Bitdefender : Ransomwares et monnaie numÃ©rique
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 22/11/2017 13:30:00

Bitdefender, leader mondial des technologies de cybersÃ©curitÃ© protÃ©geant plus de 500 millions dâutilisateurs Ã travers le monde, partage les conclusions de son Ã©tude annuelle sur les cybermenaces.

Selon la recherche, les ransomwares et les mineurs de monnaie numÃ©riques sont les deux types de malwares les plus diffusÃ©s, car ils offrent aux pirates une monÃ©tisation facile et sont facilement disponibles en libre-service sur Internet.

Contrairement aux annÃ©es prÃ©cÃ©dentes, les concepteurs de ransomware en 2017 se sont spÃ©cialement concentrÃ©s sur l'infection dâinfrastructures touchant des secteurs verticaux tels que l'Ã©ducation, la santÃ© et la finance.

Depuis la rÃ©apparition en mars dernier, de la famille de ransomware Troldesh, les entreprises ont Ã©tÃ© confrontÃ©es Ã des attaques extrÃªmement ciblÃ©es qui exploitent les failles du Remote Desktop Protocol pour se connecter aux infrastructures systÃ¨mes, puis infecter manuellement les ordinateurs des entreprises.

Des variantes de ransomware particuliÃ¨res telles que Troldesh et GlobeImposter disposent dÃ©sormais d'outils de mouvement latÃ©ral (tels que Mimikatz) pour infecter les entreprises et utilisent des mÃ©canismes de nettoyage pour couvrir leurs traces.

Les mineurs de crypto-monnaie ont adoptÃ© plusieurs formes et utilisÃ© diffÃ©rentes approches en 2017. Les habituels mineurs de monnaies illÃ©gaux se sont ainsi empressÃ©s d'adopter les tactiques de mouvement latÃ©ral mis Ã leur disposition via des exploits comme EternalBlue et

EternalRomance, prÃ©tendument issus de la NSA, pour infecter les ordinateurs des entreprises et accentuer le minage.

Le mineur Monero Adylkuzz, qui est apparu dÃ©but de mai, Ã peu prÃ¨s en mÃªme temps que WannaCry, en est un exemple caractÃ©ristique.

Un autre dÃ©veloppement intÃ©ressant dans le paysage des menaces de 2017 est la rÃ©-Ã©mergence de Qbot (Ã©galement connu sous le nom de Brresmon ou Emotet), un ver polyvalent, avec des fonctionnalitÃ©s de dÃ©tection de rÃ©seau et de mise en place de backdoor qui existe depuis des annÃ©es.

Il est rÃ©apparu avec une refonte significative de l'infrastructure de commande et de contrÃ´le et, plus important encore, avec un moteur polymorphe utilisant le cloud, afin de lui permettre de prendre un nombre de formes pratiquement illimitÃ©es pour Ã©viter la dÃ©tection des antivirus.

Retrouvez Bitdefender en ligne