Le groupe de pirates utilise des méthodes innovantes pour diffuser ses logiciels malveillants

Des chercheurs d'ESET ont découvert de nouveaux outils utilisés par le groupe Gamaredon dans ses dernières campagnes malveillantes. Le premier outil cible Microsoft Outlook à l'aide d'un projet personnalisé Microsoft Outlook Visual Basic for Applications (VBA), qui permet aux pirates d'utiliser le compte de messagerie d'une victime pour envoyer des emails d'hameçonnage à des contacts de son carnet d'adresses. L'utilisation de macros Outlook pour diffuser des logiciels malveillants est une méthode rarement vue par les chercheurs. Le second outil est utilisé par ce groupe très actif pour injecter des macros et des références à des modèles distants dans des documents Word et Excel. Ces deux outils sont conçus pour aider le groupe Gamaredon à se propager davantage dans des réseaux déjà compromis.

« Au cours des mois précédents, nous avons constaté une augmentation de l'activité de ce groupe, avec des vagues constantes d'emails malveillants frappant les boîtes de messagerie de leurs cibles. Les pièces jointes de ces emails sont des documents contenant des macros malveillantes qui, lorsqu'elles sont exécutées, tentent de télécharger une multitude de types de logiciels malveillants différents, » explique Jean-Ian Boutin, Head of Threat Research chez ESET.

Les dernières versions de ces outils injectent des macros malveillantes ou des références à des modèles distants dans les documents existants sur le système attaqué, ce qui est un moyen très efficace pour se déplacer dans le réseau d'une entreprise, car les collaborateurs partagent régulièrement des documents. Grâce à une fonctionnalité spéciale qui permet de modifier les paramètres de sécurité des macros de Microsoft Office, les utilisateurs concernés n'ont absolument pas conscience qu'ils compromettent à nouveau leur poste de travail lorsqu'ils ouvrent les documents.

Le groupe utilise des portes dérobées et des analyseurs de fichiers pour identifier et collecter des documents sensibles dans un système compromis, afin de les télécharger sur un serveur de commande et de contrôle. Ces analyseurs de fichiers possèdent également des fonctions d'exécution de code arbitraire à partir du serveur de commande et de contrôle.
Il existe une distinction majeure entre Gamaredon et d'autres groupes : ces pirates ne font que peu ou pas d'efforts pour échapper à toute détection. Même si leurs outils sont capables d'utiliser des techniques furtives, il semble que le principal objectif de ce groupe soit de se répandre sur le plus profondément et le plus rapidement possible dans le réseau de ses cibles pour y exfiltrer des données.

« Bien que le détournement d'une boîte de messagerie compromise pour envoyer des emails malveillants sans le consentement de la victime ne soit pas une nouveauté, nous pensons qu'il s'agit du premier cas publiquement documenté d'un groupe de pirates utilisant un fichier OTM et une macro Outlook pour y parvenir, » ajoute M. Boutin à propos de la découverte d'ESET. « Nous avons pu collecter de nombreux échantillons de différents scripts, exécutables et documents malveillants utilisés par le groupe Gamaredon tout au long de ses campagnes. »

Chaîne d'infection typique d'une campagne de Gamaredon

Le groupe Gamaredon est actif depuis au moins 2013. Il est responsable d'un certain nombre d'attaques, principalement contre des institutions ukrainiennes.

Les outils analysés dans cette étude ont été détectés comme étant des variantes de MSIL/Pterodo, Win32/Pterodo ou Win64/Pterodo, par les produits d'ESET.

Pour plus de détails techniques sur les derniers outils de Gamaredon, lisez l'article complet « Le groupe Gamaredon continue de se développer » sur le blog WeLiveSecurity.com. Suivez l'actualité d'ESET Research sur Twitter.