Des logiciels malveillants chinois en hausse.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 22/9/2023 13:00:00

Alors que le paysage de la menace cyber semble dominÃ© par des acteurs liÃ©s au gouvernement de Moscou â notamment le groupe TA499 aussi connu sous le nom de Vovan et Lexus â les derniÃ¨res recherches menÃ©es par Proofpoint, lâun des leaders dans les domaines de la conformitÃ© et de la cybersÃ©curitÃ©, dÃ©montrent une recrudescence dans lâutilisation de logiciels malveillants ciblant des organisations internationales ayant des activitÃ©s en Chine.

Dans les campagnes dâattaques observÃ©es par Proofpoint, les sujets et le contenu des courriels sont gÃ©nÃ©ralement rÃ©digÃ©s en chinois et portent sur des thÃ¨mes liÃ©s Ã lâactivitÃ© de lâorganisme (factures, paiements, nouveaux produits). Les utilisateurs ciblÃ©s ont des noms en chinois, orthographiÃ©s avec des caractÃ¨res chinois, ou des adresses Ã©lectroniques d'entreprises spÃ©cifiques qui semblent correspondre aux activitÃ©s des entreprises en Chine.

Les mÃ©thodes incluent notamment des tentatives de diffusion du cheval de Troie d'accÃ¨s Ã distance (RAT, Remote Access Trojan) Sainbox :

Ãchantillon de courrier Ã©lectronique du 17 mai 2023 envoyÃ© par Sainbox, contenant une URL liÃ©e Ã un fichier zip, "26866498.exe".
S'il est exÃ©cutÃ©, il conduit Ã l'installation du Sainbox RAT (Remote Access Trojan) â recherches Proofpoint

Les recherches soulignent l'expansion de l'Ã©cosystÃ¨me des logiciels malveillants chinois, l'augmentation des Ã©changes cybercriminels en chinois et l'accÃ¨s dÃ©sormais Ã©tendu aux ressources et aux cibles propres Ã la Chine. Tous ces Ã©lÃ©ments remettent sÃ©rieusement en question la domination actuelle du marchÃ© russophone de la cybercriminalitÃ© dans le paysage des menaces.

Â« Cette activitÃ© ne semble pas Ãªtre liÃ©e Ã une entitÃ© unique, mais plutÃ´t Ã un ensemble dâacteurs. L'apparition de ValleyRAT aux cÃ´tÃ©s des souches de logiciels malveillants plus anciennes laisse entrevoir la possibilitÃ© d'une relation entre les acteurs. MÃªme si ces familles de logiciels malveillants ne sont pas nouvelles, les organisations ne peuvent pas se permettre de sous-estimer le risque qu'elles reprÃ©sentent. Â» expliquent les chercheurs Proofpoint.

Voici un aperÃ§u de lâÃ©tude :

â¢ En 2023, Proofpoint a observÃ© plus de 30 campagnes utilisant des logiciels malveillants en chinois, tels que ValleyRAT, rÃ©cemment dÃ©couvert, et les anciens Sainbox RAT (une variante de Gh0stRAT) et Purple Fox.

â¢ Presque tous les leurres sont en chinois, bien que Proofpoint ait Ã©galement observÃ© des messages en japonais ciblant des organisations dans ce pays.
â¢ AprÃ¨s des annÃ©es d'absence de ces logiciels malveillants dans les donnÃ©es de Proofpoint sur les menaces, leur apparition dans de multiples campagnes au cours des six derniers mois est remarquable.

â¢ Ce sont plusieurs acteurs de la menace plutÃ´t qu'un seul qui sont Ã l'origine de ce pic. Ces

attaques semblent Ãªtre motivÃ©es par des considÃ©rations financiÃ¨res et rien n'indique qu'elles soient soutenues par un Ã□tat.

Vous trouverez lâ□□intÃ©gralitÃ© de lâ□□Ã©tude sur le site de Proofpoint :Â