บทที่ 6 การกระทำความผิดทางคอมพิวเตอร์

การกระทำความผิดทางคอมพิวเตอร์ คือ การกระทำการที่ถือว่าเป็นความผิดตามกฎหมายและเป็นการกระทำผ่านหรือโดยอาศัยคอมพิวเตอร์ในการกระทำความผิด ซึ่งมีวัตถุประสงค์มุ่งต่อระบบคอมพิวเตอร์ ข้อมูลของคอมพิวเตอร์ หรือบุคคล

6.1 ประเภทการกระทำความผิดทางคอมพิวเตอร์

เมื่อพูดถึงภัยบนโลกอินเทอร์เน็ตที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ “ไวรัสคอมพิวเตอร์” มีบทบาทตั้งแต่ยุคแรกเริ่มของคอมพิวเตอร์จนถึงปัจจุบัน เป็นที่คุ้นเคยของคนทุกเพศทุกวัยไม่ว่าจะเป็นผู้ที่เชี่ยวชาญ หรือบุคคลทั่วไป ไวรัสคอมพิวเตอร์เป็นเพียงส่วนหนึ่งของภัยคุกคามทางคอมพิวเตอร์จัดอยู่ในกลุ่ม มัลแวร์ (Malware หรือ Malicious Code Software) ซึ่งสามารถจำแนกได้ 2 ประเภท คือ การกระทำต่อระบบคอมพิวเตอร์ และ การใช้คอมพิวเตอร์ในการกระทำความผิด ดังนี้ [1]

6.1.1 การกระทำต่อระบบคอมพิวเตอร์

1) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 1

สปายแวร์ (Spyware), สนิฟเฟอร์ (Sniffer) มีผลกระทบต่อความมั่นคงปลอดภัย และความเสียหายคือ การสอดแนมข้อมูลส่วนตัว การแอบดักฟัง packet

2) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 2

การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses มีผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์, การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service) [1]

3) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 3

การทำสแปม (Spamming) ปกปิด/ปลอมแปลงแหล่งที่มา ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ รบกวนการใช้ระบบคอมพิวเตอร์ตามปกติ อาจถึงขั้นทำให้เป็น Zombie [1]

4) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 4

BOT หรือ Botnet ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ ผลกระทบต่อความมั่นคงปลอดภัยของประเทศ หรือทางเศรษฐกิจ, ความปลอดภัยสาธารณะ, การบริการสาธารณะ อาจเกิดสงครามข้อมูลข่าวสาร (Information Warfare) [1]

5) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 5

Hacking Tools, Spam Tools ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหายคือ สอดแนมข้อมูลส่วนตัว, การแอบดักฟัง packet, การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service) [1]

6.1.2 การใช้คอมพิวเตอร์ในการกระทำความผิด

6) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 6

การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses, Phishing, ยุยง, หลอกลวง, ภาพลามก ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์, การทำให้ระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม หรือหยุดทำงาน (Denial of Service) หรือทำให้เกิดความวุ่นวายต่อเศรษฐกิจ ความมั่นคงของประเทศ

7) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 7

การสนับสนุน ส่งเสริม การใช้ชุดคำสั่งในทางมิชอบ (Malicious Code) เช่น Viruses, Worms, Trojan Horses, Phishing, ยุยง, หลอกลวง, ภาพลามก ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ เกิดความเสียหายต่อผู้อื่น

8) กลุ่มตัวอย่างรูปแบบการกระทำความผิด กลุ่มที่ 8

การตัดต่อภาพ ผลกระทบต่อความมั่นคงปลอดภัย และความเสียหาย คือ ผู้ถูกกระทำถูกดูหมิ่น ถูกเกลียดชัง หรืออับอาย

6.2 ชนิดภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ต

เมื่อพูดถึงภัยบนโลกอินเทอร์เน็ตที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ “ไวรัสคอมพิวเตอร์” มีบทบาทตั้งแต่ยุคแรกเริ่มของคอมพิวเตอร์จนถึงปัจจุบัน เป็นที่คุ้นเคยของคนทุกเพศทุกวัยไม่ว่าจะเป็นผู้ที่เชี่ยวชาญ หรือบุคคลทั่วไป ไวรัสคอมพิวเตอร์เป็นเพียงส่วนหนึ่งของภัยคุกคามทางคอมพิวเตอร์จัดอยู่ในกลุ่ม มัลแวร์ (Malware หรือ Malicious Code Software) ซึ่งสามารถจำแนกออกไปได้อีกหลากหลายรูปแบบ [2]

1) ชนิดภัยคุกคามรูปแบบมัลแวร์ (Malware)

