Se préparer aux attaques visant un anéantissement total

Le paysage des menaces a connu des changements considérables. Êtes-vous prêt à faire face aux nouvelles attaques destructrices ?

Écrit par Brian Hymer, architecte des systèmes stratégiques chez Quest® Software, en collaboration avec Randy Franklin Smith, expert de la sécurité Windows et Active Directory

INTRODUCTION

Les professionnels de l'informatique et de la sécurité ont longtemps lutté contre de sérieuses menaces. D'une part, les coupures de courant, les pannes de matériel et les catastrophes naturelles. D'autre part, les menaces provenant d'utilisateurs internes et de pirates habiles, disposant d'une panoplie de techniques et d'outils innovants pour exploiter les vulnérabilités et créer des virus, des logiciels malveillants et des rançongiciels de plus en plus sophistiqués.

Se défendre contre ces menaces n'a jamais été chose facile, mais dans l'ensemble, les risques sont majoritairement limités. Les menaces d'origine naturelle se limitent généralement à une zone géographique, c'est pourquoi avoir un datacenter de secours situé à un autre endroit constitue un moyen de défense efficace. Les attaques d'origine humaine visent habituellement un objectif précis : accéder à vos données pour les voler et les vendre ou pour les chiffrer, les tenir en otage et demander une rançon. Les professionnels de l'informatique savent donc établir un ordre de priorité des stratégies de protection des données.

Mais, dernièrement, la situation a pris un tournant catastrophique. En effet, de plus en plus d'attaques cherchent tout bonnement à anéantir l'intégralité de votre infrastructure. Malheureusement, de nombreuses entreprises ne sont tout simplement pas préparées. Ce livre blanc examine certaines des récentes attaques les plus destructrices, analyse leur vitesse, leur étendue et les méthodes employées, et explore les meilleures stratégies de défense.

VITESSE ET PUISSANCE DES ATTAQUES DESTRUCTRICES

Vous avez certainement entendu ces noms aux accents futuristes : NotPetya. Shamoon. Stuxnet. Olympic Destroyer. BlackEnergy. Destover. Wiper. Triton. Que s'est-il passé lors de ces attaques destructrices ? Passons en revue certains incidents récents pour comprendre la vitesse et l'étendue de ces attaques, et par conséquent l'urgence de trouver une stratégie de défense.

Stuxnet

À la fin des années 2000, Israël et les États-Unis étaient de plus en plus inquiets au sujet du programme nucléaire iranien. En 2009, l'Iran produisait tellement d'uranium enrichi qu'il pouvait fabriquer deux armes nucléaires en un an. Pour faire face à ce problème, Israël et les États-Unis auraient commencé à développer un ver informatique sophistiqué, Stuxnet, conçu non pas pour pirater les ordinateurs ou voler les données, mais pour détruire l'équipement physique. Plus précisément, Stuxnet infecte un ordinateur

De plus en plus d'attaques cherchent à anéantir l'intégralité de votre infrastructure. De nombreuses entreprises ne sont tout simplement pas préparées.

connecté à des contrôleurs logiques programmables spécifiques qui gèrent les équipements industriels, comme les centrifugeuses à uranium. Il modifie la programmation des contrôleurs et peut ainsi forcer les centrifugeuses à tourner trop vite et trop longtemps, alors que les contrôleurs indiquent un fonctionnement normal. Le comportement anormal ne peut donc pas être repéré par le personnel qui surveille les installations. Au fil du temps, les machines infectées cessent de fonctionner sous l'effet d'une utilisation intensive. En 2010, plus d'une quinzaine d'usines iraniennes étaient infectées par Stuxnet, et près d'un cinquième des centrifugeuses nucléaires du pays étaient hors service.

Stuxnet n'était pas censé se propager au-delà des installations nucléaires iraniennes, isolées physiquement et non connectées à Internet. Curieusement, le logiciel malveillant a pourtant atteint Internet et s'est propagé. Petit à petit, d'autres groupes ont modifié le virus pour cibler divers types d'installations, comme les usines de traitement des eaux, les centrales électriques, les agences gouvernementales et des entreprises des secteurs de l'aviation, de la défense et pharmaceutique. Ces virus modifiés, parfois appelés les « fils de Stuxnet », sont Duqu, Flame, Havex, Industroyer et Triton.

