LIVRE BLANC

Rompre la chaîne d'attaque des ransomwares avec la suite de produits de sécurité d'entreprise d'Akamai

Table des matières

Comprendre la chaîne d'attaque des ransomwares **4**

Accès initial 5

Protection des serveurs exposés à Internet 5

Blocage des URL d'hameçonnage 5

Réduction de la surface d'attaque des VPN 6

Commande et contrôle **6**

Blocage des serveurs de commande et contrôle (C2) 6

Découverte 7

Identification des analyses réseau 7

Leurres contre la découverte 8

Mouvements latéraux 9

Identification des indicateurs d'hôte suspect 9

Blocage des attaques de LAN 10

Restriction des ports de gestion 10

Exfiltration 11

Blocage des domaines d'exfiltration 11

Défense multicouche 11

Introduction

Mettez en échec les ransomwares à chaque étape de la chaîne d'attaque grâce aux solutions de sécurité d'entreprise d'Akamai

L'une des plus grandes menaces de sécurité auxquelles les entreprises sont confrontées aujourd'hui provient des ransomwares, une forme de logiciel malveillant conçu pour chiffrer les fichiers importants stockés sur un terminal de manière à les rendre inutilisables. Les opérateurs de ransomwares demandent alors une rançon en échange d'une clé de déchiffrement ou d'un logiciel qui permet de restaurer les données d'origine des fichiers. Ces dernières années, les groupes criminels responsables d'attaques par ransomware ont fait évoluer leurs tactiques et ont commencé à exfiltrer les données de leurs victimes pour les conserver et les utiliser comme un levier supplémentaire, en menaçant de les divulguer publiquement ou de les vendre sur le Dark Web.

Pour être en mesure de se protéger contre ce type d'attaque, les personnes responsables des systèmes de défense doivent impérativement comprendre la manière dont les groupes de ransomwares opèrent pour parvenir à leurs fins. Il s'agit précisément de l'objectif de ce livre blanc.

Comprendre la chaîne d'attaque des ransomwares

Les attaques par ransomware sont de nature complexe, et l'intrusion dans le système ne constitue qu'un début. Pour provoquer un maximum de dégâts, le cybercriminel doit également répartir sa charge utile malveillante sur le réseau avant de commencer le chiffrement. Si le chiffrement se limite à un seul ordinateur, les moyens de pression seront insuffisants pour exiger une rançon. Pour que l'attaque par ransomware porte ses fruits, son opérateur doit exécuter plusieurs étapes : découvrir les ressources du réseau, se déplacer par mouvements latéraux, etc. Ces différentes étapes successives sont souvent regroupées sous le terme de « chaîne d'attaque des ransomwares ».

Fort heureusement, chaque étape de cette chaîne ouvre un grand nombre de possibilités de détection et d'atténuation. En configurant votre réseau en amont avec la suite de solutions de sécurité d'entreprise d'Akamai, vous pouvez, d'une part, réduire votre surface d'attaque et, d'autre part, atténuer et limiter les dommages éventuels causés par des ransomwares avant même que vous ne vous rendiez compte que votre réseau a été affecté. Ce livre blanc explique comment utiliser Akamai Guardicore Segmentation, Enterprise Application Access et Secure Internet Access pour détecter et bloquer toute activité de ransomwares à chaque étape de la chaîne d'attaque :

Accès initial

Première phase de l'attaque au cours de laquelle les cybercriminels s'introduisent dans le réseau interne depuis l'extérieur

Découverte

Méthodes de découverte utilisées par les cybercriminels pour identifier les ressources importantes à l'intérieur du réseau

Mouvements latéraux

Étape au cours de laquelle les cybercriminels propagent leur attaque sur le réseau et compromettent des ressources supplémentaires

Commande et contrôle

Il s'agit des différents moyens par lesquels les cybercriminels maintiennent un canal de communication avec le réseau pour envoyer des informations et des commandes aux ressources compromises

Exfiltration

Méthodes d'exfiltration utilisées par les cybercriminels pour exfiltrer de manière secrète des données sensibles volées

Accès initial

Chaque entreprise présente une multitude d'interfaces avec le réseau Internet. Et les hackers essaieront d'abuser de chacune d'entre elles pour s'introduire dans votre réseau. Akamai vous permet de protéger ces interfaces et d'empêcher les intrusions dans votre réseau en toute fluidité.

Protection des serveurs exposés à Internet

> Utilisation des capacités d'analyse des charges utiles de Secure Internet Access pour empêcher toute exploitation des serveurs exposés à Internet

Selon Kaspersky, la méthode la plus courante utilisée par les cybercriminels pour obtenir un accès initial consiste à exploiter des applications Internet, souvent en profitant de vulnérabilités Zero Day sur des systèmes n'ayant pas fait l'objet de correctifs. Des vulnérabilités comme Log4Shell (CVE-2021-44228) et ProxyLogon (CVE-2021-26855) sont aujourd'hui encore exploitées à grande échelle « in the wild » pour s'introduire dans les réseaux et déployer des ransomwares.

Enterprise Threat Protector peut être configuré pour surveiller et analyser l'ensemble du trafic Web entrant vers vos serveurs exposés à Internet de manière à vous permettre d'identifier et de bloquer toute activité malveillante ou anormale.

Blocage des URL d'hameçonnage

> Utilisation des capacités d'inspection des URL d'Enterprise Threat Protector pour détecter et bloquer les tentatives d'hameçonnage

L'hameçonnage est une technique couramment utilisée par les hackers pour s'introduire dans les réseaux. Ils procèdent souvent en envoyant des e-mails qui contiennent des liens vers des pièces jointes malveillantes ou vers de fausses pages de connexion conçues pour voler des informations d'identification. En utilisant le client Enterprise Threat Protector sur vos terminaux, vous pourrez non seulement analyser en temps réel chacune des URL sur lesquelles vos utilisateurs cliquent, mais également identifier et bloquer les liens malveillants ou anormaux.

Réduction de la surface d'attaque des VPN

Utilisation d'Enterprise Application Access pour activer un accès VPN sécurisé et spécifique aux applications, et réduire la surface d'attaque externe

En raison du mode de travail hybride adopté par de nombreuses entreprises aujourd'hui, notamment le télétravail, ces dernières autorisent de plus en plus souvent leurs collaborateurs à se connecter au réseau de l'entreprise via un VPN. Les cybercriminels se sont adaptés à cette évolution et ont commencé à exploiter ces opportunités pour accéder aux réseaux internes. Ils s'attaquent souvent aux ordinateurs personnels des collaborateurs pour compromettre leurs informations d'identification VPN et les utiliser par la suite pour accéder au réseau interne. Il leur arrive également de cibler des serveurs vulnérables pour en récupérer les informations d'identification. En novembre 2022, des hackers ont profité d'une vulnérabilité dans les serveurs VPN Fortinet pour obtenir un accès initial avant de propager des ransomwares sur l'ensemble du réseau.

Enterprise Application Access vous permet de réduire ce risque de manière significative en autorisant un accès à votre réseau en fonction de chaque rôle et de chaque application. Il n'accorde pas aux utilisateurs un accès complet à l'ensemble du réseau comme les VPN traditionnels, mais seulement un accès limité à des applications spécifiques. De cette façon, à supposer qu'un cybercriminel compromette les informations d'identification d'un utilisateur et contourne la protection de l'authentification multifacteur, il n'aura toujours pas accès au réseau interne, mais uniquement à un ensemble limité d'applications.

Commande et contrôle

Blocage des serveurs de commande et contrôle (C2)

Utilisation d'Akamai Secure Internet Access pour bloquer les serveurs de commande et contrôle de programmes malveillants connus

Les logiciels malveillants en général, et les ransomwares en particulier, ont besoin de communiquer avec des serveurs C2 externes pour envoyer des commandes et récupérer des informations à partir des ressources infectées. Grâce à l'analyse des nombreuses données de communication d'Akamai, nous sommes en mesure de surveiller les domaines C2 de ransomwares et de logiciels malveillants et de suivre l'évolution des nouvelles campagnes et de celles en cours. Le client Enterprise Threat Protector nous permet de surveiller l'ensemble de vos communications DNS en temps réel et de bloquer les communications vers les domaines malveillants, ce qui a pour effet d'empêcher le logiciel malveillant de fonctionner correctement et de parvenir à ses fins.