การที่จะบอกได้ว่าข้อมูลนั้นมีความปลอดภัยหรือไม่จะต้องทำการวิเคราะห์คุณสมบัติทั้ง 3 ด้าน คือ ความลับ ความถูกต้อง และความพร้อมใช้งานว่ามีอยู่ครบหรือไม่ ถ้าขาดคุณสมบัติด้านใดด้านหนึ่งไปแสดงว่าข้อมูลนั้นไม่มีความปลอดภัย ดังนั้น การรักษาความปลอดภัยข้อมูลจึงเป็นการปกป้องรักษาคุณสมบัติทั้ง 3 ด้าน ดังต่อไปนี้

- ความลับ (Confidentiality) หมายถึง การทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ความถูกต้อง (Integrity) หมายถึง การรักษาความคงสภาพของข้อมูลจากแหล่งที่มา หรือไม่ได้ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) หมายถึง การทำให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้เมื่อต้องการ

มัลแวร์ คือ ความไม่ปกติทางโปรแกรม ที่สูญเสีย CIA อย่างใดอย่างหนึ่ง หรือทั้งหมดจนเกิดเป็นไวรัส เวิร์ม โทรจัน สปายแวร์ แบ็คดอร์ และ รู๊ทคิต

- การสูญเสีย C (Confidentiality) คือ สูญเสียความลับทางข้อมูล
- การสูญเสีย I (Integrity) คือ สูญเสียความไม่เปลี่ยนแปลงของข้อมูล นั่นคือ ข้อมูลถูกเปลี่ยนแปลงแก้ไข โดยเฉพาะส่วนสำคัญที่เกี่ยวโยงกับระบบภายในระบบปฏิบัติการ
- การสูญเสีย A (Availability) คือ สูญเสียเสถียรภาพของระบบปฏิบัติการ

2) ไวรัสคอมพิวเตอร์ (Computer Virus)

คือ รหัสหรือโปรแกรมที่สามารถทำสำเนาตัวเองและแพร่กระจายสู่เครื่องอื่นได้ โดยเจ้าของเครื่องนั้นๆ ไม่รู้ตัว (หากไม่ติดตั้งโปรแกรมป้องกันไวรัส หรือโปรแกรมดังกล่าวไม่รู้จักไวรัสชนิดนั้นๆ) ถือเป็นสิ่งไม่พึงประสงค์ซึ่งฝังตัวเองในโปรแกรมหรือไฟล์ [1] แล้วแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นๆ ผ่านสื่อรูปแบบต่างๆ เช่น CD, DVD, Multimedia Card, USB Drive หรือผ่านทางเครือข่าย เช่น อินเทอร์เน็ตระบบ LAN หรืออีเมล เป็นต้น ไวรัสอาจอาศัยอยู่ในเครื่องคอมพิวเตอร์ แต่ไม่แสดงความผิดปกติให้พบ หากผู้ใช้ไม่เรียกใช้โปรแกรมดังกล่าว สิ่งสำคัญคือไวรัสไม่อาจแพร่กระจายได้หากขาดคนกระทำ เช่น แบ่งปันไฟล์ที่ติดไวรัส หรือส่งอีเมลโดยแนบไฟล์ที่ติดไวรัส เป็นต้น ไวรัสคอมพิวเตอร์มีความรุนแรงหลายระดับ ตั้งแต่สร้างความรำคาญให้ผู้ใช้งาน จนถึงทำลายฮาร์ดแวร์ ซอฟต์แวร์ หรือไฟล์ข้อมูล ทำให้ผู้ใช้งานคอมพิวเตอร์จำเป็นต้องติดตั้งโปรแกรมป้องกันไวรัส จนกลายเป็นโปรแกรมสำคัญสำหรับคอมพิวเตอร์ทุกเครื่อง

3) หนอนคอมพิวเตอร์ (Computer Worm)

