DATAPROTECT
Security is our commitment

Outil d'Automatisation de l'Analyse des Événement de Sécurité

Outil d'analyste SOC pour automatiser l'investigation et la validation d'éventuels indicateurs de compromission (IOC) et effectuer diverses tâches, notamment l'analyse des e-mails de phishing et la surveillance de la marque pour accélérer la réponse aux incidents.
L'objectif principal de l'utilisation de cet outil est d'automatiser autant de points de validation que possible effectués par l'équipe des opérations de sécurité d'entreprise tout en travaillant sur tout incident de sécurité, y compris la surveillance de la marque et une éventuelle attaque de phishing.
L'outil implémente également le cryptage (symétrique) afin que toutes vos clés API soient secrètes et sûres et ne puissent pas être manipulées tant que la clé de cryptage secrète n'est pas utilisée. Vous pouvez cependant modifier à tout moment vos clés API si vous avez accès à la clé de chiffrement.

CARACTÉRISTIQUES

Cet outil peut actuellement effectuer les tâches ci-dessous :
Vérification de la réputation des adresses IP, des domaines, des URL et des hachages de fichiers:

- **Virustotal**
- **Abuse IP DB**
- **Alienvault OTXv2**
- **Spyse**
- **Phishtank**
- **URL Scan**

Effectuer des recherches DNS, DNS inversé, WHOIS, ISP Lookups .
Analyse de la sécurité des e-mails (Phishing Email Analysis) :

- Analyser une URL de phishing
- Snadbox une pièce jointe malveillante présente dans un e-mail
- Analyse de l'en-tête des e-mails
- Directives pour effectuer une analyse des e-mails de phishing afin d'identifier les menaces .

Décodage des URL Office365 Safelink, des URL encodées UTF-8 ou Base64 .
Exécution de File Sandboxing pour le fichier et sa réputation de hachage de fichier associée .
Effectuer une analyse de surveillance .

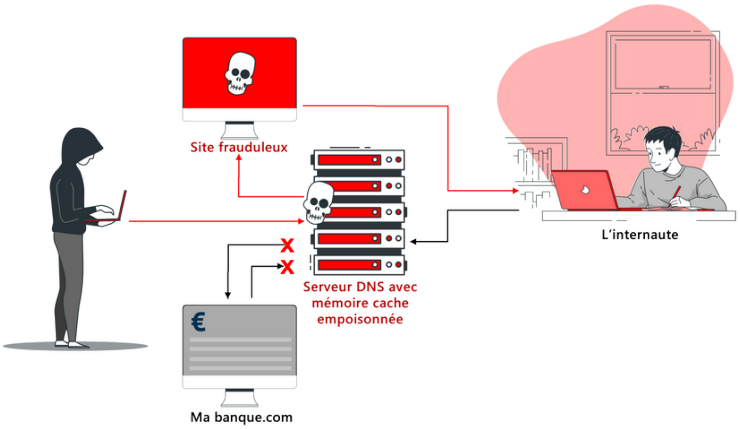
COMMENT L'UTILISER ?

Le script est simple à comprendre et à utiliser. Il peut être utilisé dans toutes ses fonctionnalités sans ouvrir le code source d'édition.

1. Lors de l'exécution du script principal pour la première fois, il vous dirigera automatiquement vers le menu de configuration, où il vous sera demandé d'entrer les clés API des plates-formes utilisées dans l'outil .
2. Toutes les clés API sont gérées séparément dans le fichier de clés API. Les clés API sont également cryptées avec un cryptage à clé symétrique .

DNS CACHE POISONING ?

Pour mener à bien une attaque par DNS Cache Poisoning, l'attaquant exploite une vulnérabilité du serveur DNS qui accepte alors des informations incorrectes. Si le serveur ne valide pas les informations reçues et qu'il ne vérifie pas qu'elles proviennent d'une source fiable, alors il stockera dans son cache ces informations erronées. Il les transmettra par la suite aux utilisateurs qui effectuent la requête visée par l'attaque.



