Bitdefender : Bad Rabbit le ransomware nouveau
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 25/10/2017 15:00:00

Apparue hier, Bad Rabbit est une nouvelle souche du ransomware GoldenEye, qui a commencÃ© par frapper un nombre d'institutions de premier plan en Russie et en Ukraine. La nouvelle famille de ransomwares est surnommÃ©e Bad Rabbit et semble cibler les infrastructures critiques et les entitÃ©s de haut niveau dans des rÃ©gions de lâ□□ancien bloc soviÃ©tique.

Notre analyse prÃ©liminaire rÃ©vÃ¨le que cette nouvelle souche de ransomware accompagne plusieurs outils open source qui sont utilisÃ©s pour le chiffrement des donnÃ©es et les mouvements latÃ©raux, comme expliquÃ© ci-dessous.

Â

Â

Premiers rÃ©sultats dâ□□analyse de l'Ã©chantillon

Ceci est une analyse continue et les informations prÃ©sentÃ©es ici seront mises Ã jour plusieurs fois jusqu'Ã ce que l'Ã©chantillon soit entiÃ¨rement rÃ©pertoriÃ©, alors assurez-vous de suivre les mises Ã jour sur cet article ou de suivre notre page Twitter.

Le processus d'infection commence par un faux programme d'installation Adobe Flash tÃ©lÃ©chargÃ© Ã partir de sites Web compromis.

Ce faux programme d'installation Flash contient la charge utile du ransomware dans une superposition de compressions ZLIB. Une fois dÃ©chiffrÃ©, il dÃ©pose et exÃ©cute le vÃ©ritable ransomware (identifiÃ© en tant que b14d8faf7f0cbcfad051cefe5f39645f).

La charge utile de ransomware mentionnÃ©e ci-dessus contient pas moins de six outils diffÃ©rents sous lâ□□apparence de ressources compressÃ©es ZLIB, qui sont utilisÃ©s Ã des fins de chiffrage, ainsi que pour la propagation latÃ©rale. Ces outils sont :

Le composant de chiffrement (identifiÃ© comme Ã©tant 5b929abed1ab5406d1e55fea1b344dab)

Le bootloader (identifiÃ© comme Ã©tant b14d8faf7f0cbcfad051cefe5f39645f)

Mimikatz - un utilitaire pour extraire les mots de passe et les tickets d'authentification de la mÃ©moire

Un binaire Mimikatz compilÃ© pour x86 (identifiÃ© comme 37945c44a897aa42a66adcab68f560e0)
Un binaire Mimikatz compilÃ© pour x64 (identifiÃ© comme 347ac3b6b791054de3e5720a7144a977)

DiskCryptor - une solution de chiffrement de partition open source

Un driver DiskCryptor compilÃ© pour x86 (identifiÃ© comme b4e6d97dafd9224ed9a547d52c26ce02)
Un driver DiskCryptor compilÃ© pour x64 (identifiÃ© comme edb72f4a46c39452d1a5414f7d26454a)

Ce que nous savons jusqu'ici

Bad Rabbit est extrÃªmement similaire Ã GoldenEye / NotPetya Ã la fois structurellement et dâ□□un point de vue plus large.

Il cible l'infrastructure critique ukrainienne et est hautement viral en raison de son implÃ©mentation de Mimikatz qui lui permet de passer d'un poste de travail infectÃ© Ã un autre au sein d'une organisation.

Il dispose Ã©galement d'un chiffrement de disque via le driver DiskCryptor afin qu'il puisse interfÃ©rer avec le processus de dÃ©marrage normal et empÃªcher ce dernier sur l'ordinateur.

IMAGE : Des noms de personnages de Game of Thrones sont rÃ©fÃ©rencÃ©s sur cet Ã©chantillon.

Dernier point, mais non des moindres, alors que le composant ransomware rÃ©fÃ©rence les personnages Game of Thrones, il possÃ¨de Ã©galement une routine de hachage de processus extrÃªmement similaire Ã celle utilisÃ©e par GoldenEye pour vÃ©rifier les solutions de sÃ©curitÃ© installÃ©es localement avant de crypter le MBR (le master boot record).

Si vous utilisez un produit antimalware Bitdefender pour particuliers ou entreprises, vous Ãªtes Ã lâ□□abri, car nos solutions dÃ©tectent cette menace comme suit :

Gen: Heur.Ransom.BadRabbit.1 et Gen: Variant.Ransom.BadRabbit.1.

Les utilisateurs de Bitdefeder Elite sont protÃ©gÃ©s par des algorithmes de machine learning plus agressifs qui signalent cette menace comme suit :

Gen:Illusion.ML.Skyline.10101 depuis son apparition (zero day).

Visitez le la boutique Bitdefender.