เรียกสั้นๆ ว่า “เวิร์ม” เป็นหน่วยย่อยลงมาจากไวรัส สามารถทำสำเนาตัวเองและแพร่กระจายผ่านเครือข่ายหรืออินเทอร์เน็ตสู่คอมพิวเตอร์หรือเครือข่ายอื่นได้ เวิร์มต่างจากไวรัสตรงที่ไม่ต้องอาศัยผู้ใช้งาน แต่จะอาศัยไฟล์หรือคุณสมบัติในการส่งต่อข้อมูลในคอมพิวเตอร์เพื่อกระจายตัวเอง [1] โดยสแกนเครือข่ายเพื่อหาระบบที่มีช่องโหว่ โจมตีช่องโหว่และบุกรุกเข้าระบบเหล่านั้นโดยอัตโนมัติ เวิร์มบางชนิดสามารถติดตั้ง Backdoor ในเครื่องคอมพิวเตอร์ที่ติดเวิร์ม และสร้างสำเนาตัวเองได้ โดยผู้สร้างเวิร์มชนิดนั้นสามารถสั่งการได้จากระยะไกล เรียกว่า Botnet มีเป้าหมายเพื่อโจมตีสร้างความเสียหายให้กับคอมพิวเตอร์และเครือข่าย หรือเพียงแค่ต้องการโฆษณาสินค้าหรือบริการ เวิร์มถึงจะเป็นหน่วยย่อยของไวรัส แต่ก็มีความรุนแรงกว่าไวรัสมาก สิ่งที่อันตรายอย่างยิ่งของเวิร์ม คือ สามารถจำลองตัวเองในคอมพิวเตอร์เครื่องหนึ่ง แล้วแพร่กระจายสำเนาของตัวเองออกไปได้จำนวนมาก ตัวอย่างเช่น สามารถดักจับ username และ password และใช้ข้อมูลนี้เพื่อบุกรุกบัญชีผู้ใช้นั้นทำสำเนาตัวเองแล้วส่งต่อไปยังทุกรายชื่อที่มีอยู่ในลิสต์อีเมล จากนั้นทำสำเนาต่อ แล้วส่งไปยังบัญชีรายชื่อของผู้รับอีเมลนั้นทุกคน ท้ายที่สุดส่งผลให้การรับส่งข้อมูลผ่านเครือข่าย (Network Bandwidth) ทำได้ช้าลง เป็นเหตุให้ Web Server, Network Server และเครื่องคอมพิวเตอร์หยุดทำงาน

4) BOTNET หรือ “Robot Network”

คือ เครือข่ายหุ่นรบที่ถือเป็นสะพานเชื่อมภัยคุกคามทางเครือข่ายคอมพิวเตอร์ด้วยมัลแวร์ทั้งหลายที่กล่าวในตอนต้น มัลแวร์ต้องการตัวนำทางเพื่อต่อยอดความเสียหายและทำให้ยากแก่การควบคุม ตัวนำทางที่ว่านี้ก็คือ Botnet ซึ่งก่อให้เกิดภัยคุกคามที่ไม่สามารถเกิดขึ้นได้เองโดยลำพัง เช่น Spam DoS/DDoS และ Phishing เป็นต้น ภัยคุกคามดังกล่าวจะมีคนควบคุมอยู่เบื้องหลัง เมื่อเครื่องของผู้

รู้เท่าไม่ถึงการณ์ติดมัลแวร์จะกลายเป็นผู้แพร่กระจาย Botnet ซึ่งจะถูกควบคุมจากระยะไกล ผู้ควบคุมอาจเป็น แฮคเกอร์ หรือกระทำการอิสระโดยอัตโนมัติตามที่ตั้งโปรแกรมไว้ แหล่งควบคุม Botnet ส่วนใหญ่อยู่ใน IRC (Internet Relay Chat) ห้องสนทนายุคแรกเริ่ม ด้วยเหตุผลหลัก 2 ประการ คือ

1.Protocol ในการติดต่อ IRC เป็นแบบ UDP (User Datagram Protocol) ซึ่งมีความเร็ว และ ไม่ต้องการความถูกต้องในการสื่อสารมากนัก ทำให้เครื่องที่ติด Botnet ไม่รู้ตัวว่าได้เชื่อมต่อ Server IRC ที่อยู่ห่างไกลออกไป
2.IRC เป็นแหล่งที่แฮคเกอร์ส่วนใหญ่ในอดีตใช้แลกเปลี่ยนเทคนิค รวมทั้งเรื่องราวต่างๆ เป็นแหล่งที่ยากต่อการควบคุมและค้นหาตัวตนที่แท้จริง

5) สปายแวร์ (Spyware)

คือ มัลแวร์ชนิดหนึ่งที่ติดตั้งบนเครื่องคอมพิวเตอร์ ทำให้ล่วงรู้ข้อมูลของผู้ใช้งานได้โดยเจ้าของเครื่องไม่รู้ตัว สปายแวร์จะทำการเฝ้าดูการใช้งานและรวบรวมข้อมูลส่วนตัวของผู้ใช้งาน อีกทั้งยังสามารถเปลี่ยนค่าที่ตั้งไว้ของคอมพิวเตอร์ ส่งผลให้ความเร็วในการเชื่อมต่ออินเทอร์เน็ตช้าลง หรือหน้าโฮมเพจเปลี่ยนแปลง เป็นต้น สปายแวร์ที่มีชื่อคุ้นเคยกันดีคือโปรแกรม Keylogger เมื่อผู้ใช้ดาวน์โหลดไฟล์จากอินเทอร์เน็ตที่แฝงโปรแกรม Keylogger ทำให้โปรแกรมเข้ามาฝังตัวในคอมพิวเตอร์ส่วนตัว เมื่อผู้ใช้ได้ใช้เครื่องคอมพิวเตอร์ทำธุรกรรมการเงินในเว็บไซต์ E-Banking ข้อมูล username และ password ของบัญชีผู้ใช้จะถูกส่งตรงถึงมิจฉาชีพ และทำการสวมรอยเป็นเจ้าของบัญชี เพื่อลักลอบโอนเงินออกมาจากบัญชีโดยที่เจ้าของนั้นไม่รู้ตัว