DNS permet d'associer un nom compréhensible, à une adresse IP. On associe donc une adresse logique, le nom de domaine, à une adresse physique l'adresse IP

HACHAGE DE FICHIER ?

Un fichier hash permet de vérifier la taille et le caractère identique d'un fichier envoyé via un réseau informatique. En effet, lorsqu'un fichier transfère via un réseau, il est découpé en plusieurs morceaux, puis recollé une fois arrivé à destination. . Grâce à cette fonction, il devient très facile de comparer deux fichiers numériques très proches en apparence et vérifier que le fichier d'origine (l'entrée) n'ait pas fait l'objet d'une modification malveillante.

MD5 une valeur de hachage de 128 bits. Il a été conçu pour être utilisé en cryptographie, mais des vulnérabilités ont été découvertes au fil du temps, Cependant, il est toujours utilisé pour le partitionnement de bases de données et le calcul de sommes de contrôle pour valider les transferts de fichiers.

SHA1 signifie Secure Hash Algorithm. La première version de l'algorithme était SHA-1, mais il s'est rapidement avéré qu'il présentait également des vulnérabilités.

SHA2 Bien qu'il ne soit pas tout à fait parfait, les recherches actuelles indiquent qu'il est considérablement plus sûr que MD5 ou SHA-1.

SHA3 est une variante avec une applicabilité équivalente à celle de l'ancien SHA2 , le premier prenant un peu plus de temps à calculer que le dernier.

PHISHING ?

L'attaquant se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme.
Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.) , ou bien un fichier malveillant de format (pdf , cvs ,exe ,dll ...) que vous devrez l'executer dans votre machine .

ANALYSER UN EMAIL HEADER A LA RECHERCHE D'UN CONTENU MALVEILLANT

L'en-tête (Email Header) est la section de votre courrier contenant des informations telles que les détails de l'expéditeur, les détails du destinataire, le sujet et la date. Autre technique des détails tels que le chemin de retour, le champ de réponse et L'ID de message est également inclus dans un en-tête d'e-mail.

Indicateurs de contenu potentiellement malveillant dans les en-têtes d'e-mails

Les en-têtes d'e-mails fournissent de nombreuses informations qui peuvent être utilisées pour identifier les e-mails de phishing potentiels. Certaines d'entre elles sont faciles à lire et à interpréter, comme les sections disant que DKIM et SPF vérification passée dans la capture d'écran ci-dessus

```
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b="bRc/MbIX";
       spf=pass (google.com: domain of           @yahoo.com designates 77.238.176.206 as permitted sender)
smtp.mailfrom=           @yahoo.com;
```

Adresses d'expéditeur incompatibles

La comparaison des différents en-têtes d'e-mail associés à l'adresse de l'expéditeur peut être utile pour identifier cette technique. Cependant, tous les e-mails avec des noms d'affichage usurpés ne sont pas malveillants.

La capture d'écran ci-dessus provient d'un courrier d'Audible, la société de livres audio d'Amazon, répertoriant l'offre quotidienne de livres audio du jour. Un certain nombre de valeurs d'en-tête différentes dans cet e-mail doivent afficher l'adresse de l'expéditeur, notamment :

- smtp.mailfrom
- Return-Path
- From:
- Reply-to/Bounces-to

En regardant la capture d'écran ci-dessus, tous les en-têtes sont les mêmes à l'exception de l'expéditeur : un, qui est ce qui serait affiché au destinataire de l'e-mail. La comparaison de ces en-têtes pour les incohérences peut aider à identifier les e-mails de phishing ; Cependant, comme indiqué ci-dessus, tous les e-mails usurpant leur nom d'affichage ne sont pas malveillants.

