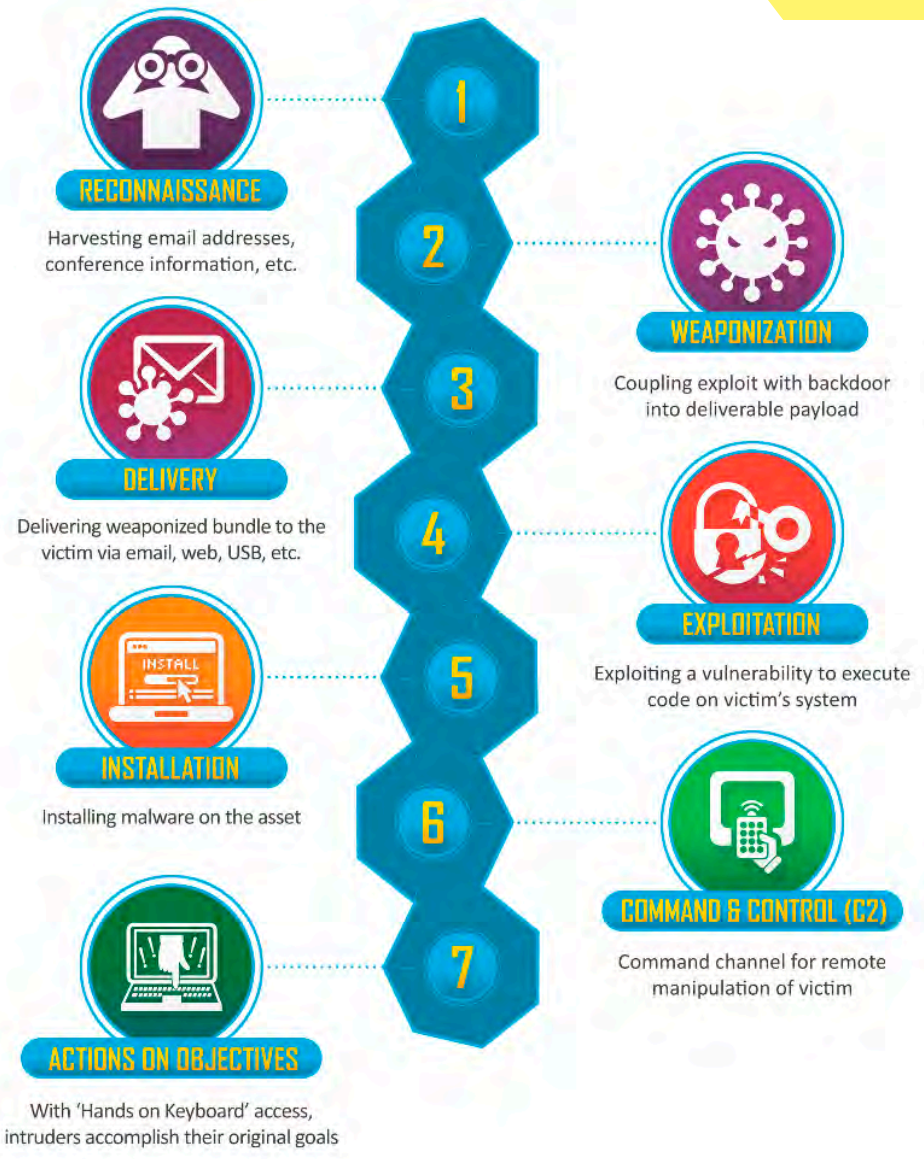
ห่วงโซ่การโจมตีทางไซเบอร์
Cyber Kill Chain

น.อ.เอกชัย สิงห์ทอง



ห่วงโซ่การโจมตีทางไซเบอร์ ๗ ขั้นตอน

ที่มา

การโจมตีทางไซเบอร์นั้นมีกระบวนการหลายขั้นตอน แตกต่างกันไปตามกลยุทธ์ของผู้โจมตี การระบุขั้นตอนการโจมตีแยกเป็นขั้น ๆ เกี่ยวเนื่องกันเป็นห่วงโซ่ จะเป็นประโยชน์ในการศึกษาและรับมือการโจมตี บริษัท Lockheed Martin จึงได้พัฒนาโมเดลห่วงโซ่การโจมตีทางไซเบอร์ (Cyber Kill Chain) ผู้เขียนขอแปล Kill เป็นการโจมตี เพราะให้ความหมายที่ตรงและเหมาะสมมากกว่า และได้รับการยอมรับถูกใช้อ้างอิงในทางวิชาการและยุทธการอย่างกว้างขวางจนถึงปัจจุบัน