6) ม้าโทรจัน (Trojan Horse)

คือ โปรแกรมชนิดหนึ่งที่ดูเหมือนจะมีประโยชน์ แต่แท้จริงแล้วก่อให้เกิดความเสียหายเมื่อติดตั้งโปรแกรมลงบนคอมพิวเตอร์ ผู้ที่ได้รับไฟล์โทรจันมักถูกหลอกให้เปิดไฟล์ดังกล่าว โดยคิดว่าเป็นซอฟต์แวร์ หรือไฟล์จากแหล่งที่ถูกต้องตามกฎหมาย เมื่อไฟล์ถูกเปิดอาจเกิดผลลัพธ์หลากหลายรูปแบบ ตั้งแต่สร้างความรำคาญ เช่น เปลี่ยนหน้า Desktop หรือสร้างไอคอนที่ไม่จำเป็นบนหน้า Desktop จนถึงขั้นสร้างความเสียหายรุนแรง ด้วยการลบไฟล์และทำลายข้อมูลในคอมพิวเตอร์ โทรจันบางชนิดอาจฝัง Backdoor ไว้ในเครื่องคอมพิวเตอร์ เป็นเหตุให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องคอมพิวเตอร์นั้นแล้วทำการล้วงข้อมูลส่วนตัว และข้อมูลที่เป็นความลับ สร้างความเสียหายได้ สิ่งหนึ่งที่โทรจันแตกต่างจากไวรัสและเวิร์มคือ โทรจันไม่สามารถสร้างสำเนาโดยแพร่กระจายสู่ไฟล์อื่น และไม่สามารถจำลองตัวเองได้

7) ประตูหลัง (Backdoor)

คือ ช่องทางลับที่เกิดจากช่องโหว่ของระบบ ทำให้ผู้ไม่ประสงค์ดีเข้าถึงระบบหรือเครื่องคอมพิวเตอร์ เพื่อใช้ทรัพยากรในเครื่องนั้นกระทำการใดๆ ได้ โดยทั่วไป Backdoor อาจเกิดจากความตั้งใจของผู้ดูแลระบบ เพื่อสร้างช่องทางลัดเข้าสู่ระบบเองก็เป็นได้ แต่เมื่อไปผสมผสานกับภัยคุกคามอื่น เช่น โทรจัน ทำให้ระบบเกิดช่องโหว่ ผู้ไม่ประสงค์ดีสามารถเข้าถึงและสร้างความเสียหายได้

8) ชนิดภัยคุกคามรูปแบบการโจมตีแบบขัดขวางหรือก่อกวนระบบ (DoS/DDoS)

คือ การพยายามโจมตีเพื่อทำให้เครื่องคอมพิวเตอร์ปลายทางหยุดทำงาน หรือสูญเสียเสถียรภาพ หากเครื่องต้นทาง (ผู้โจมตี) มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากผู้โจมตีมีมากและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS) ด้วยเทคโนโลยีที่ก้าวล้ำในปัจจุบัน ซึ่งมีภัยคุกคามมากมาย และแพร่กระจายอย่างรวดเร็ว ทำให้การโจมตีส่วนใหญ่ในโลกออนไลน์ มักเป็นการโจมตีแบบ DDoS

9) ชนิดภัยคุกคามรูปแบบข้อมูลขยะ (Spam)

ส่วนใหญ่เกิดจากอีเมลหรือเรียกว่า อีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับโดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti spam หรือหากใช้ฟรีอีเมล เช่น hotmail yahoo ก็จะมีโปรแกรมคัดกรองอีเมลขยะในระดับหนึ่ง

10) ชนิดภัยคุกคามรูปแบบการหลอกลวงข้อมูล (Phishing)

