UseCase2 Analyse de Log Antivirus - Détection de Malware

Ticket 001

Titre : Analyse de Log Antivirus - Détection de Malware

Numero : ticket numero 001

Severité : 6 (modéré)

Contexte : Le Janvier 9 à 04:01:59 Le log indique qu'un fichier infecté a été détecté par WithSecure™ Linux Security 62. La menace identifiée est Malware.Eicar-Test-Signature, ce qui correspond généralement à un fichier de test utilisé pour évaluer les performances d'un logiciel antivirus. Voici les éléments clés :

- Fichier infecté : /home/leon.marchand/.cache/mozilla/firefox/9qnfqlkl.default-esr/cache2/entries/99A5AFC59CA2D59AB83B2E632DE96A8473DE113D.malware
- Nom de l'hôte : workstation025.admastercyber.infra.descartes
- Action : Aucune action automatique n'a été effectuée.
- Chemin du domaine : Root/Descartes/Linux/workstation025.admastercyber.infra.descartes

Il n'y a pas de traces spécifiques indiquant que ce fichier a été exécuté ou utilisé par un hacker, mais sa détection dans un répertoire temporaire de Firefox pourrait indiquer une tentative de téléchargement via le navigateur.

Analyse: L'événement s'est produit le 9 janvier à 04:01:59. L'antivirus WithSecure™ Linux Security 62 a détecté un fichier malveillant, identifié comme Malware.Eicar-Test-Signature, dans le cache Firefox de l'utilisateur leon.marchand. Le fichier se trouve sous le chemin /home/leon.marchand/.cache/mozilla/firefox/.../99A5AFC59CA2D59AB83B2E632DE96A8473DE113D.malware.

L'hôte concerné, workstation025, appartient au domaine admastercyber.infra.descartes, et la menace a été enregistrée avec une sévérité critique de 10. Aucune action automatique n'a été prise par l'antivirus, laissant le fichier potentiellement exploitable. L'absence de métadonnées détaillées, comme le hash, l'origine ou la taille du fichier, complique l'analyse précise. Toutefois, son emplacement dans le cache Firefox suggère un téléchargement via un site web. Ce log indique un risque sérieux qui nécessite une intervention rapide pour isoler et sécuriser le fichier.

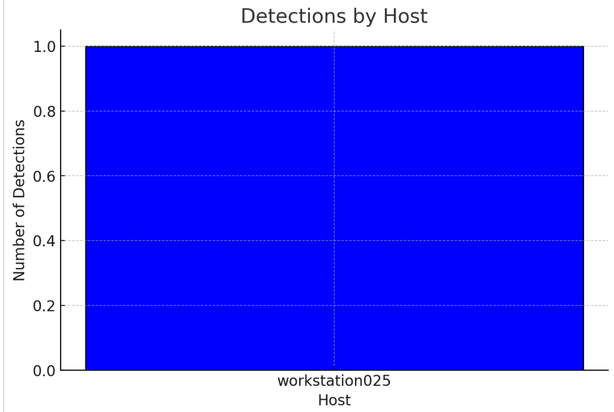
Recommandation :

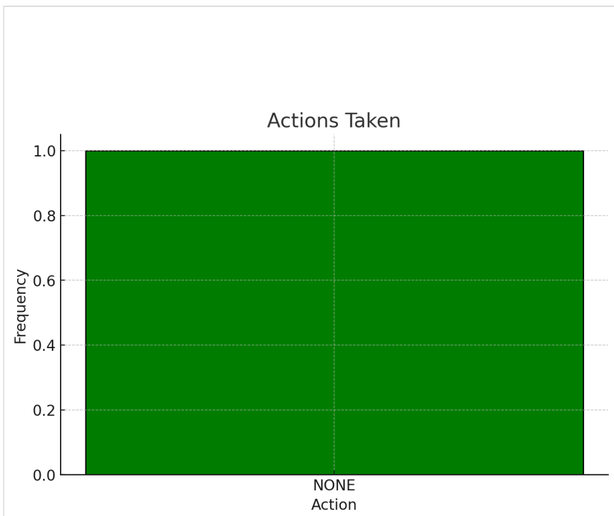
Il faut d'abord verifier que ce fichier n'a pas été telecharger lors d'un test de l'antivirus ou d'un edr , si ce n'est pas le cas pour éviter tout risque d'exécution accidentelle, il est nécessaire de supprimer ou de mettre en quarantaine le fichier infecté immédiatement. Ensuite, il faut procéder à un audit complet du système en scannant l'intégralité des fichiers pour identifier d'autres éventuelles menaces. Il est également crucial de rechercher des anomalies dans les journaux système, notamment des tentatives de connexion ou d'exécution suspectes autour de la période de détection.

Parallèlement, une surveillance des activités réseau doit être mise en place. Cela inclut la vérification des connexions suspectes établies au moment de la détection et le blocage des domaines ou des adresses IP identifiés comme potentiellement malveillants.

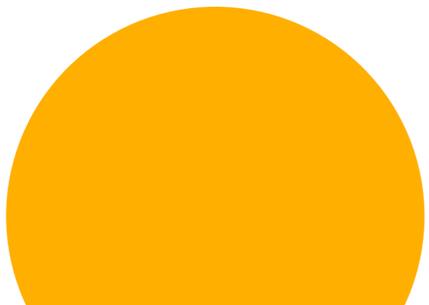
Pour renforcer les politiques de sécurité, il est recommandé de configurer l'antivirus afin qu'il prenne automatiquement des mesures comme la mise en quarantaine en cas de détection critique. Il convient aussi de restreindre les permissions sur les répertoires critiques, tels que le répertoire /home, pour limiter les risques.

Enfin, une formation des utilisateurs est indispensable. Ils doivent être sensibilisés aux risques liés aux téléchargements depuis des sites non fiables et encouragés à adopter de bonnes pratiques de navigation sur Internet



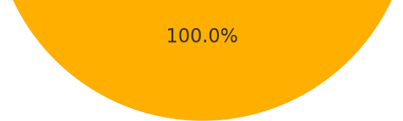


Distribution of Malware Types



log_analysis table

Date	Time	Host	Malware	Action	Severity	Path
Jan 9	04:01:59	workstation025	Malware.Eicar-Test-Signature	NONE	10	/home/leon.marchand/.cache/mozilla/firefox/.../9…



Malware.Eicar-Test-Signature