Guide de l'acheteur

Comprendre le Threat Intelligence

Un guide complet pour votre défense contre les menaces

Jakub FILIP

Digital Security
Progress. Protected.

Digital Security
Progress. Protected.

Table des matières

Introduction

Il est essentiel que les organisations restent informées et bien équipées pour lutter efficacement contre les cybermenaces. L'adoption du Threat Intelligence est l'un des moyens d'y parvenir.

Le guide que vous allez lire a été spécialement conçu pour répondre à trois objectifs essentiels :

- **Tout d'abord, il vous permet de bien comprendre ce qu'implique réellement le Threat Intelligence.**
- **Deuxièmement, il précise le fonctionnement du marché actuel du Threat Intelligence afin de vous aider à comprendre le sujet dans sa globalité.**
- **Troisièmement, il vous aide à répondre à la question fondamentale de savoir si votre organisation a besoin du Threat Intelligence et ce qu'il faut rechercher si c'est le cas.**

Ce guide souligne également l'importance de prendre en compte le contexte et les besoins plus étendus de votre organisation lors de l'évaluation de solutions de Threat Intelliigence. Il met en évidence les fonctionnalités et les critères essentiels qui doivent être évalués au cours du processus de décision d'achat. En exigeant des solutions qui correspondent à vos besoins spécifiques, vous veillez à ce que la solution de Threat Intelligence choisie réponde efficacement aux défis uniques de votre organisation.

Nous concluons ce guide en présentant une solution d'ESET qui a été développée pour vous aider à couvrir vos besoins et améliorer votre stratégie globale de défense contre les menaces. Grâce à l'expertise humaine d'ESET, la solution offre une suite complète de fonctionnalités conçues pour répondre à l'évolution du paysage des menaces.

En fournissant de précieuses informations, des connaissances complètes et une approche orientée solutions, ce guide a pour objectif de doter les spécialistes de la sécurité, les analystes, les responsables informatiques et les membres de la direction, des outils nécessaires pour se repérer dans le monde complexe du Threat Intelligence. Ces connaissances vous permettront de prendre des décisions éclairées, d'améliorer la sécurité de votre organisation et de vous prémunir contre les cybermenaces émergentes.

Ce guide a pour objectif de doter les spécialistes de la sécurité, les analystes, les responsables informatiques et les membres de la direction, des outils nécessaires pour se repérer dans le monde complexe du Threat Intelligence.

Comprendre le Threat Intelligence

2.1 Avant de se lancer

Le Threat Intelligence fait référence aux modes de pensée et à la méthode d'une approche pratique pour faire face aux cybermenaces réelles ou potentielles.

Il comprend la collecte, l'analyse et la contextualisation d'informations sur les menaces potentielles et actuelles qui pèsent sur les systèmes informatiques d'une organisation. Il s'agit d'une approche proactive de la cybersécurité qui permet aux organisations d'identifier, d'évaluer et d'atténuer les risques posés par les cybermenaces.

Une attention particulière doit être accordée à l'aspect de la **contextualisation**. Elle est essentielle pour générer des connaissances spécialisées uniques et, en ce qui concerne la complémentarité du TI, la contextualisation s'appuie sur l'expertise humaine. C'est également à ce niveau que des différences cruciales peuvent apparaître dans la qualité de ces services. Les renseignements sur les menaces peuvent provenir de différentes sources, telles que des sources ouvertes, des services de renseignement commerciaux, des agences de renseignement gouvernementales et des équipes internes de TI.

La raison pour laquelle nous pouvons considérer le Threat Intelligence comme une façon de penser est qu'il modifie le paradigme global de la protection contre les menaces, et façonne la ligne de conduite et les processus de décision. Cela permet d'identifier les vulnérabilités et les vecteurs d'attaque potentiels, qui entrent en jeu dans le processus d'amélioration de la posture de cybersécurité d'une organisation.

L'objectif ultime du Threat Intelligence est de :

- Permettre aux organisations de **prendre des mesures proactives pour prévenir** ou atténuer les **cyberattaques**,
- Vous permettre de **hiérarchiser** et de concentrer vos **ressources** limitées sur l'atténuation des risques les plus importants,
- Vous aider à **trier les événements** et réduire les dommages causés par des attaques potentielles,
- **Minimiser l'impact négatif global** d'une attaque sur une organisation,
- **Réagir efficacement** à ces incidents de sécurité.

D'un point de vue pratique, le Threat Intelligence est très utile dans les situations où, par exemple, des adresses IP associées à une infrastructure malveillante, des bots, des tactiques, techniques et procédures (TTP), des identifiants compromis ou des injections web insérant du code HTML ou JavaScript sont utilisés. Il existe cependant plus de situations réelles dans lesquels le TI peut être utile. Certaines d'entre elles seront abordées dans le présent document.

La raison pour laquelle nous pouvons considérer le Threat Intelligence comme une façon de penser est qu'il modifie le paradigme global de la protection contre les menaces, et façonne la ligne de conduite et les processus de décision.

2.2 Marché du Threat Intelligence

2.2.1 QUE FAUT-IL RECHERCHER LORS DU CHOIX D'UN FOURNISSEUR DE TI ?

Lorsque vous choisissez un fournisseur de Threat Intelligence pour votre entreprise, vous devez tenir compte de plusieurs facteurs afin de vous assurer que le fournisseur que vous sélectionnez répond aux besoins de votre organisation. Avant de procéder à leur identification, il convient toutefois de garder à l'esprit qu'il existe une distinction générale entre quatre types de renseignements sur les menaces : **stratégiques**, **tactiques**, **techniques** et **opérationnels**.

Il se peut que ces quatre éléments ne soient pas représentés de manière égale dans les offres de services des fournisseurs. L'orientation dépend en grande partie d'aspects tels que le marché cible, les objectifs de l'entreprise, les moyens des fournisseurs, le degré de sophistication des menaces qui requièrent une attention particulière, la surface d'attaque, etc.

44

milliards de dollars

de valeur prévue pour le marché du Threat Intelligence d'ici 2033.

Source : *Département de recherche de Statista, Taille du marché mondial du renseignement sur les cybermenaces (CTI) de 2023 à 2033, 31 mars 2023.*

Cette distinction est également déterminée par les consommateurs de TI et les hiérarchies organisationnelles dans ces entreprises, respectivement. Les dirigeants stratégiques, les cadres dirigeants ou les membres du conseil de direction sont les plus susceptibles d'être intéressés par **les TI stratégiques**. Les **TI tactiques** peuvent être mieux adaptés aux praticiens de la sécurité tels que les SOC, les analystes de menaces, les chasseurs de menaces ou les intervenants sur incident. Les praticiens de la sécurité au niveau opérationnel, qui sont chargés de l'allocation efficace des ressources informatiques et des contrôles de sécurité, s'orientent davantage vers les **TI opérationnels**.

STRATÉGIQUE

Les TI stratégiques ont pour but d'identifier les grandes tendances susceptibles d'améliorer les connaissances de manière globale et de placer les informations dans leur contexte respectif. Ils peuvent prendre la forme de livres blancs, de notes d'information ou de rapports.

