

ANNUAL REPORT



2019

01

Banking
Situation Analysis

02

Public Awareness

03

Threat Analysis
& Trends



รายงานประจำปี

ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
(Thailand Banking Sector CERT: TB-CERT)
ปี 2562

จัดทำโดย

ดร.กิตติ โฆษะวิสุทธิ์
กิตติศักดิ์ จีรวรรณกุล
ธาวินี วงศ์วิศว์
ชญานิน แก้วหาญ

ที่ปรึกษา

ดร.กิตติ โฆษะวิสุทธิ์

บรรณาธิการ

ธาวินี วงศ์วิศว์

ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
สมาคมธนาคารไทย

5/13 หมู่ 3 ถนนแจ้งวัฒนะ ตำบลคลองเกลือ

อำเภอปากเกร็ด จังหวัดนนทบุรี 11120

0 2558 7500

contact@tb-cert.or.th

เผยแพร่เมื่อ

มีนาคม 2563

TLP: WHITE

สารบัญ

2	เกี่ยวกับ TB-CERT
3	คำนิยม โดย ดร.วิโรท สันติประภพ ผู้ว่าการธนาคารแห่งประเทศไทย คุณปรีดี ดาวฉาย ประธานสมาคมธนาคารไทย
5	สารจากคณะกรรมการ
7	บทความประจำปี Building a cyber resilient culture for your organization
11	บทวิเคราะห์บุคลากรด้าน Cybersecurity ของภาคการธนาคาร
13	กิจกรรมในปี 2562
21	เหตุการณ์สำคัญด้านภัยไซเบอร์ในปี 2562 สรุปเหตุการณ์โลกที่น่าสนใจตามทวีปต่าง ๆ ในปี 2562 วิเคราะห์เหตุการณ์ในปี 2562 เทียบกับปี 2561 เทคนิคของกลุ่มแฮกเกอร์สถาบันการเงินที่น่าสนใจ
33	คาดการณ์แนวโน้มการโจมตีในปี 2563
36	บทสรุป
37	ภาคผนวก เอกสารเผยแพร่ คณะกรรมการ TB-CERT สมาชิก TB-CERT

เกี่ยวกับ TB-CERT

ความเป็นมา

Thailand Banking Sector Computer Emergency Response Team หรือ TB-CERT จัดตั้งขึ้นโดยความเห็นชอบของผู้บริหารระดับสูงของธนาคารพาณิชย์ในประเทศไทย เพื่อสนับสนุนให้สมาชิกกลุ่มซึ่งเป็นพนักงานของธนาคารได้มีการแลกเปลี่ยนข้อมูลและประสบการณ์เพื่อประโยชน์โดยรวมของสถาบันการเงินในประเทศไทย โดยเฉพาะเพื่อการนำไปใช้ในการป้องกันเหตุภัยคุกคามทางไซเบอร์ที่อาจจะมีผลกระทบกับการบริการ ทรัพยากร หรือบุคลากรขององค์กร โดยจะไม่เสนอความเห็นต่อผลิตภัณฑ์ทางการเงิน (Product) หรือให้ข้อมูลเชิงลบต่อหน่วยงานหรือบุคคลที่สาม อันจะทำให้เกิดความเสียหายและเป็นอุปสรรคต่อกิจกรรมการแลกเปลี่ยนความคิดเห็น หรือความสัมพันธ์อันดีของสมาชิกในกลุ่ม

คำนิยามหลัก

TB-CERT เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลในด้านความมั่นคงปลอดภัยไซเบอร์ เป็นศูนย์รวมของบุคลากรที่มีความชำนาญด้านไซเบอร์ และเป็นแหล่งให้ความรู้และสร้างความตระหนักในการระวังภัยที่อาจเกิดขึ้นได้ทุกเมื่อ ไม่ว่าจะเป็นเกิดกับบุคลากร ลูกค้า หรือธุรกิจของธนาคาร รวมถึงเป็นศูนย์กลางในการติดต่อสื่อสารกับองค์กรที่เกี่ยวข้องทั้งในและต่างประเทศ เพื่อให้สามารถรับรู้ข่าวสารและช่วยเหลือในการแก้ปัญหาภัยไซเบอร์ที่เกิดขึ้นกับสมาชิก ทั้งนี้เพื่อให้ทุกภาคส่วนมีความรู้และเข้าใจเรื่องภัยไซเบอร์และพร้อมรับมือกับภัยเหล่านี้ได้อย่างมีประสิทธิภาพ

