Carbon Black.

Next-generation Endpoint Security – แนวป้องกัน Advanced Threats รูปแบบใหม่

CARBON BLACK

ปัจจุบันการโจมตีทางด้าน Cyber Security มีรูปแบบที่หลากหลาย เพื่อหลบเลี่ยงแนวป้องกันที่เป็น Network Security โดยจากเดิมที่เน้นการโจมตีแบบแพร่กระจายให้รวดเร็วที่สุด หรือการโจมตีไปที่การทำให้ระบบหยุดให้บริการ เปลี่ยนเป็นการโจมตีที่โฟกัสเป้าหมายเฉพาะกลุ่มมากขึ้น โดยเน้นการปฏิสัมพันธ์กับมนุษย์ได้มากที่สุด เพื่อล่อลวงให้ผู้ใช้ในองค์กร ที่เป็นผู้ที่มีความตระหนักรู้ทางด้าน Cyber Security น้อยที่สุด ทำการดาวน์โหลด Malicious Software มาติดตั้งที่เครื่องคอมพิวเตอร์ของตน จากนั้นแฮ็คเกอร์ จึงทำการเข้าถึงเครื่องคอมพิวเตอร์ผ่าน Command & Control Server โดยแฮ็คเกอร์จะใช้ประโยชน์จากแอพพลิเคชันหรือเครื่องมือบนระบบปฏิบัติการบนคอมพิวเตอร์นั้นๆ เข้าทำการโจมตีไปยังเซิร์ฟเวอร์ที่เก็บข้อมูลสำคัญและทำการขโมยออกไป หรือทำการเข้ารหัสข้อมูลแล้วเรียกเก็บเงินค่าไถ่

Carbon Black: Next-generation Endpoint Security ทำงานได้อย่างไร

เพื่อที่จะหยุดและตรวจสอบ Advanced Threats ให้ได้ผล สิ่งที่ Next-generation Endpoint Security ทำคือ

1. จับตาดูทุกความเคลื่อนไหว – ทำการบันทึกกิจกรรมที่เป็นการรันการทำงานต่างๆ การเปิดแอพพลิเคชัน การติดตั้งซอฟต์แวร์ ที่ดูมีความผิดปกติ

2. ทำ Centralize ข้อมูลนั้น – ทำการส่งข้อมูลแบบเรียลไทม์มายัง Centralized Server แล้วทำการเชื่อมโยงความสัมพันธ์ขั้นตอนของการโจมตีเพื่อสร้างแผนผังรูปแบบของการโจมตีของทั้งองค์กรจากคอมพิวเตอร์ปลายทางทุกเครื่อง โดยจะไม่กระทบกับทรัพยากรบนคอมพิวเตอร์นั้นๆ

3. Customize Threat Detection – เช่นเมื่อคอมพิวเตอร์เปิดไฟล์ PDF แล้วมีการเรียกใช้งานแอพพลิเคชันอื่นๆ หรือมีการเรียก Process อื่นๆ หรือมีการสร้าง Connection เชื่อมต่อไปที่เครื่องข้างเคียงหรือไม่ โดยรูปแบบต่างๆ เหล่านี้จะมาจาก Predefine ของ Carbon Black และ Threat Intelligence จาก MSSP และ Incident Response ชั้นนำทั่วโลก ทำให้เราสามารถดึงรูปแบบของการตรวจจับเข้ามาใช้งาน และปรับให้เข้ากับองค์กรได้อย่างง่ายดายนอกจากนั้นยังสามารถสร้างรูปแบบได้ด้วยตัวเองเพื่อให้เหมาะสมกับนโยบายขององค์กร

4. Unraveling the Entire Attack – ทำการคลายปมของการโจมตี ในการโจมตีหลักๆ แล้วแฮ็คเกอร์มักเลือกที่จะโจมตีไปยังช่องโหว่ที่มีการเปิดเผยให้เป็นที่ทราบกันอยู่แล้ว หรืออีกวิธีคือการขโมยข้อมูลชื่อผู้ใช้และรหัสผ่านเพื่อการเข้าถึงข้อมูล ซึ่งหากเราสามารถวาดภาพรูปแบบการโจมตีได้ และทำการตามรอยหรือตรวจสอบแต่ละขั้นไปที่ต้นทางการโจมตีก็จะทำให้เราเข้าใจถึงต้นเหตุ (Root Cause) และสามารถแก้ปัญหาได้ตรงจุด ว่าใครรันรันที่ Process อะไร ไปที่ไหนบ้าง ไฟล์แปลกปลอมมาจากไหน Web, Gmail, USB, Disk ฯลฯ

5. Apply Multiple Forms of Prevention – เนื่องจากคอมพิวเตอร์ปลายทางแต่ละเครื่อง ทำงานคนละงาน ดังนั้น แต่ละเครื่องจึงมีความเสี่ยงไม่เท่ากัน เช่น เครื่องที่แผนกบัญชีจะมีรูปแบบการใช้งานแอพพลิเคชันที่แตกต่างจาก แผนกพัฒนาซอฟต์แวร์ จึงจะต้องทดสอบโค้ดของโปรแกรม ดังนั้น Next-generation Endpoint Security จะต้องสามารถสร้างนโยบายและความเข้มงวดที่แตกต่างกันตามบทบาทหน้าที่ได้

6. การเชื่อมต่อเพื่อขยายขอบเขตการป้องกันในปัจจุบัน – การเชื่อมต่อกันระหว่าง Security Solutions เป็นสิ่งที่จำเป็น เพื่อประสานข้อมูลซึ่งกัน

และกัน และทำให้การป้องกันครบวงจรมากขึ้นโดยการเชื่อมต่อมี 3 รูปแบบ

6.1 Prevention เชื่อมต่อกับ Network Security Appliance เพื่อปกป้องการโจมตีจาก Network มายัง Endpoint

6.2 Detection เชื่อมต่อกับ SIEM เพื่อความแม่นยำของ SIEM Alerts ทำให้ทราบผลกระทบที่แท้จริงว่า Rule ใดมีผลกระทบจริงๆ

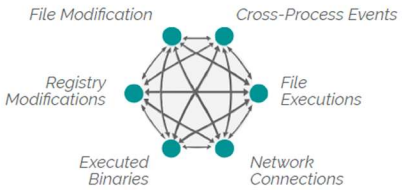
6.3 Response เชื่อมต่อกับ PLCM หรือ Patch Management เช่น เมื่อพบว่ามีการเข้าถึงช่องโหว่ใด ก็ทำการเรียกใช้งานแพทช์เพื่ออุดช่องโหว่นั้นได้อย่างทันท่วงที

7. Recovery Collection Defense – เนื่องจากความมั่นคงปลอดภัยเป็นกระบวนการอาศัยทั้ง System, Knowledge และ People ทำให้เราไม่สามารถที่จะทำงานได้คนเดียว Carbon Black ทำการแชร์ Community จากทั่วโลกที่ใช้งาน เข้าถึงกันและกันได้

รูปที่ 1

ภาพแสดงวิธีการจารกรรมบนไซเบอร์ (The 7 stages of the cyber kill chain)

รูปที่ 2



ภาพแสดง Watch Every Move จับตาดูทุกกิจกรรมการทำงานของไฟล์และแอพพลิเคชัน

CONTACT INFO

nForce Secure CO., LTD.

Tel: 02-274-0984

E-Mail: Sale@nforcesecure.com

Website: www.nforcesecure.com

Line Official: nForcesecure

Facebook: nForceSecure