Le cotÃ© obscur du Web selon Venafi
Internet
PostÃ© par : JulieM
PubliÃ©e le : 8/11/2017 13:00:00

Sur le dark web, le trafic illicite des "Code Signing Certificates" se rÃ©vÃ¨le plus lucratif que le trafic de passeports et d'armes. Venafi et le CSRI (Cyber Security Research Institute) rÃ©vÃ¨lent le commerce florissant des certificats de signature de code

Venafi, premier Ã©diteur de solutions axÃ©es sur la protection des identitÃ©s machines, annonce les conclusions dâ□□une enquÃªte menÃ©e pendant six mois, sur les ventes de certificats numÃ©riques de signature de code rÃ©alisÃ©es sur le darkweb.

MenÃ©e pour le compte de Venafi par le CSRI (Cyber Security Research Institute), cette enquÃªte a mis en Ã©vidence lâ□□abondance de certificats de signature de code sur le darkweb, qui peuvent se nÃ©gocier jusquâ□□Ã 1 200 dollars â□□ rendant ces articles plus onÃ©reux que des passeports contrefaits, des cartes bancaires dÃ©robÃ©es et mÃªme des armes de poing aux Ã□tats-Unis.

Â« Nous savons depuis plusieurs annÃ©es que les cybercriminels recherchent activement des certificats de signature de code pour diffuser des logiciels malveillants sur ordinateurs Â», indique Peter Warren, prÃ©sident du CSRI.

Â« La preuve de lâ□□existence dâ□□un marchÃ© de la criminalitÃ© aussi consÃ©quent pour les

certificats remet en question lâ□□ensemble de notre systÃ¨me dâ□□authentification sur Internet et tÃ©moigne de lâ□□urgente nÃ©cessitÃ© de dÃ©ployer des systÃ¨mes technologiques capables de faire obstacle Ã lâ□□utilisation abusive des certificats numÃ©riques. Â»

Les certificats de signature de code servent Ã vÃ©rifier lâ□□authenticitÃ© et lâ□□intÃ©gritÃ© des logiciels et applications informatiques, et constituent un Ã©lÃ©ment essentiel de la sÃ©curitÃ© sur Internet et en entreprise. NÃ©anmoins, les cybercriminels peuvent mettre Ã profit des certificats de signature de code compromis pour introduire des malwares sur des rÃ©seaux dâ□□entreprise et Ã©quipements grand public.

Â« Notre Ã©tude rÃ©vÃ¨le que les certificats de signature de code constituent des cibles lucratives pour les cybercriminels Â», souligne Kevin Bocek, stratÃ¨ge sÃ©curitÃ© chez Venafi. Â« Les certificats de signature de code dÃ©robÃ©s rendent la dÃ©tection de logiciels malveillants quasiment impossible pour les entreprises.

Nâ□□importe quel cybercriminel peut sâ□□en servir pour fiabiliser et mener Ã bien des attaques de malwares, de ransomware et aussi des attaques cinÃ©tiques.

De plus, les certificats de signature de code pouvant Ãªtre revendus plusieurs fois avant que leur valeur ne commence Ã dÃ©croÃ®tre, ils sâ□□avÃ¨rent trÃ¨s profitables aux pirates et aux nÃ©gociants prÃ©sents sur le darkweb. Autant de facteurs qui alimentent la demande en leur faveur. Â»

Â« Bien que notre enquÃªte ait mis au jour un trafic florissant au niveau des certificats de signature de code, nous avons uniquement fait apparaÃ®tre la partie Ã©mergÃ©e de lâ□□iceberg.

Ironie du sort, nos chercheurs nâ□□ont pu, bien souvent, approfondir leurs investigations, les opÃ©rateurs du darkweb se montrant mÃ©fiants Ã leur Ã©gard. Nous soupÃ§onnons un nÃ©goce de certificats et de clÃ©s TLS, VPN et SSH tout aussi prospÃ¨re, en marge du trafic de certificats de signature de code que nous avons mis au jour Â», conclut Peter Warren.

Ã□ propos de lâ□□Ã©tude :

Cette enquÃªte a Ã©tÃ© menÃ©e pendant six mois par le CSRI en partenariat avec le Centre de cybersÃ©curitÃ© de lâ□□universitÃ© du Hertfordshire, les spÃ©cialistes du darkweb chez Flashpoint et une Ã©quipe de chercheurs indÃ©pendants. Elle a Ã©tÃ© financÃ©e par Venafi, premier Ã©diteur de solutions axÃ©es sur la protection des identitÃ©s machines.Â