บทที่ 4

มัลแวร์ (Malware) และภัยคุกคามทางซอฟต์แวร์

มัลแวร์คืออะไร? ศัตรูที่มองไม่เห็นในโลกดิจิทัล

1

ซอฟต์แวร์ประสงค์ร้าย

มัลแวร์ย่อมาจาก Malicious Software คือโปรแกรมที่ถูกสร้างมาเพื่อทำอันตราย เช่น ทำลายข้อมูล, ขโมยข้อมูลส่วนตัว, หรือเข้าควบคุมระบบคอมพิวเตอร์ของคุณโดยไม่ได้รับอนุญาต.

2

แรงจูงใจของแฮกเกอร์

แฮกเกอร์มักมีเป้าหมายหลากหลาย เช่น แสวงหาผลประโยชน์ทางการเงิน, การบ่อนทำลายองค์กรคู่แข่ง, การแก้แค้นส่วนตัว หรือต้องการสร้างชื่อเสียงในโลกไซเบอร์เพื่อแสดงความสามารถ.

7 ประเภทมัลแวร์ที่ต้องรู้จัก

1. **ไวรัส (Virus):** แฝงตัวในไฟล์และแพร่เชื้อเมื่อเปิดใช้งาน.
2. **เวิร์ม (Worm):** แพร่กระจายตัวเองผ่านเครือข่าย.
3. **โทรจัน (Trojan):** หลอกให้ติดตั้งเพื่อเปิดช่องโหว่.
4. **สปายแวร์ (Spyware):** แอบเก็บข้อมูลส่วนตัวของผู้ใช้.
5. **แอดแวร์ (Adware):** แสดงโฆษณาที่ไม่พึงประสงค์.
6. **แรนซัมแวร์ (Ransomware):** เข้ารหัสไฟล์เรียกค่าไถ่.
7. **ไฟล์แลส มัลแวร์ (Fileless):** ซ่อนในหน่วยความจำ ตรวจจับยาก.

มัลแวร์ Yokai: โจมตีเจ้าหน้าที่ไทย

มัลแวร์ Yokai เป็นตัวอย่างล่าสุดที่แสดงให้เห็นถึงความซับซ้อนของภัยคุกคามทางไซเบอร์ โดยมุ่งเป้าโจมตีเจ้าหน้าที่ของรัฐในประเทศไทย ผ่านเทคนิคการหลอกลวงที่แนบเนียน

- **เทคนิค DLL Side-Loading:** แพร่กระจายผ่านไฟล์แนบอีเมลปลอม โดยใช้ชื่อที่น่าเชื่อถือ เช่น "กระทรวงยุติธรรมสหรัฐ.pdf" เพื่อหลอกให้ผู้ใช้งานเปิดไฟล์.
- **การควบคุมระยะไกล:** เมื่อติดเชื้อ มัลแวร์นี้จะสามารถควบคุมเครื่องคอมพิวเตอร์จากระยะไกล และรับคำสั่งจากเซิร์ฟเวอร์ควบคุม (C2 server) เพื่อดำเนินการต่างๆ.
- **ความซับซ้อนยุคใหม่:** แสดงให้เห็นถึงวิวัฒนาการของมัลแวร์ที่มีความสามารถในการเลี่ยงการตรวจจับได้ดีขึ้น ทำให้เป็นภัยคุกคามที่ยากต่อการรับมือ.

วิธีการแพร่กระจายมัลแวร์ที่พบบ่อย

1

อีเมลฟิชชิ่ง

ส่งไฟล์แนบหรือลิงก์อันตราย หลอกให้เปิด

2

ดาวน์โหลดจากแหล่งไม่ปลอดภัย

ไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ หรือฟรีแวร์แฝงมัลแวร์

3

อุปกรณ์ภายนอก

เช่น USB แฟลชไดรฟ์ที่ติดไวรัส

4

เครือข่าย Wi-Fi สาธารณะ

โจมตีผ่านเครือข่ายที่ไม่มีการเข้ารหัสที่ปลอดภัย

5

Drive-by Download

เพียงแค่เข้าชมเว็บไซต์ที่ถูกแฮกก็อาจติดมัลแวร์ได้ทันที

ผลกระทบจากมัลแวร์: บุคคลและองค์กร

การขโมยข้อมูลสำคัญ

มัลแวร์สามารถเข้าถึงและขโมยข้อมูลส่วนตัว, ข้อมูลทางการเงิน, หรือความลับทางธุรกิจ ทำให้เกิดความเสียหายร้ายแรง.

ระบบล่มและธุรกิจหยุดชะงัก

การติดมัลแวร์อาจทำให้ระบบคอมพิวเตอร์หรือเครือข่ายไม่สามารถทำงานได้ ส่งผลให้ธุรกิจหยุดชะงักและสูญเสียความน่าเชื่อถือ.

