Faux certificats SSL : ComodoHacker passe à l'attaque

L'attaque du fournisseur américain de certificats numériques **Comodo** ne serait pas le fait du gouvernement iranien, comme le suggérait le prestataire victime, mais d'**un « simple » pirate iranien** qui aurait agi seul comme il l'a déclaré sur la la plateforme Pastebin. Celui qui se présente sous le pseudo **ComodoHacker** y décrit, en détail, la démarche qu'il a suivi pour parvenir à ses fins. Ce qui tend à crédibiliser ses dires sans pour autant les prouver.

Rappelons que, mi-mars, Comodo s'est fait dérober pas moins de neuf certificats SSL pour les domaines touchant Microsoft, Google, Yahoo, Mozilla ou encore Skype. Plus exactement, le cybercriminel est parvenu à générer des vrais «passeports numériques» à des fins frauduleuses. L'exploitation réussie de ces certificats aurait pu avoir **de graves conséquences** pour les utilisateurs se rendant sur les sites visés.

Face au scepticisme de la profession sur la capacité qu'un individu seul ait pu parvenir à un tel exploit, ComodoHacker a décidé d'apporter la preuve de ses dires. Il a donc mis en ligne le lien pour télécharger **le certificat propre aux téléchargements des extensions Mozilla Firefox**. Et de joindre la parole au geste en se moquant, et provoquant, allègrement ceux qui doutent de l'authenticité de ses actes.

« Aux idiots dont, je serais prêt à le parier, le QI ne doit pas dépasser 75, et qui pensent encore que je ne suis pas le pirate, voici certificat 'addon' de Mozilla, vérifiez son numéro de série avec celui publié sur l'Internet. » Et d'en rajouter une couche : *« Je suis vraiment désolé pour vous, les gars (ceux qui doutent encore) [...] :* ***avez-vous déjà consulté un docteur?*** *»*

Derrière cet humour moqueur se cacherait un jeune homme de 21 ans qui revendique notamment son acte pour **se venger de Stuxnet**, le code malveillant soupçonné de viser les installations nucléaires iraniennes, notamment. Pour y parvenir, le pirate aurait réussi à pénétrer le serveur InstantSSL de GlobalTrust, un revendeur italien des applications de Comodo. Le FBI et la police italienne ont ouvert une enquête.

L'attaque du fournisseur américain de certificats numériques Comodo ne serait pas le fait du gouvernement iranien, comme le suggérait le prestataire, mais d'un « simple » pirate iranien qui aurait agi seul comme il l'a déclaré sur la la plateforme Pastebin. Celui qui se présente sous le pseudo ComodoHacker y décrit, en détail, la démarche qu'il a suivi pour parvenir à ses fins. Ce qui tend à crédibiliser ses dires sans pour autant les prouver.

Rappelons que, mi-mars, Comodo s'est fait dérober pas moins de neuf certificats SSL pour les domaines touchant Microsoft, Google, Yahoo, Mozilla ou encore Skype. L'exploitation réussie de ces certificats aurait pu avoir de graves conséquences pour les utilisateurs se rendant sur les sites visés.

Face au scepticisme de la profession sur la capacité qu'un individu seul ait pu parvenir à un tel exploit, ComodoHacker a décidé d'apporter la preuve de ses dires. Il a donc mis en ligne le lien pour télécharger le certificat propres aux téléchargements des extensions Mozilla Firefox. Et de joindre la parole au geste en se moquant, et provoquant, allègrement ceux qui doutent de la véracité de ses actes.

« Aux idiots dont, je serais prêt à le parier, le QI ne doit pas dépasser 75, et qui pensent encore que je ne suis pas le pirate, voici certificat 'addon' de Mozilla, vérifiez son numéro de série avec celui publié sur l'Internet. » Et d'en rajouter une couche : « Je suis vraiment désolé pour vous, les gars (ceux qui doutent encore) […] : avez-vous déjà consulté un docteur? »

Derrière cet humour moqueur se cacherait un jeune homme de 21 ans qui revendique notamment son acte pour se venger de Stuxnet, le code malveillant soupçonné de viser les installations nucléaires iraniennes, notamment. Pour y parvenir, le pirate aurait réussi à pénétrer le serveur InstantSSL de GlobalTrust, un revendeur italien des applications de Comodo. Le FBI et la police italienne ont ouvert une enquête.