การดำเนินงาน

การดำเนินงานของ TB-CERT จะครอบคลุม 4 ด้านที่สำคัญคือ

1. เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูล ทั้งภัยคุกคามด้านไซเบอร์และแนวทางการแก้ไข
2. สร้างมาตรฐานกลางด้านความมั่นคงปลอดภัย ของการใช้เทคโนโลยีใหม่
3. กำหนดกระบวนการในการรับมือภัยไซเบอร์ภาคธนาคาร และจัดให้มีการซ้อมรับมือร่วมกันอย่างสม่ำเสมอ
4. ส่งเสริมการพัฒนาบุคลากรด้าน Cybersecurity โดยครอบคลุมทั้งการสร้างบุคลากรใหม่เข้าสู่ภาคการเงิน และพัฒนาบุคลากรของสถาบันการเงินให้มีความรู้ความเข้าใจ และสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์

คำนิยม



ดร.วิโรจน์ สันติประภพ
ผู้ว่าการธนาคารแห่งประเทศไทย

เราทุกคนทราบว่าเทคโนโลยีสมัยใหม่เป็นหัวใจของการให้บริการทางการเงิน และจะทวีความสำคัญมากขึ้นเรื่อย ๆ ในขณะที่เทคโนโลยีสร้างประโยชน์มากมาย เทคโนโลยีก็นำมาซึ่งความเสี่ยงประเภทใหม่ ๆ โดยเฉพาะภัยคุกคามด้านไซเบอร์ที่สามารถส่งผลกระทบต่อความมั่นคงของสถาบันการเงินแต่ละแห่ง และเสถียรภาพของระบบสถาบันการเงินและระบบการชำระเงินโดยรวมด้วย

ในโลกที่ระบบการเงินดิจิทัลจะซับซ้อนและเชื่อมโยงกันมาก ภัยคุกคามไซเบอร์ที่เกิดขึ้นกับสถาบันการเงินแห่งใดแห่งหนึ่งอาจกระจายตัวเป็นวงกว้าง ทวีความรุนแรง และนำไปสู่ปัญหาของระบบการเงินได้อย่างรวดเร็ว ดังนั้น การรับมือต่อภัยคุกคามด้านไซเบอร์ จึงต้องอาศัยความร่วมมืออย่างเข้มแข็งของทุกภาคส่วนในภาคการเงิน การจัดตั้ง TB-CERT เป็นก้าวสำคัญของความร่วมมือของธนาคารพาณิชย์ TB-CERT มีพัฒนาการอย่างรวดเร็วตลอดช่วงสองปีที่ผ่านมา มีการทำงานอย่างเป็นระบบและมีประสิทธิภาพ ทำให้เกิดผลที่ชัดเจนเป็นรูปธรรม

ผมขอชื่นชมทุกท่านและทุกหน่วยงานที่ได้ร่วมกันจัดตั้ง ขับเคลื่อน และพัฒนา TB-CERT จนเป็นกลไกสำคัญของการสร้างความมั่นคงปลอดภัยจากภัยคุกคามด้านไซเบอร์ในระบบการเงินไทย นอกจากนี้ TB-CERT ยังได้สนับสนุนการสร้างความมั่นคงปลอดภัยไซเบอร์ให้แก่ภาคเศรษฐกิจอื่นของประเทศอีกด้วย

ภายใต้โลกที่เทคโนโลยีกำลังเปลี่ยนแปลงอย่างรวดเร็ว และภัยคุกคามด้านไซเบอร์รุนแรงขึ้น และมาในหลากหลายรูปแบบขึ้น TB-CERT ยังมีภารกิจที่ต้องทำอีกมาก ธปท. จะเป็นพันธมิตรทำงานร่วมกับ TB-CERT เพื่อสร้างภูมิคุ้มกันภัยคุกคามด้านไซเบอร์ให้กับระบบสถาบันการเงิน ระบบการชำระเงิน และเศรษฐกิจไทยโดยรวมอย่างเข้มแข็งต่อไป

ดร. วิโรจน์ สันติประภพ
ผู้ว่าการธนาคารแห่งประเทศไทย

คำนิยม



คุณปรีดี ดาวฉาย ประธานสมาคมธนาคารไทย

TB-CERT ได้มีพัฒนาการอย่างต่อเนื่อง นับตั้งแต่ได้มีการจัดตั้งขึ้นในปี 2560 จาก Maturity Level 2 กำลังจะเป็น Level 4 ในปี 2563 กิจกรรมต่าง ๆ ที่ TB-CERT ได้ดำเนินการในปี 2562 มีจำนวนมาก ล้วนเป็นประโยชน์ต่อภาคธนาคารและภาคการเงินของประเทศ

