Internet : Cyberguerre, Le malware Flame Ã la solde des nations ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 1/6/2012 11:30:00

Depuis lâannonce fracassante du **malware Flame** sur les systÃ¨mes informatiques Iraniens, celui-ci a Ã©tÃ© reconnu comme le virus informatique le plus sophistiquÃ© au monde â redÃ©finissant complÃ¨tement la notion de cyberguerre et d'espionnage

Plus avancÃ© que Stuxnet et Duqu, Flame semble se concentrer sur l'espionnage, et peut activer les systÃ¨mes audio d'un ordinateur pour Ã©couter les appels tÃ©lÃ©phoniques ou autres communications internes. Il peut Ã©galement prendre des screenshots, activer lâenregistrement de la saisie et mÃªme extraire des donnÃ©es de Bluetooth des tÃ©lÃ©phones mobiles compatibles. Encore aujourd'hui, l'Iran a confirmÃ© que le virus de la flamme a attaquÃ© les ordinateurs de hauts fonctionnaires provoquant une Â«massiveÂ» perte de donnÃ©es.

Bien qu'il reste encore beaucoup d'incertitude, la question de savoir si le malware est issu d'un groupe privÃ© ou Ãtat-nation a Ã©tÃ© soulevÃ©e, avec le Laboratoire Hongrois de Cryptographie et SÃ©curitÃ© du systÃ¨me (CRYSYS) indiquant qu'il a Ã©tÃ© Â« mis au point par un gouvernement dâÃtat ou une nation avec un budget important et de l'effort Â».

James Todd, responsable technique pour l'Europe Ã FireEye, chef de file dans l'arrÃªt des attaques ciblÃ©es avancÃ©es, commente :

"*La dÃ©couverte du malware Flame a embrasÃ© les mÃ©dia, et constitue un rappel fort - en particulier pour ceux qui ne se sentent que trÃ¨s peu concernÃ©s par la cyber-guerre et le cyber-espionnage, et qui les entrevoient comme de lointains et peu probables risques. Il est clair que Flame a fait pour l'espionnage ce que Stuxnet a fait pour l'infrastructure informatique.*

DorÃ©navant, il faut se poser les bonnes questions quant aux mesures Ã prendre pour Ã©viter que la prochaine attaque ait le mÃªme impact, quelle quâ□□en soit la cible."

Bien que les dÃ©tails Ã©mergent petit Ã petit, il y a encore beaucoup de doutes et spÃ©culations sur le dÃ©veloppement et l'origine du malware - en dÃ©pit de plusieurs rÃ©actions instinctives Ã partir de divers commentateurs. Cependant, une chose demeure limpide - des outils de sÃ©curitÃ© pÃ©rimÃ©trique et basÃ©e sur les signatures ont bel et bien perdu leur statut de dÃ©fenses adÃ©quates contre les attaques d'aujourd'hui, de plus en plus sophistiquÃ©es. Aujourdâ□□hui, les menaces ne visent plus le simple vol de donnÃ©es ou de mots de passe ; les enjeux sont beaucoup plus Ã©levÃ©s, et les procÃ©dures de sÃ©curitÃ© doivent emboÃ®ter le pas. Le fait que Flame ait Ã©chappÃ© Ã la dÃ©tection pendant si longtemps, et Ã autant d'outils antivirus diffÃ©rents est dÃ©plorable, et prouve que la vitesse Ã laquelle les programmes malveillants sont dÃ©veloppÃ©s est tout simplement en train dâ□□asphyxier les entreprises qui tentent de garder le rythme.

"*La prochaine grande tendance en matiÃ¨re de sÃ©curitÃ© informatique a toujours Ã©tÃ© le cyber-espionnage, Ã©tant donnÃ©es les recettes avantageuses en cas de succÃ¨s. Cela est particuliÃ¨rement vrai si les pirates rÃ©ussissent Ã s'infiltrer dans les informations relatives aux politiques, aux brevets, la propriÃ©tÃ© intellectuelle et aux plans R & D. En tant que telle, toute organisation - ou nation - avec des investissements importants en R & D ou IP doit se montrer particuliÃ¨rement exigeante sur la sÃ©curitÃ© prÃ©ventive avant qu'il ne soit trop tard. Une part trop importante dâ□□entreprises, manifestant une dÃ©pendance excessive sur les pÃ©rimÃ¨tres de dÃ©fense basÃ©es sur les signatures autres des solutions traditionnelles et heuristiques, est encore terriblement exposÃ©e au Â« zero day Â», les attaques inconnues. La plupart reconnait dÃ©sormais quâ□□en matiÃ¨re de violation, la question est de savoir non plus si elle va arriver, mais quand, et de reconnaitre que le Â«quandÂ» peut dÃ©jÃ avoir eu lieu, comme en tÃ©moigne l'Ã©chec de la dÃ©couverte de Flame jusqu'Ã prÃ©sent.* "