Ver Sober.P: dans l'attente d'une attaque massive ?...

Les éditeurs et services de sécurité sont sur les dents? Le ver Sober.P s'annonce particulièrement agressif et a annoncé la couleur pour ce lundi 23 mai.

Sober.P n'est pas un inconnu, sauf que l'on ne sait pas au juste s'il est dérivé de Sober.S, celui là même qui pour attirer le chaland promettait des places gratuites pour la prochaine coupe du monde de football. Ou l'inverse, peut-être? En réalité, Sober.P est un cheval de Troie dormant, qui s'est diffusé massivement par « spam » depuis l'Allemagne, comme les versions 'Q' et 'S', mais qui vient de révéler un secret inquiétant... CipherTrust, éditeur de solutions de sécurité, annonce avoir découvert dans le code de Sober.p une menace écrite de son auteur. Ce dernier indique que le ver devait lancer ses attaques à compter de ce lundi 23 mai. Quel type d'attaque ? C'est l'inconnue. Vraisemblablement, un virus ou une attaque par déni de service. Là où la menace devient sérieuse, c'est que d'un éditeur d'anti-virus à l'autre, les versions 'p', 'q', 'r' ou 's' de Sober créent la confusion. Il s'y ajoute, en prime, les pratiques des éditeurs qui nomment leurs découvertes sans se concerter. Ces versions pourraient n'avoir qu'une souche unique ! Si c'est le cas, Sober.P pourrait profiter d'un gigantesque '*botnet*' ? '*roBOT NETwork*' – qui qualifierait un large volume d'ordinateurs vérolés compromis par un ver, également appelé '*zombie army*'. Double menace, en réalité, car son auteur a fait preuve de plus d'ingéniosité encore : il a incorporé une dose de hasard dans son code ! Toutes les heures, un algorithme sur le poste infecté crée une clé temporaire qui génère une URL aléatoire transmise à l'un des cinq services hôtes ciblés en Allemagne et en Autriche. Avec cette URL aléatoire et cette rotation de serveurs, il devient très difficile de repérer la prolifération du 'spam' en mailing de masse; très difficile de répérer l'attaque et de remonter à la source du « zombie ». Et comme il est plus difficile encore de bloquer un serveur hôte, Sober.p peut évoluer en toute tranquillité. En revanche, comme pour la plupart des vers et virus, la menace existe, elle a été identifiée, mais son ampleur reste une inconnue?