TACTIQUE

Les TI tactiques sont utilisés pour identifier le comment et le où des attaques et, par conséquent, fournissent une visibilité plus détaillée et rétrospective sur l'incident lui-même. L'escalade de privilèges, le contournement des défenses ou le mouvement latéral en sont des exemples.

TECHNIQUE

Les TI techniques permettent d'identifier le quoi, et couvre donc principalement les types d'indicateurs de compromission (IOC) qui se produisent lors d'incidents. Ces informations peuvent être utilisées au mieux par les analystes des SOC ou les ingénieurs d'intervention sur incident.

OPÉRATIONNEL

Les TI opérationnels se concentrent principalement sur le suivi des mouvements de l'adversaire et sur la compréhension des techniques utilisées lors d'une attaque. Les URL, les hachages de fichiers, les IP malveillantes, les clés de la base de registre ou les schémas et les protocoles de trafic réseau sont des exemples d'IOC sur lesquels le niveau opérationnel se concentre.

Pour être en mesure d'évaluer les qualités des TI, une entreprise doit prendre en compte différents facteurs, dont les suivants.

COMPLÉTUDE

Recherchez un fournisseur qui propose des renseignements complets sur les menaces couvrant un large éventail d'auteurs et de vecteurs de menaces, notamment les malwares, l'hameçonnage et d'autres types de cybermenaces. Cela peut vous aider à prendre les mesures appropriées pour réduire les risques. Le fournisseur devrait avoir accès à une variété de sources de données, y compris la télémétrie interne, des sources ouvertes et d'autres sources externes.

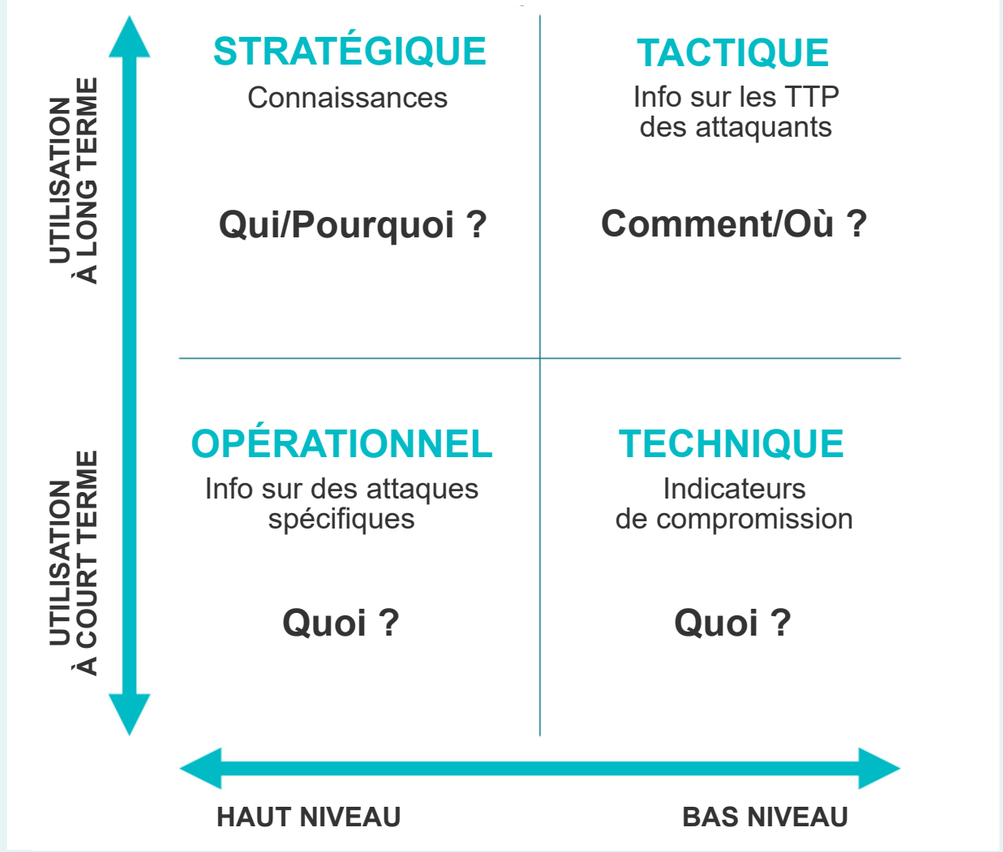


Figure 1. Diagramme en quadrant présentant les quatre types de renseignements sur les menaces.

FIABILITÉ

Un fournisseur devrait vous aider à économiser des ressources en mettant en œuvre une solution efficace plutôt qu'une solution coûteuse résultant de TI inexacts. Des renseignements peu fiables sont préjudiciables pour votre SOC, et peuvent entraîner le placement de contrôles de sécurité aux mauvais endroits ou simplement une mauvaise configuration. Il est nécessaire de maîtriser cet aspect de manière globale pour défendre votre organisation de manière fiable.

PERTINENCE

La réponse à une menace dans un environnement particulier et unique est un autre aspect important. Recherchez un fournisseur qui peut adapter les flux à votre secteur d'activité ou à la taille de votre entreprise, et qui fournit des informations pertinentes sur votre paysage de menaces spécifique. Il est également important de se concentrer sur le niveau tactique ou stratégique et de décider ce qui est pertinent pour vous à court et à long terme.

PONCTUALITÉ

Veillez à ce que le fournisseur propose des mises à jour en temps réel de ses flux de Threat Intelliigence. Les cybermenaces évoluent rapidement et il est donc essentiel de disposer d'informations de dernière minute pour conserver une longueur d'avance sur les menaces émergentes. L'envoi d'une alerte alors qu'une attaque a déjà commencé n'a que très peu d'intérêt pour une organisation.

Les autres facteurs à prendre en compte sont les suivants :

Personnalisation : Recherchez un fournisseur capable d'adapter ses flux de Threat Intelliigence aux besoins spécifiques de votre organisation. Des besoins clairement définis vous aident à trouver un fournisseur potentiel qui vous corresponde.

Évolutivité : La personnalisation seule peut ne pas suffire. Veillez donc à ce que le fournisseur puisse faire évoluer ses services pour répondre aux besoins de votre organisation au fur et à mesure de sa croissance. Cela inclut la possibilité de prendre en charge un grand nombre d'utilisateurs, de fournir des rapports et des analyses personnalisés, et les intégrer à vos outils de sécurité existants.

40 %

seront investis par les dirigeants du G2000 dans le renseignement sur les entreprises et sur le marché d'ici à la fin de 2025.

Source : *IDC FutureScape : L'avenir du renseignement dans le monde : prévisions pour 2023*.

80 %

des entreprises du G2000 augmenteront leurs investissements dans le Threat Intelligence d'ici à 2024.

Source : *IDC FutureScape : L'avenir du renseignement dans le monde : prévisions pour 2023*.

Réputation : Recherchez un fournisseur jouissant d'une solide réputation dans le secteur et ayant déjà proposé des services de TI fiables et efficaces à des organisations similaires à la vôtre. En travaillant avec un tel fournisseur, votre organisation peut garder une longueur d'avance sur les cybermenaces grâce à la protection de vos actifs et infrastructures critiques. Une bonne réputation est toujours considérée comme une indication de la qualité et des moyens.

