33 suites de sécurité et une défense solide contre les ransomwares et les voleurs de données

Dans les médias, la liste des entreprises, universités, hôpitaux ou administrations victimes de cyberattaques est de plus en plus longue.
Pour contrer ces attaques efficacement, les suites de sécurité classiques ou solutions pour entreprises doivent combiner leurs techniques de défense.
Le test Advanced Threat Protection montre dans quelle mesure ces produits mis à l'épreuve dans 10 scénarios réels sont performants.
Lors du test actuel, la mission des solutions de protection était de protéger les systèmes Windows contre les ransomwares et les voleurs de données.
Lors de ces attaques, les cybercriminels ont recours aux techniques « DNS TXT Record », et utilisent des programmes malveillants programmés en Rust et des connexions cryptées via HTTPS.

33 produits soumis au test ATP –

capacité de protection contre les voleurs de données et les ransomwares mise à l'épreuve dans le test Advanced Threat Protection

Les autorités comme Interpol, le FBI et les services de police nationaux coopèrent efficacement et ont quelques succès à leur actif.
Ainsi, certains groupes APT comme HIVE, Emotet ou QBot ont été démantelés, mais leurs programmes malveillants et leurs codes circulent encore.
Ceci incite d'autres groupes à modifier des programmes malveillants ou à en développer de nouveaux.
Et une autre variante consiste à utiliser des techniques supplémentaires.

Lors du test actuel, le laboratoire d'AV-TEST a analysé 5 attaques avec des ransomwares et 5 attaques avec des voleurs de données dans 10 scénarios réels.

Pour attaquer, les cybercriminels utilisent parfois la technique « DNS TXT Record » ou ont recours à des connexions cryptées via HTTPS.
Certains programmes malveillants sont codés en Rust, un langage de programmation relativement nouveau.
L'avantage pour les attaquants : Rust est extrêmement rapide et permet le déroulement de plusieurs événements en parallèle.
Toutefois, le plus grand avantage est que les programmes malveillants codés en Rust peuvent échapper à l'analyse statique de nombreux systèmes de détection.
C'est pourquoi le test actuel avec sa détection dynamique et son système de défense est si important.

Techniques d'attaque et programmation dans Rust

La technique d'attaque utilisée « DNS TXT Record » peut se résumer ainsi : avec l'outil DNS Lookup, Windows offre la possibilité de consulter les informations textuelles d'un domaine.
Les attaquants en profitent : ils lancent l'attaque puis consultent un DNS TXT Record via PowerShell.
Celui-ci ne contient toutefois aucune information, mais une autre ligne de commande qui est transmise et exécutée.
Par ce biais, les cybercriminels essaient de contourner la détection d'un logiciel de sécurité.

La deuxième technique, c'est l'utilisation d'HTTPS.
Le protocole de transfert hypertextuel sécurisé (Hypertext Transfer Protocol Secure) protège une connexion des écoutes, mais aussi des manipulations.
Les attaquants utilisent cette connexion directe protégée pour empêcher un logiciel de protection d'analyser le contenu.
Toutefois, les systèmes de protection n'ont en fait aucun problème à ouvrir cette connexion, à l'analyser et à la réacheminer.
Encore faut-il que cette fonction soit utilisée.
Or, les attaquants misent sur le fait que cette fonction de protection n'est pas utilisée.
Une analyse de Watchguard fin 2022 a montré que plus de 80 pour cent des attaques enregistrées ont été cryptées via HTTPS.

En juillet et août 2023, le laboratoire d'AV-TEST a testé dans 10 scénarios réels la capacité de défense de 16 suites antivirus pour particuliers et de 17 solutions de protection des points de terminaison pour entreprises sous Windows 10 Professional.

Test ATP : logiciels de sécurité pour utilisateurs particuliers

Neutralisés : Les malwares attaquant dans les scénarios du test, composés de ransomwares et de voleurs de données, ont été repoussés par les 16 suites de sécurité sous Windows destinées aux utilisateurs particuliers

1

Test ATP : logiciels de sécurité pour utilisateurs particuliers

2

Test ATP : logiciels de sécurité pour entreprises

Technique des voleurs de données et des ransomwares

Tous les produits de sécurité combinent à la détection et à la défense diverses techniques dynamiques comme l'EDR – Endpoint Detection & Response.
Le déroulement des 10 attaques et les différentes étapes de la défense sont présentés dans les images « Scénario » de 1 à 10 ci-dessous.

