

<https://tryhackme.com/room/jrsecanalystintroxo>

1) Framework cyberdéfense	3
Junior Security Analyst Intro	3
Pyramide de la douleur	8
Valeurs de hachage (Trivial)	8
CyberKillchain	22
Unified Kill Chain	31
Unified Kill Chain	31
Diamond Model	42
MITRE	55
Questions sur le framework ATT&CK	60
Cyber Analytics Repository (CAR)	61
Questions CAR	62
MITRE ENGAGE	64
MITRE D3FEND	67
Plan d'émulation d'att&ck (emulations plans)	68
ATT&CK® et Threat Intelligence	69
Conclusion	70
Endpoint Security (petite parenthèse)	70
2) Cyber Threat Intelligence	72
Introduction à Cyber Threat Intel	72
Cyber Threat Intelligence	72
Cycle de vie CTI (lifecycle)	75
CTI Standards & Frameworks	77
Threat Intelligence Tools	81
Urlscan.io	81
Abuse.ch	85
PhishTool : outil pour analyser des mails de phishing potentiels	91
Cisco Talos Intelligence	94
Scénario 1	98
Scenario 2	100
YARA	102
Tâche 3 Déployer	103
Création d'un fichier nommé myfirstrule.yar	105
Vérifier que notre exemple de règle est correct	106
Tâche 5 Développer les règles Yara	107
Cordes	107
Conditions	109
Anatomie d'une règle Yara	111
Tâche 6 Modules Yara	113

Intégration avec d'autres bibliothèques	113
Coucou	113
PythonPE	113
Tâche 7 Autres outils et Yara	113
Outils Yara	113
LOKI (Quoi, pas qui, est Loki ?)	113
THOR (programmes nommés de super-héros pour un teamer bleu de super-héros)	115
FENRIR (convention de nommage toujours à thème mythique)	117
YAYA (Encore un autre automate Yara)	118
Tâche 8 Utiliser LOKI et son ensemble de règles Yara	119
Répondre aux questions ci-dessous	120
À quelle règle Yara correspondait-il ?	121
Comment Loki classe-t-il ce fichier ?	122
Quel est le nom et la version de cet outil de hack ?	124
Tâche 9 Créer des règles Yara avec yarGen	129
Créer des règles Yara avec yarGen	129
Mise à jour de yarGen	133
Répondre aux questions ci-dessous	135
Quel est le nom de la variable pour la chaîne sur laquelle elle correspond ?	137
Tâche 10 Valhalla	139
Valhalla	139
Tâche 11 Conclusion	152
OPENCTI	153
MISP	191
Network security and traffic analysis	209
Traffic Analysis essentials	209
Snort	210

1)Framework cyberdefense

Découvrez les cadres et les politiques qui aident à établir une bonne posture de sécurité.
Découvrez comment les organisations les utilisent dans des stratégies défensives.

Junior Security Analyst Intro

Une carrière en tant qu'analyste de sécurité junior (associé)

Dans le rôle d'analyste de sécurité junior, vous serez un spécialiste du triage. Vous passerez beaucoup de temps à trier ou à surveiller les journaux d'événements et les alertes.

Les responsabilités d'un analyste de sécurité junior ou d'un analyste SOC de niveau 1 comprennent :

- Surveiller et enquêter sur les alertes (la plupart du temps, il s'agit d'un environnement d'exploitation SOC 24h/24 et 7j/7)
- Configurer et gérer les outils de sécurité
- Développer et implémenter des signatures [IDS \(Intrusion Detection System\) de base](#)
- Participer aux groupes de travail, aux réunions du SOC
- Créer des tickets et faire remonter les incidents de sécurité au niveau 2 et au chef d'équipe si nécessaire

Qualifications requises (les plus courantes) :

- 0 à 2 ans d'expérience dans les opérations de sécurité
- Compréhension de base de la mise en réseau (modèle OSI (Open Systems Interconnection Model) ou modèle TCP/IP (Transmission Control Protocol/Internet Protocol Model)), des systèmes d'exploitation (Windows, Linux), des applications Web. Pour en savoir plus sur les modèles OSI et TCP/IP, veuillez consulter la [salle de mise en réseau d'introduction](#).
- Des compétences en script/programmation sont un plus

Attestation souhaitée :

- [Sécurité CompTIA+](#)

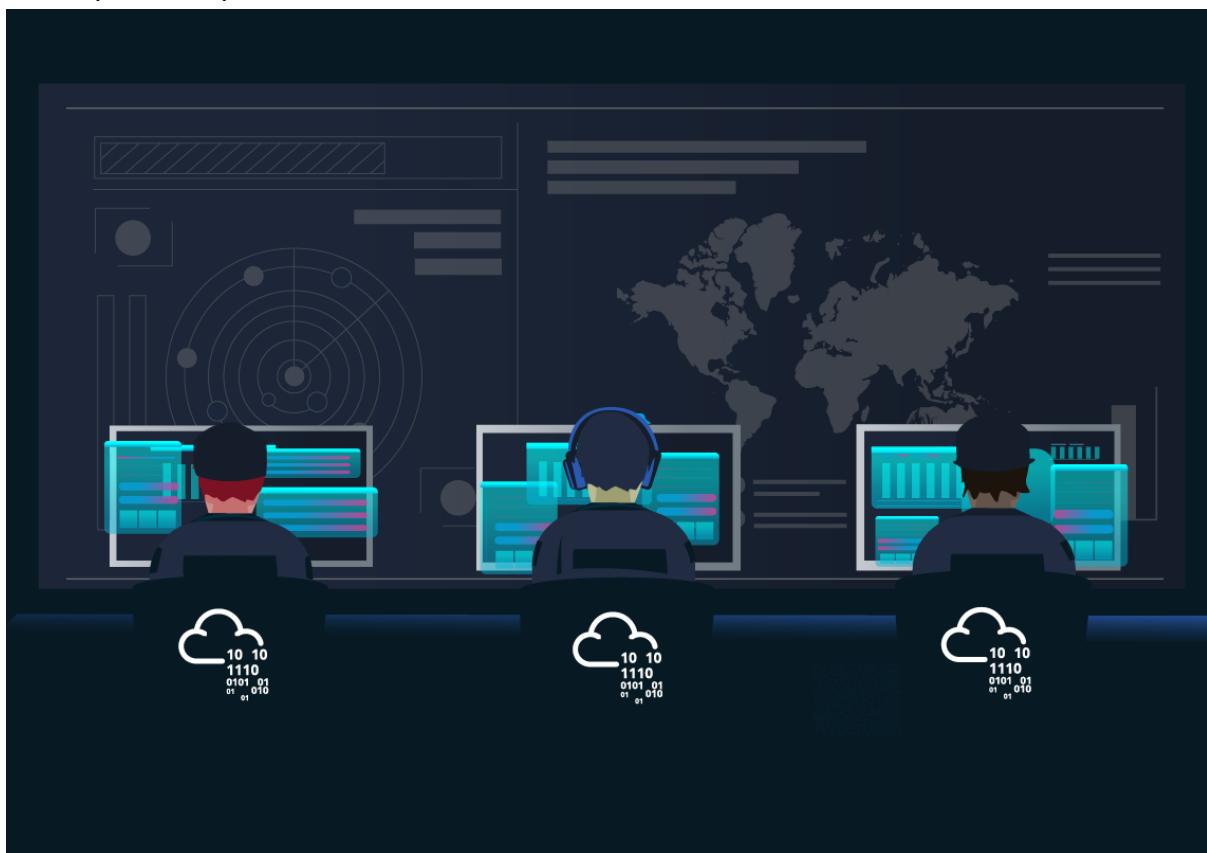
Au fur et à mesure que vous progressez et améliorez vos compétences en tant qu'analyste de sécurité junior, vous passerez éventuellement au niveau 2 et au niveau 3.

Un aperçu du modèle à trois niveaux du centre des opérations de sécurité (SOC) :



Centre des opérations de sécurité (SOC)

Alors, qu'est-ce qu'un SOC exactement ?



La fonction principale d'un SOC (Security Operations Center) est d'enquêter, de surveiller, de prévenir et de répondre aux menaces dans le domaine cybernétique 24 heures sur 24, 7 jours sur 7 ou 24 heures sur 24. Selon [la définition de McAfee d'un SOC](#), « les équipes des opérations de sécurité sont chargées de surveiller et de protéger de nombreux actifs, tels que la propriété intellectuelle, les données du personnel, les systèmes commerciaux et

l'intégrité de la marque. En tant que composant de mise en œuvre du cadre global de cybersécurité d'une organisation, les opérations de sécurité agissent comme point central de collaboration dans des efforts coordonnés pour surveiller, évaluer et se défendre contre les cyberattaques ». Le nombre de personnes travaillant dans le SOC peut varier en fonction de la taille de l'organisation.

Qu'est-ce qui est inclus dans les responsabilités du SOC ?



Préparation et Prévention

En tant qu'analyste de sécurité junior, vous devez rester informé des menaces actuelles en matière de cybersécurité (Twitter et [Feedly](#) peuvent être d'excellentes ressources pour suivre l'actualité liée à la cybersécurité). Il est crucial de détecter et de chasser les menaces, de travailler sur une [feuille de route de sécurité](#) pour protéger l'organisation et d'être prêt pour le pire des scénarios.

Les méthodes de prévention comprennent la collecte de données de renseignement sur les dernières menaces, les acteurs de la menace et leurs [TTP \(tactiques, techniques et procédures\)](#). Il comprend également les procédures de maintenance telles que la mise à jour des signatures de pare-feu, la correction des vulnérabilités dans les systèmes existants,

les applications de liste de blocage et de liste sécurisée, les adresses e-mail et les adresses IP.

Pour mieux comprendre les TTP :

<https://youtu.be/NlhRvGuYx0A?t=264>

, vous devriez consulter l'une des alertes de la CISA (Cybersecurity & Infrastructure Security Agency) sur APT40 (Chinois Advanced Persistent Threat). Consultez le lien suivant pour plus d'informations, <https://us-cert.cisa.gov/ncas/alerts/aa21-200a> .

Surveillance et enquête

Une équipe SOC utilise de manière proactive les outils [SIEM \(Security information and event management\)](#) et [EDR \(Endpoint Detection and Response\)](#) pour surveiller les activités réseau suspectes et malveillantes. Imaginez être un pompier et avoir un incendie à plusieurs alarmes - des incendies à une alarme, des incendies à deux alarmes, des incendies à trois alarmes ; les catégories classent la gravité de l'incendie, qui est une menace dans notre cas. En tant qu'analyste de la sécurité, vous apprendrez à hiérarchiser les alertes en fonction de leur niveau : faible, moyen, élevé et critique. Bien sûr, il est facile de deviner que vous devrez commencer par le niveau le plus élevé (critique) et travailler vers le bas - Alerta de niveau bas. La mise en place d'outils de surveillance de la sécurité correctement configurés vous donnera les meilleures chances d'atténuer la menace.

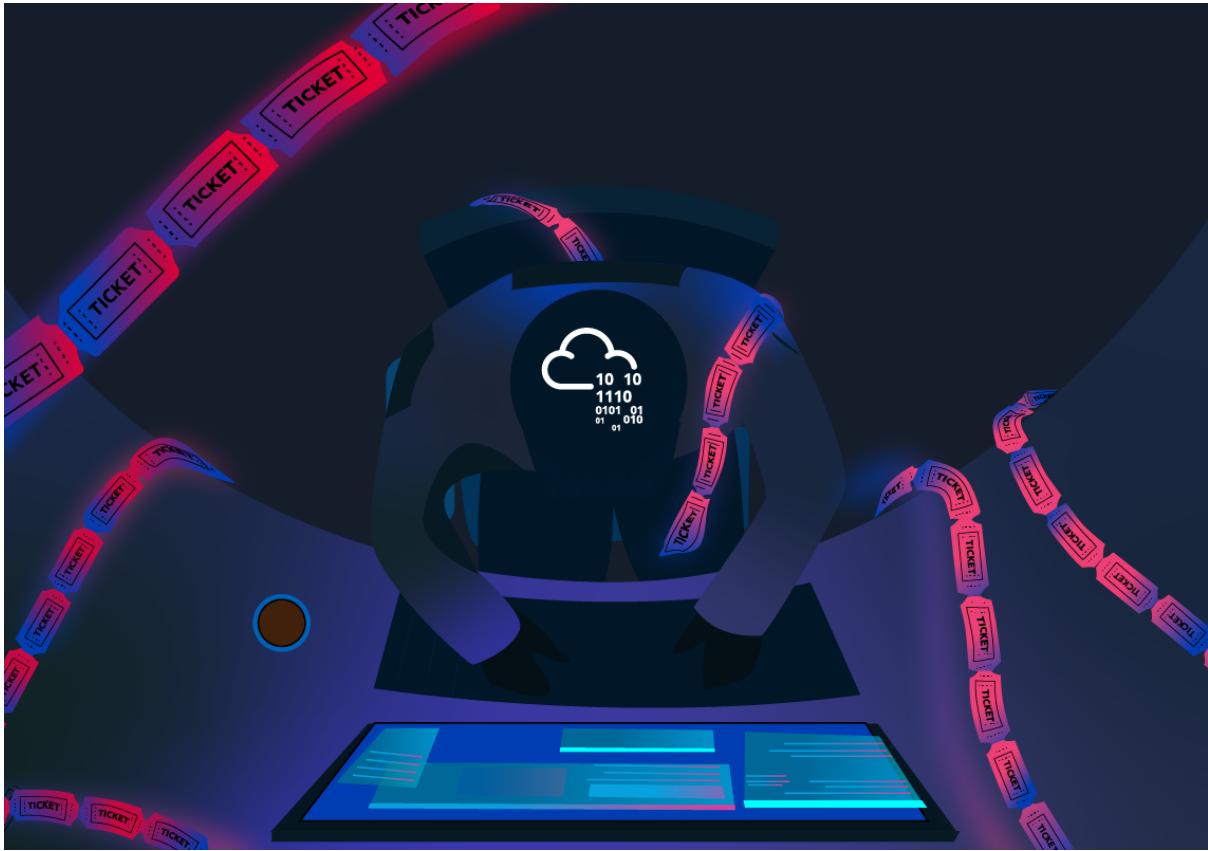
Les analystes de sécurité juniors jouent un rôle crucial dans la procédure d'enquête. Ils effectuent un tri des alertes en cours en explorant et en comprenant le fonctionnement d'une certaine attaque et en empêchant les mauvaises choses de se produire si elles le peuvent. Au cours de l'enquête, il est important de se poser la question "Comment ? Quand et pourquoi ?". Les analystes de sécurité trouvent les réponses en explorant les journaux de données et les alertes en combinaison avec l'utilisation d'outils open source, que nous aurons l'occasion d'explorer plus tard dans ce chemin.

Réponse

Après l'enquête, l'équipe SOC coordonne et prend des mesures sur les hôtes compromis, ce qui implique d'isoler les hôtes du réseau, de mettre fin aux processus malveillants, de supprimer des fichiers, etc.

Une journée dans la vie d'un analyste de sécurité junior (associé)

Voir le site



Pour comprendre les responsabilités professionnelles d'un analyste de sécurité junior (associé), laissez-nous d'abord vous montrer à quoi ressemble une journée dans la vie de l'analyste de sécurité junior et pourquoi il s'agit d'un parcours de carrière passionnant. Être en première ligne n'est pas toujours facile et peut être très difficile car vous travaillerez avec diverses sources de journaux provenant de différents outils que nous vous guiderons tout au long de ce chemin. Vous aurez la possibilité de surveiller le trafic réseau, y compris les alertes IPS (Intrusion Prevention System) et IDS (Intrusion Detection System), les e-mails suspects, extraire les données médico-légales pour analyser et détecter les attaques potentielles, utiliser l'intelligence open source pour vous aider prendre les décisions appropriées sur les alertes.

L'une des choses les plus excitantes et les plus gratifiantes est lorsque vous avez fini de travailler sur un incident et que vous avez réussi à remédier à la menace. La réponse aux incidents peut prendre des heures, des jours ou des semaines ; tout dépend de l'ampleur de l'attaque : l'attaquant a-t-il réussi à exfiltrer les données ? Combien de données l'attaquant parvient-il à exfiltrer ? L'attaquant a-t-il tenté de pivoter vers d'autres hôtes ? Il y a beaucoup de questions à poser et beaucoup de détection, de confinement et de remédiation à faire. Nous vous guiderons à travers certaines connaissances fondamentales que chaque analyste de sécurité junior (associé) doit connaître pour devenir un défenseur du réseau performant.

La première chose que presque tous les analystes de sécurité juniors (associés) font pendant leur quart de travail est de regarder les tickets pour voir si des alertes ont été générées.

Êtes-vous prêt à vous immerger un peu dans le rôle d'analyste de sécurité junior ?

Répondre aux questions ci-dessous

Cliquez sur le bouton vert Afficher le site dans cette tâche pour ouvrir le laboratoire de site statique et accédez à l'outil de surveillance de la sécurité sur le panneau de droite pour essayer d'identifier l'activité suspecte.

Aucune réponse nécessaire	Question terminée
Quelle était l'adresse IP malveillante dans les alertes ?	Bonne réponse
221.181.185.159	
À qui avez-vous transmis l'événement associé à l'adresse IP malveillante ?	Bonne réponse
Will Griffin	
Après avoir bloqué l'adresse IP malveillante sur le pare-feu, quel message l'acteur malveillant vous a-t-il laissé ?	Bonne réponse
THM{UNTIL-WE-MEET-AGAIN}	

Pyramide de la douleur

<https://tryhackme.com/room/pyramidofpainax>

Introduction

Ce concept bien connu est appliqué à des solutions de cybersécurité telles que [Cisco Security](#), [SentinelOne](#) et [SOCRadar](#) pour améliorer l'efficacité des exercices CTI (Cyber Threat Intelligence), de chasse aux menaces et de réponse aux incidents.

Il est important de comprendre le concept de Pyramid of Pain en tant que Threat Hunter, Incident Responder ou SOC Analyst.

Êtes-vous prêt à explorer ce qui se cache à l'intérieur de la Pyramide de la douleur ?

Valeurs de hachage (Trivial)

Selon Microsoft, la valeur de hachage est une valeur numérique d'une longueur fixe qui identifie de manière unique les données. Une valeur de hachage est le résultat d'un algorithme de hachage. Voici quelques-uns des algorithmes de hachage les plus courants :

- MD5 (Message Digest, défini par [RFC 1321](#)) - a été conçu par Ron Rivest en 1992 et est une fonction de hachage cryptographique largement utilisée avec une valeur de hachage de 128 bits. Les hachages MD5 ne sont PAS considérés comme cryptographiquement sécurisés. En 2011, l'IETF a publié la RFC 6151, "[Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms](#)", qui mentionnait un certain nombre d'attaques contre les hachages MD5, y compris la collision de hachage.
- SHA-1 (Secure Hash Algorithm 1, défini par [RFC 3174](#)) - a été inventé par l'Agence de sécurité nationale des États-Unis en 1995. Lorsque les données sont transmises à l'algorithme de hachage SHA-1, SHA-1 prend une entrée et produit un hachage de 160 bits. chaîne de valeur sous la forme d'un nombre hexadécimal à 40 chiffres. [Le NIST a déconseillé l'utilisation de SHA-1 en 2011](#) et a interdit son utilisation pour les signatures numériques à la fin de 2013 en raison de sa sensibilité aux attaques par

force brute. Au lieu de cela, le NIST recommande de migrer de SHA-1 vers des algorithmes de hachage plus puissants dans les familles SHA-2 et SHA-3.

- Le SHA-2 (Secure Hash Algorithm 2) - SHA-2 Hashing Algorithm a été conçu par le National Institute of Standards and Technology (NIST) et la National Security Agency (NSA) en 2001 pour remplacer SHA-1. SHA-2 a de nombreuses variantes, et sans doute la plus courante est SHA-256. L'algorithme SHA-256 renvoie une valeur de hachage de 256 bits sous la forme d'un nombre hexadécimal à 64 chiffres.

Un hachage n'est pas considéré comme étant cryptographiquement sécurisé si deux fichiers ont la même valeur de hachage ou condensé.

Les professionnels de la sécurité utilisent généralement les valeurs de hachage pour avoir un aperçu d'un échantillon de logiciel malveillant spécifique, d'un fichier malveillant ou suspect, et comme moyen d'identifier et de référencer de manière unique l'artefact malveillant.

Vous avez probablement lu des rapports sur les rançongiciels dans le passé, où les chercheurs en sécurité fourniraient les hachages liés aux fichiers malveillants ou suspects utilisés à la fin du rapport. Vous pouvez consulter [le rapport DFIR](#) et [les blogs FireEye Threat Research](#) si vous souhaitez voir un exemple.

Divers outils en ligne peuvent être utilisés pour effectuer des recherches de hachage comme [VirusTotal](#) et [Metadefender Cloud - OPSWAT](#).

VirusTotal :

The screenshot shows the VirusTotal analysis interface. At the top, there's a search bar with the hash value "3f33734b2d34cce83936ce99c3494cd845f1d2c02d7f6da31d42dfc1ca15a171". To the right of the search bar are various icons for file types (PDF, DOC, XLS, etc.) and a "Sign in" button. Below the search bar, a circular progress bar indicates "14 / 59" detections. A red circle with a white exclamation mark and the text "14 security vendors flagged this file as malicious" is prominently displayed. The main content area shows the file name "m_croetian.wnry" and its file type "rtf". It also displays the file size "38.15 KB", the upload date "2021-07-09 02:43:46 UTC", and the fact that it was uploaded "28 days ago". On the right side, there's a "RTF" download link. Below this, there's a table titled "DETECTION" with columns for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The table lists 14 detections from various vendors:

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Anti-AVL	(1) Trojan/Generic.ASSuf.19EC8		CAT-QuickHeal	(1) RTF.Trojan.Agent.40329
Comodo	(1) Malware@#1t7uob1a9vm9d		ESET-NOD32	(1) Win32/Filecoder/WannaCryptor.D
Gridinsoft	(1) Ransom.U.Ransom.oa		Ikarus	(1) Trojan.Win32.Filecoder
Lionic	(1) Trojan.MSOffice.Generic.4lc		McAfee	(1) RTF/Wannacry.a
McAfee-GW-Edition	(1) RTF/Wannacry.a		Microsoft	(1) Ransom:Win32/WannaCrypt.Alrsm
Symantec	(1) Trojan.Gen.NPE.2		Tencent	(1) Win32.Trojan.Filecoder.Dvzt
TrendMicro	(1) TROJ_RANSOMNOTE.RTF		TrendMicro-HouseCall	(1) TROJ_RANSOMNOTE.RTF

Sous le hachage dans la capture d'écran ci-dessus, vous pouvez voir le nom du fichier. Dans ce cas, il s'agit de "m_croetian.wnry"

Cloud MetaDefender - OPSWAT :

The screenshot shows the OPSWAT interface for a file named E325988F68D327743926EA317ABB9882F347.... At the top, there's a search bar with placeholder text "File, URL, IP address, Domain, Hash, or CVE", a "Process" button, and a gear icon for settings. To the right are links for "English", "Sign In", "Licensing", and a menu icon.

Below the header, the "Overview" tab is selected, showing the threat name "Trojan/WcrylyBhUK2kw". There are links to "Sanitized version", "Static Analysis", and "Community".

The main content area is divided into three columns:

- Metascan**: Threats detected: 08 / 34 ENGINES. A large red "08" is prominently displayed.
- Sandbox Threat Score**: No dynamic analysis performed. Shows a score of 00 / 10.
- Community Insight**: User votes: 0%. Includes links to "View full report", "Upgrade limits", "View dynamic analysis", "Sandbox documentation", "View leaderboards", and "Check out our community".

Comme vous l'avez peut-être remarqué, il est très facile de repérer un fichier malveillant si nous avons le hachage dans notre arsenal. Cependant, en tant qu'attaquant, modifier un fichier ne serait-ce que d'un seul bit est trivial, ce qui produirait une valeur de hachage différente. Avec autant de variantes et d'instances de logiciels malveillants ou de rançongiciels connus, la chasse aux menaces à l'aide de hachages de fichiers comme IOC (indicateurs de compromission) peut devenir difficile.

Jetons un coup d'œil à un exemple de la façon dont vous pouvez modifier la valeur de hachage d'un fichier en ajoutant simplement une chaîne à la fin d'un fichier en utilisant echo : File Hash (Before Modification)

```
PS C:\Users\THM\Downloads> Get-FileHash .\OpenVPN_2.5.1_I601_amd64.msi -Algorithm MD5
Algorithm Hash Path
----- -----
MD5      D1A008E3A606F24590A02B853E955CF7
C:\Users\THM\Downloads\OpenVPN_2.5.1_I601_amd64.msi

● ● ● Hachage de fichier (après modification)

PS C:\Users\THM\Downloads> echo "AppendTheHash" >> .\OpenVPN_2.5.1_I601_amd64.msi
PS C:\Users\THM\Downloads> Get-FileHash .\OpenVPN_2.5.1_I601_amd64.msi -Algorithm MD5
Algorithm Hash Path
----- -----
MD5      9D52B46F5DE41B73418F8E0DACEC5E9F
C:\Users\THM\Downloads\OpenVPN_2.5.1_I601_amd64.msi
```

Adresse IP

Vous avez peut-être appris l'importance d'une adresse IP à partir de la section "[Qu'est-ce que la mise en réseau ?](#)" Chambre . l'importance de l'adresse IP. Une adresse IP est utilisée pour identifier tout appareil connecté à un réseau. Ces appareils vont des ordinateurs de bureau aux serveurs et même aux caméras de vidéosurveillance ! Nous nous appuyons sur les adresses IP pour envoyer et recevoir les informations sur le réseau. Mais nous n'allons pas entrer dans la structure et la fonctionnalité de l'adresse IP. Dans le cadre de la Pyramide de la douleur, nous évaluerons comment les adresses IP sont utilisées comme indicateur.

Dans la Pyramide de la douleur, les adresses IP sont indiquées en vert. Vous vous demandez peut-être pourquoi et à quoi vous pouvez associer la couleur verte ?

Du point de vue de la défense, la connaissance des adresses IP utilisées par un adversaire peut être précieuse. Une tactique de défense courante consiste à bloquer, supprimer ou refuser les demandes entrantes provenant d'adresses IP sur votre paramètre ou votre pare-feu externe. Cette tactique n'est souvent pas à l'épreuve des balles car il est trivial pour un adversaire expérimenté de récupérer simplement en utilisant une nouvelle adresse IP publique.

Connexions IP malveillantes ([app.any.run](#)) :

HTTP Requests		0	Connections		4	DNS Requests		4	Threats	0
Timeshift	Protocol	Rep	PID	Process name	CN	IP		Port		
85528 ms	TCP	⚠	1632	some_malicious_file.bi...	🇺🇸	50.87.136.52		443		
144.95 s	TCP	?	1632	some_malicious_file.bi...	🇩🇪	78.46.1.42		443		
205.35 s	TCP	⚠	1632	some_malicious_file.bi...	🇩🇪	134.119.253.108		443		
264.76 s	TCP	⚠	1632	some_malicious_file.bi...	🇺🇸	104.21.87.185		443		

NOTE! N'essayez pas d'interagir avec les adresses IP indiquées ci-dessus.

L'un des moyens par lesquels un adversaire peut rendre difficile l'exécution réussie du blocage IP consiste à utiliser Fast Flux .

Selon [Akamai](#) , Fast Flux est une technique DNS utilisée par les botnets pour dissimuler les activités de phishing, de proxy Web, de diffusion de logiciels malveillants et de communication de logiciels malveillants derrière des hôtes compromis agissant en tant que proxys. Le but de l'utilisation du réseau Fast Flux est de rendre la communication entre les logiciels malveillants et son serveur de commande et de contrôle (C&C) difficile à découvrir par les professionnels de la sécurité.

Ainsi, le concept principal d'un réseau Fast Flux est d'avoir plusieurs adresses IP associées à un nom de domaine, qui change constamment. Palo Alto a créé un excellent scénario fictif pour expliquer Fast Flux : ["Fast Flux 101 : Comment les cybercriminels améliorent la résilience de leur infrastructure pour échapper à la détection et aux démantèlements des forces de l'ordre »](#)

Lisez le rapport suivant (généré à partir de [any.run](#)) pour cet exemple [ici](#) pour répondre aux questions ci-dessous :

Répondre aux questions ci-dessous

Lisez le rapport suivant pour répondre à cette question. Quelle est la **première adresse IP** avec laquelle le processus malveillant (**PID 1632**) tente de communiquer ?

50.87.136.52

Bonne réponse

Indice

Lisez le rapport suivant pour répondre à cette question. Quel est le **premier nom de domaine** avec lequel le processus malveillant ((**PID 1632**) tente de communiquer ?

craftingalegacy.com

Bonne réponse

Indice

Noms de domaine (simples)

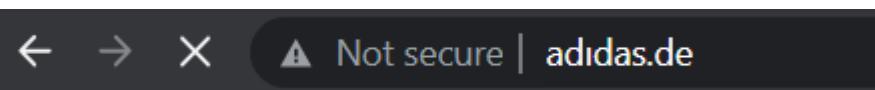
Intensifions la pyramide de la douleur et passons aux noms de domaine. Vous pouvez voir la transition des couleurs - du vert au bleu sarcelle.

Les noms de domaine peuvent être considérés comme un simple mappage d'une adresse IP à une chaîne de texte. Un nom de domaine peut contenir un domaine et un domaine de premier niveau ([evilcorp.com](#)) ou un sous-domaine suivi d'un domaine et d'un domaine de premier niveau ([tryhackme.evilcorp.com](#)). Mais nous n'entrerons pas dans les détails du fonctionnement du Domain Name System (DNS). Vous pouvez en savoir plus sur le DNS dans cette [salle "DNS en détail"](#) .

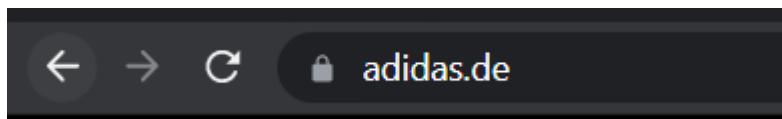
Les noms de domaine peuvent être un peu plus pénibles à changer pour l'attaquant, car il devrait très probablement acheter le domaine, l'enregistrer et modifier les enregistrements DNS . Malheureusement pour les défenseurs, de nombreux fournisseurs DNS ont des normes lâches et fournissent des API pour faciliter encore plus le changement de domaine pour l'attaquant.

Domaines malveillants Sodinokibi C2 (Command and Control Infrastructure) :

Campaign	8254																																																												
C2	<table><tbody><tr><td>boisehosting.net</td><td></td><td>fotoideaymedia.es</td><td></td></tr><tr><td>dubnew.com</td><td></td><td>stallbyggen.se</td><td></td></tr><tr><td>koken-voor-baby.nl</td><td></td><td>juneauopiodworkgroup.org</td><td></td></tr><tr><td>vancouver-print.ca</td><td></td><td>zewatchers.com</td><td></td></tr><tr><td>bouquet-de-roses.com</td><td></td><td>seevilla-dr-sturm.at</td><td></td></tr><tr><td>olejack.ru</td><td></td><td>i-trust.dk</td><td></td></tr><tr><td>wasmachtmeinfonds.at</td><td></td><td>appsformacpc.com</td><td></td></tr><tr><td>friendsandbrgrs.com</td><td></td><td>thenewrejuveme.com</td><td></td></tr><tr><td>xn--singlebrsen-vergleich-nec.com</td><td></td><td>sabel-bf.com</td><td></td></tr><tr><td>semnoc.com</td><td></td><td>ceres.org.au</td><td></td></tr><tr><td>curso porcelanato liquido.online</td><td></td><td>marietteaernoudts.nl</td><td></td></tr><tr><td>tastewilliamsburg.com</td><td></td><td>charlottepoudroux-photographie.fr</td><td></td></tr><tr><td>aselbermachen.com</td><td></td><td>klint2012.info</td><td></td></tr><tr><td>accountancywijchen.nl</td><td></td><td>creamery201.com</td><td></td></tr><tr><td>rerekatu.com</td><td></td><td>makeurvoicetheard.com</td><td></td></tr></tbody></table>	boisehosting.net		fotoideaymedia.es		dubnew.com		stallbyggen.se		koken-voor-baby.nl		juneauopiodworkgroup.org		vancouver-print.ca		zewatchers.com		bouquet-de-roses.com		seevilla-dr-sturm.at		olejack.ru		i-trust.dk		wasmachtmeinfonds.at		appsformacpc.com		friendsandbrgrs.com		thenewrejuveme.com		xn--singlebrsen-vergleich-nec.com		sabel-bf.com		semnoc.com		ceres.org.au		curso porcelanato liquido.online		marietteaernoudts.nl		tastewilliamsburg.com		charlottepoudroux-photographie.fr		aselbermachen.com		klint2012.info		accountancywijchen.nl		creamery201.com		rerekatu.com		makeurvoicetheard.com	
boisehosting.net		fotoideaymedia.es																																																											
dubnew.com		stallbyggen.se																																																											
koken-voor-baby.nl		juneauopiodworkgroup.org																																																											
vancouver-print.ca		zewatchers.com																																																											
bouquet-de-roses.com		seevilla-dr-sturm.at																																																											
olejack.ru		i-trust.dk																																																											
wasmachtmeinfonds.at		appsformacpc.com																																																											
friendsandbrgrs.com		thenewrejuveme.com																																																											
xn--singlebrsen-vergleich-nec.com		sabel-bf.com																																																											
semnoc.com		ceres.org.au																																																											
curso porcelanato liquido.online		marietteaernoudts.nl																																																											
tastewilliamsburg.com		charlottepoudroux-photographie.fr																																																											
aselbermachen.com		klint2012.info																																																											
accountancywijchen.nl		creamery201.com																																																											
rerekatu.com		makeurvoicetheard.com																																																											



Pouvez-vous repérer quelque chose de malveillant dans la capture d'écran ci-dessus ? Maintenant, comparez-le à la vue légitime du site Web ci-dessous :



'est l'un des exemples d'attaque Punycode utilisée par les attaquants pour rediriger les utilisateurs vers un domaine malveillant qui semble légitime à première vue.

Qu'est-ce que Punycode ? Selon [Wandera](#) , "Punycode est un moyen de convertir des mots qui ne peuvent pas être écrits en ASCII, en un encodage Unicode ASCII."

Ce que vous avez vu dans l'URL ci-dessus est `adidas.de` celui qui a le Punycode de <http://xn--addas-o4a.de/>

Internet Explorer, Google Chrome, Microsoft Edge et Apple Safari sont maintenant assez bons pour traduire les caractères obscurcis en nom de domaine Punycode complet.

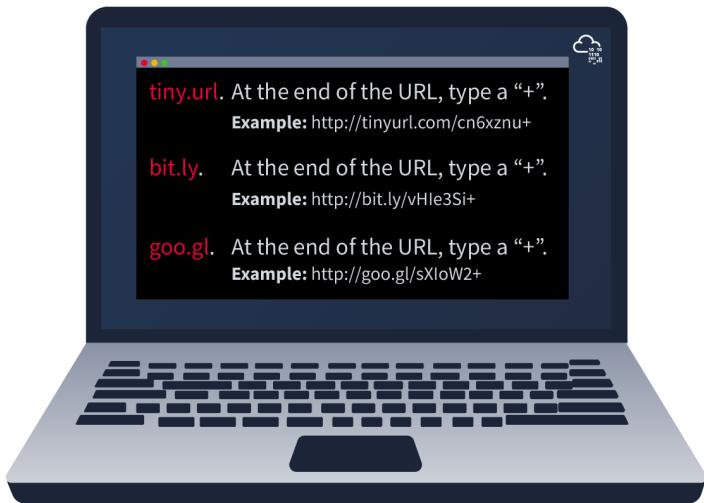
Pour détecter les domaines malveillants, des journaux de proxy ou des journaux de serveur Web peuvent être utilisés.

Les attaquants cachent généralement les domaines malveillants sous des raccourisseurs d'URL. AU RL Shortener est un outil qui crée une URL courte et unique qui redirigera vers le site Web spécifique spécifié lors de l'étape initiale de configuration du lien URL Shortener. Selon [Cofense](#) , les attaquants utilisent les services de raccourcissement d'URL suivants pour générer des liens malveillants :

- bit.ly
- goo.gl
- maintenant
- s.id
- smarturl.it
- minuscule.pl
- petiteurl.com
- x.co

Vous pouvez voir le site Web réel vers lequel le lien raccourci vous redirige en y ajoutant "+" (voir les exemples ci-dessous). Tapez l'URL raccourcie dans la barre d'adresse du navigateur Web et ajoutez les caractères ci-dessus pour voir l'URL de redirection.

REMARQUE : Les exemples de liens raccourcis ci-dessous sont inexistantes.



Affichage des connexions dans Any.run :

Étant donné que Any.run est un service de sandboxing qui exécute l'exemple, nous pouvons examiner toutes les connexions telles que les requêtes HTTP, les requêtes DNS ou les processus communiquant avec une adresse IP. Pour se faire, on peut regarder l'onglet "mise en réseau" situé juste en dessous de l'instantané de la machine.

Remarque : vous devez être extrêmement prudent lorsque vous visitez les adresses IP ou les requêtes HTTP effectuées dans un rapport. Après tout, ce sont des comportements de l'échantillon de malware - ils font donc probablement quelque chose de dangereux !

Requêtes HTTP :

Cet onglet affiche les requêtes HTTP enregistrées depuis la détonation de l'échantillon. Cela peut être utile pour voir quelles ressources sont récupérées à partir d'un serveur Web, comme un dropper ou un rappel.

	HTTP Requests	7	Connections	51	DNS Requests	20	Threats	0	PCAP
	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content	
NETWORK	25853 ms	GET 204: No Content		2572	chrome.exe	US	http://www.gstatic.com/generate_204	-	
FILES	44576 ms	GET 200: OK		2572	chrome.exe	UK	http://cddl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootsrl.cab...	62.3 Kb ↓ compressed	
DEBUG	76052 ms	HEAD 200: OK		852	svchost.exe	US	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/YGkwa4MXjWSuEryWQY...	-	
	81155 ms	GET 200: OK		852	svchost.exe	US	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/YGkwa4MXjWSuEryWQY...	3.72 Kb ↓ binary	
	105777 s	HEAD 200: OK		852	svchost.exe	US	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua62fhpj3rq46nymxtbz...	3.72 Kb ↓ crx	
	110.88 s	GET 206: Partial Con...		852	svchost.exe	US	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua62fhpj3rq46nymxtbz...	7.13 Kb ↓ binary	
		GET 206: Partial Con...		852	svchost.exe	US	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua62fhpj3rq46nymxtbz...	3.11 Kb ↓ binary	

Connexions :

Cet onglet affiche toutes les communications effectuées depuis la détonation de l'échantillon. Cela peut être utile pour voir si un processus communique avec un autre hôte. Par exemple, il peut s'agir de trafic C2 , de chargement/téléchargement de fichiers via FTP, etc.

	HTTP Requests	7	Connections	51	DNS Requests	20	Threats	0	Filter by PID, domain, name or ip	PCAP	
	Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
NETWORK	1309 ms	UDP	?	4	System	[?]	192.168.100.255	138	-	-	↑ 2.21 Kb ↓ -
FILES	1312 ms	UDP	?	1076	svchost.exe	[?]	224.0.0.252	5355	-	-	↑ 48 b ↓ -
DEBUG	1314 ms	UDP	?	3740	svchost.exe	[?]	239.255.255.250	1900	-	-	↑ 1.41 Kb ↓ -
NETWORK	1315 ms	UDP	?	4	System	[?]	192.168.100.255	137	-	-	↑ 1.70 Kb ↓ -
FILES	4397 ms	UDP	?	1076	svchost.exe	[?]	224.0.0.252	5355	-	-	↑ 44 b ↓ -
DEBUG	4399 ms	UDP	?	1076	svchost.exe	[?]	224.0.0.252	5355	-	-	↑ 48 b ↓ -
NETWORK	4405 ms	UDP	?	2044	chrome.exe	[?]	239.255.255.250	1900	-	-	↑ 696 b ↓ -
FILES	4408 ms	UDP	?	1076	svchost.exe	[?]	224.0.0.252	5355	-	-	↑ 44 b ↓ -
DEBUG	5412 ms	TCP	?	2572	chrome.exe	[US]	142.250.185.173	443	accounts.google.com	GOOGLE	No Data
NETWORK	5573 ms	TCP	?	2572	chrome.exe	[US]	142.250.186.142	443	clients2.google.com	GOOGLE	↑ 1.02 Kb ↓ 8.64 Kb

Requêtes DNS :

Cet onglet affiche les requêtes DNS effectuées depuis la détonation de l'échantillon. Les logiciels malveillants effectuent souvent des requêtes DNS pour vérifier la connectivité Internet (c'est-à-dire s'ils ne peuvent pas accéder à Internet/appeler à la maison, ils sont probablement en bac à sable ou inutiles).

	HTTP Requests	7	Connections	51	DNS Requests	20	Threats	0	Filter by IP or domain	PCAP
	Timeshift	Status	Rep	Domain					IP	
NETWORK	5371 ms	Responded	?	ice-eng.app.box.com					74.112.186.144	
FILES	5373 ms	Responded	?	accounts.google.com					142.250.185.173	
DEBUG	5373 ms	Responded	?	clients2.google.com					142.250.186.142	
NETWORK	5374 ms	Responded	?	clients2.googleusercontent.com					142.250.186.97	
FILES	11478 ms	Responded	?	ssl.gstatic.com					142.250.184.227	
DEBUG	25794 ms	Responded	?	www.gstatic.com					142.250.186.99	
NETWORK	27799 ms	Responded	?	cdn01.boxcdn.net					104.16.74.20	
FILES									104.18.103.56	
DEBUG									52.222.206.6	
NETWORK									52.222.206.178	
FILES										
DEBUG										
NETWORK	29500 ms	Responded	?	cdn.amplitude.com						
FILES										
DEBUG										

Répondre aux questions ci-dessous

Accédez à [ce rapport sur app.any.run](#) et fournissez la première requête d'URL **suspecte** que vous voyez, vous utiliserez ce rapport pour répondre aux questions restantes de cette tâche.

craftingalegacy.com

Bonne réponse

Quel terme fait référence à une adresse utilisée pour accéder à des sites Web ?

Domain Name

Bonne réponse

Quel type d'attaque utilise des caractères Unicode dans le nom de domaine pour imiter un domaine connu ?

Punycode attack

Bonne réponse

Fournissez le site Web redirigé pour l'URL raccourcie à l'aide d'un aperçu : <https://tinyurl.com/bw7t8p4u>

<https://tryhackme.com/>

Bonne réponse

Artefacts hôtes (ennuyeux)

Faisons un pas de plus vers la zone jaune.

A ce niveau, l'attaquant se sentira un peu plus ennuyé et frustré si vous pouvez détecter l'attaque. L'attaquant devrait revenir à ce niveau de détection et modifier ses outils et méthodologies d'attaque. Cela prend beaucoup de temps pour l'attaquant, et probablement, il devra dépenser plus de ressources sur les outils de son adversaire.

Les artefacts de l'hôte sont les traces ou les éléments observables que les attaquants laissent sur le système, tels que les valeurs de registre, l'exécution de processus suspects, les modèles d'attaque ou IOC (indicateurs de compromission), les fichiers déposés par des applications malveillantes ou tout ce qui est exclusif à la menace actuelle.

Exécution de processus suspect à partir de Word :

WINWORD.EXE	0.01	51,500 K	134,300 K	3640 Microsoft Word	Microsoft Corporation
 api-ms-win-downlevel-user32-l1-...		4,632 K	11,192 K	3300 EffectDemo MFC Application	

Événements suspects suivis de l'ouverture d'une application malveillante :

Les fichiers modifiés/abandonnés par l'acteur malveillant :

2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd	View	tlb
		MD5: CC11BFD1D6ECC83477B69FF06C6C587	SHA256: A4E8F5821887AC26449C33D9B027CE31BE0E7203DD035C5DC7D34A9AE01A6DA	
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~\$O-100120 CDW-102220.doc	View	pgc
		MD5: 2E7A3442236F2D50C669BC79188BBD69	SHA256: BF007001BACFB8F6ABF371B0B2797B7D13B741879E1E5B76FB616A93431841A9	
3828	PowersheLL.exe	C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe	View	executable
		MD5: 92F58C4E2F524EC53EBE10D914D96CCB	SHA256: 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	
1640	G_jugk.exe	C:\Users\admin\AppData\Local\photowiz\regidle.exe	View	executable
		MD5: 92F58C4E2F524EC53EBE10D914D96CCB	SHA256: 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	

Répondre aux questions ci-dessous

Un fournisseur de sécurité a analysé l'échantillon malveillant pour nous. Consultez le rapport [ici](#) pour répondre aux questions suivantes.

Aucune réponse nécessaire

Question terminée

Un processus nommé **regidle.exe** envoie une requête POST à une adresse IP sur **le port 8080**. Quelle est l'adresse IP ?

96.126.101.6

Bonne réponse

Indice

L'acteur dépose un exécutable malveillant (EXE). Quel est le nom de cet exécutable ?

G_jugk.exe

Bonne réponse

Indice

Regardez ce [rapport](#) de Virustotal. Combien de fournisseurs déterminent que cet hôte est malveillant ?

9

Bonne réponse

Indice

Artefacts de réseau (ennuyeux)

Les artefacts de réseau appartiennent également à la zone jaune de la pyramide de la douleur. Cela signifie que si vous pouvez détecter et répondre à la menace, l'attaquant aura besoin de plus de temps pour revenir en arrière et changer sa tactique ou modifier les outils, ce qui vous donne plus de temps pour réagir et détecter les menaces à venir ou remédier aux menaces existantes.

Un artefact réseau peut être une chaîne d'agent utilisateur, des informations C2 ou des modèles d'URI suivis par les requêtes HTTP POST. Un attaquant peut utiliser une chaîne d'agent utilisateur qui n'a jamais été observée dans votre environnement ou qui semble inhabituelle. L'agent utilisateur est défini par [RFC2616](#) comme le champ d'en-tête de demande qui contient les informations sur l'agent utilisateur à l'origine de la demande. Les artefacts réseau peuvent être détectés dans les PCAP Wireshark (fichier contenant les données de paquets d'un réseau) en utilisant un analyseur de protocole réseau tel que [TShark](#) ou en explorant la journalisation IDS (Intrusion Detection System) à partir d'une source telle que [Snort](#).

Requêtes HTTP POST contenant des chaînes suspectes :

192.168.100.140	194.187.133.160	936	HTTP	POST /Nqd1z/w2BG/ HTTP/1.1
192.168.100.140	98.174.164.72	936	HTTP	POST /ghMuzylCHmW//KmnYdVttxeVy/o2feo8eu7jyv/02M8Wf9SpypCp/yLVEV96eosyd5URJ477/8wdGxz9k9hhJjWp/ HTTP/1.1
192.168.100.140	103.86.49.11	936	HTTP	POST /VCvQqXtjgEehauu/AyEp/09Qn2/R6Rj7Gw9e0v6yJ/fC5a36YfopGe/Q2AwYvSohZiyaEtbb0/ HTTP/1.1
192.168.100.140	78.24.219.147	904	HTTP	POST /jCOC/oQPMPmfJlpM16n3/Pbao/K7oB22aUKQ61a6r/GooMY/ HTTP/1.1
192.168.100.140	50.245.107.73	888	HTTP	POST /ukC1s1jsvd7W/h2VQ1yqB/csuQkgUq1kakhvR39/NCjJodG/ HTTP/1.1
192.168.100.140	110.145.77.103	888	HTTP	POST /QZvvQ6o11/DYk9qgXU/HtoxMCRhbYCjhgamW/5NsCejn3/ HTTP/1.1

Utilisons TShark pour filtrer les chaînes User-Agent en utilisant la commande suivante :
`tshark --Y http.request -T fields -e http.host -e http.user_agent -r analysis_file.pcap`

```
(kali㉿kali)-[~/Desktop]
$ tshark -Y http.request -T fields -e http.user_agent -r analysis.pcap

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
```

Ce sont les chaînes d'agent utilisateur les plus courantes trouvées pour le [cheval de Troie Emotet Downloader](#)

Si vous pouvez détecter les chaînes User-Agent personnalisées que l'attaquant utilise, vous pourrez peut-être les bloquer, créant ainsi plus d'obstacles et rendant leur tentative de compromettre le réseau plus ennuyeuse.

Répondre aux questions ci-dessous

Quel navigateur utilise la chaîne User-Agent affichée dans la capture d'écran ci-dessus ?

Internet Explorer

Bonne réponse

Indice

Combien y a-t-il de requêtes POST dans la capture d'écran du fichier pcap ?

6

Bonne réponse

règle YARA = règles qui permettent de détecter des malwares (à partir de règles établies en copiant des samples de malware : hexa, chaîne de carac ...)

<https://www.sekoia.io/fr/glossaire/regle-yara/#:~:text=Apparu%20en%202007%2C%20YARA%20est,entreprises%20sp%C3%A9cialis%C3%A9es%20dans%20la%20cybers%C3%A9curit%C3%A9>

hachage flou = fuzzy haching

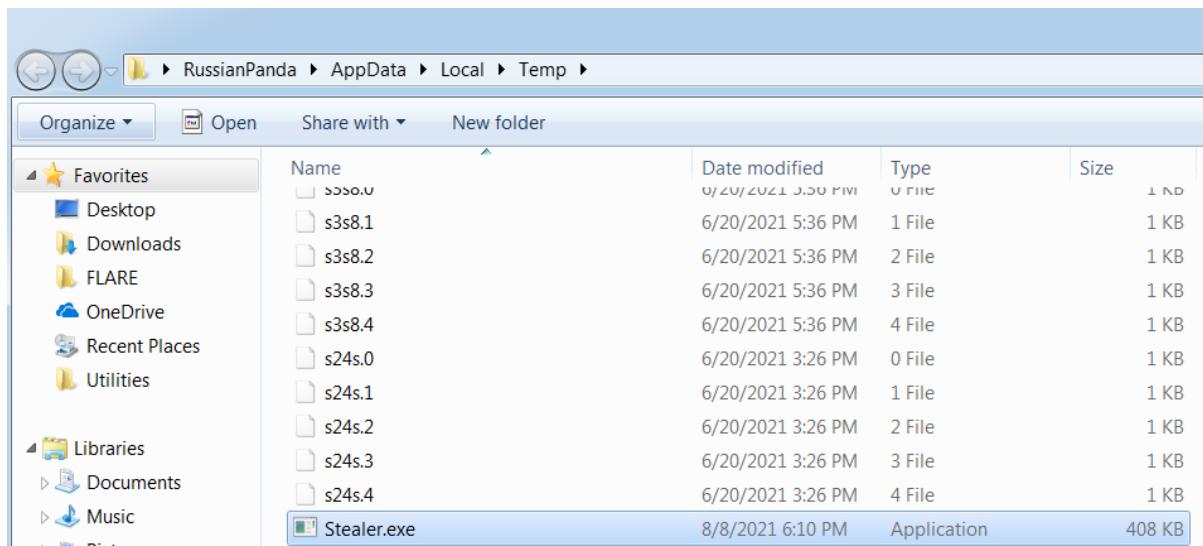
Outils (difficile)

Toutes nos félicitations! Nous avons atteint la partie difficile pour les adversaires !

À ce stade, nous avons amélioré nos capacités de détection contre les artefacts. L'attaquant renoncerait très probablement à essayer de s'introduire dans votre réseau ou reviendrait en arrière et essaierait de créer un nouvel outil ayant le même objectif. Ce sera un jeu terminé pour les attaquants car ils devront investir de l'argent dans la construction d'un nouvel outil (s'ils sont capables de le faire), trouver l'outil qui a le même potentiel, ou même suivre une formation pour apprendre à maîtriser un certain outil.

Les attaquants utiliseraient les utilitaires pour créer des documents de macro malveillants (maldocs) pour les tentatives de harponnage, une porte dérobée qui peut être utilisée pour établir [C2 \(Command and Control Infrastructure\)](#), tout .EXE personnalisé et . Fichiers DLL , charges utiles ou craqueurs de mots de passe.

Un cheval de Troie a déposé le fichier suspect "Stealer.exe" dans le dossier Temp :



L'exécution du binaire suspect :

	payload.exe	1356	12.09 MB	WIN-31...\\RussianPanda
	Stealer.exe	2928	11.63 MB	WIN-31...\\RussianPanda Galactus

Les signatures antivirus, les règles de détection et les règles YARA peuvent être d'excellentes armes à utiliser contre les attaquants à ce stade.

[MalwareBazaar](#) et [Malshare](#) sont de bonnes ressources pour vous donner accès aux échantillons, aux flux malveillants et aux résultats YARA - tout cela peut être très utile en matière de chasse aux menaces et de réponse aux incidents.

Pour les règles de détection, [SOC Prime Threat Detection Marketplace](#) est une excellente plateforme, où les professionnels de la sécurité partagent leurs règles de détection pour différents types de menaces, y compris les derniers CVE qui sont exploités à l'état sauvage par des adversaires.

Le hachage flou (fuzzy hashing) est également une arme puissante contre les outils de l'attaquant. Le hachage flou vous aide à effectuer une analyse de similarité - faites correspondre deux fichiers avec des différences mineures en fonction des valeurs de hachage floues. L'un des exemples de hachage flou est l'utilisation de [SSDeep](#) ; sur le site officiel de SSDeep, vous pouvez également trouver l'explication complète du hachage flou. Exemple de SSDeep de VirusTotal :

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY 13 +
Basic Properties ⓘ				
MD5	9498ff82a64ff445398c8426ed63ea5b			
SHA-1	36f9ca40b3ce96fce1cf1d4a7222935536fd25b			
SHA-256	8b2e701e91101955c73865589a4c72999aeabc11043f712e05fdb1c17c4ab19a			
Vhash	025056657d755510804011z9005b9z25z12z3afz			
Authentihash	ad56160b465f7bd1e7568640397f01fc4f8819ce6f0c1415690eceee646464cec			
Imphash	d7584447a5c5ca9b4a55946317137951			
Rich PE header hash	fa4dbca9180170710b3c245464efa483			
SSDEEP	6144:Gz90qLc1zR98hUb4UdzEwG+vqAWiR4ExEPbix67CNzjX:Gz90qLc1WhUhVqJPbiQ7CNzb			
TLSH	T1DB44CF267660D833D0DF94316C75C3F9673BFC2123215A6B6A4417699E307E0AE7839E			
File type	Win32 EXE			
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit			
TrID	Win32 Executable MS Visual C++ (generic) (48.8%)			
TrID	Win64 Executable (generic) (16.4%)			
TrID	Win32 Dynamic Link Library (generic) (10.2%)			
TrID	Win16 NE executable (generic) (7.8%)			
TrID	Win32 Executable (generic) (7%)			
File size	249.00 KB (254976 bytes)			

Répondre aux questions ci-dessous

Indiquez la méthode utilisée pour déterminer la similarité entre les fichiers

Fuzzy hashing

Bonne réponse

Fournissez le nom alternatif pour les hachages flous sans l'abréviation

context triggered piecewise hashes

Bonne réponse

Indice

TTP (difficiles)

Ce ne est pas encore terminée. Mais bonne nouvelle, nous avons atteint l'étape finale ou le sommet de la Pyramide de la douleur !

TTTP signifie Tactiques, Techniques et Procédures. Cela inclut l'ensemble de la matrice [MITRE ATT&CK](#), c'est-à-dire toutes les mesures prises par un adversaire pour atteindre son objectif, des tentatives de phishing à la persistance et à l'exfiltration de données. Si vous pouvez détecter et répondre rapidement aux TTP, vous ne laissez presque aucune chance aux adversaires de riposter. Par exemple, si vous pouviez détecter une attaque [Pass-the-Hash](#) à l'aide de Windows Event Log Monitoring et y remédier, vous seriez en mesure de trouver très rapidement l'hôte compromis et d'arrêter le mouvement latéral à l'intérieur de votre réseau . À ce stade, l'attaquant aurait deux options :

1. Revenir en arrière, faire plus de recherche et de formation, reconfigurer leurs outils personnalisés
2. Abandonner et trouver une autre cible

L'option 2 semble certainement moins consommatrice de temps et de ressources.

Answer the questions below

Navigate to ATT&CK Matrix webpage. How many techniques fall under the Exfiltration category?

9

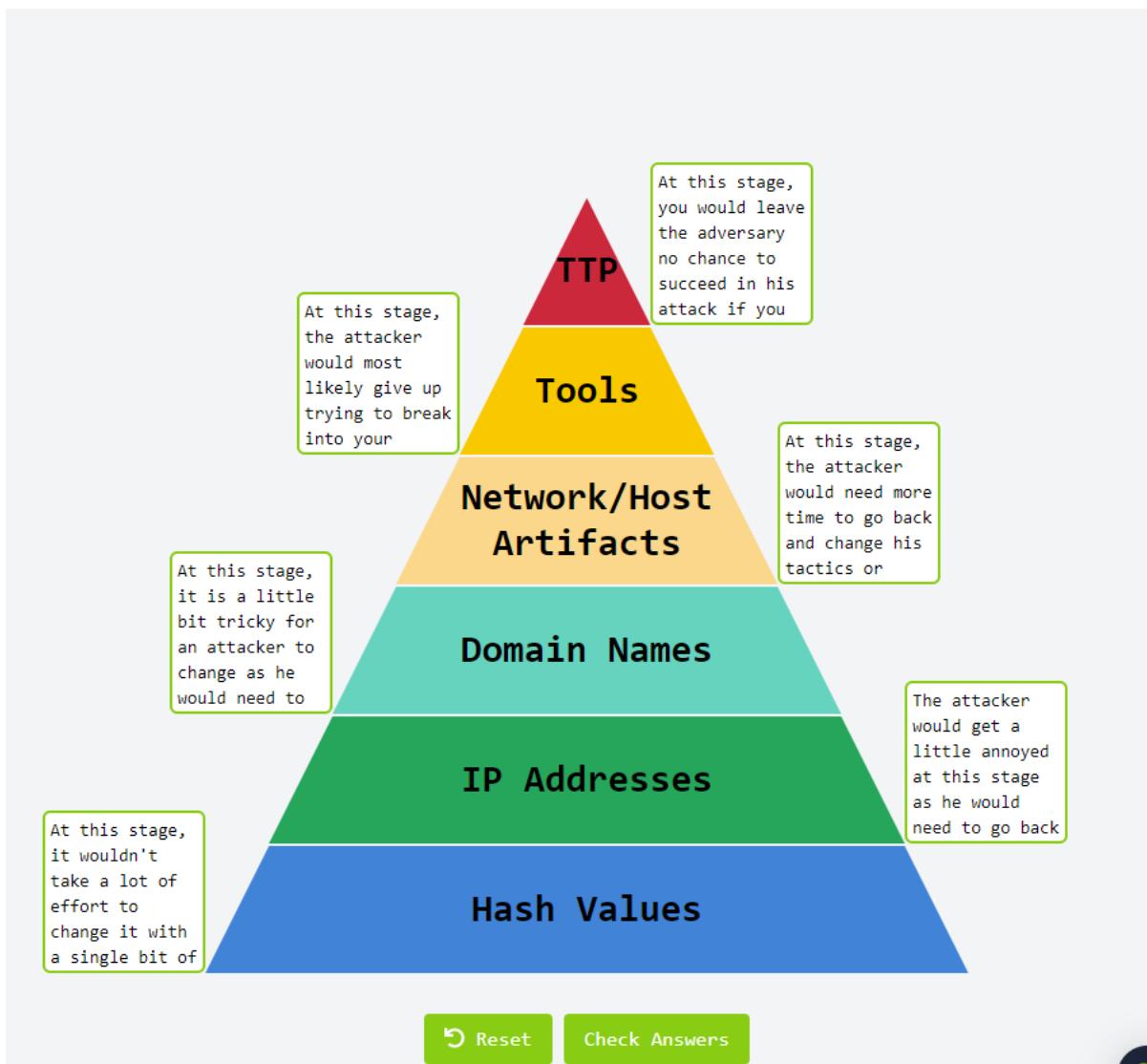
Correct Answer

Chimera is a China-based hacking group that has been active since 2018. What is the name of the commercial, remote access tool they use for C2 beacons and data exfiltration?

