DarkGate : l'exploitation des applications et services cloud
Internet
PostÃ© par : JerryG
PubliÃ©e le : 5/2/2024 13:00:00

De nouvelles attaques de phishing abusent des demandes de chat de groupe Microsoft Teams pour envoyer des piÃ¨ces jointes malveillantes qui installent des charges utiles de malware DarkGate sur les systÃ¨mes des victimes.

Les attaquants ont utilisÃ© ce qui semble Ãªtre un utilisateur (ou un domaine) Teams compromis pour envoyer plus de 1 000 invitations malveillantes Ã des discussions de groupe Teams, selon les recherches d'AT&T Cybersecurity.

Paolo Passeri, Cyber Intelligence Specialist chez Netskope, a fait le commentaire suivant :

Â« Le malware DarkGate a Ã©tÃ© dÃ©veloppÃ© en 2017 et commercialisÃ© en tant que MaaS (Malware-as-a-Service). La campagne a rÃ©cemment fait la Une des mÃ©dias aprÃ¨s avoir Ã©tÃ© dÃ©couverte dans des groupes de discussion sur Microsoft Teams, qui compte 280 millions d'utilisateurs par mois.

Alors que le DarkGate Loader Ã©tait initialement distribuÃ© via des emails de phishing, l'annÃ©e derniÃ¨re, les attaquants ont fait Ã©voluer leur mÃ©thodologie d'attaque et ont commencÃ© Ã exploiter plusieurs services cloud pour la distribution. Ce n'est pas la premiÃ¨re fois quâ□□il est actif dans Microsoft Teams - en aoÃ»t de l'annÃ©e derniÃ¨re, DarkGate a dÃ©jÃ eu recours Ã lâ□□application pour diffuser sa charge utile (qui Ã©tait hÃ©bergÃ©e sur un site Microsoft SharePoint).

Ce qu'il est important de noter, c'est que ce dernier dÃ©veloppement est tout Ã fait conforme Ã la tendance plus large des cybercriminels qui utilisent des applications cloud en de multiples points de la chaÃ®ne d'exÃ©cution de leur attaque. Les applications cloud permettent une charge utile malveillante flexible et une infrastructure cloud flexible pour l'acheminer. 46 % des logiciels malveillants ont Ã©tÃ© diffusÃ©s Ã partir du cloud en dÃ©cembre 2023.

Il n'est donc pas surprenant que les cybercriminels recherchent constamment une chaÃ®ne d'attaque de plus en plus complexe oÃ¹ de multiples services lÃ©gitimes sont intÃ©grÃ©s ; dans le seul but d'inciter les victimes Ã tÃ©lÃ©charger la charge utile malveillante et d'Ã©chapper aux technologies de sÃ©curitÃ© web (et de messagerie) existantes qui ne tiennent pas compte des instances, ne sont pas adaptÃ©es Ã l'inspection du trafic SSL Ã l'Ã©chelle et ne prennent donc pas en compte le contexte.

Les organisations doivent s'assurer que la sÃ©curitÃ© du cloud est en tÃªte de leur liste de prioritÃ©s tactiques en matiÃ¨re de cybersÃ©curitÃ© pour 2024, car les attaquants vont continuer Ã tirer parti de toutes les failles existantes. Â»