ผู้เขียนจึงอยากปลุกใจผู้อ่านทุก ๆ ท่าน ให้มาทำความเข้าใจห่วงโซ่การโจมตีทางไซเบอร์ เพื่อที่ทุก ๆ ท่านจะได้เข้าใจ สิ่งที่แฮ็กเกอร์กระทำเมื่อท่านถูกโจมตีจะสามารถคาดเดาได้ว่าอยู่ในกระบวนการใดของการโจมตี และการประสานกับทีมป้องกันหรือตอบสนองทางไซเบอร์จะได้สื่อสารเข้าใจตรงกันมากยิ่งขึ้น และที่สำคัญที่สุด คือ ความเข้าใจแนวทางในการป้องกันของแต่ละขั้นตอนในมุมมองของท่านผู้อ่านนั่นเอง

ห่วงโซ่การโจมตีทางไซเบอร์ ๗ ขั้นตอน ประกอบด้วย

๑. การลาดตระเวน (Reconnaissance) : ผู้โจมตีจะรวบรวมข้อมูลเกี่ยวกับเป้าหมายเพื่อระบุช่องโหว่และเส้นทางการโจมตีที่จะใช้ โดยส่วนใหญ่จะเป็นข้อมูลที่อยู่บนโลกอินเทอร์เน็ตหรือสื่อสังคมออนไลน์ต่าง ๆ ผู้ใช้ทั่วไปมักเข้าใจผิดว่า สื่อสังคมออนไลน์ หรือเว็บไซต์ที่น่าเชื่อถือจะมีกระบวนการรักษาความปลอดภัยดีมากอยู่แล้ว ไม่น่าจะมีข้อมูลรั่วไหลอกมาได้ แต่จริง ๆ แล้วเครื่องมือที่ใช้รวบรวมข้อมูลที่ผู้โจมตีใช้งานนั้น มีศักยภาพสูงมาก สามารถรวบรวมทั้งจากทางตรงและทางอ้อมได้

แนวทางการป้องกัน คือ

- ระมัดระวังในการแบ่งปันข้อมูลส่วนบุคคลหรือข้อมูลที่ละเอียดอ่อนทางออนไลน์ โดยเฉพาะบนแพลตฟอร์มสื่อสังคมออนไลน์ทั้งหลาย
- ใช้การตั้งค่าความเป็นส่วนตัวเพื่อจำกัดข้อมูลที่เปิดเผยต่อสาธารณะในบัญชีสื่อสังคมออนไลน์
- ระวังอีเมลหลอกล่อและโทรศัพท์ที่อาจขอข้อมูลส่วนบุคคลหรือข้อมูลรับรองการเข้าสู่ระบบ

๒. การจัดเตรียมอาวุธ (Weaponization) : ผู้โจมตีจะสร้างอาวุธ หรือรวบรวมอาวุธที่จะใช้โดยการโหลดจากเว็บไซต์หรือซอฟต์แวร์ที่ใช้หาช่องโหว่ต่าง ๆ อาวุธที่เตรียมก็จะสอดคล้องกับเส้นทางการโจมตีที่วางแผนไว้ จะเห็นได้ว่ามีความเกี่ยวเนื่องกับขั้นตอนที่ ๑ เป็นลักษณะห่วงโซ่ จึงเป็นที่มาของชื่อโมเดลนี้นั่นเอง อาวุธจะอยู่ในรูปแบบที่หลากหลาย หากเป็นการโจมตีไปที่ผู้ใช้งานส่วนใหญ่จะเป็นอีเมลหลอกล่อ (Phishing email) หรือ เว็บไซต์หลอกล่อ (Phishing website)

แนวทางการป้องกัน คือ

- ระวังข้อความอีเมลหรือไฟล์แนบที่น่าสงสัย แม้ดูเหมือนว่าจะมาจากคนที่ท่านผู้อ่านรู้จักก็ตาม
- อย่าเปิดไฟล์แนบหรือคลิกลิงก์ในอีเมลจากแหล่งที่ไม่รู้จักหรือน่าสงสัย
- ใช้ซอฟต์แวร์ป้องกันมัลแวร์และปรับปรุงให้ทันสมัยอยู่เสมอเพื่อตรวจหาและป้องกันการติดตั้งมัลแวร์

