VECTRA
SECURITY THAT THINKS

EBOOK

Comment les cybercriminels contournent les signatures de menaces

GESTION AUTOMATISÉE DES MENACES

EFFICACITÉ OPÉRATIONNELLE

NATIF AU CLOUD

ENTREPRISE

Une faille dans le dispositif de cybersécurité

Il existe une faille importante dans le dispositif de cybersécurité, à savoir le décalage entre le moment où un pirate parvient à contourner les systèmes de prévention des intrusions (IPS) au niveau du périmètre réseau et la phase d'éradication, soit lorsqu'une entreprise découvre que des ressources critiques ont été volées ou détruites.

Les cyberpirates bénéficient d'un avantage certain à cet égard. Ils peuvent en effet facilement contourner les signatures, les listes de réputation et autres mécanismes de protection préventive en appliquant des méthodes d'attaque aussi ingénieuses que complexes.

Particulièrement répandue, l'approche traditionnelle de la détection des menaces est par nature réactive, laissant l'initiative aux cybercriminels.

Les signatures, les listes de réputation et les listes noires permettent uniquement la reconnaissance de menaces déjà connues. Autrement dit, il faut nécessairement une première victime — ce que personne ne veut être.

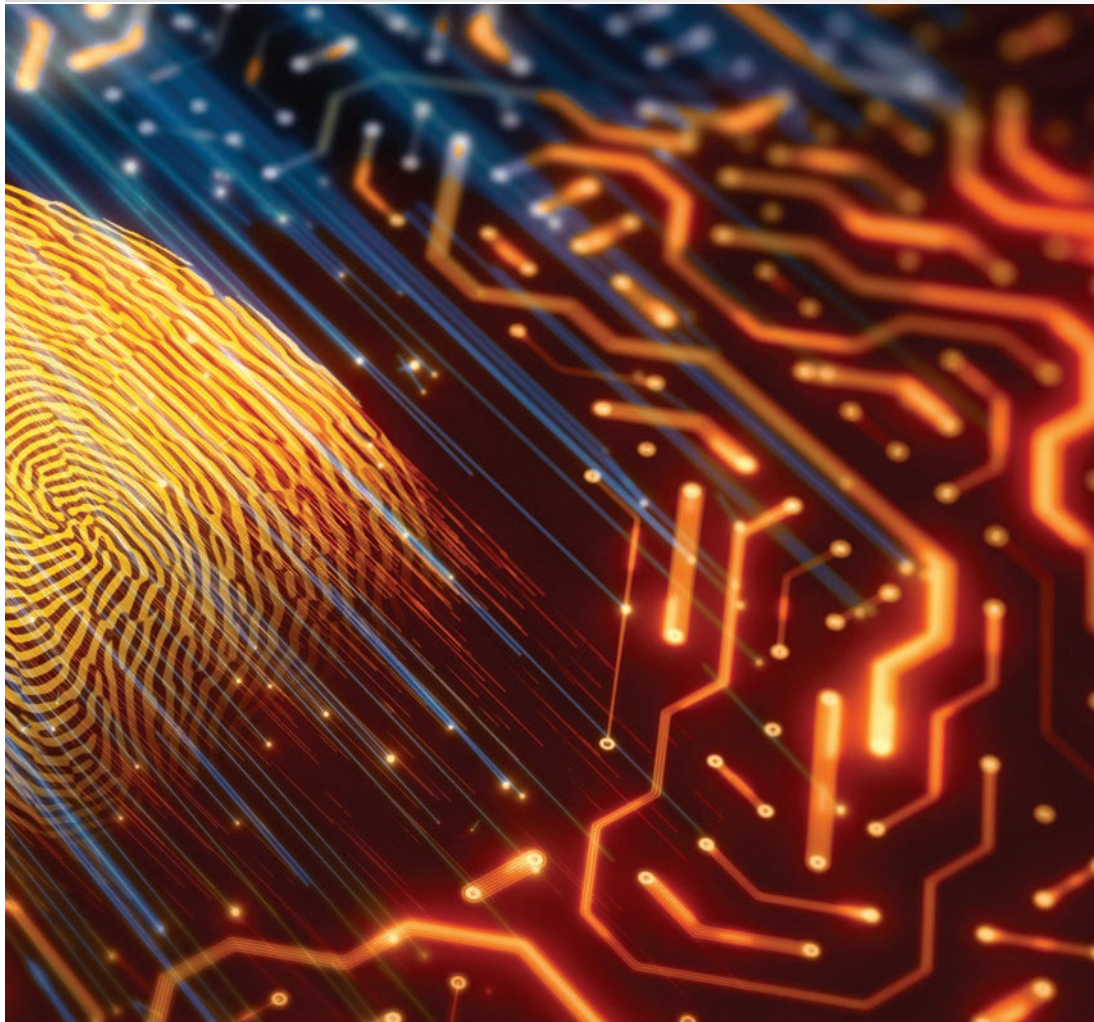
La détection des menaces dépend généralement d'applications de sécurité clés installées sur les terminaux et au niveau des passerelles. Les nouvelles cybermenaces sont interceptées et conservées dans des sandbox virtuelles et de nouvelles signatures sont générées automatiquement. Ce processus prend du temps et les malwares peuvent en profiter pour s'introduire dans les terminaux et réseaux encore vulnérables.

