Protection avancée contre les menaces contre les derniers voleurs de données et techniques de ransomware

NDLR: les tableaux ci-bas sont des captures d'écran. Pour les activer, cliquer le lien suivant:

Protection avancée contre les menaces contre les derniers voleurs de données et techniques de ransomware (av-test.org)

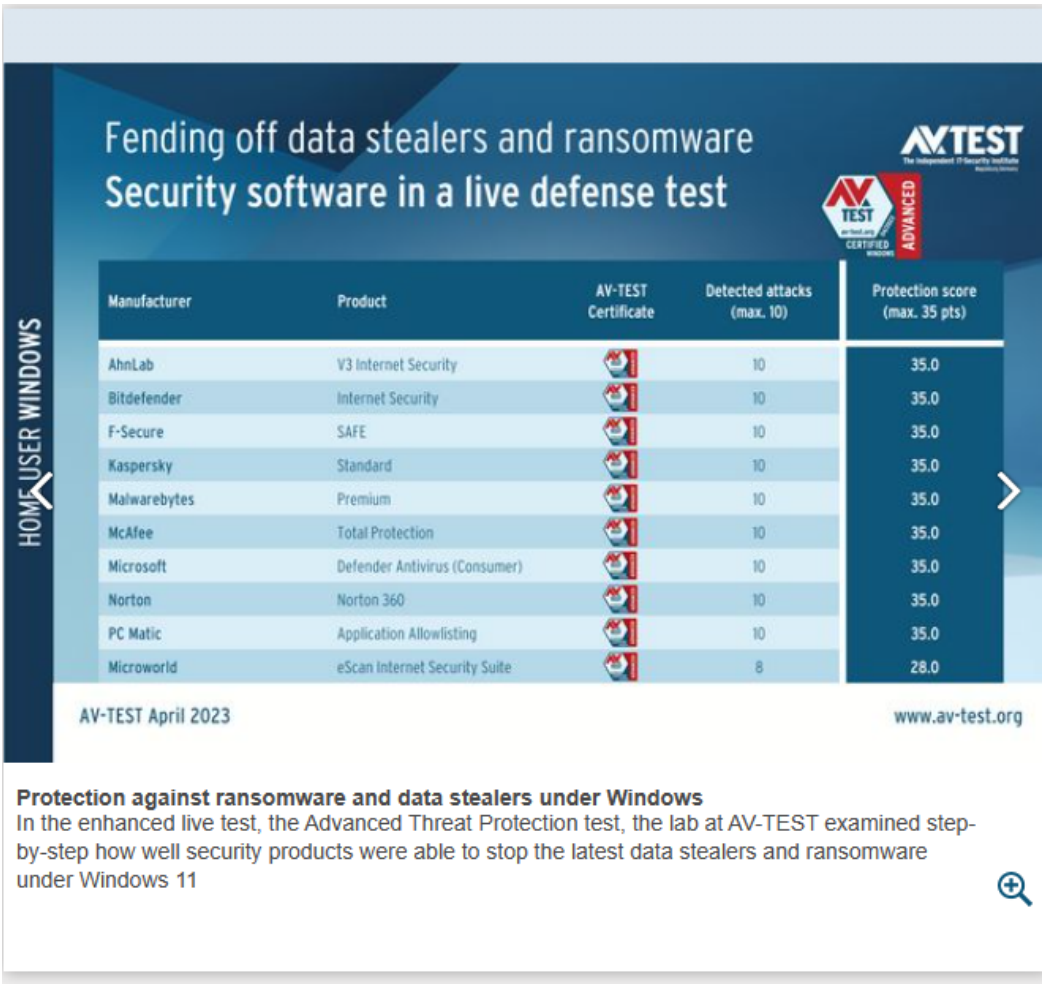
Les solutions de protection pour les PC Windows grand public ou les postes de travail d'entreprise nécessitent la meilleure protection contre les techniques d'attaque les plus récentes.
Le laboratoire d'AV-TEST a examiné un total de 25 produits de sécurité sous Windows 11 en termes de détection et de repousse la nouvelle technique d'attaque « Inline Execute Assembly » contre les voleurs de données et les ransomwares.
Le test Advanced Threat Protection fournit un aperçu clair des produits qui protègent efficacement contre les menaces les plus récentes et de ceux qui ne le font pas.