๓. การส่งอาวุธ (Delivery) : ผู้โจมตีจะส่งอาวุธที่จัดเตรียมไว้ไปถึงเป้าหมาย ในการโจมตีผู้ใช้งานมักจะเป็นการส่งอีเมลหลอกล่อ ข้อความหลอกล่อ ผ่านทางสื่อสังคมออนไลน์ต่าง ๆ

แนวทางการป้องกัน คือ

- ระมัดระวังเมื่อท่องอินเทอร์เน็ตและหลีกเลี่ยงการคลิกลิงก์ที่น่าสงสัยหรือเยี่ยมชมเว็บไซต์ที่ไม่น่าเชื่อถือ

- ใช้เว็บเบราว์เซอร์ที่มีคุณสมบัติความปลอดภัยในตัว เช่น ตัวบล็อกพ็อปอัปและการป้องกันฟิชชิ่ง

- ระวังกลวิธีทางวิศวกรรมสังคมที่ใช้ในอีเมลหลอกล่อ เช่น คำขอด่วนสำหรับการดำเนินการหรือข้อเสนอที่ดูดีเกินจริง

๔. การเจาะระบบ (Exploitation) : ในขั้นตอนนี้ผู้โจมตีจะเจาะระบบของเป้าหมายเป็นครั้งแรก เช่น ผู้ใช้อาจจะหลงกลเปิดอ่านอีเมลหลอกล่อ แล้วคลิกลิงก์โหลดโปรแกรมหรือไฟล์ที่ถูกแนบมากับอีเมล ซึ่งถูกสอดแทรกคำสั่งโจมตีไว้แล้วในขั้นตอนที่ ๒ หรือ ผู้ใช้หลงกลคลิกลิงก์ที่ส่งมาทางสื่อสังคมออนไลน์แล้วเข้าไปยังเว็บไซต์ที่มีคำสั่งโจมตีฝังไว้อยู่ เป็นต้น เมื่อเจาะระบบสำเร็จผู้โจมตีก็จะสามารถเข้าถึงข้อมูลภายในเครื่องเป้าหมายได้

แนวทางการป้องกัน คือ

- อัปเดตระบบปฏิบัติการและซอฟต์แวร์ของท่านผู้อ่านให้ทันสมัยอยู่เสมอด้วยแพทช์ (Patch) คือ โปรแกรมซ่อมแซมจุดบกพร่องหรือปรับปรุงข้อมูลโปรแกรมคอมพิวเตอร์ให้ทันสมัยอยู่เสมอ

- ใช้ซอฟต์แวร์ป้องกันมัลแวร์และปรับปรุงให้ทันสมัยอยู่เสมอเพื่อตรวจหาและป้องกันการติดตั้งมัลแวร์

- ระมัดระวังเมื่อดาวน์โหลดและติดตั้งซอฟต์แวร์ โดยเฉพาะจากแหล่งที่ไม่น่าเชื่อถือ

๕. การติดตั้งอาวุธเพิ่มเติม (Installation) : ภายหลังจากเข้าไปในระบบของเป้าหมายได้แล้ว ส่วนใหญ่จะได้สิทธิ์การใช้งานในระดับต่ำ หรือรันคำสั่งได้จำกัดไม่สะดวก ผู้โจมตีก็จะทำการติดตั้งอาวุธเพิ่มเติม เพื่อช่วยอำนวยความสะดวก

แนวทางการป้องกัน คือ

- อย่าติดตั้งซอฟต์แวร์หรือแอปพลิเคชันจากแหล่งที่ไม่น่าเชื่อถือ

- ขณะที่กำลังติดตั้งแอปพลิเคชันให้ระวังการอนุญาตที่แอปพลิเคชันร้องขอ และให้สิทธิ์ที่จำเป็นเพื่อให้แอปพลิเคชันทำงานอย่างถูกต้องเท่านั้น

- ใช้การยืนยันตัวตนแบบ ๒ ปัจจัย เพื่อเพิ่มความปลอดภัยอีกชั้นให้กับการเข้าสู่ระบบสำคัญ

