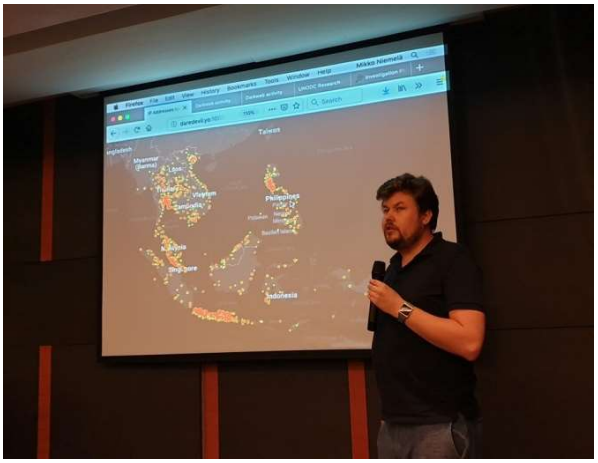
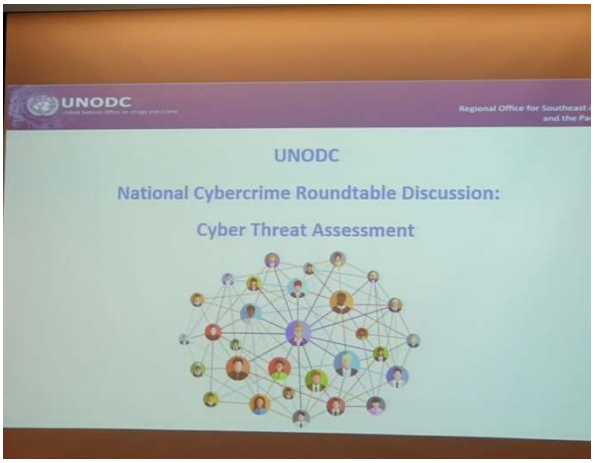
National Cybercrime Roundtable Discussion: Cyber Threat Assessment

รูปแบบของภัยคุกคามทางไซเบอร์ที่เกิดในไทย - แนวโน้มภัยคุกคามทางไซเบอร์ในปี ๒๕๖๓





ผู้แทนสำนักงานสภาความมั่นคงแห่งชาติเข้าร่วมการประชุม National Cybercrime Roundtable Discussion: Cyber Threat Assessment จัดโดย สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime: UNODC) เมื่อวันที่ ๑๐ – ๑๑ ตุลาคม ๒๕๖๒ เพื่อพัฒนาแนวทางการดำเนินการต่อปัญหาอาชญากรรมทางไซเบอร์ในภูมิภาคอาเซียน โดย UNODC จะได้จัดทำรายงานการประเมินภัยคุกคามทางไซเบอร์ (Cyber Threat Assessment Report) ทั้งนี้ ประเด็นปัญหาที่ UNODC ให้ความสำคัญ ได้แก่ ๑) อาชญากรรมทางไซเบอร์ (Cybercrime) ๒) การคุ้มครองเด็กบนพื้นที่ออนไลน์ (Online child protection) ๓) การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Digital forensics) และ ๔) สกุลเงินดิจิทัลและดาร์กเน็ต (Cryptocurrencies and darknet)

รูปแบบของภัยคุกคามทางไซเบอร์ที่เกิดในไทย

<u>การหลอกลวงบนพื้นที่ออนไลน์</u> มีหลากหลายประเภท ได้แก่ แชร์ลูกโซ่ (Ponzi scheme) การหลอกลวงข้อมูลทางออนไลน์ (Phishing) การหลอกลวงด้านความรัก (Romance scam) การหลอกลวงเพื่อประโยชน์ทางการเงินหรือการฉ้อโกงผ่านระบบคอลเซ็นเตอร์ (Call-Center scam) นอกจากนั้นยังพบว่ามีขบวนการค้ามนุษย์ใช้สื่อสังคมออนไลน์เป็นเครื่องมือหลอกลวงชักชวนประชาชนในการค้าแรงงาน และการหลอกลวงที่กำลังเป็นที่นิยมอย่างมากคือการเจาะระบบรหัสคูปองส่วนลดของร้านค้าออนไลน์แล้วนำออกจำหน่าย เช่น ร้านฟ้าสต์ฟู้ด แอพขายตั๋วภาพยนตร์

<u>การขายยาเสพติดออนไลน์</u> โดยใช้สื่อสังคมออนไลน์เป็นสื่อกลางในการติดต่อสื่อสารระหว่างผู้ซื้อและผู้ขาย และใช้ไปรษณีย์เป็นช่องทางหลักในการขนส่ง โดยการสื่อสารดังกล่าวมีลักษณะเป็นกลุ่มปิดทำให้การสืบสวนสอบสวนเป็นไปอย่างยากลำบาก