Cobalt Strike

Correct Answer

💡 Hint



Conclusion

Vous avez maintenant appris le concept de la pyramide de la douleur. Il est peut-être temps de mettre cela en pratique. Veuillez accéder au site statique pour effectuer l'exercice. Vous pouvez choisir n'importe quel APT (Advanced Persistent Threat Groups) comme autre exercice. Un bon endroit à regarder serait [FireEye Advanced Persistent Threat Groups](#). Lorsque vous avez déterminé le groupe APT que vous souhaitez rechercher, recherchez ses indicateurs et demandez-vous : " Que puis-je faire ou quelles règles de détection et quelle

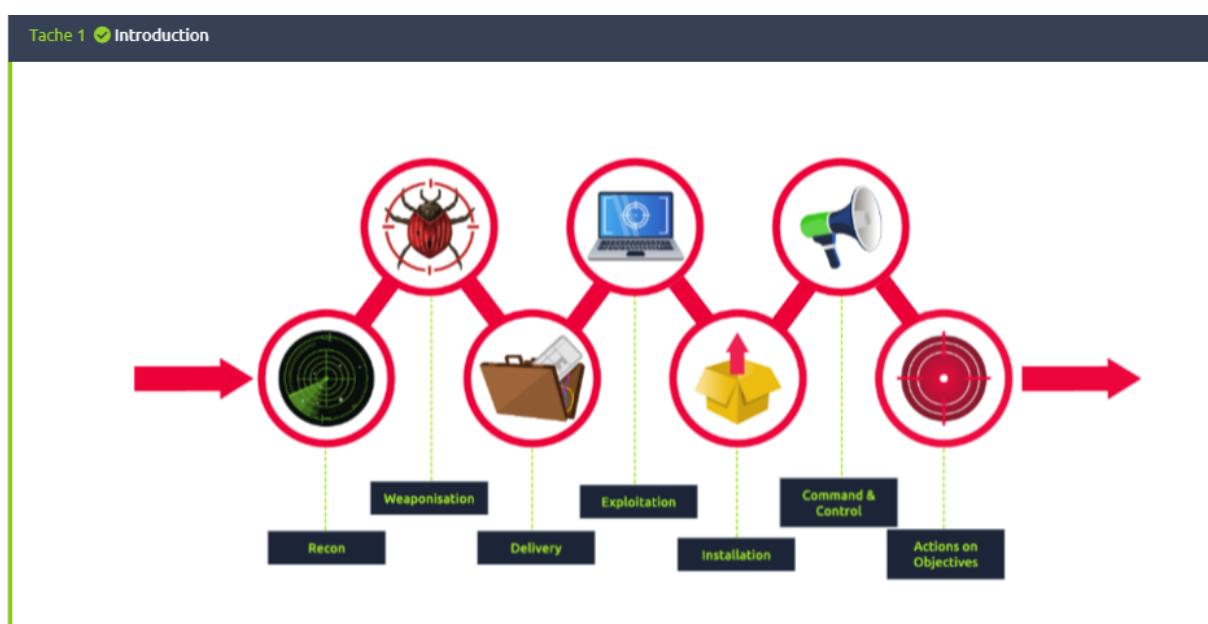
approche puis-je créer pour détecter l'activité de l'adversaire ?", et " Où se situe cette activité ou cette détection ? sur la Pyramide de la Douleur ? »

Comme l'affirme David Blanco, " la quantité de douleur que vous causez à un adversaire dépend des types d'indicateurs que vous êtes en mesure d'utiliser.".

CyberKillchain

Introduction

Le framework Cyber Kill Chain est conçu pour l'identification et la prévention des intrusions sur le réseau. Vous apprendrez ce que les adversaires doivent faire pour atteindre leurs objectifs.



Le terme kill chain est un concept militaire lié à la structure d'une attaque. Il consiste en l'identification de la cible, la décision et l'ordre d'attaquer la cible, et enfin la destruction de la cible.

Merci à Lockheed Martin, une entreprise mondiale de sécurité et d'aérospatiale, qui a établi le cadre Cyber Kill Chain® pour l'industrie de la cybersécurité en 2011 sur la base du concept militaire. Le cadre définit les étapes utilisées par les adversaires ou les acteurs malveillants dans le cyberspace. Pour réussir, un adversaire doit passer par toutes les phases de la Kill Chain. Nous passerons par les phases d'attaque et vous aiderons à mieux comprendre les adversaires et leurs techniques utilisées dans l'attaque pour vous défendre.

Alors, pourquoi est-il important de comprendre le fonctionnement de Cyber Kill Chain ?

La Cyber Kill Chain vous aidera à comprendre et à vous protéger contre les attaques de ransomwares, les failles de sécurité ainsi que les menaces persistantes avancées (APT). Vous pouvez utiliser la Cyber Kill Chain pour évaluer la sécurité de votre réseau et de votre système en identifiant les contrôles de sécurité manquants et en comblant certaines lacunes de sécurité en fonction de l'infrastructure de votre entreprise.

En comprenant la Kill Chain en tant qu'analyste SOC , chercheur en sécurité, chasseur de menaces ou intervenant en cas d'incident, vous serez en mesure de reconnaître les tentatives d'intrusion et de comprendre les buts et objectifs de l'intrus.

Nous allons explorer les phases d'attaque suivantes dans cette salle :

- Reconnaissance
- Armement
- Livraison
- Exploitation
- Installation
- Commandement et contrôle
- Actions sur les objectifs

Objectifs d'apprentissage : Dans cette salle, vous découvrirez chaque phase du cadre Cyber Kill Chain, les avantages et les inconvénients de la Cyber Kill Chain traditionnelle.

Résultat : En conséquence, vous serez prêt à reconnaître les différentes phases ou étapes de l'attaque menée par un adversaire et serez en mesure de briser la "chaîne de destruction".

Reconnaissance

Pour savoir ce qu'est la reconnaissance du point de vue de l'attaquant, définissons d'abord le terme reconnaissance.

La reconnaissance consiste à découvrir et à collecter des informations sur le système et la victime. La phase de reconnaissance est la phase de planification pour les adversaires.

OSINT (Open-Source Intelligence) relève également de la reconnaissance. OSINT est la première étape qu'un attaquant doit accomplir pour mener à bien les phases suivantes d'une attaque. L'attaquant doit étudier la victime en collectant toutes les informations disponibles sur l'entreprise et ses employés , telles que la taille de l'entreprise, les adresses e-mail, les numéros de téléphone à partir de ressources accessibles au public afin de déterminer la meilleure cible pour l'attaque.

Vous pouvez également en savoir plus sur OSINT dans cet article de Varonis, "[Qu'est-ce que l'OSINT?](#)"

Regardons cela du point de vue de l'attaquant, qui au départ ne sait pas quelle entreprise il veut attaquer.

Voici le scénario : Un attaquant malveillant qui se fait appeler Megatron" décide de mener une attaque très sophistiquée qu'il planifie depuis des années ; il a étudié et recherché différents outils et techniques qui pourraient l'aider à atteindre la dernière phase de la Cyber Kill Chain. Mais d'abord, il doit commencer par la phase de reconnaissance.

Pour opérer dans cette phase, l'attaquant devrait effectuer OSINT. Jetons un coup d'œil à la collecte d'e-mails.

La collecte d'e-mails est le processus d'obtention d'adresses e-mail auprès de services publics, payants ou gratuits . Un attaquant peut utiliser la collecte d'adresses e-mail pour une attaque de phishing (un type d'attaque d'ingénierie sociale utilisée pour voler des données sensibles, y compris

les identifiants de connexion et les numéros de carte de crédit). L'attaquant aura un grand arsenal d'outils disponibles à des fins de reconnaissance . En voici quelques uns:

- [theHarvester](#) - outre la collecte d'e-mails, cet outil est également capable de collecter des noms, des sous-domaines, des adresses IP et des URL à l'aide de plusieurs sources de données publiques
- [Hunter.io](#) - il s'agit d'un outil de chasse aux e-mails qui vous permettra d'obtenir les informations de contact associées au domaine
- [OSINT Framework](#) - OSINT Framework fournit la collection d'outils OSINT basés sur différentes catégories

Un attaquant utiliserait également des sites Web de médias sociaux tels que LinkedIn, Facebook, Twitter et Instagram pour collecter des informations sur une victime spécifique qu'il voudrait attaquer ou sur l'entreprise. Les informations trouvées sur les réseaux sociaux peuvent être utiles à un attaquant pour mener une attaque de phishing.

Répondre aux questions ci-dessous

Quel est le nom de l'Intel Gathering Tool qui est une interface Web vers les outils et ressources communs pour l'intelligence open source ?

OSINT Framework

Bonne réponse

Quelle est la définition du processus de collecte d'e-mails lors de l'étape de reconnaissance ?

email harvesting

Bonne réponse

Armement ou weaponization.

Après une étape de reconnaissance réussie, "Megatron" travaillerait à la fabrication d'une "arme de destruction". Il préférerait ne pas interagir directement avec la victime et, à la place, il créera un "armateur" qui, selon Lockheed Martin, combine malware et exploit dans une charge utile livrable . La plupart des attaquants utilisent généralement des outils automatisés pour générer le malware ou se réfèrent au [DarkWeb](#) pour acheter le malware.

Des acteurs plus sophistiqués ou des APT (Advanced Persistent Threat Groups) parrainés par un pays écriraient leur malware personnalisé pour rendre l'échantillon de malware unique et échapper à la détection sur la cible.

Définissons d'abord quelques termes avant d'analyser la phase de militarisation.

Un logiciel malveillant est un programme ou un logiciel conçu pour endommager, perturber ou obtenir un accès non autorisé à un ordinateur.

Un exploit est un programme ou un code qui tire parti de la vulnérabilité ou de la faille de l'application ou du système.

Une charge utile est un code malveillant que l'attaquant exécute sur le système.

Poursuivant avec notre adversaire, "Megatron" choisit...

"Megatron choisit d'acheter une charge utile déjà écrite à quelqu'un d'autre dans le DarkWeb, afin qu'il puisse passer plus de temps sur les autres phases.

Dans la phase de militarisation, l'attaquant :

- Créez un document Microsoft Office infecté contenant une macro malveillante ou des scripts VBA (Visual Basic pour Applications). Si vous souhaitez en savoir plus sur les macros et VBA, veuillez vous référer à l'article ["Intro to Macros and VBA For Script Kiddies" de TrustedSec](#).
- Un attaquant peut créer une charge utile malveillante ou un ver très sophistiqué, l'implanter sur les clés USB, puis les diffuser en public. Un exemple de virus.
- Un attaquant choisirait des techniques de commande et de contrôle (C2) pour exécuter les commandes sur la machine de la victime ou fournirait plus de charges utiles. Vous pouvez en savoir plus sur les techniques C2 sur [MITRE ATT&CK](#) .

- Un attaquant sélectionnerait un implant de porte dérobée (le moyen d'accéder au système informatique, qui comprend le contournement des mécanismes de sécurité).

Répondre aux questions ci-dessous

Ce terme désigne un groupe de commandes qui exécutent une tâche spécifique. Vous pouvez les considérer comme des sous-routines ou des fonctions contenant le code que la plupart des utilisateurs utilisent pour automatiser les tâches de routine. Mais les acteurs malveillants ont tendance à les utiliser à des fins malveillantes et à les inclure dans les documents Microsoft Office. Pouvez-vous en donner le terme ?

Macro

Bonne réponse

L'étape de livraison

La phase de livraison correspond au moment où "Megatron" décide de choisir la méthode de transmission de la charge utile ou du malware. Il a beaucoup d'options à choisir:

- E-mail d'hameçonnage : après avoir effectué la reconnaissance et déterminé les cibles de l'attaque, l'acteur malveillant créerait un e-mail malveillant qui ciblerait soit une personne spécifique (attaque par hameçonnage), soit plusieurs personnes dans l'entreprise. L'e-mail contiendrait une charge utile ou un logiciel malveillant. Par exemple, "Megatron" apprendrait que Nancy du département des ventes de l'entreprise A aimerait constamment les publications sur LinkedIn de Scott, un responsable de la prestation de services de l'entreprise B. Il lui donnerait une seconde hypothèse qu'ils communiquent tous les deux les uns avec les autres sur e-mails professionnels. "Megatron" créerait un e-mail en utilisant le prénom et le nom de Scott, rendant le domaine similaire à l'entreprise dans laquelle Scott travaille. Un attaquant enverrait alors un faux e-mail "Facture" à Nancy, qui contient la charge utile.
- Distribuer des clés USB infectées dans des lieux publics comme des cafés, des parkings ou dans la rue. Un attaquant pourrait décider de mener une attaque par chute USB sophistiquée en imprimant le logo de l'entreprise sur les clés USB et en les envoyant à l'entreprise tout en se faisant passer pour un client envoyant les périphériques USB en cadeau. Vous pouvez en savoir plus sur l'une de ces attaques similaires sur [CSO Online "Un groupe cybercriminel envoie des dongles USB malveillants aux entreprises ciblées"](#).
- Attaque de point d'eau (watering hole attack). Une attaque par point d'eau est une attaque ciblée conçue pour viser un groupe spécifique de personnes en compromettant le site Web qu'elles visitent habituellement, puis en les redirigeant vers le site Web malveillant choisi par l'attaquant. L'attaquant rechercherait une vulnérabilité connue pour le site Web et tenterait de l'exploiter. L'attaquant encouragerait les victimes à visiter le site Web en envoyant des e-mails "inoffensifs" indiquant l'URL malveillante pour que l'attaque fonctionne plus efficacement. Après avoir visité le site Web, la victime téléchargerait involontairement un logiciel malveillant ou une application malveillante sur son ordinateur. Ce type d'attaque est appelé téléchargement intempestif. Un exemple peut être une fenêtre contextuelle malveillante demandant de télécharger une fausse extension de navigateur.

Answer the questions below

What is the name of the attack when it is performed against a specific group of people, and the attacker seeks to infect the website that the mentioned group of people is constantly visiting.

Watering hole attack

Correct Answer

Exploitation :

Pour accéder au système, un attaquant doit exploiter la vulnérabilité. Dans cette phase, "Megatron" a fait preuve d'un peu de créativité - il a créé deux e-mails de phishing, l'un contenant un lien de phishing vers une fausse page de connexion Office 365 et un autre contenant une macro en pièce jointe qui exécuterait un ransomware lorsque la victime l'ouvrirait. "Megatron" a livré avec succès ses exploits et a obligé deux victimes à cliquer sur le lien malveillant et à ouvrir le fichier malveillant .

Après avoir accédé au système, l'acteur malveillant pourrait exploiter les vulnérabilités du logiciel, du système ou du serveur pour éléver les priviléges ou se déplacer latéralement sur le réseau. Selon [CrowdStrike](#) , le mouvement latéral fait référence aux techniques qu'un acteur malveillant utilise après avoir obtenu un accès initial à la machine de la victime pour se déplacer plus profondément dans un réseau afin d'obtenir des données sensibles.

Si vous souhaitez en savoir plus sur les vulnérabilités basées sur le serveur ou sur le Web, veuillez vous référer à la salle TryHackMe [OWASP Top 10](#) .

L'attaquant peut également appliquer un "Zero-day Exploit" à ce stade. Selon [FireEye](#) , "l'exploit zero-day ou une vulnérabilité zero-day est un exploit inconnu dans la nature qui expose une vulnérabilité logicielle ou matérielle et peut créer des problèmes complexes bien avant que quiconque ne se rende compte que quelque chose ne va pas. Un exploit zero-day laisse AUCUNE opportunité de détection au début."

Voici des exemples de la façon dont un attaquant procède à l'exploitation :

- La victime déclenche l'exploit en ouvrant la pièce jointe de l'e-mail ou en cliquant sur un lien malveillant.
- Utilisation d'un exploit zero-day.
- Exploitez les vulnérabilités logicielles, matérielles ou même humaines.
- Un attaquant déclenche l'exploit pour les vulnérabilités basées sur le serveur.

Répondre aux questions ci-dessous

Pouvez-vous donner le nom d'une cyberattaque ciblant une vulnérabilité logicielle inconnue des éditeurs d'antivirus ou de logiciels ?

zero-day

Bonne réponse

Installation



Comme vous l'avez appris lors de la phase de militarisation, la porte dérobée permet à un attaquant de contourner les mesures de sécurité et de masquer l'accès. Une porte dérobée est également connue sous le nom de point d'accès.

Une fois que l'attaquant a accès au système, il souhaite y accéder à nouveau s'il perd la connexion ou s'il est détecté et que l'accès initial est supprimé, ou si le système est ultérieurement corrigé. Il n'y aura plus accès. C'est alors que l'attaquant doit installer une [porte dérobée persistante](#) . Une porte dérobée persistante permettra à l'attaquant d'accéder au système qu'il a compromis dans le passé. Vous pouvez consulter la [salle de persistance](#)

[Windows](#) sur TryHackMe pour savoir comment un attaquant peut obtenir la persistance sur Windows.

La persistance peut être obtenue par :

- Installation d'un shell Web sur le serveur Web. Un shell Web est un script malveillant écrit dans des langages de programmation de développement Web tels que ASP, PHP ou JSP utilisé par un attaquant pour maintenir l'accès au système compromis. En raison de la simplicité du shell Web et du formatage des fichiers (.php, .asp, .aspx, .jsp, etc.) peuvent être difficiles à détecter et peuvent être classés comme bénins. Vous pouvez consulter cet excellent article publié par [Microsoft](#) sur diverses attaques Web Shell.
- Installation d'une porte dérobée sur la machine de la victime. Par exemple, l'attaquant peut utiliser [Meterpreter](#) pour installer une porte dérobée sur la machine de la victime. Meterpreter est une charge utile Metasploit Framework qui fournit un shell interactif à partir duquel un attaquant peut interagir à distance avec la machine de la victime et exécuter le code malveillant.
- Création ou modification des services Windows. Cette technique est connue sous le nom de [T1543.003](#) sur MITRE ATT&CK (MITRE ATT&CK® est une base de connaissances sur les tactiques et techniques de l'adversaire basées sur des scénarios réels) . **Un attaquant peut créer ou modifier les services Windows pour exécuter régulièrement les scripts ou charges utiles malveillants dans le cadre de la persistance. Un attaquant peut utiliser des outils tels que sc.exe (sc.exe vous permet de créer, démarrer, arrêter, interroger ou supprimer n'importe quel service Windows) et Reg pour modifier les configurations de service.** L'attaquant peut également [masquer](#) la charge utile malveillante en utilisant un nom de service connu pour être lié au système d'exploitation ou à un logiciel légitime.
- Ajout de l'entrée aux "clés d'exécution" pour la charge utile malveillante dans le registre ou le dossier de démarrage. Ce faisant, la charge utile s'exécutera chaque fois que l'utilisateur se connectera à l'ordinateur. Selon MITRE ATT&CK, il existe un emplacement de dossier de démarrage pour les comptes d'utilisateurs individuels et un dossier de démarrage à l'échelle du système qui sera vérifié quel que soit le compte d'utilisateur connecté.

Vous pouvez en savoir plus sur la persistance des clés d'exécution du registre / du dossier de démarrage sur l'une des [techniques MITRE ATT&CK](#) .

Dans cette phase, l'attaquant peut également utiliser la technique [Timestamping](#) pour éviter la détection par l'enquêteur médico-légal et également pour faire apparaître le logiciel malveillant comme faisant partie d'un programme légitime. La technique Timestamping permet à un attaquant de modifier les horodatages du fichier, y compris les heures de modification, d'accès, de création et de modification.

Answer the questions below

Can you provide the technique used to modify file time attributes to hide new or changes to existing files?

timestomping

Correct Answer

Can you name the malicious script planted by an attacker on the webserver to maintain access to the compromised system and enables the webserver to be accessed remotely?

web shell

Correct Answer

Command & Control



Après avoir obtenu la persistance et exécuté le logiciel malveillant sur la machine de la victime, "Megatron" ouvre le canal C2 (commande et contrôle) via le logiciel malveillant pour contrôler et manipuler à distance la victime. Ce terme est également connu sous le nom de C&C ou C2 Beaconing en tant que type de communication malveillante entre un serveur C&C et un logiciel malveillant sur l'hôte infecté. L'hôte infecté communiquera de manière cohérente avec le serveur C2 ; c'est aussi de là que vient le terme de balisage.

Le point de terminaison compromis communiquerait avec un serveur externe configuré par un attaquant pour établir un canal de commande et de contrôle. Après avoir établi la connexion, l'attaquant a le contrôle total de la machine de la victime. Jusqu'à récemment, IRC (Internet Relay Chat) était le canal C2 traditionnel utilisé par les attaquants. Ce n'est plus le cas, car les solutions de sécurité modernes peuvent facilement détecter le trafic IRC malveillant.

Les canaux C2 les plus couramment utilisés par les adversaires de nos jours :

- Les protocoles HTTP sur le port 80 et HTTPS sur le port 443 - ce type de balisage mélange le trafic malveillant avec le trafic légitime et peut aider l'attaquant à échapper aux pare-feu.
- DNS (serveur de noms de domaine). La machine infectée fait des requêtes DNS constantes au serveur DNS qui appartient à un attaquant, ce type de communication C2 est également connu sous le nom de DNS Tunneling.

Il est important de noter qu'un adversaire ou un autre hôte compromis peut être le propriétaire de l'infrastructure C2 .

Answer the questions below

What is the C2 communication where the victim makes regular DNS requests to a DNS server and domain which belong to an attacker.

DNS Tunneling

Correct Answer

Actions on Objectives :



Après avoir traversé six phases de l'attaque, "Megatron" peut enfin atteindre ses objectifs, ce qui signifie agir sur les objectifs initiaux. Avec un accès direct au clavier, l'attaquant peut réaliser ce qui suit :

- Collectez les informations d'identification des utilisateurs.
- Effectuer une élévation des privilèges (obtenir un accès élevé comme l'accès administrateur de domaine à partir d'un poste de travail en exploitant la mauvaise configuration).
- Reconnaissance interne (par exemple, un attaquant peut interagir avec un logiciel interne pour trouver ses vulnérabilités).
- Mouvement latéral dans l'environnement de l'entreprise.
- Collecter et exfiltrer des données sensibles.
- Suppression des sauvegardes et des shadow copies. Shadow Copy est une technologie Microsoft qui peut créer des copies de sauvegarde, des instantanés de fichiers informatiques ou de volumes.
- Écaser ou corrompre les données.

Analyse pratique



We really hope you enjoyed this room. In order to strengthen your knowledge, let's do a practice analysis.

Here is the real-world scenario for you to tackle:

The infamous Target cyber-attack, which led to one of the largest data breaches in history took place on November 27, 2013.

On December 19th, 2013, Target released a [statement](#) confirming the breach, stating that approximately 40 million credit and debit card accounts were impacted between Nov. 27 and Dec. 15,

2013. Target had to pay the fine of \$18.5 million under the terms of the multistate [settlement agreement](#). This is considered to be the largest data-breach settlement in history.

How did the data breach happen? Deploy the static site attached to this task and apply your skills to build the Cyber Kill Chain of this scenario. Here are some tips to help you complete the practical:

1. Add each item on the list in the correct Kill Chain entry-form on the Static Site Lab:

- exploit public-facing application
- data from local system
- powershell
- dynamic linker hijacking
- spearphishing attachment
- fallback channels

2. Use the 'Check answers' button to verify whether the answers are correct (where wrong answers will be underlined in red).

The diagram shows a vertical sequence of six stages connected by red arrows. Each stage is represented by a red circle containing a relevant icon. To the left of the first stage, there is a horizontal line with the text 'data from local sys'. To the left of the second stage, there is a horizontal line with the text 'spearphishing attack'. To the right of the third stage, there is a horizontal line with the text 'powershell'. To the right of the fourth stage, there is a horizontal line with the text 'exploit public-faci'. To the right of the fifth stage, there is a horizontal line with the text 'fallback channels'. To the left of the sixth stage, there is a horizontal line with the text 'dynamic linker hija'. At the bottom center of the diagram is a green button with the text 'Check answers'.

Conclusion

Cyber Kill Chain peut être un excellent outil pour améliorer la défense du réseau. Est-il parfait et peut-il être le seul outil sur lequel compter ? Non.

La Cyber Kill Chain traditionnelle ou Lockheed Martin Cyber Kill Chain a été modifiée pour la dernière fois en 2011, qui, si vous vous en souvenez, est la date de sa création. L'absence de mises à jour et de modifications crée des failles de sécurité.

La Cyber Kill Chain traditionnelle a été conçue pour sécuriser le périmètre du réseau et se protéger contre les menaces de logiciels malveillants. Mais les menaces de cybersécurité se sont considérablement développées de nos jours et les adversaires combinent plusieurs TTP (tactiques, techniques et procédures) pour atteindre leur objectif. Les adversaires sont capables de vaincre les renseignements sur les menaces en modifiant les hachages de fichiers et les adresses IP. Les entreprises de solutions de sécurité développent des technologies comme l'IA (Intelligence Artificielle) et différents algorithmes pour détecter les changements même légers et suspects.

Étant donné que l'objectif principal du cadre est la diffusion de logiciels malveillants et la sécurité du réseau, la chaîne de destruction cybernétique traditionnelle ne sera pas en mesure d'identifier les menaces internes . Selon [CISA](#), "La menace d'initié est le potentiel pour un initié d'utiliser son accès autorisé ou sa compréhension d'une organisation pour nuire à cette organisation."

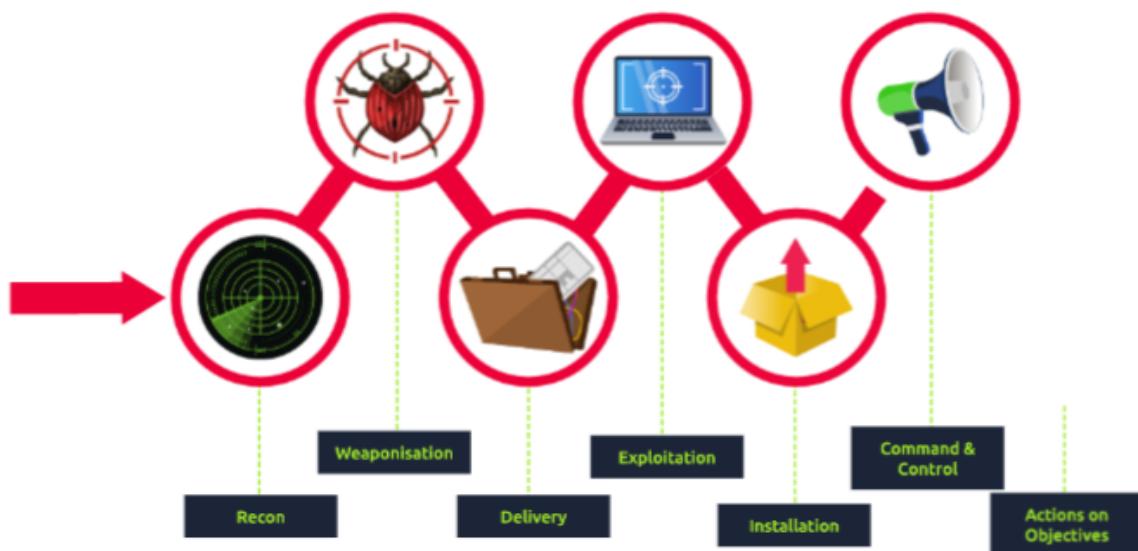
Nous recommandons non seulement de s'appuyer sur le modèle traditionnel de Cyber Kill Chain, mais également de se référer à [MITRE ATT&CK](#) ainsi qu'à [Unified Kill Chain](#) pour appliquer une approche plus complète à vos méthodologies de défense.

Unified Kill Chain

<https://tryhackme.com/room/unifiedkillchain>

framework qui établit les phases d'une attaque et un moyen d'identifier et d'atténuer les risques pour les actifs informatiques

Introduction



Comprendre les comportements, les objectifs et les méthodologies d'une cybermenace est une étape essentielle pour établir une défense solide en matière de cybersécurité (appelée posture de cybersécurité).

Dans cette salle, vous découvrirez le framework UKC (Unified Kill Chain) qui est utilisé pour aider à comprendre comment les cyberattaques se produisent.

Objectifs d'apprentissage:

- Comprendre pourquoi des framework tels que l' UKC sont importants et utiles pour établir une bonne posture de cybersécurité
- Utiliser l' UKC pour comprendre la motivation, les méthodologies et les tactiques d'un attaquant
- Comprendre les différentes phases de l' UKC
- Découvrez que l' UKC est un framework qui est utilisé pour compléter d'autres framework tels que MITRE.

Qu'est ce qu'une kill chain ?

D'origine militaire, une « Kill Chain » est un terme utilisé pour expliquer les différentes étapes d'une attaque. Dans le domaine de la cybersécurité, une « chaîne de destruction » est utilisée pour décrire la méthodologie/le chemin que les attaquants tels que les pirates ou les APT utilisent pour approcher et pénétrer une cible.

Par exemple, un attaquant scannant, exploitant une vulnérabilité Web et augmentant les priviléges sera une "Kill Chain". Nous reviendrons expliquer ces étapes de manière beaucoup plus détaillée plus loin dans cette salle.

L'objectif est de comprendre la « chaîne de destruction » d'un attaquant afin que des mesures défensives puissent être mises en place pour protéger un système de manière préventive ou perturber la tentative d'un attaquant.

Répondre aux questions ci-dessous

D'où vient le terme "Kill Chain" ?

Pour cette réponse, vous devez remplir le blanc ! : Le *****

military

Bonne réponse

What is threat modelling ?

La modélisation des menaces, dans un contexte de cybersécurité, est une série d'étapes pour finalement améliorer la sécurité d'un système. La modélisation des menaces consiste à identifier les risques et se résume essentiellement à :

- 1 . Identifier quels systèmes et applications doivent être sécurisés et quelle fonction ils remplissent dans l'environnement. Par exemple, le système est-il essentiel aux opérations normales, et un système contient-il des informations sensibles telles que des informations de paiement ou des adresses ?
- 2 . Évaluer les vulnérabilités et les faiblesses que ces systèmes et applications peuvent avoir et comment ils pourraient être potentiellement exploités
- 3 . Créer un plan d'action pour sécuriser ces systèmes et applications des vulnérabilités mises en évidence
- 4 . Mettre en place des politiques pour empêcher ces vulnérabilités de se reproduire dans la mesure du possible (par exemple, mettre en œuvre un cycle de vie de

développement logiciel (SDLC) pour une application ou former les employés à la sensibilisation au phishing).



La modélisation des menaces est une procédure importante pour réduire le risque au sein d'un système ou d'une application, car elle crée une vue d'ensemble de haut niveau des actifs informatiques d'une organisation (un actif informatique est un logiciel ou du matériel) et des procédures pour résoudre les vulnérabilités.

L' UKC peut encourager la modélisation des menaces car le framework UKC aide à identifier les surfaces d'attaque potentielles et la manière dont ces systèmes peuvent être exploités. STRIDE , DREAD et CVSS (pour n'en citer que quelques-uns) sont tous des frameworks spécifiquement utilisés dans la modélisation des menaces. Si vous souhaitez en savoir plus, consultez la salle « [Principes de sécurité](#) » sur TryHackMe.

Répondre aux questions ci-dessous

Quel est le terme technique pour désigner un logiciel ou un matériel informatique (technologie de l'information ?)

asset

Bonne réponse

Indice

Présentation de la Unified Kill Chain

Pour continuer à partir de la tâche précédente, la [chaîne de destruction unifiée](#) publiée en 2017, vise à compléter (et non à concurrencer) d'autres framework kill chain tels Lockheed Martin's and MITRE's ATT&CK.

L' UKC déclare qu'il y a 18 phases dans une attaque : Tout, de la reconnaissance à l'exfiltration de données et à la compréhension du motif d'un attaquant. Ces phases ont été regroupées dans cette salle en quelques domaines prioritaires par souci de brièveté, qui seront détaillés dans les tâches restantes.

Parmi les grands avantages de l' UKC par rapport aux framework kill chain de la cybersécurité, citons le fait qu'il est moderne et extrêmement détaillé (rappel : il comporte officiellement 18 phases, alors que d'autres cadres peuvent en avoir une petite poignée)

The Unified Kill Chain



1	Reconnaissance	Researching, identifying and selecting targets using active or passive reconnaissance.
2	Weaponization	Preparatory activities aimed at setting up the infrastructure required for the attack.
3	Delivery	Techniques resulting in the transmission of a weaponized object to the targeted environment.
4	Social Engineering	Techniques aimed at the manipulation of people to perform unsafe actions.
5	Exploitation	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6	Persistence	Any access, action or change to a system that gives an attacker persistent presence on the system.
7	Defense Evasion	Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8	Command & Control	Techniques that allow attackers to communicate with controlled systems within a target network.
9	Pivoting	Tunneling traffic through a controlled system to other systems that are not directly accessible.
10	Discovery	Techniques that allow an attacker to gain knowledge about a system and its network environment.
11	Privilege Escalation	The result of techniques that provide an attacker with higher permissions on a system or network.
12	Execution	Techniques that result in execution of attacker-controlled code on a local or remote system.
13	Credential Access	Techniques resulting in the access of, or control over, system, service or domain credentials.
14	Lateral Movement	Techniques that enable an adversary to horizontally access and control other remote systems.
15	Collection	Techniques used to identify and gather data from a target network prior to exfiltration.
16	Exfiltration	Techniques that result or aid in an attacker removing data from a target network.
17	Impact	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	Objectives	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

Benefits of the Unified Kill Chain (UKC) Framework	How do Other Frameworks Compare?
Modern (released in 2017, updated in 2022).	Some frameworks, such as MITRE's were released in 2013, when the cybersecurity landscape was very different.
The UKC is extremely detailed (18 phases).	Other frameworks often have a small handful of phases.
The UKC covers an entire attack - from reconnaissance, exploitation, post-exploitation and includes identifying an attacker's motivation.	Other frameworks cover a limited amount of phases.
The UKC highlights a much more realistic attack scenario. Various stages will often re-occur. For example, after exploiting a machine, an attacker will begin reconnaissance to pivot another system.	Other frameworks do not account for the fact that an attacker will go back and forth between the various phases during an attack.

Répondre aux questions ci-dessous

En quelle année le framework Unified Kill Chain a-t-il été publié ?

2017

Bonne réponse

Selon la Unified Kill Chain, combien de phases y a-t-il pour une attaque ?

18

Bonne réponse

Quel est le nom de la phase d'attaque où un attaquant utilise des techniques pour échapper à la détection ?

defense evasion

Bonne réponse

Quel est le nom de la phase d'attaque où un attaquant emploie des techniques pour supprimer des données d'un réseau ?

exfiltration

Bonne réponse

Comment s'appelle la phase d'attaque où un attaquant atteint ses objectifs ?

Objectives

Bonne réponse

Indice

Phase : In (Initial Foothold)

L'objectif principal de cette série de phases est pour un attaquant d'accéder à un système ou à un environnement en réseau.

Un attaquant emploiera de nombreuses tactiques pour enquêter sur le système à la recherche de vulnérabilités potentielles pouvant être exploitées pour prendre pied dans le système. Par exemple, une tactique courante consiste à utiliser la reconnaissance contre un système pour découvrir des vecteurs d'attaque potentiels (tels que des applications et des services).



Cette série de phases permet également à un attaquant de créer une forme de persistance (comme des fichiers ou un processus permettant à l'attaquant de se connecter à la machine

à tout moment). Enfin, l' UKC tient compte du fait que les attaquants utilisent souvent une combinaison des tactiques énumérées ci-dessus.

Nous explorerons les différentes phases de cette section de l' UKC dans les rubriques ci-dessous :

Reconnaissance ([MITRE Tactique TA0043](#))

Cette phase de l' UKC décrit les techniques qu'un adversaire utilise pour recueillir des informations relatives à sa cible. Ceci peut être réalisé par des moyens de reconnaissance passive et active. Les informations recueillies au cours de cette phase sont utilisées tout au long des étapes ultérieures de l'UKC (telles que l'implantation initiale).

Les informations recueillies à partir de cette phase peuvent inclure :

- Découvrir quels systèmes et services fonctionnent sur la cible, ce sont des informations utiles dans les phases de militarisation et d'exploitation de cette section.
- Trouver des listes de contacts ou des listes d'employés qui peuvent être usurpés ou utilisés dans une attaque d'ingénierie sociale ou de phishing.
- Recherche d'informations d'identification potentielles pouvant être utiles à des étapes ultérieures, telles que le pivotement ou l'accès initial.
- Comprendre la topologie du réseau et d'autres systèmes en réseau peut également être utilisé pour pivoter.

Armement ([MITRE Tactic TA0001](#))

Cette phase de l' UKC décrit l'adversaire mettant en place l'infrastructure nécessaire pour effectuer l'attaque. Par exemple, cela pourrait être la mise en place d'un serveur de commande et de contrôle, ou un système capable d'attraper des shells inversés et de fournir des charges utiles au système.

Ingénierie sociale ([MITRE Tactic TA0001](#))

Cette phase de l' UKC décrit les techniques qu'un adversaire peut utiliser pour manipuler les employés afin qu'ils effectuent des actions qui aideront l'attaque des adversaires. Par exemple, une attaque d'ingénierie sociale pourrait inclure :

- Amener un utilisateur à ouvrir une pièce jointe malveillante.
- Usurper l'identité d'une page Web et demander à l'utilisateur d'entrer ses informations d'identification.
- Appeler ou visiter la cible et se faire passer pour un utilisateur (par exemple, demander une réinitialisation du mot de passe) ou pouvoir accéder à des zones d'un site dont l'attaquant n'aurait pas été capable auparavant (par exemple, se faire passer pour un ingénieur utilitaire).

Exploitation ([MITRE Tactique TA0002](#))

Cette phase de l' UKC décrit comment un attaquant tire parti des faiblesses ou des vulnérabilités présentes dans un système. L'UKC définit "l'exploitation" comme l'abus de vulnérabilités pour effectuer l'exécution de code. Par exemple:

- Téléchargement et exécution d'un shell inversé vers une application Web.
- Interférer avec un script automatisé sur le système pour exécuter du code.
- Exploiter une vulnérabilité d'application Web pour exécuter du code sur le système sur lequel elle s'exécute.

Persistance ([MITRE Tactic TA0003](#))

Cette phase de l' UKC est plutôt courte et simple. Plus précisément, cette phase de l'UKC décrit les techniques qu'un adversaire utilise pour maintenir l'accès à un système sur lequel il a pris pied initialement. Par exemple:

- Création d'un service sur le système cible qui permettra à l'attaquant de retrouver l'accès.
- Ajout du système cible à un serveur Command & Control où les commandes peuvent être exécutées à distance à tout moment.
- Laissant d'autres formes de portes dérobées qui s'exécutent lorsqu'une certaine action se produit sur le système (c'est-à-dire qu'un reverse shell s'exécute lorsqu'un administrateur système se connecte).

Évasion de défense ([MITRE Tactic TA0005](#))

La section "Defence Evasion" de l' UKC est l'une des phases les plus précieuses de l'UKC. Cette phase est spécifiquement utilisée pour comprendre les techniques qu'un adversaire utilise pour échapper aux mesures défensives mises en place dans le système ou le réseau.

Par exemple, cela pourrait être :

- Pare-feux d'applications Web.
- Pare-feu réseau.
- Systèmes antivirus sur la machine cible.
- Systèmes de détection d'intrusion.

Cette phase est précieuse lors de l'analyse d'une attaque car elle aide à former une réponse et, mieux encore, donne à l'équipe défensive des informations sur la manière dont elle peut améliorer ses systèmes de défense à l'avenir.

Commande et contrôle ([MITRE Tactic TA0011](#))

La phase "Command & Control" de l' UKC combine les efforts déployés par un adversaire pendant la phase "Armement" de l'UKC pour établir des communications entre l'adversaire et le système cible.

Un adversaire peut établir le commandement et le contrôle d'un système cible pour réaliser son action sur des objectifs. Par exemple, l'adversaire peut :

- Exécutez les commandes.
- Voler des données, des informations d'identification et d'autres informations.
- Utilisez le serveur contrôlé pour basculer vers d'autres systèmes sur le réseau.

Pivotant ([MITRE Tactic TA0008](#))

Le "pivotement" est la technique qu'un adversaire utilise pour atteindre d'autres systèmes au sein d'un réseau qui ne sont pas autrement accessibles (par exemple, ils ne sont pas exposés à Internet). Il existe souvent de nombreux systèmes dans un réseau qui ne sont pas directement accessibles et contiennent souvent des données précieuses ou ont une sécurité plus faible.

Par exemple, un adversaire peut accéder à un serveur Web accessible publiquement pour attaquer d'autres systèmes qui se trouvent sur le même réseau (mais qui ne sont pas accessibles via Internet).

Répondre aux questions ci-dessous

Pouvez-vous donner un exemple de tactique pour prendre pied en utilisant des e-mails ?

phishing

Bonne réponse

Se faire passer pour un employé pour demander une réinitialisation de mot de passe est une forme de quoi ?

social engineering

Bonne réponse

Un adversaire mettant en place l'infrastructure du serveur Command & Control est quelle phase de la Unified Kill Chain ?

Weaponization

Bonne réponse

Exploiter une vulnérabilité présente sur un système est quelle phase de la Unified Kill Chain ?

Exploitation

Bonne réponse

Passer d'un système à un autre est un exemple de?

pivoting

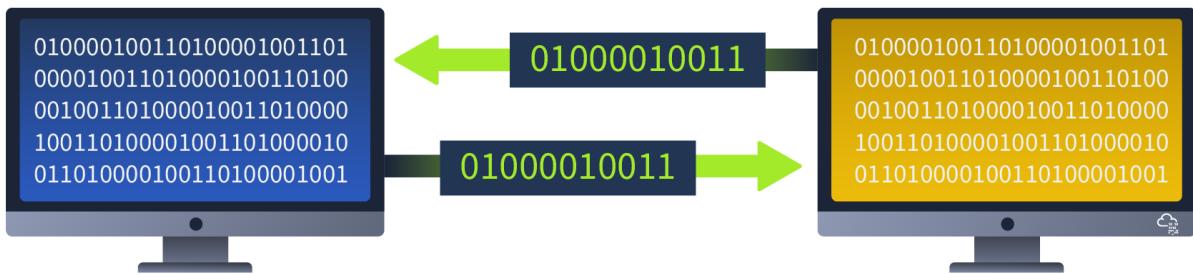
Bonne réponse

Laisser derrière un service malveillant qui permet à l'adversaire de se reconnecter à la cible, c'est quoi ?

persistence

Bonne réponse

Phase: Through (Network Propagation)



Cette phase fait suite à une prise de pied réussie sur le réseau cible. Un attaquant chercherait à obtenir un accès et des priviléges supplémentaires aux systèmes et aux données pour atteindre ses objectifs. L'attaquant mettrait en place une base sur l'un des systèmes pour agir comme leur point de pivot et l'utiliser pour recueillir des informations sur le réseau interne.



Pivotant ([MITRE Tactic TA0008](#))

Une fois que l'attaquant a accès au système, il l'utilise comme site de transit et tunnel entre ses opérations de commande et le réseau de la victime. Le système serait également utilisé comme point de distribution pour tous les logiciels malveillants et portes dérobées à des stades ultérieurs.

Découverte ([MITRE Tactic TA0007](#))

L'adversaire découvrirait des informations sur le système et le réseau auquel il est connecté. Au cours de cette étape, la base de connaissances serait construite à partir des comptes d'utilisateurs actifs, des autorisations accordées, des applications et des logiciels utilisés, de l'activité du navigateur Web, des fichiers, des répertoires et des partages réseau, et des configurations système.

Escalade des priviléges ([MITRE Tactic TA0004](#))

Suite à leur collecte de connaissances, l'adversaire essaierait d'obtenir des autorisations plus importantes au sein du système pivot. Ils tireraient parti des informations sur les comptes présentant des vulnérabilités et des erreurs de configuration trouvées pour éléver leur accès à l'un des niveaux supérieurs suivants :

- SYSTÈME/ RACINE.
- Administrateur local.
- Un compte utilisateur avec un accès de type administrateur.
- Un compte utilisateur avec un accès ou des fonctions spécifiques.

Exécution ([MITRE Tactic TA0002](#))

Rappelez-vous quand l'adversaire a mis en place son infrastructure d'attaque. Une fois que l'attaquant a accès au système, il l'utilise comme site de transit et tunnel entre ses opérations de commande et le réseau de la victime. Le système serait également utilisé comme point de distribution pour tous les logiciels malveillants et portes dérobées à des stades ultérieurs. et des charges utiles militarisées ? C'est là qu'ils déplacent leur code malveillant en utilisant le système pivot comme hôte. Des chevaux de Troie distants, des scripts C2, des liens malveillants et des tâches planifiées sont déployés et créés pour faciliter une présence récurrente sur le système et maintenir leur persistance.

Accès aux informations d'identification ([MITRE Tactic TA0006](#))

Travaillant main dans la main avec l'étape d'escalade des priviléges, l'adversaire tenterait de voler les noms de compte et les mots de passe par diverses méthodes, y compris l'enregistrement de frappe et le vidage des informations d'identification. Cela les rend plus difficiles à détecter lors de leur attaque car ils utiliseraient des informations d'identification légitimes.

Mouvement latéral ([MITRE Tactic TA0008](#))

Avec les informations d'identification et les priviléges élevés, l'adversaire chercherait à se déplacer sur le réseau et à sauter sur d'autres systèmes ciblés pour atteindre son objectif principal. Plus la technique utilisée est furtive, mieux c'est.

Répondre aux questions ci-dessous

En tant qu'analyste SOC, vous recevez de nombreuses alertes pointant vers des tentatives de connexion infructueuses à partir d'un compte administrateur. Quelle étape de la chaîne de mise à mort un attaquant chercherait-il à atteindre ?

privilege escalation

Bonne réponse

Mimikatz, un outil d'attaque connu, a été détecté en cours d'exécution sur l'ordinateur du responsable informatique. Quelle est la mission de l'outil ?

credential dumping

Bonne réponse

Phase: Out (Action on Objectives)



Cette phase conclut le parcours de l'attaque d'un adversaire sur un environnement, où il a accès aux actifs critiques et peut atteindre ses objectifs d'attaque. Ces objectifs visent généralement à compromettre la triade confidentialité, intégrité et disponibilité (CIA). Les tactiques à déployer par un attaquant comprendraient :

Collection [MITRE Tactique \(TA0009\)](#)

Après toute la chasse aux accès et aux actifs, l'adversaire cherchera à rassembler toutes les précieuses données d'intérêt. Ceci, à son tour, compromet la confidentialité des données et conduirait à la prochaine étape d'attaque - l'exfiltration. Les principales sources cibles incluent les lecteurs, les navigateurs, l'audio, la vidéo et les e-mails.

Exfiltration ([MITRE Tactic TA0010](#))

Pour éléver leur compromis, l'adversaire chercherait à voler des données, qui seraient conditionnées à l'aide de mesures de cryptage et de compression pour éviter toute détection. Le canal et le tunnel C2 déployés dans les phases précédentes seront utiles au cours de ce processus.

Impact ([MITRE Tactique TA0040](#))

Si l'adversaire cherche à compromettre l'intégrité et la disponibilité des actifs de données, il manipulera, interrompra ou détruira ces actifs. L'objectif serait de perturber les processus commerciaux et opérationnels et peut impliquer la suppression de l'accès au compte, les effacements de disque et le cryptage des données tels que les ransomwares, la dégradation et les attaques par déni de service (DoS).

Objectifs

Avec toute la puissance et l'accès aux systèmes et au réseau, l'adversaire chercherait à atteindre son objectif stratégique pour l'attaque.

Par exemple, si l'attaque était motivée par des raisons financières, ils peuvent chercher à chiffrer des fichiers et des systèmes avec un rançongiciel et demander un paiement pour

divulguer les données. Dans d'autres cas, l'attaquant peut chercher à nuire à la réputation de l'entreprise et divulguer au public des informations privées et confidentielles.

Répondre aux questions ci-dessous

Lors de la surveillance du réseau en tant qu'analyste SOC, vous vous rendez compte qu'il y a un pic d'activité du réseau et que tout le trafic est sortant vers une adresse IP inconnue. Quelle étape pourrait décrire cette activité ?

Exfiltration

Bonne réponse

Des informations personnelles identifiables (PII) ont été rendues publiques par un adversaire, et votre organisation fait l'objet d'un examen minutieux pour la violation. Quelle partie de la triade de la CIA serait affectée par cette action ?

confidentiality

Bonne réponse

conclusion

Félicitations pour avoir traversé la salle Unified Kill Chain. J'espère que vous comprenez l'importance que des cadres tels que l' UKC jouent dans l'identification des risques et des attaques potentielles d'atténuation en reconstituant les différentes étapes suivies par un attaquant.

Comme mentionné dans cette salle, l' UKC est une extension moderne d'autres cadres, tels que le cadre "Cyber Kill Chain" de Lockheed Martin. Si vous souhaitez en savoir plus sur les frameworks de cybersécurité (fortement recommandé !), vous devriez consulter ces salles sur TryHackMe :

- [Principes de sécurité](#)
- [Fondamentaux du Pentesting](#)
- [Cyber Kill Chain](#)

Diamond Model

<https://tryhackme.com/room/diamondmodelmuwwg42>

Introduction

Le Diamond Model of Intrusion Analysis a été développé par des professionnels de la cybersécurité - Sergio Caltagirone, Andrew Pendergast et Christopher Betz en 2013.

Comme décrit par ses créateurs, le modèle Diamond est composé de quatre caractéristiques principales : adversaire, infrastructure, capacité et victime, et établit l'élément atomique fondamental de toute activité d'intrusion. Vous avez peut-être également remarqué deux composants ou axes supplémentaires du modèle Diamond - social, politique et technologique ; nous entrerons dans un peu plus de détails à leur sujet plus tard dans cette salle. Pourquoi s'appelle-t-il un "Modèle Diamant" ? Les quatre caractéristiques principales sont reliées par les bords, représentant leurs relations sous-jacentes et disposées en forme de losange.

Le modèle Diamond porte les concepts essentiels de l'analyse des intrusions et des opérations adverses tout en permettant la flexibilité d'étendre et d'englober de nouvelles idées et concepts. Le modèle offre diverses possibilités d'intégrer l'intelligence en temps réel pour la défense du réseau, en automatisant la corrélation entre les événements, en classant les événements avec confiance dans les campagnes adverses et en prévoyant les opérations adverses tout en planifiant et en jouant des stratégies d'atténuation.

Adversaire

Un adversaire est également connu sous le nom d'attaquant, d'ennemi, d'acteur de cybermenace ou de pirate informatique. L'adversaire est la personne qui se tient derrière la cyberattaque. Les cyberattaques peuvent être une instruction ou une violation.

Selon les créateurs du Diamond Model, un adversaire est un acteur ou une organisation responsable d'utiliser une capacité contre la victime pour réaliser son intention. Les connaissances de l'adversaire peuvent généralement être mystérieuses, et cette caractéristique essentielle est susceptible d'être vide pour la plupart des événements - du moins au moment de la découverte.

Il est essentiel de connaître la distinction entre opérateur adverse et client adverse, car cela vous aidera à comprendre l'intention, l'attribution, l'adaptabilité et la persistance en aidant à encadrer la relation entre un adversaire et une victime.

Il est difficile d'identifier un adversaire lors des premières étapes d'une cyberattaque. L'utilisation des données collectées lors d'un incident ou d'une violation, des signatures et d'autres informations pertinentes peut vous aider à déterminer qui pourrait être l'adversaire.

L'opérateur adverse est le "pirate informatique" ou la ou les personnes menant l'activité d'intrusion.

Le client adverse est l'entité susceptible de bénéficier de l'activité menée lors de l' intrusion. Il peut s'agir de la même personne qui se tient derrière l'opérateur adverse, ou il peut s'agir d'une personne ou d'un groupe distinct.

A titre d'exemple, un client adverse pourrait contrôler simultanément différents opérateurs . Chaque opérateur peut avoir ses capacités et son infrastructure.

Répondre aux questions ci-dessous

Comment désigne-t-on une personne/un groupe qui a l'intention d'effectuer des actions malveillantes contre des cyberressources ?

adversary operator

Bonne réponse

Quel est le mandat de la personne ou du groupe qui bénéficiera des bénéfices des cyberattaques ?

adversary customer

Bonne réponse

Victime

Victime - est une cible de l'adversaire. Une victime peut être une organisation, une personne, une adresse e-mail cible, une adresse IP, un domaine, etc. Il est essentiel de comprendre la différence entre le personnage de la victime et les actifs de la victime, car ils remplissent des fonctions analytiques différentes.

Une victime peut être une opportunité pour les agresseurs de prendre pied dans l'organisation qu'ils tentent d'attaquer. Il y a toujours une victime dans chaque cyberattaque. Par exemple, l'e-mail de harponnage (un e-mail bien conçu ciblant une personne d'intérêt spécifique) a été envoyé à l'entreprise, et quelqu'un (la victime) a cliqué sur le lien. Dans ce cas, la victime est la cible d'intérêt choisie pour un adversaire.

Les personnes victimes sont les personnes et les organisations ciblées et dont les actifs sont attaqués et exploités. Il peut s'agir de noms d'organisations, de noms de personnes, d'industries, de postes, d'intérêts, etc.

Les actifs de la victime sont la surface d'attaque et comprennent l'ensemble des systèmes, réseaux, adresses e-mail, hôtes, adresses IP, comptes de réseaux sociaux, etc., vers lesquels l'adversaire dirigera ses capacités.

Répondre aux questions ci-dessous

Quel est le terme qui s'applique au modèle Diamond pour les organisations ou les personnes ciblées ?

victime personae

Bonne réponse

capability

Capacité - est également connue comme la compétence, les outils et les techniques utilisés par l'adversaire dans l'événement. La capacité met en évidence les tactiques, techniques et procédures (TTP) de l'adversaire.

La capacité peut inclure toutes les techniques utilisées pour attaquer les victimes, des méthodes les moins sophistiquées, telles que la recherche manuelle de mots de passe, aux

techniques les plus sophistiquées, telles que le développement de logiciels malveillants ou d'un outil malveillant.

Capacité La capacité est l'ensemble des vulnérabilités et des expositions que la capacité individuelle peut utiliser .

Un arsenal adverse est un ensemble de capacités qui appartiennent à un adversaire. Les capacités combinées des capacités d'un adversaire en font l'arsenal de l'adversaire.

Un adversaire doit avoir les capacités requises. Les capacités peuvent être des compétences de développement d'e-mails malveillants et de phishing ou, au moins, l'accès à des fonctionnalités, telles que l'acquisition de logiciels malveillants ou de ransomwares en tant que service.

Infrastructure

Infrastructure - est également connue sous le nom de logiciel ou de matériel. L'infrastructure est constituée des interconnexions physiques ou logiques que l'adversaire utilise pour fournir une capacité ou maintenir le contrôle des capacités. Par exemple, un centre de commandement et de contrôle (C2) et les résultats de la victime (exfiltration de données).

L'infrastructure peut également être constituée d'adresses IP, de noms de domaine, d'adresses e-mail ou même d'un périphérique USB malveillant trouvé dans la rue et branché sur un poste de travail.

L'infrastructure de type 1 est l'infrastructure contrôlée ou possédée par l'adversaire.

L' infrastructure de type 2 est l'infrastructure contrôlée par un intermédiaire. Parfois, l'intermédiaire peut ou non en être conscient. C'est l'infrastructure qu'une victime verra comme l'adversaire. L'infrastructure de type 2 a pour but d'obscurer la source et l'attribution de l'activité. L'infrastructure de type 2 comprend les serveurs de transfert de logiciels malveillants, les noms de domaine malveillants, les comptes de messagerie compromis, etc.

Les fournisseurs de services sont des organisations qui fournissent des services considérés comme critiques pour la disponibilité de l'adversaire des infrastructures de type 1 et de type 2, par exemple, les fournisseurs de services Internet, les registraires de domaine et les fournisseurs de messagerie Web.

Répondre aux questions ci-dessous

À quel type d'infrastructure appartiennent les domaines malveillants et les comptes de messagerie compromis ?

type 2 infrastructure



Quel type d'infrastructure appartient très probablement à un adversaire ?

type 1 infrastructure



Event Meta Features



Six méta-fonctionnalités possibles peuvent être ajoutées au modèle Diamond. Les méta-fonctionnalités ne sont pas nécessaires, mais elles peuvent ajouter des informations ou des renseignements précieux au modèle Diamond.

- Horodatage - est la date et l'heure de l'événement . Chaque événement peut être enregistré avec une date et une heure auxquelles il s'est produit, par exemple 2021-09-12 02:10:12.136. L'horodatage peut inclure le début et la fin de l'événement. Les horodatages sont essentiels pour aider à déterminer les modèles et regrouper l'activité malveillante. Par exemple, si l'intrusion ou la violation s'est produite à 3 heures du matin aux États-Unis, il est possible que l'attaque ait été menée à partir d'un pays spécifique avec un fuseau horaire et des heures d'ouverture standard différents.
- Phase - ce sont les phases d'une intrusion, d'une attaque ou d'une violation. Selon les créateurs du Diamond Model et l'Axiom 4, "Chaque activité malveillante contient deux phases ou plus qui doivent être exécutées successivement avec succès pour obtenir le résultat souhaité". Les activités malveillantes ne se produisent pas comme des événements uniques, mais plutôt comme une séquence d'événements. Un bon exemple peut être la Cyber Kill Chain développée par Lockheed Martin. Vous pouvez en savoir plus sur la Cyber Kill Chain en visitant la [salle Cyber Kill Chain](#) sur TryHackMe
Les phases peuvent être :
 1. Reconnaissance
 2. Armement
 3. Livraison
 4. Exploitation
 5. Installation
 6. Commandement et contrôle
 7. Actions sur objectifPar exemple, un attaquant doit faire des recherches pour découvrir la cible ou une victime. Ensuite, ils essaieraient d'exploiter la cible, d'établir un centre de commandement et de contrôle et, enfin, d'exfiltrer les informations sensibles.
- Résultat - Bien que les résultats et les post-conditions des opérations d'un adversaire ne soient pas toujours connus ou n'aient pas une valeur de confiance élevée lorsqu'ils sont connus, ils sont utiles à saisir. Il est crucial de saisir les résultats et les post-conditions des opérations d'un adversaire, mais parfois ils ne sont pas toujours

connus. Les résultats de l'événement peuvent être étiquetés comme "succès", "échec" ou "inconnu". Les résultats de l'événement peuvent également être liés à la triade CIA (confidentialité, intégrité et disponibilité), telle que Confidentialité compromise, Intégrité compromise et Disponibilité compromise. Une autre approche peut également consister à documenter toutes les post-conditions résultant de l'événement, par exemple,

- Direction - Cette méta-fonctionnalité aide à décrire les événements basés sur l'hôte et sur le réseau et représente la direction de l'attaque par intrusion. Le Diamond Model of Intrusion Analysis définit sept valeurs potentielles pour cette méta-fonctionnalité : victime à infrastructure, infrastructure à victime, infrastructure à infrastructure, adversaire à infrastructure, infrastructure à adversaire, bidirectionnel ou inconnu.
- Méthodologie - Cette méta-fonctionnalité permettra à un analyste de décrire la classification générale de l'intrusion, par exemple, hameçonnage, DDoS, violation, analyse de port, etc.
- Ressources - Selon le modèle Diamond, chaque événement d'intrusion a besoin d'une ou plusieurs ressources externes pour être satisfait pour réussir. Des exemples de ressources peuvent inclure les éléments suivants : logiciels (par exemple, systèmes d'exploitation, logiciels de virtualisation ou framework Metasploit), connaissances (par exemple, comment utiliser Metasploit pour exécuter l'attaque et exécuter l'exploit), informations (par exemple, un nom d'utilisateur/mot de passe mascarade), matériel (par exemple, serveurs, stations de travail, routeurs), fonds (par exemple, argent pour acheter des domaines), installations (par exemple, électricité ou abri), accès (par exemple, un chemin réseau de l'hôte source à la victime et vice versa, un accès réseau à partir d'un fournisseur de services Internet (ISP)).