๖. การบัญชาการและควบคุม (Command and Control (C2, CnC)) : ขั้นตอนนี้ผู้โจมตีจะควบคุมสั่งการเครื่องเหยื่อจากระยะไกล ผ่านเครื่องแม่ข่ายที่ใช้บัญชาการและควบคุม เครื่องเหยื่อจะมีการติดต่อกลับไปยังเครื่องแม่ข่ายบัญชาการและควบคุมเป็นระยะ ๆ เพื่อให้ผู้โจมตีรู้สถานะของเครื่องเหยื่อ

มาถึงจุดนี้ผู้อ่านอาจสงสัยว่าทำไมต้องมีการติดต่อกลับไปยังเครื่องแม่ข่ายของผู้โจมตี ทำไมต้องมีเครื่องแม่ข่ายบัญชาการและควบคุมด้วย คำตอบคือ การโจมตีในปัจจุบัน ต้องใช้ระยะเวลาในการโจมตีแต่ละขั้นตอน น้อยครั้งที่จะดำเนินการสำเร็จทุกขั้นตอนในช่วงเวลาสั้น ๆ ได้ เมื่อเจาะระบบได้แล้ว ยังจะต้องสำรวจภายในเครื่องเป้าหมาย หรือต้องการแสวงประโยชน์อื่น ๆ หรือ รอเวลาปฏิบัติการ จึงจำเป็นที่จะต้องมีการรักษาสถานะการเชื่อมต่อระหว่างผู้โจมตีกับเครื่องเหยื่อ ผ่านการบัญชาการและควบคุมนั่นเอง

แนวทางการป้องกัน คือ

- ใช้ไฟร์วอลล์และเปิดใช้งานไว้เพื่อป้องกันการเชื่อมต่อที่ไม่ได้รับอนุญาตกับอุปกรณ์ของท่านผู้อ่าน
- ใช้ VPN เมื่อเข้าถึงอินเทอร์เน็ตจากเครือข่าย Wi-Fi สาธารณะ
- ระวังสัญญาณบ่งบอกว่าอุปกรณ์ของท่านผู้อ่านอาจถูกบุกรุก เช่น กิจกรรมเครือข่ายที่ผิดปกติหรือโปรแกรมที่ทำงานอยู่เบื้องหลัง

๗. การปฏิบัติการตามวัตถุประสงค์ (Actions on Objectives) : เป็นการปฏิบัติการโจมตีตามวัตถุประสงค์ที่ต้องการ เช่น เข้ารหัสเรียกค่าไถ่ (Ransome) ขโมยเงินในบัญชี ขโมยข้อมูลสำคัญ ขัดขวางการให้บริการ เป็นต้น

แนวทางการป้องกัน คือ

- ใช้รหัสผ่านที่รัดกุมและไม่ซ้ำใครสำหรับบัญชีออนไลน์ทั้งหมดของท่านผู้อ่านและเปลี่ยนเป็นประจำ
- เปิดใช้งานการตรวจสอบสิทธิ์แบบ ๒ ปัจจัยในบัญชีออนไลน์ของท่านผู้อ่าน
- ตรวจสอบใบแจ้งยอดธนาคารและบัตรเครดิตของคุณสำหรับกิจกรรมที่ผิดปกติ

ทั้งนี้ ผู้เขียนแปลและเรียบเรียงโดยอิงจากประสบการณ์และความเป็นจริงตามบริบททางภาษาไทยเป็นหลัก ทำให้แตกต่างจากตำราหรือบทความอื่น ๆ ไปบ้าง เพื่อให้น้ำหนักกับการทำความเข้าใจโดยง่ายเป็นสำคัญ

สรุป

โมเดลห่วงโซ่การโจมตีทางไซเบอร์ (Cyber Kill Chain) พัฒนาโดยบริษัท Lockheed Martin มี ๗ ขั้นตอน คือ การลาดตระเวน การจัดเตรียมอาวุธ การส่งอาวุธ การเจาะระบบ การติดตั้งอาวุธเพิ่มเติม การบัญชาการและควบคุม และการปฏิบัติการตามวัตถุประสงค์ การศึกษาทำความเข้าใจจะช่วยให้รับมือและป้องกันการโจมตีทางไซเบอร์ได้ดียิ่งขึ้น

อ้างอิง

- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html