



COMMUNIQUE DE PRESSE

Sécurité informatique : l'inefficacité des antivirus confirmée

Des experts et passionnés de la sécurité informatique offensive ont réussi à contourner les 15 antivirus les plus vendus dans le monde.

Le test avait lieu dans le cadre de la conférence annuelle de sécurité iAWACS organisée par l'école d'ingénieurs ESIEA.

Paris, le 11 mai 2010 - Au cours de la deuxième édition de la conférence iAWACS dédiée à la sécurité informatique opérationnelle, des spécialistes français et internationaux ont de nouveau démontré la très grande vulnérabilité des principaux antivirus présents sur le marché.

15 antivirus contournés

Il aura fallu moins d'une après-midi aux spécialistes de la sécurité informatique -experts comme étudiants- réunis par l'ESIEA à l'occasion de la nouvelle édition d'iAWACS pour contourner les 15 antivirus les plus vendus dans le monde.

Cette expérience souligne la facilité avec laquelle tous les logiciels antivirus de référence peuvent être contournés : « *Si quasiment toutes les attaques se sont révélées efficaces, certaines sont malheureusement d'une simplicité alarmante* », observe Eric Filiol, responsable de la conférence iAWACS, et Directeur de la recherche de l'ESIEA (Ecole Supérieure d'Informatique Electronique Automatique). « *L'un des participants, avec un simple code de trois lignes, reprenant une technique vieille de 10 ans a réussi à contourner tous les antivirus. Cela prouve que la plupart des éditeurs ne font pas de veille technologique et scientifique suffisante. En matière de R&D, les plus connus du grand public ne sont d'ailleurs pas toujours les plus vertueux...* », précise l'initiateur du test.



Résultats test antivirus ESIEA

Logiciel antivirus	Attaque n°1	Attaque n°2	Attaque n°3	Attaque n°4	Attaque n°5	Attaque n°6	Attaque n°7
Avast (version gratuite)	Echec	Déte�té	Echec	Echec	Echec	Echec	Echec
AVG	Echec	Déte�té	Echec	Echec	Echec	Echec	Echec
Avira	Echec	Déte�té	Echec	Echec	Echec	Echec	Echec
BitDefender	Echec	Déte�té	Déte�té	Echec	Echec	Echec	Echec
DrWeb	Echec	Déte�té	Echec	Echec	Echec	Echec	
F-Secure	Echec	Déte�té	Déte�té	Echec	Echec	Echec	Echec
GData	Echec	Déte�té	Echec	Echec	Déte�té*	Echec	Echec
Kasperky	Echec	Déte�té	Echec	Echec	Echec	Echec	(1)
McAfee	Echec	Déte�té	Echec	Echec	Echec	Echec	Echec
MSE (Microsoft)	Echec	Déte�té	Echec	Echec	Echec	Echec	Echec
NOD 32	Echec	Déte�té	Echec	Echec	Echec	Echec	Echec
Norton Symantec	Echec	Déte�té	Echec	Echec	Echec	Echec	Echec
Safe 'n' Sec	Echec	Déte�té	Echec	Echec	Echec	Echec	Echec
Sophos	Echec	Déte�té	Echec	Echec	Echec	Echec	(2)
Trend Micro	Echec	Déte�té	Echec	Echec	Déte�té	Echec	Echec

Déte té : le logiciel antivirus a déte té le programme malveillant et a empê é l'attaque.

Echec : le logiciel antivirus n'a pas déte té l'attaque. Le système informatique est durablement affecté.

*Le logiciel antivirus a déte té le programme malveillant mais a laissé le choix à l'utilisateur d'autoriser ou non la poursuite de son exécution.

(1) : 4 attaques ont été lancées :
 - 1^{er} : échec de l'antivirus
 - 2^e et 3^e : programme malveillant déte té par l'antivirus
 - 4^e : échec de l'antivirus

(2) : 3 attaques ont été lancées :
 - 1^{er} et 2^e : programme malveillant déte té par l'antivirus
 - 3^e : échec de l'antivirus



iAWACS

*International Alternative Workshop
on Aggressive Computing and Security*
7-9 mai 2010

Conditions de test draconiennes

Pour parer aux critiques des éditeurs, les conditions du test étaient particulièrement restrictives pour l'attaquant : les ordinateurs mis à disposition des participants étaient équipés de Windows 7 en mode utilisateur (pas de droit administrateur) avec les applications courantes installées¹ (suite Microsoft, OpenOffice Suite, logiciel lecture pdf ...). Chaque code de contournement présenté devait passer la barrière de l'antivirus, en mode non exécuté (scan à la demande), puis exécuté (scan à l'accès) et permettre ensuite une attaque affectant durablement le système.

Achetés de manière anonyme en magasin ou sur internet peu avant le test (ou directement téléchargé dans le cas d'Avast), tous les logiciels testés correspondent à ceux utilisés couramment par les particuliers et professionnels.