Vous n'avez pas besoin d'être un spécialiste de la sécurité pour savoir que la cybermenace a considérablement augmenté au cours des dernières années.
Les attaques contre les systèmes Windows, le vol ultérieur de données ou le cryptage des données et le chantage pour la divulgation des données sont malheureusement une réalité courante de la vie.
C'est pourquoi il est important que les produits de sécurité destinés aux utilisateurs grand public ou aux utilisateurs professionnels soient toujours à jour avec la technologie et capables non seulement de détecter mais aussi de contrecarrer les attaques les plus insidieuses.
Le test Advanced Threat Protection est conçu pour faire exactement cela avec 25 produits de sécurité sous Windows 11.
Le laboratoire a effectué l'évaluation en mars et avril 2023 et a maintenant publié les données complètes.

25 solutions de protection contre les voleurs de données et les ransomwares

Parmi les armes d'attaque les plus couramment utilisées figurent les voleurs de données et les rançongiciels. Ils sont similaires dans les phases initiales des attaques.
Dès qu'il est sur le système, le voleur de données recueille des informations sur les fichiers importants et les transmet à l'attaquant.
Bien que les rançongiciels surveillent également les fichiers importants, ils le font dans l'intention de les chiffrer par la suite.

Dans cette évaluation, les testeurs recherchaient une technique d'attaque particulière : le « Inline Execute Assembly ».
En termes très simples, ce qui est autrement un processus Windows très inoffensif est abusé dans un environnement d'exécution .Net.
Un processus est isolé, infecté par un code malveillant, puis lancé.
En outre, l'interface d'analyse anti-programme malveillant (AMSI) est contournée à l'aide d'un contournement AMSI.
Il s'agit de l'API d'analyse fournie par Microsoft, qui est utilisée par les solutions antivirus. De plus, le suivi d'évènements intégré à Windows est désactivé afin que la routine de processus ne puisse plus être tracée.
Une fois que tout cela est réussi, le malware a carte blanche.
Cependant, une bonne solution de sécurité peut toujours empêcher d'autres actions, telles que le siphonnage ou le cryptage des données.



Protection against ransomware and data stealers under Windows
In the enhanced live test, the Advanced Threat Protection test, the lab at AV-TEST examined step-by-step how well security products were able to stop the latest data stealers and ransomware under Windows 11

