Six vecteurs d'attaque critiques à surveiller dans le datacenter

Les datacenters et la mine d'informations qu'ils renferment constituent une cible particulièrement alléchante pour les cybercriminels. Mais sauf à avoir de la chance et à tomber sur une vulnérabilité exploitable via Internet, le piratage direct d'un datacenter demande beaucoup d'efforts et de planification. C'est pourquoi les cyberattaques contre les datacenters tendent à reposer sur un mode opératoire lent, mature et persistant, suffisamment discret pour passer sous les radars des équipes de sécurité. D'après notre expérience, voici les six vecteurs et techniques d'attaque les plus critiques utilisés par les cybercriminels sophistiqués à l'encontre des datacenters.

1/ Usurpation des comptes administrateur

Dotés du plus haut niveau d'accès au datacenter, les administrateurs sont tout naturellement la cible privilégiée des cybercriminels. Les protocoles administratifs fournissent aux attaquants des portes d'accès dérobées au datacenter. Ils n'ont ainsi pas besoin d'exploiter directement la vulnérabilité d'une application. Et grâce à des outils d'administration standard tels que SSH, Telnet ou RDP, leur activité se fond facilement dans le trafic d'administration normal.

2/ Combler les failles en matière d'authentification locale

Outre les méthodes d'accès standard employées par les administrateurs, de nombreux datacenters ont recours à des options d'authentification locale utilisables en cas d'urgence pour accéder aux hôtes et aux charges de travail qu'ils gèrent. Ces options ne sont toutefois pas journalisées, et les mêmes identifiants de connexion sont souvent partagés entre les hôtes et les charges de travail pour des raisons de simplicité. Lorsque des cybercriminels s'approprient ces identifiants en piratant le compte d'un administrateur, il leur est possible d'accéder discrètement au datacenter sans craindre de voir leur activité journalisée.

3/ Porte dérobée matérielle pour le contrôle administratif

L'authentification locale est un exemple de porte dérobée utilisable aussi bien par les administrateurs que par les cybercriminels pour accéder à un datacenter. Cette approche peut cependant être étendue au matériel.

Si le datacenter est synonyme de virtualisation, il n'en reste pas moins que les environnements et ressources virtualisés fonctionnent sur un équipement physique. Les disques virtuels dépendent de disques physiques résidant dans des serveurs physiques. De la même manière, les serveurs physiques disposent de leurs propres plans de gestion en service réduit et hors bande. A leur tour les plans de gestion possèdent leurs propres protocoles de gestion, alimentation, processeurs et mémoire, qui permettent aux administrateurs de monter des disques et de ré imager les serveurs, même lorsque le serveur principal est hors tension.

Ces opérations sont souvent réalisées à l'aide de protocoles tels que l'interface de gestion intelligente de matériel (ou IPMI, Intelligent Platform Management Interface). Bien que de nombreux fournisseurs de matériel informatique aient développé leur propre version de l'IPMI, comme l'iDRAC pour Dell ou l'iLO (Integrated Lights-Out) pour HPE, elles sont toutes basées sur la technologie IPMI

et remplissent les mêmes fonctions.

Les mises à jour et correctifs de l'IPMI et des protocoles associés ne sont généralement pas très fréquents, et ce, en dépit de failles de sécurité bien documentées. Autre fait inquiétant : il existe actuellement 92 400* interfaces IPMI d'hôtes exposées à Internet. Les vulnérabilités et la très grande puissance de l'IPMI en font un vecteur d'attaque majeur pour les pirates souhaitant mettre à défaut la sécurité du datacenter.

4/ Les cybercriminels avertis visent bas

Malheureusement, les problèmes matériels au sein du datacenter ne se limitent pas à l'IPMI. Les cybercriminels avertis - y compris les États - ciblent de plus en plus les équipements physiques, comme les serveurs, les routeurs, les commutateurs et même le pare-feu. Ils exécutent des rootkits en dessous du système d'exploitation, ce qui les rend extrêmement difficiles à détecter au moyen de méthodes traditionnelles.

Ces techniques leur permettent d'infecter des dispositifs de confiance, ceux-là mêmes qui sont censés protéger le réseau, puis de mener des attaques plus profondément dans le réseau.

5/ Garder un oeil sur les données

Le but ultime de la plupart des attaques est de dérober des données. Selon leurs besoins et leur niveau de compétences, les cybercriminels emploient différentes méthodes pour extraire clandestinement des données du datacenter. La plus simple consiste en un transfert massif d'informations du datacenter vers Internet ou vers une zone intermédiaire du réseau de campus.

Certains pirates adoptent une approche plus lente et discrète en exfiltrant patiemment des quantités de données moins susceptibles d'être repérées ou d'éveiller les soupçons. L'exfiltration des données peut aussi être camouflée à l'aide de tunnels cachés parmi le trafic normalement autorisé, tel que le trafic HTTP, HTTPS ou DNS.

6/ Combiner contexte physique et virtuel

Les datacenters présentent tous des caractéristiques différentes, qui varient selon les applications mises en oeuvre par l'entreprise et la manière dont les utilisateurs interagissent avec elles. Les datacenters d'entreprise privés sont les plus répandus. Les attaques à leur encontre sont habituellement le prolongement de celles visant l'entreprise à un plus large niveau.

Par exemple, des cybercriminels pourront commencer par compromettre l'ordinateur portable d'un employé via un e?mail de phishing ou des techniques d'ingénierie sociale. En général, ils tenteront ensuite d'établir la persistance au sein du réseau en se propageant de la victime initiale à d'autres hôtes ou appareils. Pour contrôler l'attaque en cours, ils installeront des portes dérobées ou des tunnels cachés leur permettant de communiquer dans les deux sens depuis l'intérieur du réseau. Ils cartographieront petit à petit le réseau interne, repéreront les ressources dignes d'intérêt, et compromettront au passage les appareils et les informations d'identification des utilisateurs.

Les identifiants des administrateurs constituent les informations les plus convoitées par les cybercriminels, car ils leur garantissent une quasi-autonomie au sein du réseau de la victime. Ces identifiants jouent un rôle essentiel dans les attaques contre les datacenters étant donné que les administrateurs sont souvent les seuls à pouvoir accéder à un grand volume de données.

Le point clé à retenir est qu'une attaque en est généralement à un stade avancé au moment où elle atteint un datacenter privé. Le trafic caché de commande et de contrôle, la reconnaissance, le

mouvement latéral, ainsi que la compromission des informations d'identification des utilisateurs et des administrateurs sont autant d'étapes préalables à l'intrusion dans le datacenter.

Conclusion

Alors que la sécurité du datacenter s'est principalement focalisée sur la protection des couches virtualisées et la micro segmentation, les cybercriminels s'en prennent de plus en plus à l'infrastructure physique sur laquelle repose le datacenter. La capacité à identifier les cyberattaques ciblant les datacenters est essentielle. Grâce à des modèles avancés de détection des cybercriminels, qui identifient les attaques cachées, que ce soit contre les applications, les données et les couches de virtualisation du datacenter, ou bien contre l'infrastructure physique sous-jacente, les équipes de sécurité pourront traiter les vulnérabilités critiques dans toutes les couches du datacenter virtualisé, même si les pirates utilisent des services et des protocoles légitimes pour accomplir des actions illégitimes.