รายงานผลการฝึกอบรมเรื่อง "การสืบสวนสอบสวนเงินดิจิทัล (Bitcoin Investigation)"
จัดโดย สำนักงาน ปปง. ระหว่างวันที่ ๑๐ - ๑๑ ตุลาคม ๒๕๖๐

หลักการและเหตุผลของโครงการ / วัตถุประสงค์

อาชญากรในปัจจุบันนี้ใช้ช่องทางการทำธุรกรรมเงินเสมือน (Cryptocurrency) บนโลกดิจิทัล เป็นเครื่องมือในการประกอบอาชญากรรมและการฟอกเงิน และถือว่าเป็นเครื่องมือที่มีประสิทธิภาพสูงสำหรับอาชญากรหรือผู้มีส่วนร่วมในกระบวนการกระทำความผิดซึ่งไม่ว่าจะอยู่แห่งใดของโลกก็สามารถก่อภัยคุกคามให้เกิดความเดือดร้อนเสียหายให้แก่บุคคลใดๆ แม้อยู่อีกมุมหนึ่งของโลกก็ย่อมได้ การที่เจ้าหน้าที่ของรัฐเข้าดำเนินการติดตามสืบหาร่องรอยการทำธุรกรรมดังกล่าวนั้นไม่อาจกระทำได้โดยง่าย หากแต่ต้องอาศัยความรู้เฉพาะทางของผู้เชี่ยวชาญซึ่งสั่งสมจากประสบการณ์ตรงในการใช้เงินเสมือนและในการสืบสวนรวบรวมพยานหลักฐานเพื่อดำเนินคดีกับอาชญากรผู้กระทำความผิด แบ่งปันและถ่ายทอดให้แก่ผู้เข้ารับการอบรม

วิธีการฝึกอบรม

วิทยากรบรรยายให้ความรู้และยกตัวอย่างกรณีศึกษาโดยมีสื่อวีดิทัศน์ประกอบ เปิดโอกาสให้ผู้เข้ารับการอบรมซักถามข้อสงสัยได้

วิทยากร



Mr.Jaroslav Jakubcek

ผู้เชี่ยวชาญด้านการสืบสวนอาชญากรรมทางคอมพิวเตอร์ (Cyber crime) จาก European Union Agency for Law Enforcement Cooperation (Europol)

ประวัติการศึกษา:-

- วิทยาศาสตรมหาบัณฑิต สาขาเศรษฐศาสตร์ (MSc in Economics)
- วิทยาศาสตรมหาบัณฑิต สาขาการสืบสวนอาชญากรรมและการพิสูจน์หลักฐานทางคอมพิวเตอร์ (MSc in Forensic Computing and Cybercrime Investigation)

ประวัติการทำงาน:-

- โปรแกรมเมอร์และผู้ดูแลระบบข้อมูล ที่ America Online (AOL) เป็นเวลากว่า 10 ปี
- Operational Crime Analyst ที่ Ireland's National Police Service เป็นเวลากว่า 5 ปี มีประสบการณ์ในการสืบสวนคดีอาชญากรรมรุนแรงต่างๆ จำนวนมากมาย อาทิเช่น คดีฆาตกรรม, การล่วงละเมิดทางเพศ การค้ายาเสพติด การฟอกเงิน และอาชญากรรมทางคอมพิวเตอร์ เป็นต้น
- ตั้งแต่ปี 2557 ปฏิบัติหน้าที่ Strategic Analyst ที่ European Cybercrime Centre (EC3) ซึ่งเป็นหน่วยงานใน Europol

<u>สรุปสาระสำคัญจากการฝึกอบรมได้โดยสังเขป ดังนี้</u>

หัวข้อบทเรียน ได้แก่ (บรรยายและอภิปรายร่วมกัน)

1. Bitcoin crimes
2. Darknet: Underground market places
3. Tracing bitcoin transactions
4. กรณีศึกษา (Case study)

<u>หัวข้อบทเรียนที่ 1</u>

สำหรับหัวข้อบทเรียนที่ 1 – 3 วิทยากรผู้บรรยายมาจากหน่วยงาน Europol เนื้อหาที่บรรยาย ได้แก่

1. ข้อมูลเบื้องต้น ภารกิจ อำนาจหน้าที่ ของ Europol

   ที่ตั้งสำนักงาน Europol อยู่ที่กรุงเฮก ประเทศเนเธอแลนด์ และมีเครือข่ายความร่วมมือในหลายๆประเทศในทวีปยุโรป ทำหน้าที่หลักในการสนับสนุนภารกิจสืบสวนในประเทศที่มีข้อตกลงร่วมกัน แต่ไม่มีอำนาจในการจับกุมผู้กระทำผิด