เป็นคำพ้องเสียงกับ “fishing” หรือการตกปลาเพื่อให้เหยื่อมาติดเบ็ด คือ กลลวงชนิดหนึ่งในโลกไซเบอร์ด้วยการส่งข้อความผ่านอีเมลล์หรือเมสเซนเจอร์ หลอกให้เหยื่อเชื่อว่าเป็นสถาบันการเงินหรือองค์กรน่าเชื่อถือ เชิญชวนด้วยกลวิธีต่างๆ เช่น คุณได้รับรางวัล แล้วทำลิงค์หลอกให้เหยื่อคลิก เพื่อหวังจะได้ข้อมูลสำคัญ เช่น username / password เลขที่บัญชีธนาคาร เลขที่บัตรเครดิต เป็นต้น แต่ลิงค์ดังกล่าวจะนำไปสู่หน้าเว็บไซต์เลียนแบบ หากเหยื่อกรอกข้อมูลส่วนตัวลงไปมิจฉาชีพสามารถนำไปหาประโยชน์ในทางมิชอบได้ [1]

11) ชนิดภัยคุกคามรูปแบบการดักข้อมูล (Sniffing)

การดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งบนเครือข่ายในองค์กร (Local Area Network: LAN) เป็นวิธีการหนึ่งที่นักโจมตีระบบนิยมใช้ดักข้อมูล เพื่อแกะรหัสผ่านบนเครือข่ายไร้สาย (Wireless LAN) และดักข้อมูล Username / Password ของผู้อื่นที่ไม่ได้ผ่านการเข้ารหัส

6.3 แนวโน้มการกระทำความผิดทางคอมพิวเตอร์

แนวโน้มการกระทำความผิดทางคอมพิวเตอร์ในปี 2556 จะเกิดขึ้นกับอุปกรณ์พกพาเป็นส่วนมาก เนื่องจากมีผู้ใช้จำนวนมากที่หันไปใช้อุปกรณ์พกพาและคลาวด์ อาชญากรก็ปรับตัวตามไปโจมตีผู้ใช้งานเหล่านั้นเช่นกัน เราคาดการณ์ว่าแพลตฟอร์มอุปกรณ์พกพาต่างๆ และคลาวด์เซอร์วิซ จะเป็นเป้าหมายหลักที่มีแนวโน้มในการถูกโจมตีและการถูกละเมิดในปี 2556 นี่คือสิ่งที่จะเกิดมากขึ้นเป็นสองเท่าของมัลแวร์บนโทรศัพท์มือถือจากปี 2553-2554 เช่นเดียวกับการเพิ่มขึ้นอย่างรวดเร็วของมัลแวร์ของ Android ในปี 2555

นอกจากนี้ อุปกรณ์พกพาที่ไม่มีการจัดการเป็นอย่างดีและมีการเชื่อมต่อการใช้งานเข้า-ออกจากระบบเครือข่ายองค์กรและรับข้อมูลอย่างต่อเนื่อง มีแนวโน้มว่าภายหลังข้อมูลเหล่านั้นจะถูกเก็บไว้ในคลาวด์อื่นๆ โดยมีความเสี่ยงเพิ่มขึ้นจากการรั่วไหลและการโจมตีเป้าหมายของอุปกรณ์พกพา ขณะที่ผู้ใช้เพิ่มการใช้แอพพลิเคชั่นลงในโทรศัพท์มือถือก็รับเอามัลแวร์เข้ามาด้วย

จากการชำระเงินผ่านโทรศัพท์มือถือที่เพิ่มขึ้น เราอาจจะเห็นคนร้ายที่ใช้มัลแวร์ในการโจรกรรมข้อมูล

การชำระเงินจากผู้คนที่อยู่ในโลกการซื้อขายสินค้าออนไลน์ บางระบบการชำระเงินที่ใช้อย่างแพร่หลายกับผู้ไม่เคยมีประสบการณ์ด้านเทคนิค อาจมีช่องโหว่ที่ปล่อยให้ข้อมูลถูกโจรกรรมไปได้

ในขณะเดียวกัน เราคาดการณ์การเติบโตของแอดแวร์ในมือถือหรือ "ภัยร้ายทางโทรศัพท์มือถือ"ที่จะสร้างความรำคาญและรบกวนผู้ใช้และอาจจะเปิดเผยรายละเอียดสถานที่, ที่อยู่ติดต่อ และระบุอุปกรณ์ที่ใช้ให้อาชญากรไซเบอร์เห็น แมดแวร์ จะย่องเข้าไปในอุปกรณ์ของผู้ใช้เมื่อพวกเขาดาวน์โหลดแอพพลิเคชั่น - มักจะเป็นการส่งป๊อปอัพขึ้นแจ้งเตือนไปที่แถบการแจ้งเตือนบนไอคอน การเปลี่ยนแปลงการตั้งค่าเบราว์เซอร์ และรวบรวมข้อมูลส่วนบุคคล

