5 raisons dâ□□Ã©voluer de la dÃ©tection Ã la prÃ©vention des programmes malveillants

Internet

PostÃ© par : JPilo
PubliÃ©e le : 24/1/2013 13:00:00

Il n'est aujourdâ□□hui plus nÃ©cessaire de dÃ©montrer aux professionnels de la sÃ©curitÃ© informatique que le paysage des **menaces est devenu de plus en plus complexe**, tendance qui continue Ã se poursuivre.

Les attaques modernes reprÃ©sentent en effet ensemble dâ□□exploits, de programmes malveillants (malwares), dâ□□applications et de techniques Ã©vasives qui se combinent sous forme dâ□□attaques continues qui peuvent durer des jours, des mois, voire des annÃ©es.

Les donnÃ©es collectÃ©es par WildFire montrent une expansion rapide de ces nouvelles menaces, souvent utilisÃ©es dans les premiÃ¨res phases dâ□□attaques persistantes, qui utilisent des techniques dâ□□Ã©vasion leur permettant de rester transparentes aux yeux des solutions de sÃ©curitÃ© classiques.

A ce jour, WildFire a dÃ©couvert plus de 70 000 nouveaux fichiers de programmes malveillants non encore identifiÃ©s par les systÃ¨mes de protection existants

Parmi ceux-ci : 5 statistiques dÃ©montrent quâ□□il est aujourdâ□□hui nÃ©cessaire dâ□□Ã©voluer vers des solutions de la prÃ©vention contre les malwares modernes.

1) Les nouveaux programmes malveillants se rÃ©pandent rapidement

ï□□ Lors de lâ□□apparition dâ□□un nouveau malware 80 % des sites touchÃ©s le sont dans les premiÃ¨res 24 heures.

ï□□ 42% du nombre total de tentatives d'infections par malwares se produisent durant les premiÃ¨res 24 heures.

2) Les malwares basÃ©s sur le web sont 3 fois plus Ã mÃªme dâ□□Ãªtre dÃ©tectÃ©s par un systÃ¨me combinant de nombreux terminaux

ï□□ Bien que le volume de malwares soit plus important au niveau de la messagerie, il existe des variÃ©tÃ©s bien plus nombreuses de malwares sur le web. Lâ□□email reste toutefois un vecteur de 6 fois plus de malwares en volume que la navigation web.

ï□□ La navigation web a toutefois Ã©tÃ© responsable dâ□□un nombre dâ□□Ã©chantillons de malwares uniques deux fois plus importants que les applications de messagerie.

3) Les proxies http et FTP sont des sources significatives de malware zero-day

ï□□ En dehors de lâ□□email et de la navigation web, les proxies HTTP comptent pour 50 % des Ã©chantillons de malwares uniques. FTP compte de son cÃ´tÃ© pour encore 20 %.

4) Les malwares cachent leur trafic aux solutions de sÃ©curitÃ© traditionnelles

ï□□ Sur les malwares zero-day nouvellement dÃ©tectÃ©s, 80 % gÃ©nÃ©raient du trafic vers internet.

ï□□ 60 % des malwares gÃ©nÃ¨rent un trafic Ã©vasif â□□ incluant lâ□□utilisation de ports non-standards, des DNS dynamiques et des proxies.

5) Les malwares sont sources de piratages additionnels

ï□□ 41 % des malwares procÃ¨dent Ã des activitÃ©s de piratage supplÃ©mentaires, comprenant la dÃ©couverte d'ordinateurs, le scan de vulnÃ©rabilitÃ©s et la cartographie du rÃ©seau.

Les entreprises sont aujourdâ□□hui confrontÃ©es Ã des changements majeurs dans la nature des menaces contre lesquelles elles doivent lutter. Pour y rÃ©pondre, les spÃ©cialistes de lâ□□industrie de la sÃ©curitÃ© ont commencÃ© Ã adopter une approche plus globale et intÃ©grÃ©e. De la mÃªme maniÃ¨re que nous pouvons bÃ©nÃ©ficier de la corrÃ©lation de l'information provenant de nos propres silos de sÃ©curitÃ©, nous pouvons Ã©galement profiter de ce que dâ□□autres Ã©quipes de sÃ©curitÃ© peuvent Ãªtre amenÃ©es Ã rencontrer. Si ces spÃ©cialistes pouvaient s'engager Ã amÃ©liorer leur collaboration, cela permettrait de mieux dÃ©tecter et suivre les infections Ã©mergentes et de conserver une longueur dâ□□avance sur les techniques des nouveaux logiciels malveillants.