2. ความรู้เกี่ยวกับบิทคอยน์

   ผู้บรรยายได้แนะนำแหล่งข้อมูลออนไลน์ที่เป็นประโยชน์ และได้กล่าวถึงสถานการณ์ปัจจุบันของบิทคอยน์ ซึ่งมีการนำเงินเสมือน/เงินดิจิตัล หรือเงินบิทคอยน์มาใช้อย่างถูกกฎหมายในหลายรูปแบบ เช่น P2P transfer, Offline purchase, Microtransaction เป็นต้น และมีผู้ประกอบการ/บริษัท หลายแห่งยอมรับการชำระเงินด้วยบิทคอยน์แล้ว เช่น Microsoft Dell Expedia Newegg Overstock และเว็บไซต์พนันออนไลน์ เช่น Satoshi Dice และ DirectBet เป็นต้น

   จากสถิติปี ค.ศ. 2015 ถึง ค.ศ. 2016 การใช้บิทคอยน์ มีแนวโน้มที่จะเพิ่มขึ้นร้อยละ 25 ซึ่งสังเกตได้จากจำนวน Bitcoin Wallet ที่เพิ่มขึ้น จำนวนผู้ประกอบการ/บริษัท ที่ยอมรับการชำระเงินด้วยบิทคอยน์ ก็สูงขึ้นถึงร้อยละ 42 นอกจากนี้จำนวน transaction หรือธุรกรรมที่ใช้บิทคอยน์ ก็มีแนวโน้มสูงขึ้นมากเช่นกัน

3. วิธีการที่อาชญากรนำบิทคอยน์ไปใช้ในทางที่ผิดกฎหมาย

   อาชญากรมีวิธีการนำบิทคอยน์มาใช้ในการแสวงหาผลประโยชน์โดยมิชอบด้วยกฎหมายหลายวิธี เช่น

   3.1 อาชญากรกับแฮคเกอร์ทำงานร่วมกันโดยใช้บิทคอยน์แฝงตัวเป็น malware/ransomware และ scam แทรกตัวเข้าไปในคอมพิวเตอร์ของผู้เสียหาย หรือการใช้โปรแกรมจำพวก DDoS เข้าโจมตีระบบแล้วทำการแบล็คเมล์ จากนั้นจึงเรียกรับเงินจากผู้เสียหาย

   3.2 ใช้บิทคอยน์ซื้อสินค้าจากอาชญากรด้วยกันเองใน Darknet (เว็บไซต์จำหน่าย สินค้า/บริการ ผิดกฎหมาย)

2) เมื่อผู้ซื้อมีเงินบิทคอนย์แล้วก็สามารถดำเนินการซื้อสินค้าและชำระเงินบิทคอยน์ผ่าน DarkNet ซึ่งจะมี administrator หรือผู้ดูแลระบบทำหน้าที่ดูแลการซื้อขาย
3) ผู้ซื้อโอนเงินบิทคอยน์ไปยัง Administrator
4) Administrator แจ้งไปยังผู้ขาย (seller) ว่ามีผู้ซื้อต้องการซื้อสินค้า/บริการ
5) ผู้ขายสินค้า/บริการ ส่งสินค้าให้แก่ผู้ซื้อ
6) Administrator ชำระค่าสินค้า/บริการ โดยแลกเปลี่ยนเงินบิทคอยน์ที่ได้จากผู้ซื้อเป็นเงินสกุลที่ใช้ในโลกจริงผ่าน Exchanger/dealer จากนั้น Exchanger/dealer จะดำเนินการจ่ายเงินให้กับผู้ขายสินค้า/บริการ

<u>ธุรกรรมที่ใช้เงินสกุลบิทคอยน์</u>

ผู้บรรยายได้อธิบายเพิ่มเติมถึงกลไกการทำงานของการซื้อขายสินค้าและบริการด้วยเงินบิทคอยน์ว่า ผู้ซื้อสินค้าจะมีบิทคอนย์แอดเดรสเป็นของตนเอง โดยแอดเดรสจะถูกสร้างขึ้นแบบสุ่มด้วยระบบคอมพิวเตอร์ และผู้ซื้อต้องทราบแอดเดรสของผู้ขายสินค้า/บริการนั้น ๆ เพื่อใช้ในการโอนเงินบิทคอยน์สำหรับชำระค่าสินค้าและบริการด้วย แอดเดรสในธุรกรรมที่ใช้เงินบิทคอยน์ประกอบด้วยตัวเลขและตัวอักษร 26-34 ตัว เช่น

