ในมุมมืดของอาชญากรรมคอมพิวเตอร์ (computer-related crime))

ต้องยอมรับกันโดยดุษฎีว่า คอมพิวเตอร์และอุปกรณ์ดิจิตอลกลาย เป็นปัจจัยสำคัญในชีวิต ประจำวันของผู้คนในศตวรรษที่ 21 และก็ต้องยอมรับกันอีกข้อหนึ่งว่า เมื่อมีด้านสว่างของคุณประโยชน์จากคอมพิวเตอร์ ย่อมมีด้านมืดที่อาชญากรได้อาศัยคอมพิวเตอร์ในการสร้างความเสียหายให้แก่ผู้ใช้อื่นๆ ต่อไปนี้ จะเป็นตัวอย่างด้านมืดของอาชญากรรมคอมพิวเตอร์ ด้วยหวังว่าสุจริตชน ที่รับรู้ รับทราบ จะเพิ่มความระมัดระวัง ไม่พลัดหลงเข้าไปในมุมมืดเช่นนั้น

ความเป็นมา

แนวคิดและการศึกษาเรื่องอาชญากรรมคอมพิวเตอร์ มีรากฐานมาจากผลการศึกษาและรายงานของ D.B.Parker, S.Nycum and S.S.Ora แห่งสถาบันวิจัยแสตนด์ฟอร์ด แคลิฟอร์เนีย ชื่อ “ Computer Abuse “ เมื่อปี 1973 ต่อมาได้มีการปรับปรุงและนำเสนอในปี 1979 และ ปี 1989 โดยวางกรอบการศึกษาอาชญากรรมคอมพิวเตอร์ใน 3 สถานะคือ คอมพิวเตอร์ในฐานะที่เป็นตัวต้นเหตุ(subject) ของการกระทำผิด, ในฐานะที่เป็นวัตถุ(object)แห่งการกระทำผิด หรือ เป็นเครื่องมือที่ใช้ในการกระทำผิด ซึ่งแบบจำลองแนวคิดดังกล่าว ถือว่า(regard) อาชญากรรมคอมพิวเตอร์คือการกระทำที่ต้องตามตามกฎหมาย และหรือตามหลักนิติศาสตร์ ซึ่ง (ก) เกี่ยวข้องโดยตรงกับการใช้คอมพิวเตอร์และเทคโนโลยีการสื่อสาร โดยตัวของมันเอง (ข) เกี่ยวข้องกับการใช้เทคโนโลยีดิจิตอลในการกระทำผิด หรือ (ค) เกี่ยวข้องกับการใช้คอมพิวเตอร์ตามปกติธรรมดา โดยมีเจตนาที่จะก่ออาชญากรรมอื่นๆ ด้วยเหตุนี้ คอมพิวเตอร์จึงอยู่ในฐานะที่เป็นแหล่งรวมพยานหลักฐานทางดิจิตอลอีกอย่างหนึ่งด้วย

รูปแบบของอาชญากรรมคอมพิวเตอร์

คอมพิวเตอร์ในฐานที่เป็นตัวต้นเหตุในการก่ออาชญากรรม ส่วนใหญ่จะมีเป้าหมายการโจมตีอยู่ที่เทคโนโลยีสารสนเทศและการสื่อสาร ได้แก่ การทำลายระบบความมั่นคงและทำลายความราบรื่นของระบบคอมพิวเตอร์, การโจรกรรมบริการด้านโทรคมนาคม และบริการทางด้านคอมพิวเตอร์โดยการใช้เทคนิคการ hack [เช่น การเข้าระบบโดยไม่ได้รับอนุญาต, การทำลายโค้ดและรหัสผ่าน, การโคลนนิ่งดิจิตอล, การ skim บัตรเครดิตและอื่นๆ][การโจมตีแบบ DoS [Denial-of-Service เป็นการระดมคำร้องขอเข้าระบบหรือเว็บไซต์ในเวลาเดียวกันในปริมาณมากจนระบบไม่อาจให้บริการได้ เกิดสะดุดของการทำงานของสายไฟเบอร์ออปติค ระบบหยุดชะงัก][การแพร่ไวรัสคอมพิวเตอร์ เมื่อ 20 ปี ที่ผ่านมา ซึ่งในปัจจุบันพบการแพร่ระบาดของหนอนไวรัสสองชนิดที่สำคัญ คือชนิดแรกเป็นหนอนไวรัสที่ออกแบบมาเพื่อโจมตีคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการของบริษัทที่ได้รับความนิยมมากซึ่งประมาณกันว่ามีถึงสิบล้านเครื่องทั่วโลก และชนิดที่สองคือหนอนไวรัสที่ออกแบบมาเพื่อโจมตีโปรแกรมประยุกต์เพื่อความปลอดภัยระดับสูงซึ่งใช้ในฐานปฏิบัติการเพียงไม่กี่หมื่นฐานทั่วโลก