วิธีการสร้างกระแสเงินสดในเครือข่ายสังคมนำมาซึ่งภัยคุกคามรูปแบบใหม่ การเพิ่มขึ้นของรูปแบบการสร้างกระแสเงินสดผ่านทางแพลตฟอร์มของโซเชี่ยลมีเดียจะทำอาชญกรรมในโลกไซเบอร์ใช้เป็นช่องทางในการโจมตีเหยื่อได้

ในฐานะผู้บริโภค เราใช้โซเชียลมีเดียกันอย่างไว้วางใจมากขึ้น เริ่มตั้งแต่การแชร์ข้อมูลส่วนบุคคล ใช้ซื้อเกมส์ ซื้อของขวัญให้เพื่อน เครือข่ายเหล่านี้เป็นจุดเริ่มต้นในการใช้แพลตฟอร์มเป็นสื่อกลางในการซื้อขายโดยอนุญาตให้สมาชิกซื้อของขวัญและส่งให้เพื่อนฝูง ซึ่งแพลตฟอร์มเหล่านั้นก็เป็นช่องทางใหม่ที่อาชกรในโลกไซเบอร์ใช้โจมตีเหยื่อได้ ซึ่งไซแมนเทคได้คาดการณ์ไว้ว่า การขโมยข้อมูลที่เหยื่อใช้ในการซื้อของในโลกโซเชียลเน็ตเวิร์ก หรือล่อลวงให้บอกข้อมูลการชำระเงิน ข้อมูลส่วนตัว โดยปลอมแปลงเครือข่ายสังคมออนไลน์หรือโซเชียลเน็ตเวิร์กจะเพิ่มมากขึ้น ซึ่งยังรวมถึงการสร้างของขวัญปลอม หรือส่งข้อความทางอีเมลเพื่อขอที่อยู่บ้านและข้อมูลส่วนตัวอื่นๆ อีกด้วย

<u>ตัวอย่างเช่น</u>

1) บัตรของขวัญจากสตาร์บัค ที่อาชญากรที่เรียกว่า scammers เสแสร้งว่าเป็นเจ้าของบัตรกำนัลของสตาร์บัคและหลอกให้เหยื่อให้ข้อมูลส่วนตัว อาทิ อีเมล ที่อยู่ และที่อยู่ในการจัดส่งบัตรกำนัลไปให้พร้อมกับมูลค่าในบัตรที่นำไปแลกสินค้าได้ อาชญากรประเภทนี้ยังใช้วิธีการใหม่ๆ ที่จะบ่ายเบี่ยงการตรวจจับ เช่น หลอกให้เหยื่อคิดว่ากำลังสนทนากับเจ้าหน้าที่หรือพนักงานของสตาร์บัคซึ่งเป็นแบรนด์ที่เหยื่อรายนั้นชื่นชอบ

2) โปรแกรมเรียกค่าไถ่ (Ransomeware) คือ สแกร์แวร์ รูปแบบใหม่

3) โปรแกรมเรียกค่าไถ่ หรือ แรนซัมแวร์ (Ransomware) เป็นอีกหนึ่งรูปแบบของภัยที่ต้องจับตามอง เพราะมีแนวโน้มเพิ่มขึ้นเรื่อยๆ โดยเป็นการอาศัยขั้นตอนวิธีการชำระเงินเพื่อขโมยข้อมูลจากเหยื่อเป้าหมาย

แรมซัมแวร์ (Ransomware) เป็นรูปแบบหนึ่งของโปรแกรมประสงค์ร้าย (malicious software) ซึ่งจะทำลายการทำงานของระบบคอมพิวเตอร์ทำให้ไม่สามารถเข้าอินเตอร์เน็ตได้และเรียกค่าไถ่เป็นข้อมูลส่วนตัวเพื่อให้สามารถกู้คืนระบบให้กลับสู่สภาวะปกติ แรนซัมแวร์ที่พบเมื่อเร็วๆ นี้ จะใช้วิธีขึ้นภาพบนหน้าจอและข้อความเตือนในลักษณะที่มาจากตำรวจว่าต้องจ่ายค่าปรับเพราะเข้าเว็บผิดกฎหมาย มัลแวร์ประเภทนี้จะใช้บริการการระบุสถานที่ตั้งของเครื่องคอมพิวเตอร์ที่กำลังเปิดใช้งานอยู่ หลังจากทำการล็อคหน้าจอให้เข้าใช้งานอินเทอร์เน็ตไม่ได้ ก็จะส่งข้อความขู่ในภาษากฎหมายที่ใช้อยู่ทั่วไปในประเทศนั้นๆ

