LA MENACE **APT** EN EUROPE

COMMENT S'AD**APT**ER ?

DONNÉES RECUEILLIES AUPRÈS DE 300 DÉCIDEURS INFORMATIQUES EUROPÉENS EN FRANCE, AU ROYAUME-UNI ET EN ALLEMAGNE.

MAI 2023

PRESENTÉ PAR
GATEWATCHER

ENQUÊTE MENÉE PAR
VANSON BOURNE

GATEWATCHER

CONTENU_

01

INTRODUCTION_

Force est de constater que les menaces cyber évoluent pour optimiser les profits qui y sont associés. Pour survivre dans cet environnement numérique, les cybercriminels ont continuellement su s'adapter.

Dans le domaine de la cybersécurité, l'évolution de ces acteurs est souvent très rapide et les équipes opérationnelles chargées de la sécurité informatique sont bien trop souvent contraintes de rattraper leur retard en la matière. Le perfectionnement des menaces persistantes avancées (APT) est une illustration parfaite de cette évolution.

Les définitions commerciales des menaces APT sont multiples, à l'instar des nombreuses technologies déployées par les éditeurs de logiciels pour faire face à ce type d'acteurs. Le National Institute of Standards and Technology (NIST) en offre la définition la plus complète en décrivant les APT comme étant :

«Un adversaire qui possède des niveaux d'expertise sophistiqués et des ressources importantes lui permettant de créer des opportunités pour parvenir à ses fins par le biais de plusieurs vecteurs d'attaque (qu'il s'agisse d'une attaque cyber, physique ou d'une ruse).

Les objectifs de cet adversaire sont généralement l'implantation et le déploiement de leurs positions au sein du système informatique des organisations ciblées afin d'exfiltrer des informations, de saper ou d'entraver des aspects essentiels d'une mission, d'un programme ou d'une organisation, ou de se positionner pour atteindre ces objectifs ultérieurement.»

La menace persistante avancée:

- poursuit ses objectifs de manière récurrente sur une période longue;
- s'adapte aux efforts des agents de défense pour leur résister
- est déterminée à maintenir le niveau d'interaction nécessaire à la réalisation de ses objectifs [1]

En d'autres termes, l**es menaces persistantes avancées se traduisent par des attaques intelligentes et furtives qui sont patientes, répétées, intelligentes, et ciblées.** Elles se situent ainsi aux antipodes du piratage d'un compte Twitter ou d'une tentative d'escroquerie numérique visant à s'emparer des données d'un utilisateur.

Si les menaces persistantes avancées ont la caractéristique d'être ciblées, leur phase initiale est généralement massive, leur permettant de masquer leur véritable cible. Pour citer quelques exemples, on peut ainsi évoquer l'attaque par un ransomware d'envergure qui a visé les hyperviseurs VMware ESXi[2] non protégés dans le monde entier en février 2023, compromettant plus de 3 200 serveurs en Europe, aux États-Unis ou encore au Canada. En janvier 2023, une application Microsoft mal configurée a permis à tout utilisateur de se connecter et de modifier les résultats de recherche sur Bing.com, menaçant les comptes de nombreux utilisateurs d' Office 365. En mars 2023, des versions légitimes de la 3CX DesktopApp[3] ont été compromises et exploitées par des hackers pour porter atteinte à plus de 600 000 entreprises et organisations utilisant l'application, y compris le National Health Service (NHS) au Royaume-Uni.

Ainsi, les menaces persistantes avancées surviennent généralement dans le contexte du cyber espionnage, de l'hacktivisme coordonné, de la cybercriminalité financière ou dans le cadre d'une tentative organisée visant à détruire les capacités numériques d'une organisation donnée. Mais, **à l'image de toutes les entreprises criminelles, les menaces persistantes avancées se sont aussi propagées dans le monde des affaires.**

Source

[1] *NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, Mars 2011*

[2] *Bulletin d'alerte du CERTFR-2023-ALE-015*

[3] *Bulletin d'alerte du CERTFR-2023-ALE-003*

02

LA MONTÉE EN PUISSANCE DES MENACES PERSISTANTES AVANCÉES_

Ces dernières années, de nombreuses études et organisations ont mis en évidence l'augmentation des menaces APT à l'égard de certaines structures. On peut ainsi citer la pandémie du COVID-19 qui a suscité un intérêt supplémentaire de la part des menaces de type APT pour les services de santé et les services dits essentiels, tel que constaté par le CISA et le NCSC[4]. En outre, le nombre des attaques issues des APT visant les institutions, organismes et agences de l'UE a augmenté de 60 % en 2020 par rapport à 2019[5]. Les perspectives de progression du marché de la protection contre les APT est par ailleurs un signe révélateur de l'évolution des menaces persistantes avancées : il devrait dépasser les 15 milliards de dollars américains d'ici 2026[6].

Cette étude a été lancée à la lueur de ces évolutions et à la suite des tendances observées par Gatewatcher dans le cadre de sa veille active des risques cyber via sa solution de Cyber Threat Intelligence. L'objectif étant d'évaluer le niveau de préparation des entreprises face à ces menaces, à l'échelle européenne.

L'ensemble des secteurs étudiés dans cette enquête ne sont indéniablement pas épargnés par les menaces persistantes avancées. En effet, au Royaume-Uni, en France et en Allemagne, 93% des entreprises interrogées ont actuellement entrepris des efforts en faveur de la détection et de l'identification des menaces APT. Ces chiffres sont stables dans l'ensemble au sein de chaque pays et quelle que soit la taille de l'entreprise.

La lutte contre les menaces persistantes avancées semble constituer un défi interne, puisqu'un peu moins d'une entreprise sur cinq (19 %) externalise actuellement sa protection face à cette typologie de menaces auprès d'un Fournisseur de services (MSP) ou d'un Fournisseur de services de sécurité (MSSP). Ce chiffre est légèrement plus élevé en France, où 23% des entreprises font appel à un partenaire pour se protéger des menaces persistantes avancées.

Sources

[4] Bulletin d'alerte du DHS, du CISA et du NCSC, APT Groups Target Healthcare and Essential Services, 25 janvier 2022.

[5] CERT-EU, Threat Landscape Report, Juin 2021

[6] Statista, Mars 2022

LAQUELLE DE CES AFFIRMATIONS RELATIVES AUX MENACES PERSISTANTES AVANCÉES (APT) S'APPLIQUE LE MIEUX À VOTRE ORGANISATION ?

25%

Nous cherchons à détecter et à identifier les menaces persistantes avancées mais nous rencontrons des difficultés pour distinguer la méthode et les vecteurs d'entrée.

21%

Nous cherchons à détecter et à identifier les menaces persistantes avancées mais nous rencontrons des difficultés pour répondre aux besoins technologiques nécessaires pour y faire face.

15%

Nous cherchons à détecter et à identifier les menaces persistantes avancées mais faisons face à des difficultés pour remédier à l'attaque.

03

APT : LE MANQUE DE VISIBILITÉ COMME FACTEUR DE RISQUE_

Interrogés sur les facteurs de risques pouvant favoriser les APT, près de la moitié des décideurs informatiques (47%) identifient le manque de visibilité sur l'ensemble des menaces dissimulées au cœur du réseau informatique comme étant un risque majeur pour leur entreprise, tandis que 40% des personnes interrogées estiment que leurs équipes de sécurité ne disposent pas des compétences nécessaires pour faire face aux risques.

En outre, 35% mentionnent les lacunes dans la sécurité de la chaîne d'approvisionnement, en particulier au niveau des endpoints, comme pouvant compromettre la sécurité de leur organisation et près d'un tiers (30%) citent les faux positifs et la lassitude face aux alertes qui s'ensuivent comme un facteur compromettant la sécurité de leur organisation.

Signe de l'importance de sécuriser sa chaîne d'approvisionnement et de la prise de conscience pour cette dernière, 29% des sondés considèrent par ailleurs les prestataires connectés aux systèmes d'information d'une organisation comme un facteur de risque face aux menaces APT.

Si l'identification des APT constitue aujourd'hui un défi majeur pour 25% des acteurs européens interrogés, ces derniers rencontrent toutefois des difficultés à discerner la méthode et les vecteurs d'entrée. 21% des décideurs – tous pays confondus – peinent à répondre aux besoins technologiques (un défi particulièrement notable en Allemagne, où ce pourcentage s'élève à 30%). Sur l'ensemble des pays étudiés, 15% des acteurs interrogés ont par ailleurs des difficultés à remédier aux attaques de type APT.

Un peu moins d'une entreprise sur cinq externalise actuellement sa protection face à cette typologie de menaces auprès d'un Fournisseur de services (MSP) ou d'un Fournisseur de services de sécurité (MSSP). Cette protection semble également susciter une grande vigilance, puisque 28% des acteurs sondés estiment qu'une mauvaise communication de la part d'un prestataire de services peut compromettre la sécurité de leur organisation.

04

TOP 6 DES DÉFIS DE SÉCURITÉ EN EUROPE_

L'enquête identifie six défis en matière de cybersécurité classés par niveau de risque. L'inquiétude la plus forte exprimée par les décideurs européens sondés – 54 % – concerne la menace cybercriminelle que représentent les acteurs indépendants qui infiltrent les réseaux informatiques à des fins malveillantes ou militantes, tels que les « black hats » indépendants, les hacktivistes ou les « script kiddies ».