Répondre aux questions ci-dessous

À quelle méta-fonctionnalité appartient l'axiome "Toute activité malveillante contient deux phases ou plus qui doivent être exécutées successivement avec succès pour obtenir le résultat souhaité" ?

phase

Bonne réponse

Vous pouvez étiqueter les résultats de l'événement comme "succès", "échec" et "inconnu". À quelle méta-fonctionnalité cela est-il lié ?

result

Bonne réponse

À quelle méta-fonctionnalité s'applique cette phrase "Chaque événement d'intrusion nécessite qu'une ou plusieurs ressources externes soient satisfaites avant de réussir" ?

ressources

Bonne réponse

La composante sociopolitique

La composante sociopolitique décrit les besoins et l'intention de l'adversaire, par exemple, le gain financier, l'acceptation dans la communauté des hackers, le hacktivisme ou l'espionnage.

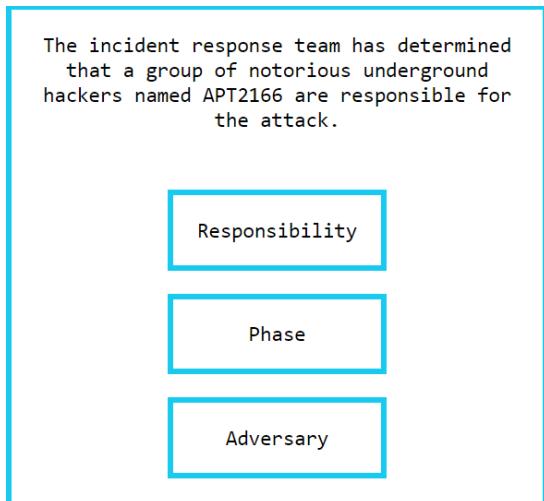
Le scénario peut être que la victime fournit un "produit", par exemple, des ressources informatiques et de la bande passante en tant que zombie dans un botnet pour l'extraction de crypto (produire de nouvelles crypto-monnaies en résolvant des équations cryptographiques à l'aide d'ordinateurs), tandis que l'adversaire consomme leur produit ou obtient un gain financier.

Composante technologique

Technologie - la métá-fonctionnalité ou le composant technologique met en évidence la relation entre les fonctionnalités de base : la capacité et l'infrastructure. La capacité et l'infrastructure décrivent comment l'adversaire opère et communique. Un scénario peut être une attaque de point d'eau qui est une méthodologie dans laquelle l'adversaire compromet des sites Web légitimes qu'il pense que ses victimes ciblées visiteront.

Analyse de la pratique

The incident response team has determined that a group of notorious underground hackers named APT2166 are responsible for the attack.



We learned about this back in Task 2 Adversary.

An **adversary** is also known as an attacker, enemy, cyber threat actor, or hacker. The adversary is the person who stands behind the cyberattack. Cyberattacks can be an instruction or a breach.

Answer: Adversary

2. The attack occurred on 2021-10-23 at 15:45:00:00.000.

The attack occurred on 2021-10-23 at
15:45:00:00.000.



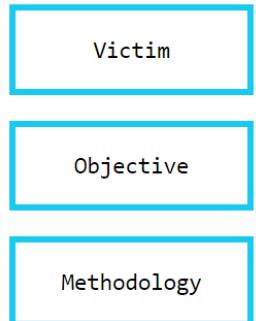
We learned about this back in Task 6 Event Meta Features, they use a different word but they both have the same meaning.

- **Timestamp** - is the date and time of the event. Each event can be recorded with a date and time that it occurred, such as 2021-09-12 02:10:12.136. The timestamp can include when the event started and stopped. Timestamps are essential to help determine the patterns and group the malicious activity. For example, if the intrusion or breach happened at 3 am in the United States, it might be possible that the attack was carried out from a specific country with a different time zone and standard business hours.

Answer: Timeline

3. The attackers targeted the Information Technology (IT) systems of the corporation.

The attackers targeted the Information Technology (IT) systems of the corporation.



We learn about this back at Task 3 Victim.

Victim – is a target of the adversary. A victim can be an organization, person, target email address, IP address, domain, etc. It's essential to understand the difference between the victim persona and the victim assets because they serve different analytic functions.

Answer: Victim

4. The attackers used a recent malware campaign known as OneTrick to ransomware the corporation's servers.

The attackers used a recent malware campaign known as OneTrick to ransomware the corporation's servers.

Methodology

Resources

Infrastructure

We learn about this back at Task 6 Event Meta Features.

- **Resources** - According to the Diamond Model, every intrusion event needs one or more external resources to be satisfied to succeed. Examples of the resources can include the following: software (e.g., operating systems, virtualization software, or Metasploit framework), knowledge (e.g., how to use Metasploit to execute the attack and run the exploit), information (e.g., a username/password to masquerade), hardware (e.g., servers, workstations, routers), funds (e.g., money to purchase domains), facilities (e.g., electricity or shelter), access (e.g., a network path from the source host to the victim and vice versa, network access from an Internet Service Provider (ISP)).

Answer: Resources

5. The attackers stole data from the corporation and sold it on an underground hacking forum.

The attackers stole data from the corporation and sold it on an underground hacking forum.

Capability

Result

Objective

We learn about this back at Task 6 Event Meta Features.

- **Result** - While the results and post-conditions of an adversary's operations will not always be known or have a high confidence value when they are known, they are helpful to capture. It is crucial to capture the results and post-conditions of an adversary's operations, but sometimes they might not always be known. The event results can be labelled as "success," "failure," or "unknown." The event results can also be related to the CIA (confidentiality, integrity, and availability) triad, such as Confidentiality Compromised, Integrity Compromised, and Availability Compromised. Another approach can also be documenting all of the post-conditions resulting from the event, for example, information gathered in the reconnaissance stage or successful passwords/sensitive data exfiltration.

Answer: Result

6. The attackers gained access using legitimate credentials that were gained as a result of a phishing attack.

The attackers gained access using legitimate credentials that were gained as a result of a phishing attack.

Capability

Technique

Victim

We learn about this back at Task 4 Capability.

Capability – is also known as the skill, tools, and techniques used by the adversary in the event. The capability highlights the adversary's tactics, techniques, and procedures (TTPs).

Answer: Capability

7. Once the attackers gained access to the network, they pivoted to the internal databases and file shares.

Once the attackers gained access to the network, they pivoted to the internal databases and file shares.

Result

Capability

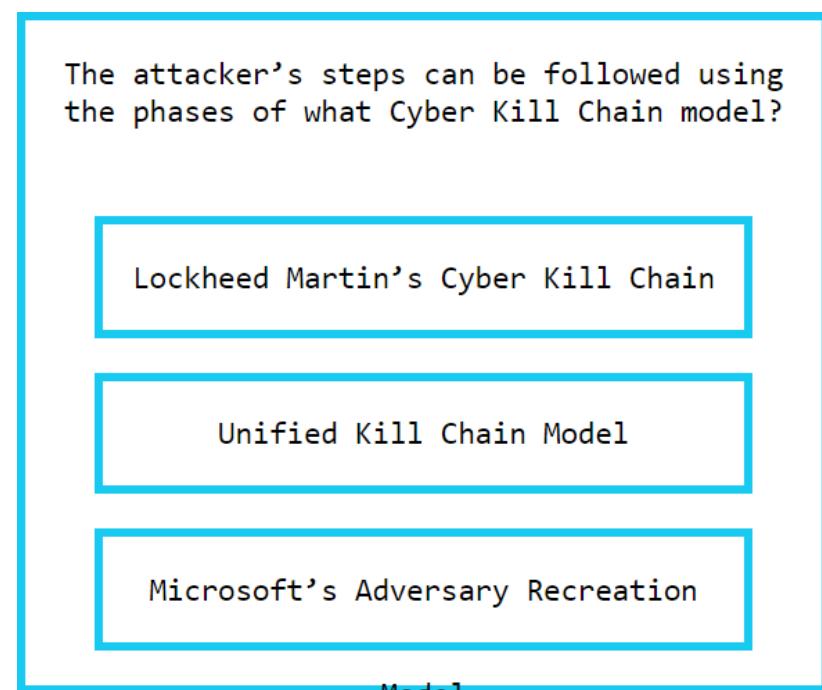
Methodology

We learn about this back at Task 6 Event Meta Features.

- **Methodology** - This meta-feature will allow an analyst to describe the general classification of intrusion, for example, phishing, DDoS, breach, port scan, etc.

Answer: Methodology

8. The attacker's steps can be followed using the phases of what Cyber Kill Chain model?



We learn about this back at Task 6 Event Meta Features.

- Phase - these are the phases of an intrusion, attack, or breach. According to the Diamond Model creators and the Axiom 4, "Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result." Malicious activities don't occur in two or more events rather than just one. A great example can be the Cyber Kill Chain developed by Lockheed Martin. You can find out more about the Cyber Kill Chain by visiting the [Cyber Kill Chain room](#) on TryHackMe
The phases can be:
 1. Reconnaissance
 2. Weaponization
 3. Delivery
 4. Exploitation
 5. Installation
 6. Command & Control
 7. Actions on Objective

Nous espérons que vous avez apprécié cette salle et que vous appliquerez les concepts du modèle Diamond pour perturber l'activité des menaces à l'aide du modèle Diamond et

apporter des informations précieuses à votre équipe et aux dirigeants d'entreprise (C-Suite), un public, un client ou un client qui n'est pas technique.

Le modèle Diamond est une méthode scientifique pour améliorer l'efficacité et la précision de l'analyse des intrusions. Avec cela dans votre arsenal, vous aurez la possibilité de tirer parti des renseignements en temps réel pour la défense du réseau et de prévoir les opérations de l'adversaire.

MITRE

this room will discuss the various resources MITRE has made available for the cybersecurity community.

<https://tryhackme.com/room/mitre>

Introduction



Pour ceux qui sont nouveaux dans le domaine de la cybersécurité, vous n'avez probablement jamais entendu parler de MITRE . Ceux d'entre nous qui ont été dans le coin ne peuvent associer MITRE qu'à la liste CVE ([Common Vulnerabilities and Exposures](#)), qui est une ressource que vous vérifierez probablement lors de la recherche d'un exploit pour une vulnérabilité donnée. Mais MITRE effectue des recherches dans de nombreux domaines, en dehors de la cybersécurité, pour "la sécurité, la stabilité et le bien-être de notre nation". Ces domaines comprennent l'intelligence artificielle, l'informatique de la santé, la sécurité spatiale, pour n'en nommer que quelques-uns.

De [Mitre.org](#) : " Chez MITRE , nous résolvons des problèmes pour un monde plus sûr. Grâce à nos centres de R&D financés par le gouvernement fédéral et à nos partenariats public-privé, nous travaillons à l'échelle du gouvernement pour relever les défis liés à la sécurité, à la stabilité et au bien-être de notre nation. "

Dans cette salle, nous nous concentrerons sur d'autres projets/recherches que l'organisation américaine à but non lucratif MITRE Corporation a créés pour la communauté de la cybersécurité, en particulier :

- Cadre ATT&CK ® (Tactiques , techniques et connaissances communes de l'adversaire)
- Base de connaissances CAR (Cyber Analytics Repository)
- ENGAGE (désolé, pas un acronyme fantaisiste)
- D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense)
- AEP (plans d'émulation ATT&CK)

Plongeons, allons-nous...

Terminologie de base

Avant de plonger, discutons brièvement de quelques termes que vous entendrez souvent lorsque vous traitez du cadre, des renseignements sur les menaces, etc.

APT est l'acronyme de Advanced Persistent Threat . Cela peut être considéré comme une équipe/un groupe (groupe menaçant), ou même un pays (groupe d'États-nations), qui s'engage dans des attaques à long terme contre des organisations et/ou des pays. Le terme « avancé » peut être trompeur car il aura tendance à nous faire croire que chaque groupe APT a tous une super-arme, c'est-à-dire un exploit zero-day, qu'ils utilisent. Ce n'est pas le cas. Comme nous le verrons un peu plus tard, les techniques utilisées par ces groupes APT sont assez courantes et peuvent être détectées avec les bonnes implémentations en place. Vous pouvez consulter la liste actuelle des groupes APT de FireEye [ici](#).

TTP est un acronyme pour Tactiques, Techniques et Procédures, mais que signifie chacun de ces termes ?

- La Tactique est le but ou l'objectif de l'adversaire.
- La technique est la façon dont l'adversaire atteint le but ou l'objectif.
- La procédure est la façon dont la technique est exécutée.

Si ce n'est pas si clair maintenant, ne vous inquiétez pas. Espérons qu'au fur et à mesure que vous progresserez dans chaque section, les TTP auront plus de sens.

Framework ATT&CK



Qu'est-ce que le framework ATT&CK® ? Selon le [site Web](#) , " MITRE ATT&CK® est une base de connaissances accessible dans le monde entier sur les tactiques et techniques de l'adversaire, basée sur des observations du monde réel". En 2013, MITRE a commencé à répondre au besoin d'enregistrer et de documenter les TTP (Tactiques, Techniques et Procédures) courants que les groupes APT (Advanced Persistent Threat) utilisaient contre les réseaux Windows d'entreprise. Cela a commencé avec un projet interne connu sous le nom de FMX (Fort Meade Experiment). Dans le cadre de ce projet, des professionnels de la sécurité sélectionnés ont été chargés d'émuler des TTP contradictoires contre un réseau, et des données ont été collectées à partir des attaques sur ce réseau. Les données recueillies ont aidé à construire les premières pièces de ce que nous connaissons aujourd'hui sous le nom de cadre ATT&CK®.

Le cadre ATT&CK® s'est développé et étendu au fil des ans. Une extension notable était que le cadre se concentrat uniquement sur la plate-forme Windows, mais s'est étendu pour couvrir d'autres plates-formes, telles que macOS et Linux . Le cadre est fortement contribué par de nombreuses sources, telles que des chercheurs en sécurité et des rapports de renseignement sur les menaces. Notez que ce n'est pas seulement un outil pour les équipes bleues. L'outil est également utile pour les équipes rouges .

Si vous ne l'avez pas encore fait, accédez au [site Web](#) d'ATT&CK® .

Dirigez votre attention vers le bas de la page pour afficher la matrice ATT&CK® pour les entreprises . En haut de la matrice, il y a 14 catégories. Chaque catégorie contient les techniques qu'un adversaire pourrait utiliser pour exécuter la tactique. Les catégories couvrent le cycle de vie de la cyberattaque en sept étapes (crédit Lockheed Martin pour la Cyber Kill Chain).



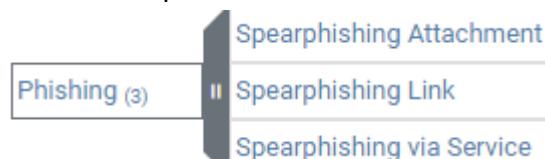
(Matrice ATT&CK v11.2)

Sous Accès initial , il existe 9 techniques. Certaines des techniques ont des sous-techniques, telles que le phishing.

Initial Access



Si on clique sur la barre grise à droite, un nouveau calque apparaît listant les sous-techniques.



Pour mieux comprendre cette technique et ses sous-techniques associées, cliquez sur Phishing .

Nous avons été dirigés vers une page dédiée à la technique connue sous le nom de Phishing et à toutes les informations connexes concernant la technique, telles qu'une brève description, des exemples de procédures et des atténuations .

Phishing

Sub-techniques (3)



Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems or to gather credentials for use of **Valid Accounts**. Phishing may also be conducted via third-party services, like social media platforms.

Vous pouvez également utiliser la fonction de recherche pour récupérer toutes les informations associées concernant une technique, une sous-technique et/ou un groupe donné.

phishing

Phishing, Technique T1566 - Enterprise
Phishing Adversaries may send **phishing** messages to gain access to victim systems. All forms of **phishing** are electronically delivered social engineering. **Phishing** can be targeted, known as spearphish...
Phishing: Spearphishing Attachment, Sub-technique T1566.001 - Enterprise
Phishing: Spearphishing Attachment Adversaries may send spear**phishing** emails with a malicious attachment in an attempt to gain access to victim systems. Spear**phishing** attachment is a specific varian...
Phishing: Spearphishing via Service, Sub-technique T1566.003 - Enterprise
Phishing: Spearphishing via Service Adversaries may send spear**phishing** messages via third-party services in an attempt to gain access to victim systems. Spear**phishing** via service is a specific varia...
Phishing: Spearphishing Link, Sub-technique T1566.002 - Enterprise
Phishing: Spearphishing Link Adversaries may send spear**phishing** emails with a malicious link in an attempt to gain access to victim systems. Spear**phishing** with a link is a specific variant of spear...
Phishing for Information, Technique T1598 - Enterprise
Phishing for Information Before compromising a victim, adversaries may send **phishing** messages to elicit sensitive information that can be used during targeting. **Phishing** for information is an attemp...

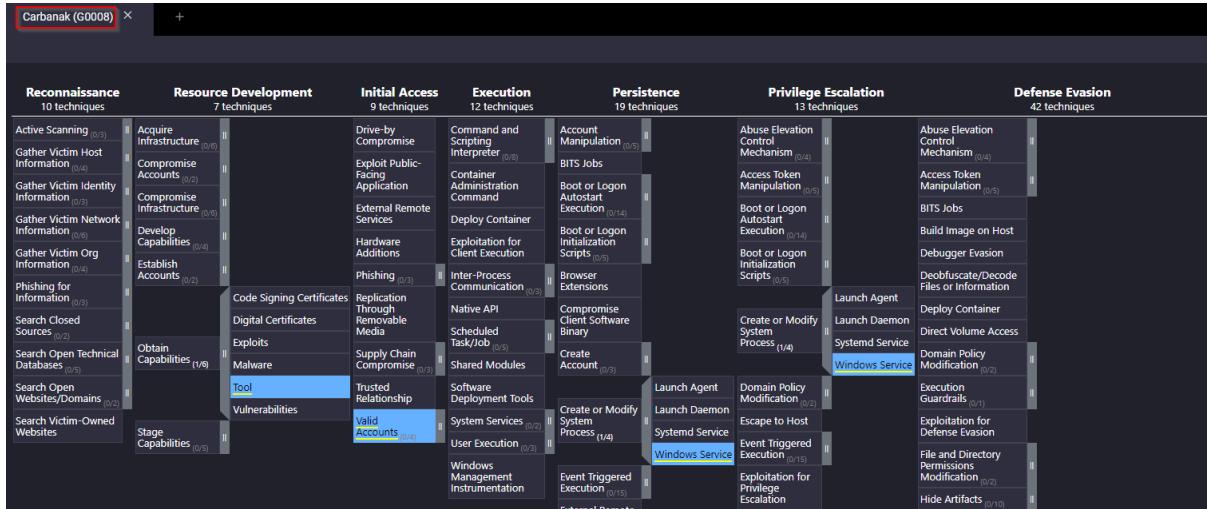
[load more results](#)

Enfin, les mêmes données peuvent être visualisées via le navigateur MITRE ATT&CK® : "Le navigateur ATT&CK® est conçu pour fournir une navigation et une annotation de base des matrices ATT&CK®, ce que les gens font déjà aujourd'hui dans des outils comme Excel. Nous l'avons conçu pour être simple et générique - vous pouvez utiliser le Navigateur pour visualiser votre couverture défensive, la planification de votre équipe rouge/bleue, la fréquence des techniques détectées, ou tout ce que vous voulez faire . "

Vous pouvez accéder à la vue Navigateur lorsque vous visitez une page de groupe ou d'outil. Le bouton ATT&CK® Navigator Layers sera disponible.

ATT&CK® Navigator Layers ▾

Dans le sous-menu, sélectionnez la vue .



Faisons connaissance avec cet outil. Cliquez [ici](#) pour afficher le navigateur ATT&CK® pour Carbanak.

En haut à gauche, il y a 3 ensembles de commandes : commandes de sélection , commandes de calque et commandes de technique . Je vous encourage à inspecter chacune des options sous chaque contrôle pour vous familiariser avec eux. Le point d'interrogation à l'extrême droite fournira des informations supplémentaires concernant le navigateur.



Pour résumer, nous pouvons utiliser la matrice ATT&CK pour mapper un groupe de menaces à leurs tactiques et techniques. Il existe différentes méthodes pour lancer la recherche.

Les questions ci-dessous vous aideront à vous familiariser avec l'ATT&CK®. Il est recommandé de commencer à répondre aux questions à partir de la [page Phishing](#). Notez que ce lien concerne la version 8 de la matrice ATT&CK.

Questions sur le framework ATT&CK

Répondre aux questions ci-dessous

Outre les équipes bleues, qui d'autre utilisera la matrice ATT&CK ? (Red Teamers, Purpe Teamers, SOC Managers ?)

Red Teamers

Bonne réponse

Quel est l'identifiant de cette technique ?

T1566

Bonne réponse

Indice

Sur la base de cette technique, quelle atténuation couvre l'identification des techniques d'ingénierie sociale ?

User Training

Bonne réponse

Quelles sont les sources de données pour la détection ? (**format : source1,source2,source3 sans espaces après les virgules**)

Application Log,File,Nework Traffic

Bonne réponse

Quels groupes ont utilisé le harponnage dans leurs campagnes ? (**format : groupe1,groupe2**)

Axiom,Gold SOUTHFIELD

Bonne réponse

D'après les informations du premier groupe, quels sont leurs groupes associés ?

Group 72

Bonne réponse

Quel logiciel est associé à ce groupe qui répertorie le phishing comme technique ?

Hikit

Bonne réponse

Quelle est la description de ce logiciel ?

Hikit is malware that has been used by Axiom for late-stage persistence and

Bonne réponse

Ce groupe chevauche (légèrement) avec quel autre groupe ?

Winnti Group

Bonne réponse

Combien de techniques sont attribuées à ce groupe ?

15

Bonne réponse

Indice

Cyber Analytics Repository (CAR)

Référentiel Cyber Analytics

La définition officielle de CAR est " Le MITRE Cyber Analytics Repository (CAR) est une base de connaissances d'analyse développée par MITRE sur la base du modèle d'adversaire MITRE ATT&CK ® . CAR définit un modèle de données qui est exploité dans ses représentations de pseudocode mais inclut également des implémentations directement ciblé sur des outils spécifiques (par exemple, Splunk, EQL) dans ses analyses. En ce qui concerne la couverture, CAR se concentre sur la fourniture d'un ensemble d'analyses validées et bien expliquées, en particulier en ce qui concerne leur théorie de fonctionnement et leur justification. "

Au lieu d'essayer d'expliquer davantage ce qu'est la CAR, plongeons-y. Avec nos connaissances nouvellement acquises dans la section précédente, nous devrions nous sentir à l'aise et comprendre les informations que la CAR nous fournit.

Commençons notre voyage en examinant [CAR-2020-09-001 : Tâche planifiée - Accès aux fichiers](#).

Lors de la visite de la page, nous recevons une brève description des analyses et des références à ATT&CK (technique , sous-technique et tactique).

MITRE Cyber Analytics Repository

CAR-2020-09-001: Scheduled Task - FileAccess

In order to gain persistence, privilege escalation, or remote execution, an adversary may use the Windows Task Scheduler to schedule a command to be run at a specified time, date, and even host. Task Scheduler stores tasks as files in two locations - C:\Windows\Tasks (legacy) or C:\Windows\System32\Tasks. Accordingly, this analytic looks for the creation of task files in these two locations.

Technique	Subtechnique(s)	Tactic(s)
Scheduled Task/Job	Scheduled Task	Execution, Persistence, Privilege Escalation

Nous recevons également un pseudocode et une requête sur la façon de rechercher cette analyse spécifique dans Splunk. Un pseudocode est une manière simple et lisible par l'homme de décrire un ensemble d'instructions ou d'algorithmes qu'un programme ou un système exécutera.

Splunk search - Windows task file creation (Splunk, Sysmon native)

This Splunk search looks for any files created under the Windows tasks directories.

```
index=__your_sysmon_index__ EventCode=11 Image!="C:\\WINDOWS\\system32\\svchost.exe" (TargetFilename="C:\\Windows\\System32\\Tasks\\*"
" OR TargetFilename="C:\\Windows\\Tasks\\*")
```

Notez la référence à Sysmon. Si vous n'êtes pas familier avec Sysmon, consultez la [salle](#) Sysmon .

Pour tirer pleinement parti de CAR, nous pouvons afficher la [liste analytique complète](#) ou la [couche CAR ATT&CK® Navigator](#) pour voir toutes les analyses.

Liste analytique complète

Analytics

Analytic List (by date added)

Analytic	ATT&CK Techniques	Implementations	Applicable Platform(s)
----------	-------------------	-----------------	------------------------

Dans la vue Liste analytique complète, nous pouvons voir d'un seul coup d'œil quelles implémentations sont disponibles pour une analyse donnée, ainsi que la plate-forme de système d'exploitation à laquelle elle s'applique.

Navigateur CAR ATTACK

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 36 techniques	Credential Access 14 techniques
Drive-by Compromise	Command and Scripting Interpreter (1/1)	Account Manipulation (0/2) BITS Jobs	Abuse Elevation Control Mechanism (1/2)	Abuse Elevation Control Mechanism (1/2)	Adversary-in-the-Middle (0/2)
Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Autostart Execution (1/15)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)
External Remote Services	Inter-Process Communication (1/2)	Boot or Logon Initialization Scripts (1/5)	Boot or Logon Autostart Execution (3/15)	BITS Jobs	Credentials from Password Stores (0/5)
Hardware Additions	Native API	Browser Extensions	Boot or Logon Initialization Scripts (1/5)	Deobfuscate/Decode Files or Information	Exploitation for Credential Access
Phishing (0/3)	Scheduled Task/Job (2/5)	Compromise Client Software Binary	Create or Modify System Process (1/4)	Direct Volume Access	Forced Authentication
Replication Through Removable Media	Shared Modules	Create Account (1/2)	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Forge Web Credentials (1/2)
Supply Chain Compromise (0/3)	Software Deployment Tools	Create or Modify System Process (1/4)	Escape to Host	Execution Guardrails (0/1)	Input Capture (0/4)
Trusted Relationship	System Services (2/2)	Event Triggered Execution (6/15)	Event Triggered Execution (6/15)	Exploitation for Defense Evasion	Modify Authentication Process (0/4)
Valid Accounts (2/3)	User Execution (1/2)	External Remote Services	Hijack Execution Flow (6/11)	File and Directory Permissions Modification (0/2)	Network Sniffing
	Windows Management Instrumentation	Hijack Execution Flow (6/11)	Hijack Execution Flow (6/11)	Hide Artifacts (1/9)	OS Credential Dumping (3/8)
		Modify Authentication Process (0/4)	Impair Defenses (2/7)	Hijack Execution Flow (6/11)	Steal or Forge Kerberos Tickets (0/4)
		Office Application Startup (0/6)	Scheduled Task/Job (2/5)	Indicator Removal on Host (3/6)	Steal Web Session Cookie
		Pre-OS Boot (0/5)	Valid Accounts (2/3)	Indirect Command Execution	Two-Factor Authentication Interception
		Scheduled Task/Job (2/5)		Masquerading (0/7)	Unsecured Credentials (2/5)
		Server Software Component (1/4)		Modify Authentication Process (0/4)	
				Modify Registry	

(Les techniques soulignées en violet sont les analyses actuellement en RCA)

Examinons une autre analyse pour voir une implémentation différente, [CAR-2014-11-004 : Remote PowerShell Sessions](#).

Sous Implementations, un pseudocode est fourni et une version EQL du pseudocode. EQL (prononcé comme "égal"), et c'est un acronyme pour Event Query Language. EQL peut être utilisé pour interroger, analyser et organiser les données d'événements Sysmon. Vous pouvez en savoir plus à ce sujet [ici](#).

Eql, EQL native

EQL version of the above pseudocode.

```
process where subtype.create and
(process_name == "wsmpprovhost.exe" and parent_process_name == "svchost.exe")
```

Pour résumer, CAR est un endroit idéal pour trouver des analyses qui nous emmènent plus loin que les résumés d'atténuation et de détection dans le cadre ATT&CK ® . Cet outil ne remplace pas ATT&CK ® mais une ressource supplémentaire.

Questions CAR

4.1 For the above analytic, what is the pseudocode a representation of?

Splunk search - Windows task file creation (Splunk, Sysmon native)

This [Splunk search](#) looks for any files created under the Windows tasks directories.

```
index=__your_sysmon_index__ EventCode=11 Image!="C:\WINDOWS\system32\svchost.exe" (TargetFilename="C:\Windows\System32\Tasks\\" OR TargetFilename="C:\Windows\Tasks\\"*)
```

Note the reference to Sysmon. We have not covered Sysmon as of yet, but you can read more about this tool [here](#).

To take full advantage of CAR, we can view the [Full Analytic List](#) or the [CAR ATT&CK® Navigator layer](#) to view all the analytics.

Answer: Splunk Search

4.2 What tactic has an ID of TA0003?

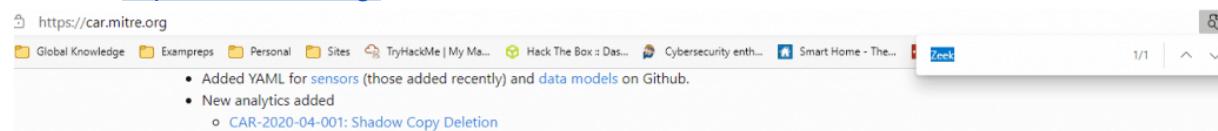
Go to mitre.org and type in the searchbox TA0003. Once found I notice the URL

[Persistence, Tactic TA0003 – Enterprise | MITRE ATT&CK®](#)

Answer: Persistence

4.3 What is the name of the library that is a collection of Zeek (BRO) scripts?

Head to <https://car.mitre.org/> and search for Zeek



Methodology

CAR analytics were developed to detect the adversary behaviors in ATT&CK. Development of an analytic is based upon the following activities:

- identifying and prioritizing adversary behaviors from the ATT&CK adversary model
- identifying the data necessary to detect the adversary behavior
- identification or creation of a sensor to collect the necessary data
- the actual creation of the analytic to detect the identified behaviors

CAR is intended to be shared with cyber-defenders throughout the community.

[This white paper on TTP-based hunting](#) provides some useful insight into many of these activities.

CAR and ATT&CK

It's important to remember that ATT&CK and CAR are separate projects for good reason. It's critical to keep how we articulate threats with ATT&CK separate from a set of possible ways to detect them with the analytics. We don't want the defender content in ATT&CK to be overly prescriptive about how someone can defend against ATT&CK techniques because there could be many different ways, and it's up to the organization implementing them to determine what works best for their environment and the threats they face. This is why we didn't put the analytics in ATT&CK to begin with. CAR is a good starting point for many organizations and can be a great platform for open analytic collaboration - but it isn't the be-all/end-all for defending against the threats described by ATT&CK.

Analytic Source Code Libraries

Some analytics are built as source code for specific products. In these cases, code might support a broad set of detections in a way that makes it hard to describe a set of distinct analytics. For these types of analytics, rather than integrating them into the main CAR site, we've collected them under a library of implementations. Currently, the only library is [BZAR](#), a collection of [Zeek](#) (Bro) scripts looking primarily at SMB and RPC traffic.

Contributing

Answer: BZAR

4.4 What is the name of the technique for running executables with the same hash and different names?

https://car.mitre.org/analytics/

	CAR-2013-04-002	Quick execution of a series of suspicious commands	April 11 2013	• OS Credential Dumping	Dnif, Logpoint, Pseudocode, Sigma
	CAR-2013-05-002	Suspicious Run Locations	May 07 2013	• Masquerading	Dnif, Logpoint, Pseudocode, Sigma
	CAR-2013-05-003	SMB Write Request	May 13 2013	• Lateral Tool Transfer • Remote Services	Pseudocode
	CAR-2013-05-004	Execution with AT	May 13 2013	• Scheduled Task/Job	Dnif, Eql, Logpoint Pseudocode, Splunk
	CAR-2013-05-005	SMB Copy and Execution	May 13 2013	• Remote Services • Valid Accounts	Pseudocode
	CAR-2013-05-009	Running executables with same hash and different names	May 23 2013	• Masquerading	Dnif, Logpoint, Sigma, Splunk

Answer: Masquerading

4.5 Examine CAR-2013-05-004, what additional information is provided to analysts to ensure coverage for this technique?

Go to this URL [CAR-2013-05-004: Execution with AT | MITRE Cyber Analytics Repository](https://car.mitre.org/case/CAR-2013-05-004)

Unit Tests

Test Case 1

Configurations: Windows 7

- From an admin account, open Windows command prompt (right click, run as administrator).
- Execute "at 10:00 calc.exe," substituting a time in the near future for 10:00.
- The program should respond with "Added a new job with job ID = 1" where the job ID is dependent on what tasks are scheduled.
- The program should execute at the time specified. This is what the analytic should fire on.
- To remove the scheduled task, execute "at 1 /delete" where you replace "1" with the job ID output in step 2a above.

```
at 10:00 calc.exe // returns a job number X
at X /delete
```

Answer: Unit Tests

MITRE ENGAGE

Selon le site Web, " MITRE Engage est un cadre de planification et de discussion des opérations d'engagement de l'adversaire qui vous permet d'engager vos adversaires et d'atteindre vos objectifs de cybersécurité. "

MITRE Engage est considéré comme une approche d'engagement avec l'adversaire . Ceci est accompli par la mise en œuvre de Cyber Denial et Cyber Deception .

Avec Cyber Denial, nous empêchons l'adversaire de mener ses opérations et avec Cyber Deception , nous plantons intentionnellement des artefacts pour tromper l'adversaire.

Le site Web Engage fournit un [kit de démarrage](#) pour vous permettre de « démarrer » avec l'approche d'engagement avec l'adversaire. Le kit de démarrage est une collection de livres blancs et de PDF expliquant diverses listes de contrôle, méthodologies et processus pour vous aider à démarrer.

Comme avec MITRE ATT&CK, Engage a sa propre matrice. Vous trouverez ci-dessous un visuel de la matrice Engage .

INTRODUCING THE ENGAGE MATRIX!								
Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

(Source : <https://engage.mitre.org>)

Expliquons rapidement chacune de ces catégories en fonction des informations du site Web Engage.

- Préparez l'ensemble des actions opérationnelles qui mèneront au résultat souhaité (input)
- Exposez les adversaires lorsqu'ils déclenchent vos activités de tromperie déployées
- Affecter les adversaires en effectuant des actions qui auront un impact négatif sur leurs opérations
- Obtenez des informations en observant l'adversaire et apprenez-en plus sur son modus operandi (TTP)
- Comprendre les résultats des actions opérationnelles (output)

Consultez le [manuel Engage](#) pour en savoir plus.

Vous pouvez interagir avec [Engage Matrix Explorer](#) . Nous pouvons filtrer les informations de [MITRE ATT&CK](#) .

Notez que par défaut, la matrice se concentre sur Operate , ce qui implique Expose , Affect et Elicit .

PREPARE **OPERATE** **UNDERSTAND**

Filter by a MITRE ATT&CK®...

Group	Tactic	Technique
-------	--------	-----------

Expose		Affect		Elicit	
Collect	Detect	Prevent	Direct	Disrupt	Reassure
Mitigation	Signature	Baseline	Email Manipulation	Isolation	Application Diversity
Network Monitoring	Lures	Hardware Manipulation	File Manipulation	Lures	Artifact Diversity
Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In
System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation
		Security Controls	Malware Detonation		Information Manipulation
			Network Manipulation		Network Diversity
			Peripheral Management		Peripheral Management
					Personas

Vous pouvez cliquer sur Préparer ou Comprendre si vous souhaitez vous concentrer uniquement sur cette partie de la matrice.

MITRE Engage™

PREPARE **OPERATE** **UNDERSTAND**

Filter by a MITRE ATT&CK®...

Group	Tactic	Technique
-------	--------	-----------

Expose		Affect		Elicit	
Collect	Detect	Prevent	Direct	Disrupt	Reassure
Mitigation	Signature	Baseline	Email Manipulation	Isolation	Application Diversity
Network Monitoring	Lures	Hardware Manipulation	File Manipulation	Lures	Artifact Diversity
Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In
System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation
		Security Controls	Malware Detonation		Information Manipulation
			Network Manipulation		Network Diversity
			Peripheral Management		Peripheral Management
					Personas

Cela devrait suffire pour un aperçu. Nous vous laissons le soin d'explorer les ressources qui vous sont fournies sur ce site Web.

Avant de continuer, pratiquons l'utilisation de cette ressource en répondant aux questions ci-dessous.

Répondre aux questions ci-dessous

Sous Préparer, qu'est-ce que l'ID SAC0002 ?

Persona Creation

Bonne réponse

Quel est le nom de la ressource qui vous aide dans l'activité d'engagement de la question précédente ?

PERSONA PROFILE WORKSHEET

Bonne réponse

Indice

Quelle activité d'engagement appelle une réponse spécifique de l'adversaire ?

Lures

Bonne réponse

Quelle est la définition de Threat Model ?

A risk assessment that models organizational strengths and weaknesses

Bonne réponse

MITRE D3FEND

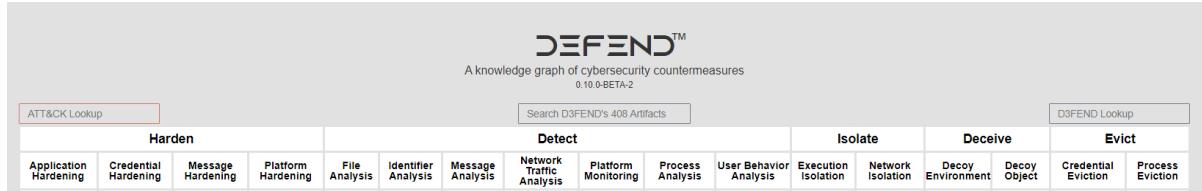
D3FEND

Quelle est cette ressource MITRE ? Selon le site Web [D3FEND](#), cette ressource est « Un graphe de connaissances sur les contre-mesures de cybersécurité ».

D3FEND est toujours en version bêta et est financé par la direction de la cybersécurité de la NSA.

D3FEND signifie Detection, Denial, and Disruption Framework Empowering Network Defense.

Au moment d'écrire ces lignes, il y a 408 artefacts dans la matrice D3FEND. Voir l'image ci-dessous.



Jetons un coup d'œil à l'un des artefacts D3FEND, tel que Decoy File.

This screenshot shows the 'Decoy File' artifact page. At the top, it says 'Decoy File' and 'D3-DF'. On the right, it says 'D3-DF (Decoy File)'. The page contains the following sections:

- Definition:** A file created for the purposes of deceiving an adversary.
- How it works:** The decoy file is made available as a local or network resource. Accesses to the file may be monitored. The files may be configurations, documents, executables, or other file types.
- Considerations:** Properties of the file such as cryptographic checksums, file creation date, file modified date, file size, file owner etc may be modified to improve the credibility of the file.
- Example:**
 - A CSV file with decoy user credentials is placed on a system. The system or network is then monitored to detect any accesses to the decoy files.
- Digital Artifact Relationships:** This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.

At the bottom left, there's a diagram showing a 'Decoy File' node connected by an arrow labeled 'spoofs' to a 'File' node.

Comme vous pouvez le constater, vous recevez des informations sur la technique (définition), son fonctionnement (comment cela fonctionne), les éléments à prendre en compte lors de la mise en œuvre de la technique (considérations) et l'utilisation de la technique (exemple).

Notez que, comme pour les autres ressources MITRE, vous pouvez filtrer en fonction de la matrice ATT&CK.

Étant donné que cette ressource est en version bêta et qu'elle changera considérablement dans les prochaines versions, nous ne passerons pas beaucoup de temps sur D3FEND.

L'objectif de cette tâche est de vous faire prendre conscience de cette ressource MITRE et j'espère que vous garderez un œil dessus à mesure qu'elle mûrira à l'avenir.

Nous vous encourageons tout de même à naviguer un peu sur le site en répondant aux questions ci-dessous.

Répondre aux questions ci-dessous

Quelle est la première technique MITRE ATT&CK répertoriée dans la liste déroulante ATT&CK Lookup ?

Data Obfuscation

Bonne réponse

Dans D3FEND Inferred Relationships , que produit la technique ATT&CK de la question précédente ?

Outbound Internet Network Traffic

Bonne réponse

Plan d'émulation d'att&ck (emulations plans)

Si ces outils qui nous sont fournis par MITRE ne suffisent pas, sous [MITRE ENGENUITY](#) , nous avons CTID , la bibliothèque d'émulation adverse et les plans d'émulation ATT&CK ® .

CTID

MITRE a formé une organisation nommée The [Center of Threat-Informed Defense](#) (CTID). Cette organisation se compose de diverses entreprises et fournisseurs du monde entier. Leur objectif est de mener des recherches sur les cybermenaces et leurs TTP et de partager ces recherches pour améliorer la cybersécurité pour tous.

Certaines des entreprises et des fournisseurs qui participent au CTID :

- AttackIQ (fondateur)
- Verizon
- Microsoft (fondateur)
- Red Canary (fondateur)
- Splunk

Selon le site Web, " En collaboration avec les organisations participantes, nous cultivons des solutions pour un monde plus sûr et faisons progresser la défense informée des menaces avec des logiciels, des méthodologies et des cadres open source. En élargissant la base de connaissances MITRE ATT&CK, notre travail élargit la compréhension globale de cyber-adversaires et leur savoir-faire avec la publication d'ensembles de données essentiels pour mieux comprendre le comportement des adversaires et leurs mouvements. »

Bibliothèque d'émulation d'adversaire et plans d'émulation ATT&CK ®

La [bibliothèque d'émulation d'adversaire](#) est une bibliothèque publique faisant des plans d'émulation d'adversaire une ressource gratuite pour les équipes bleues/rouges. La bibliothèque et les émulations sont une contribution du CTID. Il existe plusieurs [plans d'émulation ATT&CK®](#) actuellement disponibles : [APT3](#) , [APT29](#) et [FIN6](#) . Les plans d'émulation sont un guide étape par étape sur la façon d'imiter le groupe de menaces spécifique. Si l'un des C-Suite demandait, "comment serions-nous si APT29 nous frappait?" On peut facilement y répondre en se référant aux résultats de l'exécution du plan d'émulation.

Passez en revue les plans d'émulation pour répondre aux questions ci-dessous.

(Comme toujours : pour répondre aux questions il faut naviguer à travers les différentes pages (mots avec des liens) et faire des CTRL + F pour rechercher les infos)

Répondre aux questions ci-dessous

Dans la phase 1 du plan d'émulation APT3, qu'est-ce qui est répertorié en premier ?

C2 Setup

Bonne réponse

Sous Persistance, quel binaire a été remplacé par cmd.exe ?

sethc.exe

Bonne réponse

Indice

En examinant APT29, quels frameworks C2 sont répertoriés dans l'infrastructure du scénario 1 ? (format : outil1, outil2)

Pupy, Metasploit Framework

Bonne réponse

Quel cadre C2 est répertorié dans l'infrastructure du scénario 2 ?

PoshC2

Bonne réponse

Examinez le plan d'émulation pour Sandworm. Quel webshell est utilisé pour le scénario 1 ? Vérifiez MITRE ATT&CK pour l'ID du logiciel pour le webshell. Quel est l'identifiant ? (format : webshell, identifiant)

P.A.S., S0598

Bonne réponse

ATT&CK® et Threat Intelligence

Threat Intelligence (TI) ou Cyber Threat Intelligence (CTI) sont les informations, ou TTP, attribuées à l'adversaire. En utilisant le renseignement sur les menaces, en tant que défenseurs, nous pouvons prendre de meilleures décisions concernant la stratégie défensive. Les grandes entreprises peuvent avoir une équipe interne dont l'objectif principal est de recueillir des informations sur les menaces pour d'autres équipes au sein de l'organisation, en plus d'utiliser des informations sur les menaces déjà facilement disponibles. Certaines de ces informations sur les menaces peuvent être open source ou via un abonnement auprès d'un fournisseur, tel que [CrowdStrike](#). En revanche, de nombreux défenseurs portent plusieurs chapeaux (rôles) au sein de certaines organisations, et ils doivent prendre du temps sur leurs autres tâches pour se concentrer sur les renseignements sur les menaces. Pour répondre à ce dernier, nous allons travailler sur un scénario d'utilisation d'ATT&CK® pour le renseignement sur les menaces. L'objectif des renseignements sur les menaces est de rendre les informations exploitables.

Scénario : Vous êtes un analyste de sécurité qui travaille dans le secteur de l'aviation. Votre organisation migre son infrastructure vers le cloud. Votre objectif est d'utiliser la matrice ATT&CK® pour recueillir des informations sur les menaces sur les groupes APT susceptibles de cibler ce secteur particulier et d'utiliser des techniques ciblant vos domaines de préoccupation. Vous vérifiez s'il y a des lacunes dans la couverture. Après avoir sélectionné un groupe, examinez les informations du groupe sélectionné et leurs tactiques, techniques, etc.

Répondre aux questions ci-dessous

Qu'est-ce qu'un groupe qui cible votre secteur et qui est en opération depuis au moins 2013 ?

APT33

Bonne réponse

Alors que votre organisation migre vers le cloud, y a-t-il quelque chose attribué à ce groupe APT sur lequel vous devriez vous concentrer ? Si oui, qu'est-ce que c'est ?

CLOUD accounts

Bonne réponse

Quel outil est associé à la technique de la question précédente ?

Ruler

Bonne réponse

En référence à la technique de la question 2, quelle méthode d'atténuation suggère d'utiliser les SMS comme alternative à sa mise en œuvre ?

Multi-factor Authentication

Bonne réponse

Quelles plateformes la technique de la question 2 affecte-t-elle ?

Azure ad, office 365, Google Workspace, IaaS, SaaS

Bonne réponse

Conclusion

Dans cette salle, nous avons exploré les outils/ressources que MITRE a fournis à la communauté de la sécurité. L'objectif de la salle était de vous exposer à ces ressources et de vous donner une connaissance fondamentale de leurs utilisations. De nombreux fournisseurs de produits de sécurité et équipes de sécurité à travers le monde considèrent ces contributions de MITRE inestimables dans les efforts quotidiens pour contrecarrer le mal. Plus nous avons d'informations en tant que défenseurs, mieux nous sommes équipés pour riposter. Certains d'entre vous envisagent peut-être de faire la transition pour devenir analyste SOC, ingénieur en détection, analyste des cybermenaces, etc. Ces outils/ressources sont indispensables à connaître.

Comme mentionné précédemment, cependant, ce n'est pas seulement pour les défenseurs. En tant que red teamers, ces outils/ressources sont également utiles. Votre objectif est d'imiter l'adversaire et de tenter de contourner tous les contrôles en place dans l'environnement. Avec ces ressources, en tant que red teamer, vous pouvez efficacement imiter un véritable adversaire et communiquer vos découvertes dans un langage commun que les deux parties peuvent comprendre. En un mot, c'est ce qu'on appelle l'association violette .

Endpoint Security (petite parenthèse)

<https://www.youtube.com/watch?v=2CVP9-Qslcw>

Qu'est ce qu'un Endpoint ?

un ordinateur connecté à un réseau est un endpoint pour ce réseau \Leftrightarrow il s'agit de tout device connecté au réseau qui communique avec ce dernier

Exemples de Endpoint : smartphone, laptop ...

Donc il s'agit de point d'entrée potentiel pour les hackers puisqu'ils n'ont pas forcément le même niveau de sécurité que les autres endpoint du network (surtout s'il s'agit d'un nouvel appareil)

Endpoint security \Rightarrow indispensable dans les entreprises qui font du bring your own device = fait référence à toutes les solutions, pratiques et process pour assurer la sécurité des endpoints

Les solutions de endpoint security se basent sur des bdd de menaces existantes dispo en Cloud pour être constamment à jour sur les dernières menaces

On a 3 formes distinctes :

- Endpoint protection platform : pour leurs capacité d'anti malware == similaire à un antivirus car il analyse les fichiers à la recherche de hash malveillant
- Endpoint detection and response (EDR) : avec de l'IA pour détecter des patterns d'attaques (comme décrites sur MITTR par exemple)= analyse comportementale , détecter aussi les zero days, ils collectent également des logs et métadonnées provenant de différents endpoints (poste de travail au sein d'un réseau par exemple) pour travailler et font de la réponses à incidents pour isoler éliminer les menaces en temps réel
- XDR : Extended Detection and Response : pareil que les EDR mais avec des inputs provenant de sources encore plus large \Rightarrow il ne s'agit plus seulement de data provenant d'endpoint mais également provenant d'applications clouds, de serveurs
...

N'importe quelle solutions endpoint security doit être dotée de capacité de cutting edge (= stopper les malwares à l'entrée), d'analyse de fichier en sandbox, peut être automatisé et doit être rapide pour les réponses

2) Cyber Threat Intelligence

Découvrez comment identifier et utiliser les connaissances de sécurité disponibles pour atténuer et gérer les actions potentielles des adversaires

Introduction à Cyber Threat Intel

<https://tryhackme.com/room/cyberthreatintel>

Définition CTI : Cyber Threat Intelligence est une connaissance factuelle des adversaires, y compris leurs indicateurs, tactiques, motivations et conseils exploitables contre eux.

Introduction

Cette salle vous présentera le renseignement sur les cybermenaces (CTI) et divers cadres utilisés pour partager des renseignements. En tant qu'analystes de la sécurité, CTI est essentiel pour enquêter et signaler les attaques d'adversaires avec les parties prenantes de l'organisation et les communautés externes.

Objectifs d'apprentissage

- Les bases du CTI et ses différentes classifications.
- Le cycle de vie suivi pour déployer et utiliser les renseignements lors des enquêtes sur les menaces.
- Cadres et normes utilisés dans la diffusion du renseignement.

Module de renseignements sur les cybermenaces

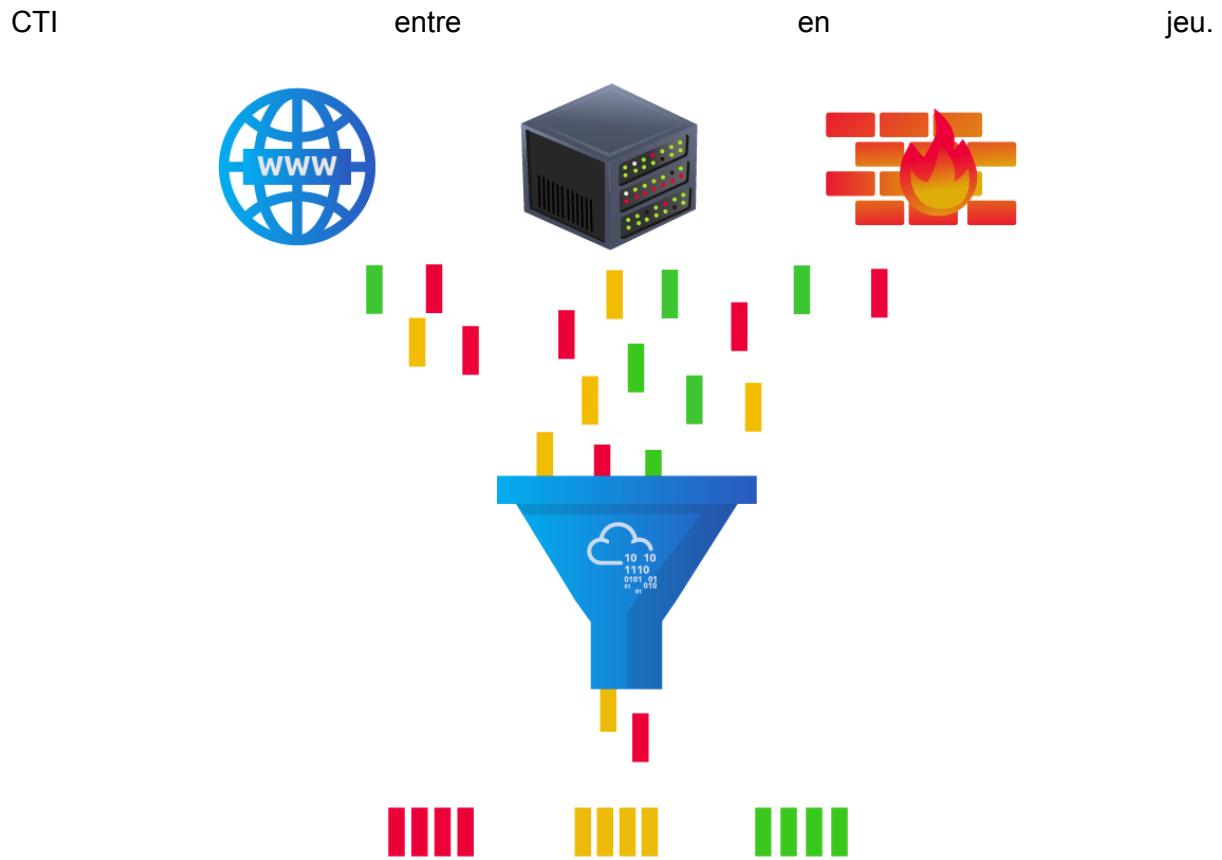
Il s'agit de la première salle d'un nouveau module Cyber Threat Intelligence. Le module contiendra également :

- [Outils de renseignement sur les menaces](#)
- [YARA](#)
- [OpenCTI](#)
- [DMU](#)

Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) peut être défini comme une connaissance factuelle des adversaires, y compris leurs indicateurs, tactiques, motivations et conseils exploitables contre eux. Ceux-ci peuvent être utilisés pour protéger les actifs critiques et informer les équipes de cybersécurité et les décisions commerciales de gestion.

Il serait typique d'utiliser les termes « données », « information » et « renseignement » de manière interchangeable. Cependant, distinguons-les pour mieux comprendre comment le



Données : indicateurs discrets associés à un adversaire, tels que des adresses IP, des URL ou des hachages.

Information : une combinaison de plusieurs points de données qui répondent à des questions telles que "Combien de fois les employés ont-ils accédé à tryhackme.com au cours du mois ?"

Intelligence : La corrélation des données et des informations pour extraire des schémas d'actions basés sur une analyse contextuelle.

L'objectif principal de CTI est de comprendre la relation entre votre environnement opérationnel et votre adversaire et comment défendre votre environnement contre toute attaque. Vous cherchez cet objectif en développant votre contexte de cybermenace en essayant de répondre aux questions suivantes :

- Qui t'attaque ?
- Quelles sont leurs motivations ?
- Quelles sont leurs capacités ?
- Quels artefacts et indicateurs de compromission (IOC) devez-vous rechercher ?

Avec ces questions, les renseignements sur les menaces seraient recueillis auprès de différentes sources dans les catégories suivantes :

- Interne:
 - Événements de sécurité d'entreprise tels que les évaluations de vulnérabilité et les rapports de réponse aux incidents.
 - Rapports de formation sur la sensibilisation à la cyber.
 - Journaux et événements du système.
- Communauté:
 - Ouvrir des forums Web.

- Communautés du dark web pour les cybercriminels.
- Externe
 - Flux de renseignements sur les menaces (commerciaux et open source)
 - Marchés en ligne.
 - Les sources publiques comprennent les données gouvernementales, les publications, les médias sociaux, les évaluations financières et industrielles.

Classifications des renseignements sur les menaces



Threat Intel vise à comprendre la relation entre votre environnement opérationnel et votre adversaire. Dans cet esprit, nous pouvons répartir les informations sur les menaces dans les classifications suivantes :

- Strategic Intel: informations de haut niveau qui examinent le paysage des menaces de l'organisation et cartographient les zones à risque en fonction des tendances, des modèles et des menaces émergentes susceptibles d'avoir un impact sur les décisions commerciales.
- Technical Intel: examine les preuves et les artefacts d'attaque utilisés par un adversaire. Les équipes de réponse aux incidents peuvent utiliser ces informations pour créer une surface d'attaque de base afin d'analyser et de développer des mécanismes de défense.
- Tactical Intel : évalue les tactiques, techniques et procédures (TTP) des adversaires. Ces informations peuvent renforcer les contrôles de sécurité et résoudre les vulnérabilités grâce à des enquêtes en temps réel.

- Operational Intel: examine les motifs spécifiques d'un adversaire et son intention d'effectuer une attaque. Les équipes de sécurité peuvent utiliser ces informations pour comprendre les actifs critiques disponibles dans l'organisation (personnes, processus et technologies) susceptibles d'être ciblés.

Answer the questions below

What does CTI stand for?

Cyber Threat Intelligence

Correct Answer

IP addresses, Hashes and other threat artefacts would be found under which Threat Intelligence classification?

Technical Intel

Correct Answer

Cycle de vie CTI (lifecycle)

Les informations sur les menaces sont obtenues à partir d'un processus de brassage de données qui transforme les données brutes en informations contextualisées et orientées vers l'action, orientées vers le triage des incidents de sécurité. Le processus de transformation suit un cycle en six phases :

Direction

Chaque programme de renseignement sur les menaces nécessite d'avoir des objectifs et des buts définis, impliquant l'identification des paramètres suivants :

- Actifs informationnels et processus métier qui doivent être protégés.
- Impact potentiel à ressentir sur la perte des actifs ou par des interruptions de processus.
- Sources de données et d'informations à utiliser pour la protection.
- Outils et ressources nécessaires pour défendre les actifs.

Cette phase permet également aux analystes de sécurité de poser des questions liées à l'investigation des incidents.



Collection

Une fois les objectifs définis, les analystes de sécurité rassembleront les données nécessaires pour les atteindre. Les analystes le feront en utilisant les ressources

commerciales, privées et open source disponibles. En raison du volume de données auquel les analystes sont généralement confrontés, il est recommandé d'automatiser cette phase afin de laisser le temps de trier les incidents.

Traitement

Les journaux bruts, les informations sur les vulnérabilités, les logiciels malveillants et le trafic réseau se présentent généralement sous différents formats et peuvent être déconnectés lorsqu'ils sont utilisés pour enquêter sur un incident. Cette phase garantit que les données sont extraites, triées, organisées, corrélées avec les balises appropriées et présentées visuellement dans un format utilisable et compréhensible pour les analystes. Les SIEM sont des outils précieux pour y parvenir et permettent une analyse rapide des données.

