FireEye rÃ©vÃ¨le la dimension mondiale des cyber-attaques Next-Gen
Internet
PostÃ© par : JPilo
PubliÃ©e le : 24/4/2013 13:00:00

Dans son Ã©tude â**The Advanced Cyber Attack Landscapeâ, FireEye** identifie 184 pays qui hÃ©bergent des serveurs de logiciels criminels. Les organisations technologiques sont les principales cibles de ces attaques. 89 % des attaques APT utilisent des outils originaires de Chine.

FireEye, Inc., le spÃ©cialiste de la lutte contre les cyber-attaques de nouvelle gÃ©nÃ©ration, annonce la parution de Â« The Advanced Cyber Attack Landscape Â» (panorama des cyber-attaques sophistiquÃ©es), un rapport qui plonge au cÅur des malwares et communications malveillantes liÃ©es aux cyber-attaques sophistiquÃ©es dans le monde.

Cette Ã©tude en trois idÃ©es clÃ©s :

â¢ 184 pays hÃ©bergent des hubs de communications ou des serveurs de type command and control (CnC), lâAsie et LâEurope de lâEst comptant pour lâessentiel de cette activitÃ© malveillante.

â¢ Les organisations technologiques figurent parmi les principales cibles de ces attaques.

â¢ La majoritÃ© des attaques APT (89 %) sont associÃ©es Ã des outils et rootkits conÃ§us et mis Ã disposition par des hackers chinois.

Â« Le panorama des menaces a Ã©voluÃ©, et les cyber-menaces ont pris une longueur dâavance sur les antivirus et autres outils traditionnels de sÃ©curitÃ© qui se basent sur des signatures virales. Ces nouvelles menaces sont prÃ©sentes Ã lâÃ©chelle mondiale et permettent aux cybercriminels de percer les lignes de dÃ©fense pour Ã©tablir des connexions au cÅur du pÃ©rimÃ¨tre dâorganisations majeures, constate David DeWalt, CEO de FireEye. LâÃ©tude de FireEye met en perspective une pandÃ©mie mondiale basÃ©e sur cette nouvelle

menace que constituent les cyber-attaques sophistiquÃ©es. Â»

Les serveurs CnC sont utilisÃ©s pendant toute la durÃ©e de vie dâ□□une attaque ciblÃ©e pour Ã©tablir des canaux de communications de type callback avec les machines infectÃ©es, permettant ainsi Ã lâ□□assaillant de tÃ©lÃ©charger et de modifier les malwares, de prÃ©server leur furtivitÃ©, dâ□□exfiltrer des donnÃ©es, ou dâ□□Ã©largir le pÃ©rimÃ¨tre dâ□□infection au sein dâ□□une organisation infectÃ©e.

Le rapport Â« The Advanced Cyber Attack Landscape Â» a Ã©tÃ© Ã©laborÃ© suite Ã lâ□□identification et la neutralisation de plus de 12 millions dâ□□Ã©vÃ©nements de type callback, dissÃ©minÃ©s sur 184 pays et enregistrÃ©s par des milliers dâ□□appareils connectÃ©s Ã la plateforme FireEye en 2012.

La plateforme FireEye se dÃ©ploie en aval des pare-feux, des pare-feux de nouvelle gÃ©nÃ©ration (NGFW), des systÃ¨mes de prÃ©vention dâ□□intrusion (IPS), des anti-virus (AV) et des autres passerelles de sÃ©curitÃ©, reprÃ©sentant ainsi lâ□□ultime ligne de dÃ©fense contre les attaques Ã©voluÃ©es qui contournent les infrastructures de sÃ©curitÃ© basÃ©es sur des signatures.

Les principaux rÃ©sultats du rapport Â« The Advanced Cyber Attack Landscape Â» sont :

â□¢ Les cyber-attaques sont devenues mondiales â□□ En 2012, les communications callback ont eu pour destination 184 pays qui hÃ©bergent des serveurs CnC, soit une progression de 41 % par rapport aux chiffres de FireEye en 2012 (130 pays).

â□¢ Lâ□□Asie et lâ□□Europe de lâ□□Est sont les principales sources des attaques â□□ En Ã©tudiant le nombre moyen de callbacks par entreprise et par pays, la Chine, la CorÃ©e, lâ□□Inde, le Japon et Hong Kong reprÃ©sentent 24% des callbacks dans le monde, suivi de prÃ¨s par les pays dâ□□Europe de lâ□□Est que sont la Russie, la Pologne, la Roumanie, lâ□□Ukraine, le Kazakhstan et la Lettonie (22%).

â□¢ Les acteurs technologiques sont les cibles principales â□□ Ces organisations technologiques ont subi la plus forte activitÃ© en matiÃ¨re de callbacks associÃ©s aux cyber-attaques. Ces organisations sont victimes de dÃ©tournement dâ□□Ã©lÃ©ments de propriÃ©tÃ© intellectuelle, de sabotage, ou de modifications de code source associÃ©es Ã des activitÃ©s cybercriminelles.

â□¢ La majoritÃ© des callback et des activitÃ©s APT ont pour origine des outils et rootkits crÃ©Ã©s par des groupuscules de hackers chinois. En associant lâ□□ADN des malwares APT connus aux callbacks, FireEye a Ã©tabli que 89 % des callback associÃ©s aux APT sont liÃ©s Ã des outils conÃ§us en Chine ou associÃ© Ã des hackers chinois. Le principal outil est le trojan (cheval de Troie) Gh0st RAT.

Pour dÃ©couvrir la cartographie interactive des callback CnC.

Pour accÃ©der Ã lâ□□Ã©tude sur les callback CnC Â« **Advanced Cyber Attack Landscape** Â».