Shamoon

En 2012, c'est au tour d'une compagnie pétrolière d'être touchée par une cyberattaque destructrice. Le 15 août, un virus, par la suite appelé Shamoon, a infecté les trois quarts du parc de 40 000 stations de travail appartenant à l'entreprise Saudi Aramco, effaçant ses disques durs et affichant l'image du drapeau américain en flammes. Bien que la compagnie a déclaré que ses activités de production et d'exploration pétrolières n'ont pas été touchées par l'attaque et que son réseau interne principal a été hors ligne pendant seulement dix jours, un consultant ayant participé à l'opération de restauration a affirmé que Saudi Aramco a dû reconstruire son centre des opérations de sécurité à partir de zéro et qu'il a ensuite fallu attendre cinq mois pour que les systèmes soient de nouveau opérationnels. Cette attaque aurait facilement conduit une entreprise plus petite à la faillite.

Shamoon s'est fait oublier pendant quatre ans avant de réapparaître en 2016 sous la forme d'une version légèrement modifiée qui a été utilisée contre plusieurs administrations et entreprises civiles en Arabie Saoudite et dans d'autres pays du Golfe. Le logiciel malveillant destructeur s'est de nouveau manifesté à la fin de l'année 2018, touchant plusieurs cibles au Moyen-Orient. Cette nouvelle variante de Shamoon est encore plus destructrice que les précédentes car elle supprime tous les fichiers des ordinateurs infectés avant d'effacer le secteur principal de démarrage (MBR), rendant impossible toute restauration des fichiers.

BlackEnergy

La première cyberattaque réussie d'un réseau électrique s'est produite en 2015. En décembre, des pirates ont utilisé le logiciel malveillant BlackEnergy pour infiltrer plusieurs centres de distribution électrique en Ukraine et entraîner la panne des systèmes électriques. Bien que cette attaque n'ait affecté que 225 000 clients et n'ait duré que quelques heures, elle montre la puissance dont peut faire preuve un logiciel malveillant pour nuire à une infrastructure stratégique. De futures attaques ciblant des fournisseurs d'énergie pourraient s'avérer bien plus dévastatrices.

NotPetya

À ce jour, l'attaque la plus vaste et la plus coûteuse a eu lieu en 2017. Un dirigeant financier du bureau ukrainien du géant des transports internationaux Maersk avait fait une demande courante : il avait demandé au département informatique d'installer un logiciel de comptabilité, M.E.Doc, sur un seul ordinateur. M.E.Doc n'étant pas une application choisie au hasard, mais la solution de fiscalité et de comptabilité utilisée partout en Ukraine, le département informatique a répondu à sa requête. Par la suite, le 27 juin, les ordinateurs du siège de Maersk ont cessé de fonctionner. Selon les enquêteurs, des pirates sponsorisés par un État auraient piraté les serveurs de mise à jour de M.E.Doc et utilisé une porte dérobée pour propager le logiciel malveillant au sein de chaque entreprise utilisant M.E.Doc.

En quelques heures, la société Maersk était paralysée. Chacun de ses 150 contrôleurs de domaine du monde entier, excepté un contrôleur situé au Ghana qui était par chance hors ligne au moment de l'attaque, était en panne. Les terminaux d'expédition ont été bloqués pendant des jours partout dans le monde, refoulant des dizaines de milliers de camions et stockant des conteneurs de denrées périssables sans réfrigération. L'opération de nettoyage a nécessité de reconstruire 4 000 serveurs et 45 000 stations de travail. Selon un dirigeant de Maersk, NotPetya a coûté

entre 250 millions et 300 millions de dollars à l'entreprise. Mais d'autres salariés pensent que le préjudice est plus important.

L'attaque n'a pas seulement touché Maersk. NotPetya a infecté d'autres entreprises autour du globe, aussi bien en Allemagne qu'aux États-Unis ou en Tasmanie, et ce, à une vitesse phénoménale. NotPetya a interrompu l'activité du réseau d'une grande banque ukrainienne en seulement 45 secondes. Une partie d'une grande plateforme de transit ukrainienne a été infectée en 16 secondes. Pratiquement tous les organismes fédéraux d'Ukraine ont été immobilisés. Le préjudice global a été estimé à plus de 10 milliards de dollars.

Attaques dans le Cloud

Les attaques destructrices ne se limitent pas aux environnements informatiques locaux. Mais cela ne signifie pas que tous les incidents ayant eu lieu dans le Cloud jusqu'à présent impliquent des logiciels malveillants aux noms saugrenus. Par exemple, en 2014, le fournisseur IaaS Code Spaces a cessé son activité après avoir subi une attaque en plusieurs étapes sur ses serveurs. La plupart des données, sauvegardes, configurations des machines et sauvegardes hors site de l'entreprise ont été partiellement ou totalement supprimées.