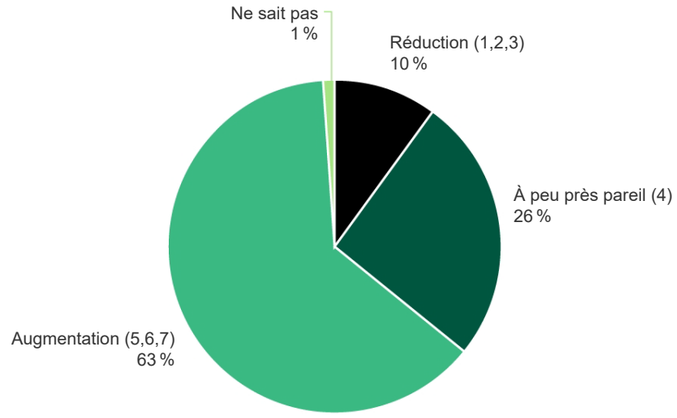
2.2.2 COMMENT LES ORGANISATIONS CONSOMMENT-ELLES HABITUELLEMENT LE TI ?

Comprendre comment les organisations utilisent habituellement les services de TI peut vous aider à acquérir une connaissance améliorée et plus prospective des options dont vous pouvez bénéficier lorsque vous envisagez d'adopter le TI dans votre entreprise.

Les organisations sont confrontées à une myriade de cybermenaces qui peuvent mettre en péril leur activité, leur réputation et leur stabilité financière. Des services de TI fiables et utilisables sont donc indispensables.

Lequel des éléments suivants décrit une évolution de votre budget consacré au renseignement sur les menaces comme technologie de sécurité (y compris les salariés, les produits et les services) entre 2022 et 2023 ?

(5, 6 ou 7 sur une échelle de 1 [réduction] à 7 [augmentation])



Base : 3 580 décideurs en matière de sécurité au niveau manager ou à un niveau hiérarchique supérieur
Source : Enquête de Forrester sur la sécurité, 2022

Source : *L'état de la veille sur les menaces, Forrester, 13 avril 2023*

Les entreprises consomment les TI de différentes manières : Il s'agit notamment de flux sectoriels, de renseignements provenant de sources ouvertes, de partage entre pairs et de prestataires.

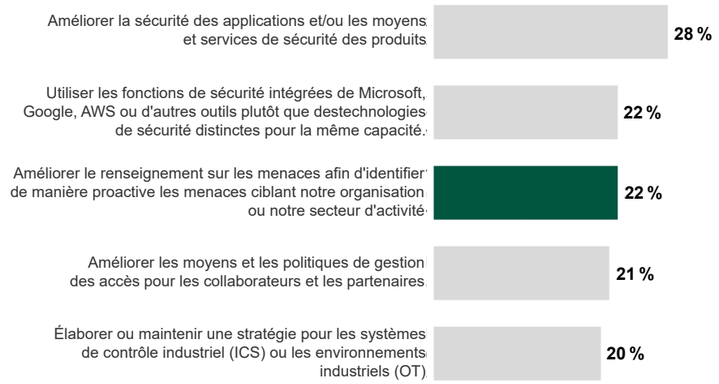
1. Les **FLUX SECTORIELS** sont des plateformes de partage d'informations qui rassemblent des organisations appartenant aux mêmes secteurs ou différents centres et cabinets d'analystes. Ces flux fournissent aux organisations des informations opportunes et pertinentes sur les menaces émergentes, les techniques d'attaque et les indicateurs de compromission (IOC) spécifiques à leur secteur d'activité. Certains flux sectoriels sont payants, tandis que d'autres sont gratuits.

2. Le **RENSEIGNEMENT OPEN SOURCE (OSINT)**, en tant que méthode de collecte et d'analyse d'informations, comprend l'utilisation de dossiers publics, d'articles de presse, de sites web gouvernementaux, de forums communautaires, de blogs et de plateformes de réseaux sociaux qui fournissent une mine d'informations sur les cybermenaces. OSINT a un objectif similaire à celui des flux sectoriels, mais il est traditionnellement utilisé par de petits groupes ou des personnes, et est plus ouvert et accessible en termes de partage d'informations qui peuvent être non officielles.

3. Le **PARTAGE ENTRE PAIRS** est un autre mode de consommation du TI par les organisations. Dans ce cas, les organisations partagent des informations au sein d'un même secteur, mais seulement dans un petit sous-ensemble de ce secteur. Le partage entre pairs se fait généralement entre des entreprises de même taille et ayant les mêmes moyens.

4. **PRESTATAIRES.** Enfin, les organisations peuvent également s'appuyer sur des prestataires qui proposent des renseignements dans le cadre de leurs services. Ce peut être des prestataires indépendants de Threat Intelligence, des éditeurs de solutions de sécurité ou des prestataires de services de sécurité managés (MSSP). Ils proposent une gamme de services, notamment des flux de TI, des rapports, des services de recherche de menaces et des services de sécurité managés.

« Parmi les initiatives suivantes, lesquelles sont susceptibles de constituer les grandes priorités tactiques de votre organisation en matière de sécurité informatique/de l'information au cours des 12 prochains mois ? »
(Plusieurs réponses acceptées)



Note : Toutes les options de réponse ne sont pas indiquées.
Base : 2 355 décideurs en matière de technologies de sécurité
Source : Enquête de Forrester sur la sécurité, 2022

Source : *L'état de la veille sur les menaces, Forrester, 13 avril 2023*

Les différents modes de consommation des TI dépendent fortement des besoins, des capacités et des ressources spécifiques des organisations. Les flux sectoriels, les sources ouvertes, le partage entre pairs et les prestataires sont tous des sources importantes de TI. En tirant parti de ces sources, les organisations peuvent améliorer leurs capacités de détection des menaces, la réponse aux incidents et, en fin de compte, renforcer leur posture globale de sécurité.

2.2.3 POURQUOI LA MATURITÉ DES ORGANISATIONS EST-ELLE IMPORTANTE ?

L'adoption de services de TI devient de plus en plus importante dans tous les secteurs d'activité, en particulier dans les grandes entreprises. Cependant, le niveau de maturité d'une organisation joue un rôle crucial dans la détermination du type de services de TI qu'elle devrait adopter.

Les organisations matures dotées d'équipes spécialisées de TI exigent souvent davantage de fonctionnalités pour collecter, traiter et diffuser leurs propres renseignements. Ces organisations ont une meilleure compréhension de leur posture de sécurité et des menaces spécifiques auxquelles elles sont confrontées. Elles consomment généralement entre huit et quinze sources de TI, qui peuvent inclure des sources gratuites, des sources ouvertes, des CERT, des ISAC et des fournisseurs commerciaux. Ces organisations recherchent des fonctions avancées telles que l'analyse des graphes, l'analyse des liens ou le suivi et la modélisation des auteurs de menaces afin d'améliorer leurs moyens de détection des menaces.

Les organisations moins sophistiquées disposant d'équipes limitées voire d'aucune équipe de TI peuvent choisir des solutions individuelles qui se concentrent sur les flux de Threat Intelliigence lisibles par machine (MRTI). Ces organisations disposent d'intégrations prêtes à l'emploi et ne sont pas tellement intéressées par des fonctionnalités

>50 %

des organisations du G2000 devront faire face à des pénalités d'ici à la fin de 2025 si elles n'utilisent pas l'IA pour la détection et la remédiation automatique des données en raison de la complexité croissante, de la volatilité et de la rareté des ressources.