Analyse

Une fois l'agrégation des informations terminée, les analystes de la sécurité doivent en tirer des informations. Les décisions à prendre peuvent concerner :

- Enquêter sur une menace potentielle en découvrant des indicateurs et des schémas d'attaque.
- Définir un plan d'action pour éviter une attaque et défendre l'infrastructure.
- Renforcer les contrôles de sécurité ou justifier l'investissement pour des ressources supplémentaires.

Dissémination

Différentes parties prenantes de l'organisation consommeront l'intelligence dans différents langages et formats. Par exemple, les membres de la suite C auront besoin d'un rapport concis couvrant les tendances des activités de l'adversaire, les implications financières et les recommandations stratégiques. Dans le même temps, les analystes informeront plus probablement l'équipe technique des IOC de la menace, des TTP de l'adversaire et des plans d'action tactiques.

Retour

La phase finale couvre la partie la plus cruciale, car les analystes s'appuient sur les réponses fournies par les parties prenantes pour améliorer le processus de renseignement sur les menaces et la mise en œuvre des contrôles de sécurité. Les commentaires doivent être une interaction régulière entre les équipes pour que le cycle de vie continue de fonctionner.

Answer the questions below

At which phase of the CTI lifecycle is data converted into usable formats through sorting, organising, correlation and presentation?

processing

Correct Answer

During which phase do security analysts get the chance to define the questions to investigate incidents?

Direction

Correct Answer

CTI Standards & Frameworks

Les normes et les cadres fournissent des structures pour rationaliser la distribution et l'utilisation des informations sur les menaces dans les industries. Ils permettent également une terminologie commune, ce qui facilite la collaboration et la communication. Ici, nous examinons brièvement quelques normes et cadres essentiels couramment utilisés.

MITRE ATT&CK

Le [cadre ATT&CK](#) est une base de connaissances sur le comportement de l'adversaire, axée sur les indicateurs et les tactiques. Les analystes de la sécurité peuvent utiliser les informations pour être approfondis lors de l'enquête et du suivi des comportements contradictoires.

ATT&CK Matrix for Enterprise																	
Reconnaissance		Resource Development		Initial Access		Execution		Persistence		Privilege Escalation		Defense Evasion		Discovery			
10 techniques		Techniques		9 techniques		12 techniques		19 techniques		13 techniques		42 techniques		16 techniques		30 techniques	
Active Scanning (3)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Control Interpreter (3)	# Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	# Abuse Elevation Control Mechanism (3)	# Application Window Discovery	# Account Discovery (4)	Exploitation of Remote Services	# Adversary-in-the-Middle (3)	# Application Layer Protocol (4)	# Automated Exfiltration (1)	Account Removal				
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Applications	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (5)	# Boot or Logon Automation (14)	# Brute Force (4)	Internal Delegating	# Archive Collected Data (2)	# Communication Through Removable Media	Data Transfer Services	Data Destruction				
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	# Boot or Logon Autostart Execution (14)	Boot or Logon Initialization Script (5)	Boot or Logon Initialization Script (5)	# Browser Extensions (3)	Credentials from Password Store (3)	Lateral Tool Transfer	# Browser Bookmark Discovery	# Data Encrypted for Impact	Data Manipulation (3)	Data Impact				
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	# Inter-Process Communication (3)	Replication Through Removable Media	Replication Through Removable Media	# Debugger Evasion (3)	Cloud Infrastructure Discovery	# Audio Capture	# Cloud Service Dashboard	# Defacement (2)	Data Manipulation (2)	Data Impact				
Gather Victim Org Information (4)	Establish Accounts (2)	# Phishing (2)	# Supply Chain Compromise (3)	Native API	Scheduled Task/Job (3)	Create or Modify System State (4)	# Deobfuscate/Decode Files or Scripts (3)	Cloud Service Discovery	# Cloud Storage Object Discovery	# Cloud Session Hijacking (2)	# Disk Wipe (2)	Defacement (2)	Defacement (2)				
Phishing for Information (3)	Obtain Capabilities (3)	# Replication Through Removable Media	Supply Chain Compromise (3)	# Trusted Relationship	# Shared Modules	# Create or Modify System State (4)	# Direct Volume Access	Forced Authentication	# Container and Resource Discovery	# Cloud Storage Object Discovery	# Endpoint Denial of Service (4)	Firmware Corruption	Firmware Corruption				
Search Closed Sources (2)	Stage Capabilities (3)	# Stage Capabilities (3)	# Valid Accounts (4)	Software Deployment Tools	# System Services (2)	# Event Triggered Execution (15)	# Exploit for Defense Evasion	# Exploit Guardrails (1)	# Debugger Evasion	# Cloud Storage Object Discovery	# Inhibit System Recovery	Inhibit System Recovery	Inhibit System Recovery				
Search Open Technical Databases (3)	Search Open Websites/Domains (2)	# Search Open Websites/Domains (2)	# Search Victim-Owned Websites	Windows Management Instrumentation	External Remote Services	# Event Triggered Execution (15)	# File and Directory Manipulation (2)	# Event Triggered Execution (15)	# File and Directory Manipulation (2)	# Container and Resource Discovery	# Network Denial of Service (2)	Network Denial of Service (2)	Network Denial of Service (2)				
						# Hijack Execution Flow (2)	# Hijack Execution Flow (2)	# Hijack Execution Flow (2)	# Hijack Execution Flow (2)	# Group Policy Discovery	# Resource Hijacking	# Service Stop	Service Stop				
						# Impersonation (2)	# Impersonation (2)	# Hide Artifacts (10)	# Impersonation (2)	# Network Service Discovery	# System Shutdown/Reboot		System Shutdown/Reboot				
						# Scheduled Task/Job (3)	# Scheduled Task/Job (3)	# Indicator Removal on Host (3)	# Indicator Removal on Host (3)	# Network Share Discovery							
						# Valid Accounts (4)	# Indirect Command Execution	# OS Credential Disclosure (2)	# OS Credential Disclosure (2)	# Network Sniffing							
							# Malsigning (7)	# Malsigning (7)	# Password Policy Discovery								
							# Modify Authentication Process (6)	# Modify Authentication Process (6)	# Peripheral Device Discovery								
							# Pre-OS Boot (2)	# Pre-OS Boot (2)	# Process Discovery								
							# Pre-OS Boot (2)	# Pre-OS Boot (2)	# Query Registry								
							# Server Software Component (3)	# Server Software Component (3)	# Remote System Discovery								
							# Traffic Signaling (1)	# Traffic Signaling (1)	# Screen Capture								
								# Steal Application Access Token	# Video Capture								
								# Steal Application Cookies									
								# Steal Application Tickets (4)									
								# Steal or Forge Kerberos Tickets (4)									
								# Steal Web Session Cookies									
								# Steal Unsecured Credentials (7)									
								# Modify Registry									

TAXII

Le [Trusted Automated eXchange of Indicator Information \(TAXII\)](#) définit des protocoles pour l'échange sécurisé d'informations sur les menaces afin d'avoir une détection, une prévention et une atténuation des menaces en temps quasi réel. Le protocole prend en charge deux modèles de partage :

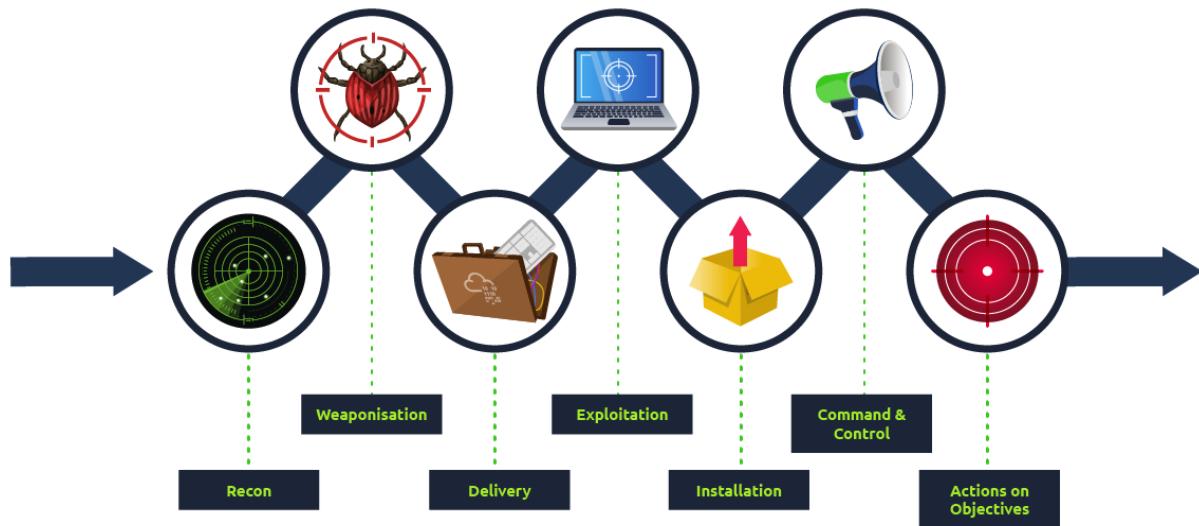
- Collecte : les informations sur les menaces sont collectées et hébergées par un producteur à la demande des utilisateurs à l'aide d'un modèle de demande-réponse.
- Canal : les informations sur les menaces sont transmises aux utilisateurs à partir d'un serveur central via un modèle de publication-abonnement.

STIX

[Structured Threat Information Expression \(STIX\)](#) est un langage développé pour "la spécification, la capture, la caractérisation et la communication d'informations standardisées sur les cybermenaces". Il fournit des relations définies entre des ensembles d'informations sur les menaces telles que des éléments observables, des indicateurs, des TTP adverses, des campagnes d'attaque, etc.

Cyber Kill Chain

Développée par Lockheed Martin, la Cyber Kill Chain décompose les actions adverses en étapes. Cette ventilation aide les analystes et les défenseurs à identifier les activités spécifiques à l'étape qui se sont produites lors de l'enquête sur une attaque. Les phases définies sont présentées dans l'image ci-dessous.



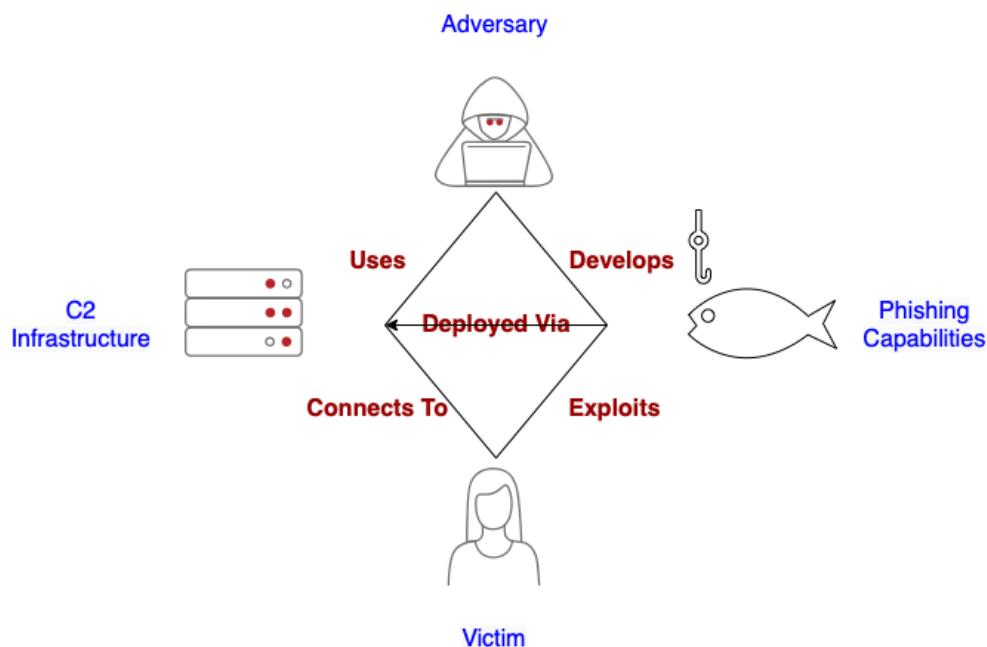
Technique	But	Exemples
Reconnaissance	Obtenir des informations sur la victime et les tactiques utilisées pour l'attaque.	Récolte des e-mails, OSINT et des réseaux sociaux, analyses du réseau
Armement	Les logiciels malveillants sont conçus en fonction des besoins et des intentions de l'attaque.	Exploiter avec une porte dérobée, un document de bureau malveillant
Livraison	Couvre comment le logiciel malveillant serait livré au système de la victime.	Courriel, liens Web, clé USB
Exploitation	Brisez les vulnérabilités du système de la victime pour exécuter du code et créer des tâches planifiées pour établir la persistance.	EternalBlue, Zero-Logon, etc.
Installation	Installez des logiciels malveillants et d'autres outils pour accéder au système de la victime.	Transfert de mots de passe, portes dérobées, chevaux de Troie d'accès à distance

Commandement et contrôle	Contrôlez à distance le système compromis, diffusez des logiciels malveillants supplémentaires, déplacez-vous sur des actifs précieux et élevez les priviléges.	Empire, Frappe de Cobalt, etc.
Actions sur les objectifs	Atteignez les objectifs visés par l'attaque : gain financier, espionnage d'entreprise et exfiltration de données.	Cryptage des données, rançongiciel, dégradation publique

Au fil du temps, la chaîne de mise à mort a été étendue à l'aide d'autres cadres tels que ATT & CK et a formulé une nouvelle chaîne de mise à mort unifiée.

Le modèle de diamant

Le modèle en losange examine l'analyse des intrusions et le suivi des groupes d'attaques dans le temps. Il se concentre sur quatre domaines clés, chacun représentant un point différent sur le diamant. Ceux-ci sont:



- Adversaire : l'accent est mis ici sur l'acteur menaçant à l'origine d'une attaque et permet aux analystes d'identifier le motif de l'attaque.
- Victime : l'extrémité opposée de l'adversaire regarde un individu, un groupe ou une organisation touchée par une attaque.
- Infrastructure : les outils, les systèmes et les logiciels des adversaires pour mener leur attaque sont au centre des préoccupations. De plus, les systèmes de la victime seraient cruciaux pour fournir des informations sur la compromission.
- Capacités : l'accent est mis ici sur l'approche de l'adversaire pour atteindre son objectif. Cela examine les moyens d'exploitation et les TTP mis en œuvre tout au long de la chronologie de l'attaque.

Un exemple du modèle de diamant en jeu impliquerait un adversaire ciblant une victime utilisant des attaques de phishing pour obtenir des informations sensibles et compromettre son système, comme indiqué sur le diagramme. En tant qu'analyste des renseignements sur

les menaces, le modèle vous permet de pivoter le long de ses propriétés pour produire une image complète d'une attaque et corréler les indicateurs.

Answer the questions below

What sharing models are supported by TAXII?

Collection and channel

Correct Answer

Hin

When an adversary has obtained access to a network and is extracting data, what phase of the kill chain are they on?

Actions On Objective

Correct Answer

Practical Analysis

As part of the dissemination phase of the lifecycle, CTI is also distributed to organisations using published threat reports. These reports come from technology and security companies that research emerging and actively used threat vectors. They are valuable for consolidating information presented to all suitable stakeholders. Some notable threat reports come from [Mandiant](#), [Recorded Future](#) and [AT&TCybersecurity](#).

All the things we have discussed come together when mapping out an adversary based on threat intel. To better understand this, we will analyse a simplified engagement example. Click on the green “View Site” button in this task to open the Static Site Lab and navigate through the security monitoring tool on the right panel and fill in the threat details.

Task 5 Practical Analysis



View Site

As part of the dissemination phase of the lifecycle, CTI is also distributed to organisations using published threat reports. These reports come from technology and security companies that research emerging and actively used threat vectors. They are valuable for consolidating information presented to all suitable stakeholders. Some notable threat reports come from [Mandiant](#), [Recorded Future](#) and [AT&TCybersecurity](#).

All the things we have discussed come together when mapping out an adversary based on threat intel. To better understand this, we will analyse a simplified engagement example. Click on the green “View Site” button in this task to open the Static Site Lab and navigate through the security monitoring tool on the right panel and fill in the threat details.

Answer the questions below

What was the source email address?
vipvillain@badbank.com

Correct Answer

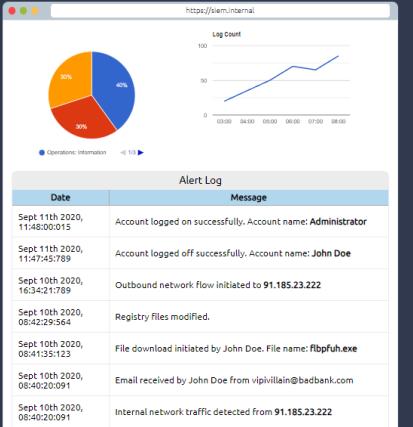
What was the name of the file downloaded?
fbpfuh.exe

Correct Answer

After building the threat profile, what message do you receive?
THIN(NOW_I_CAN_CTL)

Correct Answer

Use the information from the SIEM dashboard to answer all the questions on the threat intel flow chart below.



Alert Log

Date	Message
Sept 11th 2020, 11:48:00+0015	Account logged on successfully. Account name: Administrator
Sept 11th 2020, 11:47:45+0789	Account logged off successfully. Account name: John Doe
Sept 10th 2020, 16:34:21+0709	Outbound network flow initiated to 91.185.23.222
Sept 10th 2020, 08:42:29+064	Registry files modified.
Sept 10th 2020, 08:41:35+123	File download initiated by John Doe. File name: fbpfuh.exe
Sept 10th 2020, 08:40:20+091	Email received by John Doe from vipvillain@badbank.com
Sept 10th 2020, 08:46:20+091	Internal network traffic detected from 91.185.23.222

Threat Actor Extraction IP Address?
Attributed

Threat Actor Email Address?
Uses

Malware Tool?

Intro to CTI

Threat Intelligence Tools

Résolution de la box en vidéo :

<https://www.youtube.com/watch?v=F68zMPAdz-8>

Explore different OSINT tools used to conduct security threat assessments and investigations.

Room Outline

Cette salle couvrira les concepts de Threat Intelligence et divers outils open-source utiles. Les objectifs d'apprentissage comprennent:

- Comprendre les bases du renseignement sur les menaces et ses classifications.
- Utilisation d'UrlScan.io pour rechercher des URL malveillantes.
- Utiliser Abuse.ch pour suivre les indicateurs de malwares et de botnets.
- Enquêter sur les e-mails de phishing à l'aide de PhishTool
- Utilisation de la plate-forme Talos Intelligence de Cisco pour la collecte d'informations.

Urlscan.io

est un service gratuit développé pour aider à scanner et analyser les sites Web. Il est utilisé pour automatiser le processus de navigation et d'exploration des sites Web pour enregistrer les activités et les interactions.

Lorsqu'une URL est soumise, les informations enregistrées comprennent les domaines et les adresses IP contactés, les ressources demandées aux domaines, un instantané de la page Web, les technologies utilisées et d'autres métadonnées sur le site Web.

Le site propose deux vues, la première affichant les analyses les plus récentes effectuées et la seconde affichant les analyses en direct en cours.

URL to scan



Recent scans

URL	Age	Size	IPs	Flags	Country
www.clevescene.com/	22 seconds	7 MB	161	45	4
shopee.co.id/greetnightwear?af_click_lookback=7d&af_reengagement_window=7d &af_s...	25 seconds	6 MB	170	22	4
www.blablacar-tickets.store/	25 seconds	294 KB	15	7	4
www.mountsinai.org/locations/morningside/care/rehab?utm_source=Text&utm_me dium=...	26 seconds	3 MB	153	55	5
www.wittl-it.de/	27 seconds	192 KB	7	1	1
www.paypal.com/signin?returnUri=https://www.paypal.com/myaccount/transfer/se nd/...	27 seconds	890 KB	51	8	2
seguro.olivedream.com.br/cart	29 seconds	1 MB	37	18	4
www.megaratv.gr/	30 seconds	5 MB	222	27	5
101wap.php/user/charlesvillarreal97/ 	30 seconds	494 KB	44	3	1
writeablog.net/hatfrown6/puaka-slot-online	33 seconds	107 KB	9	4	3

Résultats de l'analyse

Les résultats de l'analyse d'URL fournissent de nombreuses informations, les domaines clés suivants étant essentiels à examiner :

- Résumé : Fournit des informations générales sur l'URL, allant de l'adresse IP identifiée, aux détails d'enregistrement du domaine, à l'historique des pages et à une capture d'écran du site.
- HTTP : Fournit des informations sur les connexions HTTP établies par le scanner au site, avec des détails sur les données récupérées et les types de fichiers reçus.
- Redirections : affiche des informations sur toutes les redirections HTTP et côté client identifiées sur le site.
- Liens : affiche tous les liens identifiés sortant de la page d'accueil du site.
- Comportement : Fournit des détails sur les variables et les cookies trouvés sur le site. Ceux-ci peuvent être utiles pour identifier les cadres utilisés dans le développement du site.
- Indicateurs : répertorie toutes les adresses IP, domaines et hachages associés au site. Ces indicateurs n'impliquent pas d'activité malveillante liée au site.

urlscan.io Home Search Live API Blog Docs Pricing Login Sponsored by SecurityTrails

www.premierleague.com 1
2600:9000:223f:5000:c:570c:d000:93a1

Submitted URL: <http://premierleague.com/>
Effective URL: <https://www.premierleague.com/>
Submission Tags: tranco_J324

Submission: On October 27 via api (October 27th 2021, 4:24:33 am UTC) from DE — Scanned from DE

[Summary](#) [HTTP 259](#) [Redirects](#) [Links 65](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary 2

This website contacted 24 IPs in 4 countries across 17 domains to perform 259 HTTP transactions. The main IP is 2600:9000:223f:5000:c:570c:d000:93a1, located in United States and belongs to AMAZON-02, US. The main domain is www.premierleague.com. TLS certificate: Issued by Amazon on April 4th 2021. Valid for: a year.

[premierleague.com](#) scanned 173 times on urlscan.io [Show Scans 173](#)
[www.premierleague.com](#) scanned 72 times on urlscan.io [Show Scans 72](#)

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for www.premierleague.com
Current DNS A record: 143.204.98.72 (AS16509 - AMAZON-02, US)
Domain created: July 16th 1997, 03:00:00 (UTC)
Domain registrar: CSC CORPORATE DOMAINS, INC.

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
1 1	IP Address 13.248.130.246	AS 16509 (AMAZON-02)				
48	2600:9000:223f:5000:c:570c:d000:93a1	16509 (AMAZON-02)				
1	2600:9000:2250:f400:0:7885:2100:93a1	16509 (AMAZON-02)				
1	2a00:1450:4001:813::2002	15169 (GOOGLE)				
1	2a00:1450:4001:831::200a	15169 (GOOGLE)				

Screenshot [Live screenshot](#) [Full Image](#)

Page URL History [Show full URLs](#)

1. <http://premierleague.com/>
<https://www.premierleague.com/>

Detected technologies

- DoubleClick for Publishers (DFP) (Advertising Networks) [Expand](#)
- Google AdSense (Advertising Networks) [Expand](#)
- Google Analytics (Analytics) [Expand](#)
- Google Tag Manager (Tag Managers) [Expand](#)
- Polyfill (JavaScript Libraries) [Expand](#)

Page Statistics

259	98 %	64 %	17	26
Requests	HTTPS	IPv6	Domains	Subdomains

Scénario

Vous avez été chargé d'effectuer une analyse sur le domaine de TryHackMe. Les résultats obtenus sont affichés dans l'image ci-dessous. Utilisez les détails sur l'image pour répondre aux questions :

urlscan.io Home Search Live API Blog Docs Pricing Login Sponsored by SecurityTrails

tryhackme.com

2606:4700:10::ac43:1b0a

Submitted URL: <http://www.tryhackme.com/>

Effective URL: <https://tryhackme.com/>

Submission: On April 20 via manual (April 20th 2022, 5:22:48 pm UTC) from KE — Scanned from DE

Q Lookup ▾ Go To C Rescan
Add Verdict Report

[Summary](#) [HTTP 109](#) [Redirects](#) [Links 9](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary

This website contacted 17 IPs in 4 countries across 13 domains to perform 109 HTTP transactions. The main IP is 2606:4700:10::ac43:1b0a, located in United States and belongs to CLOUDFLARENET, US. The main domain is tryhackme.com. The Cisco Umbrella rank of the primary domain is 345612.

TLS certificate: Issued by E1 on March 25th 2022. Valid for: 3 months.

www.tryhackme.com scanned 30 times on urlscan.io

Show Scans 30

tryhackme.com scanned 239 times on urlscan.io

Show Scans 239

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for tryhackme.com
Current DNS A record: 104.22.55.228 (AS13335 - CLOUDFLARENET, US)
Domain created: July 5th 2018, 22:46:15 (UTC)
Domain registrar: NAMECHEAP INC

Screenshot



Live screenshot Full Image

Page URL History

1. <http://www.tryhackme.com/> <https://tryhackme.com/> [Page URL](#)

Show full URLs

Detected technologies

Paths.js (JavaScript Graphics)	Expand
Bootstrap (Web Frameworks)	Expand
animate.css (Web Frameworks)	Expand
Font Awesome (Font Scripts)	Expand
Google Analytics (Analytics)	Expand
Google Tag Manager (Tag Managers)	Expand
Osano (Cookie compliance)	Expand
Slick (JavaScript Libraries)	Expand
jQuery (JavaScript Libraries)	Expand
reCAPTCHA (Captchas)	Expand

Answer the questions below

What is TryHackMe's Cisco Umbrella Rank?

345612

How many domains did UrlScan.io identify?

13

What is the main domain registrar listed?

NAMECHEAP INC

What is the main IP address identified?

2606:4700:10::ac43:1b0a

Abuse.ch

[Abus.ch](#) est un projet de recherche hébergé par l'Institut pour la cybersécurité et l'ingénierie de l'Université des sciences appliquées de Berne en Suisse. Il a été développé pour identifier et suivre les logiciels malveillants et les botnets via plusieurs plates-formes opérationnelles développées dans le cadre du projet. Ces plateformes sont :

- Malware Bazaar : une ressource pour partager des échantillons de logiciels malveillants.
- Feodo Tracker : une ressource utilisée pour suivre l'infrastructure de commande et de contrôle (C2) du botnet lié à Emotet, Dridex et TrickBot.
- SSL Blacklist : Une ressource pour collecter et fournir une liste de blocage pour les certificats SSL malveillants et les empreintes digitales JA3/JA3s.
- URL Haus : une ressource pour partager des sites de distribution de logiciels malveillants.
- Threat Fox : une ressource pour partager des indicateurs de compromission (IOC).

Examinons ces plates-formes individuellement.

[MalwareBazaar](#)

Comme son nom l'indique, ce projet est une base de données de collecte et d'analyse de logiciels malveillants tout-en-un. Le projet prend en charge les fonctionnalités suivantes :

- Téléchargement d'échantillons de logiciels malveillants : les analystes de sécurité peuvent télécharger leurs échantillons de logiciels malveillants pour analyse et créer la base de données de renseignements. Cela peut être fait via le navigateur ou une API.
- Chasse aux logiciels malveillants : la recherche d'échantillons de logiciels malveillants est possible grâce à la configuration d'alertes correspondant à divers éléments tels que les balises, les signatures, les règles YARA, les signatures ClamAV et la détection des fournisseurs.

The screenshot shows the MalwareBazaar homepage. At the top, there's a dark header bar with the text "MALWARE bazaar" and "abuse.ch". Below the header, the main title "MalwareBazaar" is prominently displayed. A subtext below the title states: "MalwareBazaar is a project from abuse.ch with the goal of sharing malware samples with the infosec community, AV vendors and threat intelligence providers." There's a blue button labeled "MalwareBazaar database »". The page is divided into several sections: "API" (with a subtext about integrating threat intel), "MalwareBazaar database" (with a subtext about getting insights and browsing the database), and "Get involved" (with a subtext about sharing malware samples). Each section has a "View details »" button. At the bottom left, there's a copyright notice: "© abuse.ch 2022".

[FeodoTracker](#)

Avec ce projet, Abuse.ch vise à partager des renseignements sur les serveurs botnet Command & Control (C&C) associés à Dridex, Emotes (alias Heodo), TrickBot, QakBot et BazarLoader/BazarBackdoor. Ceci est réalisé en fournissant une base de données des serveurs C&C dans laquelle les analystes de sécurité peuvent effectuer des recherches et enquêter sur toutes les adresses IP suspectes qu'ils ont rencontrées. En outre, ils fournissent diverses listes de blocage IP et IOC et des informations d'atténuation à utiliser pour prévenir les infections de botnet.

The screenshot shows the Feodo Tracker homepage. At the top, there's a green header bar with the text "FEODO tracker" and a "Mitigate" button. Below the header, the main title "Feodo Tracker" is displayed in a large, bold font. A subtext explains the project's goal: "Feodo Tracker is a project of abuse.ch with the goal of sharing botnet C&C servers associated with Dridex, Emotet (aka Heodo), TrickBot, QakBot (aka QualiBot / Qbot) and BazarLoader (aka BazarBackdoor). It offers various blocklists, helping network owners to protect their users from Dridex and Emotet/Heodo." A prominent green button labeled "Download Blocklist »" is located below this text. The page is divided into three main sections: "Botnet C&Cs", "Blocklist", and "About". Each section has a brief description and a "View details »" button. At the bottom left, there's a copyright notice: "© abuse.ch 2022".

Liste noire SSL (blacklist ssl)

Abus.ch a développé cet outil pour identifier et détecter les connexions SSL malveillantes. À partir de ces connexions, les certificats SSL utilisés par les serveurs de botnet C2 seraient identifiés et mis à jour sur une liste de refus fournie pour utilisation. La liste de blocage est également utilisée pour identifier les empreintes digitales JA3 qui aideraient à détecter et à bloquer les communications du botnet C2 malveillant sur la couche TCP.

Vous pouvez parcourir les certificats SSL et les listes d'empreintes digitales JA3 ou les télécharger pour les ajouter à votre liste de refus ou à vos ensembles de règles de chasse aux menaces.

URLhaus

Comme son nom l'indique, cet outil se concentre sur le partage d'URL malveillantes utilisées pour la distribution de logiciels malveillants. En tant qu'analyste, vous pouvez rechercher dans la base de données les domaines, les URL, les hachages et les types de fichiers suspectés d'être malveillants et valider vos investigations.

L'outil fournit également des flux associés au pays, au numéro AS et au domaine de premier niveau qu'un analyste peut générer en fonction de besoins de recherche spécifiques.

ThreatFox

Avec ThreatFox, les analystes de sécurité peuvent rechercher, partager et exporter des indicateurs de compromission associés à des logiciels malveillants. Les IOC peuvent être exportés dans divers formats tels que les événements MISP, l'ensemble de règles Suricata

IDS, les fichiers d'hôte de domaine, la zone de politique de réponse DNS, les fichiers JSON et les fichiers CSV.



Questions réponses

L'IOC 212.192.246.30:5555 est identifié sous quel nom d'alias de malware sur ThreatFox ?

Type **ioc:212.192.246.30:5555** in the search box (ThreatFox)

The screenshot shows a ThreatFox search interface. At the top, there is a search bar with placeholder text "See search syntax see below, example: malware:ZLoader" and a "Search" button. Below the search bar is a "Search Syntax" help section. The main area displays a table of search results. The table has columns: Date (UTC), IOC, Malware, Tags, and Reporter. One row is visible, showing the date 2022-03-15 07:20, the IOC 212.192.246.30:5555, the malware name Mirai, the tag Mirai, and the reporter @abuse_ch.

Date (UTC)	IOC	Malware	Tags	Reporter
2022-03-15 07:20	212.192.246.30:5555	Mirai	Mirai	@abuse_ch

You are viewing the ThreatFox database entry for ip:port 212.192.246.30:5555.

Database Entry

IOC ID:	395319
IOC:	212.192.246.30:5555
IOC Type ⓘ:	ip:port
Threat Type ⓘ:	botnet_cc
Malware:	Mirai
Malware alias:	
Confidence Level ⓘ:	的信心水平已提升至75%
First seen:	2022-03-15 07:20:31 UTC

Quel malware est associé à JA3 Fingerprint 51c64c77e60f3980eea90869b68c58a8 sur SSL Blacklist ?

JA3 Fingerprints

Here you can browse a list of malicious JA3 fingerprints identified by SSLBL. JA3 is an [open source tool](#) used to fingerprint SSL/TLS client applications. In the best case, you can use JA3 to identify malware traffic that is leveraging SSL/TLS.

Caution!

The JA3 fingerprints below have been collected by analysing more than 25,000,000 PCAPs generated by malware samples. These fingerprints have **not been tested against known good traffic yet and may cause a significant amount of FPs!**

Show

50

entries

Search:

51c64c77e60f3980eea90



Listing Date (UTC)	JA3 Fingerprint	Listing Reason	Malware Samples
2018-12-17 07:47:19	51c64c77e60f3980eea90869b68c58a8	Dridex	221'880

Showing 1 to 1 of 1 entries (filtered from 1 total)

Previous 1 Next

PhishTool : outil pour analyser des mails de phishing potentiels

Avant de vous lancer dans la tâche, n'oubliez pas de cliquer sur le bouton Démarrer la machine pour démarrer la machine virtuelle attachée et l'ouvrir en vue fractionnée. Vous utiliserez la même machine pour les tâches 7 et 8.

Le phishing par e-mail est l'un des principaux précurseurs de toute cyberattaque. Les utilisateurs peu méfiants sont dupés dans l'ouverture et l'accès aux fichiers et liens malveillants qui leur sont envoyés par e-mail, car ils semblent légitimes. En conséquence, les pirates infectent les systèmes de leurs victimes avec des logiciels malveillants, récupèrent leurs informations d'identification et leurs données personnelles et effectuent d'autres actions telles que la fraude financière ou la conduite d'attaques de ransomwares.

Pour plus d'informations et de contenu sur le phishing, consultez ces salles :

- [E-mails d'hameçonnage 1](#)
- [E-mails d'hameçonnage 2](#)
- [E-mails d'hameçonnage 3](#)
- [E-mails d'hameçonnage 4](#)
- [E-mails d'hameçonnage 5](#)

[PhishTool](#) cherche à éléver la perception du phishing comme une forme d'attaque grave et à fournir un moyen réactif de sécurité des e-mails. Grâce à l'analyse des e-mails, les analystes de la sécurité peuvent découvrir les IOC des e-mails, prévenir les violations et fournir des rapports forensics qui pourraient être utilisés dans le cadre de missions de confinement et de formation contre le phishing.

PhishTool a deux versions accessibles : Community et Enterprise . Nous nous concentrerons principalement sur la version communautaire et les principales fonctionnalités de cette tâche. Créez un compte via ce [lien](#) pour utiliser l'outil.

Les fonctionnalités principales incluent :

- Effectuer une analyse des e-mails : PhishTool récupère les métadonnées des e-mails de phishing et fournit aux analystes les explications et les fonctionnalités pertinentes pour suivre les actions, les pièces jointes et les URL de l'e-mail afin de trier la situation.
- Intelligence heuristique : OSINT est intégré à l'outil pour fournir aux analystes les renseignements nécessaires pour garder une longueur d'avance sur les attaques persistantes et comprendre quels TTP ont été utilisés pour échapper aux contrôles de sécurité et permettre à l'adversaire de créer une cible par ingénierie sociale.
- Classification et rapports : des classifications d'e-mails d'hameçonnage sont effectuées pour permettre aux analystes d'agir rapidement. De plus, des rapports peuvent être générés pour fournir un dossier médico-légal qui peut être partagé.

Des fonctionnalités supplémentaires sont disponibles sur la version Enterprise :

- Gérer les événements de phishing signalés par les utilisateurs.
- Signalez les découvertes d'e-mails de phishing aux utilisateurs et maintenez-les engagés dans le processus.
- Intégration de la pile de messagerie avec Microsoft 365 et Google Workspace.

Un écran de téléchargement de fichier nous est présenté à partir de l'onglet Analyse lors de la connexion. Ici, nous soumettons notre e-mail pour analyse dans les formats de fichier indiqués. Les autres onglets incluent :

- Historique : répertorie toutes les soumissions faites avec leurs résolutions.

- Boîte de réception : fonctionnalité d'entreprise utilisée pour recevoir et traiter les rapports d'hameçonnage publiés par les membres de l'équipe via l'intégration de Google Workspace et de Microsoft 365.



Onglet Analyse

Une fois téléchargé, les détails de notre e-mail nous sont présentés pour un examen plus approfondi. Ici, nous avons les onglets suivants :

- En-têtes : Fournit les informations de routage de l'e-mail, telles que les adresses e-mail source et de destination, les adresses IP et DNS d'origine et l'horodatage.
- Lignes reçues : détails sur le processus de traversée des e-mails sur divers serveurs SMTP à des fins de traçage.
- En-têtes X : il s'agit d'en-têtes d'extension ajoutés par la boîte aux lettres du destinataire pour fournir des informations supplémentaires sur l'e-mail.
- Sécurité : détails sur les cadres et politiques de sécurité des e-mails tels que Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) et Domain-based Message Authentication, Reporting and Conformance (DMARC).
- Pièces jointes : répertorie toutes les pièces jointes trouvées dans l'e-mail.
- URL des messages : les URL externes associées trouvées dans l'e-mail se trouvent ici.

Nous pouvons en outre effectuer des recherches et signaler les indicateurs comme malveillants à partir de ces options. Sur le côté droit de l'écran, nous sommes présentés avec les détails du texte brut et de la source de l'e-mail.

Your Piktochart account has been closed

From: no-reply@notifications.piktochart.com

Display name: None

To: [REDACTED]

CC: None

Timestamp: 09:20 pm, Jan 25th 2022

Reply-To: None

Return-Path: vbslbd@psrp.notifications.piktochart.com

Originating IP: 34.192.122.214 (Received-SPF) ▾
smtp.piktochart.com

DNS:

Rendered: PlainText HTML Source

PIKTOCHART

Your Piktochart account has been closed

The account under [REDACTED] has been closed.

A backup file of your visuals is available [here](#).

The download link will only be available for a week.

f t p i g y

This is an automatically generated email, please do not reply.

Au-dessus de la section Texte brut , nous avons une coche Résoudre . Ici, nous arrivons à effectuer la résolution de notre analyse en classant l'e-mail, en configurant des artefacts signalés et en définissant les codes de classification. Une fois l'e-mail classé, les détails apparaîtront dans l'onglet Résolution de l'analyse de l'e-mail.

Monthly Update

From: JerryGud@F1nachB@nk.com

Display name: Jerry Gud

To: Steve@FinanchB

CC: None

Timestamp: None

Reply-To: None

Return-Path: JerryGud@F1nachB@nk.com

Originating IP: None

DNS:

Rendered: HTML Source

Hey Steve, Find the month's updated file attached.

Vous pouvez désormais ajouter PhishTool à votre liste d'outils d'analyse d'e-mails.

Scénario

Vous êtes un analyste SOC et avez été chargé d' analyser un e-mail suspect Email1.eml . Pour résoudre la tâche, ouvrez l'e-mail à l'aide de Thunderbird sur la machine virtuelle jointe , analysez-le et répondez aux questions ci-dessous.

Answer the questions below

What social media platform is the attacker trying to pose as in the email?

Linkedin

Correct Answer

Hi

What is the senders email address?

darkabutka@sc500.whpservers.com

Correct Answer

What is the recipient's email address?

cabbagecare@hotmail.com

Correct Answer

What is the Originating IP address? Defang the IP address.

204[.]93[.]183[.]11

Correct Answer

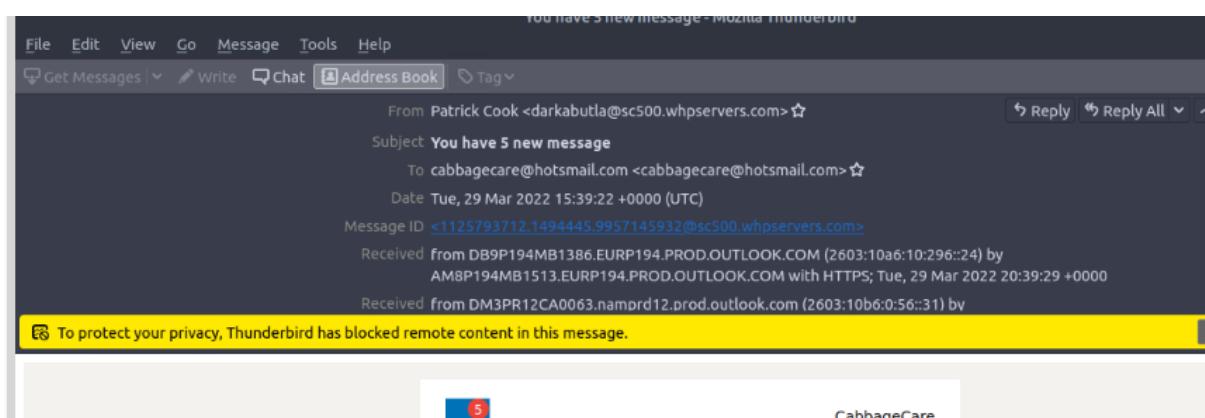
Hi

How many hops did the email go through to get to the recipient?

4

Correct Answer

Dans modzilla on peut faire view>headers> all, ce qui nous permet de visualiser plein d'informations sur le trajet des paquets, l'ip expéditeur...



Et donc la dedans on trouve X sender IP

Et on voit qu'il y a 4 machines en received ⇔ 4 sauts au final avant d'arriver au destinataire final

Cisco Talos Intelligence

Les entreprises informatiques et de cybersécurité collectent dénormes quantités d'informations qui pourraient être utilisées à des fins d'analyse des menaces et de renseignement. Étant l'une de ces sociétés, Cisco a réuni une grande équipe de praticiens de la sécurité appelée Cisco Talos pour fournir des renseignements exploitables, une visibilité sur les indicateurs et une protection contre les menaces émergentes grâce aux données collectées à partir de leurs produits. La solution est accessible sous le nom de [Talos Intelligence](#).

Cisco Talos regroupe six équipes clés :

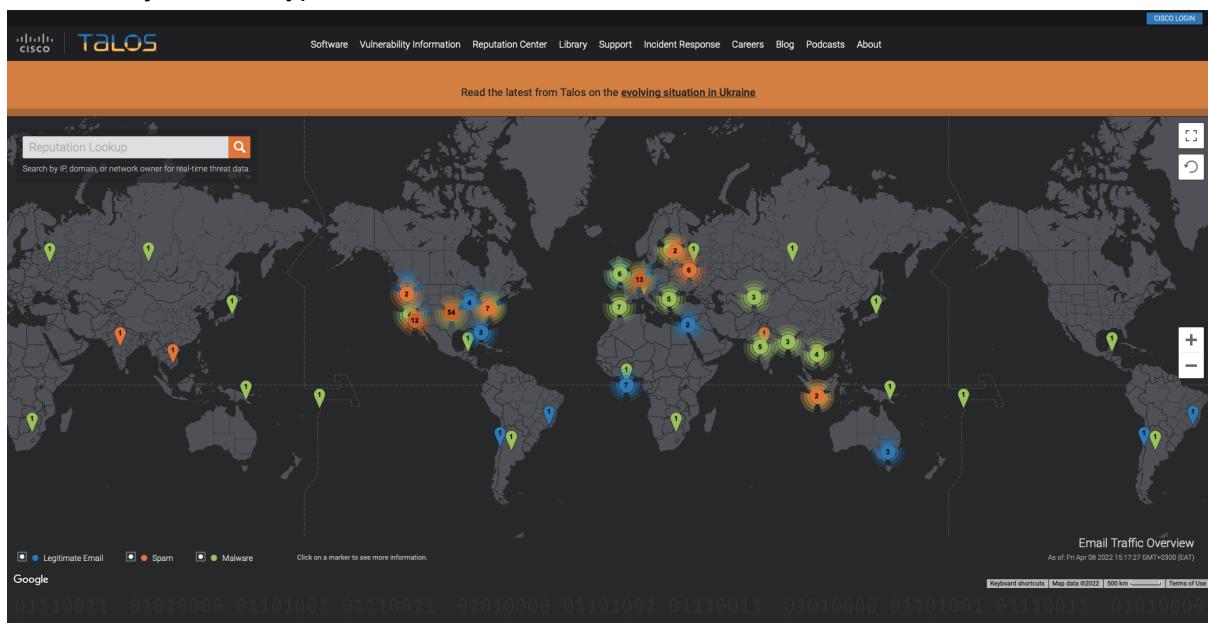
- Intelligence sur les menaces et interdiction : la corrélation et le suivi rapides des menaces permettent de transformer de simples IOC en informations riches en contexte.

- Recherche de détection : une analyse des vulnérabilités et des logiciels malveillants est effectuée pour créer des règles et du contenu pour la détection des menaces.
- Ingénierie et développement : fournit le support de maintenance pour les moteurs d'inspection et les maintient à jour pour identifier et trier les menaces émergentes.
- Recherche et découverte de vulnérabilités : travailler avec des fournisseurs de services et de logiciels pour développer des moyens reproductibles d'identification et de reporting des vulnérabilités de sécurité.
- Communautés : entretient l'image de l'équipe et des solutions open source.
- Sensibilisation mondiale : diffuse des renseignements aux clients et à la communauté de la sécurité par le biais de publications.

Plus d'informations sur Cisco Talos peuvent être trouvées dans leur [livre blanc](#).

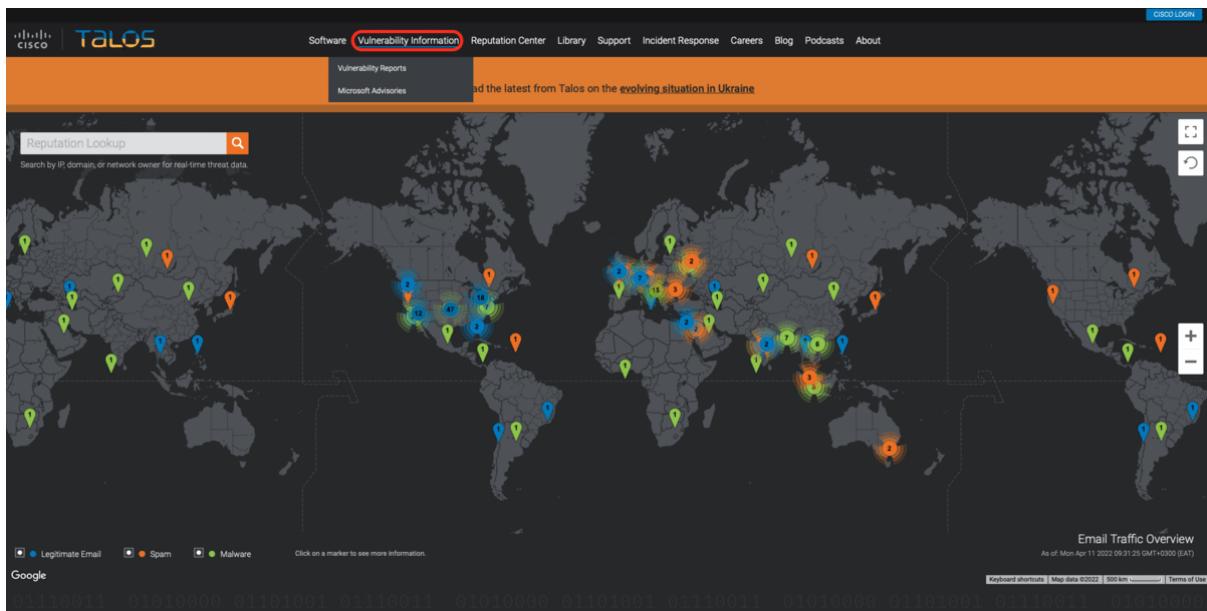
Tableau de bord Talos

En accédant à la solution open source, on nous présente d'abord un tableau de bord de recherche de réputation avec une carte du monde. Cette carte montre un aperçu du trafic de courrier électronique avec des indicateurs indiquant si les courriers électroniques sont légitimes, spam ou malware dans de nombreux pays. En cliquant sur n'importe quel marqueur, nous voyons plus d'informations associées aux adresses IP et noms d'hôte, au volume du jour et au type.



En haut, nous avons plusieurs onglets qui fournissent différents types de ressources de renseignement. Les principaux onglets avec lesquels un analyste interagirait sont :

- Informations sur la vulnérabilité : rapports de vulnérabilité divulgués et zero-day marqués de numéros CVE et de scores CVSS. Les détails des vulnérabilités signalées sont fournis lorsque vous sélectionnez un rapport spécifique, y compris le délai de publication du rapport. Des avis de vulnérabilité Microsoft sont également fournis, avec les règles de snort applicables qui peuvent être utilisées.



- Centre de réputation : permet d'accéder aux données consultables sur les menaces liées aux adresses IP et aux fichiers à l'aide de leurs hachages SHA256. Les analystes s'appuieraient sur ces options pour mener leurs enquêtes. Des données supplémentaires sur les e-mails et le spam peuvent être trouvées sous l'onglet Données de courrier électronique et de spam .

Reputation Center

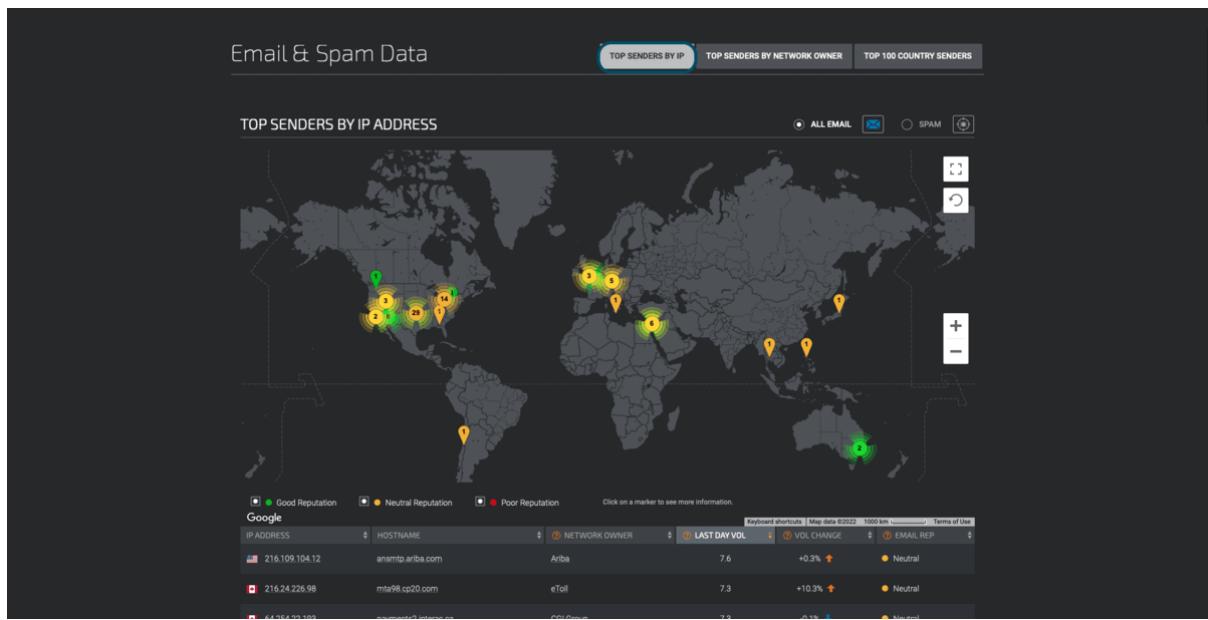
Talos' Reputation Center provides access to expansive threat data and related information.

IP and Domain Reputation Center

Talos' IP and Domain Data Center is the world's most comprehensive real-time threat detection network. The data is made up of daily security intelligence across millions of deployed web, email, firewall and IPS appliances. Talos detects and correlates threats in real time using the largest threat detection network in the world spanning web requests, emails, malware samples, open-source data sets, endpoint intelligence, and network intrusions. The Email and Web Traffic Reputation Center is able to transform some of Talos' data into actionable threat intelligence and tools to improve your security posture.

Talos File Reputation

The Cisco Talos Intelligence Group maintains a reputation disposition on billions of files. This reputation system is fed into the Cisco Secure Firewall, ClamAV, and Open-Source Snort product lines. The tools below allow you to do casual lookups against the Talos File Reputation system. This system limits you to one lookup at a time, and is limited to only hash matching.



Tâche

Utilisez le fichier .eml que vous avez téléchargé lors de la tâche précédente, PhishTool, pour répondre aux questions suivantes.

Répondre aux questions ci-dessous

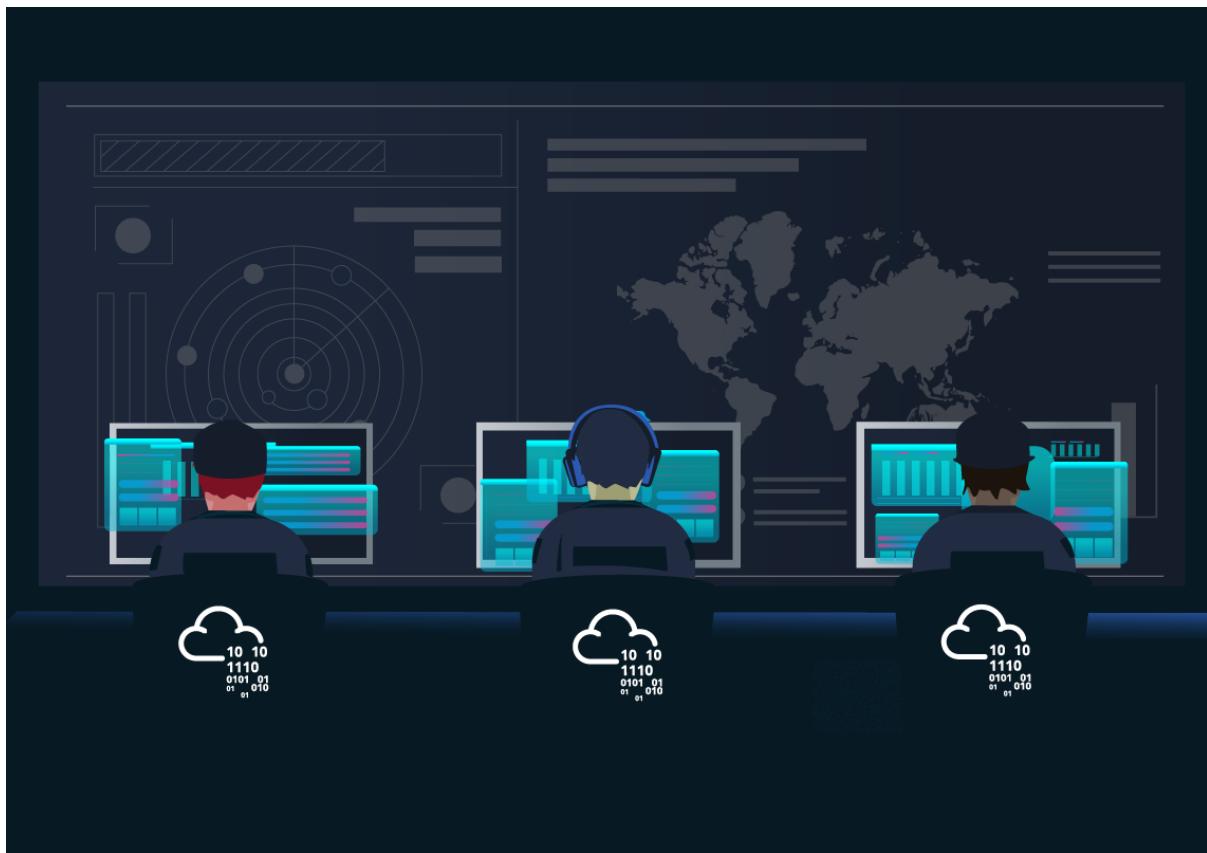
Quel est le domaine répertorié de l'adresse IP de la tâche précédente ?

scnet.net

Quel est le nom du client de l'adresse IP ?

Complete Web Reviews

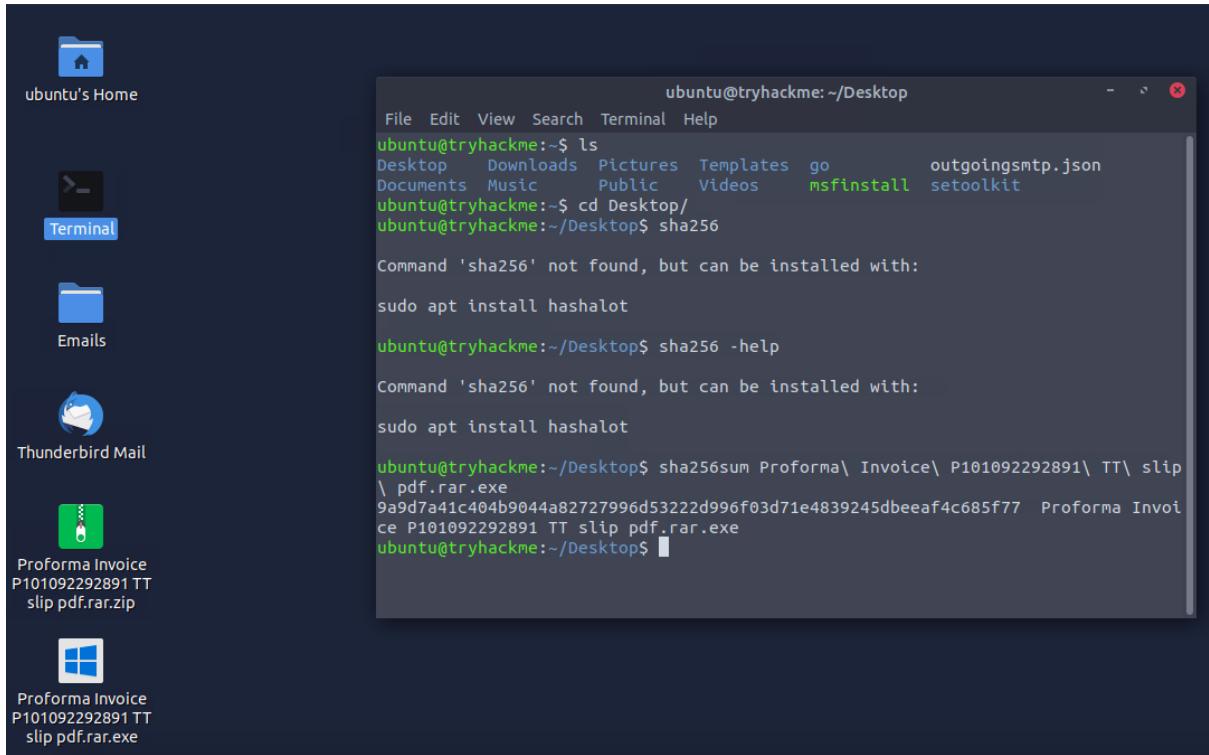
Scénario 1



Scénario : Vous êtes Analyste SOC . Plusieurs e-mails suspects vous ont été transmis par d'autres collègues. Vous devez obtenir les détails de chaque e-mail pour trier les incidents signalés.

Tâche : utilisez les outils et les connaissances discutés dans cette salle (ou utilisez vos ressources) pour vous aider à analyser Email2.eml trouvé sur la machine virtuelle attachée à la tâche 5 et utilisez les informations pour répondre aux questions.

