Dmarc.org : l'initiative Google, Yahoo et Microsoft contre le Phishing
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 31/1/2012 11:30:00

Aux cÃ´tÃ©s de Google, AOL, Yahoo! et Microsoft, **Return Path fonde DMARC.org**, afin de contribuer Ã la protection des consommateurs, des marques et des FAI **contre le phishing**.

Conforme aux spÃ©cifications DMARC, la solution anti-phishing Domain Assurance de Return Path permet aux entreprises de mettre en Å□uvre ces derniÃ¨res avec rapiditÃ© et facilitÃ©

Return Path, leader mondial de la certification des emails et de la gestion de rÃ©putation, annonce quâ□□il fait partie des membres fondateurs de DMARC.org (Domain-based Message Authentication, Reporting and Conformance), un groupe de travail technique ayant pour vocation dâ□□Ã©laborer des standards Internet visant Ã rÃ©duire la menace que reprÃ©sentent les emails frauduleux employant la technique du phishing (Â« hameÃ§onnage Â»). DÃ©veloppant une approche plus sophistiquÃ©e de lâ□□authentification des emails, DMARC publie un cahier des charges visant Ã rÃ©soudre les problÃ©matiques liÃ©es Ã lâ□□adoption rÃ©pandue de technologies dans ce domaine.

Des opÃ©rateurs majeurs de messagerie tels que Google, Yahoo!, AOL et Microsoft sont Ã©galement membres fondateurs du groupe de travail dirigÃ© par Brett McDowell, Senior Manager of Customer Security Initiatives au sein de PayPal, lâ□□une des marques les plus victimes dâ□□usurpation dâ□□identitÃ© (spoofing) Ã travers le monde. La solution anti-phishing Domain Assurance de Return Path est conforme au projet de spÃ©cifications DMARC, permettant ainsi aux entreprises de mettre en Å□uvre ces derniÃ¨res avec rapiditÃ© et facilitÃ©.

Â« *Google collabore avec Return Path depuis plus dâ□□un an dÃ©sormais, afin de fournir Ã ses clients les outils nÃ©cessaires au renforcement de la protection des utilisateurs de Gmail contre le phishing et les autres emails malveillants* Â», souligne **Adam Dawes**, Product Manager au sein de Google. Â« *La vaste expÃ©rience de Return Path place la sociÃ©tÃ© en excellente position pour amÃ©liorer les pratiques dâ□□authentification des expÃ©diteurs de courrier Ã©lectronique et contribuer ainsi Ã Â« faire le mÃ©nage Â» dans ce domaine. Plus important encore, la solution Domain Assurance de Return Path est dâ□□ores et dÃ©jÃ conforme aux spÃ©cifications DMARC, de sorte que les expÃ©diteurs peuvent dÃ¨s Ã prÃ©sent recevoir des donnÃ©es de Google et les visualiser immÃ©diatement avec le concours de Return Path.* Â»

Favoriser la mise en Å□uvre dâ□□un environnement email authentifiÃ© et fiable

Selon de rÃ©centes donnÃ©es de Return Path, les expÃ©diteurs continuent dâ□□Ã©prouver des difficultÃ©s en matiÃ¨re dâ□□authentification de leurs emails, ce qui laisse les marques vulnÃ©rables aux attaques de phishing. Un rapport de lâ□□Anti-Phishing Working Group (APWG)

rÃ©vÃ¨le que plus de 300 marques sont chaque mois dÃ©tournÃ©es par des Â« hameÃ§onneurs Â», engendrant lâ□□Ã©rosion de la confiance dans la messagerie Ã©lectronique dans des secteurs aussi divers que les services financiers, lâ□□e-commerce, les services de paiement, les jeux, les enchÃ¨res en ligne ou encore les rÃ©seaux sociaux. Bien que les marques soient encouragÃ©es Ã appliquer les meilleures pratiques pour leurs envois dâ□□emails, notamment en mettant en Å□uvre les protocoles de dâ□□authentification SPF (Sender Policy Framework) et DKIM (Domain Keys Identified Mail) - deux standards dâ□□authentification qui permettent de vÃ©rifier quâ□□un message est issu dâ□□une source lÃ©gitime, les FAI ne sont pas en mesure de prendre de dÃ©cision tranchÃ©e concernant le blocage dâ□□un email non authentifiÃ© prÃ©tendant provenir dâ□□une marque notoirement victime de spoofing.