คอมพิวเตอร์ในฐานที่เป็นวัตถุแห่งการกระทำผิด ได้แก่ การลักลอบเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาต, การโจมตี ทำลายข้อมูล ทั้งในระดับที่สามารถกู้คืนได้ ไปจนถึงระดับที่ไม่อาจกู้คืนได้ รวมถึงการทำลายอุปกรณ์การเก็บรักษาไฟล์ข้อมูลด้วย

คอมพิวเตอร์ในฐานที่เป็นเครื่องมือ หรืออุปกรณ์ในการกระทำผิด ได้แก่ การดัดแปลงข้อมูลของคนอื่น, การทำลายหรือเปลี่ยนแปลงหน้าเว็บไซต์ของคนอื่น, การใช้คอมพิวเตอร์ในการปลอมแปลงเอกสาร หรือเงินตรา ซึ่งมีความละเอียดปราณีต และแนบเนียนเหมือนจริง, การใช้คอมพิวเตอร์ในการโจรกรรมข้อมูล เช่นการจารกรรมในแวดวงอุตสาหกรรมเพื่อให้ได้ข้อมูลลับที่เป็นลิขสิทธิ์, การโจรกรรมทรัพย์สินทางปัญญา, การโจรกรรมข้อมูลเกี่ยวกับบุคคล รวมถึง การบุกรุก ละเมิดความเป็นส่วนตัว ละเมิดสิทธิส่วนบุคคล ของคนอื่น

รูปแบบของอาชญากรรมคอมพิวเตอร์มีหลายประเภท ประเภทที่เกี่ยวเนื่องกับการโจรกรรมทางเศรษฐกิจ ได้แก่ การ hack เข้าระบบธนาคารหรือสถาบันการเงิน, การฉ้อโกงด้วยการโอนย้ายเงินผ่านระบบอิเลคทรอนิคส์, การฟอกเงินและการหลบหนีภาษี ประเภทที่พบมากคือ การฉ้อโกงในซื้อขาย, การประมูลสินค้า ทางทีวี และทางอินเตอร์เน็ต ซึ่งในสหรัฐอเมริกามีการฉ้อโกงประเภทนี้สูงถึง 61% ของการร้องเรียนเกี่ยวกับการฉ้อโกงทั้งหมดในปี 2003

“phishing” หรือ “spoof spam” เป็นอีกรูปแบบหนึ่งของการโจรกรรมข้อมูลเกี่ยวกับบุคคล โดยอาชญากรจะสร้างเว็บไซต์ลง(spoof website) หรือส่ง spoof email ถึงผู้ใช้อินเตอร์เน็ตที่ไม่รู้เรื่องรู้รวม ให้หลงเชื่อว่าเป็นเว็บไซต์ของธนาคาร หรือองค์กรที่น่าเชื่อถือและถูกต้องตามกฎหมาย ซึ่งหากผู้หลงเชื่อติดต่อและให้ข้อมูลสำคัญของตนเองเช่น ข้อมูลเกี่ยวกับธนาคาร, หนังสือเดินทาง, วันเดือนปีเกิด, ที่อยู่, ใบอนุญาตขับขี่ ฯ ข้อมูลเหล่านี้จะถูกนำไปใช้โดยอาชญากร หรือถูกนำไปขายให้บุคคลที่สามต่อไป