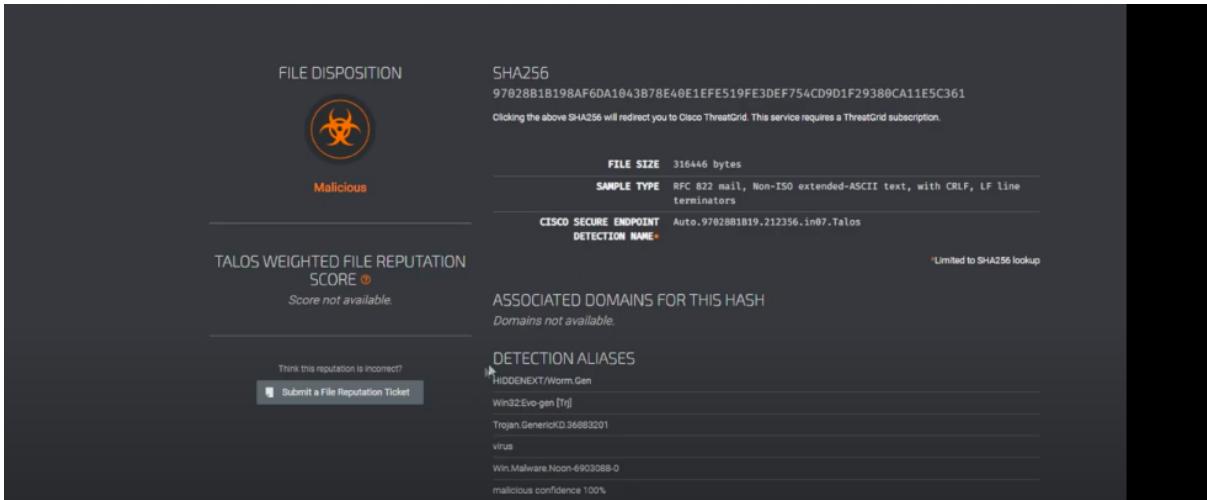
Pour la question 2 il faut calculer le hash sha256 de la pièce jointe pour voir s'il s'agit d'un truc malicieux sur le logiciel permettant de faire les analyses



The screenshot shows a desktop environment with a terminal window open. The terminal window title is "ubuntu@tryhackme: ~/Desktop". The terminal content shows the user running commands to find the sha256 command and then calculating the hash for a file named "P101092292891 TT slip pdf.rar.exe". The file is located in the "Proforma\ Invoice\ P101092292891\ TT\" directory. The calculated SHA256 hash is shown as 9702881B198AF6DA1043B78E40E1FE519FE3DEF754CD9D1F29380CA11E5C361.

```
ubuntu@tryhackme:~$ ls
Desktop  Downloads  Pictures  Templates  go      outgoingsmtp.json
Documents  Music    Public     Videos     msfinstall  setoolkit
ubuntu@tryhackme:~$ cd Desktop/
ubuntu@tryhackme:~/Desktop$ sha256
Command 'sha256' not found, but can be installed with:
sudo apt install hashalot
ubuntu@tryhackme:~/Desktop$ sha256 -help
Command 'sha256' not found, but can be installed with:
sudo apt install hashalot
ubuntu@tryhackme:~/Desktop$ sha256sum Proforma\ Invoice\ P101092292891\ TT\ \
\ pdf.rar.exe
9a9d7a41c404b9044a82727996d53222d996f03d71e4839245dbeef4c685f77  Proforma Invoi
ce P101092292891 TT slip pdf.rar.exe
ubuntu@tryhackme:~/Desktop$
```

On copie colle le hash récupéré sur l'outil Talos



The screenshot shows the Talos Intelligence file analysis interface. It displays the following details for the file:

- FILE DISPOSITION:** Malicious (indicated by a biohazard icon)
- SHA256:** 9702881B198AF6DA1043B78E40E1FE519FE3DEF754CD9D1F29380CA11E5C361
- FILE SIZE:** 316446 bytes
- SAMPLE TYPE:** RFC 822 mail, Non-ISO extended-ASCII text, with CRLF, LF line terminators
- CISCO SECURE ENDPOINT:** Auto.9702881B19.212356.in07.Talos
- DETECTION NAME:** *Limited to SHA256 lookup
- TALOS WEIGHTED FILE REPUTATION SCORE:** Score not available
- ASSOCIATED DOMAINS FOR THIS HASH:** Domains not available
- DETECTION ALIASES:** HIDDENNEXT/Worm.Gen, Win32:Evo-gen [Trj], Trojan.GenericD.36883201, virus, Win.Malware.Noon-6903068-0, malicious confidence 100%

Answer the questions below

According to Email2.eml, what is the recipient's email address?

chris.lyons@supercarcenterdetroit.com

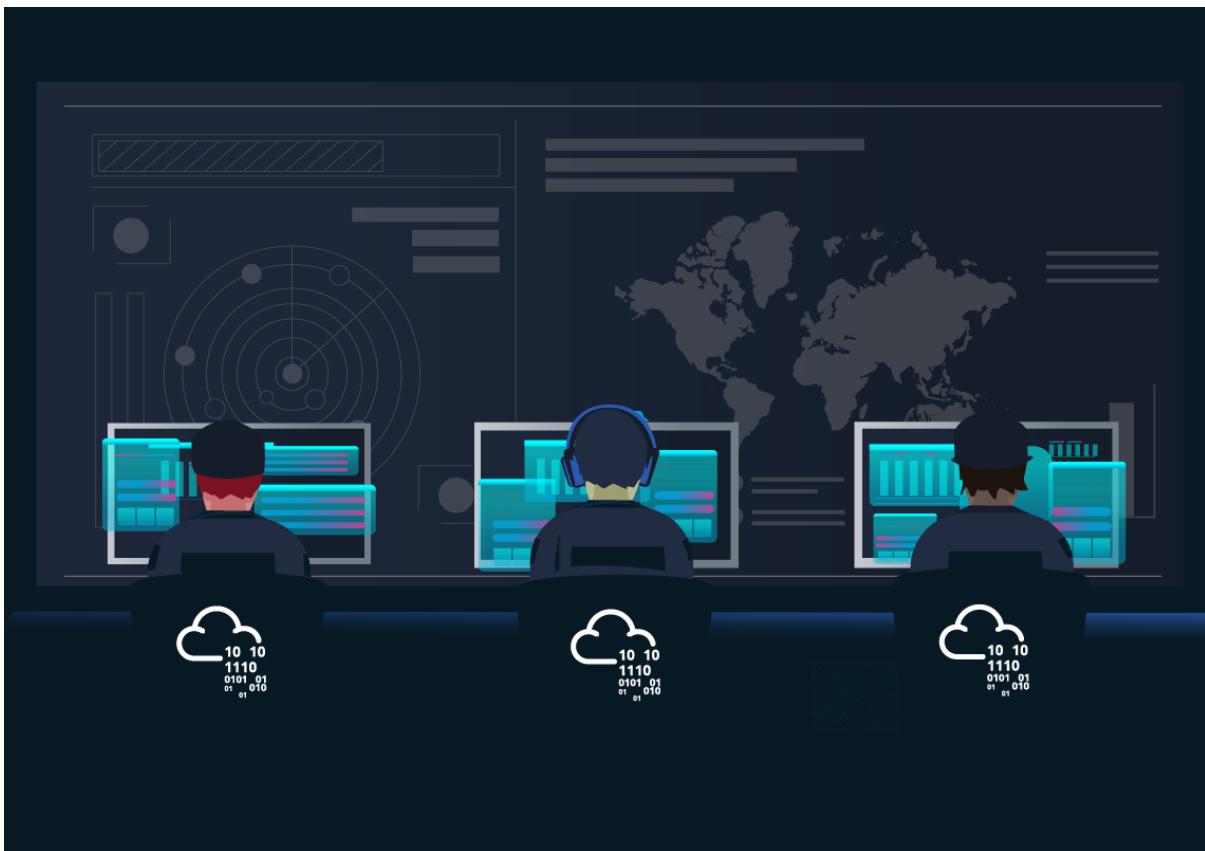
Cor

From Talos Intelligence, the attached file can also be identified by the Detection Alias that starts with an H...

HIDDENNEXT/Worm.Gen

Cor

Scenario 2



Scenario: You are a SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze Email3.eml found on the VM attached to Task 5 and use the information to answer the questions.

Answer the questions below

Answer the questions below

What is the name of the attachment on Email3.eml?

Sales_receipt 5606.xls

What malware family is associated with the attachment on Email3.eml?

dridex

FILE DISPOSITION

SHA256
F4D97603256A36E81BFE7EF5E0CCAEE44F77DE6BB041FA41F0B3A0DB53F4ABA9
Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE 117299 bytes
SAMPLE TYPE RFC 822 mail, ASCII text
CISCO SECURE ENDPOINT Auto.F4D9760325.252139.in07.Talos
DETECTION NAME*

*Limited to SHA256 lookup

TALOS WEIGHTED FILE REPUTATION
SCORE ⓘ
Score not available.

ASSOCIATED DOMAINS FOR THIS HASH
Domains not available.

DETECTION ALIASES

W97M/Agent.2325811
Other/Malware-gen [Trj]
X97M/~~Oricex~~A.gen/Eldorado
Trojan.GenericKD.47173557
VBA/Agent.ADS5itr
Trojan-Downloader.VBA.Agent

Conclusion

There's More Out There

You have come to the end of the room. However, this is just the tip of the iceberg for open-source threat intelligence tools that can help you as an analyst triage through incidents. There are plenty of more tools that may have more functionalities than the ones discussed in this room.

Check out these rooms to dive deeper into Threat Intelligence:

- [Yara](#)
- [MISP](#)
- [Red Team Threat Intel](#)

YARA

<https://medium.com/@haircutfish/tryhackme-yara-room-d279ccb5cbb3>

Apprenez les applications et le langage Yara pour tout ce qui concerne les renseignements sur les menaces, la médecine légale et la chasse aux menaces !



Tâche 1 Introduction

Introduction

Cette salle attend de vous que vous compreniez les connaissances de base de Linux, telles que l'installation de logiciels et de commandes pour la navigation générale du système. De plus, cette salle n'est pas conçue pour tester vos connaissances ou pour marquer des points. Il est là pour vous encourager à suivre et à expérimenter ce que vous avez appris ici. Comme toujours, j'espère que vous retiendrez quelques éléments de cette salle, à savoir la merveille qu'est Yara (encore un autre acronyme ridicule) et son importance dans la sécurité de l'information aujourd'hui. Yara a été développé par Victor M. Alvarez ([@plusvic](#)) et [@VirusTotal](#) . Consultez le dépôt GitHub [ici](#) .

Tâche 2 Qu'est-ce que Yara ?

Tout à propos de Yara

"Le couteau suisse de recherche de modèles pour les chercheurs en logiciels malveillants (et tout le monde)" ([Virustotal., 2020](#))

Avec une citation aussi appropriée, Yara peut identifier des informations basées à la fois sur des modèles binaires et textuels, tels que l'hexadécimal et les chaînes contenues dans un fichier.

Des règles sont utilisées pour étiqueter ces modèles. Par exemple, les règles Yara sont fréquemment écrites pour déterminer si un fichier est malveillant ou non, en fonction des fonctionnalités (ou modèles) qu'il présente. Les chaînes sont un composant fondamental des langages de programmation. Les applications utilisent des chaînes pour stocker des données telles que du texte.

Par exemple, l'extrait de code ci-dessous imprime « Hello World » en Python. Le texte « Hello World » serait stocké sous forme de chaîne.

imprimer ("Bonjour tout le monde !")

Nous pourrions écrire une règle Yara pour rechercher « hello world » dans chaque programme de notre système d'exploitation si nous le souhaitons.

Pourquoi les logiciels malveillants utilisent-ils des chaînes ?

Les logiciels malveillants, tout comme notre application « Hello World », utilisent des chaînes pour stocker des données textuelles. Voici quelques exemples de données que divers types de logiciels malveillants stockent dans des chaînes :

Type	Data	Description
Ransomware	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	Bitcoin Wallet for ransom payments
Botnet	12.34.56.7	The IP address of the Command and Control (C&C) server

Avertissement : analyse des logiciels malveillants

Expliquer la fonctionnalité des logiciels malveillants est largement hors de portée de cette salle en raison de l'ampleur du sujet. J'ai couvert les cordes beaucoup plus en détail dans la « Tâche 12 — Cordes » de mon [MAL : Salle d'introduction](#). En fait, je crée tout un parcours d'apprentissage pour cela. Si vous souhaitez avoir un avant-goût tout en apprenant les bases, je vous recommande ma chambre.

Répondre aux questions ci-dessous

Les réponses se trouvent ci-dessus, suivez-les pour vous aider à les localiser si vous rencontrez des problèmes.

Quel est le nom du système de numérotation en base 16 que Yara peut détecter ?

La question demande la version abrégée de l'hexadécimal. Une fois que vous avez compris, tapez la réponse dans le champ de réponse sur TryHackMe et cliquez sur Soumettre.

With such a fitting quote, [Yara can identify information based on both binary and textual patterns, such as hexadecimal and strings contained within a file.](#)

Abbreviation

Le texte « Entrez votre nom » serait-il une chaîne dans une application ? (Ouais/Non)

Regarder l'extrait ci-dessus devrait vous donner la réponse à cette question. Une fois que vous avez compris, tapez la réponse dans le champ de réponse sur TryHackMe et cliquez sur Soumettre.

For example, the code snippet below prints "Hello World" in Python. The text "Hello World" would be stored as a string.

```
print("Hello World!")
```

We could write a Yara rule to search for "hello world" in every program on our operating system if we would like.

Tâche 3 Déployer

Cette salle déploie une instance avec les outils présentés déjà installés pour vous. Appuyez sur le bouton « Démarrer la machine », attendez qu'une adresse IP s'affiche et connectez-vous de l'une des deux manières suivantes :

Dans le navigateur (aucun VPN requis)

Déployez votre propre instance en appuyant sur le bouton vert « Démarrer la machine », faites défiler vers le haut de la pièce et attendez le minuteur. La machine démarrera dans une vue en écran partagé. Si la VM n'est pas visible, utilisez le bouton bleu « Afficher la vue fractionnée » en haut à droite de la page.

```
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-163-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Tue Oct 11 20:12:23 UTC 2022

System load:  0.66          Processes:      115
Usage of /:   78.7% of 8.79GB  Users logged in:  0
Memory usage: 7%           IP address for eth0: 10.10.67.228
Swap usage:   0%

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

  https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

Last login: Tue Nov 30 01:24:11 2021 from 10.9.163.253
cmnatic@thm-yara:~$ █
```

Utilisation de SSH (TryHackMe VPN requis).

Vous devez être connecté au VPN TryHackMe si vous souhaitez connecter votre instance déployée à partir de votre propre appareil. Si vous n'êtes pas familier avec ce processus, veuillez visiter la salle [TryHackMe OpenVPN](#) pour commencer. Si vous rencontrez des problèmes, veuillez [lire nos articles d'assistance](#).

Adresse IP : MACHINE_IP

Nom d'utilisateur : cmnatic

Mot de passe : yararules !

Port SSH : 22

Tâche 4 Introduction aux règles Yara

Votre première règle Yara

Le langage propriétaire que Yara utilise pour les règles est assez simple à maîtriser, mais difficile à maîtriser. En effet, votre règle n'est efficace que dans la mesure où vous comprenez les modèles que vous souhaitez rechercher.

Utiliser une règle Yara est simple. Chaque yara commande nécessite deux arguments pour être valide, à savoir :

- 1) Le fichier de règles que nous créons
- 2) Le nom du fichier, du répertoire ou de l'ID de processus pour lequel utiliser la règle.

Chaque règle doit avoir un nom et une condition.

Par exemple, si nous voulions utiliser « myrule.yar » sur le répertoire « un répertoire », nous utiliserions la commande suivante :

```
yara myrule.yar somedirectory
```

Notez que .yar est l'extension de fichier standard pour toutes les règles Yara. Nous établirons ci-dessous l'une des règles les plus élémentaires que vous puissiez établir.

1. Créez un fichier nommé " somefile " via touch somefile

2. Créez un nouveau fichier et nommez-le " myfirstrule.yar " comme ci-dessous :

Création d'un fichier nommé somefile

```
cminatic@thm :~$ touche un fichier
```

Création d'un fichier nommé myfirstrule.yar

```
cminatic@thm touch myfirstrule.yar
```

3. Ouvrez « myfirstrule.yar » à l'aide d'un éditeur de texte tel que nano, saisissez l'extrait ci-dessous et enregistrez le fichier :

```
exemple de règle {
```

```
    condition : vrai
```

```
}
```

Saisir notre premier extrait dans « myfirstrule.yar » en utilisant nano

```
cminatic@thm nano myfirstrule.yar
```

```
GNU nano 4.8 myfirstrule.yar
```

```
exemple de règle modifiée {
```

```
    condition : true
```

```
}
```

Le nom de la règle dans cet extrait est `examplerule`, où nous avons une condition - dans ce cas, la condition est `condition`. Comme indiqué précédemment, chaque règle nécessite à la fois un nom et une condition pour être valide. Cette règle satisfait à ces deux exigences.

Simplement, la règle que nous avons établie vérifie si le fichier/répertoire/PID que nous spécifions existe via `condition`:

`true`. Si le fichier existe, nous recevons la sortie de `examplerule`

Essayons ceci sur le fichier "somefile" que nous avons créé à la première étape :
`yara myfirstrule.yar somefile`

Si "un fichier" existe, Yara le dira `examplerule` parce que le modèle a été respecté - comme nous pouvons le voir ci-dessous :

Vérifier que notre exemple de règle est correct

```
cmmatic@thm:~$ yara myfirstrule.yar un fichier exemple une règle
```

```
un fichier
```

Si le fichier n'existe pas, Yara affichera une erreur telle que celle ci-dessous :

Yara se plaint que le fichier n'existe pas

```
cmnatic @thm :~ $ yara myfirstrule.yar
```

```
erreur de fichier texte lors de l'analyse de fichier texte : impossible  
d' ouvrir le fichier
```

Bravo! Vous avez établi votre première règle.

Tâche 5 Développer les règles Yara

Conditions Yara (suite)...

Vérifier si un fichier existe ou non n'est pas très utile. Après tout, nous pouvons le découvrir par nous-mêmes... En utilisant de bien meilleurs outils pour le travail.

Yara a quelques conditions, que je vous encourage à lire [ici](#) à votre guise. Cependant, je vais en détailler quelques-uns ci-dessous et expliquer leur objectif.

Mot-clé

Desc

Meta

Strings

Conditions

Poids

Méta

Cette section d'une règle Yara est réservée aux informations descriptives par l'auteur de la règle. Par exemple, vous pouvez utiliser desc, abréviation de description, pour résumer ce que votre règle vérifie. Tout ce qui se trouve dans cette section n'influence pas la règle elle-même. Semblable au commentaire de code, il est utile de résumer votre règle.

Cordes

Vous vous souvenez de notre discussion sur les chaînes dans la tâche 2 ? Eh bien, c'est parti. Vous pouvez utiliser des chaînes pour rechercher du texte spécifique ou hexadécimal dans des fichiers ou des programmes. Par exemple, disons que nous voulions rechercher dans un répertoire tous les fichiers contenant « Hello World ! », nous créerions une règle telle que ci-dessous :

```
règle helloworld_checker{  
    strings :  
        $ hello_world = "Bonjour tout le monde !"  
  
}
```

Nous définissons le mot-clé String où se trouve la chaîne que nous voulons rechercher, c'est-à-dire "Hello World!" est stocké dans la variable \$hello_world

Bien sûr, nous avons besoin d'une condition ici pour rendre la règle valide. Dans cet exemple, pour faire de cette chaîne la condition, nous devons utiliser le nom de la variable.

Dans ce cas, \$hello_world:

```
règle helloworld_checker{
    strings :
        $ hello_world = "Bonjour tout le monde !"

    condition :
        $ hello_world

}
```

Essentiellement, si un fichier contient la chaîne « Hello World ! » alors la règle correspondra. Cependant, cela signifie littéralement que cela ne correspondra que si « Hello World ! » est trouvé et ne correspondra pas si « hello world » ou « HELLO WORLD ».

Pour résoudre ce problème, la condition any of them permet de rechercher plusieurs chaînes, comme ci-dessous :

```
règle helloworld_checker{
    strings :
        $ hello_world = "Bonjour tout le monde !"
        $ hello_world_lowercase = "hello world"
        $ hello_world_uppercase = "HELLO WORLD"

    condition :
        n'importe lequel d'entre eux

}
```

Maintenant, n'importe quel fichier avec les chaînes de :

1. Bonjour tout le monde !
2. bonjour tout le monde
3. BONJOUR LE MONDE

Va maintenant déclencher la règle.

Conditions

Nous avons déjà utilisé la condition true and any of them. Tout comme la programmation classique, vous pouvez utiliser des opérateurs tels que :

<= inférieur ou égal à
>= supérieur ou égal à
!= différent de

Par exemple, la règle ci-dessous aurait les effets suivants :

```
règle helloworld_checker{  
  
    strings :  
        $ hello_world = "Bonjour tout le monde !"  
  
    condition :  
        #hello_world <= 10  
}
```

La règle va désormais :

1. Recherchez le message « Hello World ! » chaîne
2. Dites uniquement que la règle correspond s'il y a moins ou égal à dix occurrences de « Hello World ! » chaîne

Combinaison de mots-clés

De plus, vous pouvez utiliser des mots-clés tels que :

et

pas

ou

Pour combiner plusieurs conditions. Dites que si vous souhaitez vérifier si un fichier contient une chaîne et est d'une certaine taille (dans cet exemple, l'exemple de fichier que nous vérifions fait moins de <10 Ko et contient « Hello World ! », vous pouvez utiliser une règle comme ci-dessous :

```
règle helloworld_checker{  
    strings :  
        $ hello_world = "Bonjour tout le monde !"  
  
    condition :  
        $hello_world et taille du fichier < 10 Ko  
  
}
```

La règle ne correspondra que si les deux conditions sont vraies. Pour illustrer : ci-dessous, la règle que nous avons créée, dans ce cas, ne correspond pas car bien que le fichier contienne « Hello World ! », sa taille est supérieure à 10 Ko :

Yara ne parvient pas à faire correspondre le fichier mytextfile car il fait plus de 10 Ko

```
cmmnatic @thm :~ $ <sortie intentionnellement laissée vide>
```

Cependant, la règle correspondait cette fois car le fichier contenait à la fois « Hello World ! » et une taille de fichier inférieure à 10 Ko.

Yara a réussi à faire correspondre le fichier mytextfile car il contient « Hello World » et une taille de fichier inférieure à 10 Ko.

```
cmmnatic @thm :~ $ yara myfirstrule.yar monfichiertexte.txt
```

```
helloworld_textfile_checker monfichiertexte.txt
```

N'oubliez pas que le texte dans la case rouge est le nom de notre règle et que le texte dans la case verte est le fichier correspondant.

Anatomie d'une règle Yara

ANATOMY OF A Yara RULE



Yara is a tool used to identify file, based on **textual or binary pattern**.



A rule consists of a **set of strings and conditions** that determine its logic.



Rules can be compiled with "yarac" to **increase the speed** of multiple Yara scans.

1 IMPORT MODULE

Yara modules allow you to extend its functionality. The PE module can be used to match specific data from a PE:

- pe.number_of_exports
- pesections[0].name
- peimphash0
- peimports("kernel32.dll")
- peis.dll0

List of modules: pe, elf, hash, math, cuckoo, dotnet, time

2 RULE NAME

The rule name identifies your Yara rule. It is recommended to add a meaningful name. There are different types of rules:

- Global rules: applies for all your rules in the file.
- Private rules: can be called in a condition of a rule but not reported.
- Rule tags: used to filter yara's output

3 METADATA

Rules can also have a metadata section where you can put additional information about your rule:

- Author
- Date
- Description
- Etc..

4 STRINGS

The field strings is used to define the strings that should match your rule. It exists 3 type of strings:

- Text strings
- Hexadecimal strings
- Regex

5 CONDITION

Conditions are Boolean expressions used to match the defined pattern:

- Boolean operators:
 - and, or, not
 - <, >, ==, <, >, !=
- Arithmetic operators:
 - +, -, *, \%, %
- Bitwise operators:
 - &, |, <<, >>, ^, ~
- Counting strings:
 - #string0 == 5
- Strings offset:
 - \$string1 at 100

```
import "pe"
rule_demo_rule : Tag1 Demo
{
meta:
  author = "Thomas Roccia"
  description = "demo"
  hash = ""
strings:
  $string0 = "hello" nocase wide
  $string1 = "world" fullword ascii
  $hex1 = { 01 23 45 ?? 89 ab cd ef }
  $rel = /md5: { 0-9a-zA-Z}{32}/
condition:
  uint16(0) == 0x5A4D and filesize < 2000KB
  or pe.number_of_sections == 1 and
  any of ($string*) and (not $hex1 or $rel)
}
```

TEXT STRINGS

Text strings can be used with modifiers:

- nocase: case insensitive
- wide: encoded strings with 2 bytes per character
- fullword: non alphanumeric
- xor(0x01-0x0f): look for xor encryption
- base64: base64 encoding

HEXADECIMAL

Hex strings can be used to match piece of code

- Wild-cards: { 00 ?2 A? }
- Jump: { 3B [2-4] BH }
- Alternatives: { F4 (B4 | 56) }

REGEX

Regular expression can also be used and defined as text strings but enclosed in forward slash

```
ADvanced CONDITION
• Accessing data at a given position: uint16(0) == 0x5A4D
• Check the size of the file: filesize < 2000KB
• Set of strings: any of ($string0, $hex1)
• Same condition to many strings: for all of them: (# > 3)
• Scan entry point: $value at peentry.point
• Match length: !rel[1] == 32
• Search within a range of offsets: $value in (0J00)
```

@FR0GGER_
THOMAS ROCCIA

Le chercheur en sécurité de l'information « fr0gger_ » a récemment créé une [aide-mémoire pratique](#) qui décompose et visualise les éléments d'une règle YARA (illustré ci-dessus, tous les crédits d'image lui reviennent). C'est un excellent point de référence pour commencer !

Tâche 6 Modules Yara

Intégration avec d'autres bibliothèques

Des frameworks tels que le [Cuckoo Sandbox](#) ou [le module PE de Python](#) vous permettent de découpler la technicité de vos règles Yara.

Coucou

Cuckoo Sandbox est un environnement d'analyse automatisé des logiciels malveillants. Ce module vous permet de générer des règles Yara basées sur les comportements découverts dans Cuckoo Sandbox. À mesure que cet environnement exécute des logiciels malveillants, vous pouvez créer des règles sur des comportements spécifiques tels que les chaînes d'exécution, etc.

PythonPE

Le module PE de Python vous permet de créer des règles Yara à partir des différentes sections et éléments de la structure Windows Portable Executable (PE).

Expliquer cette structure est hors de portée car elle est couverte dans ma [salle d'introduction aux logiciels malveillants](#). Cependant, cette structure constitue le formatage standard de tous les exécutables et fichiers DLL sous Windows. Y compris les bibliothèques de programmation utilisées.

L'examen du contenu d'un fichier PE est une technique essentielle dans l'analyse des logiciels malveillants ; en effet, des comportements tels que la cryptographie ou le vermafugation peuvent être largement identifiés sans ingénierie inverse ni exécution de l'échantillon.

Tâche 7 Autres outils et Yara

Outils Yara

Savoir comment créer des règles Yara personnalisées est utile, mais heureusement, vous n'avez pas besoin de créer de nombreuses règles à partir de zéro pour commencer à utiliser Yara pour rechercher le mal. Il existe de nombreuses [ressources](#) GitHub et outils open source (ainsi que des produits commerciaux) qui peuvent être utilisés pour tirer parti de Yara dans le cadre d'opérations de chasse et/ou de missions de réponse aux incidents.

LOKI (Quoi, pas qui, est Loki ?)

LOKI est un scanner IOC (Indicator of Compromise) open source gratuit créé/écrit par Florian Roth.

Basée sur la page GitHub, la détection repose sur 4 méthodes :

1. Nom du fichier Vérification IOC
2. Vérification des règles Yara (nous sommes ici)
3. Vérification du hachage
4. Vérification de la connexion arrière C2

Il existe des contrôles supplémentaires pour lesquels LOKI peut être utilisé. Pour un aperçu complet, veuillez consulter le [fichier readme de GitHub](#).

LOKI peut être utilisé sur les systèmes Windows et Linux et peut être téléchargé [ici](#).

Veuillez noter que vous n'êtes pas censé utiliser cet outil dans cette salle.

Affichage du menu d'aide de Loki

```
cmnatic@thm:~/Loki$ python3 loki.py -h
utilisation : loki.py [-h] [-p chemin] [-s kilo-octet] [-l fichier
journal] [-r hôte-login distant] [
    -t port-syslog distant] [-a niveau d'alerte] [-w niveau
d'avertissement]
    [-n niveau de notification] [--allhds] [--alldrives]
[--printall]
    [--allreasons] [--noprocscan] [--nofilescan]
[--vulnchecks]
    [--nolevcheck] [--scriptanalysis] [--rootkit]
[--noindicator]
    [--dontwait] [--intense] [--csv] [--onlyrelevant]
[--nolog]
    [--update] [--debug] [--maxworkingset MAXWORKINGSET]
    [--syslogtcp] [--logfolder dossier de journaux]
[--nopesieve]
    [--pesieveshellc] [--python PYTHON] [--nolisten]
    [--excludeprocess EXCLUDEPROCESS] [--force]
```

Loki -

Arguments facultatifs de Simple IOC Scanner :

-h, -- help	affiche ce message d'aide et quitte
-------------	-------------------------------------

THOR (programmes nommés de super-héros pour un teamer bleu de super-héros)

THOR Lite est le tout nouveau scanner multiplateforme IOC ET YARA de Florian. Il existe des versions précompilées pour Windows, Linux et macOS. Une fonctionnalité intéressante de THOR Lite est sa limitation d'analyse pour limiter les ressources CPU épuisantes. Pour plus d'informations et/ou pour télécharger le binaire, commencez [ici](#). Vous devez vous inscrire à leur liste de diffusion pour obtenir une copie du binaire. A noter que THOR s'adresse aux clients entreprises . THOR Lite est la version gratuite.

Veuillez noter que vous n'êtes pas censé utiliser cet outil dans cette salle.

Affichage du menu d'aide de Thor Lite

```
cmmatic@thm:~$ ./thor-lite-linux-64 -h
```

```
Thor Lite
```

```
APT Scanner
```

```
Version 10.7.3 (2022-07-27 07:33:47)
```

```
cc) Nextron Systems GmbH
```

```
Version Lite
```

> Options d'analyse

```
-t, --template string Traiter les paramètres d'analyse par défaut de ce fichier YAML
```

```
-p, --path strings Analyser un chemin de fichier spécifique. Définissez plusieurs chemins en spécifiant cette option plusieurs fois . Ajoutez ':NOWALK' au chemin d'accès pour l'analyse non récursive (par défaut : uniquement le lecteur système) (par défaut [])
```

```
--allhds (Windows uniquement) Analysez tous les disques durs locaux (par défaut : uniquement le lecteur système)
```

```
--max_file_size uint Max. taille du fichier à vérifier (les fichiers plus volumineux sont ignorés). L'augmentation de cette limite augmentera également l'utilisation de la mémoire de THOR. (30 Mo par défaut)
```

> Modes d'analyse

```
--quick Activez un certain nombre d'indicateurs pour accélérer l'analyse au prix d'une certaine détection.
```

```
Ceci est équivalent à : --noeventlog --nofirewall --noprofiles --nowebdirscan --nologscan --noevtx --nohotfixes --nomft --lookback 3 --lookback-modules filescan
```

FENRIR (convention de nommage toujours à thème mythique)

Il s'agit du 3ème [outil](#) créé par Neo23x0 (Florian Roth). Tu l'as deviné; les 2 précédents sont nommés ci-dessus. La version mise à jour a été créée pour résoudre le problème de ses prédecesseurs, où les conditions doivent être remplies pour qu'ils fonctionnent. Fenrir est un script bash ; il fonctionnera sur n'importe quel système capable d'exécuter bash (aujourd'hui même Windows).

Veuillez noter que vous n'êtes pas censé utiliser cet outil dans cette salle.

Exécuter Fenrir

```
cmnatic@thm-yara:~/tools$ ./fenrir.sh
#####
_____
/ _/_____( )_____
/_// -_) _ \/_ / / _/
/_ \__/_/_/_/_/_/
v0.9.0-log4shell
Simple Bash IOC Checker
Florian Roth, décembre 2021
#####
#
```

YAYA (Encore un autre automate Yara)

YAYA a été créé par l' [EFF](#) (Electronic Frontier Foundation) et publié en septembre 2020. D'après leur site Web, « YAYA est un nouvel outil open source pour aider les chercheurs à gérer plusieurs référentiels de règles YARA. YAYA commence par importer un ensemble de règles YARA de haute qualité, puis permet aux chercheurs d'ajouter leurs propres règles, de désactiver des ensembles de règles spécifiques et d'exécuter des analyses de fichiers. »

Remarque : Actuellement, YAYA ne fonctionnera que sur les systèmes Linux.

Courir YAYA

```
cmnatic@thm-yara:~/tools$ yaya
YAYA - Encore un autre automate Yara
Utilisation :
yaya [-h]
-h imprimer cet écran d'aide
```

Commandes :

```
mettre à jour - mettre à jour les ensembles de règles
modifier - interdire ou supprimer les ensembles de règles
ajouter - ajouter un ensemble de règles personnalisé, situé at
scan - effectuez une analyse Yara sur le répertoire à
```

Dans la section suivante, nous examinerons [LOKI](#) plus en détail...

Tâche 8 Utiliser LOKI et son ensemble de règles Yara

Assurez-vous de suivre les instructions de cette tâche, car elles vous mèneront là où vous devez être pour répondre à la première question.

Utiliser LOKI

En tant qu'analyste de sécurité, vous devrez peut-être rechercher divers rapports de renseignements sur les menaces, articles de blog, etc. et recueillir des informations sur les dernières tactiques et techniques utilisées dans la nature, passées ou présentes.

Généralement, dans ces lectures, les IOC (hachages, adresses IP, noms de domaine, etc.) seront partagés afin que des règles puissent être créées pour détecter ces menaces dans votre environnement, ainsi que les règles Yara. D'un autre côté, vous pourriez vous retrouver dans une situation où vous avez rencontré quelque chose d'inconnu, que votre pile d'outils de sécurité ne peut pas/n'a pas détecté. À l'aide d'outils tels que Loki, vous devrez ajouter vos propres règles en fonction de vos collectes de renseignements sur les menaces ou des résultats d'un engagement de réponse aux incidents (criminalistique).

Comme mentionné précédemment, Loki dispose déjà d'un ensemble de règles Yara dont nous pouvons bénéficier et commencer immédiatement à rechercher le mal sur le point final. Accédez au répertoire Loki. Loki est situé dans le tools.

Liste du répertoire des outils

```
cmmatic@thm-yara:~/tools$ ls
```

Loki yarGen

Exécutez `python loki.py -h` pour voir quelles options sont disponibles.

Si vous exécutez Loki sur votre propre système, la première commande que vous devez exécuter est `--update`. Cela ajoutera le signature-base répertoire que Loki utilise pour rechercher le mal connu. Cette commande a déjà été exécutée dans la VM attachée.

Liste du répertoire de base de signature de Loki

```
cmmatic@thm-yara:~/tools/Loki/signature-base$ ls
```

iocs divers yara

Accédez au yara répertoire. N'hésitez pas à inspecter les différents fichiers Yara utilisés par Loki pour avoir une idée de ce que ces règles vont rechercher.

Pour exécuter Loki, vous pouvez utiliser la commande suivante (notez que j'appelle Loki depuis le répertoire file 1)

Demandez à Loki d'analyser le fichier suspect

```
cmmatic@thm-yara:~/suspect-files/file1$ python ../../tools/Loki/loki.py  
-p .
```

Scénario : Vous êtes l'analyste de sécurité pour un cabinet d'avocats de taille moyenne. Un collègue a découvert des fichiers suspects sur un serveur Web au sein de votre organisation. Ces fichiers ont été découverts lors de mises à jour du site Web de l'entreprise. Les fichiers ont été copiés sur votre machine pour analyse. Les fichiers se trouvent dans le suspicious-filesrépertoire. Utilisez Loki pour répondre aux questions ci-dessous.

Répondre aux questions ci-dessous

Analyser le fichier 1. Loki détecte-t-il ce fichier comme suspect/malveillant ou inoffensif ?

Après avoir exécuté Loki pour analyser, vous obtiendrez un résultat volumineux avec de nombreuses informations à consulter. Les résultats peuvent être trouvés dans la section inférieure de la sortie. Recherchez le premier résultat jaune, la réponse sera dans cette ligne. Une fois que vous l'avez trouvé, tapez votre réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

```

[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20221207T20:2
1:46Z PLATFORM: PROC: x86 64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tool
s/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 653 Yara rules
[INFO] Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process
memory and file objects.
[NOTICE] Running plugin PluginWMI
[NOTICE] Finished running plugin PluginWMI
[INFO] Scanning . . .
[WARNING]
FILE: ./ind3x.php SCORE: 70 TYPE: PHP SIZE: 80992
FIRST BYTES: 3c3f7068700a2f2a0a09623337346b20322e320a / <?php/*?php??
MD5: 1606bdac2cb613bf0b8a22690364fbc5
SHA1: 9383ed4ee7df17193f7a034c3190ecabc9000f9f
SHA256: 5479f8cd1375364770df36e5a18262480a8f9d31le8eedb2c2390ecb233852ad CREATED
: Mon Nov 9 15:15:32 2020 MODIFIED: Mon Nov 9 13:06:56 2020 ACCESSED: Wed Dec
7 20:21:53 2022
REASON 1: Yara Rule MATCH: file metasoft.php SUBSCORE: 70
DESCRIPTION: file - file metasoft.php REF: -
MATCHES: $buff .= "<tr><td><a href=\\"?d=".pwd."\\>[ $folder ]</a></td><
td>LINK</t
[NOTICE] Results: 0 alerts, 1 warnings, 7 notices
[RESULT] suspicious objects detected! Answer
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-ba
se
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20221207T20:21:53Z

Press Enter to exit ...
cmnatic@thm-yara:~/suspicious-files/file1$ 
```

Réponse : suspect

À quelle règle Yara correspondait-il ?

La réponse suivante se trouve un peu plus haut, cherchez le texte blanc RAISON 1. Dans cette ligne, vous trouverez la réponse juste après MATCH :. Il y a un trait de soulignement entre les mots mais vous ne pouvez pas le voir sur la sortie. Une fois que vous l'avez trouvé, tapez votre réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

```

[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20221207T20:2
1:46Z PLATFORM: PROC: x86_64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tool
s/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 653 Yara rules
[INFO] Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process
memory and file objects.
[NOTICE] Running plugin PluginWMI
[NOTICE] Finished running plugin PluginWMI
[INFO] Scanning . . .
[WARNING]
FILE: ./ind3x.php SCORE: 70 TYPE: PHP SIZE: 80992
FIRST BYTES: 3c3f7068700a2f2a0a09623337346b20322e320a / <?php/*?php
MD5: 1606bdac2cb613bf0b8a22690364fbc5
SHA1: 9383ed4ee7df17193f7a034c3190ecabc9000f9f
SHA256: 5479f8cd1375364770df36e5a18262480a8f9d311e8eedb2c2390ecb233852ad CREATED
: Mon Nov 9 15:15:32 2020 MODIFIED: Mon Nov 9 13:06:56 2020 ACCESSED: Wed Dec
7 20:21:53 2022
REASON 1: Yara Rule MATCH: [REDACTED] SUBSCORE: 70
DESCRIPTION: [REDACTED] - file metaslsoft.php REF: -
MATCHES: [REDACTED]: $buff .= "<tr><td><a href=\"?d=$pwd.\\">[ $folder ]</a></td><
td>LINK</t
[NOTICE] Results: 0 alerts, 1 warnings, 7 notices
[RESULT] [REDACTED] objects detected!
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-ba
se
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20221207T20:21:53Z

Press Enter to exit ...
cmnatic@thm-yara:~/suspicious-files/file1$ 
```

Answer

Réponse : webshell_metaslsoft

Comment Loki classe-t-il ce fichier ?

Cette réponse se trouve dans la ligne située en dessous de l'endroit où vous avez trouvé la question précédente. Il se trouve juste après le texte blanc DESCRIPTION :. Il n'y a pas de soulignement entre ces deux mots dans cette réponse. Une fois que vous l'avez trouvé, tapez votre réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

```

[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20221207T20:2
1:46Z PLATFORM: PROC: x86 64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tool
s/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 653 Yara rules
[INFO] Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process
memory and file objects.
[NOTICE] Running plugin PluginWMI
[NOTICE] Finished running plugin PluginWMI
[INFO] Scanning . . .
[WARNING]
FILE: ./ind3x.php SCORE: 70 TYPE: PHP SIZE: 80992
FIRST BYTES: 3c3f7068700a2f2a0a09623337346b20322e320a / <?php/*?php??
MD5: 1606bdac2cb613bf0b8a22690364fbc5
SHA1: 9383ed4ee7df17193f7a034c3190ecabc9000f9f
SHA256: 5479f8cd1375364770df36e5a18262480a8f9d31le8eedb2c2390ecb233852ad CREATED
: Mon Nov 9 15:15:32 2020 MODIFIED: Mon Nov 9 13:06:56 2020 ACCESSED: Wed Dec
7 20:21:53 2022
REASON 1: Yara Rule MATCH: [REDACTED] SUBSCORE: 70
DESCRIPTION: [REDACTED] - file metaslsoft.php REF: -
MATCHES: [REDACTED]: $buff .= "<tr><td><a href=\"?d=".pwd."\\\">[ $folder ]</a></td><
td>LINK</t
[NOTICE] Results: 0 alerts, 1 warnings, 7 notices
[RESULT] [REDACTED] objects detected! Answer
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-ba
se
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20221207T20:21:53Z

Press Enter to exit ...
cmnatic@thm-yara:~/suspicious-files/file1$ 
```

Réponse : Web Shell

D'après le résultat, sur quelle chaîne de la règle Yara correspond-elle ?
 Cette réponse se trouve dans la ligne située en dessous de l'endroit où vous avez trouvé la question précédente. Il se trouve juste après le texte blanc MATCHES :. Une fois que vous l'avez trouvé, tapez votre réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

```

[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20221207T20:2
1:46Z PLATFORM: PROC: x86 64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tool
s/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 653 Yara rules
[INFO] Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process
memory and file objects.
[NOTICE] Running plugin PluginWMI
[NOTICE] Finished running plugin PluginWMI
[INFO] Scanning . . .
[WARNING]
FILE: ./ind3x.php SCORE: 70 TYPE: PHP SIZE: 80992
FIRST BYTES: 3c3f7068700a2f2a0a09623337346b20322e320a / <?php/*?php
MD5: 1606bdac2cb613bf0b8a22690364fbc5
SHA1: 9383ed4ee7df17193f7a034c3190ecabc9000f9f
SHA256: 5479f8cd1375364770df36e5a18262480a8f9d31le8eedb2c2390ecb233852ad CREATED
: Mon Nov 9 15:15:32 2020 MODIFIED: Mon Nov 9 13:06:56 2020 ACCESSED: Wed Dec
7 20:21:53 2022
REASON 1: Yara Rule MATCH: [REDACTED] SUBSCORE: 70
DESCRIPTION: [REDACTED] - file metaslsoft.php REF: -
MATCHES: [REDACTED]: $buff .= "<tr><td><a href=\"?d=".pwd."\\">[ $folder ]</a></td><
td>LINK</t
[NOTICE] Results: 0 alerts, 1 warnings, 7 notices Answer
[RESULT] [REDACTED] objects detected!
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-ba
se
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20221207T20:21:53Z

Press Enter to exit ...
cmnatic@thm-yara:~/suspicious-files/file1$ 
```

Réponse : Str1

Quel est le nom et la version de cet outil de hack ?

Remontez jusqu'au texte blanc PREMIER OCTETS : puis avancez jusqu'à la fin où vous trouverez la réponse. Une fois que vous l'avez trouvé, tapez votre réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

```

[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20221207T20:2
1:46Z PLATFORM: PROC: x86 64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tool
s/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 653 Yara rules
[INFO] Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process
memory and file objects.
[NOTICE] Running plugin PluginWMI
[NOTICE] Finished running plugin PluginWMI
[INFO] Scanning . . .
[WARNING]
FILE: ./ind3x.php SCORE: 70 TYPE: PHP SIZE: 80992
FIRST BYTES: 3c3f7068700a2f2a0a09623337346b20322e320a / <?php/*[REDACTED]
MD5: 1606bdac2cb613bf0b8a22690364fbc5
SHA1: 9383ed4ee7df17193f7a034c3190ecabc9000f9f
SHA256: 5479f8cd1375364770df36e5a18262480a8f9d31le8eedb2c2390ecb233852ad CREATED
: Mon Nov 9 15:15:32 2020 MODIFIED: Mon Nov 9 13:06:56 2020 ACCESSED: Wed Dec
7 20:21:53 2022
REASON 1: Yara Rule MATCH: [REDACTED] SUBSCORE: 70
DESCRIPTION: [REDACTED] - file metaslsoft.php REF: -
MATCHES: [REDACTED]: $buff .= "<tr><td><a href=\"?d=".pwd."\\">[ $folder ]</a></td><
td>LINK</t
[NOTICE] Results: 0 alerts, 1 warnings, 7 notices
[RESULT] [REDACTED] objects detected!
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-ba
se
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20221207T20:21:53Z

Press Enter to exit ...
cmnatic@thm-yara:~/suspicious-files/file1$ 
```

Answer



Réponse :b374k 2.2

Inspectez le fichier Yara qui a marqué le fichier 1. Dans le cadre de cette règle, combien de chaînes y a-t-il pour signaler ce fichier ?

Maintenant, à partir de deux des questions précédentes, nous savons que la règle Yara à laquelle il doit faire face est Web Shell, et la sortie de Loki nous montre le chemin du fichier que nous pouvons emprunter pour, espérons-le, trouver le fichier.

```
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 38 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 653 Yara rules
[INFO] Reading private rules from binary ...
```

Nous pouvons donc exécuter la commande ls /home/cmnatic/tools/Loki/signature-base/yara | grep webshell . Appuyez ensuite sur Entrée pour exécuter la commande.

```
cumnatic@thm-yara:~$ ls /home/cmnatic/tools/Loki/signature-base/yara | grep webshell
apt laudanum webshells.yar
apt webshell chinachopper.yar
cn pentestset webshells.yar
gen cn webshells.yar
thor-webshells.yar
```

Nous obtenons cinq fichiers Yara différents, le seul qui semble être celui à examiner est thor-webshells.yar. Je dis cela seulement parce que Thor a été mentionné dans la tâche précédente. Jetons donc un coup d'œil à cela et voyons ce que nous avons obtenu, utilisez la commande nano /home/cmnatic/tools/Loki/signature-base/yara/thor-webshells.yar et appuyez sur Entrée pour le regarder.

```
GNU nano 2.9.3          /home/cmnatic/tools/Loki/signature-base/yara/thor-webshells.yar

condition:
    all of them
}
rule webshell php backdoor {
    meta:
        description = "Web Shell - file php-backdoor.php"
        license = "https://creativecommons.org/licenses/by-nc/4.0/"
        author = "Florian Roth"
        date = "2014/01/28"
        score = 70
        hash = "2b5cb105c4ea9b5ebc64705b4bd86bf7"
    strings:
        $s1 = "if(!move_uploaded_file($_POST[\"file name\"], $dir.$fname))" fullword
        $s2 = "<pre><form action=\"?> echo $PHP_SELF; ?>\" METHOD=GET >execute command: <input "
    condition:
        all of them
}
rule webshell asp dabao {
    meta:
        description = "Web Shell - file dabao.asp"
        license = "https://creativecommons.org/licenses/by-nc/4.0/"
        author = "Florian Roth"
        date = "2014/01/28"
        score = 70
        hash = "3919b959e3fa7e86d52c2b0a91588d5d"
    strings:
        $s2 = "Echo \"<input type=button name=Submit onclick=\"$document.location =\"#039;\" &quot;
        $s8 = " Echo \"$document.Frm Pack.FileName.value=\"$\"\"\"+year+\"\"\"-(month+1)+\"\"\".\""
    condition:
        all of them
```

Get Help Write Out Where Is Cut Text Justify Cur Pos Undo Mark Text
Exit Read File Replace Uncut Text To Spell Go To Line Redo Copy Text

Ok, maintenant que le fichier est ouvert dans nano, recherchons-le. Appuyez sur F6 pour activer la fonction de recherche dans nano et tapez webshell_metaslsoft, puis appuyez sur Entrée.

```

} rule Webshell metaslsoft {
    meta:
        description = "Web Shell - file metaslsoft.php"
        license = "https://creativecommons.org/licenses/by-nc/4.0/"
        author = "Florian Roth"
        date = "2014/01/28"
        score = 70
        hash = "aa328ed1476f4a10c0bcc2dde4461789"
    strings:
        $s7 = "$buff .= \"<tr><td><a href=\"\\\"?d=".Spwd."\\\">[ $folder ]</a></td><td>LINK</t"
    condition:
        all of them
}

```

Nous avons le bon fichier et avons été dirigés vers la bonne règle Yara. Alors maintenant, nous recherchons la partie chaînes et comptons combien de règles se trouvent sous la catégorie chaîne. Une fois que vous avez fait cela, tapez votre réponse dans le champ de réponse de TryHackMe et cliquez sur Soumettre.

```

} rule Webshell metaslsoft {
    meta:
        description = "Web Shell - file metaslsoft.php"
        license = "https://creativecommons.org/licenses/by-nc/4.0/"
        author = "Florian Roth"
        date = "2014/01/28"
        score = 70
        hash = "aa328ed1476f4a10c0bcc2dde4461789"
    strings:
        $s7 = "$buff .= \"<tr><td><a href=\"\\\"?d=".Spwd."\\\">[ $folder ]</a></td><td>LINK</t"
    condition:
        all of them
}

```

Réponse 1

Analyser le fichier 2. Loki détecte-t-il ce fichier comme suspect/malveillant ou inoffensif ?
Alors changeons de répertoire, avec cd ..

```
cmmnatic@thm-yara:~/suspicious-files/file1$ cd ..
```

Ensuite, déplacez-vous dans le répertoire file2 avec cd file2

```
cmmnatic@thm-yara:~/suspicious-files$ cd file2
```

Nous pouvons maintenant exécuter Loki avec la commande python
/home/cmmnatic/tools/Loki/loki.py -p .

Une fois l'analyse de Loki terminée, il est temps de voir si c'est sûr ou non. D'après l'analyse, le fichier est propre.

```
[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20221208T00:53:15Z PLATFORM:      PROC: x86_64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasher
ezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 653 Yara rules
[INFO] Reading private rules from binary ...
[NOTICE] Program should be run as "root" to ensure all access rights to process memory and file objects.
[NOTICE] Running plugin PluginWMI
[NOTICE] Finished running plugin PluginWMI
[INFO] Scanning ...
[NOTICE] Results: 0 alerts, 0 warnings, 7 notices
[RESULT] SYSTEM SEEMS TO BE CLEAN.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-base
[NOTICE] Finished Loki Scan SYSTEM: thm-yara TIME: 20221208T00:53:19Z
```

Réponse : bénin

Inspecter le fichier 2. Quel est le nom et la version de ce shell Web ? Utilisez ls pour répertorier le contenu du répertoire.

```
cmmnatic@thm-yara:~/suspicious-files/file2$ ls  
Index.php loki thm-yara 2022-12-08 00-53-15.log
```

Utilisez maintenant nano sur le fichier 1ndex.php, comme ceci, nano 1ndex.php .

```
cmmnatic@thm-yara:~/suspicious-files/file2$ nano index.php
```

Cela ouvrira le fichier afin que vous puissiez en voir les détails. Si vous regardez en haut à gauche du fichier php, vous verrez le nom et la version. la réponse ne nécessite pas le mot

shell. Donc, une fois que vous l'avez trouvé, tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.



```
GNU nano 2.9.3
<?php
/*
Answer
shell
Jayalah Indonesiaku
(c)2014
https://github.com/b374k/b374k
*/
```

Tâche 9 Créer des règles Yara avec yarGen

Créer des règles Yara avec yarGen

À partir de la section précédente, nous avons réalisé que nous avions un fichier sur lequel Loki n'avait pas signalé. À ce stade, nous ne pouvons pas exécuter Loki sur d'autres serveurs Web, car si le fichier 2 existe sur l'un des serveurs Web, il ne sera pas détecté. Nous devons créer une règle Yara pour détecter ce shell Web spécifique dans notre environnement. C'est généralement ce qui est fait en cas d'incident, c'est-à-dire un événement qui affecte/impacte l'organisation de manière négative.

Nous pouvons ouvrir manuellement le fichier et tenter de parcourir lignes après lignes de code pour trouver des chaînes possibles pouvant être utilisées dans notre règle Yara nouvellement créée.

Vérifions le nombre de lignes de ce fichier particulier. Vous pouvez exécuter ce qui suit :

```
strings <file name> | wc -l.
```

Utiliser wc pour compter le nombre de lignes dans le fichier

```
cminatic@thm-yara:~/fichiers-suspects/file2$    chaînes      index.php      |
toilettes -l
```

Si vous essayez de parcourir manuellement chaque chaîne, ligne par ligne, vous comprendrez rapidement que cela peut être une tâche ardue.

Capturer la sortie de 1ndex.php

```
if (res== 'erreur' ){
$( '.ulProgress' +ulType+i).html( '( échoué )' );
}
else {
$( '.ulRes' +ulType+i).html(res);
}
chargement_stop();
},
erreur : function () {
chargement_stop();
$( '.ulProgress' +ulType+i).html( '( échoué )' );
$( '.ulProgress' +ulType+i).removeClass( 'ulProgress' +ulType+i);
$( '.ulFilename' +ulType+i).removeClass( 'ulFilename' +ulType+i);
}
);
}
}

function ul_go(ulType){
ulFile = (ulType== 'comp' ) ? $( '.ulFileComp' ):$( '.ulFileUrl' );
ulResult = (ulType== 'comp' ) ? $( '.ulCompResult' ):$( '.ulUrlResult' );
);
ulResult.html( '' );

ulFile.each( function (i){
if (((ulType== 'comp' ) &&this.files[0]) || ((ulType== 'url'
)&&(this.value!= '' ))) {
file = (ulType== 'comp' )? this.files[0] : ceci. valeur;
nom de fichier = (ulType== 'comp' ) ? fichier.nom :
fichier.substring(file.lastIndexOf('/')+1);

ulSaveTo = (ulType== 'comp' ) ? $( '.ulSaveToComp' )[i].value:$(
'.ulSaveToUrl' )[i].value;

ulFilename = (ulType== 'comp' ) ? $( '.ulFilenameComp' )[i].value:$(
'.ulFilenameUrl' )[i].value;
}
```

--extrait coupé par souci de concision--

Heureusement, nous pouvons utiliser [yarGen](#) (oui, un autre outil créé par Florian Roth) pour nous aider dans cette tâche.

Qu'est-ce que yarGen ? yarGen est un générateur de règles YARA.

Extrait du README — « Le principe principal est la création de règles Yara à partir des chaînes trouvées dans les fichiers malveillants tout en supprimant toutes les chaînes qui apparaissent également dans les fichiers goodware. Par conséquent, yarGen inclut une grande base de données de chaînes de goodware et d'opcodes sous forme d'archives ZIP qui doivent être extraites avant la première utilisation .

Accédez au yarGenrépertoire qui se trouve dans tools. Si vous exécutez yarGen sur votre propre système, vous devez d'abord le mettre à jour en exécutant la commande suivante :
python3 yarGen.py --update

Cela mettra à jour les bases de données good-opcodes et good-strings du référentiel en ligne. Cette mise à jour prendra quelques minutes.

Une fois la mise à jour réussie, vous verrez le message suivant à la fin de la sortie.

Mise à jour de yarGen

```
cmmnatic@thm-yara:~/tools/yarGen$ python3 yarGen.py --update
```

```
-----  
-----  
-----  
____ / ____  
/ / / _ `/_ / ( _ / -_) _ \\  
\_, /\_,/_/ \_\/_//_/_/  
___/ Générateur de règles Yara
```

```
Florian Roth, juillet 2020 , Version 0.23.3
```

```
Remarque : les règles doivent être post-traitées.
```

```
Voir cet article pour plus de détails :
```

```
https://medium.com/@cyb3rops/121d29322282
```

Téléchargement de good-opcodes-part1.db depuis
<https://www.bsk-consulting.de/yargen/good-opcodes-part1.db> ...

Pour utiliser yarGen afin de générer une règle Yara pour le fichier 2, vous pouvez exécuter la commande suivante :

```
python3      yarGen.py      -m      /home/cmnatic/suspicious-files/file2  
--excludegood -o /home/cmnatic/suspicious-files/file2.yar
```

Une brève explication des paramètres ci-dessus :

- -m est le chemin d'accès aux fichiers pour lesquels vous souhaitez générer des règles
- --excludegood forcer à exclure toutes les chaînes de goodware (ce sont des chaînes trouvées dans des logiciels légitimes et peuvent augmenter les faux positifs)
- -o emplacement et nom avec lesquels vous souhaitez afficher la règle Yara

Si tout va bien, vous devriez voir le résultat suivant.

Utiliser yarGen pour générer une règle pour le fichier2

```
[=] Génération de 1 règle SIMPLE.
```

```
[=] Toutes les règles écrites dans  
/home/cmnatic/suspicious-files/file2.yar
```

```
[+] L'exécution de yarGen est terminée
```

En règle générale, vous examinerez la règle Yara et supprimerez toutes les chaînes qui, selon vous, pourraient générer des faux positifs. Pour cet exercice, nous laisserons la règle Yara générée telle quelle et testerons si Yara signalera le fichier 2 ou non.

Remarque : Un autre outil créé pour vous aider s'appelle [yarAnalyzer](#) (vous l'aurez deviné – créé par Florian Roth). Nous n'examinerons pas cet outil dans cette salle, mais vous devriez le lire, surtout si vous décidez de commencer à créer vos propres règles Yara.

Lectures complémentaires sur la création de règles Yara et l'utilisation de yarGen :

- <https://www.bsk-consulting.de/2015/02/16/write-simple-sound-yara-rules/>
- <https://www.bsk-consulting.de/2015/10/17/how-to-write-simple-but-sound-yara-rules-part-2/>
- <https://www.bsk-consulting.de/2016/04/15/how-to-write-simple-but-sound-yara-rules-part-3/>

Répondre aux questions ci-dessous

À partir de la racine du répertoire des fichiers suspects, quelle commande exécuteriez-vous pour tester Yara et votre règle Yara par rapport au fichier 2 ?

Pour répondre à cette question, vous devez réfléchir à la façon dont vous exécuteriez le fichier en utilisant Yara, et non Loki comme dans la tâche précédente. Vous créez donc la

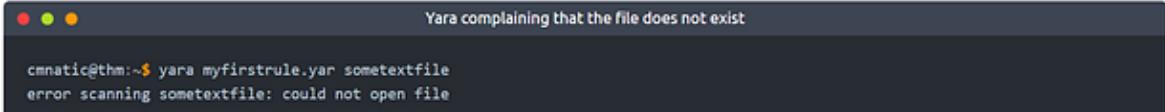
syntaxe dans laquelle vous allez exécuter la règle sur le fichier. Si nous revenons à la tâche 4, nous pouvons voir à quoi devrait ressembler le résumé.



