Proofpoint : Cyberattaques perpetrÃ©es via l'Internet des objets
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 21/1/2014 13:00:00

Plus de 750 000 courriers Ã©lectroniques indÃ©sirables et de phishing ont Ã©tÃ© envoyÃ©s via des Â« thingbots Â», parmi lesquels des tÃ©lÃ©visions et des rÃ©frigÃ©rateurs.
Proofpoint, Inc., lâun des principaux prestataires de solutions de sÃ©curitÃ©-service (SaaS), a rÃ©cemment mis au jour ce qui pourrait bien Ãªtre le premier exemple de cyberattaque commanditÃ©e via l'Internet des objets, et impliquant des appareils mÃ©nagers courants.

Cette attaque d'envergure mondiale s'est caractÃ©risÃ©e par l'envoi de plus de 750 000 courriers Ã©lectroniques frauduleux, provenant de plus de 100 000 Ã©quipements de la vie courante, comme des routeurs, des centres multimÃ©dia, des tÃ©lÃ©visions et au moins un rÃ©frigÃ©rateur. En effet, ceux-ci ont Ã©tÃ© transformÃ©s en plateformes permettant de dÃ©clencher des cyberattaques. Si l'on en croit les mÃ©dias, le nombre de ces appareils sera plus de quatre fois supÃ©rieur Ã celui des ordinateurs connectÃ©s Ã Internet dans les prochaines annÃ©es. Pour cette raison, les attaques organisÃ©es via l'Internet des objets reprÃ©sentent un danger certain pour les propriÃ©taires de tels Ã©quipements, ainsi que pour les entreprises.

Alors que les ordinateurs personnels peuvent dÃ©jÃ , Ã notre insu, Ãªtre convertis en botnets permettant le dÃ©clenchement de cyberattaques massives, Proofpoint a rÃ©cemment Ã©tabli que les cybercriminels commenÃ§aient Ã transformer des routeurs, des appareils mÃ©nagers et autres Ã©quipements faisant partie de l'Internet des objets en Â« thingbots Â» Ã des fins similaires.

DÃ©terminÃ©s Ã dÃ©rober des informations personnelles et Ã infiltrer les systÃ¨mes informatiques de certaines entreprises, ces mÃªmes personnes ont trouvÃ© dans ces appareils connectÃ©s Ã Internet (mais faiblement protÃ©gÃ©s) une vÃ©ritable mine d'or. Ceux-ci sont effectivement plus intÃ©ressants car plus simples Ã infecter qu'un PC, un ordinateur portable ou une tablette.

L'attaque rÃ©vÃ©lÃ©e par Proofpoint s'est produite entre le 23 dÃ©cembre 2013 et le 6 janvier 2014. Au cours de celle-ci, des vagues successives de courriers frauduleux, gÃ©nÃ©ralement envoyÃ©s Ã raison de 100 000 Ã la fois, Ã©taient envoyÃ©es Ã des entreprises ainsi qu'Ã des particuliers basÃ©s dans le monde entier. Plus de 25 % des messages ont Ã©tÃ© envoyÃ©s par des Ã©quipements qui n'Ã©taient pas des ordinateurs portables, des ordinateurs de bureau ou des appareils mobiles ordinaires.

Â

Ils provenaient en rÃ©alitÃ© d'Ã©quipements de la vie courante, comme des routeurs, des centres multimÃ©dia, des tÃ©lÃ©visions et au moins un rÃ©frigÃ©rateur, tous connectÃ©s Ã Internet. Pas plus de 10 messages n'ont Ã©tÃ© envoyÃ©s par adresse IP. Ainsi, il Ã©tait difficile de contrecarrer l'attaque en se basant simplement sur un emplacement donnÃ©. En outre, dans la

plupart des cas, les appareils concernÃ©s n'avaient pas fait l'objet de manipulations particuliÃ¨rement sophistiquÃ©es. Un simple dÃ©tournement des mots de passe a permis de les rendre complÃ¨tement accessibles sur les rÃ©seaux publics.

D'aprÃ¨s **David Knight**, responsable gÃ©nÃ©ral de la division dÃ©diÃ©e Ã la sÃ©curitÃ© des informations chez Proofpoint, Â« *Les botnets reprÃ©sentent dÃ©jÃ un risque certain en matiÃ¨re de sÃ©curitÃ©, et l'Ã©mergence des thingbots pourrait ne faire qu'empirer considÃ©rablement les choses* Â». Â« *Un grand nombre de ces appareils sont faiblement protÃ©gÃ©s, et leurs propriÃ©taires n'ont presque aucun moyen de dÃ©tecter les infections, ou d'y remÃ©dier. Certaines entreprises peuvent Ã©galement Ãªtre victimes de ces attaques.* Â»

Bien que les experts en technologies de l'information aient dÃ©jÃ , depuis un certain temps, pressenti le risque reprÃ©sentÃ© par le dÃ©veloppement rapide de l'Internet des objets, c'est la premiÃ¨re fois qu'il a Ã©tÃ© fait Ã©tat d'une telle cyberattaque induisant des Ã©quipements courants. Mais ce n'est certainement pas la derniÃ¨re.

L'Internet des objets englobe chaque appareil connectÃ© Ã Internet, qu'il s'agisse de thermostats, de camÃ©ras de sÃ©curitÃ©, de rÃ©frigÃ©rateurs, de micro-ondes, de tÃ©lÃ©viseurs, de consoles de jeux, de rayonnages intelligents qui se rÃ©approvisionnent lorsque cela est nÃ©cessaire dans les magasins, ou de machines industrielles. Et leur nombre ne fait qu'augmenter, de maniÃ¨re considÃ©rable. Selon IDC, plus de 200 milliards seront connectÃ©s Ã Internet d'ici 2020 .

De tels appareils ne bÃ©nÃ©ficient toutefois pas des systÃ¨mes anti-spam et anti-virus utilisÃ©s par les entreprises et les particuliers. Ils ne sont pas non plus contrÃ´lÃ©s rÃ©guliÃ¨rement par des spÃ©cialistes ou des logiciels dÃ©diÃ©s, ce qui empÃªche toute obtention de correctif permettant de remÃ©dier Ã d'Ã©ventuelles failles de sÃ©curitÃ©. Par consÃ©quent, les entreprises ne peuvent pas compter sur une rÃ©solution du problÃ¨me en s'attelant directement Ã la source. En effet, des opÃ©rations doivent Ãªtre entreprises pour pallier Ã l'augmentation inÃ©vitable du nombre d'attaques, de courriers Ã©lectroniques frauduleux et de liens douteux.

Â« *L'Internet des objets reprÃ©sente une manne certaine, car, grÃ¢ce Ã lui, il est possible de contrÃ´ler toujours plus d'Ã©quipements de la vie courante. Cette aubaine permet Ã©galement aux cybercriminels d'utiliser nos routeurs, nos tÃ©lÃ©visions, nos rÃ©frigÃ©rateurs et nos autres appareils connectÃ©s Ã Internet pour organiser des attaques de grande envergure* Â» indique **Michael Osterman,** analyste principal chez Osterman Research.

Â« *Les appareils connectÃ©s Ã Internet reprÃ©sentent une menace consÃ©quente car ils sont faciles Ã atteindre, leurs utilisateurs sont peu incitÃ©s Ã les protÃ©ger davantage, ils permettent d'envoyer du contenu dangereux qui n'est presque jamais dÃ©tectÃ©, peu de fournisseurs cherchent Ã remÃ©dier Ã cela et les possibilitÃ©s actuelles en matiÃ¨re en sÃ©curitÃ© ne sont simplement pas suffisantes.* Â»