Sécurité : Cisco tacle les méthodes agressives du Français Tuto4PC (MAJ)

La division sécurité de Cisco, Talos, a publié un post sur son blog dans lequel elle pointe du doigt la société Tuto4PC, éditeur français de logiciel (connu aussi sous le nom d'Eorezo Group). Elle l'accuse de pousser auprès des utilisateurs des logiciels non souhaités, dont certains ont des comportements proches de malwares.

A l'origine de l'affaire, Cisco a détecté un Troyen générique inexpliqué, un programme du nom de Wizz qui est en fait une partie d'un utilitaire, OneSoftPerDay, construit et distribué par Tuto4PC. Après son installation, ce logiciel effectue une liste de tâches et de contrôles identiques à ceux observés sur les malwares actuels. Il vérifie par exemple la présence d'une sandbox, d'une solution antivirus, d'autres outils de sécurité, de prise de contrôle à distance et les navigateurs installés. Il collecte donc un ensemble de données et les transmet à un serveur via un canal chiffré. Pour Cisco, il se comporte exactement comme les modules de vols de données que l'on trouve dans certains spywares ou chevaux de Troie bancaires.

Pour l'équipe de sécurité, « *en installant des droits administrateurs, Wizz est capable de recueillir des informations personnelles, d'installer et lancer des exécutables téléchargés par un tiers* ». Sur ce dernier point, Talos constate que Wizz implante secrètement des logiciels, comme System Healer (dans le cas présent), sans la permission de l'utilisateur, contrairement à ce qui est prévu dans les CGU (Conditions générales d'utilisation) de l'éditeur. Une façon de procéder qui, selon Cisco, justifie de classer ce logiciel comme « *une backdoor ou au minimum comme un programme non sollicité* ».

Un chiffrement faiblard et un passif à la CNIL

Talos s'amuse aussi des efforts maladroits de Wizz « *pour contourner les politiques de sécurité* ». En effet, les chercheurs de Cisco ont fait un copier-coller de la clé de chiffrement AES 256 utilisée par l'outil pour communiquer avec les serveurs. Après une rapide recherche, ils l'ont détecté sur un blog MSDN. Pour Talos, les développeurs de Tuto4PC ont utilisé la méthode de chiffrement décrite sur ce blog… tout en conservant la même valeur pour la clé.

Après analyses des signatures et des domaines, tous les chemins mènent à Tuto4PC, conclut Talos. Même si la division sécurité de Cisco constate que des techniques de masquage du propriétaire des domaines ont été utilisées. Selon les chiffres donnés sur le site de l'éditeur français, ses logiciels sont installés sur près de 12 millions de PC pour l'année 2014.

Cisco rappelle également les démêlés de Tuto4PC avec les autorités, notamment une décision de la CNIL en octobre 2012 enjoignant l'éditeur de cesser certaines pratiques de collecte de données et surtout le poussant à recueillir le consentement explicite des utilisateurs. En mai 2013, cette décision a fait l'objet d'une demande d'annulation de Tuto4PC auprès du Conseil d'Etat. Dans un arrêt de mars 2015, ce dernier a réaffirmé l'obligation d'enregistrer « *un consentement spécifique* » et a rappelé qu'un consentement générique pour l'ensemble des CGU ne vaut pas consentement spécifique, comme le soulignait à l'époque notre confrère *Nextinpact*. Contactées par nos soins,

Tuto4PC et la société WizzLabs, accusés par l'équipe sécurité de Cisco, n'ont pas répondu à nos demandes de commentaires.

MAJ : Franck Bosset, Président de l'éditeur français Tuto4PC group a réagi sur l'analyse de l'équipe de sécurité de Cisco. « *Nous contestons vigoureusement toute implication dans la distribution de malware et allons demander à nos avocats d'organiser un action judiciaire appropriée pour obtenir réparation de ces allégations injustifiées* ». Le dirigeant reconnaît être un distributeur d'adware, une activité connue et cotée en bourse. Dans un contexte de plus en plus difficile vis-à-vis des logiciels publicitaires, l'éditeur a « *effectivement développé des techniques d'installation des adwares qui peuvent bypasser les blocages intempestifs des logiciels antivirus qui eux-mêmes agiraient comme adware et essaieraient d'empêcher notre installation* ». Un savoir-faire que le dirigeant compte bien mettre à profit via un logiciel baptisé AV Booster développé par la filiale cybersécurité du groupe, Cloud4PC.

A lire aussi :

Chiffrement : la CNIL casse les backdoors
Linux Mint : un pirate place une backdoor dans les ISO

Crédit photo : Alexskopje-Shutterstock