Découverte

Une fois que des hackers se sont introduits dans un réseau, ils tentent d'identifier des ressources supplémentaires pour comprendre la structure du réseau avant de commencer à procéder par mouvements latéraux. Cette opération donne souvent lieu à une communication interne qui peut être détectée par Akamai Guardicore Segmentation.

Identification des analyses réseau

> Utilisation des détecteurs d'Akamai Guardicore Segmentation pour identifier les analyses réseau suspectes

En matière de découverte de réseaux, l'une des méthodes couramment utilisées par les cybercriminels consiste à analyser les ports des réseaux afin d'en identifier les services. À cet égard, on constate que de nombreux groupes de ransomwares utilisent des analyseurs de réseaux Open Source. Dans un récent avis de la CISA concernant le ransomware LockBit 3.0, il est apparu que le groupe utilisait l'utilitaire « SoftPerfect Network Scanner » pour procéder à l'analyse des ports. Autre exemple, celui du groupe de ransomwares Nokoyawa, qui a été observé en train d'analyser des réseaux à la recherche de serveurs SQL dans le but d'accéder aux données sensibles qu'ils contenaient.

Grâce à ses détecteurs intégrés, Akamai Guardicore Segmentation surveille l'ensemble des communications de votre réseau pour en identifier toute analyse et vous en alerter afin de vous permettre d'arrêter la propagation du programme malveillant avant qu'il ne cause de dégâts.

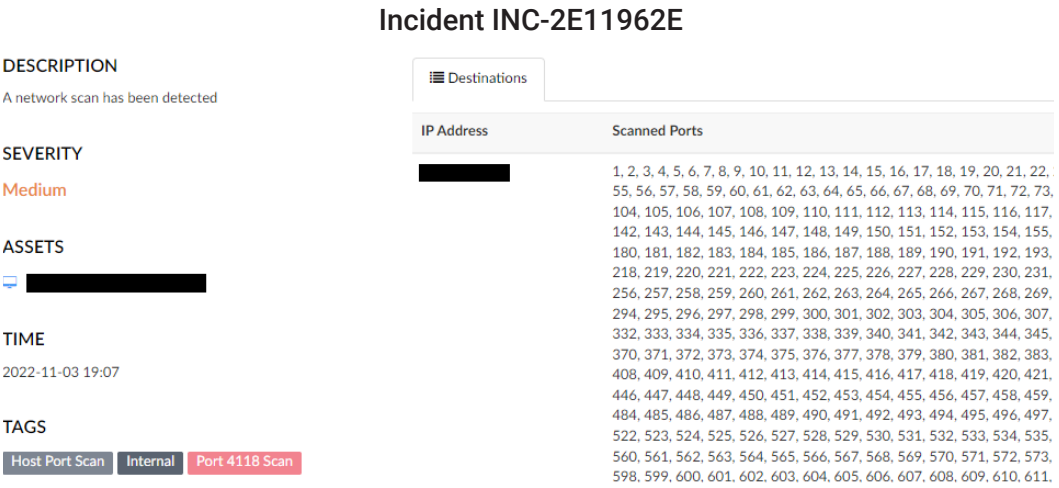
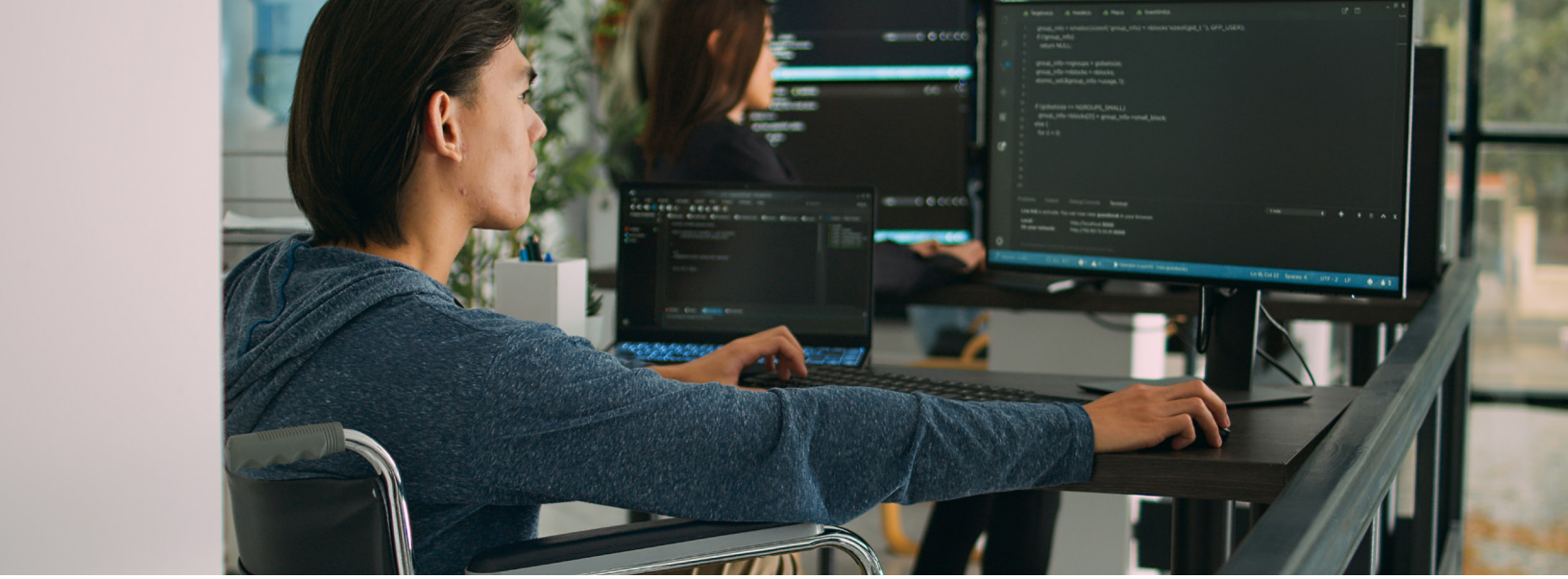


