Ransomware : augmentation des techniques de triple extorsion
Internet
PostÃ© par : JulieM
PubliÃ©e le : 4/6/2021 13:00:00

Ã lâ□□instar de tout entrepreneur avisÃ©, les cybercriminels ont conscience que le succÃ¨s de leur entreprise dÃ©pend de la valeur de leur derniÃ¨re innovation. Et lorsquâ□□il sâ□□agit de dÃ©rober lâ□□argent des organisations non sÃ©curisÃ©es, les innovations ne faiblissent jamais.

Philippe Alcoy, spÃ©cialiste sÃ©curitÃ© chez NETSCOUT, revient sur la triple extorsion, ce nouveau Â« tiercÃ© gagnant Â» du ransomware qui combine le chiffrement de fichiers, le vol de donnÃ©es et les attaques DDoS, dans un portefeuille de Ransomware-as-a-Service (RaaS) et est de plus en plus plÃ©biscitÃ© par les cybercriminels :

1. Chiffrement. Dans le cadre de la mÃ©thode traditionnelle dâ□□attaque par ransomware, les cybercriminels pÃ©nÃ¨trent dans un rÃ©seau et chiffrent des donnÃ©es prÃ©cieuses, empÃªchant ainsi lâ□□organisation victime (et parfois lâ□□ensemble du systÃ¨me) dâ□□accÃ©der Ã ces donnÃ©es. Les attaquants demandent ensuite le paiement dâ□□une rançon en Ã©change dâ□□une clÃ© de dÃ©chiffrement.

2. Vol. Les cybercriminels exfiltrent les donnÃ©es avant de neutraliser la victime. Ils menacent ensuite dâ□□exposer et/ou de vendre publiquement les donnÃ©es dÃ©robÃ©es Ã moins de recevoir une contrepartie. Dans ce deuxiÃ¨me niveau dâ□□extorsion, il est plus difficile pour les victimes de faire fi des menaces de ransomware, car mÃªme celles qui ont la possibilitÃ© dâ□□utiliser des sauvegardes pour restaurer leurs donnÃ©es demeurent vulnÃ©rables Ã lâ□□exposition de ces derniÃ¨res. Il sâ□□agit clairement dâ□□un outil de monÃ©tisation profitable, puisque Coveware estime que prÃ¨s de la moitiÃ© des cas de ransomware au troisiÃ¨me trimestre 2020 ont recouru Ã des tactiques dâ□□exfiltration.

3. Attaque DDoS. Habituellement utilisÃ©es comme mÃ©thode dâ□□extorsion autonome, les attaques DDoS sâ□□ajoutent dÃ©sormais Ã la liste des services proposÃ©s par les opÃ©rateurs RaaS. Cette situation accentue la pression exercÃ©e sur la victime, et ce, de plusieurs faÃ§ons : elle met en Ã©vidence le sÃ©rieux de lâ□□adversaire. Le maintien de la disponibilitÃ© constitue Ã©galement un facteur de stress supplÃ©mentaire pour une Ã©quipe de sÃ©curitÃ© dÃ©jÃ confrontÃ©e aux deux premiers Ã©vÃ©nements.

En combinant le chiffrement de fichiers, le vol de donnÃ©es et les attaques DDoS, les cybercriminels ont pour ainsi dire obtenu le tiercÃ© gagnant du ransomware, lequel est conÃ§u pour augmenter les chances de recevoir un paiement. Selon Bleeping Computer, SunCrypt et Ragnor Locker ont Ã©tÃ© les premiers Ã recourir Ã cette tactique. Depuis lors, dâ□□autres opÃ©rateurs de ransomware les ont rejoints, notamment Avaddon et Darkside, lâ□□auteur de lâ□□incident de Colonial Pipeline.

Du point de vue des cybercriminels, lâ□□ajout dâ□□attaques DDoS Ã la liste des services de ransomware reprÃ©sente une dÃ©marche opÃ©rationnelle avisÃ©e. Les attaques DDoS sont extrÃªmement peu coÃ»teuses et faciles Ã lancer, risquant ainsi dâ□□augmenter les chances de voir une victime payer la rançon.