Vulnérabilité face aux codes inconnus

« L'objet du test n'est pas de donner aux hackers les dernières « astuces » pour pénétrer de façon frauduleuse des systèmes informatiques », rappelle Anthony Desnos, enseignant chercheur à l'ESIEA. « Nous apportons simplement la preuve que la plupart des antivirus ne sont pas en mesure de détecter pro-activement les programmes malveillants nouvellement créés. Ils sont uniquement capables de repérer les codes déjà connus. Et encore..., un nombre important de techniques malveillantes déjà publiées (par des pirates, auteurs de programmes malveillants, chercheurs...) ne sont toujours pas prises en compte alors qu'elles représentent de véritables menaces. »

Aucun des codes mis en œuvre par les participants n'est divulgué au grand public. Ces informations sont uniquement communiquées au CERT-A (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), organisme dépendant des services du Premier Ministre. "La loi française interdit de distribuer des armes informatiques, de surcroît indétectables, a des entités étrangères (il n'existe aucun antivirus français)" affirme Eric Filiol.

¹ Conditions correspondant à l'utilisation recommandée à la fois par Microsoft et les éditeurs d'antivirus.



iAWACS
*International Alternative Workshop
on Aggressive Computing and Security*
7-9 mai 2010

« Dans un contexte évoluant vers la prise de conscience de la guerre informatique, il est logique que l'Etat soit le seul maître du jeu. ». Conscient de la primauté des intérêts de l'Etat en matière de guerre informatique, tous les participants ont d'ailleurs signé une attestation de non divulgation (NDA). Seul un résumé technique des résultats est disponible sur le site web d'iAWACS 2010 (www.esiea-recherche.eu/data/iawacs2010/pwn2kill/pwn2killdebrief.pdf)

Un jury de professionnels a désigné les 3 attaques lauréates

Le jury du test était composé de journalistes de la presse informatique et de deux personnalités de la communauté scientifique :

- Christophe Devine (société SOGETI), Président du jury,
- Marc Olanie et Solange Belkhatat-Fuchs (CNIS Mag),
- Christophe Auffray (Zdnet.fr),
- Dominique Ciupa (Mag-Securs),
- Vincent Guyot (Enseignant chercheur à l'ESIEA - Spécialiste des cartes à puces).

Le jury avait pour rôle d'enregistrer les résultats, de décider de leur validité et de sélectionner les trois attaques les plus efficaces en considérant également des critères d'élégance et de simplicité.

Les trois lauréats sont :

- 1^{er} prix : Guillaume Fahrner (Mastère Spécialisé - Télécom Bretagne)
- 2^e prix : Jonathan Dechaux, Romain Griveau, Jean-Paul Fizaine et Kenza Jaafar (étudiants en 4^{ème} année de l'ESIEA)
- 3^e prix : Baptiste David (Etudiant en 1^{ère} année de l'ESIEA)

« Au-delà de ce test, dans le contexte émergent de guerre informatique, ces résultats signifient que nos systèmes et réseaux sont totalement démunis si aucune mesure organisationnelle ne vient compenser les graves lacunes des produits sensés nous protéger » indique Eric Filiol, Directeur du Laboratoire de Cryptologie et Virologie Opérationnelles de l'ESIEA.



iAWACS
*International Alternative Workshop
on Aggressive Computing and Security*
7-9 mai 2010

« Il est temps que les utilisateurs et les décideurs comprennent que la lutte contre les programmes malveillants ne se résume pas à déployer un produit antiviral. La sécurité informatique repose avant tout sur une sensibilisation des utilisateurs aux risques et aux moyens simples qu'ils ont de les parer » précise-t-il.

iAWACS : la vision de l'agresseur informatique

Organisé par deux des laboratoires de recherche de l'ESIEA (*Cryptologie et Virologie Opérationnelles* et *Sécurité de l'Information & des Systèmes*), la conférence iAWACS a rassemblé une nouvelle fois en un même lieu des spécialistes de la sécurité dite "offensive".

Pendant 3 jours, des conférences et débats ont permis une large évaluation des principales politiques et techniques en la matière.

Tous les participants avaient un point commun : avoir développé des études sur les attaques informatiques en privilégiant la vision opérationnelle de l'attaquant sur les approches théoriques.

Alors que dans les conférences "classiques", les études non conventionnelles sont la plupart du temps rejetées, iAWACS permet aux chercheurs et aux spécialistes de présenter leurs travaux "alternatifs".