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

แอดเดรสทำหน้าที่เป็นเสมือนหมายเลขบัญชีสำหรับ ขอโอน/รับโอน เงินบิทคอยน์ อย่างไรก็ตาม แอดเดรสของธุรกรรมที่ใช้เงินบิทคอยน์จะแตกต่างจากหมายเลขบัญชีในลักษณะที่ว่า แอดเดรสจำนวน 1 แอดเดรสจะใช้สำหรับธุรกรรม 1 รายการเท่านั้น นั่นคือ ทันทีที่ผู้ซื้อทำการชำระค่าสินค้าหรือขอโอนเงินบิทคอยน์ออกจาก Bitcoin wallet แล้ว แอดเดรสของผู้ซื้อจะเปลี่ยนไป และในขณะเดียวกัน แอดเดรสของผู้รับโอนหรือผู้ขายสินค้าก็จะเปลี่ยนไปทันทีที่มีเงินบิทคอยน์โอนเข้ามาใน Bitcoin wallet ของตนเอง ผู้บรรยายกล่าวว่าคุณสมบัติที่ว่านี้ส่งผลให้การแกะรอยหรือติดตามเส้นทางการเงินได้เป็นไปได้ยาก

อีกประการหนึ่ง ผู้ที่ทำธุรกรรมสามารถมีแอดเดรสได้มากกว่า 1 แอดเดรสสำหรับการทำธุรกรรม 1 รายการ และในเว็บไซต์สำหรับซื้อขายสินค้า/บริการที่ผิดกฎหมาย เช่นเว็บไซต์ Darknet จะมีโปรแกรมที่เรียกว่า “Mixer” ที่สามารถรวม (mix) แอดเดรสทั้งหมดที่มีให้เสมือนว่าเป็นแอดเดรสเดียวหลังจากที่มีการทำธุรกรรมเกิดขึ้น ซึ่งทำให้การสืบสวนหรือติดตามเส้นทางการเงินเป็นไปได้ยากขึ้นไปอีก นอกจากการทำธุรกรรม 1 รายการจากหลาย ๆ แอดเดรสแล้ว ยังมีการทำธุรกรรมหลาย ๆ ธุรกรรมโดยใช้แอดเดรสเพียง 1 แอดเดรสอีกเช่นกัน (Multiple transactions to a single bitcoin address)

ผู้บรรยายยังได้กล่าวถึงธุรกรรมที่ใช้เงินบิทคอยน์ว่า แต่ละธุรกรรมจะมี Transaction ID ซึ่งประกอบด้วยตัวเลขและตัวอักษรแบบสุ่มจำนวน 64 ตัว เช่น

e03a9a4b5c557f6ee3400a29ff1475d1df73e9cddb48c2391abdc391d8c1504a

ที่ใช้ในการทำธุรกรรมบิทคอยน์จะเปลี่ยนแปลงไปเสมอในทุกครั้งที่มีการทำธุรกรรม แต่ปัจจุบันมีระบบ

คอมพิวเตอร์ที่เรียกว่า “Address Watcher” ช่วยในการจำแนกแอดเดรส และมีระบบ De-mixing Tool สำหรับใช้ในการจำแนกแอดเดรสหลาย ๆ แอดเดรสที่ถูกรวม (mix) จนดูเสมือนว่าเป็นแอดเดรสเดียว ให้ออกมาเป็น 1 แอดเดรส

2) ประสานงานขอข้อมูลจาก Bitcoin exchanger ซึ่งทำหน้าที่เป็นผู้ซื้อขายแลกเปลี่ยนเงินสกุลบิทคอยน์กับสกุลเงินที่ใช้ในโลกจริง

โดยทั่วไป เมื่อผู้กระทำความผิดได้เงินสกุลบิทคอยน์แล้ว ย่อมต้องการที่จะนำเงินบิทคอยน์มาแลกเปลี่ยนเป็นเงินสกุลที่ใช้ในโลกจริง เพื่อที่จะนำไปซื้อสินค้าและบริการอื่นๆในโลกจริงต่อไปได้ หรือเพื่อทำการโอน ถ่ายเท ซุกซ่อนเงินที่ได้จากการกระทำความผิด ซึ่งการที่จะแลกเปลี่ยนเงินสกุลบิทคอยน์เป็นเงินสกุลที่ใช้ในโลกจริงได้นั้น ต้องดำเนินการผ่าน Exchanger/dealer