Pourquoi ne pas en profiter ? AprÃ¨s tout, il sâ□□agit dâ□□une activitÃ© trÃ¨s lucrative et les acteurs malveillants ajoutent constamment de nouvelles armes Ã leurs campagnes dâ□□attaque multiformes. Certains opÃ©rateurs ajoutent mÃªme un service de centre dâ□□assistance pour aider les victimes Ã dÃ©chiffrer les donnÃ©es.

En fin de compte, la multiplication des moyens de pression augmente la probabilitÃ© de recevoir le paiement dâ□□une ranÃ§on, si bien que les ransomwares constituent une forme de cybercriminalitÃ© de plus en plus dÃ©stabilisante qui touche non seulement les entreprises, mais aussi les gouvernements, les Ã©coles et les infrastructures publiques.

La nature de ces attaques Ã plusieurs volets dÃ©montre la persistance d'acteurs malveillants lorsqu'ils voient une opportunitÃ© d'extorquer de l'argent. De plus, la menace d'une attaque ne disparaÃ®t pas simplement si les organisations ciblÃ©es choisissent de payer la ranÃ§on immÃ©diatement.

Dans notre monde de plus en plus digitalisÃ©, oÃ¹ la taille, la frÃ©quence et la complexitÃ© des attaques ne cessent d'augmenter, il est essentiel que les dÃ©fenseurs et les professionnels de la sÃ©curitÃ© se tiennent au courant des tendances des cyberattaques et continuent Ã se renseigner sur la maniÃ¨re de protÃ©ger les infrastructures critiques.

Des mesures sont prises pour faire face Ã la crise, comme la Ransomware Task Force (RTF) crÃ©Ã©e par lâ□□Institute for Security and Technology. ComposÃ©e dâ□□une large coalition dâ□□experts de la securitÃ©, du gouvernement, des services rÃ©pressifs, de la sociÃ©tÃ© civile et des organisations internationales, la RTF a rÃ©cemment publiÃ© des recommandations clÃ©s pour combattre ce que le groupe qualifie de risque sÃ©curitaire urgent.

Bien que cela soit un bon dÃ©but, un effort mondial de grande ampleur reste toutefois nÃ©cessaire pour mettre un frein Ã lâ□□activitÃ© des ransomwares. Les agences de sÃ©curitÃ© du monde entier, telles que lâ□□ANSSI en France sâ□□activent et ont formulÃ© des recommandations pour permettre de se prÃ©munir contre ces attaques localement.

En attendant, les entreprises peuvent recourir Ã quelques bonnes pratiques aussi simples que fondamentales pour Ã©viter ces attaques. Elles peuvent tout dâ□□abord inculquer aux employÃ©s les bases dâ□□une bonne hygiÃ¨ne de cybersÃ©curitÃ© et leur apprendre Ã utiliser les outils de protection des rÃ©seaux et des terminaux mis Ã leur disposition par les Ã©quipes IT.

Il sera alors plus facile de dÃ©tecter les logiciels malveillants, les activitÃ©s inhabituelles ou encore les indicateurs de compromission. En outre, encourager les Ã©quipes Ã sauvegarder les donnÃ©es importantes, tester les plans de restauration des donnÃ©es, effectuer des Ã©valuations de la vulnÃ©rabilitÃ©, appliquer des correctifs et mettre Ã jour les systÃ¨mes informatiques en consÃ©quence sont un ensemble de mesures qui permettront dâ□□Ã©viter de maniÃ¨re proactive et efficace toute compromission.

Face aux attaques DDoS qui ne cessent de gagner en ampleur, en frÃ©quence et en complexitÃ©, les entreprises doivent sâ□□attendre Ã tout moment Ã subir une attaque pour ne jamais Ãªtre prises de court. Les dÃ©ploiements dâ□□outils combinÃ©s Ã une visibilitÃ© complÃ¨te des rÃ©seaux et des infrastructures sur site et dans le cloud permettront aux Ã©quipes de garder une longueur dâ□□avance sur les cybercriminels et de dÃ©jouer toutes les facettes dâ□□une triple attaque dâ□□extorsion. Â»