ค่าใช้จ่ายในการกู้คืนสูง

การกู้คืนข้อมูลและระบบที่ถูกโจมตีด้วยมัลแวร์ต้องใช้เวลาและค่าใช้จ่ายจำนวนมาก ซึ่งอาจเป็นภาระทางการเงินที่หนักหน่วง.

ตัวอย่างเหตุการณ์จริง: **Conti Ransomware** เคยโจมตีองค์กรขนาดใหญ่ทั่วโลก ทำให้เกิดความเสียหายมูลค่าหลายพันล้านดอลลาร์ และส่งผลกระทบต่อบริการสาธารณะที่สำคัญ.

แนวทางป้องกันมัลแวร์ขั้นพื้นฐาน

01

อัปเดตระบบและซอฟต์แวร์

หมั่นอัปเดตระบบปฏิบัติการและโปรแกรมต่างๆ ให้เป็นเวอร์ชันล่าสุดเสมอ เพื่อปิดช่องโหว่ด้านความปลอดภัย.

02

ติดตั้งโปรแกรม Anti-malware

ใช้โปรแกรมป้องกันมัลแวร์ที่มีประสิทธิภาพ และอัปเดตฐานข้อมูลไวรัสอย่างสม่ำเสมอ.

03

ระมัดระวังอีเมลและลิงก์

อย่าเปิดไฟล์แนบหรือคลิกลิงก์จากอีเมลที่ไม่รู้จัก หรือแหล่งที่มาที่ไม่น่าเชื่อถือ.

04

สแกนอุปกรณ์ USB

ก่อนใช้งาน USB หรืออุปกรณ์จัดเก็บข้อมูลภายนอกอื่นๆ ควรสแกนหาไวรัสทุกครั้ง.

05

หลีกเลี่ยงแหล่งดาวน์โหลดที่ไม่น่าเชื่อถือ

ดาวน์โหลดโปรแกรมและไฟล์จากเว็บไซต์ที่เป็นทางการและเชื่อถือได้เท่านั้น.

เทคนิคเสริมเพื่อความปลอดภัยขั้นสูง

เปิดใช้งานไฟร์วอลล์

ไฟร์วอลล์ช่วยกรองข้อมูลที่เข้าออกเครือข่าย ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต.

ใช้รหัสผ่านที่รัดกุม

สร้างรหัสผ่านที่ซับซ้อน มีทั้งตัวอักษรพิมพ์เล็ก-ใหญ่ ตัวเลข และสัญลักษณ์ และเปลี่ยนเป็นประจำ.

จำกัดสิทธิ์ผู้ใช้งาน

ให้สิทธิ์ผู้ใช้งานในระบบเท่าที่จำเป็น หลีกเลี่ยงการให้สิทธิ์แอดมินโดยไม่จำเป็น.

สำรองข้อมูลสม่ำเสมอ

สำรองข้อมูลสำคัญไว้ในหลายๆ ช่องทาง เช่น Cloud หรือ External Drive เพื่อให้สามารถกู้คืนได้หากถูกโจมตี.

สรุป: มัลแวร์คือภัยคุกคามที่ต้องเฝ้าระวัง

ความหลากหลายของมัลแวร์

มัลแวร์มีหลายรูปแบบและวิวัฒนาการอย่างต่อเนื่อง ทำให้การโจมตีซับซ้อนและตรวจจับได้ยากขึ้น.

ความรู้คือเกราะป้องกัน

การป้องกันที่ดีที่สุดเริ่มต้นจากความรู้ ความเข้าใจ และความระมัดระวังของผู้ใช้งานทุกคน.

มาตรการป้องกันที่เหมาะสม

ทั้งองค์กรและบุคคลควรเลือกใช้เทคโนโลยีและแนวทางป้องกันที่เหมาะสม เพื่อสร้างเกราะป้องกันภัยไซเบอร์ที่แข็งแกร่ง.

ร่วมสร้างโลกไซเบอร์ที่ปลอดภัยไปด้วยกัน

อัปเดตและป้องกัน

เริ่มต้นด้วยการอัปเดตระบบและติดตั้งโปรแกรมป้องกันมัลแวร์ให้ทันสมัยอยู่เสมอ.

ระวังก่อนคลิก

ตรวจสอบและระวังก่อนเปิดไฟล์ หรือคลิกลิงก์ทุกครั้ง โดยเฉพาะจากแหล่งที่ไม่รู้จัก.

แบ่งปันความรู้

แชร์ข้อมูลและเตือนภัยให้คนรอบข้างรับรู้ถึงภัยคุกคาม เพื่อป้องกันร่วมกัน.

ความรับผิดชอบร่วมกัน

ความปลอดภัยไซเบอร์ไม่ใช่เรื่องของใครคนใดคนหนึ่ง แต่เป็นความรับผิดชอบของเราทุกคน.