SÃ©curitÃ© : Qui se cache derriÃ¨re les cyber-attaques ?
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 3/7/2013 15:00:00

Les experts FireEye ont pu mettre en Ã©vidence les nouvelles mÃ©thodes utilisÃ©es par **les cyber-activistes chinois** du Â« Comment Crew Â»

FireEye Â®, Inc., le spÃ©cialiste de la lutte contre les cyber-attaques de nouvelle gÃ©nÃ©ration, vient de rendre publique une Ã©tude permettant dâidentifier lâorigine des malwares : Â« Fil dâAriane numÃ©rique : les sept indices qui permettent dâidentifier qui se cache derriÃ¨re les cyber-attaques avancÃ©es Â» (Seven Clues To Identifying Whoâs Behind Advanced Cyber Attacks*).

Bien que les cyber-attaques soient de plus en plus sophistiquÃ©es, toutes les Ã©tapes dâune attaque laissent des traces, de lâidentification de la cible jusquâÃ la prise de contrÃ´le. Cette Ã©tude a pour but dâaider les professionnels Ã mieux identifier les hackeurs et Ã mettre en place les protections adÃ©quates pour dÃ©fendre leurs organisations des futures attaques.

Au cours de lâanalyse des mÃ©tadonnÃ©es de diffÃ©rents malwares, les experts FireEye ont dÃ©couvert de nouvelles techniques utilisÃ©es par les hackers, notamment dans le cadre dâattaques Ã©tatiques. Ces techniques, encore inconnues, ont pu Ãªtre identifiÃ©es et attribuÃ©es au groupe militaire chinois connu sous le nom de Â« Comment Crew Â», dont les mÃ©thodes sont dÃ©sormais clairement identifiÃ©es.

Â« *Dans le contexte actuel des malwares de nouvelle gÃ©nÃ©ration, il est essentiel dâidentifier*

lâ□□ennemi afin de dÃ©ployer un plan de protection appropriÃ©, explique Yogi Chandiramani, Director of Systems Engineering Europe chez FireEye.

Il est indispensable de connaÃ®tre les cybercriminels qui ciblent lâ□□entreprise, leurs motivations et leur maniÃ¨re de travailler. Savoir ce quâ□□ils recherchent est dÃ©terminant pour la protection des donnÃ©es et de la propriÃ©tÃ© intellectuelle des organisations. Â»

Une entreprise victime de cyber-attaques, si elle est bien renseignÃ©e sur les mÃ©thodes et objectifs de son agresseur, peut utiliser ces informations Ã plusieurs fins, notamment pour :

â□¢ Anticiper la protection des donnÃ©es sensibles

â□¢ Solliciter une aide supplÃ©mentaire via des ressources internes ou un renforcement du cadre lÃ©gislatif

â□¢ Examiner attentivement les autres vecteurs utilisÃ©s lors de prÃ©cÃ©dentes attaques du mÃªme du type afin de les identifier en amont

Â« *Les hackers se rÃ©vÃ¨lent Ã travers leurs rituels et leur faÃ§on de procÃ©der*, poursuit Yogi Chandiramani. *Sur le modÃ¨le des empreintes digitales, des tests ADN et de lâ□□analyse de fibres qui ont une valeur inestimable dans les enquÃªtes criminelles, relier les Ã©lÃ©ments dâ□□une cyber-attaque permet dâ□□identifier les menaces les plus sophistiquÃ©es, si lâ□□on sait quoi et oÃ¹ chercher.* Â»

*Pour plus dâ□□informations le rapport de Gartner Â« Digital Bread Crumbs: Seven Clues To Identifying Whoâ□□s Behind Advanced Cyber Attacks Â» est disponible en ligne.