Source : *IDC FutureScape : L'avenir du renseignement dans le monde : prévisions pour 2023*.

avancées. Elles recherchent une solution facile à déployer qui leur fournisse les TI nécessaires sur les menaces pour améliorer leur posture de sécurité.

Les organisations matures sont avantagées : Avec des équipes de TI dédiées, elles disposent de l'expertise et des ressources nécessaires pour tirer pleinement parti des services de TI qu'elles adoptent. Elles peuvent également intégrer les TI à leur infrastructure de sécurité existante, procéder à une analyse détaillée des données relatives aux menaces et les utiliser pour étayer leur stratégie de sécurité. Tout cela se traduit par une meilleure résilience de la cybersécurité.

Les organisations moins matures, en revanche, peuvent avoir des difficultés à tirer pleinement parti des avantages des TI. Elles peuvent manquer de ressources ou d'expertise pour intégrer efficacement les TI dans leur infrastructure de sécurité existante et ne pas avoir les compétences nécessaires pour analyser et utiliser les données afin d'améliorer leur posture de sécurité. Cela les rend plus vulnérables et moins bien préparées à faire face aux cybermenaces. La bonne nouvelle est que toute organisation moins sophistiquée en termes de moyens peut devenir une organisation mature, ce qui signifie devenir plus résistante.

2.2.4 PERSPECTIVES GÉNÉRALES DU MARCHÉ DU TI

Le marché des TI est aujourd'hui en pleine expansion et peut ressembler à un labyrinthe plein de chemins bien définis et d'options indéchiffrables. Lorsque vous envisagez d'adopter une solution de TI, vous devez tenir compte de certains aspects pour comprendre et tirer pleinement parti de cette solution. Ceux-ci peuvent être définis comme suit.

1. **Nouvelles catégories de renseignements.** Le premier aspect à garder à l'esprit lorsqu'on essaie de comprendre le marché du TI est que de nouvelles catégories de renseignements apparaissent constamment et que, par conséquent, le marché et les solutions évoluent de manière dynamique. Ces nouvelles catégories permettent d'évaluer de nouvelles menaces et de fournir des renseignements qui se reflètent dans les offres actuelles. La veille sur les risques climatiques et la veille sur les événements critiques, qui permettent aux organisations d'obtenir des données et des informations sur mesure pour un lieu et un environnement spécifiques, sont des exemples de ces catégories. Envisagez vos besoins spécifiques dans une perspective à long terme afin d'éviter une réévaluation fréquente de la stratégie.

2. **Répondre à différents types de menaces.** Le second aspect est que les grandes organisations ont généralement besoin de plusieurs services de TI pour répondre à différents types de menaces. Les organisations investissent dans un arsenal de produits pour tenir compte de chaque type de risque auquel elles sont confrontées. Il peut arriver qu'un fournisseur qui excelle dans un type de renseignement sur les événements critiques ne dispose pas de renseignements pour un autre domaine, par exemple l'analyse des malwares. Il est donc essentiel de déterminer le niveau de complexité et les particularités afin d'éviter des solutions disproportionnées et mal ciblées.

3. **Flux d'IOC.** Les flux d'IOC, qui étaient autrefois des produits autonomes, font désormais partie de services de renseignement plus importants. Aujourd'hui, les flux d'IOC autonomes ne disposent pas du contexte nécessaire pour permettre de meilleures décisions tactiques en matière de sécurité et, par conséquent, de nombreux contrôles de sécurité proposés par les fournisseurs font partie d'autres moyens de détection. Comme indiqué ci-dessus, il est essentiel de comprendre le contexte général dans lequel les menaces émergent, et qui délimite votre propre environnement, pour vous défendre contre les menaces. Nous vous invitons à rechercher des solutions globales qui permettent une analyse approfondie du paysage des menaces.

4. **Expansion des cas d'utilisation, des rôles et des processus.** Le TI se développe pour prendre en charge davantage de cas d'utilisation, de rôles et de processus, en particulier ceux liés à l'amélioration de la visibilité et la protection des actifs numériques. Les offres de TI prennent désormais en charge non seulement les rôles traditionnels en matière de sécurité, tels que les RSSI et les analystes de SOC, mais également des rôles qui ne sont généralement pas alignés sur le TI. Par exemple, les équipes chargées de la marque, les équipes marketing, les équipes chargées de la conformité et les fonctions juridiques peuvent toutes bénéficier du TI. Il est essentiel de comprendre ce changement, ainsi que son contexte et son raisonnement, pour évaluer le potentiel qu'une solution de TI peut vous apporter. Plus vos collaborateurs sont informés, plus vous pouvez compter sur eux et, par conséquent, bénéficier de leur réceptivité aux embûches et aux problèmes éventuels.

5. **Les fournisseurs de propriété intellectuelle et de TI se développent sur de nouveaux marchés.** Le cinquième aspect à garder à l'esprit est que les fournisseurs de propriété intellectuelle et de TI se développent sur de nouveaux marchés en raison de l'évolution de la situation générale des cybermenaces. L'expansion a atteint des marchés tels que SOAR, CM, XDR, la gestion des services externes et la gestion des risques des tiers. La raison en est la nécessité de faire face à des menaces très sophistiquées, les risques et les conséquences des cyberattaques étant aujourd'hui plus élevés que jamais. Cela vous donne l'occasion de réfléchir à votre propre situation et d'évaluer vos besoins éventuels.

Le marché du TI est en constante évolution et, par conséquent, il peut être difficile de le comprendre et de choisir la bonne solution. Cependant, en gardant à l'esprit les nouvelles catégories de renseignements, le besoin de faire appel à de multiples services de TI, la valeur et la nature des flux d'IOC, l'expansion des cas d'utilisation et des rôles qui peuvent être pris en charge, et l'expansion des fournisseurs de propriété intellectuelle et de TI sur de nouveaux marchés, les organisations peuvent mieux évaluer leur propre situation et leurs besoins, la situation générale dans laquelle le TI est pratiquée, et ainsi prendre la bonne décision.

Bien que le marché du TI soit aujourd'hui en pleine expansion, les fournisseurs de TI doivent relever certains défis afin de proposer une solution sur laquelle les entreprises peuvent compter. ESET peut y répondre de manière complète grâce à ses moyens avancés et son expertise. Ces défis sont notamment les suivants :

1 UNE QUANTITÉ ÉCRASANTE DE DONNÉES

ESET n'offre que des renseignements sélectionnés qui sont regroupés dans des rapports privés complets sur des APT. Nous pouvons également fournir une attribution supplémentaire aux flux de données.

2 UN MANQUE D'EXPERTISE POUR L'INTERPRÉTATION

ESET n'offre que des renseignements contextuels, étayés par MITRE ATTACK, qui marquent les TTP respectives et fournit des détails sur les secteurs d'activité ciblés, parfois même sur un pays ou une région.