Plus récemment, en février 2019, des pirates ont attaqué le fournisseur d'adresses e-mail VFemail et formaté tous les disques de chaque serveur de fichiers et de sauvegarde de son infrastructure aux États-Unis, détruisant ainsi toutes les données des e-mails de ses clients aux États-Unis. Les attaquants ont également ciblé les ressources informatiques de l'entreprise aux Pays-Bas, mais ont été pris sur le fait, ce qui a permis à VFemail de sauver une partie de ses données de sauvegarde. L'attaque a malgré tout effacé la quasi-totalité de son infrastructure en quelques heures seulement. L'entreprise pensait mettre la clé sous la porte mais parvient encore à maintenir ses activités.

LES MOTIVATIONS DES ATTAQUES DESTRUCTRICES

Les attaques traditionnelles sont généralement motivées par des raisons financières. Par exemple, les pirates demandent un paiement en échange d'une clé de décryptage lors d'une attaque par rançongiciel ; ils obtiennent des informations personnelles ou de santé protégées en vue d'une usurpation d'identité ou d'une vente sur le marché noir ; ils collectent des informations d'identification pour les utiliser lors de futures attaques permettant de gagner de l'argent. Les attaques destructrices reposent sur une multitude de motivations, notamment :

- **Motivations politiques :** le piratage par des États-nations est de plus en plus répandu. Par exemple, des experts pensent que Stuxnet a été développé conjointement par les États-Unis et Israël pour perturber le programme nucléaire de l'Iran, et que NotPetya était une attaque visant l'Ukraine pour des raisons politiques. Certains pensent que l'Iran a lancé l'attaque Shamoon de 2012 pour riposter suite à l'attaque Stuxnet lancée par les États-Unis. Les pirates sponsorisés par des États sont généralement très habiles et reçoivent un financement important pour que leurs attaques soient particulièrement dévastatrices.
- **Motivations d'ordre social :** la volonté de faire changer la société peut motiver certaines attaques. Souvent appelés « hacktivistes », ces groupes mettent au point des attaques par déni de service (DoS) pour cibler les organisations qui vont à l'encontre de leurs idées. Par exemple, le groupe d'hacktivistes Anonymous est principalement connu pour sa campagne d'attaques DoS lancée en 2010 contre PayPal.com et les sites de Visa et MasterCard en guise de représailles, car ces entreprises ont suspendu le financement du site Wikileaks à la demande du gouvernement américain.
- **Vengeance :** à l'autre extrême, les attaques peuvent provenir de personnes mécontentes au sein même des organisations. Par exemple, au début de l'année 2002, Roger Duronio, administrateur informatique chez UBS Paine Webber, aurait créé et déployé une bombe logique sur des milliers de systèmes en utilisant des outils d'administration Unix standard. Il aurait ensuite démissionné et serait immédiatement allé chez son courtier pour vendre à découvert 21 000 dollars d'actions UBS/PW. Lorsque la bombe logique a « explosé » quelques semaines plus tard, elle a paralysé 2 000 serveurs et effacé tous les fichiers qu'ils contenaient. Les dégâts causés étaient si importants que les salariés devaient utiliser du papier et un stylo pour travailler. La société a dépensé 3 millions de dollars rien qu'en honoraires de consultation pour restaurer les systèmes. Mais alors, quelle était la motivation de Roger Duronio ? Il était apparemment mécontent de sa prime, qui était inférieure de 18 000 dollars aux 50 000 dollars qu'il espérait recevoir.

  Dans un environnement Windows, il est d'autant plus facile pour un utilisateur privilégié insatisfait de causer des ravages : il suffit d'empêcher Active Directory de fonctionner. Si Active Directory est en panne, c'est tout votre réseau qui l'est, même s'il n'y a aucun problème avec vos serveurs ou vos applications.
- **Écran de fumée :** de plus en plus souvent, les pirates couvrent une attaque conçue

NotPetya a interrompu l'activité du réseau d'une grande banque ukrainienne en seulement 45 secondes. L'ensemble des dommages causés au niveau mondial par l'attaque de 2017 a été estimé à plus de 10 milliards de dollars.

pour voler des informations à l'aide d'une attaque destructrice. L'attaque destructrice peut entraver les enquêtes scientifiques, car elle empêche d'identifier les attaquants. Ils échappent ainsi aux poursuites et protègent leur mode opératoire afin de pouvoir utiliser les mêmes techniques par la suite. Par exemple, le logiciel malveillant Olympic Destroyer a paralysé des systèmes informatiques avant la cérémonie d'ouverture officielle des Jeux Olympiques d'hiver de 2018 en Corée du Sud. Et il a tellement bien brouillé les pistes que lorsqu'il est réapparu un an après, ciblant des organismes financiers et des laboratoires spécialisés dans la prévention des menaces chimiques et biologiques, les enquêteurs ne pouvaient définir avec certitude s'il avait été utilisé par le même groupe ou par d'autres pirates ayant des intérêts différents.

