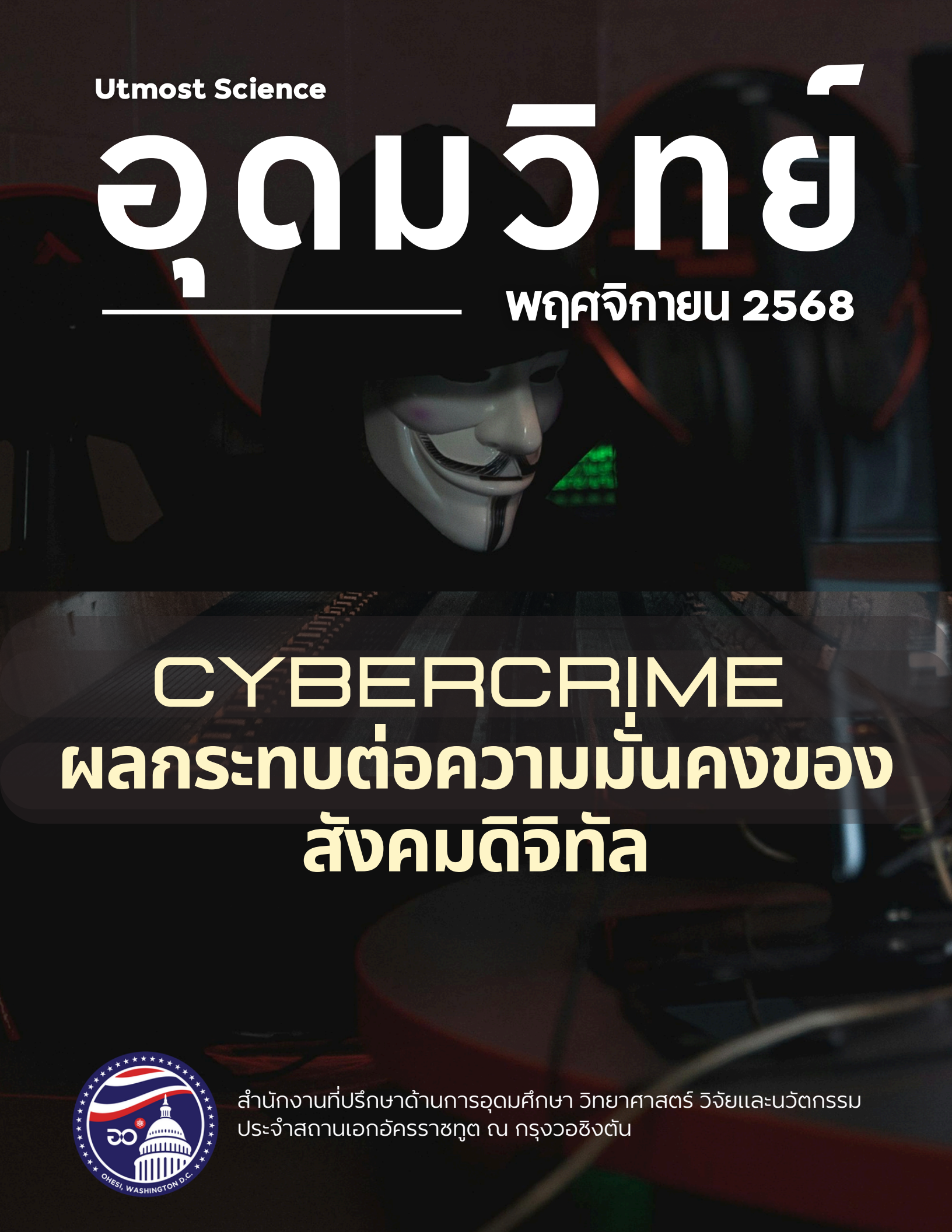
Utmost Science

อุดมวิทย์

พฤศจิกายน 2568



CYBERCRIME
ผลกระทบต่อความมั่นคงของสังคมดิจิทัล

สำนักงานที่ปรึกษาด้านการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ประจำสถานเอกอัครราชทูต ณ กรุงวอชิงตัน

วารสารอุดมวิทย์ | Utmost Sciences
เดือนพฤศจิกายน 2568 ฉบับที่ 11/2568

บรรณาธิการบริหาร:

นายฐิติเดช ตุลารักษ์
อัครราชทูตที่ปรึกษา (ฝ่ายการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม) ประจำกรุงวอชิงตัน

กองบรรณาธิการ:

ดร. ศิริพร เต่าแก้ว
นางสาวอุไรริน ขอบุญ
นายอิศรา ปทุมานนท์

จัดทำโดย

สำนักงานที่ปรึกษาด้านการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ประจำสถานเอกอัครราชทูต ณ กรุงวอชิงตัน
1024 Wisconsin Ave., N.W. Suite 104
Washington, D.C. 20007

ติดต่อคณะผู้จัดทำได้ที่
Phone: +1 (202) 944 5200
Email: ost@thaiembdc.org
Website: www.ohesdc.org
Facebook: www.facebook.com/ohesdc

คำนำ

สวัสดีท่านผู้อ่านที่เคารพ วารสารอุดมวิทย์ฉบับนี้เดือนพฤศจิกายนนี้ เราจะขอนำเรื่องที่กำลังเป็นประเด็นและปัญหาสำคัญที่สังคมโลกต้องเผชิญในปัจจุบันนี้ นั่นก็คือปัญหาที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ ในยุคที่เทคโนโลยีดิจิทัลมีบทบาทและกลายมาเป็นโครงสร้างพื้นฐานสำคัญของเศรษฐกิจ สังคม และความมั่นคงของประเทศ อาชญากรรมไซเบอร์ได้มีการพัฒนาและขยายขอบเขตอย่างรวดเร็ว ควบคู่ไปกับความก้าวหน้าทางเทคโนโลยี อาชญากรได้มีการโจมตีระบบสารสนเทศ การขโมยข้อมูลส่วนตัว ไปจนถึงการก่อกวนโครงสร้างพื้นฐานสำคัญของภาครัฐและภาคเอกชน ซึ่งไม่เพียงแต่สร้างความเสียหายทางเศรษฐกิจมูลค่ามหาศาล แต่ยังบั่นทอนความเชื่อมั่นของประชาชนต่อระบบดิจิทัล และส่งผลกระทบต่อเสถียรภาพและความมั่นคงของประเทศในระยะยาว บทความในวารสารอุดมวิทย์ฉบับนี้จึงขอนำเสนอภาพรวมของอาชญากรรมทางไซเบอร์ ตัวอย่างเหตุการณ์ที่เกิดขึ้น สถิติมูลค่าความเสียหาย และหน่วยงานรัฐบาลสหรัฐอเมริกาที่เกี่ยวข้องในการปราบปรามอาชญากรรมไซเบอร์นี้ ตลอดจนความร่วมมือระหว่างภาครัฐ เอกชน และนานาชาติ ในการรับมือภัยคุกคามดังกล่าว เพื่อเป็นความรู้และแนวคิดสำหรับการกำหนดทิศทางการพัฒนานโยบายและการป้องกันด้านไซเบอร์ของประเทศอย่างยั่งยืนในอนาคต

ทีมบรรณาธิการ
สำนักงานที่ปรึกษาด้านการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ประจำสถานเอกอัครราชทูต ณ กรุงวอชิงตัน

สารบัญ

06.....What is Cybercrime ?

09.....ภาพรวมอาชญากรรมไซเบอร์

10.....ตัวอย่างเหตุการณ์สำคัญที่เกิดขึ้นด้านภัยคุกคามทางไซเบอร์

14.....หน่วยงานที่เกี่ยวข้องกับด้านอาชญากรรมไซเบอร์

20.....การบังคับใช้กฎหมายในการป้องกันภัยคุกคามทางไซเบอร์

24.....สถิติองค์กรที่ถูกโจมตีทางไซเบอร์ทั่วโลกระหว่างปี 2021-2025

25.....การแก้ปัญหา

27.....ตัวอย่างสถานการณ์ด้านอาชญากรรมไซเบอร์ในปัจจุบัน

28.....ความร่วมมือในการกวาดล้างสแกมเมอร์ของสหรัฐอเมริกา

30.....ผลกระทบของอาชญากรรมไซเบอร์

What is Cybercrime ?

อาชญากรรมทางไซเบอร์ คือการกระทำที่ผิดกฎหมายทุกรูปแบบผ่านการใช้อุปกรณ์คอมพิวเตอร์หรืออินเทอร์เน็ต เพื่อก่อให้เกิดความเสียหายต่อบุคคล องค์กร หรือชาติ ในยุคที่อินเทอร์เน็ตเข้ามามีบทบาทสำคัญในการเปลี่ยนแปลงเศรษฐกิจและรูปแบบการดำเนินธุรกิจทั่วโลก ตลอดจนเป็นส่วนหนึ่งของการดำรงชีวิตประจำวัน การพึ่งพาบริการออนไลน์และอุปกรณ์ดิจิทัลที่เพิ่มขึ้นอย่างต่อเนื่องได้เปิดโอกาสให้อาชญากรไซเบอร์สามารถเข้าถึงข้อมูลส่วนตัวจำนวนมหาศาล และสามารถนำข้อมูลที่ sensitive เหล่านี้ไปใช้เพื่อผลประโยชน์ส่วนตนหรือใช้ในวัตถุประสงค์ที่ผิดกฎหมาย ซึ่งเป็นภัยคุกคามแก่ประชาชน องค์กร และรัฐบาล ประเด็นปัญหาด้านอาชญากรรมทางไซเบอร์ได้ขยายขอบเขตไปทั่วโลก และสร้างมูลค่าความเสียหายในแต่ละปีเทียบเท่ากับผลิตภัณฑ์มวลรวมภายในประเทศของประเทศเศรษฐกิจขนาดใหญ่ เช่น สหรัฐอเมริกา ผู้ก่อภัยคุกคามทางไซเบอร์สามารถสร้างรายได้มหาศาลในแต่ละปี จนกลายเป็นหนึ่งในรูปแบบอาชญากรรมที่ทำเงินและกำไรได้มากที่สุดในโลก การโจมตีทางไซเบอร์ไม่ได้มีเป้าหมายเพื่อขโมยทรัพย์สินหรือเงินเพียงอย่างเดียว แต่อาจมุ่งทำลายระบบควบคุมข้อมูล หรือปิดกั้นการให้บริการเทคโนโลยี ไปจนถึงการก่อสงครามข้อมูลหรือการก่อการร้ายทางไซเบอร์

อาชญากรทางไซเบอร์อาจเป็นบุคคลที่กระทำผิดเพียงลำพัง หรือกลุ่มอาชญากรรมที่จัดตั้งอย่างเป็นระบบ อาจเกี่ยวข้องกับผู้ก่อภัยคุกคามที่ร่วมมือกันจากหลายประเทศโดยใช้โครงสร้างพื้นฐานทางเทคโนโลยีที่กระจายอยู่ในหลายอาณาเขต หรือแม้แต่หน่วยงานที่ได้รับการสนับสนุนจากรัฐ ซึ่งกลุ่มอาชญากรนี้ได้ใช้เทคโนโลยีเพื่อแสวงหาผลประโยชน์ โดยอาศัยความไม่เปิดเผยตัวตนของโลกออนไลน์และการใช้สกุลเงินดิจิทัลเป็นเครื่องมือในการก่อภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของชาติ ความปลอดภัยสาธารณะและเสถียรภาพทางเศรษฐกิจโลกจากรายงานของสำนักงานสอบสวนกลางสหรัฐฯ (Federal Bureau of Investigation) ประเมินมูลค่าความเสียหายที่เกิดขึ้นจากอาชญากรรมทางไซเบอร์ในปี 2020 เพียงปีเดียว มีมูลค่าความเสียหายมากกว่า 4 พันล้านเหรียญสหรัฐฯ ซึ่งภาคส่วนสำคัญหลายด้านโดยเฉพาะผู้ให้บริการด้านสุขภาพได้รับผลกระทบจากการโจมตีด้วย ransomware อย่างต่อเนื่องจนทำให้ระบบล่มในช่วงการแพร่ระบาดครั้งใหญ่ของ COVID-19 อาชญากรได้อาศัยช่องโหว่ทางเทคโนโลยีประกอบกับการที่ผู้ใช้งานจำนวนมากยังขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ จึงทำให้สามารถแสวงหาผลประโยชน์ได้จากการโจรกรรมทางไซเบอร์ซึ่งมีความเสี่ยงต่ำแต่ผลตอบแทนสูง อีกทั้งกฎระเบียบด้านความปลอดภัยทางไซเบอร์ยังไม่เพียงพอและการบังคับใช้กฎหมายที่อ่อนแอในหลายประเทศส่งผลให้อาชญากรรมไซเบอร์ขยายตัวอย่างรวดเร็ว