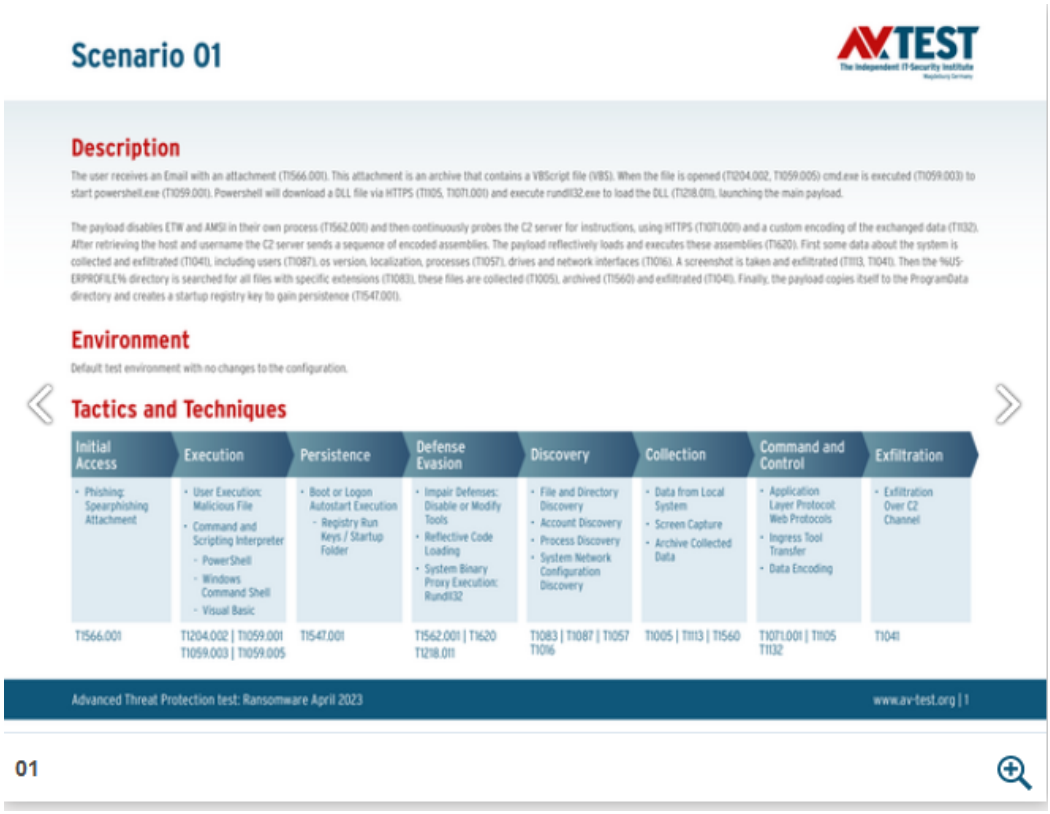
Dans ce test, le laboratoire a envoyé 5 échantillons de voleurs de données et 5 échantillons de ransomware via un courriel de spearphishing aux systèmes de test.
Par la suite, ils se sont d'abord retrouvés sur le système et sont devenus actifs à l'étape suivante.
Déjà dans ces deux étapes, de nombreux produits ont détecté le danger et repoussé l'attaque.
Si ce n'est pas le cas, les voleurs de données sont en mesure de recueillir des informations sur les données qu'ils « exfiltrent » vers un serveur C2.
Le ransomware recueille également des informations, mais avec l'intention d'envoyer une liste de fichiers au serveur C2 pendant le lancement du cryptage des données.
Les graphiques de 10 scénarios montrent les routines d'attaque.
Les cas 1 à 5 décrivent l'attaque des voleurs de données et les cas 6 à 10 les attaques de ransomware.

Encore une autre particularité de ce test : le laboratoire a attribué des points pour la détection d'étapes d'attaque significatives.
Pour des étapes défensives réussies, cela signifiait jusqu'à 4 points pour chaque voleur de données et jusqu'à 3 points pour les ransomwares.
Ainsi, le meilleur score de protection possible dans ce test était de 35 points.

Pour trouver une explication plus détaillée des tableaux d'évaluation et des codes de couleur individuels dans le système de feux tricolores, veuillez également consulter l'article « Test et étude: Les solutions de sécurité arrêtent-elles les ransomwares actuels sous Windows 11? ».

Les 10 scénarios de test

Tous les scénarios d'attaque sont documentés selon la norme de la base de données MITRE ATT&CK.
Les différentes sous-techniques, par exemple « T1566.001 », sont répertoriées dans la base de données MITRE pour « Techniques » sous « Phishing: Spearphishing Attachment ».
Chaque étape de test est ainsi définie par les experts et peut être logiquement comprise. En outre, toutes les techniques d'attaque sont expliquées, ainsi que le succès du logiciel malveillant.



Test avancé : protection des utilisateurs grand public

Un total de 10 produits pour les utilisateurs grand public ont été confrontés dans le test Advanced Threat Protection sous Windows 11.
Les produits concernés provenaient d'AhnLab, Bitdefender, F-Secure, Kaspersky, Malwarebytes, McAfee, Microsoft, Microworld, Norton et PC Matic.