Les spÃ©cifications DMARC permettent aux entreprises de toutes tailles dâ□□autoriser les FAI Ã prendre des mesures Ã lâ□□encontre des emails malveillants et non authentifiÃ©s paraissant provenir de marques Ã©tablies. Les donnÃ©es relatives Ã tout flux de messages douteux sont renvoyÃ©es Ã la marque ou Ã un intermÃ©diaire tel que Return Path, permettant ainsi leur vÃ©rification aux fins dâ□□authentification. En instaurant cette boucle de rÃ©troaction entre les FAI et les marques, le dispositif DMARC aide ces derniÃ¨res Ã formuler des instructions indiquant aux FAI de bloquer ou de mettre en quarantaine les messages qui ne sont pas correctement authentifiÃ©s, ce qui procure le cadre nÃ©cessaire pour dÃ©jouer les tentatives de phishing et favoriser la gÃ©nÃ©ralisation dâ□□un Ã©cosystÃ¨me email fiable.

Â« *Lâ□□email a rÃ©volutionnÃ© notre faÃ§on de communiquer. Cependant, les caractÃ©ristiques mÃªmes qui en font lâ□□attrait â□□ lâ□□ouverture, lâ□□interopÃ©rabilitÃ© â□□ le rendent Ã©galement vulnÃ©rables aux actions malveillantes. Le principal atout de DMARC est de sâ□□attaquer aux menaces pour la sÃ©curitÃ© de lâ□□Ã©cosystÃ¨me email et de ses acteurs, sans compromettre son utilitÃ© en tant que moyen de communication* Â», explique **Matt Blumberg**, CEO de **Return Path**. Â« *Return Path est fier dâ□□apporter son active contribution au projet DMARC et nous encourageons les entreprises Ã le mettre en Å□uvre dÃ¨s que possible. Son adoption rapide et rÃ©pandue portera un sÃ©rieux coup Ã la capacitÃ© des auteurs dâ□□escroqueries de perpÃ©trer leurs mÃ©faits par voie dâ□□email.* Â»

Domain Assurance, conforme aux spÃ©cifications DMARC

La conformitÃ© de la solution anti-phishing Domain Assurance de Return Path avec les spÃ©cifications DMARC facilite le dÃ©ploiement desdites rÃ¨gles dâ□□authentification par les entreprises. Sâ□□appuyant sur les donnÃ©es en provenance des FAI, Domain Assurance apporte le degrÃ© dâ□□intelligence, la logique intÃ©grÃ©e et les alertes Ã©voluÃ©es nÃ©cessaires pour signaler tout dÃ©faut de conformitÃ© ou toute usurpation dâ□□identitÃ© susceptible de nuire Ã lâ□□intÃ©gritÃ© dâ□□une marque. Domain Assurance recueille les donnÃ©es transmises par les FAI qui communiquent des rÃ©sultats dâ□□authentification DMARC (ainsi que dâ□□autres sources de donnÃ©es dâ□□authentification pour les FAI nâ□□ayant pas dÃ©ployÃ© DMARC) et en tire des rapports dÃ©taillÃ©s, contenant notamment des informations sur chaque message envoyÃ© au nom dâ□□une marque, quâ□□il soit lÃ©gitime ou pas.

Ces informations permettent notamment aux marques de mieux apprÃ©hender leurs flux dâ□□emails et de dÃ©terminer quels messages ne sont pas authentifiÃ©s correctement mais Ã©galement de mieux cerner les sources des attaques de phishing et de mesurer lâ□□impact potentiel de ces activitÃ©s criminelles ; elles permettent enfin dâ□□Ã©tablir des rÃ¨gles visant Ã bloquer toute future attaque de phishing. GrÃ¢ce Ã son vaste rÃ©seau et Ã ses relations avec Google, Hotmail, Yahoo! et plus de 70 autres FAI partenaires Ã travers le monde, Return Path a accÃ¨s Ã plus de 2,2 milliards de messages par jour, collectant ainsi plus de donnÃ©es de phishing que quiconque dans le secteur, ce qui lui offre la possibilitÃ© dâ□□identifier, de signaler et de bloquer un plus grand nombre dâ□□attaques de ce type. Domain Assurance fait quant Ã lui le lien entre les expÃ©diteurs et leurs FAI, bloquant les emails frauduleux avant quâ□□ils nâ□□atteignent leurs destinataires. Return Path diffuse Ã©galement les URL et les adresses IP Ã©mettant du

phishing auprÃ¨s de sociÃ©tÃ©s tierces spÃ©cialisÃ©es dans la sÃ©curitÃ© et la fermeture de domaines et sites web afin de renforcer la protection contre ces menaces.