ที่มา: What is Cybercrime: https://www.ice.gov/about-ice/hsi/investigate/cybercrime
https://www.state.gov/cybercrime

คำศัพท์ที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์

Phishing - คือการโจรกรรมข้อมูลส่วนตัวผ่านการสื่อสาร เช่น การปลอมแปลงอีเมลส่วนตัว การหลอกเป็นบุคคลต่างๆ เพื่อหลอกขอข้อมูลส่วนตัว หรือลิงก์อันตรายให้ผู้เสียหายกดเข้าไปเพื่อกรอกข้อมูลส่วนตัว เช่น บัญชีธนาคาร หรือบัตรเครดิต โดยข้อมูลที่ได้เหล่านี้จะถูกนำไปใช้ทำธุรกรรมทางเงินโดยที่เจ้าของบัญชีไม่ได้รับความยินยอม ไปจนถึงการนำข้อมูลส่วนตัวไปขายต่อให้แก่ผู้ไม่ประสงค์ดีอื่นๆ

Ransomware – หรือการเรียกค่าไถ่ของอาชญากรไซเบอร์ โดยการล็อคระบบคอมพิวเตอร์และไฟล์สำคัญ โดยผู้เสียหายจะต้องจ่ายเงินเรียกค่าไถ่ตามจำนวนเงินที่อาชญากรกำหนด ซึ่งส่วนมากจะเป็นการจ่ายผ่านสกุลเงินดิจิทัล เพื่อแลกกับการเข้าใช้งานคอมพิวเตอร์และเข้าถึงไฟล์อีกครั้ง

Malware – หรือ Malicious Software คือเหล่าโปรแกรมคอมพิวเตอร์ที่ถูกสร้างขึ้นเพื่อแอบเข้าสู่ระบบคอมพิวเตอร์และเครือข่ายโดยที่ผู้ใช้งานไม่ได้อนุญาต ไม่ว่าจะเป็น Virus, Worms Trojan หรือ Spyware เป็นต้น

Spyware – เป็นซอฟต์แวร์ที่ติดตั้งมากับอุปกรณ์โดยที่ผู้ใช้งานไม่รับรู้ โดย Spyware จะเข้ามาขโมยข้อมูลส่วนตัวหรือข้อมูลลับผ่านการใช้งานบนโลกอินเทอร์เน็ต Spyware ยังสามารถเปลี่ยนการตั้งค่าคอมพิวเตอร์เป้าหมายได้โดยที่ผู้ใช้งานไม่รู้ตัว เช่น แอบเปิด GPS หรือกล้องบันทึกภาพ เป็นต้น

Virus – มักแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์ ซึ่งสามารถแพร่กระจายไปยังเครือข่ายอื่นๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว และจะทำงานก็ต่อเมื่อมีการเปิดใช้งานโปรแกรมหรือเปิดไฟล์เท่านั้น

Worms - โปรแกรมที่หลอกล่อผู้ใช้งานว่ามีความปลอดภัย แต่ในความเป็นจริงแล้วสามารถสร้างความเสียหายให้แก่ผู้ใช้งานเป็นอย่างมากหากมีการติดตั้งในเครื่องคอมพิวเตอร์ ซึ่งสามารถแพร่กระจายได้อัตโนมัติผ่านระบบคอมพิวเตอร์โดยที่ผู้ใช้งานไม่รู้ตัว และมักแทรกตัวเข้ามาพร้อมกันในปริมาณมากและส่งผลให้ระบบเครือข่ายถูกปิดกั้น

Trojan – เป็นมัลแวร์ในรูปแบบที่สามรถติดตั้งได้เองอัตโนมัติในเครื่องคอมพิวเตอร์นั้นๆ โดย Trojan มักแฝงมาพร้อมกับซอฟต์แวร์หรือไฟล์ที่ผู้ใช้งานตั้งใจดาวน์โหลดหรือติดตั้ง เช่น การดาวน์โหลดภาพยนต์หรือซอฟต์แวร์ทางอินเทอร์เน็ต ซอฟต์แวร์ผิดกฎหมายหรือไฟล์ที่แนบมากับอีเมล ซึ่งแฮ็กเกอร์จะใช้โปรแกรมดังกล่าวเข้าควบคุมเครื่องคอมพิวเตอร์ผ่านระบบทางไกลและสามรถขโมยข้อมูลสำคัญจากไฟล์ในเครื่องคอมพิวเตอร์นั้นๆ ได้

Botnet – คืออุปกรณ์ที่ติด Malware และถูกเปลี่ยนเป็น Bot ที่ย่อมาจาก Robot ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ Router หรือ IoT (Internet of Things) เพื่อรอรับคำสั่งจาก Hacker โดยแฮ็กเกอร์จะนำ Botnet ที่มีไปใช้ในการโจมตีทางไซเบอร์ เช่น DDoS เป็นต้น

Distributed Denial of Service (DDoS) – เป็นรูปแบบหนึ่งของการโจมตีทางไซเบอร์ที่มีเป้าหมายเพื่อทำให้ระบบคอมพิวเตอร์ เซิร์ฟเวอร์ หรือเว็บไซต์ไม่สามารถเข้าใช้งานได้ โดยใช้ Botnet โจมตีไปยังเป้าหมายพร้อมๆกัน เพื่อให้เครื่องเซิร์ฟเวอร์หรือเว็บไซต์ปลายทางล่มและไม่สามารถให้บริการผู้ใช้งานได้

Two -Factor Authentication – การยืนยันตัวตนแบบสองชั้นเวลา Login เข้าบัญชีผู้ใช้งานต่างๆ ซึ่งสามารถใช้ได้ทั้งอีเมล โทรศัพท์มือถือ หรือธุรกรรมออนไลน์ต่าง ๆ เพื่อป้องกันการถูกปลอมแปลงตัวตน หรือแฮคบัญชีผู้ใช้งาน โดยระบบจะส่งแจ้งเตือนไปยังอีเมล หรือแอปพลิเคชันที่ผู้ใช้ตั้งค่าผูกบัญชีไว้ในการกดยืนยันการ Login หรือใส่รหัส PIN เพื่อยืนยันตัวตนอีกชั้นหนึ่ง ระบบนี้จะเพิ่มความปลอดภัยให้กับบัญชีผู้ใช้หรืออุปกรณ์ต่างๆที่เปิดใช้งาน

ที่มา: Cybersecurity terms https://www.it.chula.ac.th https://www.gwscloud.com/th

ภาพรวมอาชญากรรมไซเบอร์
Cybercrime History Overview

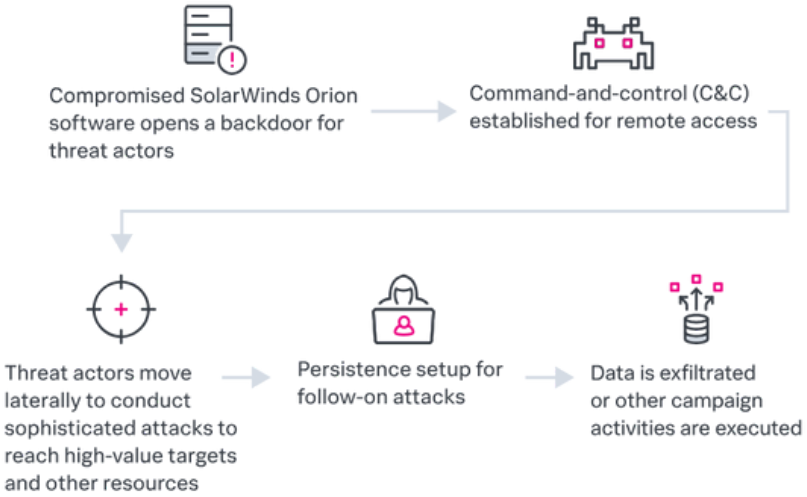
อาชญากรรมไซเบอร์เกิดขึ้นควบคู่กับการถือกำเนิดของอินเทอร์เน็ต และได้พัฒนาอย่างรวดเร็วตามความก้าวหน้าของเทคโนโลยีสารสนเทศ พัฒนาการของภัยคุกคามทางไซเบอร์ในแต่ละยุคมีดังนี้

ยุคเริ่มแรก (ทศวรรษ 1970-1980) ภัยคุกคามทางไซเบอร์ส่วนใหญ่จะอยู่ในรูปแบบของไวรัสและเวิร์ม (Worms) ที่ถูกพัฒนาขึ้นเพื่อการทดลองทางเทคนิคมากกว่าการทำลายล้าง แต่ก็ถือเป็นจุดกำเนิดของความเสี่ยงด้านไซเบอร์บนโลกดิจิทัล

การเพิ่มขึ้นของมัลแวร์ (ทศวรรษ 1990) เมื่อคอมพิวเตอร์ส่วนบุคคลได้มีการนำมาใช้มากขึ้น การโจมตีผ่านไวรัส (Virus) โทรจัน (Trojan) และ อีเมลเวิร์ม (Email worms) เริ่มแพร่กระจายผ่านไฟล์แนบทางอีเมลและฟล็อปปี้ดิสก์ ทำให้ภัยไซเบอร์เริ่มส่งผลกระทบต่อผู้ใช้งานทั่วไปในวงกว้าง

การโจมตีเพื่อผลประโยชน์ทางการเงิน (ทศวรรษ 2000) ในช่วงนี้อาชญากรไซเบอร์เริ่มมุ่งหวังผลประโยชน์ทางการเงินจากการโจรกรรมทางไซเบอร์อย่างจริงจัง โดยเริ่มมีการแพร่ระจายของสปายแวร์ (Spyware) ฟิชชิ่ง (Phishing) และ social engineering campaigns รวมถึงการสร้าง botnets ในการโจมตีโดยการปฏิเสธการให้บริการแบบกระจาย (Distributed Denial-of-Service: DDoS)

ภัยคุกคามสมัยใหม่ (ช่วงปี 2020 เป็นต้นมา) อาชญากรรมไซเบอร์ในยุคปัจจุบันมีช่องทางในการเข้าถึงการโจมตีได้ง่ายขึ้น เช่น รูปแบบบริการ Ransomware-as-a-Service (RaaS) และเทคโนโลยี AI ยังถูกนำมาใช้สร้าง Deepfake เพื่อใช้หลอกลวง โจมตี เช่น เหตุการณ์ SolarWinds และการโจมตีระบบโครงสร้างพื้นฐานสำคัญ เช่น ระบบสาธารณสุข ซึ่งล้วนสะท้อนให้เห็นถึงความซับซ้อนและผลกระทบลึกซึ้งของภัยคุกคามไซเบอร์ยุคใหม่



ตัวอย่างเหตุการณ์สำคัญที่เกิดขึ้นด้านภัยคุกคามทางไซเบอร์

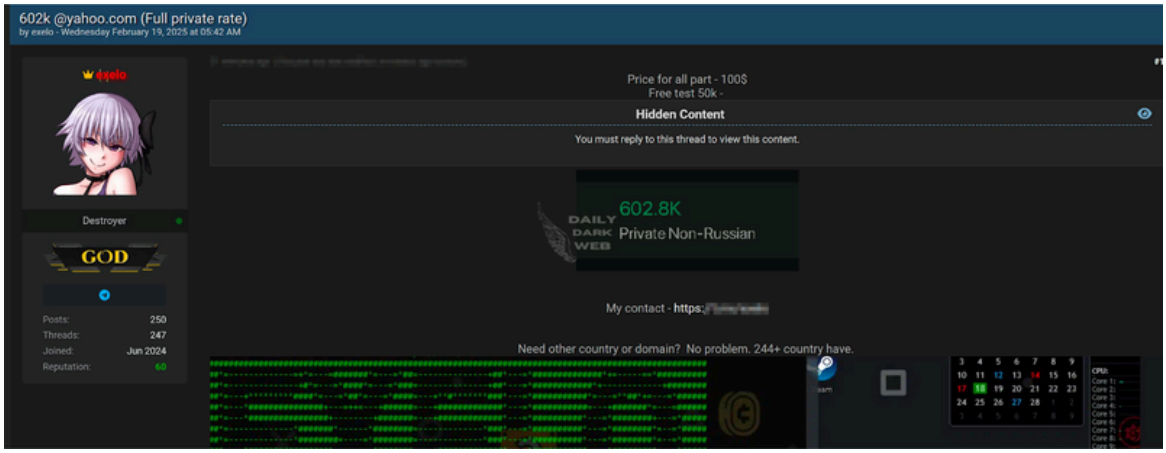
1. เหตุการณ์ WannaCry (2017)

