Rouge = Léandro

Bleu = Tanguy

Introduction : (1 minute)

Bonjour à tous. Aujourd'hui, je vais aborder un sujet essentiel dans le domaine de la cybersécurité : l'identification des virus par les antivirus. En France, selon le rapport Hiscox 2023, 53% des entreprises ont subi une cyberattaque, et les virus informatiques sont parmi les menaces les plus courantes. La détection efficace de ces virus est cruciale pour protéger les données sensibles, maintenir la confiance des utilisateurs et également pour des raisons économiques (dégradation de matériel etc ...). Avec l'augmentation des ransomwares et des attaques ciblées, il est vital de comprendre comment les antivirus identifient et neutralisent ces menaces. Dans cet exposé, nous examinerons les méthodes utilisées par ces logiciels ainsi que les défis auxquels ils font face.

Types de virus : (3 minutes -> 1m30 par personne)

Virus classique :

Un virus classique s'attache à un fichier exécutable, tel qu'un programme ou un document. Lorsqu'un utilisateur exécute ce fichier, le virus est activé. Il peut alors commencer à infecter d'autres fichiers sur le même système.

Vers informatiques :

Les vers ciblent généralement des failles de sécurité dans les systèmes d'exploitation, les applications ou les protocoles réseau. Par exemple, ils peuvent exploiter une vulnérabilité dans un logiciel non mis à jour pour accéder à un système sans que l'utilisateur n'ait besoin d'exécuter un fichier ou d'ouvrir une pièce jointe.

Chevaux de Troie :

Les chevaux de Troie, ou "Trojans", sont des programmes malveillants dissimulés dans des logiciels légitimes. Ils incitent les utilisateurs à les installer, souvent en promettant des fonctionnalités utiles ou des divertissements.

Ransomeware, spyware, Adware :

Ce sont des malwares avec divers objectifs. Le ransomeware crypte les fichiers de la victime et demande une rançon en échange. Le spyware aussi appelé logiciel espion récolte des informations d'un utilisateur à son insu (mots de passes ...). L'adware quant à lui est conçu pour afficher des publicités de manière excessive. Ce dernier n'est pas forcément malveillant mais peut rendre l'expérience de l'utilisateur très désagréable. (Bien que certains adware récoltent des données pour de la publicité ciblé.)

Fonctionnement des antivirus : (4 minutes -> 2 minutes par personne)

Analyse par signature :

Lorsqu'un nouveau malware est découvert, son code est analysé par un expert pour identifier une séquence unique (suite de chiffres, lignes de codes etc). Cette séquence devient alors une signature spécifique au malware et est stocké dans une base de données utilisé par l'antivirus pour comparer les signatures avec les fichiers analysés. La base de données est constamment mise à jour.

Analyse heuristique :

L'antivirus utilise des algorithmes spécifiques et des méthodes empiriques (observation, expériences et expérimentation) pour définir des règles heuristiques basés sur le comportement et la structure du virus. Par exemple si un fichier analysé par l'antivirus établi des connexions à des adresses IP inconnus et qu'il enfreint une règle heuristique en faisant cela alors ce fichier sera donc examiné de plus près par l'antivirus. L'analyse heuristique est souvent appliquée lors de scans programmés ou à la demande et **est appliqué avant l'exécution du fichier pour prédire la malveillance de celui-ci**.

Analyse comportementale et en temps réel :

L’analyse comportementale consiste à surveiller les actions des programmes en cours d’exécution en temps réel. Cette analyse fonctionne en observant les actions des programmes comme la création de fichiers et détecte les comportements suspects. L’analyse comportementale prend des mesures immédiatement lorsqu'un comportement suspect est détecté. Les comportements suspects sont définis notamment grâce à des profils comportementaux des utilisateurs ou des programmes. Ce profil inclus par exemple les actions réalisées et la fréquence de ces actions. Par exemple un utilisateur qui accède à des fichiers sensibles sans raison pourrait être considéré comme suspect si cela est inhabituel et n’est pas inclus dans son profile. Cette analyse utilise aussi les règles heuristiques pour identifier les comportements suspects en temps réel. Cette méthode permet donc une analyse efficace des chevaux de Troie puisqu’elle détecte les comportements anormaux des programmes.

Sandboxing :

Cette technique permet d’exécuter des logiciels malveillants dans un environnement isolé et contrôlé appelé « sandbox ». Cette méthode est utilisée pour tester des logiciels (vérifier qu’ils ne comportent pas de risques pour le système) et analyser les comportements potentiellement malveillants de certains programmes. Cette méthode est notamment utile pour la création de profils comportemental de virus qui ont été découvert pour la première fois et ces profils vont être utilisés pour l’analyse comportemental. La sandbox est un environnement virtuel qui simule le système d’exploitation. Les activités des programmes présent dans cette sandbox peuvent être surveillé, donc la détection d’actions malveillantes peut vite être détecté par les experts.

Nouveaux défis dans la détection des virus : (2 minutes)

Virus polymorphe et métamorphe :

Un virus polymorphe modifie certaines parties de son code non essentielle à son exécution chaque fois qu’il se réplique. Cela trompe donc les systèmes de détections qui se basent sur des signatures. Ces virus peuvent être détectés car ils suivent un cycle de mutations répétitives.

Un virus métamorphe peut modifier complètement son code à chaque fois qu'il se propage (tout en conservant la même fonctionnalité malveillante). Ils utilisent des algorithmes complexes de mutation pour éviter les détections ce qui les rendent très difficile à détecté (il n'y a pas de signature stable).

Limites des antivirus actuels face aux menaces de plus en plus sophistiqués :

Les antivirus classiques reposent souvent sur l'utilisation des bases de signatures et règles heuristiques.

Signatures : Chaque nouvelle menace nécessite une mise à jour de la base de données ; les attaques inconnus (appelés zero-day) peuvent donc contourner cette identification. Les virus polymorphes et métamorphes également (comme dit précédemment). Les virus sans fichiers (exécuté dans la ram) n'ont pas de signatures.

Règles heuristiques : Les attaquants peuvent concevoir des malwares en évitant les comportements suspectés par les heuristiques.

Analyse comportementale : Les menaces modernes adaptent leurs comportements pour paraître légitimes et échapper aux analyses.

Rôle de l'intelligence artificiel dans les antivirus modernes :

Par exemple l'IA, couplée au sandboxing, peut exécuter et observer automatiquement les fichiers dans un environnement sécurisé, en analysant les comportements sans intervention humaine et pourrait devenir plus efficace qu'une intervention humaine.

L'apprentissage automatique permet aux systèmes de sécurité d'apprendre des motifs de comportement inhabituel à partir de données historiques. Ces comportements inhabituels vont servir à augmenter l'efficacité de l'analyse comportementale et de l'analyse heuristique (en connaissant d'avantage de comportements suspects).

Conclusion : (1 minute)

Pour conclure, nous avons vu qu'il existe beaucoup de types de virus et qu'il est nécessaire d'utiliser différents types d'identifications afin de

détecter efficacement les malwares. En combinant ces identifications on obtient donc un antivirus puissant. Malgré cela, les menaces évoluent et des virus de plus en plus performants voient le jour comme des virus polymorphes ou métamorphes. Il faut donc redoubler d'effort afin de concevoir des antivirus encore plus performants et ce notamment en utilisant l'intelligence artificielle et le machine learning pour détecter les comportements suspects de manière encore plus efficace.