutale, purement criminelle et vise sans discernement les particuliers, les hôpitaux, les écoles et toutes les organisations et entreprises vulnérables.

Les organisations cybercriminelles sont aujourd'hui bien organisées et leurs façons de procéder évoluent pour plus d'efficacité : l'économie et l'écosystème souterrains à l'origine de ces cyberattaques sont très modulables et se sont même « uberisé », ce qui les rend résilients aux démantèlements et actions en justice.

C'est une plongée dans ce monde de la cyberextorsion que nous vous proposons ici.



Le mode opératoire des cybercriminels utilisant des rançongiciels est en constante évolution. Jean-Yves Marion, Fourni par l'auteur

L'extorsion cyber en constante évolution

Quand on parle de rançongiciel, on pense à un programme malveillant qui va chiffrer (crypter) les données d'un ordinateur et demander une rançon pour rendre ces données. Par exemple, le rançongiciel Wannacry, qualifié de « sans précédent » par Europol, avait compromis environ 5 millions d'appareils en 2017, après avoir exploité une vulnérabilité pour se propager automatiquement.

Aujourd'hui, cette notion a évolué : les rançongiciels sont opérés par des humains qui explorent l'ensemble du système informatique compromis. Les attaques peuvent se déployer sur plusieurs mois, tenir compte des systèmes attaqués et « avancer » à l'intérieur du réseau informatique. Les données sensibles et d'autres informations peuvent être exfiltrées et stockées sur des serveurs contrôlés par les cybercriminels.

Le groupe cybercriminel Royal a par exemple publié en mai 2023 des informations de la ville de Dallas, y compris des informations confidentielles sur la police et sur des affaires pénales.

De fait, des données partiellement rendues publiques permettent déjà de faire pression sur la victime, et l'exfiltration suffit à demander une rançon. Les données peuvent aussi être revendues à un tiers.

Les attaquants peuvent aussi procéder au chiffrement des données sur les serveurs de leur propriétaire. Ce mécanisme est dit de « double extorsion » : exfiltration et chiffrement.

Enfin, le harcèlement sur la victime peut aller jusqu'à une attaque par « déni de service (DDOS) », qui rendent les services web de la victime inaccessibles. On parle alors de « triple extorsion ».

Le gain financier est le principal moteur des campagnes de rançongiciels, et en fait il faudrait plutôt parler aujourd'hui d'« extortion-wares », qui mobilisent toute une économie souterraine.

schéma de l'écosystème des rançongiciels

L'écosystème des rançongiciels s'est ubérisé, avec des services disponibles, dont des fournisseurs de logiciels d'attaques ainsi « facilitées », qui permettent à de la main-d'œuvre relativement peu qualifiée en informatique, les « affiliés », de sous-traiter les attaques des commanditaires. Jean-Yves Marion, Fourni par l'auteur

Un écosystème souterrain

Les organisations souterraines responsables de ces cyberextorsions ont gagné en maturité. Le modèle *Ransomware as a Service* (RaaS) s'est imposé comme à la fois la structure principale d'organisation et comme modèle économique.

Le RaaS est un ensemble d'acteurs qui monnayent des infrastructures, des services et des savoir-faire à leurs « affiliés » : c'est ainsi que ceux-ci disposent des moyens technologiques et humains pour réaliser concrètement les cyberattaques par rançongiciel.

Nos connaissances sur ce système cybercriminel proviennent d'interviews et des fuites d'information. Les « ContiLeaks » en particulier furent le fait de disputes entre les acteurs. Pour certaines des fuites documentées sur ContiLeaks, les fuites émanent plus précisément de désaccords subséquents à l'invasion de l'Ukraine.

Le monde de la cybercriminalité s'est ubérisé

Dans ce modèle économique du *Ransomware as a Service*, le recrutement d'« affiliés » est essentiel : ce sont eux qui réalisent les cyberattaques grâce à un certain nombre d'outils et de panneaux de contrôle fournis par l'organisation cybercriminelle à l'initiative de l'attaque. Ces organisations sont assez disparates : il existe à la fois des groupes d'acteurs et des acteurs isolés. Dans tous les cas, ces organisations sont fragmentées – ce qui, on le verra par la suite, leur permet de se reconfigurer, en cas de démantèlement notamment.

Ce soutien « technique » permet de recruter des exécutants dont le niveau technique n'est pas forcément élevé, car ils bénéficient d'outils relativement faciles à mettre en œuvre. Ironiquement d'ailleurs, un groupe se nomme « Read the Manual ».

Autrement dit, le monde de la cybercriminalité s'est, lui aussi, ubérisé. Les profits sont partagés entre les commanditaires et les affiliés (environ 70 % du paiement de la victime est reversé à l'affilié).