รูปแบบอาชญากรรมอื่นๆที่พบเห็นได้แก่ การข่มขู่ กรรโชกว่าจะเปิดเผยข้อมูลที่เจ้าของสงวนสิทธิ์ หรือข้อมูลเกี่ยวกับบุคคลให้คนอื่นได้รับรู้ หรือการข่มขู่ว่าจะทำลายระบบ หรือทำลายฐานข้อมูล การรบกวน รังควาญแบบอื่นๆ เช่น การหมิ่นประมาท การใส่ร้ายป้ายสี อ่านระบบเครือข่ายคอมพิวเตอร์ซึ่งมีการสืบสวนติดตามจับกุมได้จำนวนมาก

อาชญากรรมที่เกี่ยวเนื่องกับความบันเทิง ซึ่งมีคอมพิวเตอร์เข้าไปเกี่ยวข้องด้วย รวมถึงข้อถกเถียงเกี่ยวกับวัตถุที่เป็นอัตรายและผิดกฎหมาย คือการเผยแพร่ภาพเด็กในลักษณะที่เป็นสื่อลามกอนาจาร ซึ่งนานาชาติก็ให้ความห่วงในเรื่องนี้ แม้ว่าจะปรากฏเรื่องนี้มาหลายสิบปีแล้ว แต่ในปี 1980 ได้มีการเติบโตของการเผยแพร่ภาพเด็กในลักษณะลามาอนาจารผ่านระบบเครือข่ายคอมพิวเตอร์ ทั้งในระบบ เว็บไซต์, Usenetnewsgroup, Internet Relay Chat(IRC) และ peer-to-peer(P2P) การแพร่ข่าวสารในเรื่องการท่องเที่ยวเพื่อมีเพศสัมพันธ์กับเด็ก(child sex tour) โดยใช้ระบบเครือข่ายคอมพิวเตอร์ในการแลกเปลี่ยนข่าวสารและการโอนเงินระหว่างกัน ซึ่งเข้าข่ายเป็นการค้าให้กับกลุ่มผู้มีรสนิยมมีเพศสัมพันธ์กับเด็ก และมีความเชื่อมโยงกับอาชญากรที่เป็นองค์กรข้ามชาติ นอกจากนี้ยังมีการแพร่สื่อโฆษณาและสิ่งที่ก่อให้เกิดความเกลียดชังระหว่างกลุ่มชน, เชื่อชาติ และเผ่าพันธ์อีกด้วย เมื่อไม่กี่ปีที่ผ่านมา นานาชาติได้เพิ่มความสนใจมากขึ้นในเรื่องความสัมพันธ์ระหว่างกลุ่มก่อการร้ายและอินเตอร์เน็ต มีข้อบ่งชี้ว่า อินเตอร์เน็ตถูกใช้เพื่ออำนวยการทางการเงินของกลุ่มก่อการร้าย, ใช้เป็นเครื่องมือทางยุทธศาสตร์เพื่อการวางแผนและปฏิบัติการก่อการร้าย, ใช้ในการเผยแพร่คำชวนเชื่อหาแนวร่วม หาสมาชิกใหม่ผ่านอินเตอร์เน็ต

ในหลายปีที่ผ่านมา ได้มีความพยายามแก้ไขปรับปรุงระบบการส่งข้อมูลผ่านเครื่อข่ายคอมพิวเตอร์ให้มีความปลอดภัยมากขึ้น ซึ่งยุคใหม่ของ Quantum Cryptography (การแปลงข้อมูลให้เป็นรหัสที่คนอื่นอ่านไม่ได้ แล้ว