- **Dommages collatéraux :** les attaques destructrices ne ciblent pas particulièrement toutes les victimes. Certaines font partie des dommages collatéraux. Par exemple, les architectes de l'attaque NotPetya visaient clairement l'Ukraine (d'après les estimations, 80 % des infections ont eu lieu dans ce pays), mais des entreprises du monde entier, dont Maersk, ont subi des dommages considérables.

Toute entreprise peut être la cible d'une attaque destructrice ou subir les dommages collatéraux d'une attaque ciblant une autre entreprise.

MÉTHODOLOGIE

Nous avons constaté que les attaques destructrices prennent diverses formes. Certaines reposent sur des logiciels malveillants ou des virus, d'autres sur la force brute. Certaines tentent d'effacer des données, tandis que d'autres visent à causer des dommages physiques. Examinons plus en détail le déroulement de ces attaques.

Accès initial

La première étape d'une attaque consiste généralement à accéder à votre réseau. Vous connaissez certainement la plupart des techniques utilisées, comme celles listées ci-dessous. Il est important de souligner que les attaques destructrices ne ciblent pas uniquement les ordinateurs, les stations de travail et les serveurs, mais qu'elles portent également sur les appareils IoT, les routeurs et plus encore.

- **Hameçonnage :** Shamoon a infiltré le réseau de l'entreprise Saudi Aramco lorsqu'un salarié de l'équipe informatique a ouvert un e-mail d'hameçonnage malveillant.
- **Porte dérobée :** le logiciel de mise à jour d'une solution tierce contenait une porte dérobée qui a permis à des pirates de répandre NotPetya au sein de Maersk et d'autres organisations dans le monde entier.
- **Appareil USB infecté :** étant donné que les installations nucléaires iraniennes n'étaient pas connectées à Internet, Stuxnet a dû être introduit à l'aide d'un appareil USB physique, de façon délibérée ou accidentelle.
- **Vulnérabilités logicielles :** une technique utilisée dans le cadre de l'attaque NotPetya, ainsi que l'attaque par rançongiciel WannaCry en 2017, repose sur l'outil d'infiltration EternalBlue, créé par la NSA (National Security Agency), qui a été divulgué lors d'une terrible faille. EternalBlue tire parti d'une vulnérabilité d'un protocole Windows spécifique, et permet ainsi aux pirates d'exécuter librement à distance leur propre code sur toute machine non corrigée.
- **Détournement de réseau Wi-Fi ou d'émetteur :** en 2015, les fabricants de la Jeep Cherokee ont dû rappeler 1,4 million de véhicules après que des chercheurs aient montré qu'ils pouvaient détourner à distance les systèmes des voitures via Internet. Des attaquants pouvaient potentiellement prendre le contrôle du système de verrouillage des portes, des freins, du moteur ou des fonctions de conduite autonome des véhicules. De même, la FDA a confirmé que certains implants cardiaques présentent des failles qui permettraient aux pirates de vider la batterie ou d'appliquer des stimulations ou chocs erronés.
- **Vulnérabilités des appareils IoT :** en octobre 2016, la pire attaque par déni de service distribué (DDoS) a paralysé de nombreux sites Internet, notamment Twitter, Netflix, Reddit et CNN, en visant le fournisseur de services Dyn. Le botnet utilisé pendant l'attaque était constitué d'un grand nombre d'appareils connectés à Internet, tels que des imprimantes, des appareils photo numériques, des moniteurs pour bébé et des routeurs grand public, infectés par un programme malveillant appelé Mirai.
- **Vulnérabilités des autres appareils :** que feriez-vous si un individu réinitialisait tous vos routeurs, pare-feu et points d'accès sans fil aux valeurs d'usine ou autres paramètres de son choix ? Et s'il volaitvos données pour s'en servir à ses propres fins ? En 2018, le FBI a encouragé les consommateurs à redémarrer leurs routeurs pour interrompre la diffusion d'un programme malveillant appelé VPNFilter. Les chercheurs soupçonnaient un groupe lié au service de renseignement militaire russe de lancer des cyberattaques coordonnées contre l'Ukraine. Le logiciel malveillant a depuis été mis à niveau et peut survivre à un redémarrage système. Toute personne utilisant l'un des 70 appareils les plus vulnérables est désormais invitée à mettre immédiatement à jour le firmware.[1]

Propagation à l'intérieur du réseau et dommages causés

Une fois installé, le programme malveillant se propage de la machine infectée

1 Pour plus d'informations, consultez le rapport initial de Cisco Talus sur VPNFilter et l'article de blog mentionnant la liste mise à jour des appareils concernés. Cependant, veillez à chercher les informations les plus récentes via votre moteur de recherche préféré ou toute autre option de recherche.