อย่างไรก็ตาม ในขณะที่ประเทศไทยกำลังพัฒนาไปสู่เศรษฐกิจและสังคมดิจิทัล ภัยไซเบอร์ต่าง ๆ ก็มีมากขึ้น ทั้งในรูปแบบที่เรารู้จัก และรูปแบบใหม่ ๆ ที่เราไม่เคยรู้จัก TB-CERT จะต้องเป็นองค์กรที่ตื่นตัว และทำงานเชิงรุกเพื่อที่จะช่วยปกป้องอุตสาหกรรมธนาคารจากภัยไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งพัฒนาตัวเองอย่างต่อเนื่องและรวดเร็ว

ในนามของสมาคมธนาคารไทย ผมขอขอบคุณทีมงานของ TB-CERT และสมาชิกที่ได้ร่วมมือกันในกิจกรรมต่าง ๆ ในปีที่ผ่านมา และพร้อมที่จะให้การสนับสนุนการพัฒนาและกิจกรรมของ TB-CERT เพื่อให้ลูกค้าและภาคธนาคารมีความปลอดภัยจากภัยไซเบอร์ตลอดไป

ปรีดี ดาวฉาย
ประธานสมาคมธนาคารไทย

สารจาก คณะกรรมการ

“สิ่งสำคัญในการรับมือกับภัยคุกคามด้านไซเบอร์ได้อย่างทันท่วงทีและมีประสิทธิภาพนั้น ทุก ๆ คนในองค์กร ไม่ว่าจะเป็น บอร์ดบริหาร, ผู้บริหารระดับสูง จำเป็นต้องเข้าใจและตระหนักรู้รวมถึงให้ความสำคัญในเรื่องของความเสี่ยงด้านไซเบอร์ให้เป็นส่วนหนึ่งของการทำงานในทุก ๆ วัน”

ยศ กิมสวัสดิ์

“Security management is a good balance among head, heart and hands”

ดร.กิตติ โฆษะวิสุทธิ

“การทำงานเป็นทีมได้อย่างมีประสิทธิภาพ พื้นฐานต้องเกิดจากความไว้วางใจ (Trust) ซึ่งกันและกัน ภายในทีม ความไว้วางใจจะเกิดขึ้นได้ก็ต่อเมื่อสมาชิกในทีมมีความเป็นมืออาชีพ (Professionalism) มีจริยธรรม (Ethical) และรู้จริงในสิ่งที่ทำ (Expert)”

ชัชวัฒน์ อัครวิวงศ์

“การส่งต่อสิ่งที่เราเรียนรู้มา (Learning) ได้นั้นเป็นเรื่องสำคัญ และจะดียิ่งขึ้นไปกว่า ถ้าเราส่งต่อไปยังเครื่องจักร (Machine) ให้ทำงานแทนเรา”

นฤตม รุ่งศิริวงศ์

“ปัจจัยในความสำเร็จขององค์กรในการบริหารความปลอดภัยด้านไซเบอร์ คือ การพัฒนาบุคลากร ให้มีความพร้อม ความรู้ ความเข้าใจ ในภัยคุกคาม ตลอดจนการตระหนักการเลือกใช้เทคโนโลยีที่เหมาะสมในการควบคุมช่องโหว่ด้านความปลอดภัย และหมั่นซักซ้อมการรับมือ เพื่อพัฒนาศักยภาพขององค์กรให้ยั่งยืนต่อไป”

ประภลฤช แสงชูวงศ์

สารจาก คณะกรรมการ

“ในปี 2019 ภาคราชการต้องผ่านบททดสอบในหลายด้าน ทั้งการปรับรูปแบบบริการ ขั้นตอนการทำงาน เพื่อบริการที่ครอบคลุม เข้าถึงได้ ง่ายต่อการใช้งาน เพื่อประโยชน์ต่อภาคประชาชน/ผู้บริโภค การประยุกต์ใช้ Emerging Technologies เป็นเรื่องจำเป็น ด้วยปัจจัยเหล่านี้ หน้าที่รักษาความปลอดภัย ด้านไซเบอร์ จึงมีส่วนสำคัญอย่างมาก เพื่อรักษาความเชื่อมั่นของประชาชน ผู้บริโภค ภัยไซเบอร์ รูปแบบใหม่ที่เราไม่เคยพบ เกิดขึ้นมากมาย การมีพันธมิตรเพื่อร่วม share information, practices เป็นเรื่องจำเป็นที่มีความสำคัญอย่างยิ่ง ต่อการทำ proactive response TB-CERT เป็น Threat Intelligence Community ที่มีบทบาทอย่างมากที่จะเสริมสร้าง ให้เกิดความร่วมมือและสร้างความเชื่อมั่นต่อภาคการเงินของประเทศ ปี 2019 เราทำได้ดี แต่ยังคงต้องรักษาระดับคุณภาพให้ดียิ่งขึ้น เพื่อความพร้อมรับ ความท้าทายในปี 2020”