ส่งผ่านระบบไฟเบอร์ออปติก หรือเครือข่ายไร้สาย ซึ่งผู้รับต้องแปลงรหัสให้กลับเป็นข้อความปกติก่อน จึงจะเข้าใจ) ได้ถูกนำมาใช้ในวงกว้าง ซึ่งเกิดประโยชน์อย่างมากกับภาคธุรกิจและ e-commerce แต่มันก็เป็นประโยชน์กับอาชญากรเช่นกัน นอกจากนี้ เทคโนโยลีที่ใช้ระหว่างผู้ใช้สองฝ่ายภายใต้ระบบการแปลงรหัส (steganography) ที่ใช้กันอย่างแพร่หลายในระบบเครือข่ายแบบ peer-to-peer โดยมีระบบรหัสผ่านอย่างเข้มงวดนั้น เป็นการตรวจสอบการเข้าถึงระบบของบุคคลที่ไม่เกี่ยวข้องที่มีความปลอดภัยในระดับสูง ซึ่งถือว่าเป็นด้านสว่างของการใช้ระบบเครือข่ายคอมพิวเตอร์ที่มีประโยชน์และมีความปลอดภัย แต่ก็มีด้านมืดอยู่ด้วยเสมอ คือ กลุ่มอาชญากรก็ได้ใช้เทคโนโลยีดังกล่าวเป็นที่หลบซ่อน ปิดบัง การติดต่อสื่อสารภายในกลุ่ม หรือใช้เผยแพร่ข่าวสาร สิ่งผิดกฎหมายอื่นๆ อีกด้วย

กรณีตัวอย่างของอาชญากรคอมพิวเตอร์

1. ชาวเมืองเมลเบอร์น ออสเตรเลีย จำนวนสองคน ได้ส่งอีเมล์ จำนวน 6-7 ล้านฉบับ และ post ข้อความบนกระดานข่าวอิเลคทรอนิคส์ จำนวนมาก เพื่อเข้าร่วมซื้อหุ้นบริษัทสัญชาติอเมริกาที่ทำการซื้อขายในตลาดหลักทรัพย์ NASDAQ ซึ่งตั้งอยู่ใน สหรัฐอเมริกา โดยวิธีการใช้ชื่อปลอมและส่งอ้อมผ่านผู้ให้บริการอินเตอร์เน็ตรายที่สาม แจ้งราคาซื้อหุ้นสูงขึ้นถึง 900% ในชั่วเวลาสั้นๆหลังจากนั้น ทำให้ปริมาณซื้อขายเพิ่มขึ้นถึงสิบเท่าและราคาสูงเป็นเท่าตัว ก่อนที่การซื้อขายจะหยุดชะงักลงและบริษัทปฏิเสธคำเสนอซื้อขายที่ส่งผ่านช่องทางสื่อสารทุกรูปแบบ ทั้งสองคนนี้ได้กำไรจากการกระทำที่เรียกว่าการ “ pump and dump “ หรือการปั่นหุ้น ทั้งสองคนกระทำการละเมิดต่อกฎหมายของออสเตรเลียและสหรัฐอเมริกา ในข้อหาติดต่อและแจ้งข้อมูลข่าวสารแก่ตลาดหลักทรัพย์ด้วยข้อความอันเป็นเท็จ, การทำการแทรกแซง กีดขวาง การปฏิบัติการของคอมพิวเตอร์ด้วยการสร้างอีเมล์ลวงในการเสนอซื้อ-ขาย ผู้กระทำผิดทั้งสองคนถูกสืบสวนติดตามได้จากการแกะรอยข้อความอีเมล์ที่ส่งผ่านเครือข่ายธุรกิจ และจากเส้นทางการเงินที่ใช้ไปในการจ่ายเป็นค่าบริการอินเตอร์เน็ต และถูกพิพากษาลงโทษในออสเตรเลีย โดยความเห็นชอบของสหรัฐอเมริกา(ไม่ต้องส่งไปดำเนินคดีที่สหรัฐ)

2. เด็กชาวแคนาดา วัย 15 ปี ทำการบางอย่างให้ได้มาซึ่งการควบคุมคอมพิวเตอร์จำนวนมาก และใช้เป็นเครื่องมือในการโจมตีแบบ denial-of-service ซึ่งมีเป้าหมายคือ Yahoo, Amazon.com และเว็บไซต์ที่ให้บริการ e-commerce อื่นๆ เมื่อเดือนกุมภาพันธ์ ค.ศ. 2000 การกระทำของเขาได้สร้างความเสียหายให้กับบริษัทเหล่านั้นทั้งในรูปความเสียหายทางธุรกิจ, ตลาดเงินทุน และค่าใช้จ่ายในการปรับปรุงระบบรักษาความปลอดภัย นับเป็นมูลค่าหลายล้านเหรียญสหรัฐ หลังจากที่เขาได้เข้าไปคุยโม้ถึงผลงานดังกล่าวในห้องสนทนาอินเตอร์เน็ต หน่วย FBI ของสหรัฐอเมริกาก็สามารถแกะรอยพบตัวเขาได้ และส่งเรื่องให้ตำรวจแคนาดาดำเนินคดี ภายใต้อำนาจศาลคดีเด็กและเยาวชนของแคนาดา

