90% des entreprises attaquées par des failles de plus de 3 ans

Les anciennes vulnérabilités système ont la vie dure. Selon le rapport «Global Threat Landscape» de Fortinet sur les menaces mondiales constatées au cours du deuxième trimestre 2017, 90% de ses entreprises clientes ont connu des tentatives d'intrusions à partir de méthodes d'exploitation de failles vieilles d'au moins trois ans. Plus étonnant encore, 60% des organisations ont été attaquées avec des exploits vieux de dix ans.

Le rapport nous apprend aussi que les attaques se déroulent majoritairement au cours du week-end. Les taux des tentatives de pénétration atteignent 22,3% le samedi et 21,4% le dimanche, par contre moins de 13% le vendredi, troisième jour le plus «dynamique» pour les charges. Un phénomène qui s'explique principalement par le fait que les équipes de sécurité se mettent en veille dans la plupart des entreprises en fin de semaine. Une négligence dont tente de tirer parti les assaillants. Par ailleurs, nombre de ces derniers exercent également un métier à plein temps qui les oblige à concentrer leurs efforts malveillants sur le week-end.

Des attaques stimulées par les outils Open Source

Les entreprises qui mettent régulièrement à jour leurs systèmes sont donc, *a priori*, protégées des tentatives d'attaques qui exploitent aussi bien des vulnérabilités récentes que les plus anciennes. D'autant que les assauts sont souvent menés juste après la révélation d'une faille par un éditeur. Publication publique généralement accompagnée d'un correctif qu'il convient de mettre à jour dans la foulée.

Les organisations qui ne le font pas prennent le risque de se mettre à découvert. Le populaire gestionnaire de contenus web WordPress est coutumier du fait. Récemment, une brèche du greffon WP Statistics menaçait quelque 300000 sites. En décembre 2015, Joomla, un autre système d'édition de contenus web, était victime d'une faille zero day. Des sites avaient été attaqués quelques jours avant la publication du correctif.

L'attrait des pirates pour les vulnérabilités anciennes s'explique notamment par le fait que les hackers ne sont pas tous des experts en cyber-espionnage capables de déjouer la résistance des systèmes. Et nombre de pirates se contentent de s'appuyer sur les outils Open Source pour exploiter des failles. Et plus celles-ci sont anciennes et plus les chances de trouver les outils adéquats en ligne augmentent. De la à conclure que la plupart des assaillants sont des pirates en herbe…

Lire également
Les conteneurs Docker, une planque pour les malwares
Les boîtes emails des entreprises sont des aimants à malware
Quand les entreprises ne vérifient pas la sécurité des services Cloud

crédit photo @ GlebStock – Shutterstock