La création de nouvelles signatures est une solution éprouvée. Elle sert d'ailleurs de pierre angulaire aussi bien aux logiciels antivirus qu'aux pare-feux de nouvelle génération, mais aussi aux systèmes de détection et prévention des intrusions (IDS/IPS). Les cyberpirates ont toutefois toujours plusieurs longueurs d'avance et ces solutions peuvent donner un faux sentiment de sécurité.

Bien que les signatures puissent bloquer les menaces connues (chevaux de Troie, rootkits et autres codes malveillants), les cyberattaques les plus dangereuses restent celles qui n'ont encore jamais été détectées et analysées. Sans connaître leur existence, nous n'avons forcément aucune visibilité sur leur comportement et les signatures ne peuvent en aucun cas aider à les intercepter.

70 à 90 %

Entre 70 et 90 % des échantillons de malwares présentent des caractéristiques qui sont propres aux entreprises attaquées.



Des limitations inhérentes

Les signatures peuvent avoir une vraie utilité, notamment pour la détection de menaces de base à grande échelle, comme les communications C&C de botnets, les robots de balayage automatisés ou les analyseurs de vulnérabilités.

S'appuyer uniquement sur les signatures reste une solution limitée, qui laisse de nombreuses zones d'ombre face au déferlement continu d'attaques plus dangereuses les unes que les autres.

Les cyberpirates privilégiant les attaques furtives au contrôle d'un nombre important de systèmes trouvent en permanence de nouvelles méthodes pour contourner les signatures. Malheureusement, ces ingénieux cyberpirates ont tendance à aborder les attaques de manière stratégique et représentent un risque significatif pour les entreprises.

Comprendre quelles sont les zones d'ombre inhérentes aux signatures nécessite également de comprendre leurs faiblesses.

Les signatures n'offrent par exemple aucune protection face aux menaces internes. Elles ne permettront ni d'identifier ni de bloquer les utilisateurs internes malveillants disposant d'un accès légitime et utilisant des outils tout aussi légitimes. Les comportements d'attaque et les écarts par rapport aux activités normales ne peuvent être détectés grâce aux signatures.

D'après le rapport d'enquête *2020 Verizon Data Beach Investigation Report*, les attaques axées sur les identifiants tendent à remplacer les attaques par malware.

Les malwares personnalisés permettent eux aussi de contourner les signatures. La plupart des malwares sont spécifiquement adaptés aux entreprises visées, ce qui veut dire qu'il ne sera pas possible de les détecter à l'aide de signatures. Entre 70 et 90 % des échantillons de malwares présentent des caractéristiques qui sont propres aux entreprises attaquées.

Pour cela, les cyberpirates ne créent pas ces logiciels malveillants de toutes pièces : ils modifient des malwares existants juste assez pour échapper à la vigilance des solutions de sécurité basées sur les signatures. Les signatures de malware s'appuient sur la création de hachages de fichiers dangereux connus. En conséquence, la moindre modification empêche toute correspondance et donc toute détection.