Figure 1 : Incidents d'analyse réseau dans Akamai Guardicore Segmentation



Leurres contre la découverte

Utilisation d'Akamai Guardicore Segmentation pour identifier les tentatives de découverte

Lorsque des cybercriminels s'introduisent dans un réseau, ils n'ont pas de connaissance préalable de sa structure et des différentes ressources qu'il contient. Pour pallier cette difficulté, ils doivent « avancer à tâtons » et essayer de trouver leur chemin de façon manuelle. Akamai Guardicore Segmentation vous permet d'en tirer parti à l'aide de leurres, en attirant les cybercriminels sur des serveurs « honeypot », en surveillant leurs activités et en vous alertant dès que des anomalies sont détectées.

Prenons l'exemple d'un hacker qui s'introduit dans un réseau et tente une attaque par force brute afin d'obtenir les informations d'identification SSH d'un serveur Linux. Akamai Guardicore Segmentation identifiera cette anomalie et dirigera le cybercriminel vers un honeypot généré de manière dynamique. Une fois à l'intérieur du honeypot, toutes les actions du hacker seront enregistrées et une alerte sera générée.

Voici un exemple d'une alerte de ce type :

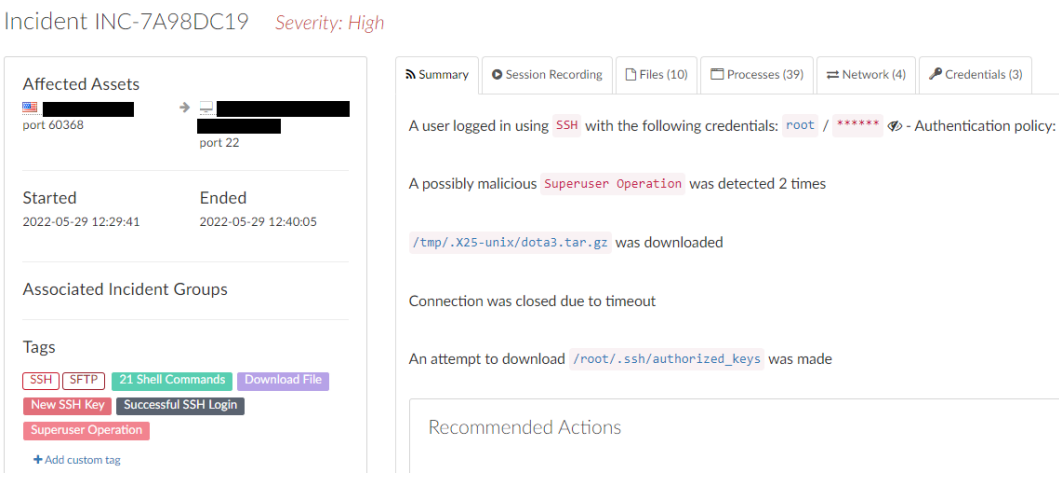


Figure 2 : Incidents de leurre dans Akamai Guardicore Segmentation

Mouvements latéraux

Après s'être introduit dans un réseau et s'être familiarisé avec sa topologie, le cybercriminel cherchera à s'en servir pour continuer son attaque par mouvements latéraux. Les groupes de ransomwares récents pénètrent un réseau, puis se déplacent latéralement pour accéder à autant de ressources que possible et les compromettre en les chiffrant toutes. Les produits de sécurité d'entreprise d'Akamai vous permettent de limiter les possibilités de mouvements latéraux et de minimiser la portée des intrusions.

Identification des indicateurs d'hôte suspect

> Utilisation du module Akamai Guardicore Segmentation Insight pour identifier les indicateurs d'hôte suspect de différentes manières