Le déroulement d'une attaque dans un test Advanced Threat Protection suit la plupart du temps le même modèle : un courriel d'hameçonnage contenant une pièce jointe dangereuse atterrit sur un système Windows.
C'est à ce moment que les systèmes de défense détectent l'attaquant soit immédiatement, soit dès qu'il s'active.
Dans les graphiques, ce résultat est confirmé par un champ vert sous « Initial Access » ou « Execution ».
Si tel est le cas, l'attaque est d'ores et déjà neutralisée.

Dans le cas contraire, les attaquants se mettent au travail : les voleurs de données collectent des informations sur les données et les « exfiltrent » ensuite sur un serveur C2. Le ransomware collecte certes aussi des informations, mais n'envoie en général qu'une liste de fichiers de tous les disques durs au serveur C2.
Le cryptage des données et le renommage de fichiers sont ensuite lancés.
Une fois le cryptage effectué, un fichier texte s'affiche sur l'ordinateur pour informer de l'attaque et demander une rançon.

Le laboratoire attribue des points pour chaque étape d'attaque marquante détectée.
Cela représente jusqu'à 4 points pour les voleurs de données et jusqu'à 3 points pour les ransomwares.
La note maximale du score de protection se situe donc à 20 points pour les voleurs de données plus 15 points au maximum pour les ransomwares.
Au total, le laboratoire attribue donc jusqu'à 35 points.

Une explication plus détaillée des tableaux évaluatifs et des différents codes couleur sous forme de feu de signalisation se trouve dans l'article « Test et étude : les logiciels de sécurité sont-ils efficaces contre les ransomwares actuels sous Windows 11 ? ».

Les 10 scénarios utilisés pour le test

Tous les scénarios d'attaque sont documentés selon la norme de la base de données MITRE ATT&CK.
Les différentes sous-rubriques, par ex. « T1566.001 », correspondent dans la base de données Mitre à « Techniques » sous le point « Phishing: Spearphishing Attachment ». Ainsi, chaque étape du test est définie entre les spécialistes et peut être mieux retracée. De plus, toutes les techniques d'attaque sont expliquées, ainsi que la manière dont les logiciels malveillants opèrent.

01

Test ATP sur les produits pour particuliers

Au total, 16 produits de sécurité pour utilisateurs particuliers ont été soumis au test Advanced Threat Protection (ATP) en juillet et en août 2023.
Il s'agit des produits des fabricants suivants : AhnLab, Avast, AVG, Avira, Bitdefender, F-Secure, Kaspersky, Malwarebytes, McAfee, Microsoft, Microworld, Norton, Panda, PC Matic, Protected.net et Trend Micro.

Tous les produits ont repoussé les attaques de manière infaillible dans les 10 scénarios. Les techniques « DNS TXT Record » ou les connexions chiffrées utilisées par les attaquants n'ont pas servi à grand-chose, tout comme le codage du programme malveillant en langage de programmation Rust.
Chaque produit a donc inscrit les 35 points maximum à son score de protection.

Tous les produits pour utilisateurs finaux se voient attribuer le certificat « Advanced Certified » puisqu'ils ont atteint au minimum 75 pour cent des 35 points (soit 26,3 points) comme score de protection.

Presque tous les produits offrent une défense infaillible

L'actuel test Advanced Threat Protection réalisé en juillet-août présente vraiment une particularité. 32 produits sur les 33 testés, qu'ils soient destinés aux particuliers ou aux entreprises ont réalisé un sans-faute à toutes les épreuves du test, décrochant ainsi le score maximal de 35 points.

Dans les 10 scénarios du test, les attaquants ont misé sur les techniques les plus récentes telles que DNS TXT Record, connexions cryptées ou langage de programmation Rust.
Or, toutes les techniques sont connues des programmes de protection qui ont réagi en conséquence, avec une détection et une défense efficaces.
En résumé : une performance presque parfaite.

Particuliers 08/2023

Microsoft

Defender Antivirus (Consumer)

AV-TEST CERTIFIED ADVANCED

eScan™ Enterprise Security

eScan Internet Security Suite

AV-TEST CERTIFIED ADVANCED

Solutions pour Entreprises 08/2023

Avast

Ultimate Business Security

Bitdefender

Endpoint Security (Ultra)

Symantec
A Division of Broadcom

Endpoint Security Complete

Elements Endpoint Protection

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231031
"C'est ensemble qu'on avance"