Les cyberpirates n'ont ainsi qu'à ajouter quelques bits à un fichier de malware pour que le hachage ne permette pas de le reconnaître en tant que malware. Ces modifications sont opérées automatiquement, sans aucune intervention humaine. D'importants volumes de tels malwares « personnalisés » sont ainsi générés chaque jour.

Le problème est que même si le code d'un malware est légèrement différent d'un malware connu, son comportement reste identique. Ces modifications, uniquement destinées à contourner la détection basée sur les signatures, sont superficielles.

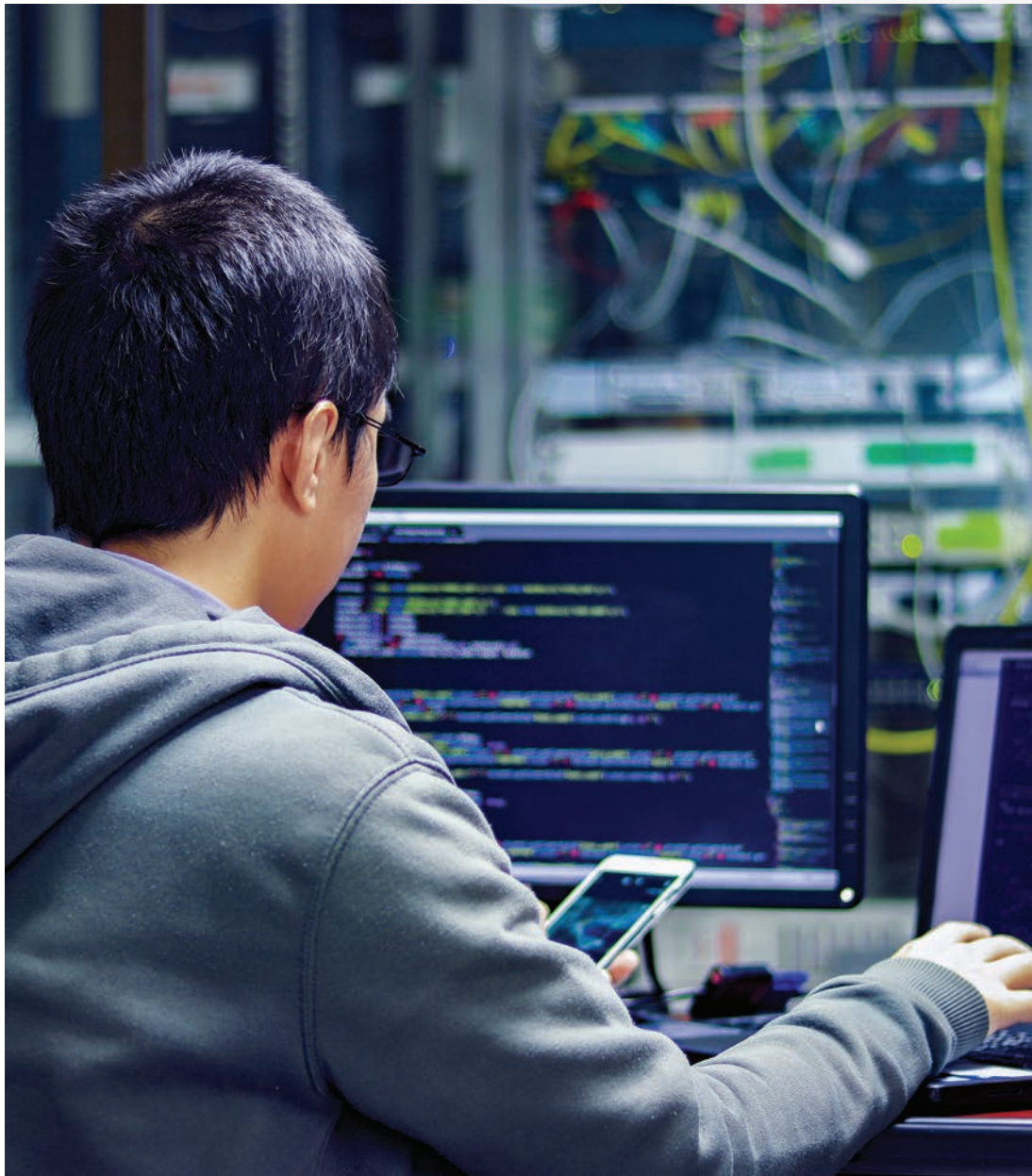
Les signatures ne permettent pas non plus de détecter les attaques jour zéro qui ciblent les vulnérabilités des logiciels ou des systèmes d'exploitation comme Heartbleed ou Duqu 2.0. Ces vulnérabilités sont pratiquement impossibles à détecter par le biais des signatures, car celles-ci permettent uniquement de bloquer les menaces connues.