If "somefile" exists, Yara will say `examplerule` because the pattern has been met - as we can see below:

```
cmnatic@thm:~$ yara myfirstrule.yar somefile
examplerule somefile
```

If the file does not exist, Yara will output an error such as that below:



```
cmnatic@thm:~$ yara myfirstrule.yar sometextfile
error scanning sometextfile: could not open file
```

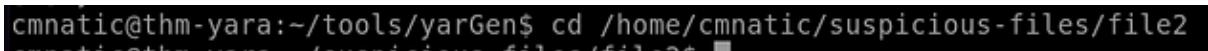
Congrats! You've made your first rule.

Donc, avec cette connaissance et le nom et l'emplacement de la nouvelle règle Yara, nous répondons à cette question. Vous devrez échanger le nom du fichier et l'emplacement/nom du fichier de règles Yara pour la réponse, vous ne savez pas pourquoi c'est comme ça, mais c'est le format de la réponse. Une fois que vous l'avez bien compris, saisissez-le dans le champ de réponse TryHackMe et cliquez sur Soumettre.

Réponse : yara 1index.php fichier2/fichier2.yar

La règle Yara a-t-elle signalé le fichier 2 ? (Ouais/Non)

Avant d'exécuter cela, passons au fichier avec `cd /home/cmnatic/suspicious-files/file2`.



```
cmnatic@thm-yara:~/tools/yarGen$ cd /home/cmnatic/suspicious-files/file2
```

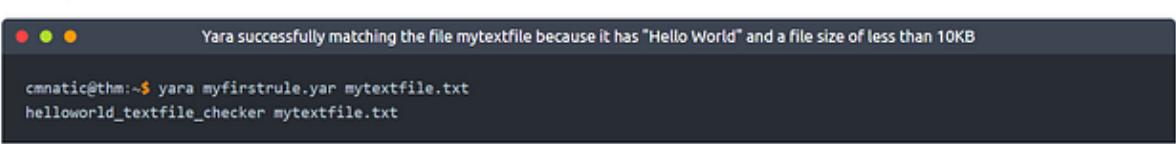
Maintenant que nous sommes dans ce répertoire, modifions la syntaxe de la question précédente, afin de pouvoir exécuter cette règle yara sur le fichier php. Nous pouvons donc configurer la syntaxe comme celle-ci, `yara /home/cmnatic/suspicious-files/file2.yar 1index.php`



```
cmnatic@thm-yara:~/suspicious-files/file2$ yara /home/cmnatic/suspicious-files/file2.yar index.php
/home cmnatic suspicious_files file2 index index.php
```

Alors, que signifie ce résultat, si nous revenons à la tâche 5, nous pouvons voir ce que signifie le résultat.

However, the rule matched this time because the file has both "Hello World!" and a file size of less than 10KB.



```
cmnatic@thm:~$ yara myfirstrule.yar mytextfile.txt
helloworld_textfile_checker mytextfile.txt
```

Du coup trouvé assorti au yararule !! Puisqu'il a trouvé une correspondance, nous connaissons notre réponse et pouvons la saisir dans le champ de réponse TryHackMe et cliquer sur Soumettre.

Réponse : Ouais

Copiez la règle Yara que vous avez créée dans le répertoire des signatures Loki. Cette question n'appelle pas de réponse mais nécessite un peu de travail. Pour déplacer la règle Yara vers le répertoire Loki Yara. Vous pouvez revenir sur le résultat de l'analyse Loki, si vous ne l'avez pas, voici la syntaxe pour déplacer le fichier vers le répertoire approprié :
mv /home/cmnatic/suspicious-files/file2.yar /home/cmnatic/ outils/Loki/signature-base/yara/

```
cmmatic@thm-yara:~/suspicious-files/file2$ mv /home/cmnatic/suspicious-files/file2.yar /home/cmnatic/tools/Loki/signature-base/yara/
```

Maintenant que le fichier est déplacé vers le bon répertoire, vous pouvez maintenant passer à la question suivante.

Testez la règle Yara avec Loki, est-ce qu'elle signale le fichier 2 ? (Ouais/Non)

Nous exécuterons à nouveau Loki, comme nous l'avons fait dans la tâche précédente. Commençons par changer le répertoire vers le fichier que nous voulons analyser avec cd /home/cmnatic/suspicious-files/file2

```
cmmatic@thm-yara:~/tools/yarGen$ cd /home/cmnatic/suspicious-files/file2
```

Étant dans le bon répertoire, nous devons saisir la syntaxe correcte dans le terminal, python /home/cmnatic/tools/Loki/loki.py -p . , et appuyez sur Entrée pour exécuter le programme.

```
cmmatic@thm-yara:~/suspicious-files/file2$ python /home/cmnatic/tools/Loki/loki.py -p .
```

```
Copyright by Florian Roth, Released under the GNU General Public License  
Version 0.32.1  
DISCLAIMER - USE AT YOUR OWN RISK  
Please report false positives via https://github.com/Neo23x0/Loki/issues
```

Cette fois, nous obtenons des résultats sur le dossier, et puisque nous voyons que nous obtenons des résultats, répondez à cette question. Tapez la réponse dans le champ de réponse sur TryHackMe et cliquez sur Soumettre.

```
[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20221208T14:28:10Z PLATFORM:      PROC: x86_64 ARCH: 64bit
[NOTICE] Registered plugin PluginMMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO]  File Name Characteristics initialized with 2841 regex patterns
[INFO]  C2 server indicators initialized with 1541 elements
[INFO]  Malicious MD5 Hashes initialized with 19034 hashes
[INFO]  Malicious SHA Hashes initialized with 7159 hashes
[INFO]  Malicious SHA256 Hashes initialized with 22841 hashes
[INFO]  False Positive Hashes initialized with 30 hashes
[INFO]  Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO]  Initializing all YARA rules at once (composed string of all rule files)
[INFO]  Initialized 654 Yara rules
[INFO]  Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process memory and file objects.
[NOTICE] Running plugin PluginMMI
[NOTICE] Finished running plugin PluginMMI
[INFO] Scanning . ...
[WARNING]
FILE: ./index.php SCORE: 70 TYPE: PHP SIZE: 223978
FIRST_BYTES: 3c3f7068700a2f2a0a0623337346b207368656c / <?php/*b374k shel
MD5: c6a7ebafde239d65248e2b69b670157
SHA1: 3926ab64dcf04e87024011cf39902beac3271lida
SHA256: 53fe44b4753874f079a936325d1fdc9b1691956a29c3aaef8643cdbd49f5984bf CREATED: Mon Nov  9 15:16:03 2020 MODIFIED: Mon Nov  9 13:09:18 2020 ACCESSED: Th
v Dec  8 13:14:09 2022
REASON 1: Yara Rule MATCH: _home_cmnatic_suspicious_files_file2_index SUBSCORE: 70
DESCRIPTION: file2 - file index.php REF: https://github.com/Neo23x0/yarGen
MATCHES: Str1: var [REDACTED]=function(){function G(a){return a==null?String(a):z[A.call(a)]}||"object"}function H(a){return G(a)=="function"}fun Str2: $c ... (truncated)
[NOTICE] Results: 0 alerts, 1 warnings, 7 notices
[RESULT] Suspicious objects detected!
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-base
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20221208T14:28:15Z
```

Réponse : Ouais

Quel est le nom de la variable pour la chaîne sur laquelle elle correspond ?

En revenant à notre sortie du scan Loki, recherchez le texte blanc qui dit MATCHES : après le mot var se trouve la réponse. Une fois que vous l'avez trouvé, tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

```
[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20221208T14:28:10Z PLATFORM:      PROC: x86_64 ARCH: 64bit
[NOTICE] Registered plugin PluginMMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO]  File Name Characteristics initialized with 2841 regex patterns
[INFO]  C2 server indicators initialized with 1541 elements
[INFO]  Malicious MD5 Hashes initialized with 19034 hashes
[INFO]  Malicious SHA Hashes initialized with 7159 hashes
[INFO]  Malicious SHA256 Hashes initialized with 22841 hashes
[INFO]  False Positive Hashes initialized with 30 hashes
[INFO]  Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO]  Initializing all YARA rules at once (composed string of all rule files)
[INFO]  Initialized 654 Yara rules
[INFO]  Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process memory and file objects.
[NOTICE] Running plugin PluginMMI
[NOTICE] Finished running plugin PluginMMI
[INFO] Scanning . ...
[WARNING]
FILE: ./index.php SCORE: 70 TYPE: PHP SIZE: 223978
FIRST_BYTES: 3c3f7068700a2f2a0a0623337346b207368656c / <?php/*b374k shel
MD5: c6a7ebafde239d65248e2b69b670157
SHA1: 3926ab64dcf04e87024011cf39902beac3271lida
SHA256: 53fe44b4753874f079a936325d1fdc9b1691956a29c3aaef8643cdbd49f5984bf CREATED: Mon Nov  9 15:16:03 2020 MODIFIED: Mon Nov  9 13:09:18 2020 ACCESSED: Th
v Dec  8 13:14:09 2022
REASON 1: Yara Rule MATCH: _home_cmnatic_suspicious_files_file2_index SUBSCORE: 70
DESCRIPTION: file2 - file index.php REF: https://github.com/Neo23x0/yarGen
MATCHES: Str1: var [REDACTED]=function(){function G(a){return a==null?String(a):z[A.call(a)]}||"object"}function H(a){return G(a)=="function"}fun Str2: $c ... (truncated)
[NOTICE] Results: 0 alerts, 1 warnings, 7 notices
[RESULT] Suspicious objects detected!
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-base
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20221208T14:28:15Z
```

Réponse : Zepto

Inspectez la règle Yara, combien de chaînes ont été générées ?

Puisque nous savons où se trouve le fichier, nous n'avons pas besoin de changer de répertoire, nous pouvons ouvrir nano directement sur le fichier. Nous pouvons le faire avec la syntaxe nano /home/cmnatic/tools/Loki/sigature-base/yara/file2.yar

```
GNU nano 2.0.9.3                               /home/cmnatic/tools/Loki/signature-base/yara/file2.yar

YARA Rule Set
Author: yarGen Rule Generator
Date: 2022-12-08
Identifier: file2
Reference: https://github.com/Neo23x0/yarGen
*/
/* Rule Set ..... */

rule _home_cmnatic_suspicious_files_file2_index {
meta:
    description = "file2 - file index.php"
    author = "yarGen Rule Generator"
    reference = "https://github.com/Neo23x0/yarGen"
    date = "2022-12-08"
    hash1 = "53fe44bf4753874f079a936325d1fc9b1691956a29c3aa8643cd8d49f5984bf"
strings:
    $x1 = "var Zepto=function(){function G(a){return a==null?String(a):z[A.call(a)]}||\"object\");function H(a){return G(a)==\"function\");fun" ascii
    $x2 = "$cmd = execute(\"taskkill /F /PID \\",$pid);\") fullword ascii
    $x3 = "return (res = new RegExp(\"(?::|^\") + encodeURIComponent(key) + '(?:[^"]*)').exec(document.cookie)) ? (res[1]) : null;" fullword ascii
    $x4 = "$cmd = trim(execute(\"ps -p \",$pid);\") fullword ascii
    $x5 = "$buff = execute(\"wget \",Surl,\",\" -O \",$saveas);\") fullword ascii
    $x6 = "$id = \"0\"*4; $dt=d2t?0:dt1*dt2?1:1; r=function(a,b){for(var c=0,e=a.length-1,g=h:g;){for(var g=j,f=c;f<e;+f)0" ascii
    $x7 = "$buff = execute(\"curl \",Surl,\",\" -o \",$saveas);\") fullword ascii
    $x8 = "$cmd = execute(\"\\kill -9 \",$pid);\") fullword ascii
    $x9 = "$cmd = execute(\"Tasklist /FI \"/\"PID eq \",$pid,\") fullword ascii
    $x10 = "execute(\"tar xzf \",basename($archive),\" \",\" -C \",basename($archive),\" \",\"Starget.\",\" \",\" \");\" fullword ascii
    $x11 = "execute(\"tar xf \",basename($archive),\" \",\" -C \",basename($archive),\" \",\"Starget.\",\" \",\" \");\" fullword ascii
    $x12 = "ngs.nameType@/xhr.getResponseHeader('Content-Type')/result=xhr.responseText;try{datatype=\"script\"?1,eval(result):datatype\" ascii
    $x13 = "$body = preg_replace('/> href=\"([^\"]*)http://([^\"]*)\.zend\.com/([^\"]*)?</a>/i', '\", \"$1\", $body);\" fullword ascii
    $x14 = "$check = strtolower(execute(\"nodejs -h\"));\" fullword ascii
    $x15 = "$check = strtolower(execute(\"java -help\"));\" fullword ascii
    $x16 = "$buff = execute(\"lynx -source \",Surl,\",\" -O \",$saveas);\") fullword ascii

Get Help      To Write Out      To Where Is      To Cut Text      To Justify      To Cur Pos      M-U Undo      M-A Mark Text      M-] To Bracket
Q Exit        To Read File     To Replace      To Uncut Text     To To Spell      M-E Go To Line      M-E Redo      M-B Copy Text      M-[ WhereIs Next
```

Comme nous pouvons le voir, les chaînes que nous recherchons commencent au milieu du terminal et vont au-delà. Tout ce que vous avez à faire est de compter le nombre de chaînes et de saisir ce nombre dans le champ de réponse TryHackMe, puis de cliquer sur Soumettre.

```
strings:
  "var Zepto=function(){function G(a){return a==null?String(a):z[A.call(a)]||"\object"}function M(a){return G(a)=="function"}fun" ascii
  "+$cmd = execute(`taskkill /F /PID ${_Spid}`);" fullword ascii
  "return [res = new RegExp(`[?]:${_Spid}`)] + encodeURIComponent(key) + `(${[^;]*})`.exec(document.cookie)) ? (res[1]) : null;" fullword ascii
  "$cmd = trim(execute(`ps -p ${_Spid}`));" fullword ascii
  "$buf = execute(`wget ${_Url}`) -O ${_Ssaveas};" fullword ascii
  "+d1=0;" d2=0;d1=d1?0:d1+1?1:1;,+function(a,b){for(var c=0,e=a.length-1,g=h;r;)for(var g=j,f=c;f<e++f)0" ascii
  "$buf = execute(`curl -s ${_Url}`) -o ${_Ssaveas};" fullword ascii
  "$cmd = execute(`kill -9 ${_Spid}`);" fullword ascii
  "$cmd = execute(`tasklist /FI ${_PID} eq ${_Spid}`);" fullword ascii
  "+execute(`tar xf ${_tarname}`,"${baseName(_archive)}\${_tarname}\${_tarname}.tar${_tarname}.tar${_tarname}`);" fullword ascii
  "+execute(`tar xf ${_tarname}`,"${baseName(_archive)}\${_tarname}\${_tarname}\${_tarname}.tar${_tarname}`);" fullword ascii
  "+ngs.mimeType[xhr.getResponseHeader('Content-Type')];" result=xhr.responseText;try{datatype=?{1,eval}(result):dataType" ascii
  "$body = preg_replace('/<a href=\\"http://www.zend.com/\?.+\?>/i', '\\", \$body);" fullword ascii
  "$check = strtolower(execute(`nodejs -h`));" fullword ascii
  "$check = strtolower(execute(`java -help`));" fullword ascii
  "$buff = execute(`lynx -source ${_Url}`) > ${_Ssaveas};" fullword ascii
  "$buff = execute(`lwp-download ${_Url}`) > ${_Ssaveas};" fullword ascii
  "$src=urldata(application/x-font-woff;charset=utf-8;base64,d09RGrgABAAAAGKYAAABAAAAAp+gAAQABAAAAA" ascii
  "$check = strtolower(execute(`perl -h`));" fullword ascii
  "$check = strtolower(execute(`python -h`));" fullword ascii

condition:
  uint16(0) == 0x3f3c and filesize < ===== and
  1 of ($x*) and 4 of them
```

Réponse : 20

L'une des conditions à respecter dans la règle Yara spécifie la taille du fichier. Le dossier doit être inférieur à quel montant ?

Cette réponse se trouve sous la section chaîne, dans la section conditions. Dans la première ligne, vous verrez la taille du fichier, puis à droite la taille du fichier. Une fois que vous avez trouvé la réponse, saisissez-la dans le champ de réponse TryHackMe et cliquez sur Soumettre.

```
strings:
= "var Zepto=function(){function G(a){return a==null?String(a)|||\\"object\\\"}function H(a){return G(a)==\\\"function\\\"}fun"
= "$cmd = execute(\"taskkill /F /PID \".$pid);\" fullword ascii
= \"return [res = new RegExp('(?:(?:[^";]+";)+([^\"]*)').exec(document.cookie) ? (res[1]) : null];\" fullword ascii
= \"$cmd = trim(execute(\"ps -o pid --sort=-pid\"));\" fullword ascii
= \"$buff = execute(\"wget \".$url.\" -O \".$saveas);\" fullword ascii
= \"(de\"0\"+d);dt2ywid;return dt1=dt2?dt1<dt2?-1:1},r:function[a,b]{for(var c=0,e=a.length-1,g=h;z){{for(var g=j,f=c;f<e;+f)0\" ascii
= \"$buff = execute(\"curl \".$url.\" -o \".$saveas);\" fullword ascii
= \"$cmd = execute(\"kill -9 \".$pid);\" fullword ascii
= \"$cmd = execute(\"tasklist /FI \\"PID eq \".$pid\\\".basename($archive),\\\"\\\"-c \\\"\\\".startget,\\\"\\\"\\\");\" fullword ascii
= \"execute(\"tar xf \\"\\\".basename($archive).\\\"\\\" -C \\"\\\".startget,\\\"\\\"\\\");\" fullword ascii
= \"nsg.mimeTypelxhr.getResponseHeader(\"content-type\").result=xhr.responseText;try{dataType=\"script\"?1,eval}(result):dataTyp\" ascii
= \"$body = preg_replace(\"<a href=\"\\\\"http://\\\\"www.zend.com\\\\"/(.*?)\\\\">\\"\\\", \\"\\\", $body);\" fullword ascii
= \"$check = strtolower(execute(\"nodejs -h\"));\" fullword ascii
= \"$check = strtolower(execute(\"java -help\"));\" fullword ascii
= \"$buf = execute(\"lynx -source \".$url.\" > \".$saveas);\" fullword ascii
= \"$buf = execute(\"lwp-download \".$url.\" \".$saveas);\" fullword ascii
= \"$src:urlidata:application/x-font-woff;charset=utf-8;base64,d09GrgABAAAAAGKYAAA8AAAAAp+gAAQABAAAAA8AAAAAAAAAAABGRlRNAAAABWA\" ascii
= \"$check = strtolower(execute(\"perl -h\"));\" fullword ascii
= \"$check = strtolower(execute(\"python -h\"));\" fullword ascii

condition:
vint16(0) == 0x3f3c and filesize < [REDACTED] and [REDACTED]
1 of {$x*} and 4 of them
```

Réponse : 700 Ko

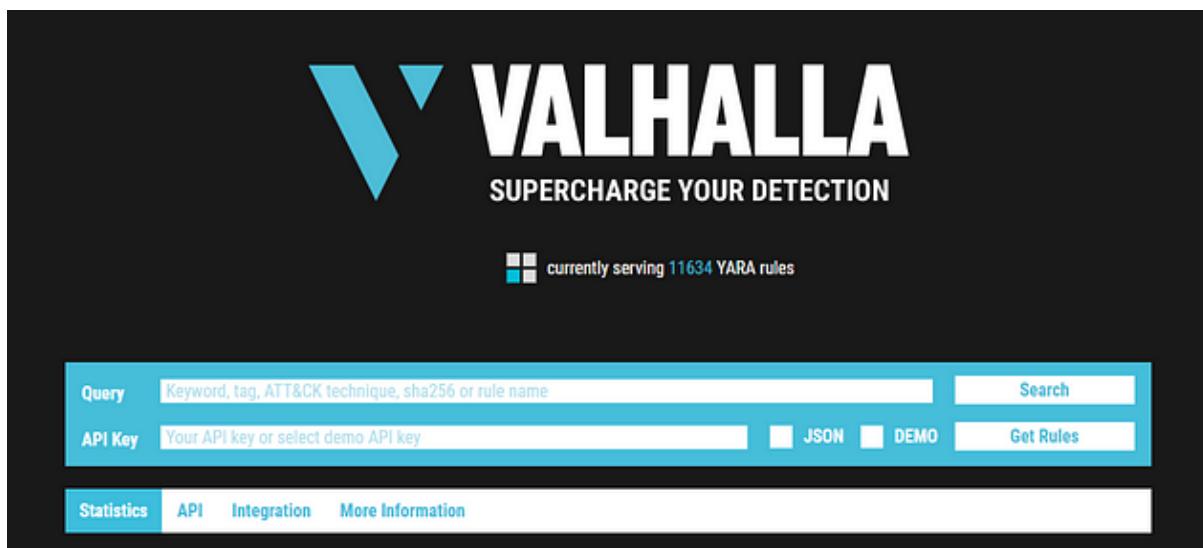
Tâche 10 Valhalla

Valhalla

Valhalla est un flux Yara en ligne créé et hébergé par [Nextron-Systems](#) (eh, Florian Roth).

À présent, vous devriez être conscient du temps et de l'énergie ridicules que Florian a consacrés à la création de ces outils pour la communauté. Peut-être aurions-nous dû simplement appeler cela la salle Florian Roth. (mdr)

Selon le site Web, « Valhalla améliore vos capacités de détection grâce à la puissance de milliers de règles YARA de haute qualité fabriquées à la main. »



À partir de l'image ci-dessus, nous devons indiquer que nous pouvons effectuer des recherches basées sur un mot-clé, une balise, une technique ATT&CK, sha256 ou un nom de règle.

Remarque : Pour plus d'informations sur ATT&CK, veuillez visiter la salle [MITRE](#).

En examinant les données qui nous ont été fournies, examinons la règle dans la capture d'écran ci-dessous :

Newest YARA Rules			
This table shows the newest additions to the rule set			
Rule	Description	Date	Ref
SUSP_Base64_Encoded_WhomAmI	Detects suspicious encoded whomami string that is a program to evaluate the current user name and often used in malicious or benign recon scripts	09.11.2020	🔗

Nous recevons le nom de la règle, une brève description, un lien de référence pour plus d'informations sur la règle, ainsi que la date de la règle.

N'hésitez pas à regarder quelques règles pour vous familiariser avec l'utilité du Valhalla. La meilleure façon d'apprendre le produit est de se lancer directement.

En reprenant notre scénario, à ce stade, vous savez que les 2 fichiers sont liés. Même si Loki a classé les fichiers comme suspects, vous savez au fond de votre instinct qu'ils sont malveillants. D'où la raison pour laquelle vous avez créé une règle Yara en utilisant yarGen pour la détecter sur d'autres serveurs Web. Mais imaginons en outre que vous n'êtes pas doué en code (pour information, tous les professionnels de la sécurité ne savent pas comment coder/scripter ou le lire). Vous devez effectuer des recherches plus approfondies concernant ces fichiers pour recevoir l'autorisation de les éradiquer du réseau.

Il est temps d'utiliser Valhalla pour collecter des renseignements sur les menaces...

Répondre aux questions ci-dessous

Avant de répondre, passons au site [Valhalla](#), voici le lien vers ledit site <https://valhalla.nextron-systems.com>. Maintenez ctrl et cliquez sur le lien pour l'ouvrir dans un nouvel onglet.

The screenshot shows the Valhalla web application. At the top, there's a large logo with a stylized 'V' and the word 'VALHALLA' in bold capital letters, with the tagline 'SUPERCHARGE YOUR DETECTION' below it. Below the logo, a message indicates 'currently serving 17337 YARA rules and 2686 Sigma rules'. The main search area has a 'Query' field containing 'Keyword, tag, ATT&CK technique, sha256 or rule name', an 'API Key' field, and buttons for 'Search', 'JSON', 'DEMO', 'Get YARA Rules', and 'Get Sigma Rules'. Below this is a navigation bar with tabs for 'Statistics' (which is active), 'API', 'Integration', and 'Get Access'. A chart titled 'New Rules per Day' shows a single data point at approximately 32 rules on day 25. The background is dark with light-colored text and buttons.

Entrez le hachage SHA256 du fichier 1 dans Valhalla. Ce fichier est-il attribué à un groupe APT ? (Ouais/Non)

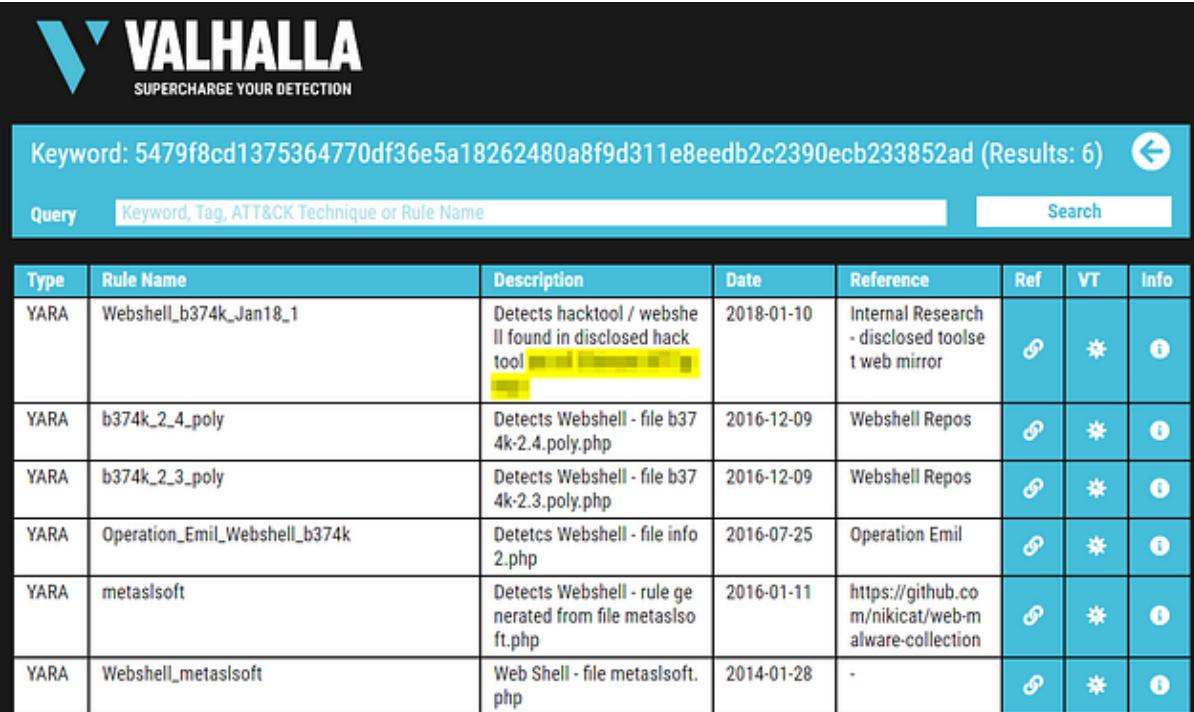
Si vous avez toujours le hachage SHA256 pour le fichier 1 de la tâche précédente, génial, sinon le voici :

5479f8cd1375364770df36e5a18262480a8f9d311e8eedb2c2390ecb233852ad

Vous devriez être sur le site Web de Valhalla, vous verrez un champ de recherche de requête. Prenez le hachage SHA256 ci-dessus, copiez (ctrl + c) et collez (ctrl + v) dans le champ Requête sur Valhalla. Cliquez ensuite sur le bouton Rechercher à droite.

This screenshot of the Valhalla interface is identical to the one above, but with two red arrows added. One arrow points from the number '1' to the 'Query' input field where the SHA256 hash '5479f8cd1375364770df36e5a18262480a8f9d311e8eedb2c2390ecb233852ad' is entered. Another arrow points from the number '2' to the 'Search' button.

Après avoir recherché le SHA256, vous pouvez trouver la réponse dans le premier résultat. Lisez la description, une fois que vous avez trouvé la réponse, saisissez-la dans le champ de réponse TryHackMe et cliquez sur Soumettre.



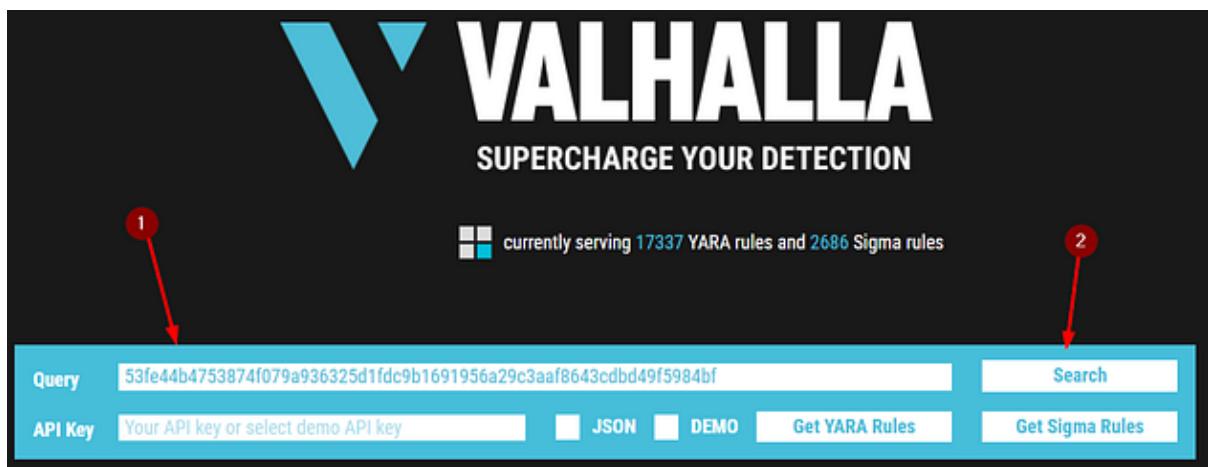
The screenshot shows the Valhalla search interface. At the top, there's a logo with the word "VALHALLA" and the tagline "SUPERCHARGE YOUR DETECTION". Below the logo, a search bar contains the keyword "5479f8cd1375364770df36e5a18262480a8f9d311e8eedb2c2390ecb233852ad" and indicates "(Results: 6)". There's a back arrow icon next to the results count. Below the search bar is a form with "Query" and "Search" fields. The main area is a table with the following columns: Type, Rule Name, Description, Date, Reference, Ref, VT, and Info. The table rows are as follows:

Type	Rule Name	Description	Date	Reference	Ref	VT	Info
YARA	Webshell_b374k_Jan18_1	Detects hacktool / webshe ll found in disclosed hack tool [REDACTED]	2018-01-10	Internal Research - disclosed tools e t web mirror			
YARA	b374k_2_4_poly	Detects Webshell - file b37 4k-2.4.poly.php	2016-12-09	Webshell Repos			
YARA	b374k_2_3_poly	Detects Webshell - file b37 4k-2.3.poly.php	2016-12-09	Webshell Repos			
YARA	Operation_Emil_Webshell_b374k	Detetcs Webshell - file info 2.php	2016-07-25	Operation Emil			
YARA	metasisoft	Detects Webshell - rule ge nerated from file metaslso ft.php	2016-01-11	https://github.co m/nikicat/web-m alware-collection			
YARA	Webshell_metaslsoft	Web Shell - file metaslsoft. php	2014-01-28	-			

Réponse : Ouais

Faites de même pour le fichier 2. Quel est le nom de la première règle Yara à détecter le fichier 2 ?

Si vous avez toujours le hachage SHA256 pour le fichier 2 de la tâche précédente, génial, sinon le voici : 53fe44b4753874f079a936325d1fdc9b1691956a29c3aaf8643cdbd49f5984bf Sur votre navigateur Web, appuyez sur le bouton Retour pour revenir à la page d'accueil de Valhalla. Avant de pouvoir insérer le hachage file2 SHA256, vous devrez supprimer le hachage précédent, cela peut facilement être fait en mettant en surbrillance et en appuyant sur Supprimer ou en cliquant à l'extrême droite de la recherche de requête et en maintenant l'espace arrière jusqu'à ce qu'il disparaisse. Maintenant, prenez le hachage SHA256 ci-dessus, copiez (ctrl + c) et collez (ctrl + v) dans le champ Requête de Valhalla. Cliquez ensuite sur le bouton Rechercher à droite.



Lorsque les résultats de la recherche se chargeront, vous en verrez quatre. Même si la question demande la première règle pour détecter le fichier, regardez d'abord la colonne de date et partez de là. Une fois que vous l'avez compris, mettez en surbrillance copier (ctrl + c) et collez (ctrl + v) ou tapez la réponse dans le champ TryHackMe Answer et cliquez sur Soumettre.

The screenshot shows the search results page for the keyword '53fe44b4753874f079a936325d1fdc9b1691956a29c3aa8643cdbd49f5984bf'. The results section has a header 'Keyword: 53fe44b4753874f079a936325d1fdc9b1691956a29c3aa8643cdbd49f5984bf (Results: 4)' with a back arrow icon. Below the header is a search bar with the placeholder 'Query Keyword, Tag, ATT&CK Technique or Rule Name' and a 'Search' button. The main area contains a table with four rows of search results:

Type	Rule Name	Description	Date	Reference	Ref	VT	Info
YARA	WebshellRepo_convert	Detects Webshell - file convert.php	2016-12-09	Webshell Repos			
YARA	Operation_Emil_Webshell_pluginsphp	Detects an Operation Emil Webshell - file plugins.php	2016-07-29	Operation Emil			
YARA		Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			
YARA	Webshell_b374k_rule2	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			

Réponse : Webshell_b374k_rule1

Examinez les informations du fichier 2 de Virus Total (VT). Le Yara Signature Match provient de quel scanner ?

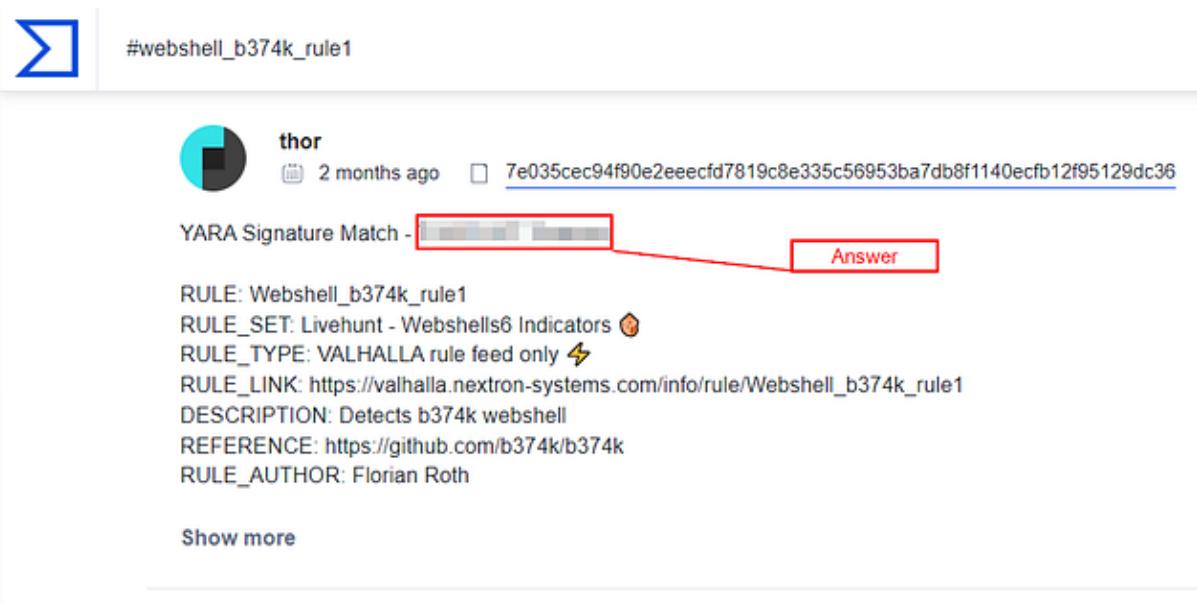
En revenant à Valhalla, de retour dans la rangée dont nous avons obtenu la réponse à la question précédente, déplacez-vous vers la droite vers les cases bleues. Celui du milieu avec la petite icône de virus vous amène à VirusTotal, cliquez dessus.



Keyword: 53fe44b4753874f079a936325d1fdc9b1691956a29c3aaf8643cdbd49f5984bf (Results: 4) ←

Query	Keyword, Tag, ATT&CK Technique or Rule Name	Search					
Type	Rule Name	Description	Date	Reference	Ref	VT	Info
YARA	WebshellRepo_convert	Detects Webshell - file convert.php	2016-12-09	Webshell Repos			
YARA	Operation_Emil_Webshell_pluginsphp	Detects an Operation Emil Webshell - file plugins.php	2016-07-29	Operation Emil			
YARA	[REDACTED]	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			
YARA	Webshell_b374k_rule2	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			

Lorsque la page se charge, la première ligne indique YARA Signature Match, suivi du nom du scanner et de la réponse à cette question. Une fois que vous l'avez trouvé, mettez en surbrillance copier (ctrl + c) et collez (ctrl + v) ou tapez la réponse dans le champ TryHackMe Answer et cliquez sur Soumettre.



#webshell_b374k_rule1

thor 2 months ago 7e035cec94f90e2eeecfd7819c8e335c56953ba7db8f1140ecfb12f95129dc36

YARA Signature Match - [REDACTED] Answer

RULE: Webshell_b374k_rule1
 RULE_SET: Livehunt - Webshells6 Indicators
 RULE_TYPE: VALHALLA rule feed only
 RULE_LINK: https://valhalla.nextron-systems.com/info/rule/Webshell_b374k_rule1
 DESCRIPTION: Detects b374k webshell
 REFERENCE: <https://github.com/b374k/b374k>
 RULE_AUTHOR: Florian Roth

Show more

Réponse : Scanner THOR APT

Entrez le hachage SHA256 du fichier 2 dans Virus Total. Est-ce que chaque antivirus a détecté cela comme malveillant ? (Ouais/Non)

Pour en revenir à VirusTotal, avant de pouvoir insérer le hachage file2 SHA256, vous devrez cependant supprimer l'entrée de recherche précédente. Cela peut facilement être fait en mettant en surbrillance et en appuyant sur Supprimer ou en cliquant à l'extrême droite de la recherche de requête et en maintenant l'espace arrière. jusqu'à ce qu'il soit parti.

#webshell_b374k_rule1

thor · 2 months ago · 7e035cec94f90e2eeecfd7819c8e335c56953ba7db8f1140ecfb12f95129dc36

YARA Signature Match - [REDACTED]

RULE: Webshell_b374k_rule1
RULE_SET: Livehunt - Webshells6 Indicators 🛡
RULE_TYPE: VALHALLA rule feed only ⚡
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/Webshell_b374k_rule1
DESCRIPTION: Detects b374k webshell
REFERENCE: <https://github.com/b374k/b374k>
RULE_AUTHOR: Florian Roth

Show more

Une fois cela fait, copiez le hachage SHA256 ci-dessus (ctrl + c) et collez-le (ctrl + v) dans la barre de recherche VirusTotal en haut de la page, appuyez sur Entrée pour le rechercher.

53fe44b4753874f079a936325d1fdc9b1691956a29c3aa8643cdbd49f5984bf

À première vue, il semble qu'il ait été détecté par tous les fournisseurs audiovisuels, mais faites défiler vers le bas pour vous en assurer. Une fois que vous avez compris, tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

34 / 62

34 security vendors and no sandboxes flagged this file as malicious

53fe44b4753874f079a936325d1fdc9b1691956a29c3aa8643cdbd49f5984bf
index.php
php

Community Score: ✓

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY ⓘ

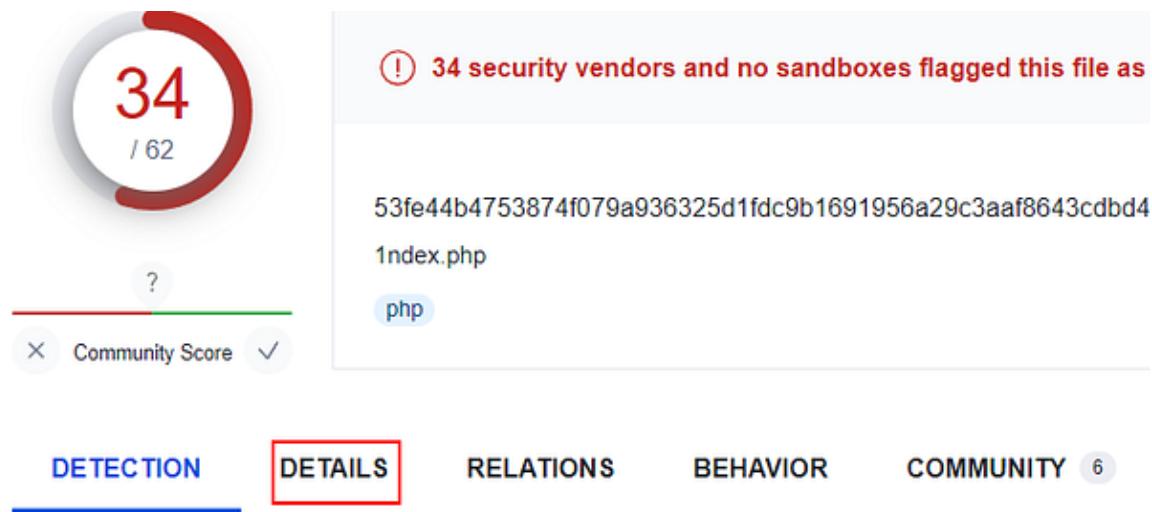
Security Vendors' Analysis ⓘ

Ad-Aware	Backdoor PHP:Webshell.EB	AhnLab-V3	WebShell/PHP.Agent.SC182864
AI.Yac	Backdoor PHP:Webshell.EB	Arcabit	Backdoor PHP:Webshell.EB
Avast	PHP.BackDoor:EP [T!]	AVG	PHP.BackDoor:EP [T!]
Baidu	PHP.Backdoor.PhPShell.b	BitDefender	Backdoor PHP:Webshell.EB
ClamAV	Txt Backdoor Webshell.9891631.0	Comodo	Malware@{tgtoInteb}
Cynet	PHPWebShell.BV	DrWeb	PHP.BackDoor.110
Emsisoft	Backdoor PHP:Webshell.EB (B)	eScan	Backdoor PHP:Webshell.EB
ESET-NOD32	PHP:Webshell.NKV	Fortinet	PHP/CoinMiner.EDR

Réponse : Non

Outre .PHP, quelle autre extension est enregistrée pour ce fichier ?

De retour sur le site VirusTotal, cliquez sur l'onglet DÉTAILS, cela ouvrira l'onglet où se trouvait justement les DÉTECTIONS.



Maintenant que l'onglet DÉTAILS est ouvert, nous devons faire défiler jusqu'à la section Nom. Alors commencez à faire défiler, ce n'est pas loin et c'est la dernière section.

34 / 62

?

X Community Score ✓

DETENTION DETAILS RELATIONS BEHAVIOR COMMUNITY 6

Basic Properties ⓘ

MD5	c6a7ebafdbe239d65248e2b69b670157
SHA-1	3926ab64dcf04e87024011cf39902beac32711da
SHA-256	53fe44b4753874f079a936325d1fd9b1691956a29c3aa8643cdbd49f5984bf
SSDEEP	6144:xihiD/gB0xNissAzm4mZEf+yNTU23vktfwMi7+rlHTg5TZ16uh15YOYs1E1tQL5j:xK/qOzissAzm4mSRB7+zCYOYs1EDwGdA
TLSH	T19A245C90F75E763201F720B6827F26CAB4BE447168084C60FC6C25F859E896D75EBE6C
File type	PHP
Magic	PHP script text
TrID	PHP source (62.5%) HyperText Markup Language (37.5%)
File size	218.73 KB (223978 bytes)

History ⓘ

First Seen In The Wild	2021-10-28 17:07:49 UTC
First Submission	2015-09-17 16:09:41 UTC
Last Submission	2022-12-03 07:21:00 UTC

218. Size

Ok, maintenant que nous sommes ici, il ne nous montre pas tous les noms, cliquez sur la carotte vers le bas pour exposer le reste.

Names 

1ndex.php
b374k-3.2.3.php
3.php
partmgr.sys
f4b3569f68cf9ef1013bc6dc7418077d.txt
c6a7ebafdbe239d65248e2b69b670157.php
file_577.php5
fc9b6386-15bd-11ea-af9f-94f6d6244eb4.php
3926ab64dcf04e87024011cf39902beac32711da.php
001078.php



En regardant la liste complète des noms avec les extensions de fichiers, la plupart d'entre eux sont php. Mais nous avons quelques outliers, l'une des différentes extensions ne correspond pas au type de réponse demandé par TryHackMe, elle ne peut contenir que trois lettres. Cela ne nous laisse donc que trois choix. Une fois que vous avez compris, tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

Names ⓘ

1index.php
b374k-3.2.3.php
3.php
partmgr.sys
f4b3569f68cf9ef1013bc6dc7418077d.txt
c6a7ebafdbbe239d65248e2b69b670157.php
file_577.php5
fc9b6386-15bd-11ea-af9f-94f6d6244eb4.php
3926ab64dcf04e87024011cf39902beac32711da.php
001078.php
b374k-3_621.php
ewq1.html
C6A7EBAFDBE239D65248E2B69B670157 [redacted]

^

Réponse : exe

Quelle bibliothèque JavaScript est utilisée par le fichier 2 ?
Nous en avons terminé avec VirusTotal, alors revenez aux résultats de recherche Valhalla pour file2. Cette fois, cliquez sur l'icône du maillon de chaîne, cela vous amènera au github, qui nous donnera de nombreuses informations.

The screenshot shows the Valhalla web application interface. At the top, there is a logo with the word "VALHALLA" and the tagline "SUPERCHARGE YOUR DETECTION". Below the logo is a search bar with the placeholder "Keyword, Tag, ATT&CK Technique or Rule Name". To the right of the search bar is a "Search" button. The main area displays a table of search results:

Type	Rule Name	Description	Date	Reference	Ref	VT	Info
YARA	WebshellRepo_convert	Detects Webshell - file convert.php	2016-12-09	Webshell Repos			
YARA	Operation_Emil_Webshell_pluginsphp	Detects an Operation Emil Webshell - file plugins.php	2016-07-29	Operation Emil			
YARA	[REDACTED]	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			
YARA	Webshell_b374k_rule2	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			

Une fois la page chargée, nous allons utiliser la fonction de recherche du navigateur. Appuyez sur ctrl + f pour ouvrir la barre de recherche.

The screenshot shows a GitHub repository page for the user "b374k" with the repository name "b374k". The page includes a navigation bar with links for Product, Solutions, Open Source, Pricing, Search, Sign in, and Sign up. Below the navigation bar, there are links for Code, Issues (15), Pull requests (3), Actions, Projects, Wiki, Security, and Insights. The main content area shows the repository's code structure and commit history. A red arrow points to the search bar at the top left of the page.

Puisqu'il s'agit d'une bibliothèque Javascript que nous recherchons, le fichier se termine probablement par .js, alors tapez .js dans la barre de recherche. Nous obtenons trois résultats possibles, parcourez-les, les deux seconds devraient être ce que vous recherchez. Une fois que vous l'avez trouvé, mettez en surbrillance copier (ctrl + c) et collez (ctrl + v) ou tapez la réponse dans le champ TryHackMe Answer et cliquez sur Soumettre.

README.md

- SQL Explorer
- Process list/Task manager
- Send mail with attachment (you can attach local file on server)
- String conversion
- All of that only in 1 file, no installation needed
- Support PHP > 4.3.3 and PHP 5

Requirements :

- PHP version > 4.3.3 and PHP 5
- As it using v1.1.2, you need modern browser to use b374k shell. See browser support on website <http://zeptojs.com/>
- Responsibility of what you do with this shell

Answer

Réponse : Zepto

Cette règle Yara est-elle dans le fichier Yara par défaut que Loki utilise pour détecter ce type d'outils de piratage ? (Ouais/Non)

Pour la dernière fois, retournez sur le site du Valhalla. Mettez en surbrillance et copiez (ctrl + c) le nom de la règle que nous avons examiné.

Keyword: 53fe44b4753874f079a936325d1fdc9b1691956a29c3aaef8643cdbd49f5984bf (Results: 4)

Type	Rule Name	Description	Date	Reference	Ref	VT	Info
YARA	WebshellRepo_convert	Detects Webshell - file convert.php	2016-12-09	Webshell Repos			
YARA	Operation_Emil_Webshell_pluginsphp	Detects an Operation Emil Webshell - file plugins.php	2016-07-29	Operation Emil			
YARA	Webshell_b374k_rule1	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			
YARA	Webshell_b374k_rule2	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			

De retour au terminal, voyons si nous pouvons trouver cette règle Yara dans notre répertoire Loki. Nous pouvons le faire avec `ls /home/cmnatic/tools/Loki/signature-base/yara/ | grep "Webshell_b374k_rule1"`

```
cmnatic@thm-yara:~$ ls /home/cmnatic/tools/Loki/signature-base/yara/ | grep "Webshell_b374k_rule1"
```

Rien ne revient, donc cela devrait vous donner la réponse. Une fois que vous avez compris, tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

```
cmmatic@thm-yara:~$ ls /home/cmmatic/tools/Loki/signature-base/yara/ | grep "Webshell_b374k_rule1"  
cmmatic@thm-yara:~$
```

Réponse : Non

Tâche 11 Conclusion

Dans cette salle, nous avons exploré Yara, comment utiliser Yara et créé manuellement les règles de base de Yara. Nous avons également exploré divers outils open source pour démarrer, qui utilisent les règles Yara pour détecter les éléments malveillants sur les points finaux.

En parcourant le scénario de la salle, vous devez comprendre la nécessité (en tant que blue teamer) de savoir comment créer efficacement des règles Yara si l'on s'appuie sur de tels outils. Les produits commerciaux, même s'ils ne sont pas parfaits, auront un ensemble de règles Yara beaucoup plus riche qu'un produit open source. Les versions commerciales et open source vous permettront d'ajouter des règles Yara pour étendre davantage ses capacités de détection des menaces.

Si ce n'est pas clair, la raison pour laquelle le fichier 2 n'a pas été détecté est que la règle Yara n'était pas dans le fichier Yara utilisé par Loki pour détecter l'outil de piratage (shell Web), même si cet outil de piratage existe depuis des années et a même été attribué à au moins un État-nation. La règle Yara est présente dans la variante commerciale de Loki, qui est Thor.

Il y a bien plus à faire avec Yara et les règles de Yara. Nous vous encourageons à explorer davantage cet outil à votre guise.

🎉🎉🎉 Félicitations !! Vous avez terminé la salle Yara !!!! 🎉🎉🎉

OPENCTI

TryHackMe OpenCTI - Tâche 1 à Tâche 5



[Poisson-coupe](#)

[Suivre](#)

13 minutes de lecture

5

Fournir une compréhension du projet OpenCTI

Aperçu de la salle de la tâche 1

Cette salle couvrira les concepts et l'utilisation d'OpenCTI, une plateforme open source de renseignement sur les menaces. La salle vous aidera à comprendre et à répondre aux questions suivantes :

- Qu'est-ce qu'OpenCTI et comment est-il utilisé ?
- Comment naviguer sur la plateforme ?
- Quelles fonctionnalités seront importantes lors d'une analyse des menaces de sécurité ?

Avant de parcourir cette salle, nous vous recommandons de consulter ces salles comme prérequis :

- [Cadre MITRE ATT&CK](#)
- [La ruche](#)
- [DMU](#)
- [Outils de renseignement sur les menaces](#)



Tâche 2 Introduction à OpenCTI

Les renseignements sur les cybermenaces sont généralement un mystère de gestion à gérer, les organisations se débattant pour savoir comment saisir, digérer, analyser et présenter les données sur les menaces d'une manière logique. D'après les salles liées dans l'aperçu, il est clair qu'il existe de nombreuses plates-formes qui ont été développées pour lutter contre le poids lourd qu'est la Threat Intelligence.

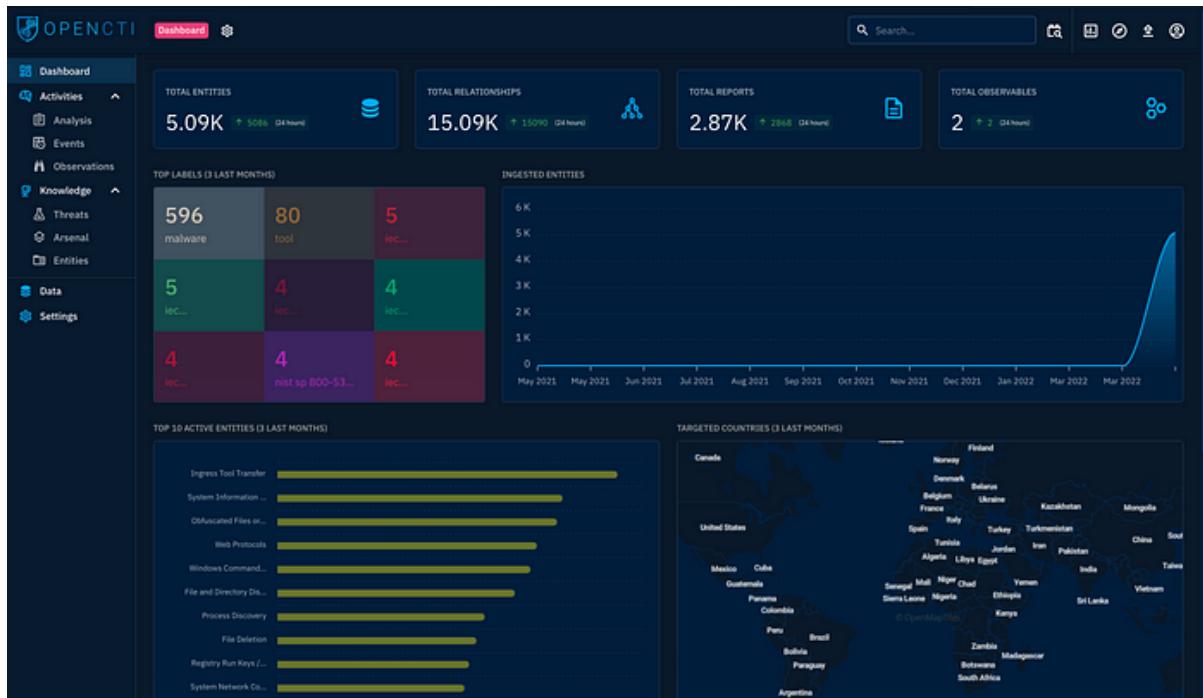
OuvrirCTI

[OpenCTI](#) est une autre plate-forme open source conçue pour fournir aux organisations les moyens de gérer le CTI grâce au stockage, à l'analyse, à la visualisation et à la présentation des campagnes de menaces, des logiciels malveillants et des IOC.

Objectif

Développée en collaboration avec l'[Agence nationale de cybersécurité \(ANSSI\)](#), l'objectif principal de la plateforme est de créer un outil complet permettant aux utilisateurs de

capitaliser sur des informations techniques et non techniques tout en développant les relations entre chaque information et sa source primaire. La plateforme peut utiliser le [framework MITRE ATT&CK](#) pour structurer les données. De plus, il peut être intégré à d'autres outils de renseignement sur les menaces tels que MISP et TheHive. Les pièces vers ces outils ont été liées dans l'aperçu.

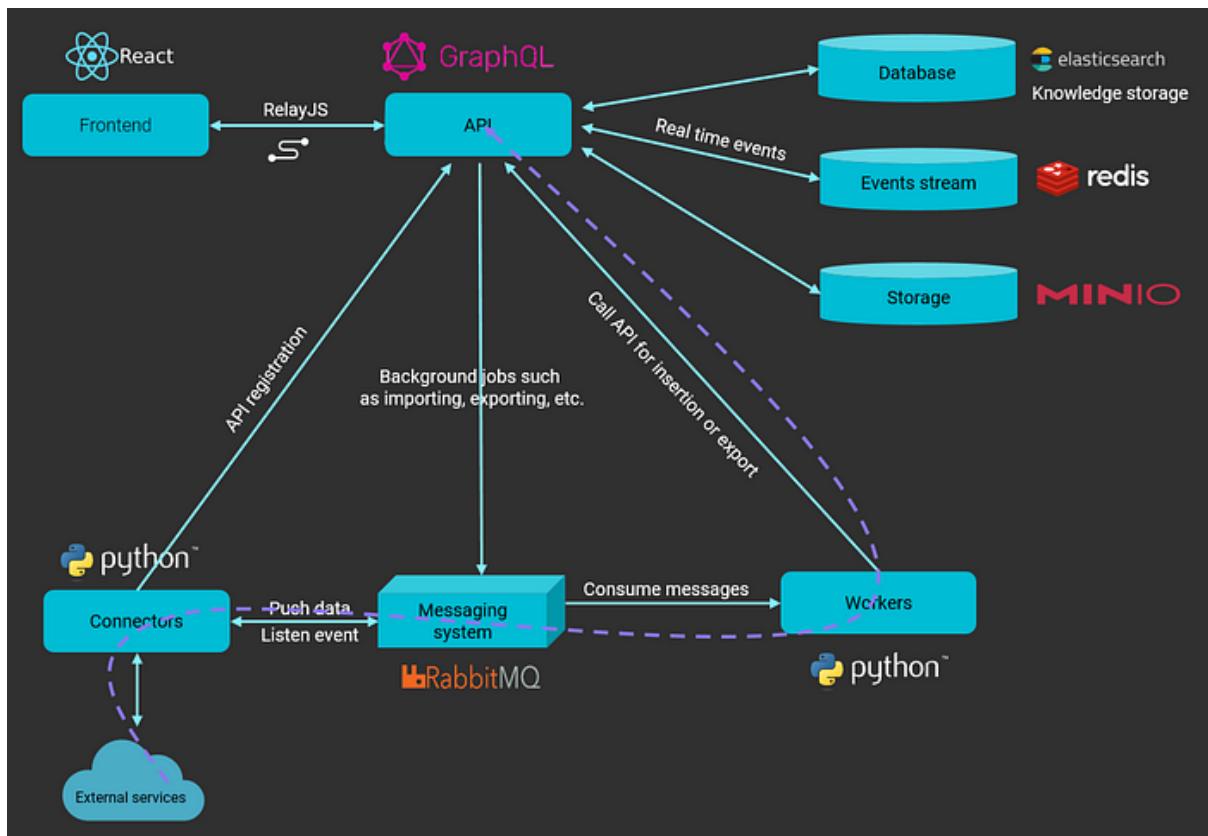


Tâche 3 Modèle de données OpenCTI

Modèle de données OpenCTI

OpenCTI utilise une variété de schémas de connaissances pour structurer les données, le principal étant les normes Structured Threat Information Expression ([STIX2](#)). STIX est un format de langage sérialisé et standardisé utilisé dans l'échange de renseignements sur les menaces. Il permet de mettre en œuvre les données en tant qu'entités et relations, retracant efficacement l'origine des informations fournies.

Ce modèle de données est pris en charge par la façon dont l'architecture de la plateforme a été conçue. L'image ci-dessous donne une structure architecturale à votre savoir-faire.