แรมซัมแวร์ เป็นการหลอกลวงที่เหนือชั้นกว่าการพยายามหลอกเหยื่อ เพราะมันจะพยายามบังคับให้เหยื่อต้องยอมจำนน อาชญากรประเภทนี้ เลียนแบบวิธีการจับตัวประกันไปเรียกค่าไถ่ แต่ทำในโลกไซเบอร์คือ อาศัยหน้าจอเว็บไซต์ที่ผู้ใช้กำลังทำการชำระเงินทางออนไลน์[3]

6.4 กรณีศึกษาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์

6.4.1 กรณีศึกษาที่ 1

เมื่อวันที่ 16 ม.ค. 2556 ผู้สื่อข่าวได้รับการร้องเรียนจากประชาชนว่าขณะนี้มีภาพเด็กนักเรียนแต่งกายไม่เหมาะสมถูกนำมาเผยแพร่ผ่านทางอินเตอร์เน็ตในโลกโซเชียลเน็ตเวิร์ค และเว็บไซต์เฟซบุ๊ค โดยมีการส่งเผยแพร่ต่อกันมาเป็นจำนวนมาก รายละเอียดของภาพเป็นภาพเด็กสวมใส่ชุดนักเรียนหญิง 7 คน ส่วนใหญ่มีการถอดเสื้อผ้าออกเหลือเพียงยกทรงนั่งบ้างยืนบ้างโชว์หน้าอก ส่วนอีกคนสวมใส่เสื้อชุดนักเรียนคอซองแต่นั่งถ่างขาโชว์กางเกงในสีแดง และยังมีบางคนใส่เสื้อสายเดี่ยวและมีการแสดงท่าทางกอดรัดกัน โดยทั้งหมดได้ถ่ายภาพด้วยสีหน้ายิ้มแย้มแจ่มใสไม่ละอายในสิ่งที่ทำ

ผู้สื่อข่าวได้ตรวจสอบภาพดังกล่าว พบว่า มีต้นตอการส่งภาพมาจากบุคคลที่ใช้ชื่อว่า Beer nirvana มีผู้มาแสดงความคิดเห็นแสดงความชื่นชอบภาพดังกล่าวอย่างรวดเร็ว ในระยะเวลา 10 นาที มีผู้กดชื่นชอบเพิ่มขึ้นนับพันๆราย รวมทั้งมีการนำภาพดังกล่าวไปเผยแพร่แบ่งปันต่อๆกันเป็นจำนวนมาก.....[4]

<u>การกระทำความผิดตาม พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550</u>

จากข่าวข้างต้นเป็นการโพสต์รูปที่ไม่เหมาะสมลง Internet ในระบบ Social network ที่เข้าถึงได้ง่าย ซึ่งการโพสต์รูปเป็นรูปที่มีลักษณะโป๊เปลือย เป็นรูปเด็กนักเรียนหญิงม.ต้น 7 คน โพสต์ท่ายั่วยวน นุ่งน้อยห่มน้อย ถือว่าเป็นการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ใน มาตราต่อไปนี้

1) มาตรา 14 (4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

2) มาตรา 14 (5) ผู้ใดเผยแพร่และส่งต่อซึ่งข้อมูลลามก ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ

อีกทั้งยังผิดประมวลกฎหมายอาญาฐานหมิ่นประมาท มาตรา 326 และ 328 โดยต้องโทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 2 แสนบาท

6.4.2 กรณีศึกษาที่ 2

กองปราบบุก จู่โจมค้น-จับ "เว็บประชาไท" หมิ่นสถาบัน

(6 มี.ค.) เมื่อเวลา 14.00 น.พล.ต.ต.วรศักดิ์ นพสิทธิพร รอง ผบช.ก.พ.ต.อ.สาธิต ต ชยภพ รอง ผบก.ป.พร้อมกำลังเจ้าหน้าที่ตำรวจกองปราบปรามนำหมายค้น ศาลอาญา เลขที่ 183/2552 ลงวันที่ 5 มี.ค. 2551 เข้าตรวจค้นภายในสำนักงานเว็บไซต์ประชาไท เลขที่ 409 ชั้น 1 อาคาร มอส.ซอยประชาราษฎร์ บำเพ็ญ 5 แขวงและเขตห้วยขวาง หลังจากทางเจ้าหน้าที่ตำรวจได้รับการร้องเรียนจากทางกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) ว่า เว็บไซต์หนังสือพิมพ์ประชาไทออนไลน์ (www.prachatai.com) มีการโพสต์ข้อความลักษณะหมิ่นเบื้องสูง ในช่วงตั้งแต่วันที่ 15 ต.ค.-3 พ.ย.2551 ต่อเนื่องกัน เหตุเกิดในพื้นที่เขตพระราชวัง เขตปทุมวัน และ เขตห้วยขวาง