ในเดือนพฤษภาคม 2017 เหตุการณ์การโจมตีครั้งใหญ่ที่สุดในประวัติศาสตร์ไซเบอร์ และส่งผลกระทบต่อผู้ใช้งานและองค์กรทั่วโลกภายในเวลาไม่กี่ชั่วโมง WannaCry เป็น ransomware ที่แพร่ระบาดเข้าโจมตีเครือข่ายคอมพิวเตอร์ต่างๆ ทั่วโลก เพื่อเรียกค่าไถ่ในการปลดล็อกข้อมูลเป็นเงินบิตคอยน์ ransomware นี้โจมตีพร้อมกัน 28 ภาษาในกว่า 99 ประเทศทั่วโลก โดยกลุ่มแฮ็กเกอร์ที่ใช้ชื่อว่า Shadow Brokers ที่ใช้ช่องโหว่ในระบบปฏิบัติการ Windows ที่ชื่อว่า EternalBlue โดยคาดว่าช่องโหว่นี้พัฒนาโดยหน่วยข่าวกรองสหรัฐฯ (National Security Agency: NSA) และถูกกลุ่มแฮ็กเกอร์นำข้อมูลมาเปิดเผยแพร่ต่อสาธารณะ บริษัท Microsoft ได้ออกแบบระบบรักษาความปลอดภัยอย่างเร่งด่วนเพื่อแก้ไขช่องโหว่ที่ EternalBlue นำไปใช้ในทางที่ผิด แต่หลายองค์กรยังคงไม่ดำเนินการอัปเดตระบบที่สำคัญนี้โดยทันที ภายในไม่กี่วัน WannaCry โจมตีระบบคอมพิวเตอร์กว่า 200,000 เครื่องใน 150 ประเทศ ซึ่งสร้างความเสียหายให้แก่องค์กรสำคัญ อย่าง ระบบสาธารณสุขอังกฤษ (UK National Health Services: NHS) ต้องหยุดชะงัก การนัดหมายแพทย์ถูกยกเลิกหลายพันครั้ง และขั้นตอนการแพทย์ล่าช้าออกไป ซึ่งประเมินว่าได้สร้างความเสียหายกว่า 4 พันล้านเหรียญสหรัฐฯถึง 8 พันล้านเหรียญสหรัฐฯ เหตุการณ์นี้ทำให้ทั่วโลกตระหนักถึงอันตรายของการละเลยการอัปเดตระบบความปลอดภัยเป็นอย่างมาก อีกทั้งยังได้เน้นย้ำถึงความสำคัญของการสำรองข้อมูลระบบอย่างสม่ำเสมอ การป้องกันอุปกรณ์ปลายทางที่แข็งแกร่ง และการฝึกอบรมพนักงานให้มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญของความปลอดภัยด้านไซเบอร์

รูปตัวอย่างแสดงมัลแวร์เรียกค่าไถ่ WannaCry

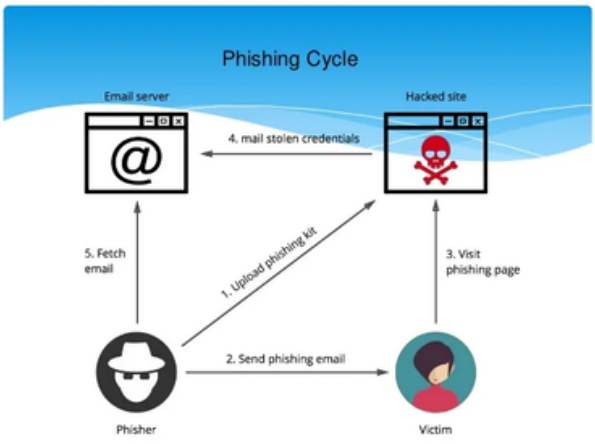
2. Yahoo (2014)

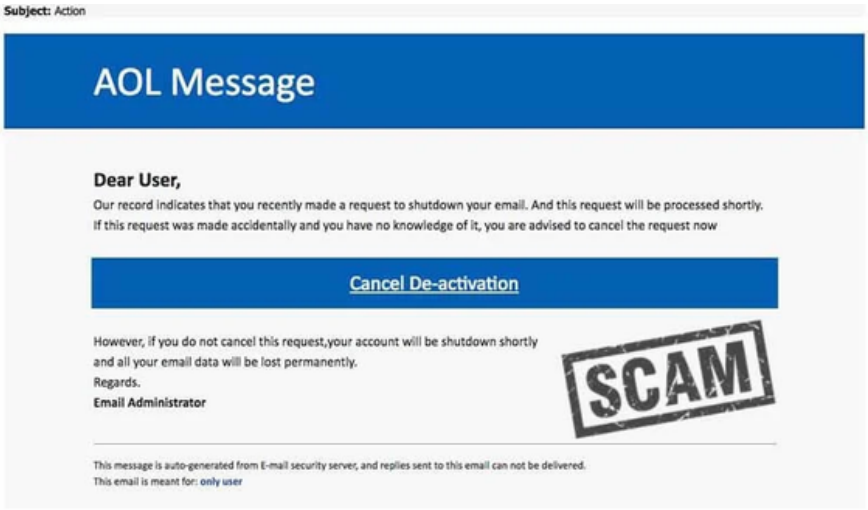
ในปี 2014 เกิดเหตุการณ์การละเมิดข้อมูลครั้งใหญ่ของบริษัท Yahoo ส่งผลให้ข้อมูลของผู้ใช้งานกว่า 500 ล้านบัญชีถูกเผยแพร่ต่อสาธารณะ แม้ว่าบริษัทจะไม่มีการออกมาชี้แจงถึงเหตุการณ์ดังกล่าวจนกระทั่งผ่านไปเป็นระยะเวลาสองปี และก่อนหน้านี้ในปี 2013 บริษัท Yahoo ยังเคยถูกละเมิดข้อมูลผู้ใช้ ซึ่งส่งผลกระทบต่อผู้ใช้ถึง 3 พันล้านบัญชี ทำให้เหตุการณ์ทั้งสองครั้งรวมกันกลายเป็นการละเมิดข้อมูลครั้งใหญ่ที่สุดในประวัติศาสตร์ โดยอาชญากรไซเบอร์ได้ใช้เทคนิค spear-phishing และเทคนิคอื่นๆ ในการเจาะเข้าสู่ระบบ Yahoo และเข้าถึงข้อมูลผู้ใช้งานกว่า 500 ล้านราย ซึ่งรวมถึงชื่อ ที่อยู่อีเมล รหัสผ่านที่ตั้งโดยอัลกอริทึมที่อ่อนแอ วันเกิด หมายเลขโทรศัพท์ ตลอดจนคำถาม-คำตอบเพื่อความปลอดภัย ภายหลังจากเหตุการณ์ที่เกิดขึ้น ผู้ใช้ถูกแนะนำให้รีเซ็ตรหัสผ่าน ตั้งค่าการยืนยันตัวตนแบบหลายปัจจัยและคอยตรวจสอบความเคลื่อนไหวของบัญชีอยู่เสมอ อย่างไรก็ตาม เหตุการณ์ที่เกิดขึ้นนี้ส่งผลต่อภาพลักษณ์และความเชื่อมั่นของผู้ใช้งาน รวมถึงบริษัทได้ถูกวิจารณ์อย่างหนัก เนื่องจากการไม่เปิดเผยเหตุการณ์ที่เกิดขึ้นทันที ส่งผลให้มีกระแสเรียกร้องให้มีกฎหมายการแจ้งเหตุละเมิดข้อมูลที่เข้มงวดมากขึ้น บริษัท Yahoo ได้เผชิญกับคดีความ และต้องจ่ายค่าชดเชยแก่ผู้ใช้งานเป็นจำนวนเงินหลายร้อยล้านเหรียญสหรัฐฯ และกิจการได้ถูกขายต่อให้บริษัท Verizon ในปี 2017 เหตุการณ์นี้ตอกย้ำความจำเป็นของกฎหมายคุ้มครองข้อมูลที่ครอบคลุม เช่น General Data Protection Regulation (GDPR) เพื่อเพิ่มความรับผิดชอบขององค์กรและเสริมการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้ในระยะยาว



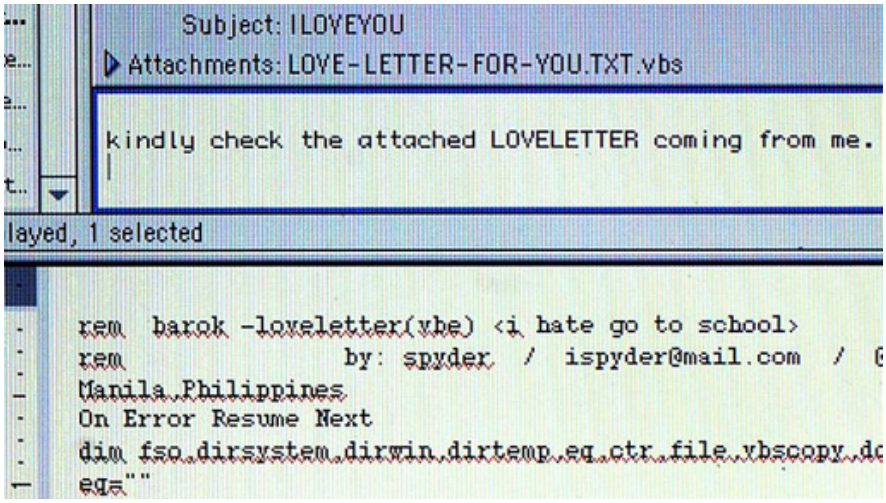
Post on the dark web forum (Source: Dark web intelligence)

3. **AOHell** เป็นโปรแกรมที่ถูกคิดค้นโดยกลุ่มแฮ็กเกอร์ ที่เชื่อว่าเป็นกลุ่มวัยรุ่นจากรัฐ Pennsylvania และนำมาใช้ในการโจมตีทางไซเบอร์แบบฟิชชิง (phishing) ครั้งแรกในปี 1994 AOHell ถูกพัฒนาขึ้นเพื่อเจาะช่องโหว่ของบริการ America Online (AOL) โดยกลุ่มแฮ็กเกอร์สามารถปลอมแปลงข้อความในห้องสนทนา ดาวน์โหลดไฟล์สำคัญ หรือสร้างบัญชีปลอมได้อย่างง่ายดาย การโจมตีในยุคแรกนี้เป็นจุดเปลี่ยนสำคัญของการโจมตีแบบวิศวกรรมสังคม หรือ Social Engineering เพราะแฮ็กเกอร์เลือกวิธีใช้การหลอกล่อผู้เสียหายให้เปิดเผยข้อมูลด้วยตัวเอง แทนการใช้วิธีทางเทคนิค เช่น ชื่อผู้ใช้ และรหัสผ่าน เป็นต้น phishing เป็นเทคนิคการหลอกลวงที่อาชญากรไซเบอร์เลือกใช้ ซึ่งในปัจจุบัน phishing ได้ถูกพัฒนาให้มีความซับซ้อนมากยิ่งขึ้น ไม่ว่าจะเป็นการหลอกให้ผู้ใช้คลิกลิงก์ปลอม ดาวน์โหลดไฟล์แนบอันตราย หรือกรอกข้อมูลที่มีความละเอียดอ่อน เช่น รหัสผ่าน เลขบัตรเครดิต หรือข้อมูลที่เป็นความลับทางธุรกิจ เมื่อโจมตีได้แล้ว อาชญากรเหล่านี้จะนำข้อมูลที่ได้ไปใช้ในการเข้าถึงบัญชีทางการเงิน และทำธุรกรรมโดยไม่ได้รับอนุญาต ซึ่งสร้างความเสียหายเป็นอย่างมาก อีกทั้ง ในหลายกรณี การโจมตีแบบ phishing ยังเป็นช่องทางนำ malware หรือ ransomware เข้าสู่ข้อมูลความเป็นส่วนตัวของเหยื่อ ทำให้ข้อมูลสูญหาย ถูกล็อก หรือเกิดความเสียหายอย่างต่อเนื่อง ซึ่งอาชญากรไซเบอร์เลือกใช้วิธีดังกล่าวในการโจรกรรมข้อมูลผู้เสียหายเนื่องจากเข้าถึงข้อมูลส่วนบุคคล การเงิน และเข้าถึงระบบระดับองค์กรได้ง่าย ในปัจจุบัน phishing ได้ถูกพัฒนาให้มีความซับซ้อนยิ่งขึ้น ไม่ว่าจะเป็นการหลอกให้ผู้เสียหายใช้ลิงก์ปลอมในการดาวน์โหลดไฟล์แนบที่เป็นอันตราย หรือกรอกข้อมูลที่มีความละเอียดอ่อน ซึ่งเป็นสิ่งที่ทำให้อาชญากรสามารถเข้าถึงบัญชีทางการเงิน และทำธุรกรรมทางการเงินได้





ภาพจาก : www.mailjet.com



ภาพจาก : https://www.bbc.co.uk
และ Association for Computing Machinery - UP Diliman Student Chapter, Inc.