3 DES COÛTS ÉLEVÉS

Bien qu'il s'agisse généralement d'une question assez subjective, ESET propose une offre compétitive qui se caractérise par un rapport coût/bénéfice positif, en particulier si l'on prend en considération les coûts globaux du marché.

4 UN MANQUE DE DIFFÉRENCIATION DES SOURCES

ESET offre des renseignements propriétaires uniques pris en charge par les propres équipes de recherche d'ESET et fournissant une expertise en temps réel dans le ciblage des attaques, des auteurs d'APT, des menaces zero-day, ou des activités de botnet. Les renseignements d'ESET sur les menaces s'appuient sur une télémétrie unique, et utilisent les technologies multicouches d'ESET.

5 UNE MAUVAISE OPÉRATIONNALISATION

ESET propose des flux MRTI (renseignements sur les menaces lisibles par machine) agrégés et des détails d'attribution complets, notamment la chronologie d'une attaque, la technique d'attaque MITRE ou d'autres détails d'attribution utiles pour les organisations.

Bien que le marché du TI soit aujourd'hui en pleine expansion, les fournisseurs de TI doivent relever certains défis afin de proposer une solution sur laquelle les entreprises peuvent compter.

ESET Threat Intelligence

3.1 Qu'est-ce qu'ESET Threat Intelligence (ETI) ?

ESET Threat Intelligence se définit par son **approche préventive de la cybersécurité qui a pour objectif d'accélérer la réactivité, d'améliorer la préparation** et de mettre en œuvre des **mesures proactives** face aux différents types de cybermenaces.

Il s'agit donc d'un service de renseignement complet et avancé qui permet aux clients de détecter et d'analyser les cybermenaces, et d'y répondre rapidement et efficacement. Il propose une série de techniques et de ressources de collecte de renseignements, telles que l'analyse des malwares, les flux de renseignements sur les menaces et une liste d'URL et de domaines suspects, afin de fournir aux clients des informations utilisables et une compréhension approfondie des menaces émergentes

L'un des principaux avantages d'ETI est qu'il permet aux clients d'identifier rapidement les cybermenaces et d'y répondre. ETI permet également aux clients de mieux comprendre leur propre posture de sécurité et de l'améliorer au fil du temps. ESET Threat Intelligence peut également être une excellente solution pour les organisations qui n'ont jamais utilisé de solutions et de produits ESET dans leur environnement, car il leur fournit une approche holistique et entièrement personnalisée pour leurs politiques de sécurité.

ETI offre aux organisations l'avantage de disposer d'une **couverture géographique unique** qui s'est avérée cruciale ces dernières années en raison de l'évolution imprévue des défis de la cybersécurité, notamment des attaques plus sophistiquées, plus ciblées et plus localisées, et des exigences spécifiques de conformité, mais également en raison de changements significatifs dans la géopolitique. Les cybercriminels sponsorisés par des états et les groupes d'APT jouent un rôle crucial dans l'amélioration du potentiel destructeur des cybermenaces. Ces acteurs s'attaquent non seulement à des organisations publiques, mais également le plus souvent, à des organisations privées qui peuvent avoir une importance stratégique. Par conséquent, l'investissement dans le Threat Intelligence devient une nouvelle norme pour les organisations privées de toutes tailles.

Grâce à ETI, ESET a été à plusieurs reprises l'un des meilleurs fournisseurs de renseignements sur la cyberguerre lors de l'agression russe contre l'Ukraine. Nos chercheurs et nos experts cartographient un large éventail de groupes de pirates, dont les activités les plus notoires sont souvent menées depuis la Russie, la Chine, la Corée du Nord et l'Iran. Une couverture géographique unique permet aux organisations d'identifier les outils et les techniques utilisés par les adversaires dans d'autres pays et d'anticiper ainsi les attaques potentielles dans une région spécifique, ce qui les rend plus résistantes.

3.1.1 QUE PEUT APPORTER ETI ?

ETI est conçu pour fournir des connaissances et de l'expertise afin d'aider les organisations à atténuer les risques liés à la cybersécurité. Il intègre différents flux de données, des métadonnées, des flux sélectionnés, et se concentre sur la qualité plutôt que sur la quantité, tout en fournissant des informations très pertinentes et à la pointe du marché. Les flux en temps réel qui fournissent des informations de dernière minute sur les menaces les plus récentes sont l'une des caractéristiques les plus importantes d'ETI.

Grâce à ETI, votre organisation peut enquêter sur les incidents, tester des hypothèses et améliorer ses moyens de recherche de menaces. ETI fournit également de nombreuses métadonnées qui peuvent vous apporter des informations contextuelles sur les menaces, telles que la source, le type et la gravité des menaces. Ces métadonnées sont fréquemment actualisées, ce qui permet aux organisations d'avoir toujours accès aux informations les plus récentes.

En disposant des rapports d'ESET sur les APT, vous pouvez acquérir une connaissance complète du paysage des menaces, y compris une analyse des auteurs de menaces, leurs méthodes de compromission et leur comportement, des détails techniques spécifiques, des résumés d'activité, et plus encore. Ces rapports sont conçus pour être utilisés par les analystes de la sécurité, le personnel chargé de répondre aux incidents et d'autres professionnels de la cybersécurité.

« ESET a acquis une notoriété bien méritée et fait l'objet d'une demande accrue de la part des gouvernements, des organisations basées en Ukraine et des organisations internationales pour ses services de Threat Intelligence et ses produits de sécurité.

Source : *IDC, Parts du marché mondial de la sécurité moderne des endpoints, juillet 2021–juin 2022 : le taux de change légèrement réduit accélère la croissance (doc n° US49982022, janvier 2023.*

ETI permet aux organisations de vérifier les niveaux de confiance pour évaluer les données collectées. Ceci est particulièrement important pour définir la fiabilité des données utilisées par les organisations, et par conséquent pour prendre des décisions mieux informées. Grâce aux tests d'hypothèses, les clients peuvent améliorer la recherche des menaces. C'est un point crucial pour devenir plus proactif au lieu de se contenter d'attendre passivement qu'une attaque se produise.

Les principaux avantages d'ETI, qui peuvent renforcer votre posture de cybersécurité, sont les suivants :

- **Expertise humaine** basée sur l'expérience des analystes d'ESET
- **Compréhension** des risques et donc **prévision des menaces**, **atténuation des** incidents et **réduction** de l'exposition aux menaces actuelles
- Amélioration de la **recherche** et de la **remédiation** des menaces
- Rassemblement de TI à partir d'un **éventail unique de sources**
- Découverte de risques potentiels par **l'analyse des systèmes** via Yara ou la vérification des réseaux
- **Surveillance des groupes de pirates** et acquisition d'une connaissance approfondie sur leurs tactiques, leurs méthodes, voire leurs motivations
- **Économie de ressources** grâce à du contenu bien structuré nécessitant peu de maintenance
- **Des décisions plus rapides**, **plus utiles** et **meilleures** à court terme (blocage de plages d'adresses IP, hachages, etc.) et à long terme (stratégie de renseignement et de cybersécurité)
- Recherche constante de menaces, via **plusieurs couches**, depuis la phase d'avant le démarrage jusqu'aux périodes d'inactivité

ESET fournit un type de TI facile à utiliser et à maintenir. Il comprend :