Traditionnellement iAWACS accueille un grand nombre d'étudiants, notamment de Mastère (Bac+6). « C'est la marque de fabrique de nos mastères en sécurité (SI&S et N&IS) que d'offrir une vision riche, allant vraiment du code au réseau, avec les meilleurs spécialistes nationaux et internationaux du domaine, et placée sous le double signe de l'opérationnel et de la compréhension fine des concepts » souligne Robert Erra, responsable scientifique de ces deux mastères réputés. « Pour preuve, notre capacité d'accueil étant limitée (18 places pour le mastère SI&S et 24 pour le mastère anglophone N&IS), nous exportons sans problème une partie de cette vision de l'attaquant, laquelle est aussi très appréciée par les élèves d'autres mastères (en particulier Telecom Bretagne et Supelec) où Eric intervient en virologie et en cryptologie. »



iAWACS
*International Alternative Workshop
on Aggressive Computing and Security*
7-9 mai 2010

Des sujets aussi divers que les techniques de cryptanalyse, la cryptographie malicieuse, les techniques avancées de codes malveillants ou les techniques de cyberguerre ont été abordés. L'ensemble des travaux présentés ont été sélectionnés selon leur intérêt scientifique, leur originalité, et leur qualité opérationnelle. Les auditeurs ont pu eux-mêmes manipuler des techniques innovantes au cours de deux ateliers pratiques : l'un sur la sensibilisation aux failles de programmation des cartes à puces et l'autre sur la technologie du courant porteur en ligne.

« *iAWACS a pleinement rempli son but* » conclut Anthony Desnos. « *Celui de contribuer à offrir la meilleure réponse aux nouvelles exigences des entreprises et des Etats face aux attaques des hackers, crackers et autres pirates du web.* ».

La prochaine édition d'iAWACS se tiendra sur le campus Lavallois de l'ESIEA fin 2010. Toujours avec la vision de l'attaquant, le concours concernera cette fois la **sécurité des principaux Firewalls** du marché.

Retrouver toutes les informations sur iAWACS 2010 et le test de contournement d'antivirus sur : http://www.esiea-recherche.eu/iawacs_2010.html

▪ **Disponible pour des interviews :**

Eric FILIOL (Directeur de la recherche du Groupe ESIEA, Directeur du laboratoire de cryptologie et virologie opérationnelles et organisateur de la conférence iAWACS).

▪ **A propos du laboratoire de Cryptologie et Virologie Opérationnelles de l'ESIEA**

Grâce à l'intégration d'un laboratoire spécialisé dans la sécurité informatique, l'ESIEA est devenu un acteur incontournable dans ce domaine. Dirigé par Eric FILIOL, le laboratoire de cryptologie et virologie opérationnelles est un des 5 pôles de recherche de l'ESIEA. D'origine militaire, il rassemble une équipe d'experts composée d'un directeur, d'un chercheur, de deux ingénieurs de recherche auxquels s'ajoutent quatre doctorants.

Contact presse : Philippe Hériard
Agence Droit Devant
Tél. : +33(0)1 39 53 53 33 – Port. : +33(0)6 12 46 21 38
heriard@droitdevant.fr



iAWACS
International Alternative Workshop
on Aggressive Computing and Security
7-9 mai 2010

- **A propos du Laboratoire de Sécurité de l'Information & des Systèmes (SI&S)**

Les projets du pôle SI&S concernent aussi bien la recherche fondamentale que la recherche appliquée au côté d'entreprises privées et d'organismes nationaux. Le laboratoire travaille par exemple sur le vol ou le détournement d'informations, fatals pour une entreprise ou une organisation.

L'équipe dirigé par Robert Erra a en charge, de surcroît, le Mastère spécialisé SI&S et son équivalent enseigné en anglais le Mastère N&IS (Network and information Security).

- **A propos du Groupe ESIEA**

Le Groupe ESIEA est composé d'une Grande Ecole d'Ingénieurs en informatique électronique et automatique « **ESIEA** », de cinq pôles et laboratoires regroupés sous la dénomination « **ESIEA recherche** », de l'Ecole Supérieure d'ingénierie informatique « **IN'TECH INFO** », d'un centre de formation continue « **Institut ESIEA** » et du Centre de Formation et d'Apprentissage Informatique Télécom et Électronique « **CFA-ITE** ».

- **A propos de l'ESIEA www.esiea.fr**

Grande Ecole d'ingénieurs reconnue par l'État, l'Ecole Supérieure d'Informatique Electronique Automatique a été fondée à Paris en 1958. L'ESIEA est membre de la CGE (Conférence des Grandes Écoles) et délivre un diplôme d'ingénieur (grade Master) habilité par la CTI (Commission des Titres d'Ingénieur).

En interaction permanente avec le monde de l'entreprise, l'ESIEA est une école généraliste liée aux nouvelles technologies et basée sur un haut niveau technico-scientifique avec des enseignements en formation humaine et management. L'école compte plus de 1000 étudiants sur deux sites (Paris et Laval). Elle est gérée bénévolement par l'association de ses 6.200 anciens élèves qui investissent la totalité des ressources du groupe dans les enseignements et la recherche.

Dès la première année, la recherche est au cœur de la pédagogie de l'ESIEA. Elle se structure autour de 5 laboratoires qui sont autant de pôles d'expertise reconnus dans des domaines de pointe : Réalité Virtuelle et Système Embarqués ; Sécurité de l'Information et des Systèmes ; Acquisition et Traitement des Images et du Signal ; Cryptologie et Virologie Opérationnelle ; Art et Recherche Numérique.

Contact presse : Philippe Hériard
Agence Droit Devant
Tél. : +33(0)1 39 53 53 33 – Port. : +33(0)6 12 46 21 38
heriard@droitdevant.fr