aux autres ordinateurs du réseau. Une technique adoptée par les pirates consiste à exploiter l'outil Mimikatz pour recueillir les identifiants stockés dans la mémoire de l'ordinateur et les utiliser pour accéder à d'autres machines. Il arrive que les pirates remportent le jackpot en récupérant des informations d'identification de l'administrateur en plus des identifiants utilisateur ordinaires. Dans le cas d'entreprises ne possédant pas de segmentation réseau appropriée ou d'autres limites de sécurité, le logiciel malveillant se propage rapidement et d'autres pirates peuvent se déplacer latéralement bien plus facilement. La discrétion des techniques d'intrusion et le manque de surveillance et d'alerte continues leur permettent de passer inaperçus.

Ensuite, l'essentiel de l'attaque est lancé. Le plus souvent, l'objectif est de supprimer des données spécifiques, voire l'ensemble du système de fichiers. Pour supprimer des données, certaines attaques remplacent des fichiers entiers. Toutefois, cette option exigeant du temps, d'autres utilisent des raccourcis tout aussi efficaces. À titre d'exemple, une attaque peut remplacer un bloc de 500 octets tous les deux mégaoctets ou simplement remplacer les premiers octets d'un fichier pour supprimer les informations d'en-tête. Dans les deux cas, cette technique rend les fichiers inutilisables même s'ils ne sont pas complètement supprimés. Il existe également des logiciels malveillants destructeurs qui s'attaquent au sous-système d'initialisation (BIOS) et des logiciels malveillants conçus pour désactiver des services.

Le plus souvent, une attaque n'est déclenchée que lorsque le logiciel malveillant atteint un point de saturation, afin d'empêcher la victime de détecter l'attaque à temps et de prendre des mesures défensives. Pour éviter une signature élevée d'E/S, qui peut être plus facilement détectée, le logiciel malveillant transfère parfois les tâches les plus lourdes au chargeur de démarrage. De plus, les attaques sont souvent programmées pour causer le plus de dommages possible. Les logiciels malveillants NotPetya et Shamoon ont tous deux été déclenchés alors que la plupart des employés étaient absents pour une fête nationale ou religieuse, limitant ainsi les chances de détecter l'attaque rapidement et empêchant les victimes de réagir.

STRATÉGIES DE PRÉVENTION ET DE DÉTECTION

Toute entreprise peut être la cible d'une attaque destructrice ou subir les dommages collatéraux d'une attaque ciblant une autre entreprise. Il est donc nécessaire de prendre des mesures pour limiter les risques. La première étape consiste à mettre en place des bonnes pratiques de sécurité standard pour empêcher les pirates d'accéder à votre réseau, limiter leur déplacement latéral en cas d'intrusion ainsi que la portée de l'attaque, et détecter leur activité malveillante. Voici certaines des principales stratégies :

- Assignez des autorisations basées uniquement sur le principe de « privilège minimal ».
- Utilisez un modèle de sécurité à plusieurs niveaux, tel que l'ESAE (Enhanced Security Administrative Environment) de Microsoft, plus communément appelé le modèle « Forêt rouge », pour séparer les utilisateurs privilégiés des utilisateurs professionnels réguliers.
- N'autorisez pas le fonctionnement de codes non approuvés.
- N'exécutez pas de logiciels obsolètes et renouvelez les correctifs.
- Auditez les modifications apportées à votre environnement et utilisez des outils qui vous permettent d'empêcher la modification des objets les plus stratégiques, tels que les groupes hautement privilégiés.
- Surveillez de près les configurations et autres changements de système, ainsi que les opérations inhabituelles, telles que les commandes pouvant altérer les partitions de démarrage ou bloquer un système.
- Contrôlez l'activité des utilisateurs, en particulier l'activité des comptes à privilèges. Utilisez de préférence un outil qui crée une référence d'activité normale, surveillez toute anomalie et analysez-la en contexte pour réduire le nombre d'alertes et détecter rapidement les vraies menaces.
- Automatisez les mesures d'intervention. Aujourd'hui, le déroulement d'une attaque ne prend que quelques secondes. Vous ne pouvez pas vous contenter d'un tableau de bord dans votre centre des opérations de sécurité. Le temps qu'une intervention humaine détecte le problème, l'examine et réagisse, le mal est déjà fait. C'est pour cette raison que l'automatisation de la sécurité et l'orchestration sont essentielles.