จาก AOL สู่ ILOVEYOU

แม้ว่าเหตุการณ์ AOL จะเป็นเพียงแค่จุดเริ่มต้นในการหลอกลวงทางไซเบอร์ ยังมีอีกหลายเหตุการณ์ที่เหล่าอาชญากรนำวิธีการ phishing มาใช้เป็นช่องทางในการโจมตีเหยื่อเพื่อโจรกรรมข้อมูลสำคัญ โดยมีสถิติแสดงว่าในปี 2022 ศูนย์ร้องเรียนอาชญากรรมทางอินเทอร์เน็ต หรือ Internet Crime Complaint Center (IC3) ของหน่วยงาน The Federal Bureau of Investigation (FBI) ระบุว่า phishing เป็นอาชญากรรมไซเบอร์อันดับหนึ่ง มีผู้ร้องเรียนมากกว่า 300,000 ราย หลังจากยุค AOL ไม่นานนั้น โลกก็ต้องเผชิญกับการโจมตีไซเบอร์แบบ phishing ครั้งใหญ่และส่งผลกระทบเป็นวงกว้างอีกครั้งหนึ่ง นั่นก็คือเหตุการณ์ ILOVEYOU หรือ “Love Bug” ซึ่งเป็นเหตุการณ์ที่เชื่อว่าหลายท่านอาจได้รับข่าวสารเกี่ยวกับการโจมตีนี้ โดยเหตุการณ์ ILOVEYOU นี้แพร่ระบาดไปยังอีเมลแก่ผู้ใช้งานทั่วโลกในเดือนพฤษภาคม ปี 2000 ผู้ใช้งานอินเทอร์เน็ตได้รับอีเมลหัวข้อ ILOVEYOU พร้อมข้อความเรียบง่ายว่า “กรุณาเปิดจดหมายรักที่แนบมาด้วย” และเมื่อผู้ใช้เปิดไฟล์ที่แนบมาในอีเมลนั้น เวิร์มก็จะสามารถแพร่กระจายเข้าเครื่อง ลบและเขียนทับไฟล์ต่างๆ ที่สำคัญ รวมถึงส่งตัวมันเองไปยังรายชื่อผู้ติดต่อทั้งหมดใน outlook ทำให้การแพร่กระจายรุนแรงและรวดเร็วอย่างไม่เคยมีมาก่อน ซึ่งภายหลังจากสองเหตุการณ์ที่เกิดขึ้น การก่ออาชญากรรมแบบ phishing ได้ถูกพัฒนาไปในรูปแบบต่างๆ และถูกนำมาใช้ในหลายเหตุการณ์สำคัญ เช่น FACC และเหตุการณ์ Colonial Pipeline เป็นต้น

ที่มา: The first phishing attack is launched on AOL

หน่วยงานที่เกี่ยวข้องกับด้านอาชญากรรมไซเบอร์

Federal Bureau of Investigation

Federal Bureau of Investigation (FBI) หรือ สำนักงานสอบสวนกลาง เป็นหน่วยงานของรัฐที่อยู่ภายใต้กระทรวงยุติธรรมของสหรัฐอเมริกา ก่อตั้งขึ้นเมื่อปีค.ศ. 1908 โดยมีชื่อเดิมว่า Bureau of Investigation และต่อมาในปี 1924 ได้มีการปรับปรุงหน่วยงานขึ้นใหม่ และเปลี่ยนชื่อเป็น Federal Bureau of Investigation ซึ่งใช้มาจนถึงในปัจจุบัน FBI ทำหน้าที่บังคับใช้กฎหมายรัฐบาลกลาง และสืบสวนคดีอาชญากรรมหลากหลายประเภท เช่น การละเมิดกฎหมายของรัฐบาลกลาง การก่อวินาศกรรม การก่อการร้าย การทุจริตในภาครัฐ การละเมิดสิทธิมนุษยชน อาชญากรรมร้ายแรงอื่นๆ รวมถึงอาชญากรรมไซเบอร์ เป็นต้น FBI มีการทำงานร่วมกับกองกำลังเฉพาะกิจหรือ Joint Task Force ในการติดตามคดีระดับประเทศ FBI ยังประกอบไปด้วยหน่วยงานและระบบทำงานที่สำคัญเช่น หน่วยรวบรวมรูปพรรณบุคคล (Identification Division) ระบบรายงานอาชญากรรม (Criminal Report System) ซึ่งเน้นการนำหลักวิทยาศาสตร์มาใช้ในการสืบสวนและหาพยานหลักฐาน อย่างไรก็ตาม FBI ยังจัดตั้งกองกำลังเฉพาะกิจด้านไซเบอร์ที่ทำหน้าที่กำกับดูแลภัยคุกคามที่เกิดขึ้นทางไซเบอร์ คือ กองกำลังร่วมสืบสวนทางไซเบอร์แห่งชาติ หรือ National Cyber Investigative Joint Task Force (NCIJTF) ทำหน้าที่เป็นศูนย์กลางในการประสานงานระหว่างหลายหน่วยงานของรัฐบาลสหรัฐฯ บูรณาการ และแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆ เพื่อสนับสนุนการสืบสวนคดีที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ อีกทั้งยังทำหน้าที่วิเคราะห์ข่าวกรองเชิงลึก และประสานงานปฏิบัติการเฉพาะทาง เพื่อระบุ ติดตาม และยับยั้งผู้ก่อการร้าย สายลับ และอาชญากรทางไซเบอร์ที่พยายามเข้าถึงข้อมูลหรือใช้ประโยชน์จากระบบสำคัญของประเทศ

NCIJTF ยังประกอบด้วยหน่วยงานพันธมิตรมากกว่า 30 แห่ง ครอบคลุมทั้งหน่วยงานบังคับใช้กฎหมาย หน่วยข่าวกรอง และกระทรวงกลาโหม โดยมีเจ้าหน้าที่ปฏิบัติงานประจำร่วมกันเพื่อขับเคลื่อนภารกิจในลักษณะ “รัฐบาลโดยรวม” ตลอดจนการทำงานอย่างใกล้ชิดกับพันธมิตรระหว่างประเทศและภาคเอกชน เพื่อป้องกันและรับมือกับภัยคุกคามไซเบอร์ทั้งภายในประเทศและจากต่างประเทศ ด้วยการประสานงาน การทำงานร่วมกัน และการแบ่งปันข้อมูลที่เกิดขึ้นภายใต้ NCIJTF หน่วยงานทั่วทั้งรัฐบาลสหรัฐฯ สามารถร่วมกันติดตาม จับกุม และนำอาชญากรไซเบอร์ออกจากเครือข่ายของประเทศได้อย่างมีประสิทธิผล ทั้งนี้ NCIJTF ยังมีการดำเนินงานภายใต้กรอบกฎหมายอย่างเคร่งครัด พร้อมยึดมั่นในการคุ้มครองสิทธิความเป็นส่วนตัวของพลเมืองอเมริกันตลอดกระบวนการสืบสวนและปฏิบัติการที่เกี่ยวข้อง

Internet Crime Complaint Center

Internet Crime Complaint Center (IC3) หรือศูนย์ร้องเรียนอาชญากรรมทางอินเทอร์เน็ตของหน่วยงาน FBI เป็นศูนย์กลางในการรับเรื่องร้องเรียนที่เกี่ยวข้องกับการฉ้อโกงที่เกิดขึ้นออนไลน์ ก่อตั้งขึ้นในปี 2000 เป็นความร่วมมือที่เกิดขึ้นระหว่าง FBI และ National White Collar Crime Center ซึ่งได้รับแจ้งเบาะแสและข้อร้องเรียนหลากหลายรูปแบบ ตั้งแต่การฉ้อโกงออนไลน์ คดีทรัพย์สินทางปัญญา การบุกรุกระบบคอมพิวเตอร์ การโจรกรรมทางเศรษฐกิจ การกรรโชกทรัพย์ทางออนไลน์ การฟอกเงินระหว่างประเทศ การขโมยข้อมูลส่วนบุคคล รวมถึงอาชญากรรมที่เกิดขึ้นทางอินเทอร์เน็ตที่มีความซับซ้อนที่เพิ่มขึ้นอย่างต่อเนื่อง โดยศูนย์ร้องเรียนอาชญากรรมนี้ได้เปลี่ยนชื่อจาก Internet Fraud Complaint Center (IFCC) มาเป็น Internet Crime Complaint Center (IC3) ในเดือนตุลาคม ปี 2003 เพื่อสะท้อนบทบาทใหม่ที่ครอบคลุมอาชญากรรมไซเบอร์ทุกประเภท และเพื่อลดความจำเป็นในการแยกแยะการฉ้อโกงทางอินเทอร์เน็ตออกจากอาชญากรรมไซเบอร์อื่นๆ ที่อาจซ้ำซ้อนกัน โดยผู้เสียหายสามารถส่งเรื่องร้องเรียนที่เกิดขึ้นด้านอาชญากรรมไซเบอร์ผ่านทาง portal ในเว็บไซต์ https://www.ic3.gov/ ซึ่งข้อมูลที่ได้จะถูกรวบรวมและนำไปให้หน่วยงาน FBI สืบสวนอาชญากรรมที่ได้รับรายงานมา รวมถึงติดตามแนวโน้มและภัยคุกคามที่อาจเกิดขึ้น และในบางกรณีอาจถึงขั้นอายัดเงินที่ถูกโจรกรรมผ่านทางไซเบอร์ได้ โดย IC3 จะทำงานและแบ่งปันข้อมูลผ่านเครือข่ายสำนักงานภาคสนามของ FBI และหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องในการติดตามและแก้ไขปัญหาอาชญากรรมไซเบอร์ที่เกิดขึ้นผ่านการร้องเรียนของประชาชน IC3 ยังได้มีการรายงานสถิติเกี่ยวกับข้อมูลอาชญากรรมไซเบอร์ที่ได้รับการร้องเรียนผ่านรายงานประจำปี โดยในปี 2024 จำนวนครั้งที่ได้รับการร้องเรียน (By Complaint Count) ทั้งสิ้น 850,532 ครั้ง มูลค่าความเสียหายกว่า 16.6 พันล้านเหรียญสหรัฐ เพิ่มขึ้นจากปี 2023 คิดเป็นร้อยละ 33

Cybersecurity and Infrastructure Security Agency

Cybersecurity and Infrastructure Security Agency (CISA) สำนักงานความมั่นคงทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐอเมริกา เป็นหน่วยงานภายใต้กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security: DHS) ทำหน้าที่เป็นหน่วยงานป้องกันภัยที่เกิดขึ้นด้านไซเบอร์และประสานงานระหว่างพันธมิตรเพื่อเสริมสร้างความมั่นคงปลอดภัย และความยืดหยุ่นของโครงสร้างพื้นฐานสำคัญของประเทศ โดยมีหน้าที่รับผิดชอบหลักในการปกป้องระบบไซเบอร์ของรัฐบาลกลาง และเป็นศูนย์ประเมินความเสี่ยง ให้คำแนะนำ และออกแนวทางสำหรับ 16 ภาคส่วนโครงสร้างพื้นฐานที่สำคัญ เช่น ภาคการสื่อสาร การเงิน พลังงาน และภาคการขนส่ง CISA ทำหน้าที่ตั้งแต่ออกคำสั่งด้านความมั่นคงไซเบอร์ให้กับหน่วยงานรัฐบาลกลาง เช่น แนวทางรักษาความมั่นคงของระบบคลาวด์ ไปจนถึงการเผยแพร่คำแนะนำด้านการปกป้องโครงสร้างพื้นฐานสำคัญจากภัยคุกคามทางไซเบอร์ นอกจากนี้ยังทำงานร่วมกับพันธมิตร ภาคเอกชน หรือหน่วยงานรัฐบาลอื่น เพื่อรับมือกับความเสี่ยงที่อาจเกิดขึ้น ซับซ้อนและขยายตัวอย่างรวดเร็วในยุคดิจิทัลนี้

CISA ยังมีบทบาทสำคัญในยุคปัญญาประดิษฐ์ โดยภายหลังจากคำสั่งฝ่ายบริหารของประธานาธิบดีโจ ไบเดนในปี 2023 CISA ได้ขยายขอบเขตความรับผิดชอบไปครอบคลุมด้านความมั่นคงและการกำกับดูแลความเสี่ยงของ AI ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญ โดยทำหน้าที่ประเมินและบรรเทาความเสี่ยงของ AI ที่อาจส่งผลกระทบต่อระบบที่ประเทศยังต้องพึ่งพา เช่น ระบบควบคุมอุตสาหกรรม การสื่อสาร หรือบริการฉุกเฉิน เป็นต้น นอกจากนี้ CISA ยังทำหน้าที่เป็นผู้นำด้านการจัดทำการประเมินความเสี่ยงปัญญาประดิษฐ์ประจำปีในทุกภาคส่วนโครงสร้างพื้นฐานสำคัญ รวมถึงสนับสนุนการพัฒนาแนวทางการใช้ AI อย่างปลอดภัย มีความรับผิดชอบ และโปร่งใส ผ่านความร่วมมือระหว่างภาคเอกชน ผู้กำหนดนโยบาย หน่วยงานรัฐบาลอื่นๆ และองค์กรระหว่างประเทศ