Email travel path

Entre l'expéditeur et la destination, un e-mail passe par plusieurs serveurs de messagerie. Le nombre de serveurs dépend de l'e-mail, mais il doit toujours en avoir au moins deux : le serveur d'envoi et le serveur de réception.

```
Received: from sonic306-20.consmr.mail.ir2.yahoo.com (sonic306-20.consmr.mail.ir2.yahoo.com. [77.238.176.206])
        by mx.google.com with ESMTPS id qu22si111129667ejb.436.2020.03.31.10.07.26
        for
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 31 Mar 2020 10:07:27 -0700 (PDT)
```

Un enregistrement de ces serveurs de messagerie est stocké dans les en-têtes de courrier électronique, comme indiqué dans la capture d'écran ci-dessus. Cet e-mail provenait d'une adresse yahoo.com, il est donc logique que son serveur d'envoi soit un serveur yahoo.com.

L'examen de ces serveurs de messagerie peut aider à identifier les incohérences concernant les origines supposées d'un e-mail.

Lors de l'examen de ces en-têtes, il est également important de garder à l'esprit qu'ils ne sont pas entièrement fiables. À chaque étape du parcours, un serveur de messagerie a la capacité de modifier les en-têtes des e-mails. Si DKIM et SPF sont activés, cela devrait entraîner un échec de la vérification.

Cependant, l'expéditeur d'origine de l'e-mail peut avoir inclus des en-têtes falsifiés pour essayer de cacher qu'il est l'expéditeur d'origine du message (au lieu d'un simple point de cheminement). Les seuls en-têtes **Received:** auxquels on peut faire confiance sont ceux générés par une infrastructure interne de confiance.

Email Client

Lors de l'envoi d'un e-mail, la plupart des gens ne se connectent pas directement au serveur de messagerie et saisissent un e-mail dans la ligne de commande. Au lieu de cela, ils utilisent un client de messagerie, comme Outlook ou Gmail.

```
X-Mailer: WebService/1.1.15555 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/79.0.3945.88 Safari/537.36
```

Le client de messagerie utilisé par l'expéditeur d'un e-mail est inclus dans les en-têtes d'un e-mail. Si cet en-tête semble inhabituel de quelque manière que ce soit, cela pourrait être une raison de suspicion. Cependant, comme pour les autres en-têtes d'e-mails, cet en-tête peut être usurpé par l'expéditeur de l'e-mail.

MALWARE

Un malware, ou logiciels malveillants et souvent placé avec une technique de Spoofing, est un terme générique utilisé pour désigner une variété de logiciels hostiles ou intrusifs : virus informatique, vers, cheval de Troie, ransomware, spyware, adware, scareware, etc. Il peut prendre la forme de code exécutable, de scripts, de contenu actif et d'autres logiciels, ce qui le différencie du phishing.

Les malwares sont définis par leur intention malveillante, agissant contre les exigences de l'utilisateur de l'ordinateur.
Les malwares sont utilisés à la fois par les attaquants et les gouvernements pour voler des renseignements personnels, financiers ou commerciaux.
Le logiciel malveillant peut aussi :

- Chiffrer ou supprimer des données sensibles
- Modifier ou détourner des fonctions IT de base
- Espionner l'activité IT des utilisateurs.

TYPE DE MALWRE

TROJAN : logiciel malveillant qui se déguise en programme ordinaire pour inciter les utilisateurs à l'installer sur leurs systèmes. Une fois installé, il peut effectuer des actions malveillantes telles que voler des données sensibles, télécharger des fichiers sur le serveur de l'attaquant ou surveiller webcams

BACKDOOR : il s'agit d'un type de cheval de Troie qui l'attaquant d'accéder et d'exécuter des commandes sur le système compromis.

DOWNLOADER / DROPPER : Malware conçu pour télécharger ou installer des composants malveillants.

I**NFORMATION STEALER** : logiciel malveillant conçu pour voler des données sensibles telles que des données bancaires les informations d'identification ou les frappes au clavier du système infecté. Quelques exemples de ces les programmes malveillants incluent les enregistreurs de frappe, les logiciels espions, les renifleurs et les récupérateurs de formulaires.

VIRUS / WORM: logiciel malveillant capable de se copier et de se propager à d'autres des ordinateurs. Un virus nécessite l'intervention de l'utilisateur, alors qu'un ver peut se propager sans intervention de l'utilisateur.