Les hackers utilisent des outils comme PowerShell pour atteindre divers objectifs, dont l'un consiste à attaquer par mouvements latéraux. Les injecteurs PowerShell sont extrêmement répandus et les cybercriminels les utilisent souvent comme premier élément de code à exécuter sur une ressource compromise. Il a été récemment établi lors de la découverte du ransomware Quantum que c'est exactement la manière dont il procède : exécuter du code PowerShell par l'intermédiaire de Windows Management Instrumentation (WMI).

Grâce au module Insight d'Akamai Guardicore Segmentation, vous pouvez exécuter des requêtes planifiées pour analyser le journal des événements PowerShell sur toutes vos ressources, étiqueter les ressources avec des indicateurs malveillants et les mettre en quarantaine.

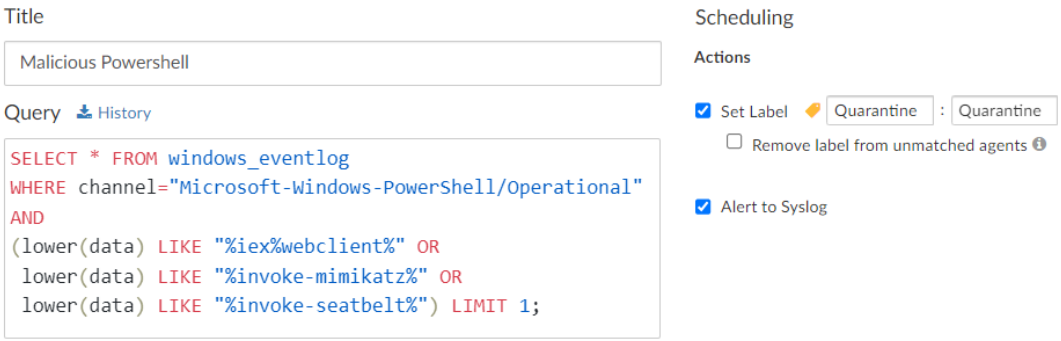


Figure 3 : Création d'une requête Insight planifiée pour détecter un PowerShell malveillant

Malheureusement, PowerShell n'en est qu'un exemple. Insight peut être exploité pour analyser une grande variété d'indicateurs de mouvements latéraux à l'aide de n'importe laquelle des tables d'osquery existantes, par exemple :

- Utilisation de la table File (Fichier) pour détecter les fichiers malveillants basés sur des noms ou des hachages
- Utilisation de la table Startup Items (Éléments de démarrage) pour détecter les entrées d'exécution automatique suspectes sur vos ressources
- Utilisation de la table Yara pour analyser des fichiers sur vos ressources à l'aide des règles YARA et détecter des souches de logiciel malveillant

Blocage des attaques de LAN

Utilisation d'Akamai Guardicore Segmentation pour bloquer et détecter des attaques sur les protocoles réseau locaux

Après s'être introduits dans le réseau à l'aide du « patient zéro », les cybercriminels abusent des vulnérabilités dans les protocoles LAN, comme ARP, pour compromettre d'autres ressources. En utilisant un pare-feu traditionnel, ces attaques peuvent facilement passer sous le radar, car elles sont effectuées dans la couche 2, et ce type de communication n'atteint pas le pare-feu.