- Des **renseignements d'experts sélectionnés** et **hautement utilisables**
- **Une télémétrie robuste**
- **Automatisation sur plusieurs couches** avec recherche et détection des menaces depuis la phase d'avant le démarrage jusqu'aux périodes d'inactivité
- **Intégration des flux** dans votre architecture actuelle (SIEM/SOAR/TIP) conformément aux directives d'ESET
- Options d'intégration étendues telles que la compatibilité avec TAXII 2
- **Actualisation fréquente** des flux (toutes les 5 à 10 minutes) et filtrage des IOC en fonction de leur gravité et de leur prévalence

3.1.2 FLUX DE DONNÉES D'ETI

Comme indiqué ci-dessus, ETI fournit aux organisations des flux uniques. Il s'agit de flux de données couvrant les menaces potentielles ou réelles pour la sécurité d'une organisation, fournissant des informations complètes et utilisables en temps opportun. Les flux de données d'ETI proviennent d'un ensemble d'environ 110 millions de capteurs, d'ESET LiveGrid® et d'un système automatisé de suivi des botnets, ce qui permet de réduire au maximum le nombre de faux positifs.

FLUX DE FICHIERS MALVEILLANTS

Ce flux fournit des informations en temps réel sur les échantillons de malwares actuellement répandus, ainsi que sur leurs caractéristiques et leurs IOC. Il vous aide à comprendre quels fichiers malveillants sont découverts et vous permet de les bloquer de manière proactive avant qu'ils ne causent des dommages. Le flux comprend une évaluation des hachages d'exécutables malveillants et des données associées. Il est fréquemment actualisé et peut être filtré afin que les clients n'obtiennent que des données pertinentes avec de faibles niveaux de redondance.

FLUX D'APT

Comme son nom l'indique, ce flux couvre les APT du point de vue de la recherche, en se concentrant principalement sur les IOC associés aux attaques des groupes d'APT. Le flux permet une détection et une réponse précises et fiables, la protection des actifs critiques, et permet d'empêcher l'exfiltration de données. Il est basé sur des données collectées et produites directement par la recherche ESET, et est exporté depuis le serveur interne MISP d'ESET. Toutes les informations sont partagées dans le cadre d'un rapport détaillé qui les présente dans leur contexte et les explique de manière exhaustive. Le flux peut également être acheté séparément.

FLUX DE DOMAINES

Ce flux bloque les domaines malveillants afin d'empêcher les utilisateurs de consulter ces sites et, par conséquent, de les protéger contre les infections et les atteintes à la sécurité données. Ces domaines font généralement partie des campagnes d'hameçonnage, de l'infrastructure de commande et de contrôle des malwares ou d'une cyberattaque de plus grande envergure. Le flux couvre le nom de domaine, l'adresse IP, la date associée et l'activité malveillante correspondante. Il classe les domaines en fonction de leur gravité, ce qui vous permet d'adapter la réponse en conséquence, par ex. en ne bloquant que les domaines les plus risqués. Le flux fournit également des informations sur le niveau de confiance sous la forme d'une évaluation du domaine à bloquer.

FLUX D'URL

Informations sur les URL malveillants actuelles et courantes, et données associées. Le flux est créé à partir de toutes les sources URL toutes les 5 minutes. Sa déduplication est effectuée toutes les 24 heures et le filtrage dans ce cas est un peu plus strict pour veiller à ce qu'aucune information sensible ne soit partagée. Il est donc basé sur le partage d'URL sans paramètres. Contrairement au flux de domaines, le flux d'URL est beaucoup plus petit et plus ciblé, car il permet aux analystes de bloquer des URL malveillantes spécifiques au lieu de bloquer des domaines entiers.

FLUX D'ADRESSES IP

Ce flux partage les adresses IP malveillantes actuelles et courantes, ainsi que certaines données qui leur sont associées. La structure des données est similaire à celle utilisée pour les flux de domaines et d'URL. Le principal cas d'utilisation est de comprendre quelles adresses IP malveillantes sont actuellement répandues, de bloquer celles dont la gravité est élevée et d'inspecter les moins graves grâce à des données supplémentaires, et de voir quels dommages ont déjà été causés. Le filtrage dans ce cas est très similaire à celui du flux d'URL.

FLUX DE BOTNETS

Basé sur le système propriétaire et automatisé de suivi des botnets d'ESET, ce flux comporte deux types de sous-flux : commande et contrôle, et cibles. Les données fournies comprennent des éléments tels que la détection, le hachage, la date de la dernière activité, les fichiers téléchargés, les adresses IP, les protocoles, les cibles et d'autres informations. Les IOC comprennent MD5, SHA1, SHA256 ; serveurs de commande et de contrôle (URL).

3.1.3 RAPPORTS SUR LES APT

Les rapports d'ESET sur les menaces persistantes avancées (APT) représentent une source fiable de renseignements sur les cybermenaces qui couvre leurs auteurs et leurs activités. Ils fournissent des informations stratégiques, tactiques, techniques et opérationnelles qui permettent aux organisations d'améliorer la détection des menaces et de développer une posture de cybersécurité plus proactive.

Les rapports facilitent la recherche de menaces ainsi que l'investigation et l'atténuation des incidents en cours. Plus important encore, ils permettent également d'être proactifs, voire prédictifs, au lieu d'être réactifs, et de prendre de meilleures décisions, plus rapidement, tant au niveau technique qu'au niveau hiérarchique. La connaissance de l'adversaire aide les responsables de la sécurité à déterminer quelles menaces potentielles sont les plus susceptibles de devenir des menaces réelles pour leur organisation, et décider où investir et sur quoi se concentrer.

INTÉGRATION AVEC MISP

Une pratique très utile pour les organisations consiste à consolider toutes les données des rapports dans une plateforme de Threat Intelligence. ESET offre un accès à son système interne MISP (plateforme de partage d'informations sur les malwares), qui contient toutes les données pertinentes et utiles. Les clients peuvent donc facilement les synchroniser avec leurs propres systèmes pour une intégration transparente.

Cette intégration via MISP s'avère extrêmement utile pour différents experts, car elle leur permet d'économiser du temps et des ressources, tout en leur permettant de se familiariser facilement avec le pool de données approfondies. Les clients ont notamment la possibilité de créer leurs propres requêtes, d'établir des connexions spécifiques, d'effectuer des analyses approfondies et tirer parti de la diversité des données disponibles dans MISP. L'intégration fait partie du package Premium et représente une approche unique qui distingue ESET des autres fournisseurs qui n'offrent généralement pas d'intégration aussi complète.

49 %

d'augmentation des flux commerciaux payants de renseignements sur les menaces, de 2021 à 2022.

Source : *L'état du renseignement sur les menaces, Forrester, 13 avril 2023.*

60 %

d'augmentation des flux provenant des communautés de partage d'informations, de 2021 à 2022.

Source : *L'état du renseignement sur les menaces, Forrester, 13 avril 2023.*

65 %

d'augmentation des flux de renseignements sur les menaces en libre accès, de 2021 à 2022.