United State Secret Service

United State Secret Service (USSS) หน่วยสืบราชการลับสหรัฐฯ มีการจัดตั้งหน่วยปฏิบัติการเฉพาะกิจด้านอาชญากรรมไซเบอร์ที่ทำหน้าที่ติดตามและจับกุมอาชญากรไซเบอร์ระดับนานาชาติ ซึ่งเกี่ยวข้องกับการเจาะระบบ การฉ้อโกงทางธนาคาร การละเมิดข้อมูล และอาชญากรรมคอมพิวเตอร์รูปแบบต่างๆ โดยหน่วยข่าวกรองไซเบอร์ของ USSS นี้มีบทบาทสำคัญในการจับกุมผู้กระทำผิดที่ขโมยข้อมูลบัตรเครดิตหลายร้อยล้านรายการ ซึ่งสร้างความเสียหายกว่า 600 ล้านเหรียญสหรัฐฯ ต่อสถาบันการเงินและร้านค้าปลีกจำนวนมาก นอกจากนี้ USSS ยังดูแลสถาบันนิติวิทยาศาสตร์คอมพิวเตอร์แห่งชาติ หรือ National Computer Forensic Institute ซึ่งให้การฝึกอบรมด้านไซเบอร์แก่เจ้าหน้าที่ที่บังคับใช้กฎหมาย อัยการ และผู้พิพากษา เพื่อเสริมความสามารถในการรับมือกับอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ

Department of Justice

Department of Justice (DOJ) กระทรวงยุติธรรมแห่งสหรัฐฯ จัดตั้งแผนกอาชญากรรมคอมพิวเตอร์และทรัพย์สินทางปัญญา (Computer Crime and Intellectual Property Section : CCIPS) ให้ทำหน้าที่สืบสวนและดำเนินคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ เช่น การแฮ็ก การแพร่ไวรัสและเวิร์ม ตลอดจนคดีอาชญากรรมด้านทรัพย์สินทางปัญญา นอกจากนี้ CCIPS ยังทำหน้าที่ดูแลการดำเนินคดีที่เกี่ยวข้องกับการละเมิดความเป็นส่วนตัวโดยอาชญากรไซเบอร์ รวมถึงแฮ็กเกอร์ Cyber Stalker และผู้เผยแพร่สปายแวร์บนอุปกรณ์มือถือ ตลอดจนการค้นหา ยึด และวิเคราะห์หลักฐานดิจิทัลจากคอมพิวเตอร์และเครือข่าย

U.S. Immigration and Customs Enforcement

U.S. Immigration and Customs Enforcement (ICE) ศูนย์อาชญากรรมไซเบอร์ (C3) ของสำนักงานตรวจคนเข้าเมืองสหรัฐฯ (ICE) ภายใต้ฝ่ายสืบสวนความมั่นคงแห่งมาตุภูมิ (HIS) เป็นหน่วยงานด้านเทคนิคที่สนับสนุนการสืบสวนอาชญากรรมข้ามพรมแดน ทั้งในสหรัฐฯ และต่างประเทศ โดยศูนย์อาชญากรรมไซเบอร์ประกอบไปด้วย หน่วยอาชญากรรมไซเบอร์ หน่วยสืบสวนการแสวงประโยชน์จากเด็ก และหน่วยนิติวิทยาศาสตร์คอมพิวเตอร์ โดยให้บริการสนับสนุนทางเทคนิคและการฝึกอบรมแก่หน่วยงานบังคับใช้กฎหมายทุกระดับทั่วโลก

International Criminal Police Organization

International Criminal Police Organization (INTERPOL) องค์การตำรวจอาชญากรรมระหว่างประเทศ หรือที่รู้จักกันในนาม “ตำรวจสากล” เป็นองค์กรระหว่างรัฐบาล (Intergovernmental Organization) มีประเทศสมาชิกทั้งสิ้น 194 ประเทศ มีหน้าที่เพื่อช่วยเหลือตำรวจในประเทศสมาชิกให้สามารถทำงานร่วมกันโดยผ่านการแลกเปลี่ยนการเข้าถึงข้อมูลเกี่ยวกับอาชญากรรมต่างๆ รวมไปถึงการสนับสนุนทางเทคนิคและปฏิบัติการต่างๆ ที่เกี่ยวข้องกับประเด็นอาชญากรรมระหว่างประเทศ 3 ประเด็นหลัก ได้แก่ การต่อต้านการก่อการร้าย (Counter-Terrorism) องค์กรอาชญากรรม (Organized and Emerging Crime) และอาชญากรรมไซเบอร์ (Cybercrime)

ในปัจจุบัน อาชญากรรมทางไซเบอร์ได้ทวีความรุนแรงและซับซ้อนขึ้นจนกลายมาเป็นหนึ่งในภัยคุกคามข้ามชาติมากที่สุดในยุคดิจิทัล ปรากฏการณ์มัลแวร์ การโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (Distributed Denial-of-Service : DDoS) และแรนซัมแวร์ ที่ไม่เพียงแต่สร้างความเสียหายทางเทคนิคและเศรษฐกิจ แต่ยังเพิ่มความท้าทายให้กับหน่วยงานบังคับใช้กฎหมายทั่วโลก โดยต้องเผชิญทั้งปริมาณข้อมูลที่มหาศาล การสืบสวนที่ขยายข้ามเขตแดน และการพัฒนาเชิงเทคนิคที่ซับซ้อนอย่างต่อเนื่อง INTERPOL จึงเข้ามามีบทบาสำคัญในการพัฒนากลไกการสื่อสารที่ปลอดภัยและยืดหยุ่นซึ่งได้แก่ พื้นที่ทำงาน Cybercrime Knowledge Exchange (CKE) ซึ่งเป็นเวทีแลกเปลี่ยนองค์ความรู้ด้านอาชญากรรมไซเบอร์ที่ไม่ใช่ข้อมูลเชิงตำรวจ โดยเปิดให้หน่วยงานรัฐ องค์กรระหว่างประเทศ และผู้เชี่ยวชาญด้านความมั่นคงไซเบอร์ได้เข้ามาทำงานร่วมกันผ่านแพลตฟอร์ม Cybercrime Collaboration Platform - Operation ในการสนับสนุนหน่วยงานผู้บังคับใช้กฎหมายในการประสานงาน ปฏิบัติการ และแบ่งปันข้อมูลเชิงลึกด้านการสืบสวนอย่างมีประสิทธิผล

ที่มา:

National Cyber Investigative Joint Task Force

How can a task force like the NCIJTF help me fight Cybercrime?

FBI Cyber Division?

Cybersecurity and Infrastructure Security Agency (CISA)

Computer Crime and Intellectual Property Section (CCIPS)

Combatting Cybercrime

International Criminal Police Organization

ในปัจจุบัน หน่วยงานของรัฐบาลสหรัฐฯ อย่างน้อย 20 แห่ง มีบทบาทและความรับผิดชอบหลักในด้านการสืบสวน ติดตาม และการดำเนินคดีกับอาชญากรทางไซเบอร์ อย่างไรก็ตาม บทบาทเหล่านี้มักมีการทำงานที่ซ้ำซ้อนกัน กฎหมายและนโยบายของรัฐบาลกลางได้ระบุองค์ประกอบของบทบาทและความรับผิดชอบไว้แก่หน่วยงานนั้นๆ แต่ไม่ได้ชี้แนะแนวทางการประสานงานระหว่างหน่วยงานในกรณีที่เขตอำนาจทับซ้อน เช่น กระทรวงการต่างประเทศ (Department of State: DOS) เป็นผู้นำในการมีส่วนร่วมทางการทูตด้านไซเบอร์ แต่กระทรวงยุติธรรม (DOJ) และหน่วยงานอื่นๆ ก็พัฒนานโยบายไซเบอร์ระดับโลกและทำงานร่วมกับพันธมิตรต่างประเทศด้วยเช่นกัน การกำหนดบทบาทและความรับผิดชอบอย่างชัดเจนในการมีส่วนร่วมด้านไซเบอร์จึงมีความสำคัญเป็นอย่างมากในการสร้างประสิทธิภาพในการทำงานในแต่ละหน่วยงาน เจ้าหน้าที่บังคับใช้กฎหมายของรัฐบาลกลางจึงจำเป็นต้องพัฒนากรอบการทำงานที่ชัดเจนสำหรับการร่วมมือระหว่างภาคส่วนต่างๆ ที่เกี่ยวข้อง

การปรับปรุงการรายงานอาชญากรรมและการช่วยเหลือเหยื่อ

เพื่อยกระดับประสิทธิภาพในการรายงานอาชญากรรมและการช่วยเหลือเหยื่อ หน่วยงานที่เกี่ยวข้องในการดำเนินการด้านภัยคุกคามทางไซเบอร์จำเป็นต้องมีการจัดทำนโยบายและข้อเสนอทางกฎหมายที่ชัดเจนและครอบคลุม ซึ่งรวมถึงประเด็นสำคัญดังนี้ :

1. ปรับปรุงแนวปฏิบัติของอัยการสูงสุด 2012 ให้ครอบคลุมเหยื่ออาชญากรรมไซเบอร์อย่างชัดเจน นอกเหนือจากข้อมูลส่วนบุคคลที่ถูกขโมย

2. แก้ไขพระราชบัญญัติสิทธิเหยื่อและการชดใช้ความเสียหาย รวมถึงพระราชบัญญัติสิทธิเหยื่ออาชญากรรม เพื่อให้บุคคลที่เข้าข่ายนิยาม “เหยื่อ” และ “อันตราย” สามารถเข้าถึงสิทธิและความคุ้มครองต่ออาชญากรรมไซเบอร์ได้

3.ร่วมมือกับสำนักงานช่วยเหลือเหยื่ออาชญากรรมของ DOJ เพื่อเผยแพร่กฎเกณฑ์ที่ปรับปรุงใหม่ ซึ่งขยายสิทธิ์ของโครงการช่วยเหลือให้ครอบคลุมเหยื่ออาชญากรรมไซเบอร์ โดยระบุค่าใช้จ่ายที่อนุญาต เช่น การให้คำปรึกษาด้านกฎหมาย การสนับสนุนด้านสุขภาพจิต และบริการอื่นๆ ตามข้อกำหนดของสำนักงานช่วยเหลือเหยื่ออาชญากรรม

4.ประเมินความเป็นไปได้ในการจัดตั้งศูนย์รับสายโทรศัพท์แห่งชาติ สำหรับประชาชนและธุรกิจขนาดกลางและขนาดย่อม เพื่อรายงานอาชญากรรมไซเบอร์

5.ปรับปรุงกระบวนการแจ้งเหยื่ออาชญากรรมไซเบอร์ของ FBI ตามคำแนะนำของผู้ตรวจ DOJ เพื่อให้การสื่อสารกับเหยื่อมีประสิทธิภาพและชัดเจนมากขึ้น

6.ระบุความท้าทายในการรายงานต่อ IC3 และ Consumer Sentinel Network รวมถึงวิธีการที่หน่วยงานต่างๆ ติดต่อผู้รายงานกับอาชญากรรม และแนวทางแก้ไขข้อขัดแย้ง

7.สำรวจสถิติของอาชญากรรมไซเบอร์ ผ่านสำนักงานสถิติยุติธรรม โดยดำเนินการสำรวจทุกสองปี และอนุญาตให้เผยแพร่ผลการสำรวจโดยไม่ระบุชื่อ เพื่อสร้างฐานข้อมูลสำหรับการวางนโยบายและปรับปรุงมาตรการที่เกี่ยวข้อง

8.ปรับปรุงแนวปฏิบัติที่ดีที่สุดสำหรับการตอบสนองและรายงานเหตุการณ์ทางไซเบอร์ของ DOJ เพื่อให้หน่วยงานรัฐบาลสามารถช่วยเหลือผู้เสียหายได้ทันท่วงทีและชัดเจน

9.ส่งเสริมรัฐให้ขยายการชดเชยผู้เสียหายจากอาชญากรรมไซเบอร์ โดยเฉพาะรัฐที่ปัจจุบันจำกัดสิทธิ์เฉพาะผู้เสียหายจากอาชญากรรมรุนแรง

10.จัดทำแคมเปญสื่อสาธารณะ เพื่อให้ประชาชนรับทราบวิธีการรายงานอาชญากรรมไซเบอร์ สถานที่รายงาน และขั้นตอนที่เจ้าหน้าที่บังคับใช้กฎหมายดำเนินการ เพื่อสร้างความมั่นใจว่าเจ้าหน้าที่กำลังดำเนินการอย่างจริงจัง

ประเภทอาชญากรรมทางไซเบอร์ที่ได้รับการร้องเรียนสูงสุดได้แก่

2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441
*Descriptor***			
Cryptocurrency	149,686		

*IPR: Intellectual Property Rights

** This descriptor relates to the medium or tool used to facilitate the crime and used by IC3 for tracking purposes only. It is available as a descriptor only after a crime type has been selected.