Exchanger หรือ dealer จะมีข้อมูลแอดเดรสที่ผู้กระทำความผิดใช้ครั้งล่าสุดในการทำธุรกรรมแลกเปลี่ยนเงินบิทคอยน์เป็นเงินสกุลที่ใช้ในโลกจริง นอกจากนี้ยังมีข้อมูลในส่วนของบัญชี (Account) ที่ผู้ทำธุรกรรมลงทะเบียนไว้ ซึ่งข้อมูลประกอบไปด้วย Username Real name Email address รวมไปถึง IP address และ Transaction data เป็นต้น

3) นำ username, real name, email, IP address และ transaction data ไปค้นหาข้อมูลในข้อจากเว็บไซต์ในข้อ 1) และเมื่อดำเนินการสืบสวนต่อไป ก็จะได้ข้อมูลชื่อผู้รับผลประโยชน์ ชื่อธนาคาร/บัญชี ที่ใช้ทำธุรกรรม รวมไปถึงชื่อ Twitter/Facebook/Paypal ซึ่งสามารถสืบสวนขยายผลไปถึงที่อยู่ของผู้กระทำความผิดได้

4) ใช้โปรแกรม Chainanalysis วาดแผนผังความเชื่อมโยงการทำธุรกรรมที่ใช้เงินสกุลบิทคอยน์ ซึ่งจะทำให้ทราบเส้นทางการเงินและ ตัวการ/ผู้กระทำผิด ที่มีเงินไหล เข้า/ออก มากที่สุด

ผู้บรรยายกล่าวว่า ปัจจุบัน Europol มี European Cyber Crime Centre (EC3) ซึ่งเป็นหน่วนงานที่ตั้งขึ้นเพื่อเสริมกำลังในการบังคับใช้กฎหมายป้องกันและปราบปรามอาชญากรรมไซเบอร์ในยุโรป EC3 มีขีดความสามารถในการเข้าถึงข้อมูลเชิงลึก และมีอุปกรณ์/เครื่องมือเชิงพาณิชย์ (Commercial tool) สำหรับใช้ในการสืบสวนด้วย

EC3 มียุทธศาสตร์ในการปฏิบัติการป้องกันและปราบปรามอาชญากรรมไซเบอร์ ดังนี้

- ฝึกฝนเจ้าหน้าที่ โดยดำเนินการฝึกทั้งในสถานที่จริงและผ่านระบบออนไลน์
- จัดประชุม เพื่อให้เจ้าหน้าที่ตำรวจ Europol ได้แลกเปลี่ยนความรู้และประสบการณ์
- จัดงานพบปะพูดคุยเพื่อสร้างความสัมพันธ์อันดีระหว่าง Europol กับ Exchanger เพื่อให้การขอข้อมูลเป็นไปด้วยความราบรื่น
- วิจัยพัฒนาเครื่องมือที่ใช้ในการแกะรอยเส้นทางการเงินที่ใช้เงินสกุลบิทคอยน์
- จัดทำคู่มือเพื่อเป็นแนวทางปฏิบัติให้กับเจ้าหน้าที่สืบสวนและเจ้าหน้าที่บังคับใช้กฎหมาย

นอกจากนี้ การบรรยายยังมีเนื้อหาเกี่ยวกับกรณีศึกษาว่า รายงานของ Europol ประจำกรุงเฮก ประเทศเนเธอร์แลนด์ ที่เผยแพร่ต่อสาธารณชนในวันที่ 12 มกราคม 2559 กล่าวถึงกรณีศึกษาที่ถูกนำมาใช้เป็นตัวอย่างในการสืบสวนนี้ว่า หน่วยงานบังคับใช้กฎหมายในประเทศออสเตรีย บอสเนียแอนด์เฮอเซโกวีนา เยอรมนี และ สหราชอาณาจักร ได้ร่วมมือกับ Europol ในการสืบสวนเหตุการโจมตีระบบคอมพิวเตอร์โดยกลุ่ม DD4BC ซึ่งการสืบสวนได้นำไปสู่การจับกุมผู้ต้องสงสัยในประเทศบอสเนีย และการตรวจค้นทรัพย์สินและการเก็บรวบรวมพยานหลักฐานหลายรายการ

ผู้บรรยายยังกล่าวอีกว่า ประเทศออสเตรียเป็นผู้เปิดปฏิบัติการตรวจค้นจับกุมในครั้งนี้โดยมี EC3 และ J-CAT เป็นหน่วยงานสนับสนุน ในส่วนของ Europol นั้น ทำหน้าที่ให้การสนับสนุนฐานปฏิบัติการเคลื่อนที่ซึ่งมีเครื่องมือพิสูจน์หลักฐาน (forensic tool) รวมทั้งฐานข้อมูลที่ใช้วิเคราะห์หาตัวผู้กระทำความผิดและข้อมูลด้านข่าวกรองในรูปแบบ real-time