Emotet : Au premier plan des menaces cet automne
Internet
PostÃ© par : JulieM
PubliÃ©e le : 21/11/2022 13:00:00

TA542, un acteur malveillant qui distribue le malware Emotet, est (encore) de retour, aprÃ¨s une longue pause dans la distribution dâ□□emails malveillants.

L'acteur sâ□□est absentÃ© pendant prÃ¨s de quatre mois, vu pour la derniÃ¨re fois le 13 juillet 2022 avant de revenir le 2 novembre 2022.Â

Proofpoint a suivi les mÃ©thodes de diffusion, le ciblage rÃ©gional et a effectuÃ© une analyse du malware Emotet et de la charge utile IcedID.

Dans l'ensemble, cette activitÃ© est similaire aux campagnes de juillet et de nombreuses tactiques observÃ©es prÃ©cÃ©demment restent les mÃªmes, cependant les nouveaux changements et amÃ©liorations incluent :

â□¢ De nouveaux leurres visuels d'attachement Excel
â□¢ Changements apportÃ©s au binaire d'Emotet
â□¢ Le chargeur IcedID dÃ©posÃ© par Emotet est une nouvelle version lÃ©gÃ¨re du chargeur
â□¢ Rapports sur le largage de Bumblebee en plus de IcedID

Sherrod DeGrippo Vice PrÃ©sidente de lâ□□Ã©quipe Threat Research and Detection de Proofpoint, a dÃ©clarÃ© Â« Emotet est un rÃ©seau incroyablement puissant de propagation de malware.

Lâ□□entitÃ© existe depuis des annÃ©es, et reprÃ©sente lâ□□un des acteurs de la menace les plus importants que nous ayons jamais suivis en termes de volume dâ□□attaques ciblÃ©es. Nous le suivons de trÃ¨s prÃ¨s en raison de sa persÃ©vÃ©rance et de ses tactiques toujours plus innovantes.

Nous nâ□□avions pas vu Emotet depuis juillet dernier, et il est rÃ©apparu ce mois-ci.

Avec ce retour, nous avons pu constater certains changements et quelques amÃ©liorations dans leur stratÃ©gie dâ□□attaque â□□ le groupe utilise dÃ©sormais de nouvelles piÃ¨ces jointes Excel comme leurres ; il y a plusieurs mises Ã jour notables du code binaire, et certaines personnes rapportent quâ□□il aurait laissÃ© tomber un autre tÃ©lÃ©chargeur de logiciels malveillants appelÃ© Bumblebee.

Par ailleurs, et comme nous lâ□□avions dÃ©jÃ signalÃ©, Emotet semble avoir dÃ©laissÃ© lâ□□utilisation du chargeur de payload IcedID. Nous avons aussi pu observer des centaines de milliers de messages par jour utilisant Emotet, y compris des piÃ¨ces jointes en grec, anglais, italien, FranÃ§ais et japonais.

Tous les signaux indiquent un retour dâ□□Emotet en pleine capacitÃ©, et ses nouvelles fonctionnalitÃ©s dÃ©montrent lâ□□Ã©mergence dâ□□un rÃ©seau de diffusion puissant, faisant appel Ã de nombreuses et grandes familles de logiciels malveillants.

Ce qui est particuliÃ¨rement intÃ©ressant ici, câ□□est quâ□□Emotet continue de fonctionner et dâ□□Ã©voluer. Nous lâ□□avons vu pendant des annÃ©es, et il ne montre aucun signe dâ□□arrÃªt de ses activitÃ©s. Il continue de mourir et de revenir Ã la vie tel un phÃ©nix ou un chat avec

plus de neuf vies. Â»

Si vous souhaitez en savoir plus.