À l'exception de Microworld, tous les fournisseurs de produits de sécurité ont pu obtenir un résultat parfait.
Tous les scénarios ont été étouffés dans l'œuf.
Les systèmes n'ont jamais été mis en danger.
Chaque produit a reçu 35 points sur son score de protection pour cette performance.

Microworld avait un problème dans chaque scénario avec un voleur de données et un ransomware, en ce sens qu'il ne détectait rien.
Les deux attaquants ont recueilli ou chiffré les données sans être dérangés.
C'est pourquoi Microworld a eu respectivement 4 points et 3 points enlevés dans un cas. Cela a abouti à un total de 28 points pour le score de protection.

Chaque produit destiné aux utilisateurs grand public obtenant un score de protection de 75% des 35 points (soit 26,3 points) a reçu le certificat « Advanced Certified ».
Tous les produits de ce test ont reçu le certificat.

Test avancé : protection des utilisateurs professionnels

Les 15 produits destinés aux entreprises dans le test Advanced Threat Protection pour les terminaux sous Windows 11 provenaient d'Acronis, AhnLab, Bitdefender (avec 2 versions), Check Point, Kaspersky (avec 2 versions), Malwarebytes, Microsoft, Seqrite, Symantec, Trellix, VMware, WithSecure et Xcitium.

Le groupe le plus important avec 12 produits a réussi le test avec les meilleurs scores, chacun recevant les 35 points complets pour le score de protection : Acronis, AhnLab, Bitdefender Version Ultra, Check Point, Kaspersky (les deux versions), Malwarebytes, Microsoft, Seqrite, Symantec, WithSecure et Xcitium.

Bien que Bitdefender Endpoint Security ait détecté les attaquants dans les 10 scénarios de test, il n'a pas été en mesure d'arrêter complètement les attaquants dans 2 cas impliquant des ransomwares.
Il a exécuté plusieurs contre-mesures, mais à la fin, un cryptage partiel des fichiers individuels s'est produit dans les deux cas.

Cela a conduit à une déduction de points.
Le résultat était 33 points sur 35 possibles pour le score de protection.

Trellix a fourni des performances impeccables dans 9 cas, mais a rencontré d'énormes problèmes avec l'un des voleurs de données.
Le produit était en fait capable de détecter l'attaquant, mais était impuissant à faire quoi que ce soit à ce sujet.
Dans ce cas, seulement 0,5 point sur 4 a été atteint.
Le résultat du test était un score de protection de 31,5 points.

Le produit ayant rencontré les plus grandes difficultés lors du test provenait de VMware.
Il n'a pu ni détecter ni arrêter un voleur de données, ce qui a permis à l'attaque de se dérouler.
Cela a entraîné un décollage complet de 4 points et, à la fin, un score de protection de 31 points.

Chaque produit utilisateur d'entreprise obtenant un score de protection de 75 % des 35 points (soit 26,3 points) a reçu le certificat « Advanced Approved Endpoint Protection ». Tous les produits ont reçu le certificat, à l'exception d'Acronis.
Le produit a passé le test sans erreur, mais AV-TEST ne certifie que les produits qui obtiennent la certification lors des tests mensuels réguliers et qui remplissent tous leurs critères.

Qui a peur des voleurs de données et des ransomwares

Le test actuel Advanced Threat Protection va bien au-delà des tests de détection classiques.
Se tenir au courant des derniers échantillons de voleurs de données et de ransomwares avec la technique d'attaque déployée « Inline Execute Assembly » représente un défi de taille pour de nombreuses solutions de sécurité.
C'est pourquoi le dernier résultat est d'autant plus favorable, où la plupart des produits examinés ont fourni une défense sans erreur des systèmes Windows: 9 des 10 produits pour les utilisateurs grand public et 12 des 15 solutions pour les utilisateurs professionnels.

Les fabricants restants avec leurs produits doivent apprendre de leurs erreurs et devenir encore meilleurs.
Au moins, il n'y a eu que des erreurs et aucune défaillance catastrophique.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230727
"C'est ensemble qu'on avance"