STRATÉGIES DE REPRISE D'ACTIVITÉ

Associer des stratégies efficaces de protection et de détection est primordial, mais en aucun cas suffisant. Dans la plupart des attaques mentionnées

Des techniques efficaces de protection et de détection sont essentielles mais ne suffisent pas. Vous devez également disposer d'une stratégie complète de reprise d'activité.

plus haut, il a été reproché à juste titre aux victimes de ne pas avoir mis en place des principes de base de sécurité. À titre d'exemple, au moment de l'attaque NotPetya de 2017, certains serveurs de Maersk exécutaient encore Windows 2000, une version que Microsoft a cessé de prendre en charge en 2010. De plus, la segmentation réseau de Maersk n'étant pas suffisante, le logiciel malveillant s'est propagé facilement de la brèche initiale à l'ensemble du réseau.

Toutefois, il est important de souligner que Maersk n'a pas commis d'erreur qui aurait provoqué l'infection de son système. Le logiciel malveillant a été activé via un package logiciel standard de comptabilité fiscale utilisé par la majorité des entreprises en Ukraine. Plusieurs entreprises ont subi des dommages dévastateurs suite à cette attaque. À l'instar de Maersk, la plupart d'entre elles n'étaient pas les cibles directes, mais seulement des victimes collatérales.

La leçon à tirer est simple : même si votre entreprise ne pense pas avoir d'ennemis et même si elle met en place les bonnes pratiques de sécurité recommandées par les experts, elle peut être victime d'une attaque destructrice. Il est donc crucial d'avoir une stratégie de reprise d'activité testée et reconnue.

Maersk n'avait pas de stratégie. Ils ont pu s'en sortir par un heureux hasard. Lorsque NotPetya a neutralisé l'ensemble de ses 150 contrôleurs de domaine, aucune sauvegarde n'a été trouvée. Or, sans la restauration de ses contrôleurs, l'entreprise était paralysée. Par chance, une coupure de courant a provoqué la panne d'un contrôleur de domaine situé au Ghana au moment de l'attaque. Malheureusement, la bande passante du bureau du Ghana était si lente que le téléchargement des données depuis le contrôleur de domaine aurait demandé plusieurs jours. Aucun collaborateur sur place n'avait de visa britannique, l'équipe chargée de la restauration a donc dû se lancer dans une sorte de course de relais et ramener la précieuse machine au siège britannique de l'entreprise. L'entreprise a finalement pu utiliser cette machine pour recréer les autres contrôleurs de domaine.

Avoir recours à une stratégie de reprise d'activité improvisée est trop courant et beaucoup trop risqué. Comme nous avons pu le constater, l'attaque contre VFemail a presque anéanti l'entreprise, qui survit tant bien que mal grâce à certains de ses serveurs de sauvegarde. Ce cas est particulièrement ironique, car l'entreprise a été fondée en 2001 en réponse au virus ILoveYou propagé par e-mail, et que l'un de ses principaux arguments de vente est justement sa capacité à détecter les spams et les logiciels malveillants. Le plus regrettable est que VFemail avait déjà subi plusieurs attaques DDoS débilitantes au fil des ans, mais ne les a, semble-t-il, jamais prises au sérieux.

Si vous subissez une attaque sérieuse et disposez uniquement d'outils natifs, attendez-vous à un processus de restauration de forêt compliqué, propice aux erreurs et interminable.

Outils natifs

Si vous subissez une attaque sérieuse et disposez uniquement d'outils natifs, attendez-vous à un processus de restauration de forêt compliqué, propice aux erreurs et interminable.

La restauration d'une forêt AD est un processus complexe en raison des nombreuses interconnexions nécessaires au fonctionnement des contrôleurs de domaine. Vous devez notamment :

- Reconstruire les services AD
- Nettoyer les métadonnées
- Rétablir les relations d'approbation
- Réinitialiser les comptes
- Redémarrer la réplication

Toutes ces tâches font appel à des procédures complexes qui doivent être exécutées correctement. L'oubli d'une étape ou l'exécution de certaines étapes dans le mauvais ordre peut faire échouer le processus complet. Restaurer une forêt manuellement à l'aide d'outils natifs uniquement, dans une situation stressante comme une panne sérieuse et sous la pression de l'équipe de direction est une tâche peu enviable.

Vous pouvez le constater par vous-même en consultant le Guide de récupération de forêt Active Directory de Microsoft[2]. Ce document fournit un modèle de restauration d'une forêt Active Directory dans le cas où une panne à l'échelle d'une forêt empêche l'ensemble des contrôleurs de domaine de fonctionner correctement. Voici un aperçu détaillé des étapes impliquées dans le cadre d'une restauration de forêt :

1. **Déterminez comment restaurer une forêt :** pour vous préparer à la restauration, Microsoft vous recommande dans un premier temps d'analyser la structure de la forêt actuelle, d'identifier les fonctions de chaque contrôleur de domaine, de choisir les contrôleurs à restaurer pour chaque domaine et de veiller à ce que tous les

2 Le Guide de récupération de forêt Active Directory de Microsoft est disponible sur https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide.

contrôleurs de domaine accessibles en écriture sont mis hors ligne.