<u>การขายสินค้าละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา</u> โดยการใช้เว็บไซต์ e-commerce และสื่อสังคมออนไลน์เป็นพื้นที่ขายสินค้า โดยเมื่อมีการตรวจค้นจับกุม ผู้ขายมักจะนำสินค้าออกจากระบบและนำขึ้นทำการขายใหม่เมื่อเจ้าหน้าที่ละเลยการตรวจค้น

<u>การขายภาพลามกอนาจารเด็ก</u> ในห้วงที่ผ่านมากรมสอบสวนคดีพิเศษร่วมกับกระทรวงความมั่นคงแห่งมาตุภูมิแห่งสหรัฐอเมริกาและหน่วยงานบังคับใช้กฎหมายของประเทศที่เกี่ยวข้อง ทำการสืบสวนสอบสวนและจับกุมชาวต่างชาติที่ทำการบันทึกภาพการล่วงละเมิดเด็กเพื่อขายในประเทศออสเตรเลียและสหรัฐอเมริกา

<u>การพนันออนไลน์</u> การพนันออนไลน์ถือเป็นแหล่งเงินทุนสำคัญในการก่ออาชญากรรมประเภทอื่น โดยเว็บไซต์เหล่านี้มีทั้งชาวไทยและชาวต่างชาติเป็นเจ้าของ ทั้งนี้ เซิร์ฟเวอร์ของเว็บไซต์พนันออนไลน์ส่วนใหญ่ตั้งอยู่และจดทะเบียนในต่างประเทศ ทำให้การบังคับใช้กฎหมายเพื่อติดตามและปิดกั้นเว็บไซต์พนันออนไลน์มีข้อจำกัด

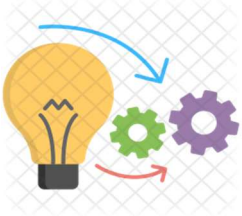
<u>การเรียกค่าไถ่จากข้อมูลที่ถูกเข้ารหัส (Ransomware)</u> ปัจจุบันสถิติเกี่ยวกับ Ransomware มีจำนวนน้อยลง อย่างไรก็ตาม บริษัทเอกชนที่เป็นเป้าหมายส่วนใหญ่มักจะปกปิดข้อมูลการถูกโจมตีเนื่องจากกังวลเกี่ยวกับผลกระทบด้านความน่าเชื่อถือ จึงไม่สามารถดำเนินกระบวนการทางกฎหมายและการจับกุมผู้กระทำความผิดได้

ปัญหาจากการดำเนินการ พบว่าปัญหาในด้านกฎหมายและการบังคับใช้กฎหมาย ส่งผลกระทบต่อการดำเนินการในการป้องกันและแก้ไขปัญหาอาชญากรรมทางไซเบอร์ ดังนี้

<u>ในด้านกฎหมาย</u> เนื่องจากยังไม่มีการกำหนดคำนิยามคำว่าอาชญากรรมไซเบอร์ที่เป็น ที่ยอมรับในระดับสากล ทำให้การกำหนดฐานความผิดเกี่ยวกับการประกอบอาชญากรรมโดยอาศัยระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด การใช้ระบบคอมพิวเตอร์เป็นเป้าหมายในการโจมตี และการนำเข้าข้อมูลที่ไม่เหมาะสม ยังไม่มีความชัดเจน ดังนั้นที่ประชุมจึงเสนอให้มีการปรับปรุงกฎหมายที่เกี่ยวข้องกับการต่อต้านองค์กรอาชญากรรมข้ามชาติให้ครอบคลุมฐานความผิดด้านอาชญากรรมไซเบอร์ด้วย

<u>ในด้านการบังคับใช้กฎหมาย</u> UNODC ได้เสนอให้มีการจัดตั้งคณะทำงานร่วมว่าด้วยการแก้ไขปัญหาอาชญากรรมทางไซเบอร์เฉพาะด้านในระดับชาติ เพื่อร่วมกันแก้ไขปัญหาและตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที รวมถึงช่วยลดระยะเวลาในการสืบสวนสอบสวนคดีอาชญากรรมทางไซเบอร์ ซึ่งเป็นคดีที่กระทำความผิดเกิดขึ้นอย่างรวดเร็ว แต่กระบวนการสืบสวนสอบสวนและการดำเนินคดีเป็นไปอย่างล่าช้า ทำให้มีจำนวนผู้กระทำความผิดและเหยื่อเพิ่มขึ้นในเวลาเดียวกัน