Surveillance du comportement

Les cyberpirates peuvent modifier des malwares, chercher des vulnérabilités connues et voler des données sur des systèmes sur lesquels ils ont un droit d'accès. Ils ne peuvent toutefois pas modifier leurs comportements d'attaque, consistant à espionner le réseau d'une victime, s'y propager et y voler des données.

Ces comportements peuvent être concrètement observés, offrant aux entreprises une visibilité en temps réel sur les menaces actives sur leurs réseaux. Aujourd'hui, les organisations les plus aguerries complètent leurs systèmes de protection basés sur les signatures avec des solutions automatisées de détection et de résolution des incidents sur le réseau (NDR, Network Detection and Response).

S'appuyant sur la science des données, l'apprentissage automatique et l'analyse comportementale, la gestion automatisée des menaces permet de détecter les comportements malveillants au sein du réseau, quels que soient les mécanismes utilisés par les cyberpirates pour contourner les signatures et que les menaces soient internes ou externes.



En se concentrant sur les actions et modes opératoires spécifiques des cybercriminels, les solutions NDR sont capables d'identifier chaque phase d'une attaque active (C&C, monétisation de botnets, reconnaissance interne, déplacement latéral et exfiltration de données), et ce, sans dépendre de signatures ou de listes de réputation.

Les solutions de détection des menaces basées sur le comportement peuvent également identifier les opérations de reconnaissance interne, les analyses de ports, l'activité de clients Kerberos et la propagation de malwares sur le réseau. Les modèles fondés sur la science des données permettent une neutralisation efficace des algorithmes de génération de domaines utilisés par les cyberpirates pour créer une réserve inépuisable d'URL pour leurs menaces.

Pour plus d'informations, veuillez contacter l'un de nos représentants à l'adresse sales-inquiries@vectra.ai.

Les cybercriminels cherchent en permanence de nouvelles techniques pour masquer leurs communications d'attaque, et l'une des plus efficaces (connaissant aussi la plus forte croissance) est de les dissimuler au sein d'un protocole légitime.

Un cyberpirate peut par exemple utiliser des communications HTTP par nature inoffensives pour y cacher des messages codés dans les champs de texte, les en-têtes ou autres paramètres de la session. En transitant clandestinement sous le couvert de protocoles autorisés, les cyberpirates peuvent communiquer sans craindre d'être détectés.

Les modèles de détection inhérents à la gestion automatisée des menaces peuvent toutefois mettre au jour ces tunnels cachés en analysant la chronologie, le volume et le séquencement du trafic, et en mémorisant ces informations.

Garder une longueur d'avance sur les menaces ciblant le réseau

Les cyberpirates les plus agiles peuvent facilement créer et dissimuler des exploits par un nombre incalculable de méthodes. Les carences inhérentes aux signatures doivent ainsi être comblées par des modèles de gestion automatisée des menaces qui intègrent en permanence de nouveaux comportements d'attaque et s'adaptent aux modifications du réseau.

Il est désormais temps d'abandonner les protections basées uniquement sur les signatures et de prendre une longueur d'avance sur les cyberpirates en détectant et en analysant automatiquement les actions et modes opératoires qui sous-tendent une attaque, pour neutraliser les menaces avant qu'il ne soit trop tard.

E-mail : info_france@vectra.ai / info_dach@vectra.ai vectra.ai/fr