Selon les estimations de Microsoft, le temps de lecture de cette étape de préparation est de 12 minutes. La description de chaque sous-étape est d'une page minimum.

2. **Exécutez la restauration initiale (un contrôleur par domaine) :** au niveau global, les étapes consistent ici à restaurer le premier contrôleur accessible en écriture dans chaque domaine, à reconnecter au réseau les contrôleurs restaurés et à ajouter le catalogue global à un contrôleur du domaine root de la forêt.

   L'exécution de la première étape, à savoir la restauration du premier contrôleur, inclut 13 sous-étapes distinctes, dont certaines comportent des procédures à plusieurs étapes documentées séparément par Microsoft. Par exemple, vous devez créer un réseau isolé, saisir les rôles des maîtres d'opérations, augmenter la valeur du pool RID disponible et supprimer les métadonnées AD des contrôleurs de domaine qui n'ont pas été restaurés à partir de la sauvegarde.

3. **Redéploiement des autres contrôleurs de domaine dans la forêt :** une fois la forêt stable, avec un contrôleur par domaine et un catalogue global, vous pouvez commencer le redéploiement des autres contrôleurs de domaine dans la forêt en installant le rôle AD DS.

4. **Effectuez le nettoyage :** lorsque l'ensemble de la forêt est restaurée, vous devez permettre aux utilisateurs de reprendre le travail et aux applications métier de fonctionner. Pour ce faire, vous devez notamment reconfigurer la résolution de noms (DNS) et identifier les modifications apportées entre l'heure de sauvegarde et l'heure du sinistre pour les réappliquer.

Ces étapes sont non seulement complexes et très sensibles aux erreurs humaines, mais chacune d'entre elles exige également beaucoup de temps. De fait, Microsoft reconnaît que « la rapidité de la restauration n'est pas l'objectif premier » de ce guide. Le Forum Aux Questions associé indique que la plupart des étapes de restauration d'une forêt peuvent être effectuées à l'aide d'outils de ligne de commande, ce qui vous permet d'automatiser certaines parties du processus de restauration. Toutefois, Microsoft vous rappelle que vous devez tester minutieusement vos scripts avant de les utiliser dans le cadre d'une restauration réelle. Vous devez également les mettre à jour lorsque vous effectuez des modifications dans votre environnement AD, telles que l'ajout d'un nouveau domaine ou contrôleur de domaine ou encore la mise à niveau d'une nouvelle version d'Active Directory.

Recovery Manager for AD – Disaster Recovery Edition

Heureusement, il existe des outils pour automatiser le processus de restauration de forêt et permettre à votre entreprise de reprendre ses activités de façon plus rapide, simple et sûre. Quest® Recovery Manager for Active Directory – Disaster Recovery Edition vous permet de mettre en œuvre une stratégie complète de sauvegarde et de restauration d'AD en cas de sinistre pour une reprise rapide au niveau des objets et des attributs, de l'annuaire et du système d'exploitation dans l'ensemble de votre forêt AD. En effet, la fonctionnalité de restauration automatique permet de réduire jusqu'à 95 % le délai de restauration en cas de sinistre d'AD au niveau d'un contrôleur de domaine.

Quest On Demand Recovery étend au Cloud la sauvegarde et la restauration AD au niveau des objets et des attributs pour protéger non seulement vos environnements sur site, mais également vos déploiements hybrides. On Demand Recovery vous permet de sauvegarder et de restaurer rapidement et en toute sécurité un environnement Azure AD ou Office 365, de synchroniser des objets ou objets Cloud avec Azure AD Connect, d'exécuter des rapports de comparaison entre sauvegardes de production et en temps réel, et de réaliser des restaurations coordonnées dans vos environnements AD local et Azure AD.

CONCLUSION

Le nombre d'attaques destructrices est en hausse et les conséquences peuvent être catastrophiques. Toute entreprise est vulnérable, qu'elle soit la cible directe ou seulement une victime collatérale. Suite à l'attaque dévastatrice contre VFemail, son PDG et fondateur Rick Romero a twitté « Je n'aurais jamais pensé que quelqu'un se soucierait de mon travail au point de vouloir le détruire complètement ». Ne faites pas la même erreur.

