ในช่วงหลายวันที่ผ่านมา หลายๆ ท่านอาจจะได้ยินข่าว หรือประสบปัญหาพบการโจมตี จากไวรัสที่ชื่อ WannaCry เวอร์ชั่นใหม่ ซึ่งมีการแพร่ระบาดอย่างรวดเร็ว โดยมีการตรวจพบการโจมตีเป็นวงกว้างทั่วทั้งโลก นับตั้งแต่วันที่ 12 พฤษภาคม เป็นต้นมา

โดยไวรัส WannaCry เป็นไวรัสประเภท Crypto Ransomware ซึ่งจะทำการเข้ารหัสไฟล์ บนเครื่องที่ติดเชื้อ และเรียกค่าไถ่ราวๆ 300 เหรียญสหรัฐ ผ่านสกุลเงิน Bitcoin และจะเพิ่มค่าไถ่เป็นสองเท่าหลังจาก 3 วัน และจะลบไฟล์หลังจากติดเชื้อไปแล้ว 7 วัน สิ่งที่ทำให้ไวรัสตัวนี้แพร่ระบาดอย่างรวดเร็วเนื่องมาจาก เทคนิคที่ไวรัสใช้ในการโจมตี ซึ่งเป็นช่องโหว่ SMBv1 remote code execution บนระบบปฏิบัติการ Windows (ทาง Microsoft ออก patch เพื่อแก้ไขช่องโหว่นี้ในวันที่ 14 มีนาคมที่ผ่านมา) โดยช่องโหว่นี้มาจาก เครื่องมือโจมตีชื่อ Eternal Blue ที่ถูกกลุ่มแฮกเกอร์ Shadow Brokers ปล่อยข้อมูล และเครื่องมือดังกล่าวออกมาในวันที่ 14 เมษายน

คุณจะป้องกันตัวได้อย่างไร ในสถานการณ์นี้?

ทาง Symantec มี Security Solution แบบครบวงจร ที่ช่วยปกป้องเครือข่ายของคุณให้ปลอดภัย ตั้งแต่ Gateway มาจนถึง Endpoint

Symantec Endpoint Protection 14 ระบบป้องกันไวรัสบนเครื่องปลายทางแห่งอนาคตที่มีเทคโนโลยี Advanced Machine Learning สามารถตรวจจับไวรัสตระกูลนี้ได้ตั้งแต่ 31 มีนาคมที่ผ่านมา และด้วยเทคโนโลยี Intrusion Prevention System ที่ช่วยป้องกันการโจมตีทางเครือข่าย โดยสามารถป้องกันไวรัสที่โจมตีช่องโหว่นี้ ได้ตั้งแต่ช่วงต้นเดือนพฤษภาคม เราแนะนำให้ทางลูกค้าเปิดใช้งาน Advanced Machine Learning, Intelligent Threat Cloud, SONAR และ Download Insight เพื่อช่วยให้การป้องกันไวรัสสายพันธุ์ใหม่ๆ ได้อย่างมีประสิทธิภาพ