Cette inquiétude est suivie de près par la menace de perte de données – identifiée par 51 % des sondés sur l'ensemble des trois pays – puis par les rançongiciels (47 %), les menaces cybercriminelles posées aux entreprises par les États-nations (38 %) et l'espionnage industriel (34 %). Les menaces internes, causées par les employés mécontents et insatisfaits arrivent en dernière position, selon 28 % des sondés.

Au-delà de ces données, on constate que l'échelle du risque n'est pas perçue de la même manière en France, en Allemagne et au Royaume-Uni. En France, la perte de données arrive en tête des préoccupations (65 %), tandis que la menace générée par les hackers indépendants se place en première position en Allemagne et au Royaume-Uni (respectivement 62 % et 52 %). Les rançongiciels représentent également la seconde préoccupation des décideurs informatiques allemands (52 %), contre 47 % et 43 % en France et au Royaume-Uni.

LAQUELLE DE CES CATÉGORIES CORRESPOND AUX DÉFIS ENCOURUS PAR VOTRE ORGANISATION EN MATIÈRE DE CYBERSÉCURITÉ ?

54%

Les acteurs individuels qui infiltrent les réseaux informatiques à des fins malveillantes ou militantes

51%

La perte de données

38%

Les menaces cybercriminelles posées aux entreprises par les États-nations

47%

Les rançongiciels

34%

L'espionnage industriel

28%

Les menaces internes causées par les employés mécontents et insatisfaits

01%

Ne sait pas

55% DES SONDÉS CLASSENT LES SOLUTIONS DE DÉTECTION ET DE RÉPONSE - **NDR** - PARMI LES PRINCIPALES TECHNOLOGIES UTILISÉES PAR LEUR ORGANISATION POUR SE DÉFENDRE CONTRE LES MENACES PERSISTANTES AVANCÉES.

05

SOLUTIONS & TECHNOLOGIES PLÉBISCITÉES PAR LES ENTREPRISES EUROPÉENNES_

Parmi les technologies déployées pour lutter contre les APT, les solutions de détection et de réponse des points d'accès (EDR), arrivent en tête (62%), suivies par les pare-feux (57%).

Les systèmes de gestion des événements et des informations de sécurité (SIEM) et les solutions de détection et de réponse (NDR - Network Detection and Response) représentent respectivement 56% et 55% des solutions utilisées. La technologie de détection et de réponse étendues (XDR) vient clore ce classement des cinq technologies les plus utilisées dans la lutte contre les menaces persistantes avancées (38%).

Les solutions NDR continuent de retenir l'intérêt de nombreuses entreprises confrontées aux menaces APT: le marché du NDR devrait atteindre environ 5,4 milliards de dollars d'ici 2028, avec un taux de croissance annuel composé (TCAC) estimé à 13,7% entre 2022 et 2028. Cela s'explique non seulement par la sensibilisation accrue à cette technologie, mais également par le fait que cet instrument fait partie intégrante des 3 piliers de la cybersécurité tels que définis par Gartner : l'EDR, le SIEM et le NDR.

Cette association de technologies constitue une réponse bienvenue aux menaces persistantes avancées. Interrogés sur les facteurs de risques pouvant favoriser les APT, près de la moitié des décideurs informatiques (47%) identifient le manque de visibilité sur l'ensemble des menaces dissimulées au cœur du réseau informatique comme étant un risque majeur pour leur entreprise. C'est là qu' interviennent les solutions NDR, qui permettent d'identifier spécifiquement les comportements suspects et menaces dissimulées au cœur du réseau. Cet enjeu technologique se double de la question urgente et permanente que constitue le manque de compétences au sein des équipes de sécurité informatique : un défi pour 40% des décideurs informatiques interrogés.

Dans ce contexte, l'intérêt accru suscité par le NDR et l'attention portée par les entreprises aux solutions EDR paraissent évidents, surtout lorsque ces technologies sont associées à l'automatisation offerte par certains pare-feux. Grâce à des performances d'analyse rapide, une haute visibilité sur les comportements suspects dissimulés au cœur du réseau, une réponse intelligente et une détection augmentée des menaces, le NDR permet de protéger efficacement les organisations contre les intrusions.

Sources

[6] *Industry Research, Global "Network Detection and Response (NDR) Market" Research Report 2022-2028, Juin 2022.*

LEQUEL DE CES FACTEURS COMPROMET LA POSTURE DE VOTRE ORGANISATION EN MATIÈRE DE CYBERSÉCURITÉ ?