Ventes d'« accès » : comment pénétrer chez la victime

Un des services les plus importants est celui des fournisseurs d'accès (*Internet Access Brokers*) qui vendent notamment des mots de passe et des cookies provenant de campagnes précédentes, soit de phishing qui cherche à manipuler une victime pour obtenir un mot de passe, soit d'infostealers qui sont des logiciels spécialisés dans le vol d'information, ou enfin à la suite d'une exfiltration de données par une précédente attaque d'un rançongiciel.

En 2021, l'attaque de Colonial Pipeline a forcé l'arrêt de toutes les opérations d'un pipeline qui transporte environ 400 millions de litres d'essence par jour, ce qui a amené le ministère américain de la Justice à élever les attaques par rançongiciel au niveau du terrorisme. En effet, selon l'audition de la commission de la sécurité intérieure de la Chambre des représentants des États-Unis, l'accès initial au réseau s'est fait à partir d'un mot de passe réutilisé.

Ce type de « vente d'accès » se fait dans des marchés souterrains et des forums, comme RaidForums.

Blanchiment des rançons : démêler les flux de cryptomonnaies

Pour faire fonctionner l'écosystème, un autre service important est celui du blanchiment des rançons (en cryptomonnaies, souvent en Bitcoin). Pour cela, des outils informatiques sont utilisés : des « mixeurs » pour rendre les transactions financières intraçables, et des « échangeurs » pour échanger les cryptoactifs.

Afin de démanteler les services de blanchiment et d'arrêter les cybercriminels, les forces de l'ordre essaient de surveiller ces échanges de cryptomonnaies. C'est ainsi qu'une action internationale a permis de démanteler la plate-forme d'échange de cryptoactifs Bitzlato.

Une des limitations à ces actions internationales est que les organisations RaaS s'appuient le plus souvent sur des infrastructures hébergées dans des pays qui ne collaborent pas, ou peu, avec les forces de l'ordre européennes et américaines.

Une économie souterraine résiliente

Le modèle RaaS permet de réduire les risques pour les cybercriminels, comme l'observe le rapport 2022 de l'agence européenne pour la cybersécurité (Enisa). En effet, l'arrestation d'un seul cybercriminel n'est pas suffisante pour stopper les méfaits d'un rançongiciel : les groupes comme Conti se fragmentent et se recomposent en différents autres groupes.

frise chronologiques d'activités cybercriminelles

Synthèse chronologique des activités connues du groupe cybercriminel FIN12, illustrant le fait que ce type de gang se désagrège et se reconstitue, ce qui démontre leur adaptabilité et leur résilience. Agence nationale de la sécurité des systèmes d'information (ANSSI) -- septembre 2023. Licence ouverte (Étalab -- v2.0)

Aussi efficaces soient-elles, les actions de justice internationale n'ont parfois qu'un effet limité. Par exemple, le « world's most dangerous malware », appelé Emotet, a été démantelé en janvier 2021… pour reprendre du service un an plus tard.

Ce constat peut sembler pessimiste mais ne doit pas masquer que les actions de justice secouent de fait le monde cybercriminel, comme l'ont montré l'opération offensive contre le rançongiciel Hive ou le démantèlement de Ragnar Locker (suite notamment à une arrestation à Paris).

D'un point de vue économique, le modèle RaaS optimise le retour sur investissement (ROI). L'économie souterraine RaaS prospère. Elle est basée sur des marchés illicites dans le dark web. En moyenne, un ransomware est vendu pour 56 dollars américains selon l'étude menée entre novembre 2022 et février 2023.

Les marchés souterrains sont très volatils et fragmentés. Cette fragmentation permet aux cybercriminels de poursuivre leurs activités commerciales, même après une saisie par les forces de l'ordre comme celles de DarkMarket et de HydraMarket.

Cyberattaques et conflits armés : la naissance des « cyber-mercenaires » ?

Des organisations clandestines prennent forme, disparaissent et renaissent, parfois instrumentalisées par les États, comme l'a montré le conflit ukrainien. Rien d'étonnant à cela, puisque les moyens d'une cyberattaque sont quasiment les mêmes, que l'objectif soit financier, d'espionnage ou de destruction.

Déjà en 2017, et malgré sa ressemblance avec le rançongiciel WannaCry déjà bien connu, les actions du malware NoPetya ont été destructrices, causant environ 10 milliards de dollars de dommages totaux, et préfigurant les cyberattaques menées pendant le conflit ukrainien à l'aide d'armes avec les « wipers », qui effacent les informations de systèmes compromis.

Les tensions géopolitiques pourraient encourager les acteurs à l'origine des rançongiciels à poursuivre les cyberconflits en cours : en adaptant légèrement leurs comportements, ils peuvent facilement devenir des sources d'espionnage, comme des « cyber-mercenaires ».

Le PEPR Cybersécurité et le projet ANR-22-PECY-0007 sont opérés par l'Agence nationale de la recherche (ANR), qui finance en France la recherche sur projets. Elle a pour mission de soutenir et de promouvoir le développement de recherches fondamentales et finalisées dans toutes les disciplines, et de renforcer le dialogue entre science et société. Pour en savoir plus, consultez le site de l'ANR.