Source : *L'état du renseignement sur les menaces, Forrester, 13 avril 2023.*

APERÇU DÉTAILLÉ DES RAPPORTS PREMIUM SUR LES GROUPES DE PIRATES

Les rapports sur les APT ne comprennent pas seulement des IOC, mais également des informations contextuelles et d'autres détails pertinents. Ils se présentent sous la forme d'un ensemble de plusieurs types de résultats :

- Rapports de synthèse des activités,
- Rapports d'analyse technique,
- Rapports mensuels de synthèse,
- Rapports mensuels,
- Flux de données sur les APT,
- Accès au serveur MISP APT (permet aux clients de consommer des données de manière plus automatique),
- Accès aux analystes des menaces

Les organisations bénéficient également d'un accès en avant-première aux articles techniques publiés sur WeLiveSecurity.

1. **Rapports de synthèse des activités**
Ces rapports sont publiés dans un délai de deux semaines et décrivent les dernières campagnes d'APT suivies par les chercheurs d'ESET avec les cibles et les IOC associés. Ces rapports permettent aux défenseurs de suivre les auteurs des menaces les plus avancés avec un contexte sur leurs activités actuelles. Ces données peuvent être utilisées par les **défenseurs** pour protéger leurs réseaux en bloquant ces IOC. Ils permettent également aux **chercheurs** et au **personnel chargé de la réponse aux incidents** d'améliorer leur compréhension des groupes d'APT qui ciblent leurs organisations en connaissant leurs tactiques, techniques et procédures (TTP) les plus récentes.

2. **Rapports d'analyse technique**
Dans une certaine mesure, les rapports d'analyse technique sont similaires aux livres blancs publiés sur WeLiveSecurity. Ils relèvent du domaine du renseignement tactique sur les menaces et décrivent les campagnes récentes, les nouveaux outils et les sujets associés. Ils contiennent des données utilisables telles que des règles YARA, des règles Snort, des requêtes pivotantes telles que Shodan et Censys, des correspondances MITRE ATT&CK®, des recommandations sur la manière de protéger le réseau et des conseils de remédiation le cas échéant. Lorsque des structures complexes de malwares sont décrites, ESET fournit également des outils pour aider les analystes de ses clients, tels que des scripts de désobfuscation ou de déchiffrement. Les rapports sont utiles aux **défenseurs** qui cherchent à protéger leur réseau contre les menaces les plus récentes. Ils sont également utiles aux chercheurs et au **personnel chargé de répondre aux incidents**, qui doivent analyser et signaler les menaces susceptibles de cibler leur organisation.

3. **Rapports de synthèse mensuels**
Les rapports de synthèse mensuels regroupent les informations de tous les rapports d'analyse technique et de synthèse d'activité publiés au cours du mois précédent sous une forme plus courte et plus digeste. Ils se concentrent sur le renseignement stratégique, tactique et opérationnel sur les menaces et couvrent les nouvelles activités de différents auteurs de menaces, avec les régions et les secteurs ciblés. Ces rapports conviennent donc même aux **cadres dirigeants**, aux **managers** et aux **décideurs** hors du domaine de

la cybersécurité, ou peuvent servir de rapports mensuels de synthèse pour les chercheurs et le personnel chargé de répondre aux incidents. Les aperçus mensuels sont automatiquement envoyés aux clients qui s'abonnent au rapports ESET APT Reports PREMIUM. Ils sont plutôt autonomes et peuvent être proposés comme un niveau de rapport plus accessible aux clients qui ne souscrivent à aucun autre produit ou service proposé par ESET. Les rapports mensuels ne contiennent pas d'IOC, car ceux-ci sont inclus dans les rapports d'analyse technique et de synthèse des activités.

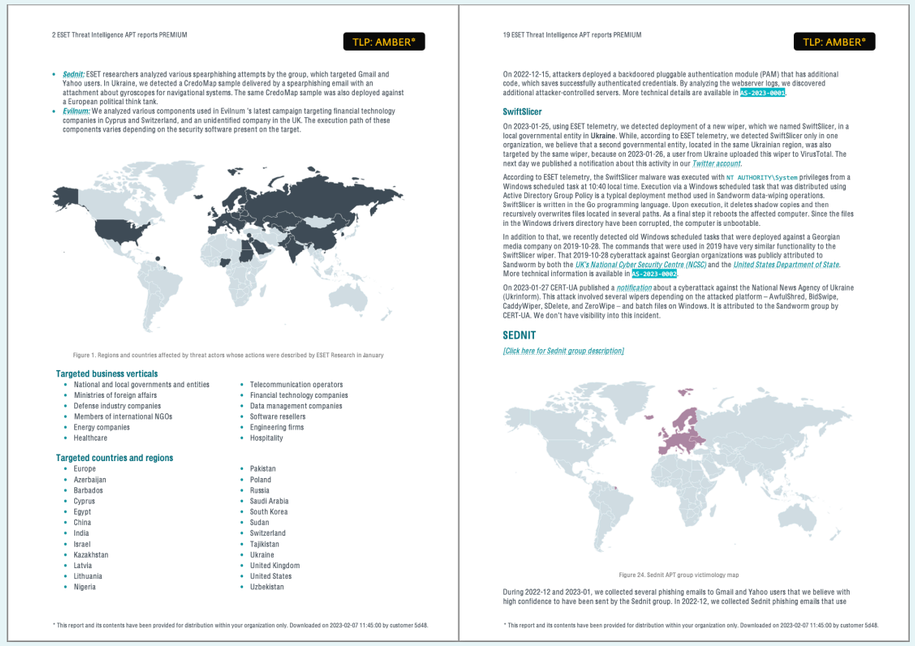
4. Rapports mensuels succincts

Ces rapports sont beaucoup moins techniques et fournissent des informations essentielles tirées des rapports de synthèse mensuels dans un format bref, complet et digeste. Ils sont publiés régulièrement à un rythme d'un rapport par mois (12 par an au total), et contiennent des informations précieuses sur des secteurs, des régions et des pays ciblés, ainsi que des faits essentiels et utilisables dont tout **défenseur**, **cadre**, **RSSI** ou tout autre **décideur** peut tirer profit. Les rapports sont présentés dans un format concis d'une page, ce qui les rend exceptionnellement pratiques.

ESET offre un accès en avant-première à une série de rapports qui se sont avérés très utiles pour les organisations et leur préparation. Il s'agit notamment des Rapports sur les menaces qui sont publiés sur WeLiveSecurity deux fois par an. Les abonnés bénéficient d'un accès exclusif à ces rapports environ 6 à 7 jours avant leur mise à disposition du public.

Il en va de même pour les rapports d'activité des APT qui reflètent le calendrier de publication des Rapports sur les menaces. Les abonnés peuvent également bénéficier d'un accès en avant-première à nos articles techniques qui sont publiés au moins une fois par mois. Ces articles sont accessibles environ 2 à 3 jours avant leur publication normale.

Ces quelques jours de disponibilité en avant-première pourraient être un avantage crucial pour les chasseurs de menaces et les défenseurs afin d'analyser les systèmes, car les adversaires qui suivent nos études pourraient modifier leur comportement et s'adapter à la nouvelle situation découlant de l'exposition des détails de leurs activités. Ces avant-premières aident donc simplement les organisations à prendre de l'avance.



