Chronologie de défense contre le Ransomware ‘Wannacry’

Bulletin de sécurité Microsoft
14 mars 2017

Le 14 mars, Microsoft publie un correctif (MS17-010) pour une nouvelle vulnérabilité SMB.

Cisco NGFW | Meraki MX
14 mars 2017

Le jour même, Cisco Talos publie la signature Snort™ #41978 pour détécter les vulnérabilités identifiées dans MS17-010.

Shadow Brokers
14 avril 2017

Le groupe “The Shadow Brokers” rend public un ensemble de vulnérabilités qui seraient issues de la NSA (National Security Agency) nommées Eternal Blue and Double Pulsar.

Cisco NGFW | Meraki MX
25 avril 2017

Talos publie les signatures Snort™ #42329, #42332, #42340 pour Double Pulsar et pour le partage SMB anonymes.

Cisco TALOS

Avec une équipe de plus de 250 chercheurs et un réseau de connaissance et de données unique au monde, Cisco continue ses recherches et protège nos clients contre « Wannacry » et autres menaces émergentes.

Cisco Umbrella
12 mai 2017 | 10:12 GMT

Cisco Umbrella attribue le type ransomware à l’attaque et bascule le kill switch domain dans la catégorie malware.

Cisco AMP
12 mai 2017 | 9:33 GMT

Environ 60 minutes après l’apparition des premiers échantillons, AMP détecte le ransomware. La menace a été identifiée grâce aux analyses automatiques et méthodes de détection de faible prévalence.

AMP a détecté et bloqué la menace avec succès sur les terminaux, passerelles mail/web et sécurité périmétrique (firewall, IPS).

Cisco Umbrella
12 mai 2017 | 7:43 GMT

Cisco Umbrella ajoute au niveau mondial le domaine du kill switch dans la catégorie des Nouveaux Domaines Découverts, assurant ainsi la protection contre le ransomware et la diffusion du vers.

Cisco Investigate
12 mai 2017 | 7:30 GMT

@MalwareTechBlog informe d’une nouvelle attaque baptisée ‘WannaCry’ sur son compte Twitter et son blog.

Il partage un screenshot Cisco Investigate attestant de ses recherches et de sa découverte.

Pour plus d'informations, rendez-vous sur **cisco.fr** et **talosintelligence.com**