Please see Appendix C for more information regarding IC3 data.

ที่มา: A Roadmap to Strengthen US Cyber Enforcement: Where Do We Go From Here?

มูลค่าความเสียหายที่เกิดขึ้นในปี 2024 (แบ่งตามประเภท)

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss	Crime Type	Loss
Investment	$6,570,639,864	Extortion	$143,185,736
Business Email Compromise	$2,770,151,146	Lottery/Sweepstakes/ Inheritance	$102,212,250
Tech Support	$1,464,755,976	Advanced Fee	$102,074,512
Personal Data Breach	$1,453,296,303	Phishing/Spoofing	$70,013,036
Non-Payment/Non-Delivery	$785,436,888	SIM Swap	$25,983,946
Confidence/Romance	$672,009,052	Overpayment	$21,452,521
Government Impersonation	$405,624,084	Ransomware *	$12,473,156
Data Breach	$364,855,818	Harassment/Stalking	$10,611,223
Other	$280,278,325	Botnet	$8,860,202
Employment	$264,223,271	IPR/Copyright and Counterfeit	$8,715,512
Credit Card/Check Fraud	$199,889,841	Threats of Violence	$1,842,186
Identity Theft	$174,354,745	Malware	$1,365,945
Real Estate	$173,586,820	Crimes Against Children	$519,424

*Descriptor***	
Cryptocurrency	$9,322,335,911

* Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by an entity. In some cases, entities do not report any loss amount to FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to FBI via IC3 and does not account for the entity directly reporting to FBI field offices/agents.

** This descriptor relates to the medium or tool used to facilitate the crime and is used by IC3 for tracking purposes only. It is available as a descriptor only after a crime type has been selected.

Please see Appendix C for more information regarding IC3 data.

การฉ้อโกงที่เกิดขึ้นทางไซเบอร์ ซึ่งรวมถึงการร้องเรียนที่อาชญากรใช้อินเทอร์เน็ตหรือเทคโนโลยีอื่นๆ กระทำการฉ้อโกง หลอกลวงซึ่งมักจะเกี่ยวข้องกับการขโมยเงิน ข้อมูลส่วนบุคคล การระบุตัวตน หรือเพื่อขายสินค้าและบริการปลอมแปลง รูปแบบการฉ้อโกงเหล่านี้ยังคงเป็นปัญหาหลักในโลกออนไลน์ โดยในปี 2024 การฉ้อโกงทางไซเบอร์คิดเป็นสัดส่วนเกือบร้อยละ 83 ของมูลค่าความเสียหายทั้งหมดที่ถูกรายงานต่อ IC3 ทำให้เห็นว่าปัญหาอาชญากรรมทางไซเบอร์ยังคงเกิดขึ้นและมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง

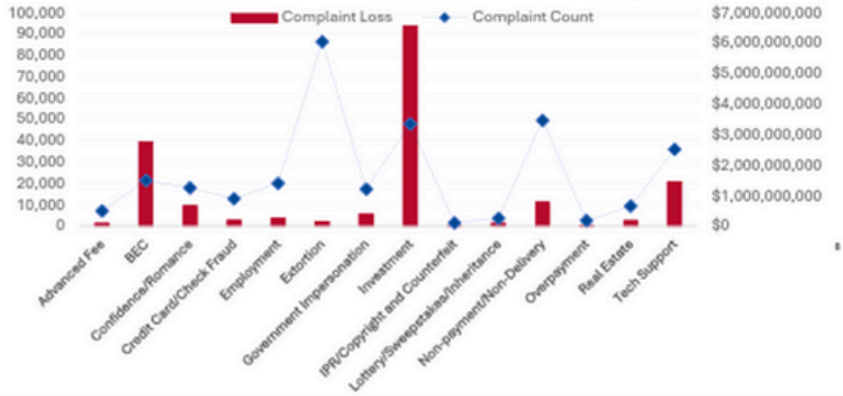
รูปภาพแสดงจำนวนครั้งในการร้องเรียน ประเภท และมูลค่าความเสียหายของอาชญากรรมทางไซเบอร์ปี 2024

CYBER-ENABLED FRAUD

Cyber-enabled fraud includes complaints where criminals use the Internet or other technology to commit fraudulent activities, often involving the theft of money, data, or identity, or the creation of counterfeit goods or services. Cyber-enabled fraud is responsible for almost 83% of all losses reported to IC3 in 2024. [7]

CYBER-ENABLED FRAUD in 2024

333,981 Complaints	$13.7 Billion Losses	38% of 2024 Complaints	83% of 2024 Losses



[8]

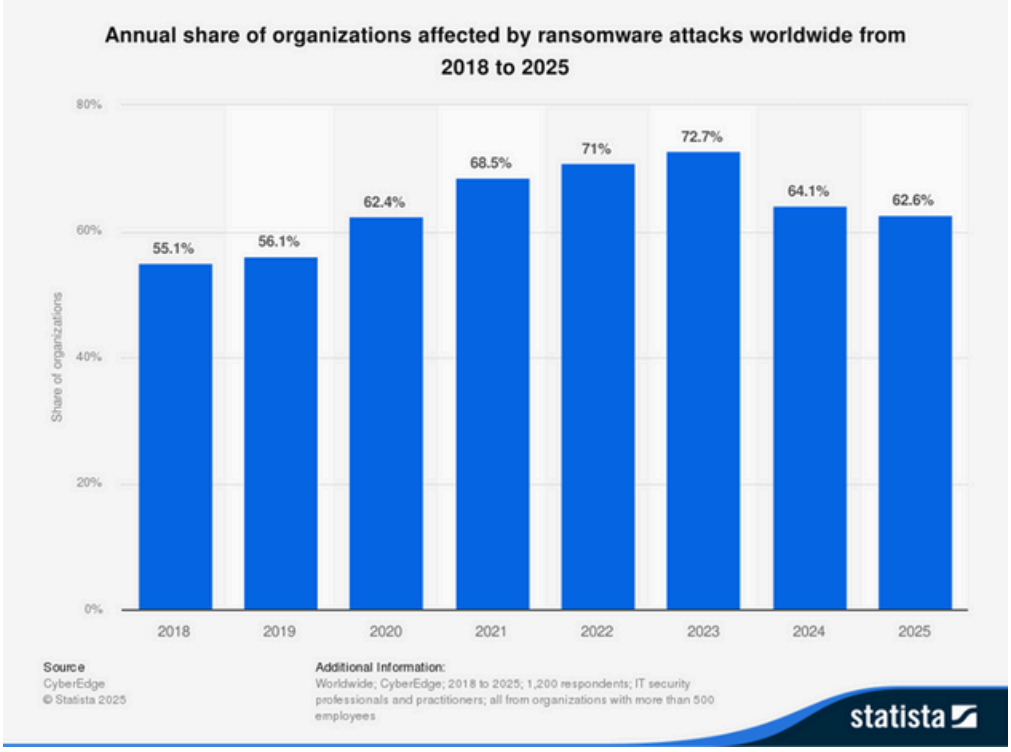
TRENDS

Call Center Scams	Emergency Scams
53,369 complaints; $1.9 billion in losses FBI Warns of Scammers Impersonating Cryptocurrency Exchanges Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash...	357 complaints; $2.7 million in losses FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams... Telephone Scam Alleging a Relative is in a Financial or Legal Crisis
Toll Scams	**Gold Courier Scams**
59,271 complaints; $129,624 in losses Smishing Scam Regarding Debt for Road Toll Services	525 complaints; $219 million in losses Scammers Use Couriers to Retrieve Cash and Precious Metals...

[7] Accessibility description: Chart describes totals for crime types generally considered to be cyber-enabled fraud: 333,981 complaints; $13.7 billion in losses; 38% of 2024 complaints received; 83% of 2024 losses. * Please see Appendix C for more information regarding IC3 data.

[8] Accessibility description: Chart describes counts and losses for crime types generally considered to be cyber-enabled fraud.

สถิติองค์กรที่ถูกโจมตีทางไซเบอร์ทั่วโลกระหว่างปี 2021-2025



ในปี 2025 มีองค์กรธุรกิจเกือบร้อยละ 63 ทั่วโลกได้รับผลกระทบจากการโจมตีทางไซเบอร์ แม้ว่าตัวเลขดังกล่าวจะลดลงจากปีก่อนหน้า และนับเป็นอัตราที่ต่ำที่สุดตั้งแต่ปี 2020 โดยภาพรวมแล้วตั้งแต่ปี 2018 พบว่าในแต่ละปี ผู้ทำแบบสำรวจมากกว่าครึ่งหนึ่งระบุว่าองค์กรของตนเคยตกเป็นเหยื่อของการโจมตีด้วย Ransomware อย่างน้อยหนึ่งครั้ง

อุตสาหกรรมที่ตกเป็นเป้าหมายมากที่สุด

ในปี 2024 อุตสาหกรรมการผลิตที่สำคัญในสหรัฐฯ ยังคงเป็นเป้าหมายหลักของอาชญากรไซเบอร์ในการโจมตีด้วย Ransomware มากที่สุด โดยองค์กรในภาคส่วนดังกล่าวประสบกับการโจมตีทางไซเบอร์รวม 258 ครั้ง รองลงมาคือภาคการดูแลสุขภาพและสาธารณสุข (Healthcare) โดนโจมตี 238 ครั้ง และหน่วยงานภาครัฐ 220 ครั้ง ตามลำดับ อุตสาหกรรมการผลิตและอุตสาหกรรมย่อยยังคงเผชิญกับการโจมตีด้วย Ransomware อย่างต่อเนื่อง ซึ่งส่งผลกระทบต่อภาคธุรกิจทั้งการสูญเสียข้อมูลสำคัญ การหยุดชะงักของกระบวนการทางธุรกิจ และสร้างความเสียหายต่อภาพลักษณ์องค์กร ในหลายกรณี มีการโจมตีข้ามพรมแดนและแฝงนัยทางการเมือง โดยใช้ประโยชน์จากช่องโหว่ของระบบในการโจมตีด้วย Ransomeware ในอุตสาหกรรมการผลิต

ที่มา: ANNUAL SHARE OF ORGANIZATIONS AFFECTED BY RANSOMWARE ATTACKS WORLDWIDE FROM 2018 TO 2025

การแก้ปัญหา

- **Operation Level Up หรือ ปฏิบัติการ “Level Up”**

แนวทางเชิงรุกของหน่วยงาน FBI ในการปกป้องเหยื่ออาชญากรรมไซเบอร์ด้านการลงทุนคริปโต ปฏิบัติการนี้เริ่มขึ้นเมื่อเดือนมกราคม 2024 ด้วยความร่วมมือระหว่างสำนักงานสอบสวนกลาง (FBI) และหน่วยงานราชการลับแห่งสหรัฐอเมริกา (United States Secret Service: USSS) มีเป้าหมายหลักในการระบุตัวเหยื่อของการฉ้อโกงจากการลงทุนสกุลเงินดิจิทัล และแจ้งเตือนให้ทราบถึงพฤติกรรมหลอกลวงที่กำลังเกิดขึ้น ตลอดจนช่วยลดความเสียหายทางการเงินที่อาจเกิดขึ้นเพิ่มเติม ซึ่งหนึ่งในรูปแบบการฉ้อโกงการลงทุนสกุลเงินดิจิทัลที่เป็นที่นิยมนั่นก็คือการหลอกลวงที่เรียกว่า “การฆ่าหมู (Pig Butchering Scam)” เป็นการหลอกลวงเชิงจิตวิทยาที่อาชญากรมักใช้วิธีเข้าหาเหยื่อทางออนไลน์ สร้างความสัมพันธ์ ความไว้เนื้อเชื่อใจ และจากนั้นจะค่อยๆ ชักชวนให้ลงทุนในแพลตฟอร์มสกุลเงินดิจิทัลปลอม เหยื่อมักถูกกระตุ้นให้เพิ่มเงินลงทุนอย่างต่อเนื่องด้วยข้อมูลผลตอบแทนที่น่าเชื่อถือ แต่เมื่อถึงเวลาที่ต้องการถอนเงินกลับไม่สามารถทำได้ ปฏิบัติการ Level Up ยังสามารถระบุเหยื่อของการหลอกลวงอีกหลายรูปแบบ เช่น การหลอกลวงให้ทำงานจากที่บ้าน โดยมิจฉาชีพจะแอบอ้างเป็นพนักงานบริษัทที่ถูกต้องตามกฎหมาย จากนั้นจะชักชวนเหยื่อให้เข้าร่วมการฝึกอบรมออนไลน์ และกำหนดให้เหยื่อต้องทำงานให้สำเร็จโดยการโอนเงินหรือซื้อสกุลเงินดิจิทัลเข้าสู่แพลตฟอร์มที่สร้างขึ้นเพื่อการหลอกลวงโดยเฉพาะ จากข้อมูลการร้องเรียนของ IC3 Operation Level Up รายงานว่า มีผู้เสียหายจากการหลอกให้ลงทุนสกุลเงินดิจิทัลจำนวน 4,323 ราย ร้อยละ 76 ของผู้เสียหายเหล่านี้ไม่ทราบว่าตัวเองถูกหลอก คาดการณ์ว่าการปฏิบัติการ Level Up นี้จะช่วยให้ผู้เสียหายไม่เสียทรัพย์สินได้กว่า 285 ล้านเหรียญสหรัฐฯ