ADWARE: Malware qui présente des publicités indésirables (publicités) à l'utilisateur. Ils sont généralement livrés via des téléchargements gratuits et peuvent installer de force des logiciels sur votre système.

ROOTKIT : logiciel malveillant qui fournit à l'attaquant un accès privilégié aux personnes infectées système et dissimule sa présence ou la présence d'autres logiciels.

RANSOMWARE : logiciel malveillant qui retient le système contre une rançon en bloquant les utilisateurs leur ordinateur ou en chiffrant leurs fichiers

BOTNET : Il s'agit d'un groupe d'ordinateurs infectés par le même logiciel malveillant (appelé bots), en attente de recevoir des instructions du serveur de commande et de contrôlé par l'agresseur. L'attaquant peut alors envoyer une commande à ces bots, qui peut effectuer des activités malveillantes telles que des attaques DDOS ou l'envoi de spam e-mails

LES DIFFERENTS METHODES D'ANALYSE MALWARE

ANALYSE STATIQUE : C'est le processus d'analyse d'un binaire sans l'exécuter. Il est plus facile à réaliser et permet d'extraire les métadonnées associées au binaire suspect. L'analyse statique peut ne pas révéler toutes les informations requises, mais elle peut parfois fournir des informations intéressantes qui aident à déterminer où concentrer vos efforts d'analyse ultérieurs. Le chapitre 2, Analyse statique, couvre les outils et les techniques permettant d'extraire des informations utiles du binaire malveillant à l'aide de l'analyse statique .

ANALYSE DYNAMIQUE : il s'agit du processus d'exécution du binaire suspect dans un environnement isolé et de surveillance de son comportement. Cette technique d'analyse est facile à réaliser et donne des informations précieuses sur l'activité du binaire lors de son exécution. Cette technique d'analyse est utile mais ne révéler toutes les fonctionnalités du programme hostile

SANBOXING

Sandboxing est une stratégie de gestion logicielle qui isole les applications des ressources système critiques et des autres programmes. Le sandboxing aide à réduire l'impact que tout programme ou application individuel aura sur votre système .

MALWARE ET LES SANDBOXES EN LIGNE

Le développement de la technologie sandbox a continué de progresser et à mesure que la demande d'une méthode rapide pour tester les logiciels se faisait sentir, nous avons assisté à l'introduction de sandbox en ligne. Ce sont des sites Web où vous pouvez soumettre un échantillon et recevoir un rapport sur les actions de l'échantillon telles qu'observées par des sandboxes en ligne .

SANDBOXES ET LES VIRTUELLES MACHINES

Lorsque vous créez votre sandbox, il est conseillé de créer deux images pour chaque conception, à savoir une "renforcée" conçue avec les mêmes protections installées au sein de votre entreprise et une "vulnérable" dans laquelle la plupart des protections sont désactivées. Grâce à cette solution, l'image renforcée vous montrera ce qui pourrait se passer dans votre environnement si un utilisateur exécutait le fichier, tandis que l'image vulnérable vous montrera l'exécution complète du malware.

Certaines des méthodes utilisées par les logiciels malveillants pour déterminer s'ils s'exécutent dans le sandbox sont :

- Retarder l'exécution pour utiliser le délai d'attente intégré à la plupart des sandboxes.
- Empreinte matérielle. Les bacs à sable et les machines virtuelles peuvent être reconnus car ils sont généralement différents des machines physiques. Une utilisation beaucoup plus faible des ressources, par exemple, est l'un de ces indicateurs.
- Mesurer l'interaction de l'utilisateur. Certains logiciels malveillants nécessitent que l'utilisateur soit actif pour s'exécuter, même s'il ne s'agit que d'un pointeur de souris en mouvement.
- Détection de réseau. Certains exemples ne fonctionneront pas sur des systèmes hors réseau.
- Vérification d'autres programmes en cours d'exécution. Certains exemples recherchent des processus connus pour être utilisés pour la surveillance et refusent de s'exécuter lorsqu'ils sont actifs. De plus, l'absence d'autres logiciels peut être considérée comme un indicateur d'exécution sur le sandbox.