Source : [Base de connaissances publique OpenCTI](#)

Les services phares comprennent :

- API GraphQL : L'API connecte les clients à la base de données et au système de messagerie.
- Write Workers : processus Python utilisés pour écrire des requêtes de manière asynchrone à partir du système de messagerie RabbitMQ.
- Connecteurs : un autre ensemble de processus Python utilisés pour ingérer, enrichir ou exporter des données sur la plateforme. Ces connecteurs fournissent à l'application un réseau robuste de systèmes et de cadres intégrés pour créer des relations de renseignement sur les menaces et permettre aux utilisateurs d'améliorer leurs tactiques de défense.

Selon OpenCTI, les connecteurs appartiennent aux classes suivantes :

Class	Description	Examples
External Input Connector	Ingests information from external sources	CVE, MISP, TheHive, MITRE
Stream Connector	Consumes platform data stream	History, Tanium
Internal Enrichment Connector	Takes in new OpenCTI entities from user requests	Observables enrichment
Internal Import File Connector	Extracts information from uploaded reports	PDFs, STIX2 Import
Internal Export File Connector	Exports information from OpenCTI into different file formats	CSV, STIX2 export, PDF

Reportez-vous à la documentation [des connecteurs](#) et [du modèle de données](#) pour plus de détails sur la configuration des connecteurs et du schéma de données.

Tâche 4 Tableau de bord OpenCTI 1

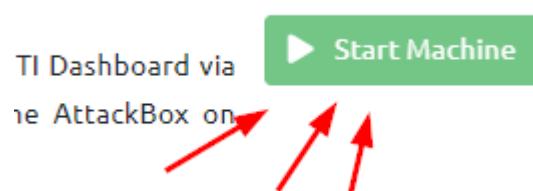
Suivez la tâche en lançant la machine connectée et en utilisant les informations d'identification fournies ; connectez-vous au tableau de bord OpenCTI via AttackBox sur http://MACHINE_IP:8080/. Donnez à la machine 5 minutes pour démarrer et il est conseillé d'utiliser l'AttackBox en plein écran.

Nom d'utilisateur : info@tryhack.io

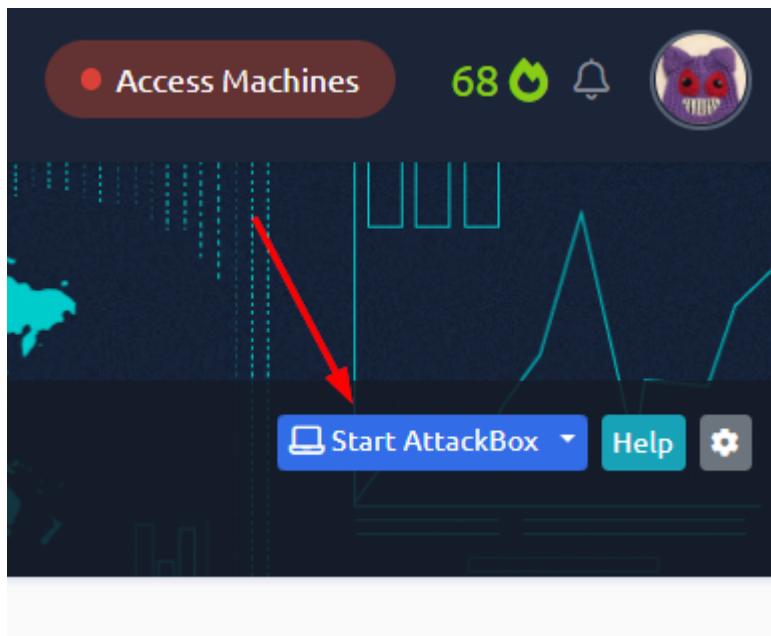
Mot de passe : TryHackMe1234

Démarrer OpenCTI

Donc, avant d'aller plus loin, passons au tableau de bord OpenCTI. Pour ce faire, nous devons d'abord cliquer sur le bouton vert Démarrer la machine en haut de la tâche, pour que la VM soit opérationnelle.



Ensuite, allez en haut de la page Web et cliquez sur l'icône bleue Démarrer AttackBox, l'écran se divisera et prendra environ une minute et demie pour que la VM se charge.



Au bas de la VM se trouvent deux flèches pointant dans les directions opposées, c'est l'icône plein écran. Cliquez dessus.



Un nouvel onglet s'ouvrira avec la VM dedans, pendant le chargement, retournez à l'onglet TryHackMe. Revenez à la barre en bas de la VM et cliquez sur le bouton — pour quitter l'écran partagé.



Il y a un terminal sur l'écran, si vous l'avez lu, appuyez sur Entrée pour le fermer.

```
Terminal
File Edit View Search Terminal Help
01

This machine can access other machines you deploy on TryHackMe.

Please keep in mind the following:
1. Pentesting any target that is not deployed by you on TryHackMe is prohibited.
2. You are solely responsible for your actions.
3. This machine expires. Check TryHackMe to ensure you still have time left.
4. Once this machine is terminated, all data will be lost.

View the changes made to the AttackBox: https://help.tryhackme.com/106142-my-machine/tryhackme-attack-machine#changelog

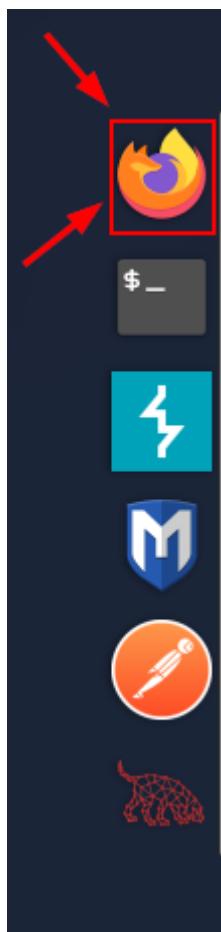
Usage Instructions:

1. Tools are located in /root/Desktop/Tools & /opt/
2. Webshells are located in /usr/share/webshells
3. Wordlists are located in /usr/share/wordlists
4. To use Empire & Starkiller, read the following file: /root/Instructions/empire-starkiller.txt

Do you think something's missing? Let us know! support@tryhackme.com

Press ENTER key to close.
```

Sur le côté droit de la VM se trouve un panneau rapide, en haut de ce panneau se trouve Firefox. Cliquez sur l'icône Firefox.



Pendant le chargement de Firefox, revenez à la tâche TryHackMe. Dans le premier paragraphe, vous verrez un lien qui vous mènera à la page de connexion OpenCTI. Mettez en surbrillance et copiez (ctrl + c) le lien.

Follow along with the task by launching the attack

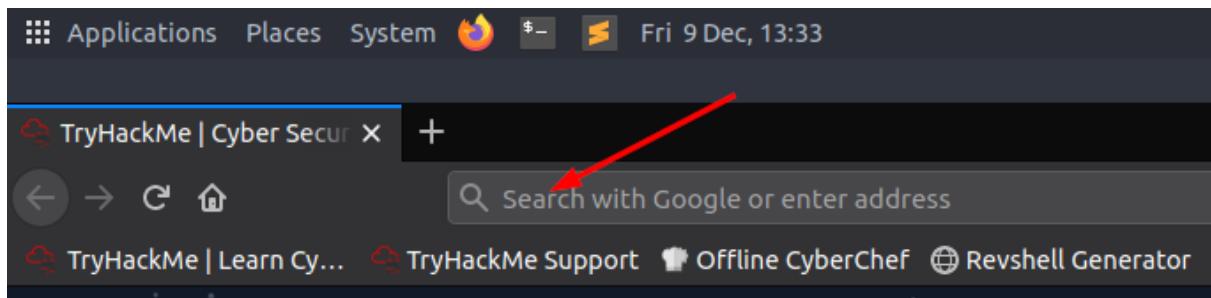
the AttackBox on <http://10.10.246.188:8080/>.

Fullscreen.

Username: `info@tryhack.io`

Password: `TryHackMe1234`

Revenez à l'onglet VM, cliquez sur la barre d'URL. Collez (ctrl + v) l'adresse OpenCTI dans la barre et appuyez sur Entrée.



Le site chargera la page de connexion pour OpenCTI. Les informations de connexion sont de retour sur la tâche TryHackMe, vous pouvez soit mettre en surbrillance copier (ctrl + c) et coller (ctrl + v), soit saisir les informations d'identification dans la page de connexion. Cliquez ensuite sur le bouton bleu Se connecter.

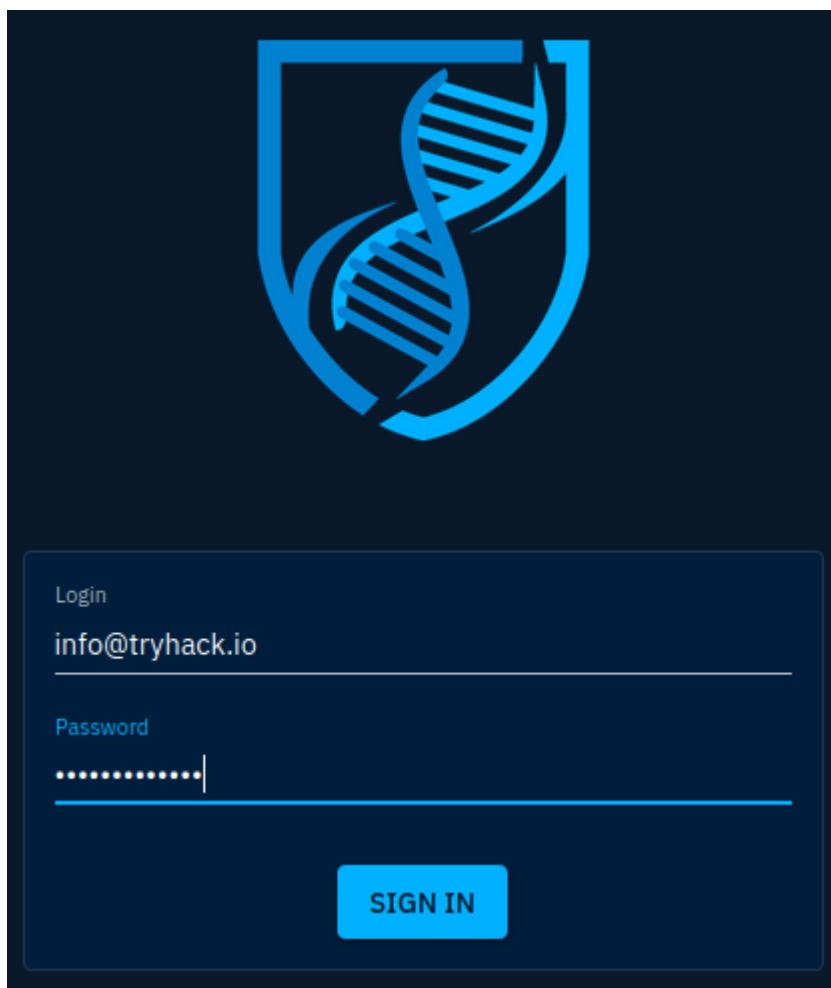
Follow along with the task by launching the attack

the AttackBox on <http://10.10.246.188:8080/>.

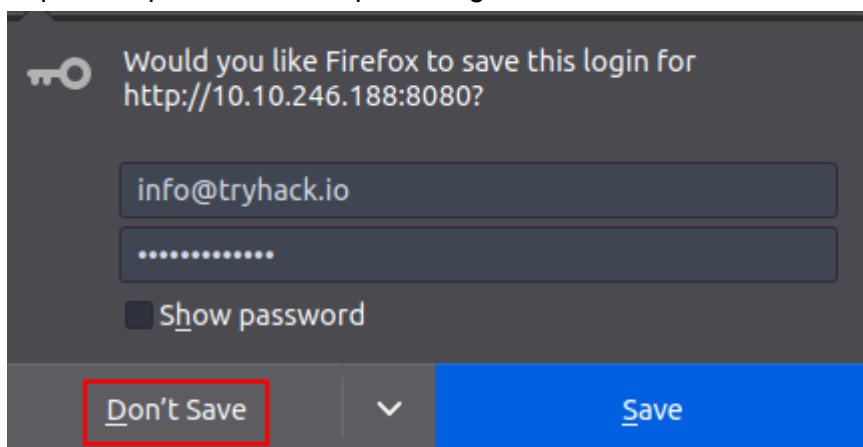
Fullscreen.

Username: `info@tryhack.io`

Password: `TryHackMe1234`



Vous aurez une petite fenêtre contextuelle pour enregistrer votre mot de passe dans Firefox, cliquez simplement sur Ne pas enregistrer.



Vous êtes maintenant dans le tableau de bord OpenCTI et prêt à continuer !!!

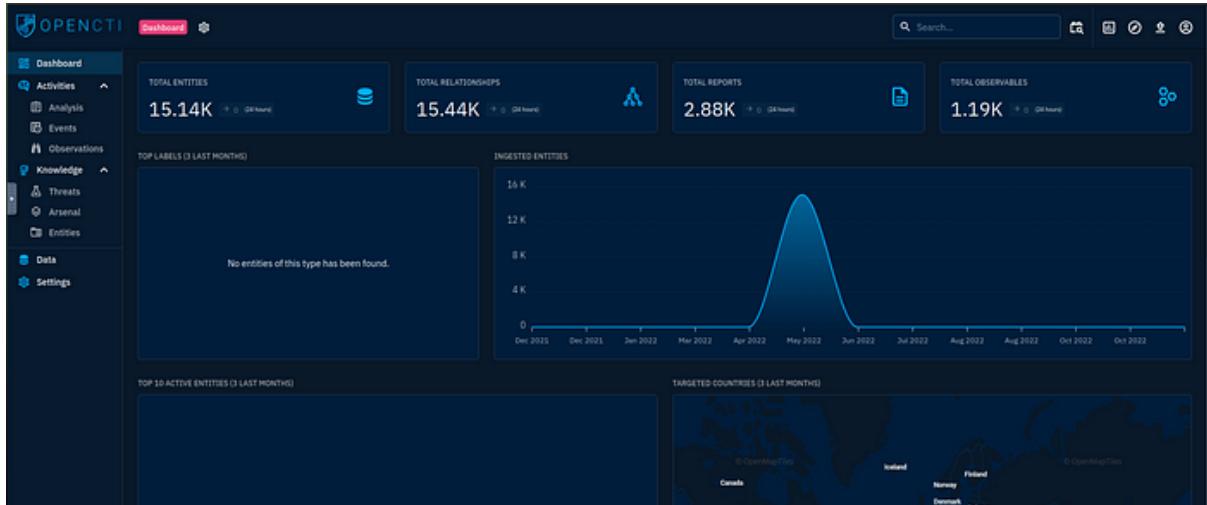
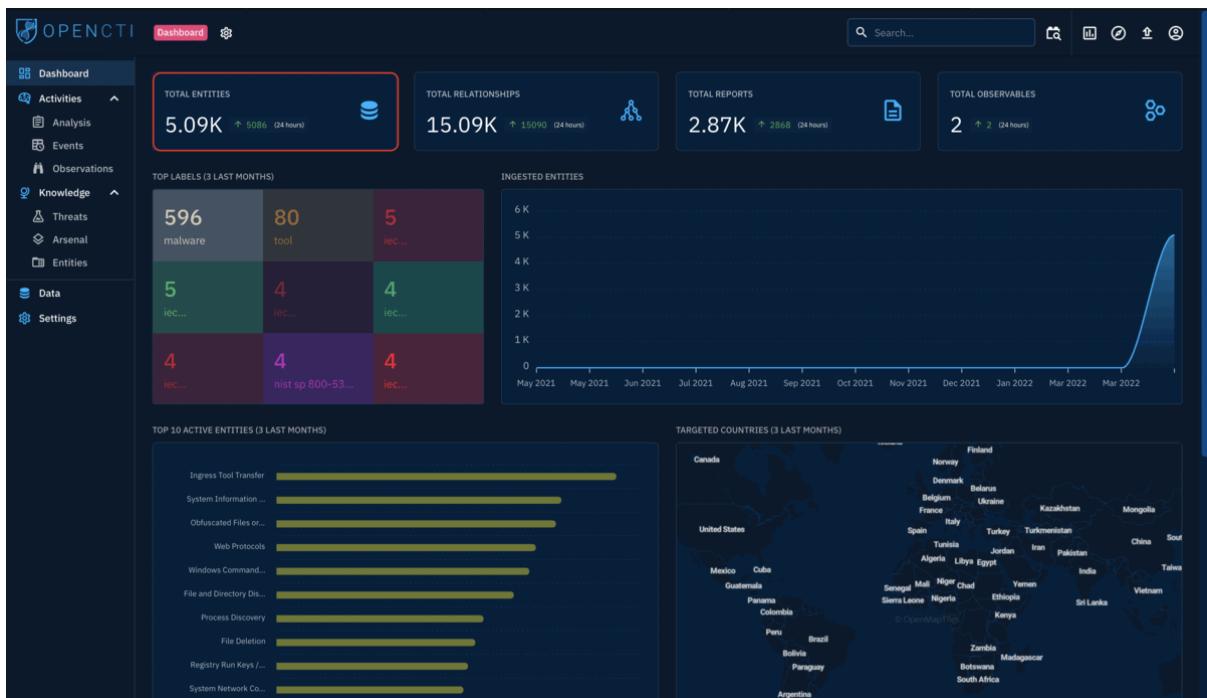


Tableau de bord OpenCTI

Une fois connecté à la plateforme, le tableau de bord d'ouverture présente divers widgets visuels résumant les données sur les menaces ingérées dans OpenCTI. Les widgets du tableau de bord présentent l'état actuel des entités ingérées sur la plateforme via le nombre total d'entités, de relations, de rapports et d'observables ingérés, ainsi que les modifications apportées à ces propriétés notées dans les 24 heures.

Voir image.



Activités et connaissances

L'OpenCTI catégorise et présente les entités sous les groupes Activités et Connaissances sur le panneau de gauche. La section activités couvre les incidents de sécurité ingérés sur la plateforme sous forme de rapports. Cela permet aux analystes d'enquêter facilement sur ces incidents. En revanche, la section Connaissances fournit des données liées relatives aux outils utilisés par les adversaires, aux victimes ciblées et au type d'acteurs de menace et de campagnes utilisés.

Analyse

L'onglet Analyse contient les entités d'entrée dans les rapports analysés et les références externes associées. Les rapports sont au cœur d'OpenCTI, car les connaissances sur les menaces et les événements sont extraites et traitées. Ils permettent aux analystes d'identifier plus facilement la source de l'information. De plus, les analystes peuvent ajouter leurs notes d'enquête et d'autres ressources externes pour enrichir leurs connaissances. Comme indiqué ci-dessous, nous pouvons consulter le rapport Triton Software publié par MITRE ATT&CK et observer ou ajouter des détails fournis.

Voir image.

The screenshot shows the OpenCTI web interface. The left sidebar has 'Analysis' selected. The main area is a table titled 'Report type' with columns: TITLE, AUTHOR, LABELS, DATE, STATUS, and MARKING. There are 2.87K entity(s) listed. One specific entry, '[MITRE ATT&CK] Triton (S1009)', is highlighted with a red circle. The table includes other entries like 'rpt_APT37.pdf', 'threats-swedish-financial-sector.pdf', and various MITRE ATT&CK techniques.

Événements

Les analystes de sécurité enquêtent et recherchent les événements impliquant des activités suspectes et malveillantes sur l'ensemble de leur réseau organisationnel. Dans l'onglet Événements, les analystes peuvent enregistrer leurs conclusions et enrichir leurs informations sur les menaces en créant des associations pour leurs incidents.

Voir image.

The screenshot shows the OpenCTI web interface with 'Events' selected in the sidebar. The main area is a table with columns: NAME, LABELS, CREATION DATE, MODIFICATION DATE, STATUS, and MARKING. It shows one entity, 'Incident 1', with a creation date of Apr 20, 2022, and a modification date of Apr 20, 2022. The status is 'NEW'. A red circle highlights the 'Events' tab in the sidebar.

Observations

Sous cet onglet sont répertoriés les éléments techniques, les règles de détection et les artefacts identifiés lors d'une cyberattaque : un ou plusieurs indicateurs de composition identifiables. Ces éléments aident les analystes à cartographier les événements de menace au cours d'une chasse et à établir des corrélations entre ce qu'ils observent dans leur environnement et les flux d'informations.

Voir image.

Type	Value	Labels	Creation Date	Marking
Artifact	b8973bf33b31eb324e4b29d7a7e1e64455216ed8db28519c8ecad...	[...], [suspicious], [malware-bazaar]	May 13, 2022, 2:14:18 PM	
Artifact	76209c7f60db832e93b0d5e68bc2ba9f14d2094f7db636e8a19...	[...], [malware-bazaar]	May 13, 2022, 1:49:10 PM	
Artifact	65b329e466d4e90c976d4d2772a531547e9b9e7b3a6c344c42...	[...], [malware-bazaar]	May 13, 2022, 0:31:15 PM	
Artifact	0285e1d1301d0cc6dcf076c3a5897010a2c52724016c246a52d...	[...], [exe], [malware-bazaar]	May 13, 2022, 12:45:58 PM	
Artifact	9c8fc845a781f3b2936d30b729d1a090314ee34b23000cb70...	[...], [malware-bazaar]	May 13, 2022, 12:45:52 PM	
Artifact	42a2782ef5284d7a9b8d295c3d18cc548963ebc6e2d25fb2...	[...], [malware-bazaar]	May 13, 2022, 12:45:48 PM	
Artifact	300b12de8752d830459a0beb61c40ad1a946cb6e641128ac0...	[...], [kotak], [malware-bazaar]	May 13, 2022, 12:45:46 PM	
Artifact	f40aa2e60fc4311fd6c52c908b57505b6a681b651fb75e43f2...	[...], [kotak], [malware-bazaar]	May 13, 2022, 12:45:44 PM	
Artifact	5700788088c1da1c95992ab7f716a9301329fb1a933c6d238ed0...	[...], [kotak], [malware-bazaar]	May 13, 2022, 12:45:42 PM	
Artifact	bdb195ea6dd8e3908fe3bab6857cb06b70798dd109f25be834...	[...], [malware-bazaar]	May 13, 2022, 12:40:36 PM	
Artifact	4021a1093486ed57ed531ff7d71685cf4bbaafb551ab02c...	[...], [malware-bazaar]	May 13, 2022, 12:40:34 PM	
Artifact	64ffe9d393bdc03979ba6f3f4305935050516a7b7928c5e43e2...	[...], [malware-bazaar]	May 13, 2022, 12:40:33 PM	
Artifact	e6d2261c5ab8d44520a7c08a20a2a272bea8404268d020bbe3...	[...], [malware-bazaar]	May 13, 2022, 12:40:22 PM	
Artifact	3795060c90b143559c968c8f7279365185930cad97d6ed77fb...	[...], [malware-bazaar]	May 13, 2022, 12:40:30 PM	
Artifact	063bde18392cecc632c7d6c4998592e1ebd4503ba7630b2e...	[...], [malware-bazaar]	May 13, 2022, 12:40:29 PM	
Artifact	6513b521a9cc189a19373141fc5f0b2f6a4fa045cc083dee8c403...	[...], [malware-bazaar]	May 13, 2022, 12:40:28 PM	
Artifact	161c471b0aaaf0d7c1f0267ebbb37e10f8c5ede09b000bf2472...	[...], [hidden], [malware-bazaar]	May 13, 2022, 12:40:26 PM	
Artifact	74b8483e001e913e77fb491c12feed9a8062c52a067b3e06a32...	[...], [exe], [malware-bazaar]	May 13, 2022, 12:40:24 PM	

Des menaces

Toutes les informations classées comme menaçantes pour une organisation ou une information seraient classées sous menace. Ceux-ci comprendront :

- Acteurs de menace : individu ou groupe d'attaquants cherchant à propager des actions malveillantes contre une cible.
- Ensembles d'intrusions : ensemble de TTP, d'outils, de logiciels malveillants et d'infrastructures utilisés par un acteur malveillant contre des cibles partageant certains attributs. Les APT et les groupes menaçants sont répertoriés dans cette catégorie sur la plateforme en raison de leur schéma d'action connu.
- Campagnes : série d'attaques se déroulant au cours d'une période donnée et contre des victimes spécifiques, initiées par des acteurs de menaces persistantes avancées qui emploient divers TTP. Les campagnes ont généralement des objectifs précis et sont orchestrées par des acteurs menaçants issus d'un État-nation, d'un syndicat du crime ou d'une autre organisation peu recommandable.

Voir image.

Arsenal

Cet onglet répertorie tous les éléments liés à une attaque et tous les outils légitimes identifiés auprès des entités.

- Logiciels malveillants : les logiciels malveillants et les chevaux de Troie connus et actifs sont répertoriés avec des détails sur leur identification et leur cartographie en fonction des connaissances ingérées dans la plate-forme. Dans notre exemple, nous analysons le malware 4H RAT et nous pouvons extraire des informations et des associations faites sur le malware.
- Modèles d'attaque : les adversaires mettent en œuvre et utilisent différents TTP pour cibler, compromettre et atteindre leurs objectifs. Ici, nous pouvons examiner les détails de l'interface de ligne de commande et prendre des décisions basées sur les relations établies sur la plateforme et naviguer dans une enquête associée à la technique.
- Plans d'action : MITRE décrit les concepts et les technologies qui peuvent être utilisés pour empêcher l'utilisation réussie d'une technique d'attaque. Ceux-ci sont représentés sous forme de plans d'action (CoA) contre les TTP.
- Outils : répertorie tous les outils et services légitimes développés pour la maintenance, la surveillance et la gestion du réseau. Les adversaires peuvent également utiliser ces outils pour atteindre leurs objectifs. Par exemple, pour le modèle d'attaque de l'interface de ligne de commande, il est possible de préciser que CMD serait utilisé comme outil d'exécution. En tant qu'analyste, on peut enquêter sur les rapports et les instances associés à l'utilisation de l'outil.
- Vulnérabilités : les bogues logiciels connus, les faiblesses du système et les expositions sont répertoriés pour enrichir ce que les attaquants peuvent utiliser pour exploiter et accéder aux systèmes. La liste des vulnérabilités et expositions communes (CVE) maintenue par MITRE est utilisée et importée via un connecteur.

Voir image.

10.10.41.94:8080/dashboard/personal/malwares/feed73aa-adbb-4914-adc7-480d926aa200

Entités

Cet onglet catégorise toutes les entités en fonction des secteurs opérationnels, des pays, des organisations et des individus. Ces informations permettent d'enrichir les connaissances sur les attaques, les organisations ou les ensembles d'intrusions.

Voir image.

10.10.41.94:8080/dashboard/entities/sectors/870dc659-0fa8-4720-8602-098b13d6eac0

Répondre aux questions ci-dessous

Quel est le nom du groupe qui utilise le malware 4H RAT ?

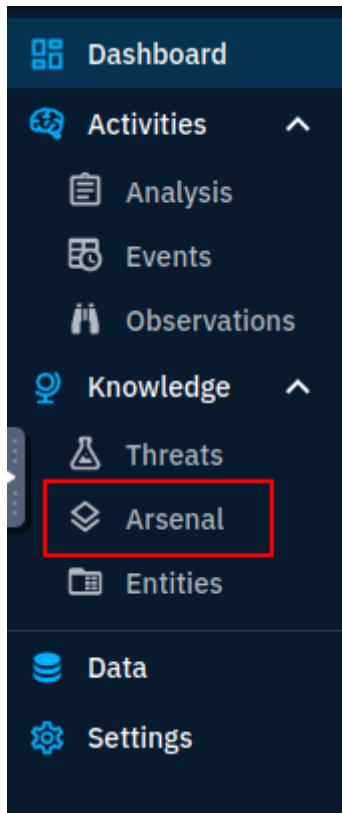
Nous avons donc appris de la section Arsenal ci-dessus que nous pouvons nous renseigner sur les logiciels malveillants dans l'onglet Arsenal. Alors rendez-vous sur le tableau de bord OpenCTI.

Arsenal

This tab lists all items related to an attack and any legitimate tools identified from the entities.

- **Malware:** Known and active malware and trojan are listed with details of their identification and mapping based on the knowledge ingested into the platform. In our example, we analyse the 4H RAT malware and we can extract information and associations made about the malware.

Une fois sur le tableau de bord OpenCTI, regardez le panneau de gauche. Vous verrez Arsenal en gris près du bas, cliquez dessus. Cela ouvrira la section Malware dans la partie principale de la fenêtre à droite.



Vous pouvez utiliser la barre de recherche pour rechercher le malware 4H RAT, mais comme il est classé par ordre alphabétique, vous pouvez le trouver tout en haut. Cliquez sur la case 4H RAT.

A screenshot of the OpenCTI main interface. The left sidebar shows the navigation menu with 'Arsenal' selected. The main area displays a grid of cards representing different entities. One card for '4H RAT' is highlighted with a red box. The card contains the following information:

4H RAT Updated the May 24, 2022

4H RAT is malware that has been used by Putter Panda since at least 2007. (Citation: CrowdStrike Putter...

malware

Other visible cards include: 3PARA RAT, ABK, ACAD/Medro.A, adupd, Adups, ADVSTORESHELL, Agent Smith, Agent Tesla, Agent.MI, Altwinner, Anchor, and ANDROIDOS_ANSERVER.A.

Vous verrez deux panneaux au milieu de l'écran, le panneau de droite est le panneau Détails et celui sur lequel vous souhaitez vous concentrer. Si vous lisez la description, vous trouverez la réponse. Une fois que vous l'avez trouvé, mettez en surbrillance copier (ctrl + c)

et collez (ctrl + v) ou tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

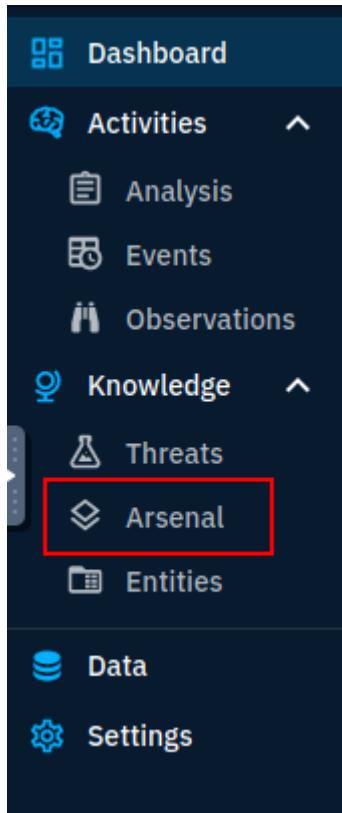
The screenshot shows the OpenCTI interface with the 'Arsenal' tab selected in the sidebar. The main content area displays the details of a malware entity named '4H RAT'. Key information includes:

- BASIC INFORMATION**: Standard STIX ID: malware--e980f592-7d1b-55aa-a030-6e3f119edc5b; Other STIX IDs: malware--8e461ca3-0996-4e6e-ebef-e2a5bbcc31ec.
- Marking**: Covsoft.
- Author**: THE METRE CORPORATION.
- Distribution of opinions**: 59% strongly-agree, 30% agree, 10% neutral.
- Confidence level**: LOW.
- Creation date (in this platform)**: May 2, 2022, 12:35:28 PM.
- Creator**: ADMIN.
- Processing status**: DISABLED.
- DETAILS**: Is family: NO; Malware types: **Arsenal**; Description: 4H RAT is malware that has been used by [redacted] since at least 2007. (Citation: CrowdStrike [redacted]); First seen: None; Last seen: None; Architecture execution env.: Unknown; Kill chain phases: Unknown; Implementation languages: Unknown; Capabilities: Unknown.

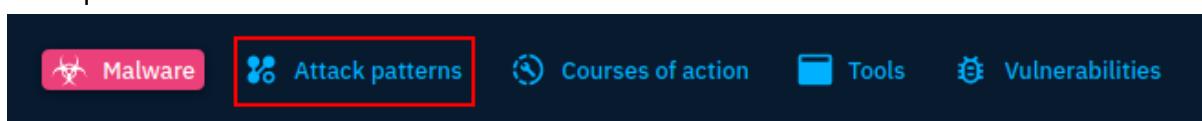
Réponse : Putter Panda

Quelle phase d'exécution de la kill-chain est liée au modèle d'attaque de l'interface de ligne de commande ?

Revenez au panneau de gauche, cliquez à nouveau sur Arsenal.



Au-dessus des panneaux centraux, vous verrez ce panneau d'onglets, cliquez sur Modèles d'attaque.



En haut du panneau Modèle d'attaque se trouve une barre de recherche, tapez Command-Line Interface, dans la barre de recherche et appuyez sur Entrée pour la rechercher.

The screenshot shows the OpenCTI web application. At the top, there is a navigation bar with tabs: Malware, Attack patterns (which is highlighted in pink), Courses of action, Tools, and Vulnerabilities. Below the navigation bar is a search bar containing the text "Command-Line Interface".

Votre meilleur résultat sera ce que vous recherchez, cliquez dessus.

The screenshot shows the search results for "Command-Line Interface". There is one result listed: "TOB07 - Command-Line Interface". The result is described as follows: "Adversaries may utilize command-line interfaces (CLIs) to interact with systems and execute commands. CLIs provide a means of interacting with computer systems and are a common feature across many types of platforms and devices within control systems environments. [Creation: Enterprise ATTACK...]".

Encore une fois, vous aurez deux panneaux au milieu de l'écran, et encore une fois nous nous concentrerons sur le panneau Détails. Cette fois cependant, sur le côté droit du panneau, vous devriez voir Kill Chain Phase, juste en dessous se trouve la réponse. Une fois que vous l'avez trouvé, mettez en surbrillance copier (ctrl + c) et collez (ctrl + v) ou tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

The screenshot shows the "COMMAND-LINE INTERFACE" details panel in OpenCTI. On the left, there is a sidebar with various navigation options like Dashboard, Activities, Knowledge, Threats, Arsenal, Data, and Settings. The main panel is titled "COMMAND-LINE INTERFACE". It contains several sections: "BASIC INFORMATION" (Standard STIX ID: attack-pattern--c1605a2bf-2564-569a-aaa3-114fde757fe7, Other STIX IDs: attack-pattern--24a9253e-8948-4198-b751-8e2ae53127c), "DETAILS" (External ID: TOB07, Description: "Adversaries may utilize command-line interfaces (CLIs) to interact with systems and execute commands. CLIs provide a means of interacting with computer systems and are a common feature across many types of platforms and devices within control systems environments. [Creation: Enterprise ATTACK...]", Platforms: Control Server, Data Historian, Field Controller/RTU/PLC/IED, Human-Machine Interface, Input/Output Server), and "Kill chain phases" (Detection, Answer). A red box highlights the "Answer" button under the Kill chain phases section.

Réponse : exécution-ics

Dans la catégorie Activités, quel onglet hébergerait les indicateurs ?

Cette réponse se trouve ci-dessus, dans cette section il est mentionné que sous cet onglet se trouvent un ou plusieurs indicateurs. Une fois que vous l'avez trouvé, mettez en surbrillance copier (ctrl + c) et collez (ctrl + v) ou tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

The screenshot shows the "Activities" section in OpenCTI. It highlights the "Indicators" tab. Below it, there is a text block: "Technical elements, detection rules and artefacts identified during a cyber attack are listed under this tab: one or several identifiable makeup indicators. These elements assist analysts in mapping out threat events during a hunt and perform correlations between what they observe in their environments against the intel feeds." A red box highlights the first sentence of this text.

Sur OpenCTI, c'est ici que vous pouvez le trouver.

The screenshot shows the OpenCTI web application. At the top, there is a navigation bar with tabs: Observables (highlighted in pink), Artifacts, Indicators (highlighted with a red border), and Infrastructure. Below the navigation bar is a search bar with placeholder text 'Search...' and a dropdown menu set to 'Sighted by/in'. On the left side, there is a sidebar with several sections: Dashboard, Activities (with Analysis, Events, and Answer links), Knowledge (with Threats, Arsenal, and Entities), Data, and Settings. The 'Answer' link under 'Activities' is highlighted with a red box. The main content area displays a table with columns 'TYPE' and 'VALUE'. The table contains six rows, all of which are 'Artifact' type with different IDs.

	TYPE	VALUE
<input type="checkbox"/>	Artifact	7dcdf51ed86049b6140c391c4
<input type="checkbox"/>	Artifact	7476c00856b41a60a78fbfc6b9
<input type="checkbox"/>	Artifact	a25f8973ec9af55bd5382cc5e7
<input type="checkbox"/>	Artifact	67acc6bb31e198cb372e8d717
<input type="checkbox"/>	Artifact	dad2eca50b5f47a0280cf871d9
<input type="checkbox"/>	Artifact	4136cbd135de0a67aecbb84e9

Réponse : Observations

Tâche 5 Tableau de bord OpenCTI 2

Navigation par onglets généraux

L'utilisation quotidienne d'OpenCTI impliquerait de naviguer à travers différentes entités au sein de la plateforme pour comprendre et utiliser les informations pour toute analyse des menaces. Nous examinerons l'entité malveillante Cobalt Strike pour notre procédure pas à pas, que l'on trouve principalement sous l'onglet Arsenal que nous avons couvert précédemment. Lorsque vous sélectionnez une entité de renseignement, les détails sont présentés à l'utilisateur via :

- Onglet Présentation : fournit des informations générales sur une entité analysée et étudiée. Dans notre cas, le tableau de bord vous présentera l'ID de l'entité, le niveau de confiance, la description, les relations créées en fonction des menaces, les ensembles d'intrusions et les modèles d'attaque, les rapports mentionnant l'entité et les éventuelles références externes.

Voir image.

- Onglet Connaissance : présente les informations liées associées à l'entité sélectionnée. Cet onglet comprendra les rapports associés, les indicateurs, les relations et la chronologie des modèles d'attaque de l'entité. De plus, un analyste peut afficher des détails précis à partir des onglets du volet de droite, où sont présentées des informations sur les menaces, les vecteurs d'attaque, les événements et les observables utilisés au sein de l'entité.

Voir image.

- Onglet Analyse : Fournit les rapports dans lesquels l'entrée identifiée a été vue. L'analyse fournit des informations utilisables sur une menace et guide les tâches d'enquête.

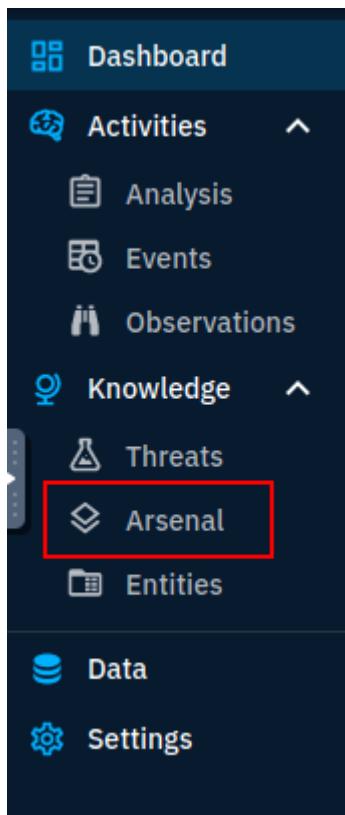
Voir image.

- Onglet Indicateurs : Fournit des informations sur les IOC identifiés pour toutes les menaces et entités.
- Onglet Données : contient les fichiers téléchargés ou générés pour l'exportation liés à l'entité. Ceux-ci aident à communiquer des informations sur les menaces faisant l'objet d'une enquête dans des formats techniques ou non techniques.
- Onglet Historique : les modifications apportées à l'élément, aux attributs et aux relations sont suivies par le travailleur de la plateforme et cet onglet présentera les modifications.

Répondre aux questions ci-dessous

Quels ensembles d'intrusions sont associés au malware Cobalt Strike avec un niveau de confiance bon ? (Intrusion1, Intrusion2)

Une fois sur le tableau de bord OpenCTI, regardez le panneau de gauche. Vous verrez Arsenal en gris près du bas, cliquez dessus. Cela ouvrira la section Malware dans la partie principale de la fenêtre à droite.



À l'aide de la barre de recherche, tapez Cobalt Strike et appuyez sur Entrée.

The screenshot shows the main search interface of the OpenCTI platform. At the top, there are tabs for Malware, Attack patterns, Courses of action, Tools, and Vulnerabilities. Below the tabs is a search bar with the text 'Cobalt Strike'. A red arrow points to the search bar. To the right of the search bar are buttons for sorting by 'Name' (with an upward arrow) and a refresh icon. The results section below shows several items, with the first one, 'Cobalt Strike', highlighted with a red box.

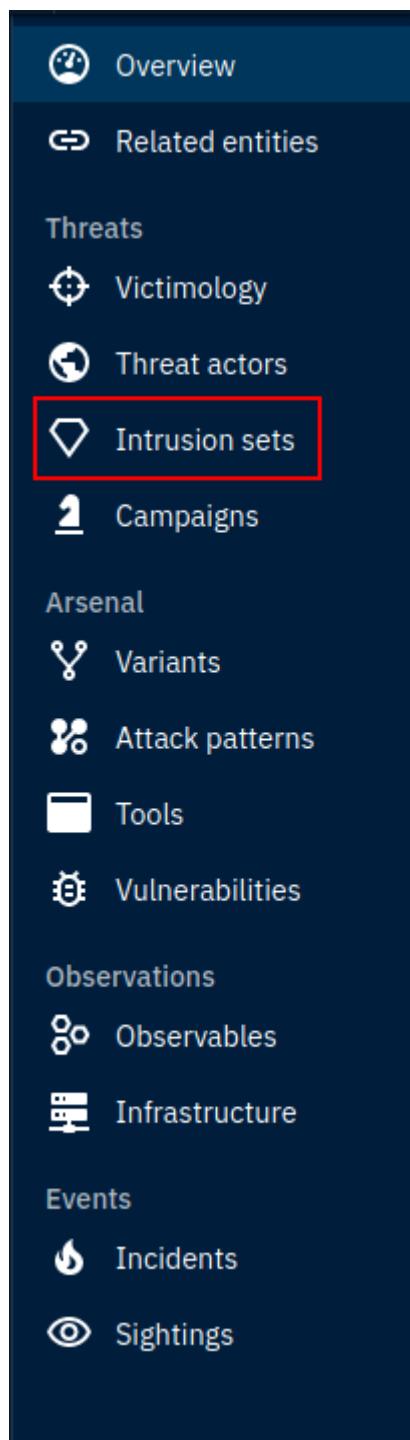
Votre premier résultat sera Cobalt Strike, cliquez dessus.

The screenshot shows the search results for 'Cobalt Strike'. The results are displayed in a grid format. The first result, 'Cobalt Strike', is highlighted with a red box. The results include: Cobalt Strike (malware), Goopy (malware), More_eggs (malware), and NativeZone (malware). Each result card provides a brief description and a 'malware' tag.

À partir de là, nous allons cliquer sur l'onglet Connaissances dans le panneau supérieur.

The screenshot shows the OpenCTI interface with the 'Knowledge' tab selected. On the left, the navigation sidebar includes 'Dashboard', 'Activities' (selected), 'Analysis', 'Events', 'Observations', 'Threats', 'Arsenal', 'Entities' (selected), 'Data', and 'Settings'. The main content area displays the 'COBALT STRIKE' entity. The 'BASIC INFORMATION' section contains fields like 'Standard STIX ID' (Malware--60817342-7c91-563c-6685-a51e805c30e4) and 'Other STIX IDs' (Malware--a7881f21-9870-4fe4-a5f6-92c9416a2616). It also shows 'Marking' (CobaltStrike), 'Author' (THE MITRE CORPORATION), 'Distribution of opinions' (5 stars), 'Confidence level' (Low), 'Creation date (in this platform)' (May 2, 2022, 12:36:22 PM), 'Creator' (ADMIN), and 'Processing status' (DISABLED). The 'DETAILS' section includes fields for 'Is family' (No), 'Malware types' (None), 'First seen' (None), 'Last seen' (None), 'Kill chain phases' (Unknown), 'Architecture execution env.' (Unknown), 'Implementation languages' (Unknown), and 'Capabilities' (Unknown). A pink edit icon is located in the bottom right corner of the main content area.

Lorsque le panneau Connaissances se charge au milieu de l'écran, vous verrez maintenant un autre panneau sur le côté droit de la page. Accédez à ce nouveau panneau et cliquez sur l'icône en forme de diamant indiquant Ensembles d'intrusion.



Lorsque l'intrusion définit le chargement du panneau, la première entrée nous donne la première moitié de la réponse. Maintenant, faites simplement défiler vers le bas jusqu'à ce que vous voyiez le prochain ensemble d'intrusions avec un score de confiance de Bon, lorsque vous le trouvez, c'est la seconde moitié de la réponse. Une fois que vous l'avez trouvé, tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

The screenshot shows the OpenCTI interface with the 'Knowledge' tab selected. On the left, a sidebar lists various modules like Dashboard, Activities, Events, Threats, Arsenal, Entities, Data, and Settings. The main area displays a table titled 'COBALT STRIKE' with the following columns: RELATIONSHIP TYPE, NAME, ENTITY TYPE, START TIME, STOP TIME, and CONFIDENCE. The first row, 'Cobalt Strike', is highlighted with a red box. The 'NAME' column header is also highlighted with a red box. The table contains 19 entity(s).

Réponse : CopyKittens, FIN7

Qui est l'auteur de l'entité ?

Revenez au panneau supérieur et cliquez sur l'onglet Présentation.

The screenshot shows the OpenCTI interface with the 'Overview' tab selected. The top navigation bar includes tabs for Malware, Overview, Knowledge, Analysis, Indicators, Data, and History. The main area displays a summary of Cobalt Strike information, including its STIX ID, other IDs, marking, author, distribution of opinions, and creation date.

Cette fois, au lieu de regarder le panneau Détails à droite, nous allons examiner le panneau Informations de base à gauche. Au-dessus de la répartition des opinions se trouve l'auteur. Une fois que vous l'avez trouvé, tapez la réponse dans le champ de réponse TryHackMe et cliquez sur Soumettre.

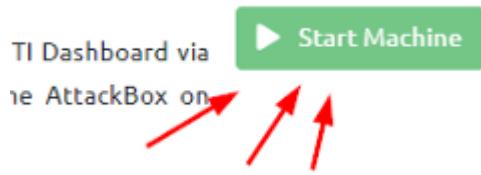
The screenshot shows the OpenCTI interface with the 'Details' tab selected. The main area is divided into two sections: 'BASIC INFORMATION' on the left and 'DÉTAILS' on the right. In the 'BASIC INFORMATION' section, fields include Standard STIX ID (Malware--62617342-7b91-563c-8485-a51d0f5c39e4), Other STIX IDs (Malware--47881f25-e978-4fe4-a156-92c9436a2616), Marking (CopyRight), Author (MITRE), Distribution of opinions (a 5-point Likert scale from strongly-disagree to strongly-agree), Creation date (May 2, 2022, 12:36:22 PM), Creator (ADMIN), and Processing status (DISABLED). In the 'DÉTAILS' section, fields include Is Family (NO), Malware types (None), Description (Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single...), First seen (None), Last seen (None), Kill chain phases (Unknown), Architecture execution env. (Unknown), Capabilities (Unknown), Implementation languages (Unknown), and a red edit icon.

Réponse : La société MITRE

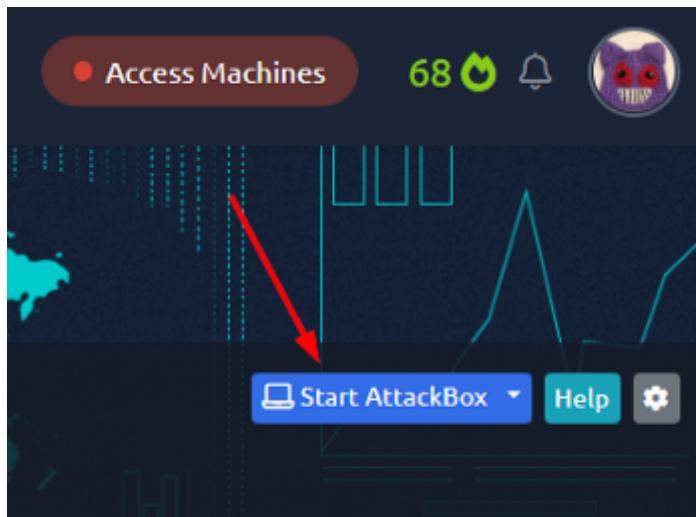
Vous avez terminé ces tâches et pouvez maintenant passer à [la tâche 6, scénario d'enquête et à la tâche 7, conclusion de la salle.](#)

Accéder au tableau de bord OpenCTI

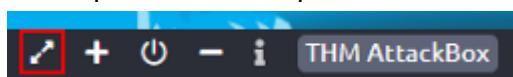
Passons au tableau de bord OpenCTI, pour ce faire, nous devons d'abord cliquer sur le bouton vert Démarrer la machine en haut de la tâche 4, pour que la VM soit opérationnelle.



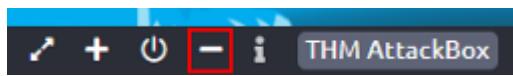
Ensuite, allez en haut de la page Web et cliquez sur l'icône bleue Démarrer AttackBox, l'écran se divisera et prendra environ une minute et demie pour que la VM se charge.



Au bas de la VM se trouvent deux flèches pointant dans les directions opposées, c'est l'icône plein écran. Clique dessus.



Un nouvel onglet s'ouvrira avec la VM dedans, pendant le chargement, retournez à l'onglet TryHackMe. Revenez à la barre en bas de la VM et cliquez sur le bouton — pour quitter l'écran partagé.



Il y a un terminal sur l'écran, si vous l'avez lu, appuyez sur Entrée pour le fermer.

```
Terminal
File Edit View Search Terminal Help
01

This machine can access other machines you deploy on TryHackMe.

Please keep in mind the following:
1. Pentesting any target that is not deployed by you on TryHackMe is prohibited.
2. You are solely responsible for your actions.
3. This machine expires. Check TryHackMe to ensure you still have time left.
4. Once this machine is terminated, all data will be lost.

View the changes made to the AttackBox: https://help.tryhackme.com/106142-my-machine/tryhackme-attack-machine#changelog

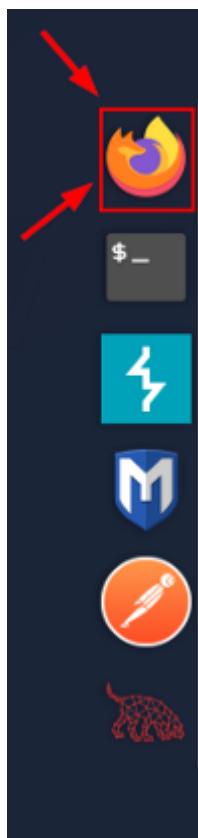
Usage Instructions:

1. Tools are located in /root/Desktop/Tools & /opt/
2. Webshells are located in /usr/share/webshells
3. Wordlists are located in /usr/share/wordlists
4. To use Empire & Starkiller, read the following file: /root/Instructions/empire-starkiller.txt

Do you think something's missing? Let us know! support@tryhackme.com

Press ENTER key to close.
```

Sur le côté droit de la VM se trouve un panneau rapide, en haut de ce panneau se trouve Firefox. Cliquez sur l'icône Firefox.



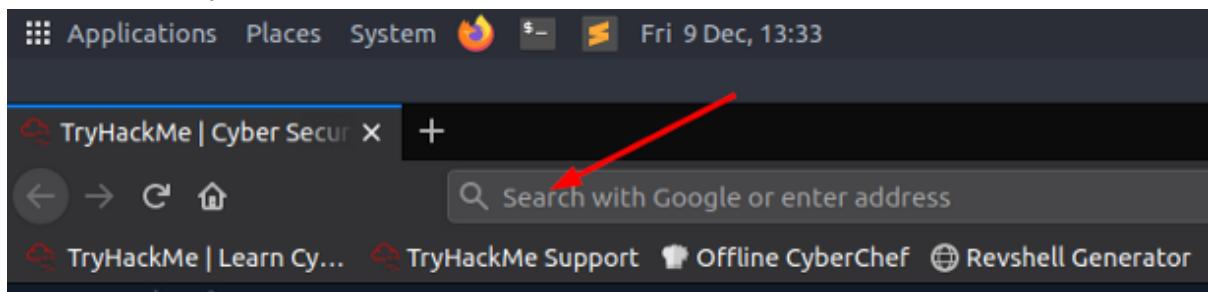
Pendant le chargement de Firefox, revenez à la tâche TryHackMe. Dans le premier paragraphe, vous verrez un lien qui vous mènera à la page de connexion OpenCTI. Mettez en surbrillance et copiez (ctrl + c) le lien.

Follow along with the task by launching the attack box on the AttackBox on <http://10.10.246.188:8080/>.
fullscreen.

Username: info@tryhack.io

Password: TryHackMe1234

Revenez à l'onglet VM, cliquez sur la barre d'URL. Collez (ctrl + v) l'adresse OpenCTI dans la barre et appuyez sur Entrée.

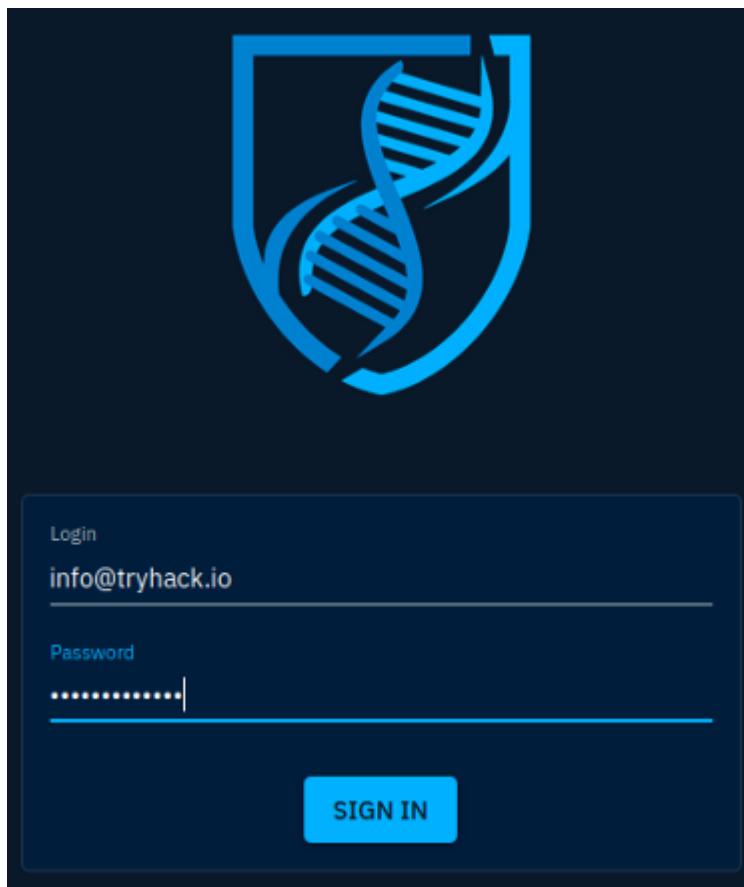


Le site chargera la page de connexion pour OpenCTI. Les informations de connexion sont de retour sur la tâche TryHackMe, vous pouvez soit mettre en surbrillance copier (ctrl + c) et coller (ctrl + v), soit saisir les informations d'identification dans la page de connexion. Cliquez ensuite sur le bouton bleu Se connecter.

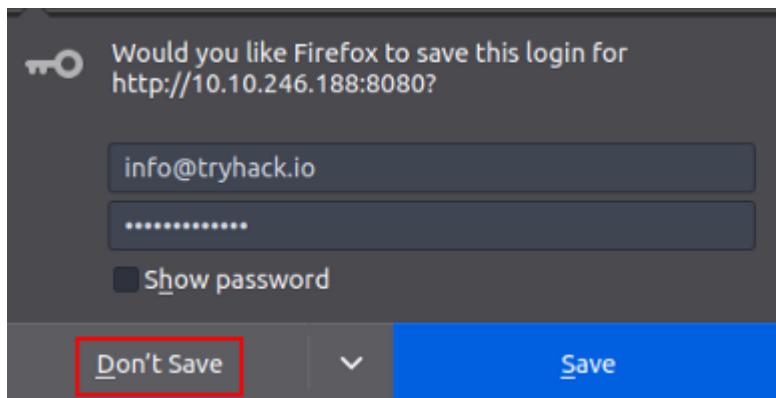
Follow along with the task by launching the attack box on the AttackBox on <http://10.10.246.188:8080/>.
fullscreen.

Username: info@tryhack.io

Password: TryHackMe1234



Vous aurez une petite fenêtre contextuelle pour enregistrer votre mot de passe dans Firefox, cliquez simplement sur Ne pas enregistrer.



Vous êtes maintenant dans le tableau de bord OpenCTI et prêt à continuer !!!

Scénario d'enquête de la tâche 6

En tant qu'analyste SOC, vous avez été chargé d'enquêter sur les logiciels malveillants et les groupes APT qui sévissent à travers le monde. Votre mission consiste à examiner le malware CaddyWiper et le groupe APT37 . Recueillez des informations auprès d'OpenCTI pour répondre aux questions suivantes.

Répondre aux questions ci-dessous

Quelle est la date la plus ancienne enregistrée concernant CaddyWiper ? Format : AAAA/MM/JJ

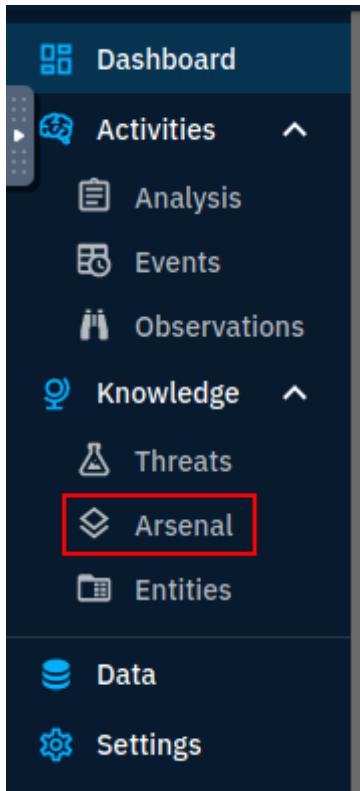
Nous savons donc d'en haut que CaddyWiper est un logiciel malveillant, et nous avons appris de la tâche 4 que sur le tableau de bord OpenCTI, nous pouvons trouver des logiciels malveillants sous l'onglet Arsenal.

Arsenal

This tab lists all items related to an attack and any legitimate tools identified from the entities.

- **Malware:** Known and active malware and trojan are listed with details of their identification and mapping based on the knowledge ingested into the platform. In our example, we analyse the 4H RAT malware and we can extract information and associations made about the malware.

En passant au tableau de bord OpenCTI dans la VM, nous voyons les différents onglets sur le côté gauche de l'écran. Allez à Arsenal et cliquez dessus.



L'onglet Malware est déjà sélectionné, après avoir cliqué sur l'onglet Arsenal. Donc en haut, il y aura une barre de recherche, tapez Caddywiper dans la barre de recherche et appuyez sur Entrée.

A screenshot of the OpenCTI interface showing search results for 'Caddywiper'. The search bar at the top contains 'Caddywiper' with a red arrow pointing to it. Below the search bar, there is a grid of cards displaying various malware entries. One card for '3PARA RAT' has a red circle with the letter 'a' on it, and another card for 'Agent Smith' has a red circle with a plus sign on it. The cards provide details such as name, update date, and a brief description. A total of 596 entities are shown.

Vous aurez un résultat, cliquez sur le résultat.