L'approche logicielle d'Akamai Guardicore Segmentation vous permet de surveiller et de bloquer tout le trafic entrant ou sortant d'une ressource, y compris le trafic local qui n'atteindrait normalement pas le pare-feu mis en œuvre.

Restriction des ports de gestion

Utilisation d'Akamai Guardicore Segmentation pour créer une stratégie au niveau des processus afin de réduire la surface d'attaque sur les ports sensibles

Une fois à l'intérieur du réseau, les hackers procèdent généralement à une élévation des privilèges sur les ressources compromises dans le but de voler des informations d'identification. Une fois les informations d'identification obtenues, les cybercriminels utilisent souvent des protocoles de gestion tels que RDP, RPC, SMB et WinRM pour exécuter une charge utile de ransomware sur toutes les ressources du réseau. Toutefois, bloquer complètement l'ensemble de ces ports ne représente souvent pas une alternative viable dans la mesure où les administrateurs en ont besoin pour leurs opérations régulières.

Akamai Guardicore Segmentation vous permet d'appliquer une stratégie au niveau des processus de manière à définir les processus que vous autorisez ou non à communiquer sur des ports de gestion sensibles. Prenons l'exemple de l'utilitaire WinRM qui est utilisé par de nombreux programmes d'administration, dont l'outil d'automatisation Ansible. Or, celui-ci est également souvent détourné par des hackers qui utilisent des outils comme Evil-WinRM pour attaquer par mouvements latéraux. Grâce à Akamai Guardicore Segmentation, vous pouvez créer une stratégie qui autorise les connexions WinRM entrantes uniquement à partir du processus Ansible et bloque les autres processus sur le même port :

Section	Source	Destination	Ports/Protocols	Action
Allow	ansible-operator	Windows Any	5985 TCP | UDP	Allow
Block	Any	Windows Any	5985 TCP | UDP	Block

Figure 4 : Exemple de la stratégie d'Akamai Guardicore Segmentation pour limiter les communications WinRM

Exfiltration

Ces dernières années, les cybercriminels ont adapté leurs tactiques d'extorsion et commencé à divulguer des fichiers sensibles de leurs victimes pour les utiliser comme un moyen de pression supplémentaire. Les hackers essaient de se fondre dans le bruit du réseau lorsqu'ils exfiltrent les données d'une entreprise, mais ils peuvent souvent encore être détectés et bloqués au cours de cette étape.

Blocage des domaines d'exfiltration

Utilisation d'Akamai Guardicore Segmentation pour limiter l'accès aux services susceptibles d'être utilisés à des fins d'exfiltration de données

Les cybercriminels utilisent souvent des plateformes publiques pour divulguer des données du réseau, une option très répandue étant le recours à des services d'hébergement public tels que MEGA, Dropbox et Google Drive. La difficulté de la surveillance de ces domaines réside dans le fait qu'ils sont couramment utilisés de façon légitime à l'intérieur du réseau. Par exemple, l'accès au domaine MEGA via un navigateur peut être considéré comme légitime, mais en utilisant l'outil rclone, qui est activement utilisé par plusieurs groupes d'attaque pour exfiltrer des données, il serait considéré comme malveillant.

Grâce à Akamai Guardicore Segmentation, vous pouvez minimiser les risques liés à ces outils en bloquant leurs domaines à partir de tous les terminaux qui n'ont pas besoin d'y accéder, et en autorisant uniquement l'accès via des applications approuvées telles que les navigateurs.

Défense multicouche

Pour parvenir à leur objectif ultime, les cybercriminels doivent attaquer en procédant par étapes successives. Chaque étape donne aux personnes responsables des systèmes de défense une opportunité de détecter l'activité malveillante associée et de la bloquer. En utilisant les différents produits de sécurité d'Akamai, les responsables des systèmes de défense peuvent déployer des mécanismes d'atténuation à chaque étape d'une chaîne d'attaque d'un ransomware, et ce, dans le but de détecter tout comportement anormal et de mettre un terme aux activités malveillantes.

Pour en savoir plus sur Akamai Guardicore Segmentation ou pour demander une démonstration personnalisée du produit, consultez notre site à l'adresse akamai.com/guardicore