2 ESET Threat Intelligence APT reports PREMIUM

TLP: AMBER*

- *Sednit:* ESET researchers analyzed various spearphishing attempts by the group, which targeted Gmail and Yahoo users. In Ukraine, we detected a CredoMap sample delivered by a spearphishing email with an attachment about gyroscopes for navigational systems. The same CredoMap sample was also deployed against a European political think tank.
- *Evilnum:* We analyzed various components used in Evilnum 's latest campaign targeting financial technology companies in Cyprus and Switzerland, and an unidentified company in the UK. The execution path of these components varies depending on the security software present on the target.

Figure 1. Regions and countries affected by threat actors whose actions were described by ESET Research in January

Targeted business verticals

- National and local governments and entities
- Ministries of foreign affairs
- Defense industry companies
- Members of international NGOs
- Energy companies
- Healthcare
- Telecommunication operators
- Financial technology companies
- Data management companies
- Software resellers
- Engineering firms
- Hospitality

Targeted countries and regions

- Europe
- Azerbaijan
- Barbados
- Cyprus
- Egypt
- China
- India
- Israel
- Kazakhstan
- Latvia
- Lithuania
- Nigeria
- Pakistan
- Poland
- Russia
- Saudi Arabia
- South Korea
- Sudan
- Switzerland
- Tajikistan
- Ukraine
- United Kingdom
- United States
- Uzbekistan

* This report and its contents have been provided for distribution within your organization only. Downloaded on 2023-02-07 11:45:00 by customer 5d48.

19 ESET Threat Intelligence APT reports PREMIUM

TLP: AMBER*

On 2022-12-15, attackers deployed a backdoored pluggable authentication module (PAM) that has additional code, which saves successfully authenticated credentials. By analyzing the webserver logs, we discovered additional attacker-controlled servers. More technical details are available in `AS-2023-0003`.

SwiftSlicer

On 2023-01-25, using ESET telemetry, we detected deployment of a new wiper, which we named SwiftSlicer, in a local governmental entity in **Ukraine.** While, according to ESET telemetry, we detected SwiftSlicer only in one organization, we believe that a second governmental entity, located in the same Ukrainian region, was also targeted by the same wiper, because on 2023-01-26, a user from Ukraine uploaded this wiper to VirusTotal. The next day we published a notification about this activity in our *Twitter account*.

According to ESET telemetry, the SwiftSlicer malware was executed with `NT AUTHORITY\System` privileges from a Windows scheduled task at 10:40 local time. Execution via a Windows scheduled task that was distributed using Active Directory Group Policy is a typical deployment method used in Sandworm data-wiping operations. SwiftSlicer is written in the Go programming language. Upon execution, it deletes shadow copies and then recursively overwrites files located in several paths. As a final step it reboots the affected computer. Since the files in the Windows drivers directory have been corrupted, the computer is unbootable.

In addition to that, we recently detected old Windows scheduled tasks that were deployed against a Georgian media company on 2019-10-28. The commands that were used in 2019 have very similar functionality to the SwiftSlicer wiper. That 2019-10-28 cyberattack against Georgian organizations was publicly attributed to Sandworm by both the *UK's National Cyber Security Centre (NCSC)* and the *United States Department of State*. More technical information is available in `AS-2023-0002`.

On 2023-01-27 CERT-UA published a *notification* about a cyberattack against the National News Agency of Ukraine (Ukrinform). This attack involved several wipers depending on the attacked platform – AwfulShred, BidSwipe, CaddyWiper, SDelete, and ZeroWipe – and batch files on Windows. It is attributed to the Sandworm group by CERT-UA. We don't have visibility into this incident.

SEDNIT

[Click here for Sednit group description]

Figure 24. Sednit APT group victimology map

During 2022-12 and 2023-01, we collected several phishing emails to Gmail and Yahoo users that we believe with high confidence to have been sent by the Sednit group. In 2022-12, we collected Sednit phishing emails that use

* This report and its contents have been provided for distribution within your organization only. Downloaded on 2023-02-07 11:45:00 by customer 5d48.

Figure 2 Extrait d'un rapport mensuel d'ESET. Tels qu'ils sont présentés, ces rapports contiennent des informations sur les pays et les secteurs ciblés, ainsi que différentes cartes et chronologies.

Conclusion

Comprendre le Threat Intelligence peut vous aider à réaliser l'importance de la perspective contextuelle sur le paysage des menaces.

Répondre aux besoins de votre organisation est un aspect crucial de la conception de votre stratégie de défense, et bien que le Threat Intelligence ne soit pas toujours considéré comme une priorité absolue par certaines organisations, l'expérience pratique et un aperçu détaillé du marché suggèrent qu'il est en train de devenir essentiel.

Ce guide explique ce qu'est le Threat Intelligence, fournit des conseils sur ce qu'il faut rechercher lors du choix d'un fournisseur de TI, se penche sur le marché du TI et sur la façon dont les organisations utilisent ce service, et présente la solution ESET. Tout cela est motivé par le fait que pour devancer les adversaires, il faut toujours disposer de connaissances d'experts bien informées et dignes de confiance.

Ceux qui réalisent le potentiel du TI font souvent appel à plus de cinquante fournisseurs. Ce n'est pas nécessairement le meilleur choix, car la qualité des données et des informations est plus importante que la quantité elle-même. De grandes quantités de données peuvent être collectées, mais sans une véritable structuration et sans intégration avec vos systèmes, s'appuyer sur ces données peut difficilement améliorer votre résilience et votre posture.

C'est là qu'ESET peut être utile en fournissant des moyens complexes de renseignement sur les cybermenaces qui sont basées sur la technologie, la connaissance, l'expertise humaine et une approche sur mesure. Le service fournit des données sélectionnées, pertinentes, fiables et fréquemment actualisées, avec intégration MISP, afin que vous puissiez enquêter sur les incidents, tester des hypothèses et améliorer la recherche de menaces.

À propos d'ESET

Quand la technologie engendre le **progrès**, ESET est là pour le **protéger**.

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour offrir une protection complète et multicouche contre les menaces de cybersécurité aux entreprises et aux particuliers du monde entier.

ESET est depuis longtemps un pionnier des technologies de machine learning et dans le Cloud qui préviennent, détectent et traitent les malwares. ESET est une société privée qui encourage la recherche et le développement scientifiques dans le monde entier.

Canon

protégé par ESET depuis 2016
plus de 32 000 endpoints

partenaire FAI depuis 2008
2 millions d'utilisateurs

Allianz Suisse

protégé par ESET depuis 2016
plus de 4 000 boîtes mail

MITSUBISHI MOTORS
Drive your Ambition

protégé par ESET depuis 2017
plus de 9 000 endpoints

+ 30
années d'expertise

+ 1 Mrd
d'internautes protégés

+ 400 k
entreprises clientes

195
pays et territoires

13
centres de recherche

Besoin de renseignements ?
Contactez-nous :

01 55 89 08 85
clientsfinaux@eset-nod32.fr

Scannez ce code QR pour télécharger nos documentations ou obtenir gratuitement une version d'évaluation de nos solutions

www.eset.com/fr

Plus de 30 ans d'innovation continue

1er éditeur Européen de solutions de sécurité

Focus continu sur la technologie

Croissance continue depuis sa création