3. กรณีโด่งดังมาก เมื่อปี ค.ศ. 1990 คือกรณีโจมตีธนาคาร Citibank โดยเด็กหนุ่มที่อยู่ในรัสเซียได้เข้าถึงฐานข้อมูลของธนาคารที่ตั้งอยู่ในสหรัฐอเมริกาโดยไม่ได้รับอนุญาต เขาได้ทำการเปิดบัญชีธนาคารหลายบัญชีทั่วโลกและสั่งให้คอมพิวเตอร์ของธนาคาร Citibank โอนเงินไปเข้าบัญชีที่เขาเปิดไว้ เมื่อมีการตรวจพบการกระทำผิด ผู้มีอำนาจออกหมายจับคือศาลแห่งสหรัฐอเมริกา แต่ในขณะนั้น สหรัฐอเมริกาและรัสเซียไม่มีสนธิสัญญาส่งผู้ร้ายข้ามแดน อย่างไรก็ตามผู้ก่อกรรมย่อมหนีวิบากกรรมไม่พ้น เมื่อเด็กหนุ่มชาวรัสเซียคนนี้ได้เดินทางมายังประเทศอังกฤษ เพื่อชมงานแสดงสินค้าเกี่ยวกับคอมพิวเตอร์ และถูกจับกุม ซึ่งอังกฤษมีสนธิสัญญาส่งผู้ร้ายข้าม

แดนกับสหรัฐอเมริกา ภายใต้สนธิสัญญาส่งผู้ร้ายข้ามแดนของอังกฤษข้อหนึ่งระบุว่า อังกฤษจะส่งผู้ร้ายข้ามแดนได้หากข้อหาหรือความผิดที่ผู้ต้องหาถูกจับกุมนั้นเป็นความผิดเช่นเดียวกันกับกฎหมายของอังกฤษ ผู้ต้องหาได้ต่อสู้ว่าการกระทำผิดได้เกิดขึ้นในประเทศรัสเซีย กล่าวคือ คีย์บอร์ดคอมพิวเตอร์ที่เขาใช้กระทำความผิดตั้งอยู่ในประเทศรัสเซีย ไม่ใช่ในสหรัฐอเมริกา เขาจึงควรถูกดำเนินคดีในรัสเซีย แต่ศาลได้พิจารณาว่า การแสดงออกทางกายภาพของผู้ต้องหาในเมืองปีเตอรส์เบอร์ก มีนัยยะสำคัญน้อยกว่าความจริงที่ว่าเขาได้ปฏิบัติการบนจานแม่เหล็ก(หรืออุปกรณ์บรรจุข้อมูลและการสั่งการของคอมพิวเตอร์) ของธนาคาร ที่ตั้งอยู่ในสหรัฐอเมริกา นอกจากนี้ความผิดที่เขาถูกจับกุมตามหมายจับของสหรัฐอเมริกา เป็นความผิดที่เหมือนกันกับกฎหมาย Computer Misuse Act 1990 ของอังกฤษ ศาลอังกฤษจึงมีอำนาจส่งตัวผู้ต้องหาให้ศาลสหรัฐอเมริกาพิจารณาดำเนินคดี และผู้ต้องหารายนี้ได้ถูกพิพากษาจำคุกในสหรัฐอเมริกา

ที่มา : Eleventh United Nation Congress On Crime Prevention and Criminal Justice

Bangkok, 18-25 April 2005

Workshop 6: Measures to Combat Computer-related Crime

Background paper (Distr.: general on 14 March 2005)