- **Call Center Fraud**

1.การฉ้อโกงผ่านศูนย์บริการทางโทรศัพท์ หรือที่เราคุ้นหูว่า แกงค์คอลเซ็นเตอร์ การฉ้อโกงโดยกลุ่ม Call Center ที่ผิดกฎหมายนี้ส่งผลกระทบต่อเหยื่อหลายพันรายในแต่ละปี โดยมีการรายงานการฉ้อโกงของคอลเซ็นเตอร์ เช่น การปลอมแปลงตัวตน และ Tech/Customer Support การจัดการเกี่ยวกับการฉ้อโกงผ่านศูนย์บริการที่ผิดกฎหมายนี้ กระทรวงยุติธรรมสหรัฐอเมริกา (U.S. Department of Justice: DOJ) หน่วยงาน FBI และ Central Bureau of Investigation ได้ร่วมมือกับหน่วยงานบังคับใช้กฎหมายอินเดีย เช่น สำนักงานสอบสวนกลางอินเดีย (CBI) ในเมืองนิวเดลี และหน่วยงานระดับรัฐต่างๆ เพื่อปราบปรามอาชญากรรมด้านการเงินทางไซเบอร์และการฉ้อโกงทางโทรศัพท์ข้ามชาติ โดยความร่วมมือนี้นำไปสู่การจับกุมยึดทรัพย์เครือข่ายอาชญากรที่ต้องสงสัยว่าเชื่อมโยงกับกิจกรรมผิดกฎหมายดังกล่าว

- **Ransomware**

ทีม IC3 ได้มีการตรวจพบแรนซัมแวร์สายพันธุ์ใหม่ 67 ตัวในปี 2024 โดยสายพันธุ์ที่ได้รับรายงานมากที่สุด ได้แก่ FOG, Lynx, Cicada 3301, Dragonforce และ Frag เป็นต้น IC3 ได้ทำการรวบรวมข้อมูลที่ได้รับร้องเรียนจากการโจมตีของแรนซัมแวร์ชนิดใหม่นี้แก่หน่วยงาน FBI เพื่อให้ช่วยระบุที่มาและค้นหาองค์กรผู้ก่อภัยคุกคาม โดยในเดือนกุมภาพันธ์ 2024 ได้มีปฏิบัติการยึดโดเมนที่ใช้เผยแพร่มัลแวร์ Warzone RAT ซึ่งเจ้าหน้าที่ FBI ของเมืองบอสตันได้เข้ายึด www.warzone.ws พร้อมโดเมนที่เกี่ยวข้องอีกสามแห่ง ซึ่งถูกใช้เป็นแพลตฟอร์มในการจำหน่าย Warzone RAT มัลแวร์ประเภทโทรจันสำหรับการเข้าถึงระยะไกลที่มีความซับซ้อนสูง มัลแวร์ชนิดนี้เปิดทางให้อาชญากรไซเบอร์สามารถลักลอบควบคุมคอมพิวเตอร์ของเหยื่อได้โดยที่เหยื่อไม่ทราบ เพื่อใช้ในการกระทำที่มุ่งร้ายหลากหลายรูปแบบ Warzone RAT ช่วยให้อาชญากรสามารถเข้าถึงระบบไฟล์ ถ่ายภาพหน้าจอ บันทึกการกดแป้นพิมพ์ ขโมยข้อมูลชื่อผู้ใช้และรหัสผ่าน รวมถึงสอดส่องเหยื่อผ่านกล้องเว็บแคม โดยการกระทำเหล่านี้เหยื่อไม่สามารถทราบได้ ปฏิบัติการดังกล่าวสะท้อนให้เห็นถึงความพยายามของรัฐบาลสหรัฐฯ ในการขัดขวางโครงสร้างพื้นฐานของผู้พัฒนาและจำหน่ายเครื่องมือโจมตีทางไซเบอร์ที่ใช้ในการเจาะระบบและละเมิดความเป็นส่วนตัวของประชาชนเหล่านี้

- **Financial Fraud Kill Chain**

ทีม IC3 Recovery Asset ได้ทำการขัดขวางการฉ้อโกงทางการเงิน โดยทำหน้าที่ประสานงานระหว่างสถาบันการเงินกับหน่วยงาน FBI ภาคสนามทั่วประเทศ เพื่อเร่งรัดการอายัดเงินที่ถูกโอนออกไปจากการฉ้อโกง ทั้งที่เกิดภายในสหรัฐฯ และระหว่างประเทศ ซึ่งถือเป็นการช่วยลดความสูญเสียของเหยื่อได้อย่างมีนัยสำคัญ โดยหนึ่งในตัวอย่างที่โดดเด่นเกิดขึ้นเมื่อเดือนมีนาคม 2024 โดยทีม Recovery Asset จากหน่วยงาน FBI เมืองเดนเวอร์ ได้รับแจ้งเหตุการณ์หลอกลวงแบบ Business Email Compromise ที่เกี่ยวข้องกับการซื้อขายอสังหาริมทรัพย์ โดยเหยื่ออยู่ระหว่างขั้นตอนการเปิดขาย และได้รับอีเมลปลอมซึ่งแอบอ้างว่าเป็นตัวแทนอสังหาริมทรัพย์ของตน อีเมลดังกล่าวหลอกให้เหยื่อโอนเงินจำนวน 956,342 เหรียญสหรัฐฯ ไปยังบัญชีธนาคารแห่งหนึ่งในสหรัฐฯ เพื่อดำเนินการปิดการขาย ภายหลังสองวันหลังจากเหยื่อโอนเงินแล้วพบว่าคำสั่งดังกล่าวมาจากผู้ไม่หวังดี จึงได้รีบรายงาน IC3 และทีม Recovery Asset ได้ดำเนินการประสานงานกับธนาคารเพื่ออายัดบัญชีผู้รับที่เกี่ยวข้องกับการฉ้อโกงนี้โดยทันที ผลลัพธ์คือสามารถอายัดเงินได้ 955,060 เหรียญสหรัฐฯ และคืนเงินเกือบทั้งหมดให้แก่เหยื่อได้สำเร็จ ซึ่งเหตุการณ์นี้สะท้อนให้เห็นถึงความสำคัญของกลไกการประสานงานระหว่างหน่วยงานที่รวดเร็วและมีประสิทธิภาพในการรับมือกับอาชญากรรมทางการเงินในยุคดิจิทัล ซึ่งเป็นประโยชน์และช่วยลดผลกระทบต่อผู้เสียหายได้อย่างเป็นรูปธรรม

ที่มา:

OPERATION LEVEL UP

FBI INTERNET CRIME REPORT 2024

INTERNET CRIME COMPLAINT CENTER

ตัวอย่างสถานการณ์ด้านอาชญากรรมไซเบอร์ในปัจจุบัน

ภาพจาก : https://www.bbc.com

ในช่วงไม่กี่ปีให้หลัง ท่านผู้อ่านอาจพอทราบข่าวสารที่เกี่ยวข้องกับแกงค์สแกมเมอร์ที่ระบาดหนักในประเทศไทย ซึ่งเป็นกระบวนการหลอกลวงโดยใช้วิธีการฟิชชิง หลอกผู้เสียหายให้มีการโอนเงินผ่านทางลิงก์หรือใช้วิธีการสร้างเรื่องราวปลอมแปลงเอกสารในการทำให้เหยื่อหลงเชื่อและให้ข้อมูลที่สำคัญด้านการเงินแก่เหล่าอาชญากรเหล่านี้ โดยเชื่อว่ากระบวนการสแกมเมอร์นี้มีฐานทำงานสำคัญตั้งอยู่ในประเทศเพื่อนบ้านของไทย เราจะขอยกตัวอย่างเหตุการณ์กวาดล้างศูนย์อาชญากรรมไซเบอร์ที่เกิดขึ้นล่าสุดเมื่อช่วงเดือนตุลาคม 2025 ตามรายงานข่าวของสำนักข่าว BBC ระบุว่า การกวาดล้างเคเค พาร์ค (KK Park) ศูนย์อาชญากรรมไซเบอร์ติดชายแดนไทยใหญ่อันดับสองในพื้นที่ควบคุมของกะเหรี่ยงบีจีเอฟ โดยกองทัพเมียนมาเปิดปฏิบัติการกวาดล้างเมืองเคเค พาร์คเมื่อวันที่ 16 ต.ค. ที่ผ่านมาและสามารถเข้าควบคุมพื้นที่ทั้งหมดไว้ได้ในวันที่ 22 ต.ค. ส่งผลให้ชาวต่างชาติที่ทำงานอยู่ในนั้นเร่งพากันหลบหนีไปยังพื้นที่อื่นๆ ขณะที่บางส่วนได้ข้ามมายังฝั่งประเทศไทย ซึ่งคาดว่ามีจำนวนกว่า 1 พันราย

ที่มา:

OPERATION LEVEL UP

FBI INTERNET CRIME REPORT 2024

INTERNET CRIME COMPLAINT CENTER

เคเค พาร์ค คืออะไร?

เคเค พาร์ค เป็นศูนย์อาชญากรรมไซเบอร์มีขนาดใหญ่เป็นอันดับสองในพื้นที่ควบคุมของกะเหรี่ยงบีจีเอฟ โดยย้อนกลับไปในปี 2020 กลุ่มบริษัท ตงเหมยกรุ๊ป (Dongmei Group) นำโดยนาย Wan Kuok-Koi อดีตหัวหน้ากลุ่ม 14K นำกลุ่มนักลงทุนจากมาเลเซียเข้ามาลงทุนสร้างเมืองใหม่ชื่อว่า “เขตอุตสาหกรรมไซซีกัง” ในพื้นที่รัฐกะเหรี่ยงของเมียนมา ซึ่งเป็นพื้นที่ควบคุมของ พ.ต.เต่ง วิน รองผู้บังคับกองพันกะเหรี่ยงบีจีเอฟ ซึ่งในเวลาต่อมา เมืองอุตสาหกรรมไซซีกังได้ถูกเปลี่ยนชื่อเป็นเคเค พาร์ค และสามารถดึงดูดกลุ่มนักลงทุนจากประเทศจีน หรือที่เรียกกันว่ากลุ่มจีนเทา ก่อนจะมีศูนย์สแกมเมอร์ในเมืองไท่ฉาง ซึ่งอยู่ตรงข้ามช่องแคบของอำเภอพบพระ จังหวัดตาก ประเทศไทย เคเค พาร์คได้ขึ้นชื่อว่าเป็นเมืองที่มีความโหดร้ายทารุณ ประกอบไปด้วยแหล่งอบายมุข ทั้งคาสิโน ศูนย์ความบันเทิง ร้านค้า สำนักงาน แหล่งที่อยู่อาศัยของผู้บังคับบัญชาเหล่าสแกมเมอร์ และเต็มไปด้วยผู้คนที่ถูกหลอกลวงมาทำงานในศูนย์สแกมเมอร์ การลักพาตัว การเรียกค่าไถ่ การค้าประเวณี และข่าวลือเรื่องการค้าอวัยวะ เมืองแห่งนี้ยังถูกล้อมด้วยรั้วสูง และป้อมยามทหารของกะเหรี่ยงบีจีเอฟคอยอำนวยความสะดวกและช่วยรักษาความปลอดภัย ซึ่งในปัจจุบันผู้ที่เกี่ยวข้องกับเคเค พาร์คทั้ง พ.อ.ชิต ตุ พ.ต.เต่ง วิน บริษัท ตงเหมยกรุ๊ป บริษัท ดอกงิ้วคำ และนายจ้าว เหว่ย ต่างก็ถูกขึ้นบัญชีดำอยู่ในกลุ่มผู้ที่ถูกมาตรการคว่ำบาตรทางการเงินของรัฐบาลสหรัฐอเมริกา ในฐานะที่เกี่ยวข้องกับองค์กรอาชญากรรมข้ามชาติที่พัวพันกับอาชญากรรมออนไลน์ระดับโลก ในการปฏิบัติการครั้งนี้ รัฐบาลทหารเมียนมาได้มีการกล่าวโทษกลุ่มชาติพันธุ์ นั่นก็คือ กองสหภาพแห่งชาติกะเหรี่ยง หรือ Karen National Union (KNU) ว่ามีส่วนเกี่ยวข้องกับเคเค พาร์ค ซึ่ง KNU ก็ได้ออกมาปฏิเสธและกล่าวว่าโฆษกคณะทหารเมียนมาจงใจเผยแพร่ข้อมูลเท็จ เพื่อปกปิดผลประโยชน์ทางการเมือง เศรษฐกิจ และผลประโยชน์ที่กองทัพเมียนมาถูกกล่าวหาว่าได้จากปฏิบัติการหลอกลวงต่างๆ ที่เกิดขึ้นภายในประเทศเมียนมา