ทั้งนี้ จากหลักฐานที่ทางกระทรวงไอซีที มอบให้กับทางเจ้าหน้าที่พบข้อความภายในเว็บไซต์ดังกล่าวที่เข้าข่ายหมิ่นเบื้องสูงมากกว่า 40 ข้อความ จึงได้รวบรวมพยานหลักฐานเพื่อขอหมายค้น และหมายจับ นางสาวจีรนุช เปรมชัยพร อายุ 42 ปี ผู้อำนวยการเว็บไซต์ประชาไท อยู่บ้านเลขที่ 48/282 ซอยรามคำแหง 104 แขวงและเขตสะพานสูง ซึ่งทางศาลอาญาได้อนุมัติหมายจับผู้ต้องหา เลขที่551/2552 ลงวันที่ 3 มี.ค. 2551 ในข้อหากระทำผิด พ.ร.บ.คอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1)(3)(5) เป็นผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำผิด นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมด หรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่จะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน, นำเข้าสู่ระบบคอมพิวเตอร์ ข้อมูลอันเป็นเท็จโดยประการที่จะเกิดความเสียหายต่อความมั่นคงประเทศ และเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพ์ตาม (1)(3)(5) และผิด พ.ร.บ.คอมพ์ มาตรา 15

จากการตรวจค้นภายในสำนักงานเว็บไซต์ดังกล่าว เจ้าหน้าที่ได้ทำการยึดคอมพิวเตอร์โน้ตบุ๊กของนางสาวจีรนุช มาทำการตรวจสอบ พร้อมกับเชิญตัว นางสาวจีรนุช ผอ.เว็บไซต์ประชาไท มาสอบปากคำที่กองปราบปราม โดยผู้ต้องหาได้ให้การปฏิเสธตลอดข้อกล่าวหา โดยอ้างว่าข้อความดังกล่าวที่อยู่ในเว็บไซต์ประชาไท เป็นข้อความของผู้ที่เข้ามาอ่านข่าวสารในเว็บ และเขียนไว้ในเว็บบอร์ดสาธารณะของเว็บไซต์ดังกล่าว ซึ่งภายหลังเจ้าหน้าที่ผู้ดูแลเว็บไซต์ตรวจพบก็ได้ลบข้อความที่มีเนื้อหาเชิงหมิ่นเบื้องสูงทิ้งหมดแล้ว

ผู้สื่อข่าวรายงานว่า สำหรับกรณีการตรวจค้นและจับกุม ผอ.เว็บไซต์หนังสือพิมพ์ประชาไทออนไลน์ ครั้งนี้ ทางเจ้าหน้าที่ตำรวจชุดจับกุมไม่สามารถเปิดเผยข้อมูลรายละเอียดเชิงลึกต่อสื่อมวลชนได้ เนื่องจากเป็นคดีสำคัญ

อย่างไรก็ตาม จากการสอบถาม นายชูวัส ฤกษ์ศิริสุข บรรณาธิการ ให้การในเบื้องต้น ว่า เข้าใจว่าประเด็นที่เจ้าหน้าที่ตำรวจจับกุมในครั้งนี้ น่าจะเกิดจากการที่มีผู้เข้ามาโพสต์ข้อความในเว็บบอร์ด ซึ่งมีข้อความเป็นจำนวนมาก อาจลบไม่ทันจึงเกิดปัญหาขึ้น

<u>การกระทำความผิดตาม พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550</u>

จากข่าวข้องต้น เป็นการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ในมาตรา 14 ระบุว่า ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ ได้แก่

14 (1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอม ไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

14 (3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

14 (5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1)(2)(3)(4)

มาตรา 15 ระบุว่า ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมา

และ ตามประมวลกฎหมายอาญา มาตรา 112 ซึ่งบัญญัติว่า “ผู้ใดหมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์ ต้องระวางโทษจำคุกตั้งแต่สามปี ถึงสิบห้าปี”

บรรณนานุกรมประจำบทที่ 6

[1] http://www.slideshare.net/tasawawan2k/04-rull-12767545 (สืบค้นเมื่อวันที่ 10 กรกฎาคม 2556).

[2] samtech-lms.net/Intranet_km/file_pdf/Threats.pdf (สืบค้นเมื่อวันที่ 10 กรกฎาคม 2556).

[3] http://www.ryt9.com/s/prg/1616696 (สืบค้นเมื่อวันที่ 10 กรกฎาคม 2556).

[4] http://www.komchadluek.net (สืบค้นเมื่อวันที่ 10 กรกฎาคม 2556).

[5] http://www.manager.co.th/Crime/ViewNews.aspx?NewsID=9520000025994 (สืบค้นเมื่อวันที่ 6 สิงหาคม 2556).