URL ENCODING

Le codage d'URL est un mécanisme permettant de traduire des caractères non imprimables ou spéciaux dans un format universellement accepté par les serveurs Web et les navigateurs. . Les chiffres hexadécimaux dans les triplets de caractères représentent la valeur numérique des caractères qui sont remplacés. Le codage d'URL est largement utilisé dans la soumission de données de formulaire HTML dans les requêtes HTTP

INDICATEURS DE COMPROMIS - IOC

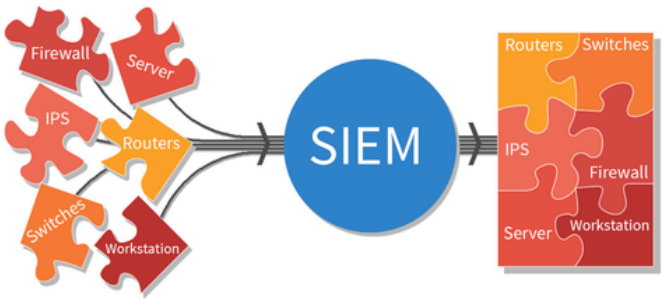
Les Indicateurs de Compromis sont utilisés pour déterminer dans quelle mesure une compromission a affecté une organisation ou pour tirer les leçons d'une attaque, afin d'aider à protéger l'environnement contre de futures attaques.
Les indicateurs sont généralement collectés à partir d'antimalwares et d'antivirus, mais d'autres outils de cybersécurité à intelligence artificielle peuvent être utilisés pour agréger et organiser les indicateurs lors de la réponse à un incident

COMMENT FONCTIONNENT LES INDICATEURS DE COMPROMIS ?

Même si les auteurs de malware essaient de créer des logiciels qui évitent la détection, chaque application laisse des traces de son existence sur le réseau. Ces indices peuvent être utilisés pour déterminer si le réseau est attaqué ou si une fuite de données s'est produite.
Les enquêteurs utilisent ces indices pour rassembler des preuves après un incident de cybersécurité afin de préparer des contre-mesures et d'engager des poursuites pénales contre un attaquant.
Ces indicateurs sont cruciaux pour trouver les vulnérabilités et les exploits utilisés par les attaquants pour voler des données car ils offrent à l'organisation des informations sur les moyens de mieux protéger le réseau à l'avenir.

UTILISER LES IOCs POUR AMELIORER LA DETECTION ET LA REPONSE

Après un incident de cybersécurité, les IoC peuvent être utilisés pour déterminer les causes d'une attaque et éviter tout exploit de la même vulnérabilité dans le futur.
Dans certains cas, les organisations n'enregistrent pas et ne surveillent pas correctement les bonnes ressources. Cette surveillance les laisse à la merci d'un attaquant, qui peut alors éviter d'être détecté après une enquête. Il est important de mettre avant tout en place une surveillance sur le réseau pour détecter une attaque, mais les logs et les pistes d'audit sont tout aussi importants pour enquêter.
Les points de données des IoC peuvent être collectés en temps réel pour réduire le temps de réponse pendant une enquête. Les SIEM sont utilisés pour séparer le bruit de fond des preuves véritables et précieuses nécessaires pour identifier une attaque et ses vecteurs d'exploitation.



La documentation des procédures de réponse aux incidents en cours peut également réduire le temps d'enquête. Ces procédures devraient être revues après une compromission afin de les améliorer.
Lors de la réponse à un incident, la phase des "leçons apprises" est la dernière étape. Les IoC sont utiles durant cette phase pour identifier quelles défenses de cybersécurité ont été mal configurées ou insuffisantes pour arrêter un attaquant. Plus les journaux et les pistes d'audit sont complets, plus leur enquête est efficace pendant la réponse à l'incident.