แนวโน้มภัยคุกคามทางไซเบอร์ในปี ๒๕๖๓




บริษัท Cyber Intelligence House ซึ่งทำหน้าที่ประเมินความเสี่ยงและให้คำปรึกษาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่ UNODC ได้นำเสนอแนวโน้มภัยคุกคามทางไซเบอร์ ในปี ๒๕๖๓ ใน ๘ ประเด็น ได้แก่ ๑) การโจมตีโดยวิเคราะห์จากประวัติการโจมตีและการถูกคุกคาม (Attack & Previous Compromises) ๒) การเปิดเผยข้อมูลความลับส่วนบุคคล (Disclosure of sensitive information) ๓) การสนทนาเกี่ยวกับข้อมูลสำคัญขององค์กร (Discussions) ๔) การซื้อขายสินค้าในตลาดมืดออนไลน์ (Black markets) ๕) การโจมตีข้อมูลทางการเงิน (Financial information) ๖) การเปิดเผยข้อมูลการระบุตัวตนเพื่อเข้าสู่ระบบหรือรหัสอื่น ๆ (Exposed credentials) ๗) การเข้าถึงข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (Personally identifiable information) และ ๘) การตกเป็นเป้าหมายของกลุ่มแฮกเกอร์ (Hacker group targeting)

ดาร์กเว็บ (Dark Web) เป็นภัยคุกคามทางไซเบอร์ที่จำเป็นต้องมีการติดตามอย่างใกล้ชิด เนื่องจากพบการกระทำที่ผิดกฎหมายบนดาร์กเว็บจำนวนมาก อาทิ การซื้อขายบัญชีธนาคาร บัญชีบัตรเครดิต หนังสือเดินทาง ข้อมูลส่วนบุคคล ตลอดจนการซื้อขายยาเสพติด อาวุธ และการค้ามนุษย์ที่เกี่ยวข้องกับกลุ่มอาชญากรรมข้ามชาติ โดยที่การเข้าถึง Dark Web ทำให้ผู้ให้บริการอินเทอร์เน็ตไม่สามารถระบุตัวตนผู้ใช้บริการและประเภทของเว็บไซต์ที่ถูกใช้บริการ จึงยากต่อการตรวจสอบและเป็นปัญหาในเชิงการบังคับใช้กฎหมาย หน่วยงานที่เกี่ยวข้องไม่อาจติดตามถึงการกระทำความผิดที่เกิดขึ้นบนเว็บไซต์เหล่านี้

ควรให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ หรือ CERT เข้ามามีบทบาทร่วมในการติดตามตรวจสอบการกระทำความผิดบนไซเบอร์สเปซ และแจ้งเตือนไปยังหน่วยงานบังคับใช้กฎหมาย รวมถึงสร้างความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ให้แก่บุคลากรภาครัฐ ภาคเอกชน และประชาชน โดยเฉพาะการเผยแพร่ข้อมูลส่วนบุคคลหรือรหัสผ่านในเว็บไซต์ที่ไม่น่าเชื่อถือมีความเสี่ยงที่จะทำให้ข้อมูลดังกล่าวถูกนำไปขายบนดาร์กเว็บ

ความเห็นที่ประชุม ที่ประชุมเสนอให้เร่งดำเนินการเกี่ยวกับการสร้างความตระหนักรู้และส่งเสริมความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยการประชาสัมพันธ์ข้อมูลข่าวสารให้เข้าถึงกลุ่มเสี่ยงทุกกลุ่ม โดยเฉพาะกลุ่มผู้ใช้ที่ขาดทักษะในการรับรู้ข้อมูลข่าวสาร (Baby user) รวมถึงมุ่งเน้นการดำเนินการเชิงรุกอย่างต่อเนื่องเพื่อให้การกระจายข้อมูลข่าวสาร การเฝ้าระวังและการแจ้งเตือนภัยครอบคลุมมากที่สุด ตลอดจนให้ความสำคัญกับการสร้างเครือข่ายการประสานงานระหว่างหน่วยงานบังคับใช้กฎหมายอย่างเป็นระบบ รวดเร็ว และมีประสิทธิภาพทั้งในประเทศและต่างประเทศ

ข้อเสนอแนะเพิ่มเติม

- หน่วยงานที่เกี่ยวข้องควรให้ความสำคัญกับการพิสูจน์หลักฐานทางดิจิทัลหรือทางไซเบอร์ (Digital Forensics/Cyber Forensics) เป็นกรณีเร่งด่วนสำหรับการพัฒนาศักยภาพบุคลากรด้านไซเบอร์ เนื่องจากปัจจุบันประเทศไทยยังขาดแคลนบุคลากรด้านนี้ที่ต้องอาศัยความรู้ความเชี่ยวชาญเฉพาะด้านในการปฏิบัติงาน จึงทำให้การบังคับใช้กฎหมายเพื่อป้องกันและแก้ไขปัญหาดังกล่าวไม่มีประสิทธิภาพ
- ควรมีการพัฒนาฐานข้อมูลเกี่ยวกับการกระทำความผิดบนดาร์กเว็บเพื่อเป็นข้อมูลในการจัดทำแนวทางหรือมาตรการการแก้ไขปัญหาอาชญากรรมที่เกิดขึ้นบนไซเบอร์สเปซ ในโอกาสต่อไป

สำนักยุทธศาสตร์ความมั่นคงเกี่ยวกับภัยคุกคามข้ามชาติ
สำนักงานสภาความมั่นคงแห่งชาติ
๒๘ ตุลาคม ๒๕๖๒