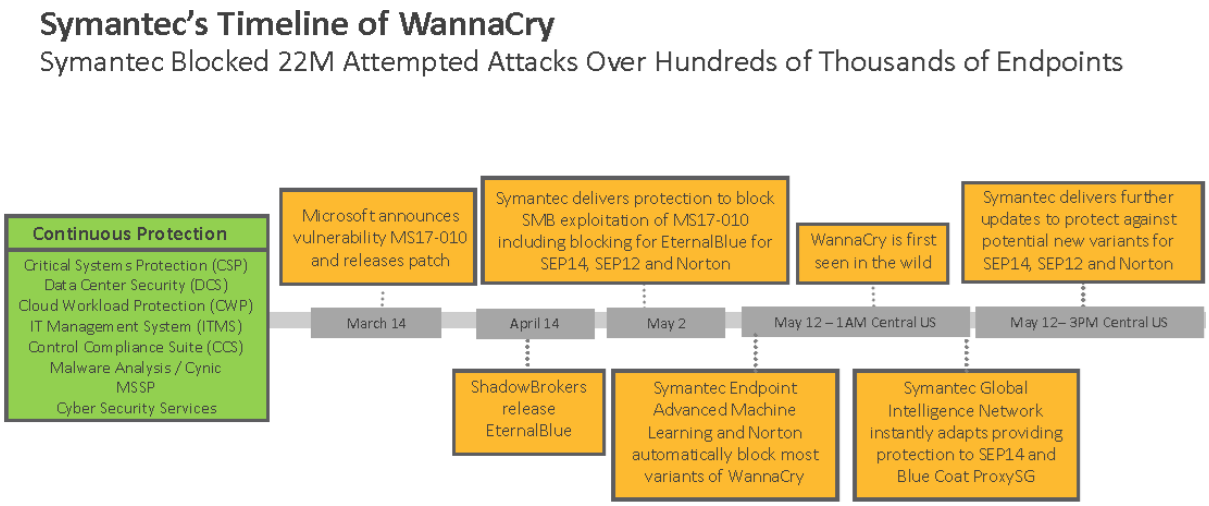
นอกจากนี้ สำหรับองค์กรขนาดใหญ่ที่เน้นการป้องกันเป็นพิเศษ สามารถซื้อ Advanced Threat Protection Module ซึ่งเป็นระบบ Sandbox เพิ่มเติม เพื่อช่วยให้การตรวจจับไวรัสประเภท Targeted attacks เป็นไปได้อย่างมีประสิทธิภาพสูงสุด

ลูกค้า Bluecoat Advanced Secure Gateway และ Bluecoat Content Analysis จะได้รับการป้องกันที่ระดับ Gateway/Proxy อย่างมีประสิทธิภาพเช่นเดียวกัน โดยข้อมูลของไวรัสทุกสายพันธุ์ที่ทาง Bluecoat หรือ Symantec เจอ จะได้รับการอัพเดต และเชื่อมโยงกันโดยอัตโนมัติ

สำหรับระบบ Server ที่ต้องการป้องกันเป็นพิเศษ ทาง Symantec มี Solution Data Center Security: Server Advanced ที่ได้รับการออกแบบมาเพื่อปกป้องเครื่องแม่ข่ายโดยเฉพาะ ด้วยเทคโนโลยี Signature-less, Application isolation, Whitelisting และ Privilege de-escalation technologies ทำให้ช่วยป้องกันเครื่องแม่ข่ายได้อย่างมีประสิทธิภาพ โดยไม่ต้องการการอัพเดต Signature อีกต่อไป

สำหรับการอัพเดตระบบปฏิบัติการ และโปรแกรม 3rd party ต่างๆ ทาง Symantec มี Solution Altiris Patch Management เพื่อช่วยผู้ดูแลระบบลดภาระในการ Deploy patch สำคัญต่างๆ ไปยังระบบที่เกี่ยวข้อง โดยไม่ขัดขวางการทำงานตามปกติ

และสำหรับลูกค้าที่กังวลการโจมตีทางอีเมล์ ซึ่งปัจจุบันนับว่าเป็นช่องทางในการโจมตีมากที่สุด ช่องทางหนึ่งทาง Symantec มี Solution E-mail Security.cloud ที่มีเทคโนโลยี Skeptic, Click time Protection และ Real-time link following technologies เพื่อช่วยปกป้องคุณจากไวรัสสายพันธุ์ใหม่บนระบบอีเมล์ ได้อย่างมีประสิทธิภาพ



ข้อแนะนำโดยสรุป สำหรับลูกค้า ให้ทำการอัพเดตระบบต่างๆ ให้เป็นปัจจุบันอยู่เสมอ ทั้งระบบปฏิบัติการ, โปรแกรมที่ใช้งานต่างๆ รวมทั้ง Security Solution ที่ติดตั้งไว้ เพื่อให้การป้องกันมีประสิทธิภาพสูงสุด

Patch และข้อมูลที่เกี่ยวข้อง

https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx