Verlauf der Verteidigung gegen den „WannaCry“ Ransomware-Angriff

Microsoft-Security Bulletin
14. März 2017

Am 14. März stellte Microsoft einen Patch (MS17-010) für eine neue SMB-Schwachstelle bereit.

Cisco NGFW | Meraki MX
14. März 2017

Am selben Tag veröffentlichte Cisco Talos die Snort™-Signatur #41978, um Schwachstellen zu ermitteln, die in MS17-010 identifiziert wurden.

Shadow Brokers
14. April 2017

Eine Gruppe, die sich „Shadow Brokers“ nennt, veröffentlichte eine Reihe von Schwachstellen, die angeblich von der National Security Agency (NSA) und unter den Namen „Eternal Blue“ sowie „Double Pulsar“ bekannt sind.

Cisco NGFW | Meraki MX
25. April 2017

Talos veröffentlicht die Snort™ Signaturen #42329, #42332 und #42340 für Double Pulsar und anonyme SMB-Freigaben.

Cisco TALOS

Mit mehr als 250 fachkundigen Forschern in der ganzen Welt und einem globalen Netzwerk von Intelligence- und Datenquellen sorgt Cisco weiterhin für Überwachung, Weiterentwicklung und den Schutz seiner Kunden vor „WannaCry“ und anderen aufkommenden Bedrohungen.

Cisco Umbrella
12. Mai 2017 | 10:12 Uhr (UTC)

Cisco Umbrella ordnet den Angriffstyp dem Attribut „Ransomware“ zu und verschiebt die Kill-Switch-Domain in die Kategorie „Malware“.

Cisco AMP
12. Mai 2017 | 09:33 Uhr (UTC)

Etwa 60 Minuten nach den ersten Stichproben erkennt AMP die Ransomware. Die Bedrohung wurde über automatische Analyseregeln und Low-Prevalence-Methoden erkannt.

AMP hat die Bedrohung erfolgreich auf Endgeräten, in E-Mail- und Web-Gateways sowie in der Netzwerksicherheit erkannt und blockiert.

Cisco Umbrella
12. Mai 2017 | 07:43 Uhr (UTC)

Cisco Umbrella integriert eine Kill-Switch-Domain global in „Newly Seen Domains“-Kategorien und ermöglicht so einen Schutz gegen die Ransomware sowie eine weitere Verbreitung des Wurms.

Cisco Investigate
12. Mai 2017 | 7:30 Uhr (UTC)

@MalwareTechBlog veröffentlicht Informationen über einen neuen Angriff mit der Bezeichnung „WannaCry“ via Twitter und seinen Blog.

Im Blog wurde ein Screenshot von Cisco Investigate gezeigt, da er als Teil der Informationssuche und -sammlung verwendet wurde.

Weitere Informationen finden Sie unter **cisco.de** und **talosintelligence.com**.