47%

LE MANQUE DE VISIBILITÉ SUR L'ENSEMBLE DES MENACES DISSIMULÉES AU CŒUR DU RÉSEAU INFORMATIQUE

40%

LE DÉFICIT DE COMPÉTENCES NÉCESSAIRES AU SEIN DES ÉQUIPES DE SÉCURITÉ INFORMATIQUE

35%

LES LACUNES DANS LA SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT, EN PARTICULIER AU NIVEAU DES ENDPOINTS

06

LES APT… LA NOUVELLE NORMALITÉ EN MATIÈRE DE CYBERSÉCURITÉ_

L'identification des menaces APT constitue le principal défi posé par ces dernières – et que les organisations cherchent à relever. Or il est par nature difficile de détecter les menaces persistantes avancées, car une partie de leur mode opératoire consiste à rester aussi dissimulées que possible et de façon prolongée. C'est fort de ce constat que la présente enquête vise à identifier les plus grandes menaces APT telles qu' elles sont perçues par les décideurs informatiques dans les trois pays étudiés. L'étude inclut des catégories représentatives des méthodes de ces attaques et les plus susceptibles d'être déployées par les cybercriminels.

Cette étude montre que les entreprises continuent de s'appuyer fortement sur la protection des terminaux endpoints via les technologies EDR, tout en reconnaissant que la visibilité de l'ensemble du réseau informatique et la protection de ce dernier sont désormais nécessaires pour lutter contre les menaces APT. Elle révèle par ailleurs la prise de conscience technologique encourageante et graduelle des organisations en faveur des technologies réseaux – tel que le NDR – qui s'imposeront, à l'avenir, comme solution et levier privilégiés pour protéger la cybersécurité des entreprises.

À juste titre, car le développement et l'évolution des menaces persistantes avancées ont favorisé un écosystème qui rétribue des criminels capables de faire preuve de patience, de perspicacité et de logique.

Ainsi, pour faire face aux menaces APT, le secteur de la cybersécurité doit apporter une réponse qui, conjuguant une visibilité augmentée, une présence accrue sur l'ensemble du réseau et une démarche plus prudente et approfondie, permet la détection précoce des premiers signes d'attaques d'envergure et prolongées dans le temps.

Il est donc temps d'évoluer et d'adapter notre approche à ce nouvel environnement des menaces et de considérer les menaces APT comme la nouvelle normalité en matière de cybersécurité.

07

METHODOLOGIE _

La présente étude s'appuie sur une enquête menée par le cabinet britannique Vanson Bourne entre janvier et février 2023 auprès de 300 décideurs informatiques au Royaume-Uni, en France et en Allemagne. Les 300 personnes interrogées sont réparties dans les secteurs suivants : Informatique, Technologie et télécommunications, Services financiers, Commerce de détail, Distribution et Transport, Industrie manufacturière, Services aux entreprises et services professionnels, Autres secteurs commerciaux. Parmi les personnes interrogées, 204 personnes sont issues d'entreprises de 3 000 salariés ou plus ; les 96 décideurs informatiques restants font partie d'entreprises comptant 1 000 à 3 000 salariés.

A PROPOS DE CETTE ENQUÊTE

PAYS DES SONDÉS

ROYAUME-UNI
100

FRANCE
100

ALLEMAGNE
100

RÉPARTITION DES SONDÉS SELON LA TAILLE DE L'ENTREPRISE :

TOTAL
300

3 000 EMPLOYÉS OU PLUS
204

1 000 À 2 999 SALARIÉS
96

SECTEURS DES SONDÉS

300 DÉCIDEURS IT RÉPARTIS DANS LES SECTEURS SUIVANTS :

INFORMATIQUE, TECHNOLOGIE ET TÉLÉCOMMUNICATIONS
72

SERVICES FINANCIERS
67

COMMERCE DE DÉTAIL, DISTRIBUTION ET TRANSPORT
48

INDUSTRIE MANUFACTURIÈRE
41

SERVICES AUX ENTREPRISES ET SERVICES PROFESSIONNELS
17

AUTRES SECTEURS COMMERCIAUX
55

LA MENACE **APT** EN EUROPE

GATEWATCHER X VANSON BOURNE

08

À PROPOS_

GATEWATCHER

Leader technologique dans la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux critiques des grandes entreprises et des institutions publiques. Nos solutions associent l'IA à des techniques d'analyse dynamiques pour offrir une vision à 360° et en temps réel des cybermenaces sur l'ensemble du réseau, dans le cloud et on premise.

www.gatewatcher.com

VANSON BOURNE

Vanson Bourne est un cabinet d'études indépendant spécialisé dans le secteur de la technologie. La réputation de ce cabinet et la crédibilité de ses analyses se fondent sur des principes rigoureux utilisés dans le cadre de ses études de marché et sur sa capacité à interroger des décideurs dans des fonctions IT et métier, dans tous les secteurs d'activité et sur les principaux marchés.

www.vansonbourne.com