ก่อนหน้านี้ สถาบันสันติภาพแห่งสหรัฐอเมริกา หรือ United States Institute of Peace (USIP) ซึ่งเป็นหน่วยงานอิสระที่ก่อตั้งโดยรัฐสภาของสหรัฐฯ เคยระบุว่า ผู้นำกองพลที่ 7 มีส่วนเกี่ยวข้องกับเมืองใหม่หวันหยา ศูนย์สแกมเมอร์อีกหนึ่งแห่งที่สร้างในพื้นที่ประชิดริมแม่น้ำเมยตายแดนไทย และอยู่ห่างจากเคเค พาร์คขึ้นมาทางเหนือประมาณ 3 กิโลเมตร โดยผู้นำกองพลที่ 7 พ.ท.โรเจอร์ ขิ่น มีสายสัมพันธ์ใกล้ชิดกับพ.อ.ชิต ตุ และกองทัพกะเหรี่ยงพุทธประชาธิปไตย หรือ Democratic Karen Buddhist Army (DKBA) ซึ่งเป็นกลุ่มที่เกี่ยวข้อง กับอาชญากรรมไซเบอร์ในแนวชายแดนไทย-เมียนมาด้วยเช่นกัน

ความร่วมมือในการกวาดล้างสแกมเมอร์ของสหรัฐอเมริกา

หากมองในภาพกว้างๆ การเคลื่อนไหวของกองทัพเมียนมาเกิดขึ้นจากแรงผลักดันชาติตะวันตก โดยเฉพาะสหรัฐอเมริกา การปฏิบัติการกวาดล้างครั้งนี้ก็ได้รับความร่วมมือจากสหรัฐฯ เช่นกัน การเร่งปราบปรามเครือข่ายอาชญากรรมออนไลน์ในเอเชียตะวันออกเฉียงใต้อย่างต่อเนื่อง โดยในช่วงที่ผ่านมาสหรัฐฯ ได้ประกาศคว่ำบาตรบุคคลและบริษัทหลายรายที่เชื่อมโยงกับขบวนการสแกมเมอร์ออนไลน์ทั้งในประเทศเมียนมา ลาว กัมพูชา และไทยตั้งแต่กลุ่มผู้นำกะเหรี่ยง กลุ่มผู้มีอิทธิพล ไปจนถึงนักธุรกิจที่ใกล้ชิดผู้นำกัมพูชา ซึ่งถูกกล่าวหาว่ามีบทบาทในองค์กรอาชญากรรมข้ามชาติที่สร้างความเสียหายต่อชาวอเมริกันมหาศาล โดยกระทรวงการคลังของสหรัฐฯ รายงานว่าชาวอเมริกันจำนวนมากสูญเงินจากการถูกหลอกลวงทางออนไลน์ไปอย่างน้อย 10,000 เหรียญสหรัฐฯ ทำให้ยิ่งมีแรงกดดันจากสหรัฐฯ มากยิ่งขึ้น อีกทั้ง นายชรีฟ เจฟเฟอร์สัน สมาชิกผู้แทนราษฎรจากพรรครีพับลิกัน จากรัฐอินเดียนา ได้เสนอร่างกฎหมายต่อรัฐสภาของสหรัฐฯ ในการจัดตั้งหน่วยงานเฉพาะกิจร่วมระหว่างหน่วยงานเพื่อปราบปรามกลุ่มอาชญากรข้ามชาติที่ฉ้อโกงชาวอเมริกัน โดยในร่างกฎหมายฉบับดังกล่าวระบุชัดถึงความเชื่อมโยงที่น่ากังวลระหว่างรัฐบาลจีน กลุ่มอาชญากรรมจีน และนักการเมืองท้องถิ่นที่คอรัปชัน ซึ่งล้วนเป็นปัจจัยที่ผลักดันให้กลุ่มสแกมเมอร์ออนไลน์เติบโตในช่วงการระบาดของโควิด-19 องค์กรอาชาญากรรมจีนในเอเชียตะวันออกเฉียงใต้ได้หันมาใช้รูปแบบการหลอกลวงออนไลน์ที่ซับซ้อนมากยิ่งขึ้น โดยเฉพาะอย่างยิ่งการลงทุนผ่านสกุลเงินดิจิทัล รูปแบบที่พบมากที่สุดคือ การหลอกลวงแบบเชือดหมู (Pig butchering) คือสร้างความสัมพันธ์กับเหยื่อเพื่อหลอกให้ลงทุนเรื่อยๆ ผ่านแพลตฟอร์มการเงินปลอมก่อนจะยักยอกเงินไปทั้งหมด ข้อมูลในร่างกฎหมายระบุเพิ่มเติมว่า ผู้ที่ปฏิบัติการหลอกลวงจำนวนมากเป็นเหยื่อจากการค้ามนุษย์และแรงงานบังคับ โดยถูกล่อลวงด้วยประกาศรับสมัครงานปลอม ถูกนำตัวไปกักขังในสถานที่ปิด และถูกบังคับให้ทำยอดการหลอกลวงตามเป้าหมาย หากไม่เช่นนั้นจะถูกทำร้ายอย่างโหดร้าย ร่างกฎหมายนี้ยังชี้ว่า ศูนย์สแกมเมอร์เหล่านี้พบมากในประเทศเมียนมา ลาว และกัมพูชา ซึ่งเป็นประเทศที่ประสบปัญหาคอรัปชัน ไม่โปร่งใส เหล่าองค์กรอาชญากรรมเหล่านี้จึงอาศัยช่องโหว่ในการเข้ามาสร้างศูนย์อบายมุขนี้ มีการรายงานถึงจำนวนชาวอเมริกันที่ตกเป็นเหยื่อของแกงค์สแกมเมอร์นี้ว่าเพิ่มขึ้นถึงร้อยละ 33 เมื่อเทียบกับปี 2023 สะท้อนให้เห็นว่า กลุ่มอาชญากรได้เพิ่มการมุ่งเป้ามายังประชาชนชาวสหรัฐฯ อย่างชัดเจน ขณะเดียวกันทั่วโลกมีความเสียหายจากอาชญากรรมประเภทนี้มากกว่า 60,000 ล้านเหรียญสหรัฐฯ ต่อปี แต่คาดว่าตัวเลขจริงอาจสูงกว่านี้มาก เนื่องจากหลายกรณีที่ไม่ได้ถูกรายงาน ร่างกฎหมายยังเตือนถึงความเชื่อมโยงที่น่ากังวลระหว่างรัฐบาลจีน เครือข่ายอาชญากรรมจีน และนักการเมืองท้องถิ่นที่ทุจริต ซึ่งเป็นส่วนสำคัญที่ช่วยหล่อเลี้ยงให้ขบวนการเหล่านี้เติบโต

ร่างกฎหมายฉบับนี้ยังให้อำนาจแก่ประธานาธิบดีในการใช้มาตรการคว่ำบาตรต่อชาวต่างชาติและบริษัทที่เกี่ยวข้องกับศูนย์หลอกลวงหรือการค้ามนุษย์ อย่างไรก็ตาม สหรัฐอเมริกายังได้ร่วมมือกับสหราชอาณาจักรในการดำเนินคดีของนายเฉิน จื้อ หรือที่รู้จักกันในนาม Vincent ชายเชื้อสายจีน สัญชาติสหราชอาณาจักรและกัมพูชา ผู้ก่อตั้งและเป็นประธานกลุ่มบริษัท Prince Holding Group ซึ่งเป็นกลุ่มบริษัทธุรกิจข้ามชาติขนาดใหญ่ในกัมพูชา กระทรวงยุติธรรมสหรัฐอเมริกาทำการยื่นฟ้องริบทรัพย์ของนายเฉินเป็นบิตคอยน์มูลค่าประมาณ 15,000 ล้านเหรียญสหรัฐฯ และดำเนินคดีต่อนายเฉินในข้อหาฉ้อโกงทางอิเล็กทรอนิกส์และคบคิดฟอกเงิน แม้ภายนอกบริษัท Prince Group จะประกอบธุรกิจด้านอสังหาริมทรัพย์ บริการทางการเงิน และธุรกิจผู้บริโภค แต่ทางการสหรัฐฯ ระบุว่า ผู้บริหารระดับสูงรวมถึงนายเฉินได้ใช้บริษัทเป็นฉากบังหน้าในการดำเนินองค์กรอาชญากรรมข้ามชาติ เป็นศูนย์ดำเนินการหลอกลวงแรงงานบังคับและมีส่วนเกี่ยวข้องกับการหลอกลวงให้ลงทุนในสกุลเงินดิจิทัล ซึ่งมีผู้เสียหายในสหรัฐฯ และทั่วโลกจำนวนมาก ส่งผลให้สหรัฐฯ และสหราชอาณาจักรทำความร่วมมือในการริบทรัพย์และออกมาตรการคว่ำบาตรในครั้งนี้ครอบคลุมถึงบริษัทที่เชื่อมโยงกับ Prince Group เช่น Jinbei Group ผู้ดำเนินธุรกิจบันเทิงครบวงจรและคาสิโนในเมืองสีหนุวิลล์ ประเทศกัมพูชา รวมถึงศูนย์สแกมเมอร์ต่างๆ และ Golden Fortune Resort World ซึ่งอ้างว่าเป็น “อุทยานเทคโนโลยีขนาดใหญ่” ใช้ชื่อว่า Golden Fortune Science and Technology Park ตั้งอยู่ใจกลางกรุงพนมเปญ แต่แท้จริงเป็นที่ตั้งของศูนย์ปฏิบัติการสแกมเมอร์ นอกจากนี้ยังมีแพลตฟอร์ม คริปโตที่เกี่ยวข้องกับเครือข่ายดังกล่าวที่ชื่อว่า Byex Exchange ก็ถูกคว่ำบาตรด้วยเช่นกัน

ผลกระทบของอาชญากรรมไซเบอร์

ความเสียหายที่เกิดขึ้นจากอาชญากรรมไซเบอร์ในปัจจุบันมีมูลค่าสูงถึงหลายแสนล้านเหรียญสหรัฐในแต่ละปีทั่วโลก ซึ่งไม่เพียงแต่สะท้อนให้เห็นถึงผลกระทบทางเศรษฐกิจเท่านั้น แต่ยังขยายไปสู่มิติอื่นๆ ของสังคมเป็นวงกว้าง ผลกระทบที่เกิดขึ้นไม่เพียงแต่สร้างปัญหาทางเทคโนโลยี แต่ยังสร้างภัยคุกคามต่อความมั่นคงทางเศรษฐกิจ สังคม และความเชื่อมั่นของประชาชน อาชญากรรมไซเบอร์มักก่อให้เกิดผลเสียหายหลายประการ ได้แก่ การเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ประสิทธิภาพในการตอบสนองต่อเหตุฉุกเฉินลดลงเนื่องจากระบบถูกบุกรุก และการเปลี่ยนแปลงราคาหรือมูลค่าทางเศรษฐกิจที่ไม่เป็นธรรมหลังจากการโจมตีทางดิจิทัล เป็นต้น เหตุการณ์เหล่านี้สามารถบั่นทอนความเชื่อมั่น ความไว้วางใจของสาธารณชนและเพิ่มความเสี่ยงให้ผู้คนตกเป็นเหยื่อซ้ำๆ เนื่องจากข้อมูลที่ถูกขโมยไปอาจถูกเผยแพร่ในมุมมืดของอินเทอร์เน็ตและถูกนำไปใช้ในกิจกรรมผิดกฎหมายอย่างต่อเนื่อง

ที่มา:

CHAIRMAN OF PRINCE GROUP INDICTED FOR OPERATING CAMBODIAN FORCED LABOR SCAM COMPOUNDS ENGAGED IN CRYPTOCURRENCY FRAUD SCHEMES

HTTPS://WWW.BBC.COM

https://www.bbc.com/thai/articles/c77z6mp4k86o

https://www.bbc.com/thai/articles/cr70v0nvk4xo