Avec Sonar, Microsoft pousse la chasse aux malware dans Azure

Microsoft est en quête de compétences pour renforcer son équipe de développeurs travaillant sur le projet Sonar. L'entreprise est à la recherche de profils spécialisés dans le domaine de la sécurité. *« Le candidat retenu pour ce poste vient de l'environnement des services avec une expérience en matière de logiciels de sécurité »*, indique l'annonce du poste à pourvoir au siège américain de Microsoft.

Mais que recouvre Project Sonar précisément (à ne pas confondre avec le projet de recherche en sécurité homonyme de Rapid7)□? Probablement un service Azure dédié à la sécurité. Selon le descriptif de l'annonce, *« l'équipe Sonar construit et exploite une plate-forme as-a-service de 'détonation' de logiciels malveillants à base de VM. Notre système fait tourner jusqu'à des dizaines de milliers de machines virtuelles par jour pour détecter les logiciels malveillants et protéger les clients. Nous l'avons déployé dans des endroits comme Windows App Store et Exchange Online. »*

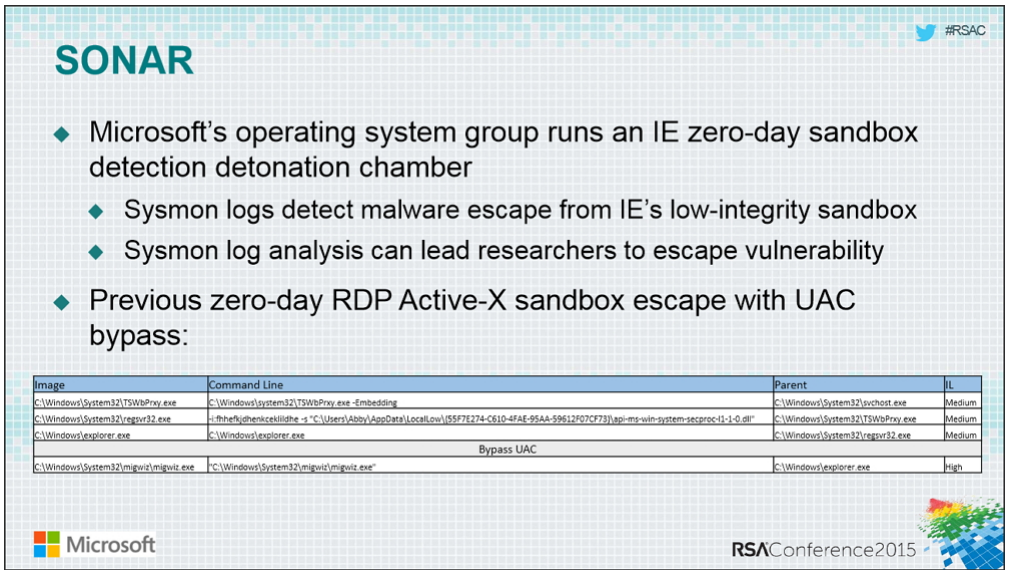
Des millions de malwares analysés

Cette solution de sécurité *« analyse dynamiquement des millions d'exploits potentiels (outils de piratage, NDLR) et d'échantillons de malwares dans des machines virtuelles et collecte des téraoctets de données quotidiennement »*, précise une précédente offre d'emploi, toujours consacrée au projet Sonar. L'objet du recrutement portait cette fois au développement d'un outil en ligne, Analyst Studio, visant à filtrer et analyser les données ainsi récoltées afin de les utiliser à travers d'autres solutions de sécurité de la firme.

ZDNet remarque que, lors de l'événement Ignite 2015, en mai dernier, une diapositive de la conférence baptisée «□Deep dive how Microsoft handles spam and advanced email threats□» (Plongée en profondeur sur la façon dont Microsoft prend en charge le spam et les menaces avancées par email) laissait transparaitre l'existence d'une «□detonation chamber□» utilisée pour sécuriser les services Exchange Online. Cette «□chambre de détonation□», évoquée dans le projet Sonar, s'apparente à un bac-a-sable (sandbox) de filtrage des données en amont des services de messagerie récemment introduit dans le service Exchange Online Advanced Threat Protection (ATP). Lequel s'appuie sur une machine virtuelle Azure et des technique d'intelligence artificielle (machine learning) pour déjouer les tentatives d'intrusion des agents malveillants.

Sonar utilisé en interne

Par ailleurs, à l'occasion de la RSA Conference 2015, Mark Russinovich, CTO d'Azure, indiquait que l'équipe de développement du système d'exploitation chez Microsoft utilise un Internet Explorer équipé de la « chambre de détonation » pour détecter les malwares et échapper à l'exploitation des vulnérabilité à partir de l'analyse des logs (voir capture ci-dessous).



S'il est donc visiblement clair que Microsoft développe et s'appuie sur des outils d'analyse des données pour déceler et prévenir les menaces qui tentent de s'introduire sur un réseau d'entreprise, il reste à savoir si Sonar restera confiné aux services de l'éditeur ou si ce dernier le commercialisera d'une manière ou d'une autre directement à ses clients depuis son Cloud Azure. Cette dernière hypothèse semble la plus probable puisque l'éditeur expliquait, dans son offre d'emploi, que *« nous portons le service au prochain niveau pour gérer plus de clients et de données à grande échelle »*.

Lire également

Sécurité : Adallom passe sous la coupe de Microsoft
Microsoft soigne la sécurité de son navigateur web Internet Explorer
4 failles zero day dans IE publiées, que fait Microsoft ?

crédit photot © Nikuwka – shutterstock