A screenshot of a search results page. At the top, there is a search bar containing the text "Caddywiper". To the right of the search bar are sorting options: "Sort by" and "Name" with a dropdown arrow. Below the search bar is a card for "CaddyWiper". The card features a blue circular icon with a white letter "C", the text "CaddyWiper Updated the May 24, 2022", a star icon, and a brief description: "CaddyWiper is a destructive data wiper that has been used in...". A button labeled "malware" is at the bottom of the card. The entire card is highlighted with a red border.

Vous serez maintenant sur la page de présentation du logiciel malveillant CaddyWiper, faites défiler vers le bas jusqu'à atteindre les derniers rapports sur cette entité.

A screenshot of the "CADDYWIPER" entity details page in the OpenCTI platform. The left sidebar shows navigation links for Dashboard, Activities, Knowledge, Threats, Arsenal, Entities, Data, and Settings. The main content area is titled "CADDYWIPER". It contains two main sections: "BASIC INFORMATION" and "DETAILS". The "BASIC INFORMATION" section includes fields for Standard STIX ID (malware--39dbe411-6c83-5e99-8903-821276a3454e), Other STIX IDs (malware--b30d999d-64e0-4e35-9056-884e4b83d611), Marking (Copyright...), Author (THE MITRE CORPORATION), Revoked (NO), Labels (malware), and a "Details" button. The "DETAILS" section includes fields for Is family (NO), Malware types (dropdown menu), Description (CaddyWiper is a destructive data wiper that has been used in attacks against organizations in Ukraine since at least March 2022. (Citation: ESET CaddyWiper March 2022) (Citation: Cisco CaddyWiper March 2022)), First seen (None), Last seen (None), Kill chain phases (Architecture execution env.), and Capabilities (Unknown). A red circle with a white edit icon is located in the bottom right corner of the main content area.

Une fois que vous êtes sur le panneau Derniers rapports sur cette entité, l'entrée du bas est celle que nous recherchons. Vous pouvez y voir une partie de la date. Cliquez sur cette entrée.

A screenshot of the "LATEST REPORTS ABOUT THIS ENTITY" section. It displays four reports in a table format:

	[MITRE ATT&CK]...	The MITR...	Apr 11, 20...	TLP:WHITE
	Malwarebytes Is...		Mar 18, 2...	TLP:WHITE
	ESET CaddyWip...	ESET	Mar 15, 2...	TLP:WHITE
	Cisco CaddyWip...		Mar 15, 2...	TLP:WHITE

The last row, which corresponds to the Cisco CaddyWiper report, is highlighted with a red border.

Sur cette page, vous verrez deux panneaux, celui que vous recherchez est le panneau Détails de l'entité. A l'intérieur de ce panneau, regardez la Description, vous trouverez ici la date la plus ancienne. Une fois que vous l'avez trouvé, saisissez-le dans le champ de réponse TryHackMe et cliquez sur Soumettre.

Réponse : 2022/03/15

Quelle technique d'attaque le malware utilise-t-il pour son exécution ?

Revenez au panneau supérieur et cliquez sur l'onglet Connaissances.

Lorsque le panneau Connaissances se charge, un nouveau panneau se chargera sur le côté droit de l'écran. Sur ce panneau, cliquez sur les modèles d'attaque.

La question demande la technique d'attaque pendant la phase d'exécution, alors faites défiler jusqu'à ce que vous voyiez la colonne Exécution.

The screenshot shows the CaddyWiper tool interface. At the top, there's a search bar labeled "Search..." and a tab labeled "CaddyWiper". Below the search bar, there are several categories with their respective technique counts and names:

- defense-evasion**: 45 techniques (Abuse Elevation Control Mechanism, Access Token Manipulation, BITS Jobs, Build Image on Host)
- persistence**: 22 techniques (Account Manipulation, BITS Jobs, Boot or Logon Autostart Execution, Boot or Logon Initialization Scripts)
- privilege-escalation**: 14 techniques (Abuse Elevation Control Mechanism, Access Token Manipulation, Boot or Logon Autostart Execution, Boot or Logon Initialization)
- collection**: 17 techniques (Adversary-in-the-Middle, Archive Collected Data, Audio Capture, Automated Collection, Browser Session Hijacking)
- credential-access**: 16 techniques (Adversary-in-the-Middle, Brute Force, Credentials from Password Stores, Exploitation for Credential Access)
- discovery**: 30 techniques (Account Discovery, Application Win32 Discovery, Browser Bookmarks Discovery, Cloud Infrastructure Discovery)

At the bottom left, there's a dropdown menu set to "mitre-attack", a refresh button, and a "TryHackMe" icon. On the right side, there's a pink circular button with a plus sign.

Une fois que vous atteignez la colonne Exécution, vous verrez que l'une des cases techniques est rouge, cela indique qu'elle est utilisée dans le malware Caddywiper. La réponse est donc celle qui est écrite dans l'encadré rouge. Une fois que vous l'avez trouvé, saisissez-le dans le champ de réponse TryHackMe et cliquez sur Soumettre.

execution
16 techniques
Command and Scripting Interpreter
Component Object Model and Distributed COM
Container Administration Command
Deploy Container
Exploitation for Client Execution
Graphical User Interface
Inter-Process Communication
Scheduled Task/Job
Scripting
Shared Modules

Réponse : API native

Combien de relations malware sont liées à cette technique d'Attaque ?

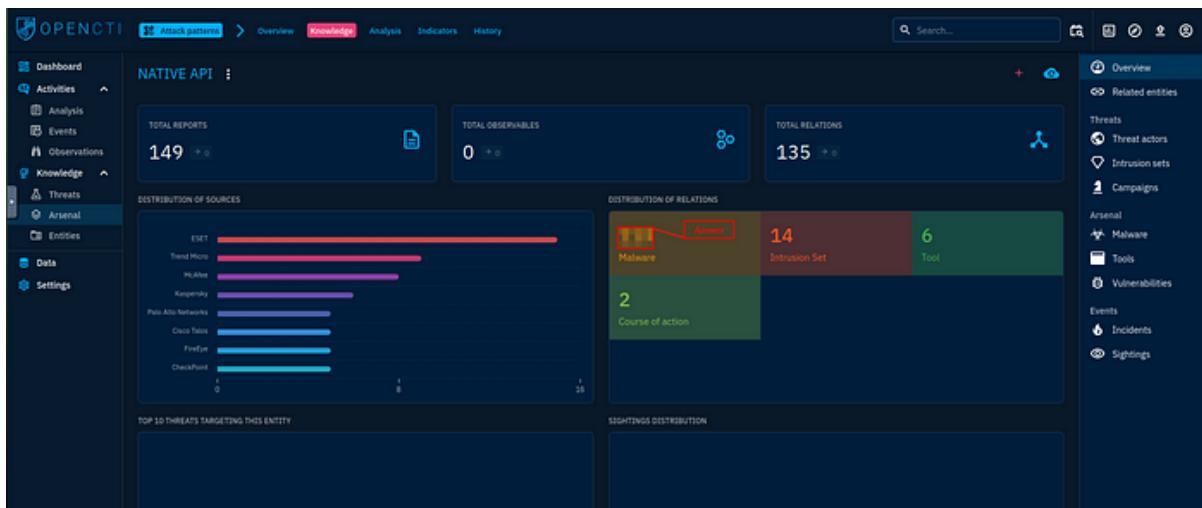
En revenant à la section Technique d'exécution, cliquez sur la réponse à la question précédente.

The screenshot shows a list of 16 execution techniques. The techniques listed are: Command and Scripting Interpreter, Component Object Model and Distributed COM, Container Administration Command, Deploy Container, Exploitation for Client Execution, Graphical User Interface, Inter-Process Communication (with a red box and 'Click Here' text overlaid), Scheduled Task/Job, Scripting, and Shared Modules.

Lorsque la page se charge pour cette technique d'exécution, cliquez sur l'onglet Connaissances en haut de la page.



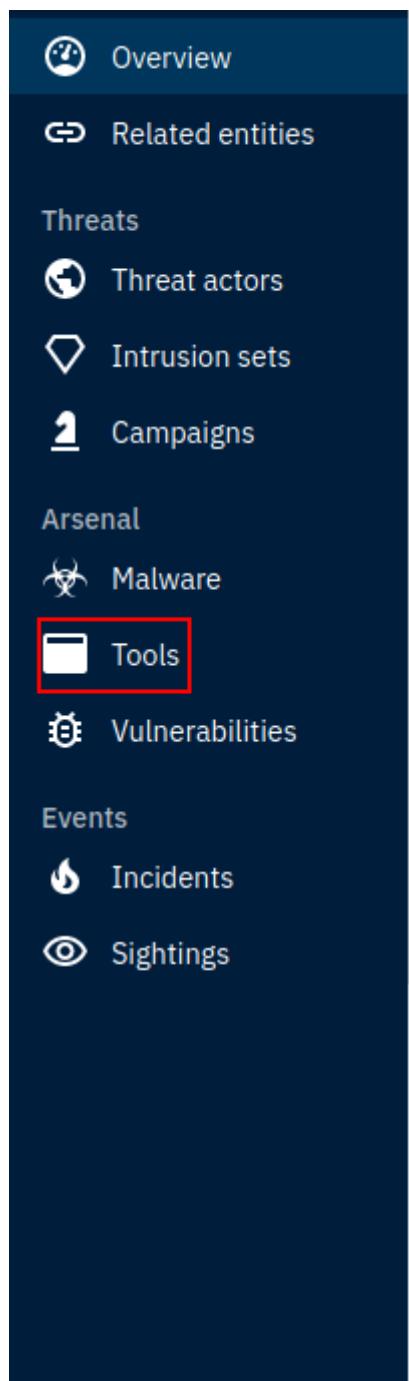
Sur la page Connaissances, vous trouverez la réponse. Vous verrez trois panneaux en haut du centre de la page, en dessous se trouvent deux panneaux, en regardant ces deux panneaux, regardez celui de droite. Il est étiqueté Distribution des relations et l'une des catégories est Malware. À l'intérieur de cette case se trouve un nombre, ce nombre est la réponse à la question. Une fois que vous l'avez trouvé, saisissez-le dans le champ de réponse TryHackMe et cliquez sur Soumettre.



Réponse : 113

Quels sont les 3 outils utilisés par la Technique d'Attaque en 2016 ? (Réponse : Outil 1, Outil 2, Outil 3)

En restant dans l'onglet Connaissances de cette technique, regardez à droite et vous verrez un panneau avec différents onglets, l'un des onglets est intitulé Outils. Clique dessus.



Génial, nous avons les outils, mais nous avons mélangé 2019 et 2016. Donc, pour mieux l'organiser, cliquez sur l'heure de début, cela mettra 2019 en haut et les trois de 2016 en bas.

RELATIONSHIP TYPE	NAME	ENTITY TYPE	START TIME	STOP TIME	CONFIDENCE
uses	ShimRatReporter	Tool	May 17, 2016	May 17, 2016	LOW
uses	BloodHound	Tool	Apr 17, 2016	Apr 17, 2016	LOW
uses	SILENTTRINITY	Tool	Aug 6, 2019	Aug 6, 2019	LOW
uses	Donut	Tool	May 9, 2019	May 9, 2019	LOW
uses	Imminent Monitor	Tool	Feb 18, 2019	Feb 18, 2019	LOW
uses	Empire	Tool	Apr 28, 2016	Apr 28, 2016	LOW

Mieux organisés, nous pouvons désormais les saisir dans le champ de réponse TryHackMe. Commencez par le haut de la liste et descendez avec une virgule et un espace entre les deux. Cliquez ensuite sur Soumettre.

RELATIONSHIP TYPE	NAME	ENTITY TYPE	START TIME	STOP TIME	CONFIDENCE
uses	SILENTTRINITY	Tool	Aug 6, 2019	Aug 6, 2019	LOW
uses	Donut	Tool	May 9, 2019	May 9, 2019	LOW
uses	Imminent Monitor	Tool	Feb 18, 2019	Feb 18, 2019	LOW
uses	██████████	Tool	May 17, 2016	May 17, 2016	LOW
uses	██████████	Tool	Apr 28, 2016	Apr 28, 2016	LOW
uses	██████████	Tool	Apr 17, 2016	Apr 17, 2016	LOW

Réponse : ShimRatReporter, Empire, Bloodhound

À quel pays APT37 est-il associé ?

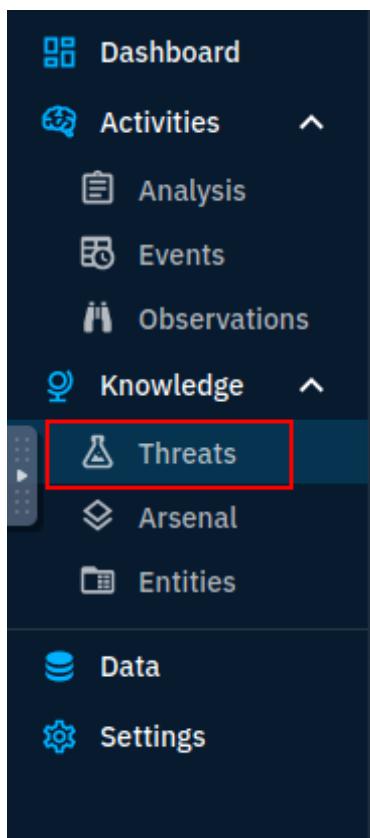
Nous avons donc appris que nous pouvons trouver où se trouvent les groupes APT dans la tâche 4, alors transmettons-nous ces connaissances.

Threats

All information classified as threatening to an organisation or information would be classified under threats. These will include:

- Threat Actors:** An individual or group of attackers seeking to propagate malicious actions against a target.
- Intrusion Sets:** An array of TTPs, tools, malware and infrastructure used by a threat actor against targets who share some attributes. APTs and threat groups are listed under this category on the platform due to their known pattern of actions.

En revenant à OpenCTI, regardez le panneau sur le côté gauche de l'écran. Cette fois, cliquez sur l'onglet Menaces.



Après avoir cliqué sur l'onglet Menaces, regardez en haut de l'écran, vous devriez voir un onglet Ensembles d'intrusions, cliquez dessus.



Nous sommes prêts à rechercher le groupe APT37, donc en haut du panneau central se trouve une barre de recherche. Cliquez dessus et tapez APT37, puis appuyez sur Entrée pour le rechercher.

A screenshot of the Threats page in the OpenCTI platform. The search bar at the top contains the text "APT37". Below the search bar, there is a table of threat groups. The first result is "admin@338" (No label), which is described as a China-based cyber threat group. The second result is "APT1" (No label), which is described as a Chinese threat group. Other results include "APT12" (No label), "APT16" (No label), "APT17" (No label), "APT18" (No label), "APT19" (No label), "APT20" (No label), "APT25" (No label), and "APT33" (No label). The table has columns for Name, Description, and Status.

Vous aurez deux résultats, cliquez sur le premier intitulé APT37.

Sort by Name ↓

A APT37 Updated the May 24, 2022 ☆

APT37 is a North Korean state-sponsored cyber espionage group that has been active since at least... No label

L Lazarus Group Updated the May 24, 2022 ☆

Lazarus Group is a North Korean state-sponsored cyber threat group that has been attributed to the... No label

Lorsque la page se charge, vous aurez deux panneaux. Regardez le panneau de droite intitulé Détails, la réponse se trouve sous la description dans la première phrase. Une fois que vous l'avez trouvé, saisissez-le dans le champ de réponse TryHackMe et cliquez sur Soumettre.

APT37

BASIC INFORMATION

Standard STIX ID: [Intrusion-set--e3e7be15-9a37-5c25-9141-797b40829469](#)

Other STIX IDs: [Intrusion-set--4a2ce82e-1a74-468a-adf9-bbead541383c](#)

Marking: Collected Revoked: NO

Author: THE MITRE CORPORATION

Distribution of opinions: 

Creation date: May 2, 2022, 12:45:55 PM

Modification date: April 18, 2018, 6:59:24 PM

Creator: ADMIN

Processing status: DISABLED

DETAILS

Description: Answer Originates from

APT37 is a [REDACTED] state-sponsored cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East. APT37 has also been linked to the following...

First seen: None

Last seen: None

Primary motivation: None

Secondary motivations: None

Réponse : Nord-Coréen

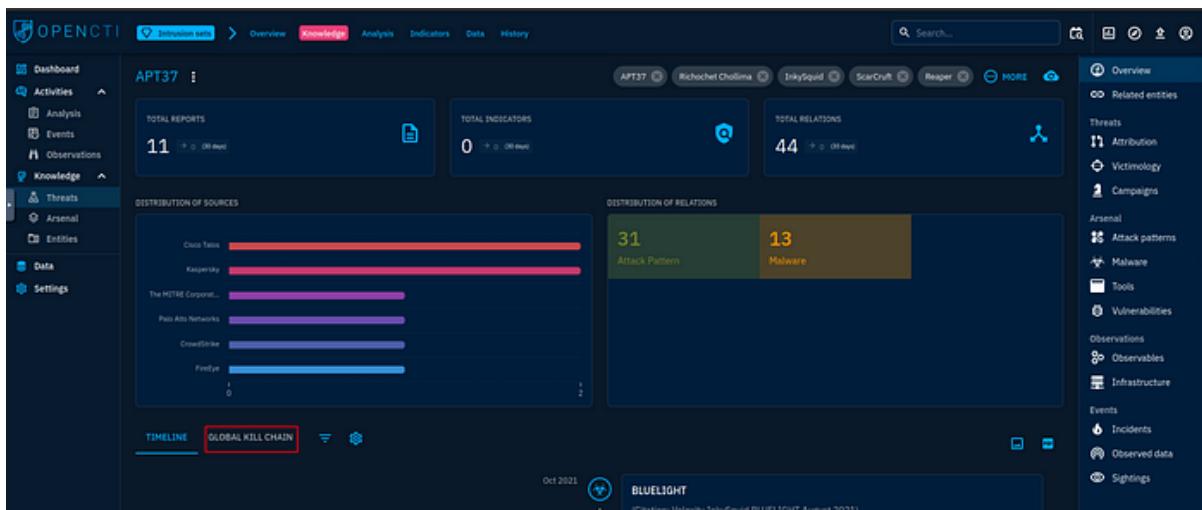
Quelles techniques d'attaque sont utilisées par le groupe pour l'accès initial ? (Réponse : Technique1, Technique2)

La question ne le dit pas, mais elle recherche l'ID technique, après avoir appris cela, il a été un peu plus facile de trouver la réponse.

En restant sur l'APT37, regardez en haut de la page et cliquez sur l'onglet Connaissance.

Intrusion sets > Overview Knowledge Analysis Indicators Data History

Dans l'onglet Connaissances, vous verrez deux grands panneaux. Sous ces panneaux sur la gauche se trouvent deux onglets, cliquez sur l'onglet Global Kill Chain.



Faites défiler vers le bas jusqu'à ce que vous atteigniez l'accès initial, une fois que vous aurez atteint cette section, vous verrez la réponse. TryHackMe fait commencer l'ordre en bas puis en haut, alors tapez les réponses dans le champ de réponse de cette façon, puis cliquez sur Soumettre.

Réponse : T1189, T1566

Conclusion de la salle de la tâche 7

Un travail fantastique pour parcourir et compléter la salle OpenCTI.

Dans cette salle, nous avons examiné l'utilisation de la plateforme OpenCTI pour traiter les informations sur les menaces et aider les analystes à enquêter sur les incidents. Consultez la documentation liée dans la salle pour obtenir plus d'informations sur OpenCTI et les différents outils et frameworks utilisés.

FÉLICITATIONS !!! Vous avez complété la salle OpenCTI !!!

MISP

write up :

partie 1

<https://medium.com/@haircutfish/tryhackme-misp-task-1-room-overview-task-2-misp-introduction-features-terminologies-task-b80b73d31d17>

partie 2

<https://medium.com/@haircutfish/tryhackme-misp-task-4-feeds-taxonomies-task-5-scenario-event-task-6-conclusion-1eab9d364039>

video :

https://www.youtube.com/watch?v=obdafIUI_k

\$\$\$\$\$\$

Walkthrough on the use of MISP as a Threat Sharing Platform

Task 1 Room Overview

MISP — MALWARE INFORMATION SHARING PLATFORM

This room explores the MISP Malware & Threat Sharing Platform through its core objective to foster sharing of structured threat information among security analysts, malware researchers and IT professionals.

Room Objectives

We will be covering the following areas within the room:

- Introduction to MISP and why it was developed.
- Use cases MISP can be applied to
- Core features and terminologies.
- Dashboard Navigation.
- Event Creation and Management.
- Feeds and Taxonomies.

Room Prerequisites

General familiarity with security concepts is: check out the [Pre Security](#) path and the [Jr. Security Analyst](#) room.

At the end of the room, we will have an exercise task to test your knowledge of the use of MISP.



Task 2 MISP Introduction: Features & Terminologies

What is MISP?

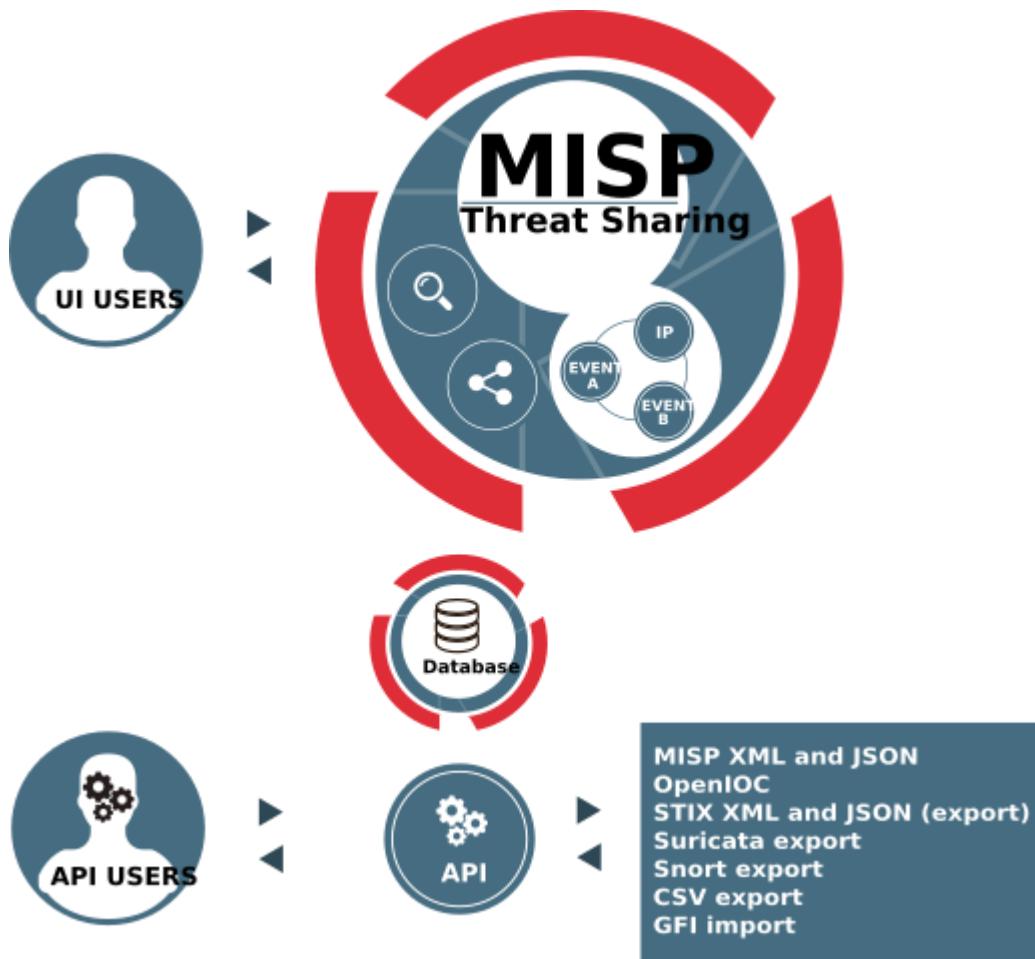
[MISP \(Malware Information Sharing Platform\)](#) is an open-source threat information platform that facilitates the collection, storage and distribution of threat intelligence and Indicators of Compromise (IOCs) related to malware, cyber attacks, financial fraud or any intelligence within a community of trusted members.

Information sharing follows a distributed model, with supported closed, semi-private, and open communities (public). Additionally, the threat information can be distributed and consumed by Network Intrusion Detection Systems (NIDS), log analysis tools and Security Information and Event Management Systems (SIEM).

MISP is effectively useful for the following use cases:

- Malware Reverse Engineering: Sharing of malware indicators to understand how different malware families function.
- Security Investigations: Searching, validating and using indicators in investigating security breaches.
- Intelligence Analysis: Gathering information about adversary groups and their capabilities.
- Law Enforcement: Using indicators to support forensic investigations.
- Risk Analysis: Researching new threats, their likelihood and occurrences.
- Fraud Analysis: Sharing of financial indicators to detect financial fraud.

What does MISP support?



MISP provides the following core functionalities:

- IOC database: This allows for the storage of technical and non-technical information about malware samples, incidents, attackers and intelligence.
- Automatic Correlation: Identification of relationships between attributes and indicators from malware, attack campaigns or analysis.
- Data Sharing: This allows for sharing of information using different models of distributions and among different MISP instances.
- Import & Export Features: This allows the import and export of events in different formats to integrate other systems such as NIDS, HIDS, and OpenIOC.
- Event Graph: Showcases the relationships between objects and attributes identified from events.
- API support: Supports integration with own systems to fetch and export events and intelligence.

The following terms are commonly used within MISP and are related to the functionalities described above and the general usage of the platform:

- Events: Collection of contextually linked information.
- Attributes: Individual data points associated with an event, such as network or system indicators.
- Objects: Custom attribute compositions.
- Object References: Relationships between different objects.
- Sightings: Time-specific occurrences of a given data point or attribute detected to provide more credibility.
- Tags: Labels attached to events/attributes.

- Taxonomies: Classification libraries are used to tag, classify and organise information.
- Galaxies: Knowledge base items used to label events/attributes.
- Indicators: Pieces of information that can detect suspicious or malicious cyber activity.

Task 3 Using the System

For you to understand how MISP works and follow along in the task, launch the attached machine and use the credentials provided to log in to the Analyst Account on https://LAB_WEB_URL.p.thmlabs.com/. Wait 1 minute for the URL and lab to start up.

Username: Analyst@THM.thm

Password: Analyst1234&

Dashboard

The analyst's view of MISP provides you with the functionalities to track, share and correlate events and IOCs identified during your investigation. The dashboard's menu contains the following options, and we shall look into them further:

- Home button: Returns you to the application's start screen, the event index page or the page set as a custom home page using the star in the top bar.
- Event Actions: All the malware data entered into MISP comprises an event object described by its connected attributes. The Event actions menu gives access to all the functionality related to the creation, modification, deletion, publishing, searching and listing of events and attributes.
- Dashboard: This allows you to create a custom dashboard using widgets.
- Galaxies: Shortcut to the list of [MISP Galaxies](#) on the MISP instance. More on these on the Feeds & Taxonomies Task.
- Input Filters: Input filters alter how users enter data into this instance. Apart from the basic validation of attribute entry by type, the site administrators can define regular expression replacements and blocklists for specific values and block certain values from being exportable. Users can view these replacement and blocklist rules here, while an administrator can alter them.
- Global Actions: Access to information about MISP and this instance. You can view and edit your profile, view the manual, read the news or the terms of use again, see a list of the active organisations on this instance and a histogram of their contributions by an attribute type.
- MISP: Simple link to your baseurl.
- Name: Name (Auto-generated from Mail address) of currently logged in user.
- Envelope: Link to User Dashboard to consult some of your notifications and changes since the last visit. Like some of the proposals received for your organisation.
- Log out: The Log out button to end your session immediately.

The screenshot shows the MISP interface with the 'Events' tab selected. On the left, there's a sidebar with various management links like 'List Events', 'Add Event', 'Import from...', 'REST client', etc. The main area displays a table of events. The columns include: Published, Creator org, ID, Clusters, Tags, #Attr., #Corr., Date, Last modified at, Info, Distribution, and Actions. There are 9 records shown, starting from record 1. One event is highlighted with a red icon and the text 'Threat Actor'. Other events are listed with their IDs and creation dates.



The Event Actions tab is where you, as an analyst, will create all malware investigation correlations by providing descriptions and attributes associated with the investigation. Splitting the process into three significant phases, we have:

- Event Creation.
- Populating events with attributes and attachments.
- Publishing.

We shall follow this process to create an event based on an investigation of Emotet Epoch 4 infection with Cobalt Strike and Spambot from malware-traffic-analysis.net. Follow along with the examples provided below.

Event Creation

In the beginning, events are a storage of general information about an incident or investigation. We add the description, time, and risk level deemed appropriate for the incident by clicking the Add Event button. Additionally, we specify the distribution level we would like our event to have on the MISP network and community. According to MISP, the following distribution options are available:

- Your organisation only: This only allows members of your organisation to see the event.
- This Community-only: Users that are part of your MISP community will be able to see the event. This includes your organisation, organisations on this MISP server and organisations running MISP servers that synchronise with this server.
- Connected communities: Users who are part of your MISP community will see the event, including all organisations on this MISP server, all organisations on MISP servers synchronising with this server, and the hosting organisations of servers that are two hops away from this one.
- All communities: This will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next.

Additionally, MISP provides a means to add a sharing group, where an analyst can define a predefined list of organisations to share events.

Published	Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Last modified at	Info	Distribution	Actions
✓ Cthulhu/SPRL.be	?	150		↳ type:OSINT ↳ type:white ↳ malware_classification:malware-category="malware" ↳ osint:source-type="blog-post"	2308	18	2015-11-05	2020-08-03 08:40:59	OSINT Expansion on Systematic cyber attacks against Israeli and Palestinian targets going on for a year by Norman	All ↗	
✓ Cthulhu/SPRL.be	?	23	Threat Actor ↳ Sofacy ↳	↳ type:OSINT ↳ type:white	945	15	2014-11-18	2020-08-03 08:34:15	OSINT Expansion on Additional indicators relating to Sofacy (APT28) phishing blog post by PWC	All ↗	
✓ Cthulhu/SPRL.be	→ 91	91	Threat Actor ↳ WildNeutron ↳	↳ type:OSINT ↳ type:white	143	1	2015-07-08	2020-08-03 08:31:12	OSINT Morphic: Profiting from high-level corporate attacks by Symantec	All ↗	
✓	→ 237	237		↳ type:OSINT ↳ type:white ↳ malware_classification:malware-category="Ransomware" ↳ osint:source-type="blog-post"	6		2016-04-08	2018-12-12 14:53:11	OSINT - Locky: the encryptor taking the world by storm	All ↗	
✓	→ 9	9	Threat Actor ↳ Axiom ↳	↳ type:OSINT ↳ type:white ↳ osint:source-type="blog-post" ↳ type:OSINT	20970	9	2014-10-28	2018-09-23 13:50:09	OSINT - Operation SMN (Novetta)	All ↗	
✓ Cthulhu/SPRL.be	→ 72	72	Threat Actor ↳ Sofacy ↳	↳ type:OSINT ↳ type:white ↳ malip-galaxy/mits-enterprise-attack-intrusion-set#APT28	1522	10	2015-04-20	2018-07-25 13:29:31	Expansion based on shared nameserver with a lot of Sofacy domain	All ↗	
✓ Cthulhu/SPRL.be	→ 32	32	Tool ↳ Regin ↳	↳ type:OSINT ↳ type:white	35	2	2014-12-04	2018-03-18 22:50:02	Regin Scanner	All ↗	
✓ Cthulhu/SPRL.be	→ 135	135	Threat Actor ↳ APT 30 ↳	↳ type:OSINT ↳ type:white	58	1	2015-04-13	2018-03-18 21:57:30	OSINT APT30 detection rules Loki Scanner Yara rules by Florian Roth	All ↗	
✓ Cthulhu/SPRL.be	→ 25	25		↳ type:OSINT ↳ type:white	7440	28	2014-11-20	2018-02-05 08:53:58	Import of CitizenLab public DB of malware indicators	All ↗	
✓ Cthulhu/SPRL.be	→ 1	1		↳ type:OSINT ↳ type:green ↳ type:white	1067	2	2014-10-02	2018-02-05 08:50:37	OSINT ShellShock scanning IPs from OpenDNS	All ↗	
✓ Cthulhu/SPRL.be	→ 74	74		↳ type:white ↳ type:OSINT	125	1	2015-04-27	2018-02-04 22:23:19	OSINT Attacks against Israel & Palestinian interests by PvC	All ↗	
✓ Cthulhu/SPRL.be	→ 43	43		↳ type:OSINT ↳ type:green ↳ type:white	886	12	2015-01-26	2018-02-02 14:28:38	OSINT I Know You Want Me - Unplugging Plugg from Takahiro Hayayama & Hiroshi	All ↗	

Event details can also be populated by filling out predefined fields on a defined template, including adding attributes to the event. We can use the email details of the CobaltStrike investigation to populate details of our event. We will be using the Phishing E-mail category from the templates.



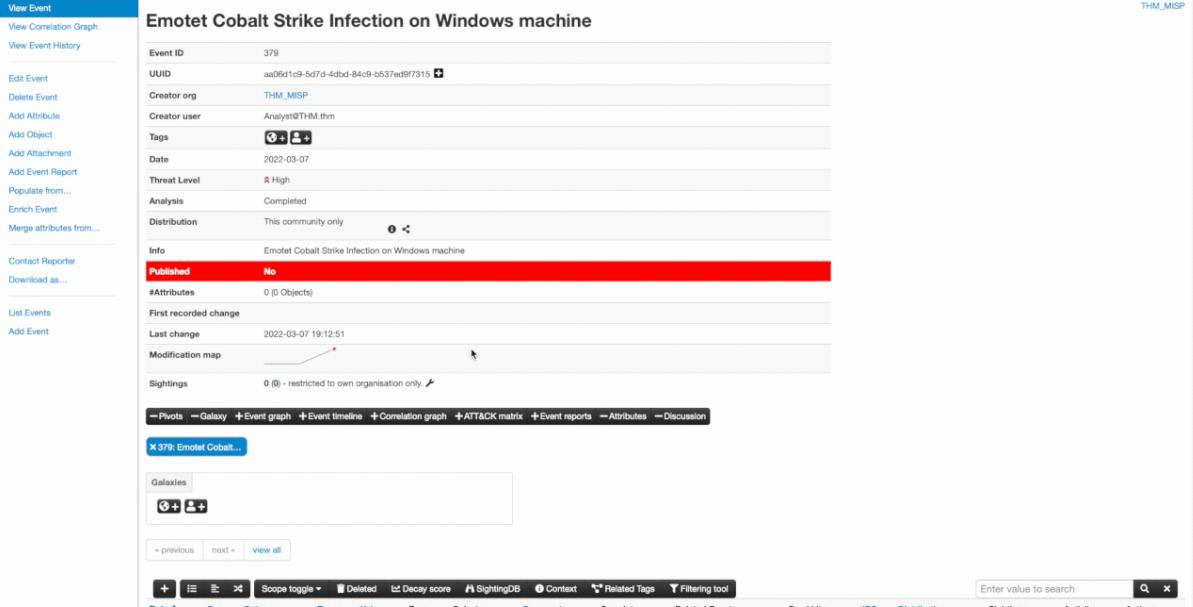
Attributes & Attachments

Attributes can be added manually or imported through other formats such as OpenIOC and ThreatConnect. To add them manually, click the Add Attribute and populate the form fields. Some essential options to note are:

- For Intrusion Detection System: This allows the attribute to be used as an IDS signature when exporting the NIDS data unless it overrides the permitted list. If not set, the attribute is considered contextual information and not used for automatic detection.

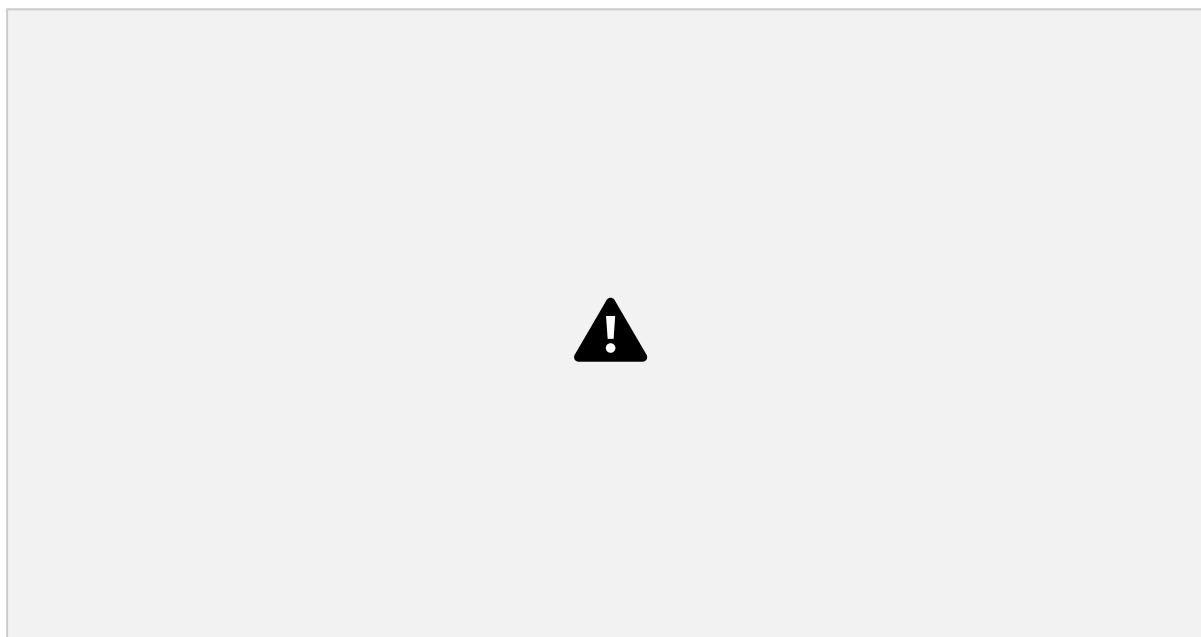
- Batch import: If there are several attributes of the same type to enter (such as a list of IP addresses), it is possible to join them all into the same value field, separated by a line break between each line. This will allow the system to create separate lines for each attribute.

In our example below, we add an Emotet Epoch 4 C2 IP address associated with the infection as our attributes, obtained from the IOC text file.



The screenshot shows the MISP Event Detail page for Event ID 379. The event title is "Emotet Cobalt Strike Infection on Windows machine". The left sidebar contains various navigation links like View Event, Edit Event, Add Attribute, etc. The main content area displays event details such as Event ID (379), UUID (aa0fd1c9-5d7d-4dbd-84c9-b537ed9f7315), Creator org (THM_MISP), and Threat Level (High). The "Published" status is set to "No". The "Attributes" section shows 0 attributes. The "Galaxies" section is empty. A warning icon (!) is located in the bottom right corner of the main content area.

The analyst can also add file attachments to the event. These may include malware, report files from external analysis or simply artefacts dropped by the malware. We have added the Cobalt Strike EXE binary file to our event in our example. You also have to check the Malware checkbox to mark the file as malware. This will ensure that it is zipped and passworded to protect users from accidentally downloading and executing the file.



Publish Event

Once the analysts have created events, the organisation admin will review and publish those events to add them to the pool of events. This will also share the events to the distribution channels set during the creation of the events.

Answer the questions below

Since the answer can be found above I won't be posting the answer here, follow along so that you can better find the answer.

How many distribution options does MISP provide to share threat information?

Scroll up to the Event creation section. In the final sentence of the first paragraph, it describes the following distribution options. All you need to do is count the number of options listed below that statement. Once you have counted them, type your answer into the TryHackMe answer field, then click submit.

Event Creation

In the beginning, events are a storage of general information about an incident or investigation. We add the description, time, and risk level deemed appropriate for the incident by clicking the [Add Event](#) button. Additionally, we specify the distribution level we would like our event to have on the [MISP](#) network and community. According to MISP, the following distribution options are available:

- **Your organisation only:** This only allows members of your organisation to see the event.
- **This Community-only:** Users that are part of your [MISP](#) community will be able to see the event. This includes your organisation, organisations on this MISP server and organisations running MISP servers that synchronise with this server.
- **Connected communities:** Users who are part of your [MISP](#) community will see the event, including all organisations on this MISP server, all organisations on MISP servers synchronising with this server, and the hosting organisations of servers that are two hops away from this one.
- **All communities:** This will share the event with all [MISP](#) communities, allowing the event to be freely propagated from one server to the next.

Which user has the role to publish events?

This answer can be found in the final section of the task. Reading through the first sentence the answer should stand out to you. Once you find it, highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer into the TryHackMe answer field then click submit.

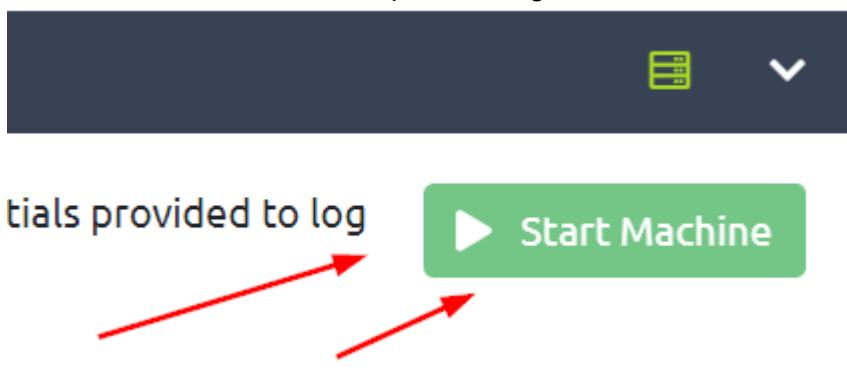
Publish Event

Once the analysts have created events, the will review and publish those events to add them to the pool of events. This will also share the events to the distribution channels set during the creation of the events.

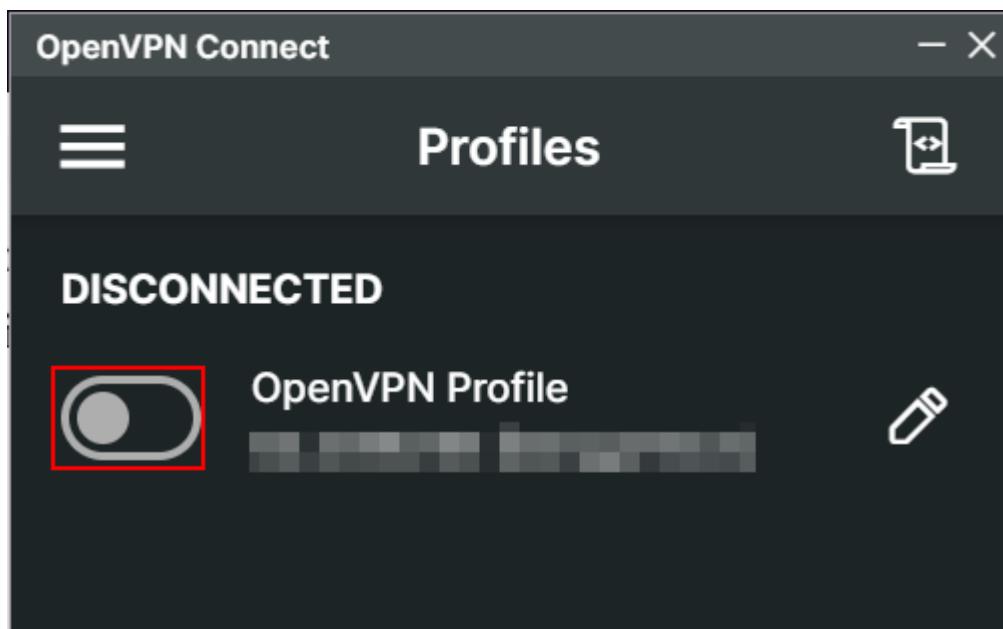
You have finished these tasks and can move onto [Task 4 Feeds & Taxonomies, Task 5 Scenario Event, & Task 6 Conclusion.](#)

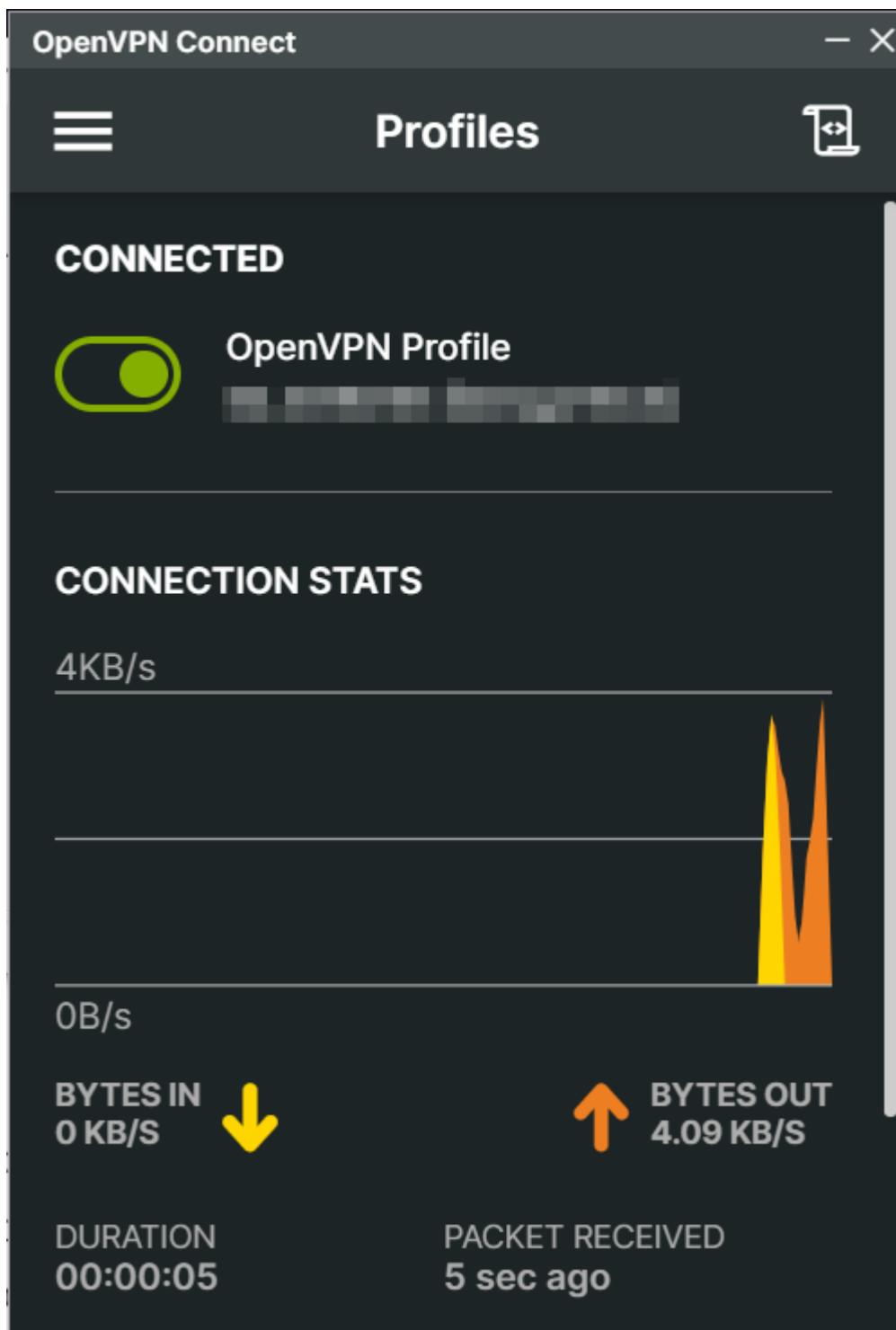
Getting to the MISP Dashboard

Head back to Task 3, at the top will be a green button labeled Start Machine. Click it.



On your local machine, open the OpenVPN program. Once the program loads, click on the toggle button to connect to your TryHackMe OpenVPN profile.





Head back to task 3, once the VM is done booting up and ready to go, in the top paragraph of the Task will be a link to click on. When you click on this link, it will open a new tab to the MISP log in page. Click this link.

Task 3 ✔ Using the System

For you to understand how MISP works and follow along in the task, launch the attached machine and use the credentials provided to log in to the Analyst Account on <https://10-10-187-3.p.thmlabs.com/>. Wait 1 minute for the URL and lab to start up.
Username: Analyst@THM.thm Password: Analyst1234&

Now you will need a Username and Password, which you can copy (ctrl + c) and paste (ctrl + v) into the boxes on the MISP login page.

Task 3 ✓ Using the System

For you to understand how MISP works and follow along in the task, launch the attached machine and use the credentials provided to log in to the Analyst Account on <https://10-10-187-3.p.thmlabs.com/>. Wait 1 minute for the URL and lab to start up.

Username: **Analyst@THM.thm** Password: **Analyst1234&**

Once you have paste the Username and Password into the login page fields, click the login button.

TryHackMe MISP Instance



Welcome to TryHackMe MISP. Learn how to create and manage your investigation events.

Login

Username: Password:

Email: Password:

Login

You are now in the MISP Dashboard and are ready to go!!!!

Task 4 Feeds & Taxonomies

Feeds

Feeds are resources that contain indicators that can be imported into MISP and provide attributed information about security events. These feeds provide analysts and organisations with continuously updated information on threats and adversaries and aid in their proactive defence against attacks.

MISP Feeds provide a way to:

- Exchange threat information.
- Preview events along with associated attributes and objects.
- Select and import events to your instance.
- Correlate attributes identified between events and feeds.

Feeds are enabled and managed by the Site Admin for the analysts to obtain information on events and indicators.

Taxonomies

A taxonomy is a means of classifying information based on standard features or attributes. On MISP, taxonomies are used to categorise events, indicators and threat actors based on tags that identify them.

MISP taxonomies - Flexible Classification for Information Sharing

MISP taxonomies is a solution to use existing taxonomies (or create your own) to **classify your cybersecurity events, indicators and threats**. This technique is integrated as a default mechanism for tagging in MISP (Malware Information Sharing Platform & Threat Sharing) and to support a distributed classification where organizations can share **common taxonomies in a local or distributed fashion**.

Classifications are distributed as simple JSON files to use with MISP but **can be easily integrated into any other information sharing software**. You can also propose new taxonomies to the community.

Examples of machine tags and human readable tags :

admiralty-scale:source-reliability="c"
admiralty-scale:Source Reliability="Fairly reliable"

admiralty-scale:information-credibility="3"
admiralty-scale:Information Credibility="Possibly true"

nato:classification="NU"
nato:Classification="NATO UNCLASSIFIED"

tlp:amber

Traffic Light Protocol:(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.

namespace predicate value



<https://github.com/MISP/misp-taxonomies/>

Analysts can use taxonomies to:

- Set events for further processing by external tools such as [VirusTotal](#).
- Ensure events are classified appropriately before the Organisation Admin publishes them.
- Enrich intrusion detection systems' export values with tags that fit specific deployments.

Taxonomies are expressed in machine tags, which comprise three vital parts:

- Namespace: Defines the tag's property to be used.
- Predicate: Specifies the property attached to the data.
- Value: Numerical or text details to map the property.

(Source: MISP)

Taxonomies are listed under the Event Actions tab. The site admin can enable relevant taxonomies.



Tagging

Information from feeds and taxonomies, tags can be placed on events and attributes to identify them based on the indicators or threats identified correctly. Tagging allows for effective sharing of threat information between users, communities and other organisations using MISP to identify various threats.

In our CobaltStrike event example, we can add tags by clicking on the buttons in the Tags section and searching from the available options appropriate to the case. The buttons represent global tags and local tags, respectively. It is also important to note that you can add your unique tags to your MISP instance as an analyst or organisation that would allow you to ingest, navigate through and share information quickly within the organisation.



Tagging Best Practices

Tagging at Event level vs Attribute Level

Tags can be added to an event and attributes. Tags are also inheritable when set. It is recommended to set tags on the entire event and only include tags on attributes when they are an exception from what the event indicates. This will provide a more fine-grained analysis.

The minimal subset of Tags

The following tags can be considered a must-have to provide a well-defined event for distribution:

- [Traffic Light Protocol](#): Provides a colour schema to guide how intelligence can be shared.
- Confidence: Provides an indication as to whether or not the data being shared is of high quality and has been vetted so that it can be trusted to be good for immediate usage.
- Origin: Describes the source of information and whether it was from automation or manual investigation.
- Permissible Actions Protocol: An advanced classification that indicates how the data can be used to search for compromises within the organisation.

Task 5 Scenario Event

[CIRCL](#) (Computer Incident Response Center Luxembourg) published an event associated with PupyRAT infection. Your organisation is on alert for remote access trojans and malware in the wild, and you have been tasked to investigate this event and correlate the details with your SIEM. Use what you have learned from the room to identify the event and complete this task.

Answer the questions below

What event ID has been assigned to the PupyRAT event?

On the Event list page is a filter bar, on the right side above the Event list. Type in the field PupyRat, and click Filter.



When the page loads, the answer will be the first column at the top labeled Event ID. Once you find it, highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer in the TryHackMe answer field.

OSINT - Iranian PupyRAT Bites Middle Eastern Organizations

Event ID: Answer

UUID: 5e2a97e7-4bd4-41c4-8aaf-42620950d210

Creator org: CIRCL

Tags:

- misp-galaxy.malware-enterprise-attack-intrusion-set
- ms-caro-malware.malware-type
- enisa.referrals-activity-abuse
- vert-assess.variety
- vert-action-misuse.vectors
- ms-caro-malware-full.malware-type
- CERT.XML.malicious-code
- type:OSINT
- osint:life-time=perpetual
- certainty=99
- sp:white

Date: 2020-01-23

Threat Level: High

Analysis: Initial

Distribution: All communities

Info: OSINT - Iranian PupyRAT Bites Middle Eastern Organizations

Published: Yes (2022-03-07 16:06:52)

#Attributes: 52 (14 Objects)

First recorded change: 2020-01-24 08:44:31

Last change: 2020-02-26 07:57:06

Modification map:

Sightings: 0 (0) - restricted to own organisation only

Download PGP public key

Welcome to TryHackMe's MISp Instance Powered by MISp 2.4.153 Learn and Grow! May the Force be with You! - 2022-12-13 16:09:40

Answer: 1146

The event is associated with the adversary gaining _____ into organisations.

From the way that the question is worded, it looks like we are looking for a type of access into an organization. Go back to the PupyRAT MISp page again, this time we are going to look at the tags. When we look at the tags, we see several that say about a type of access. Once you figure it out, highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer in the TryHackMe answer field.

OSINT - Iranian PupyRAT Bites Middle Eastern Organizations

Event ID: Answer

UUID: 5e2a97e7-4bd4-41c4-8aaf-42620950d210

Creator org: CIRCL

Tags:

- misp-galaxy.malware-enterprise-attack-intrusion-set
- ms-caro-malware.malware-type
- enisa.referrals-activity-abuse
- vert-assess.variety
- vert-action-misuse.vectors
- ms-caro-malware-full.malware-type
- CERT.XML.malicious-code
- type:OSINT
- osint:life-time=perpetual
- certainty=99
- sp:white

Date: 2020-01-23

Threat Level: High

Analysis: Initial

Distribution: All communities

Info: OSINT - Iranian PupyRAT Bites Middle Eastern Organizations

Published: Yes (2022-03-07 16:06:52)

#Attributes: 52 (14 Objects)

First recorded change: 2020-01-24 08:44:31

Last change: 2020-02-26 07:57:06

Modification map:

Sightings: 0 (0) - restricted to own organisation only

Download PGP public key

Welcome to TryHackMe's MISp Instance Powered by MISp 2.4.153 Learn and Grow! May the Force be with You! - 2022-12-13 16:09:40

Answer: Remote Access

What IP address has been mapped as the PupyRAT C2 Server

For this we can't find it in the tag's at the top, so we need to look into the information below. So let's narrow down those search results by using the find (ctrl + f) feature of the browser. First type in C2, we get five results, look through them.

C2

< > 1 of 5

Nothing good, let's think about what C2 stands for, command and control server. So let's just try command, we get one result, looking at it, it is the result we are looking for.



Look to the left in this row, you will see an IP address, this is the IP address associated with the PupyRAT C2 server and thus the answer to the question. Highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer in the TryHackMe answer field.

2020-01-29 Network activity ip-dst [REDACTED] Answer PupyRAT Command and control server

Answer: 89.107.62.39

From the Intrusion Set Galaxy, what attack group is known to use this form of attack?

Go back to the PupyRAT MISP page again, and again we can find the answer in the tag section. If you look at the first tag it mentions galaxy and intrusion set, so if you look at the end of it you will find the answer. Once you find it, highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer in the TryHackMe answer field.

OSINT - Iranian PupyRAT Bites Middle Eastern Organizations

Event ID: [REDACTED] **UUID:** 5e2a97e7-4bd4-41c4-8aaf-4262950d210f **Creator org:** CIRCL

Tags: `misdp-galaxy.mitre-enterprise-attack-intrusion-set*` `ms-carbo-malware.malware-type="ransomware"` `enisa-referious-activity-abuse*` `ms-carbo-malware.malware-type="ransomware"` `veris-assec.variety="5"` `veris-action.misuse.vector="ransomware"` `ms-carbo-malware-full.malware-type="ransomware"` `CER.XLM.malicious-code="spyware-rat"` `type:OSINT` `osint:lifetime="perpetual"` `certainty="50"` `sp:white`

Date: 2020-01-23 **Threat Level:** High **Analysis:** Initial **Distribution:** All communities **Info:** OSINT - Iranian PupyRAT Bites Middle Eastern Organizations **Published:** Yes (2022-03-07 16:06:52) **#Attributes:** 52 (14 Objects) **First recorded change:** 2020-01-24 08:44:31 **Last change:** 2020-02-26 07:57:09 **Modification map:** [REDACTED] **Sightings:** 0 (0) - restricted to own organisation only

Related Events: OSINT - The #BronzeUnion#LuckyMouse#APT27 infection checker 2019-12-27

Answer: Magic Hound

There is a taxonomy tag set with a Certainty level of 50. Which one is it?

Go back to the PupyRAT MISP page for the final time, and also look at the tags for the final time. Look for the blue tag on the bottom line, it will say certainty = "50", the first word or acronym is the answer to this question. Once you find it, highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer in the TryHackMe answer field.

Answer: OSINT

Task 6 Conclusion

Recap

Hopefully, you learned a lot about MISP and its use in sharing malware and threat information in this room. This tool is useful in the real world regarding incident reporting. You should be able to use the knowledge gained to effectively document, report and share incident information.

Additional Resources

There is plenty of information and capabilities that were not covered in this room. This leaves plenty of room for research and learning more about MISP. To guide you towards that, look at the following attached links and feel free to come back to the room to practice.

- [MISP Book](#)
- [MISP GitHub](#)
- [CIRCL MISP Training Module 1](#)
- [CIRCL MISP Training Module 2](#)

We wish to give credit to [CIRCL](#) for providing guidelines that supported this room.

🎉 CONGRATS!!!! You completed the MISP room!!! 🎉

Network security and traffic analysis

Comprendre les concepts de base de la sécurité du réseau et de l'analyse du trafic pour détecter et sonder les anomalies du réseau à l'aide des outils et techniques de l'industrie.

Traffic Analysis essentials

video : <https://www.youtube.com/watch?v=EikWCVNbps>

Snort

vidéo : <https://www.youtube.com/watch?v=pvPdOO2VcwM>