Limitez les risques en mettant en place des bonnes pratiques de sécurité pour bloquer les attaques, limiter leur portée et accélérer la détection et la réaction. Toutefois, les experts de la sécurité et les attaques en conditions réelles indiquent clairement la nécessité d'une stratégie complète de reprise d'activité. Pour en savoir plus sur Recovery Manager for AD – Disaster Recovery Edition et On Demand Recovery, rendez-vous sur quest.com/products/recovery-manager-for-active-directory-disaster-recovery-edition et quest.com/products/on-demand-recovery.

Mettez en place une stratégie complète de sauvegarde et de restauration dans l'ensemble de votre environnement hybride avec Quest Recovery Manager for AD et On Demand Recovery.

PROFIL DE QUEST

Quest fournit des solutions logicielles adaptées au monde de l'informatique d'entreprise en rapide évolution. Nous simplifions les défis associés à l'explosion des données, à l'expansion dans le Cloud, aux datacenters hybrides, aux menaces de sécurité et aux exigences de conformité. Nous fournissons des solutions à 130 000 entreprises dans 100 pays, dont 95 % des entreprises du classement Fortune 500 et 90 % des entreprises du classement Global 1000. Depuis 1987, nous développons une gamme de solutions qui couvre désormais la gestion des bases de données, la protection des données, la gestion des accès et des identités, la gestion des plateformes Microsoft et la gestion unifiée des terminaux. Avec Quest, les entreprises consacrent moins de temps à la gestion informatique et plus de temps à l'innovation. Pour en savoir plus, consultez le site www.quest.com.

© 2019 Quest Software Inc. TOUS DROITS RÉSERVÉS.

Ce guide contient des informations propriétaires protégées par des droits d'auteur. Les logiciels présentés dans ce guide sont concédés sous licence logicielle ou dans le cadre d'un accord de confidentialité. Ces logiciels ne peuvent être utilisés ou copiés que conformément aux dispositions de l'accord applicable. Toute reproduction ou transmission de ce guide sous quelque forme ou par quelque moyen que ce soit (électronique ou mécanique, notamment par photocopie ou par enregistrement), à des fins autres que l'usage personnel par l'acheteur, est interdite sans l'autorisation écrite préalable de Quest Software Inc.

Les informations fournies dans ce document sont liées aux produits Quest Software. Aucune licence de droit de propriété intellectuelle, expresse ou implicite, par préclusion ou autre, n'est accordée par le présent document ou en relation avec la vente de produits Quest Software. SAUF STIPULATION EXPRESSE DANS LES CONDITIONS GÉNÉRALES MENTIONNÉES DANS LE CONTRAT DE LICENCE DE CE PRODUIT, QUEST DÉCLINE TOUTE RESPONSABILITÉ QUELLE QU'ELLE SOIT ET N'ACCORDE AUCUNE GARANTIE EXPRESSE, IMPLICITE OU LÉGALE QUANT À SES PRODUITS, NOTAMMENT, MAIS SANS S'Y LIMITER, LA GARANTIE IMPLICITE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET D'ABSENCE DE CONTREFAÇON. LA SOCIÉTÉ QUEST SOFTWARE NE PEUT EN AUCUN CAS ÊTRE TENUE RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, CONSÉCUTIFS, PUNITIFS, SPÉCIAUX OU FORTUITS (NOTAMMENT, MAIS SANS S'Y LIMITER, CEUX DÉCOULANT D'UNE PERTE DE BÉNÉFICES, D'UNE INTERRUPTION D'ACTIVITÉ OU D'UNE PERTE D'INFORMATIONS) ATTRIBUABLES À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISER LE PRÉSENT DOCUMENT, MÊME SI QUEST SOFTWARE A ÉTÉ AVERTIE DE L'ÉVENTUALITÉ DE TELS DOMMAGES. Quest Software ne se soumet à aucune déclaration ou garantie quant à l'exactitude ou l'exhaustivité du contenu du présent document et se réserve le droit de modifier les spécifications et les descriptions de produits à tout moment et sans préavis. Quest Software ne saurait s'engager à actualiser les informations contenues dans le présent document.

Brevets

Chez Quest Software, nous sommes fiers de notre technologie avancée. Des brevets et des demandes de brevets peuvent s'appliquer à ce produit. Pour obtenir des informations sur les brevets actuellement applicables à ce produit, visitez notre site Web à l'adresse www.quest.com/legal.

Marques

Quest et le logo Quest sont des marques et des marques déposées de Quest Software, Inc. Pour obtenir la liste complète des produits Quest, rendez-vous sur le site www.quest.com/legal/trademark-information.aspx. Toutes les autres marques commerciales sont la propriété de leurs détenteurs respectifs.

En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :
www.quest.com/fr-fr/company/contact-us.aspx