ภาคพงศ์ จุลวงศาศิลป์

“ไวรัสคอมพิวเตอร์หรือภัยทางไซเบอร์ก็เหมือนเชื้อโรค กลายพันธุ์ได้ และมีวิวัฒนาการตลอด เราต้องเรียนรู้ที่จะป้องกันตัวเอง ป้องกันสภาพแวดล้อม และแบ่งปันความรู้ซึ่งกันและกัน เพื่อให้เราทุกคนปลอดภัย”

สมบุรณ์ หิรัญภัทรศิลป์

บทความประจำปี

Organizational Resilience

เพื่อการเตรียมความพร้อมรับมือภัยด้านไซเบอร์
ในยุคเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

การพัฒนาของเทคโนโลยีในช่วง 4-5 ปีที่ผ่านมาจะเห็นได้ว่าเป็นไปในอัตราเร่งและมักจะถูกเรียกกันว่าเป็นช่วงเวลาหรือยุคของ disruption ซึ่งให้ความหมายในมุมของผลกระทบจากการเปลี่ยนแปลงในเชิงลบ ขณะที่การเปลี่ยนแปลงดังกล่าวในอีกหลายด้านจะเป็นไปในทางสร้างสรรค์และเป็นการพัฒนาสังคมให้มีประสิทธิภาพที่ดีขึ้นในยุคดิจิทัล อย่างไรก็ตาม ด้วยสภาพการเปลี่ยนแปลงที่รวดเร็วซึ่งเกิดจากการนำเทคโนโลยีที่ได้สร้างสมไว้เป็นพื้นฐานนำมาประกอบรวมกัน และด้วยความพร้อมของโครงสร้างพื้นฐานไม่ว่าจะเป็นระบบคลาวด์ การเชื่อมต่ออินเทอร์เน็ตความเร็วสูง และการเข้าถึงจำนวนผู้ใช้งานอุปกรณ์เคลื่อนที่ที่มีมากถึง 5.17 พันล้านคน หรือประมาณ 66% ของประชากรโลกในปัจจุบัน จึงก่อให้เกิดการนำเทคโนโลยีไปประยุกต์ใช้ในรูปแบบที่สร้างการเปลี่ยนแปลงได้ใน scale ขนาดใหญ่ จึงทำให้เกิดการเปลี่ยนแปลงสภาพแวดล้อมและการนำไปใช้งานแบบพลิกผันไปในรูปแบบที่ไม่เคยเป็นมาก่อน สภาพการณ์นี้จึงก่อให้เกิดผลกระทบทั้งธุรกิจและบุคคลธรรมดาที่ยังไม่เข้าใจเทคโนโลยี ยังไม่สามารถปรับเปลี่ยนวิธีการทำงานหรือวิถีการดำรงชีวิตได้เร็วเพียงพอกับการเปลี่ยนแปลงเหล่านั้น

การที่เทคโนโลยีถูกนำมาสร้างนวัตกรรมใหม่ๆ บริการใหม่ๆ และสร้างการเปลี่ยนแปลงอย่างรวดเร็วนั้น สภาพการใช้งานเทคโนโลยีเหล่านั้นจะกลายเป็นบรรทัดฐานใหม่ในการดำเนินของสังคม เช่น การใช้งาน chat หรือสื่อสารผ่าน mobile application แทนการส่งจดหมายและโทรศัพท์ ความเปลี่ยนแปลงของบรรทัดฐานในยุคดิจิทัลนี้จะแตกต่างจากช่วงก่อน กล่าวคือ ผู้ที่กำหนดบรรทัดฐานของสังคมนั้นไม่ใช่คนในสังคมแต่กลับเป็นบริษัทเทคโนโลยีผู้ที่นำเทคโนโลยีมาใช้ในการให้บริการ นั่นจึงเป็นปัจจัยหลักหนึ่งในการเร่งการเปลี่ยนแปลงให้เร็วขึ้น เนื่องจากไม่จำเป็นต้องใช้เวลาในการพัฒนาบรรทัดฐานของสังคม ยิ่งอัตราการนำเอาเทคโนโลยีมาใช้เป็นไปอย่างรวดเร็วเท่าใด โอกาสในการที่จะเตรียมการรับมือการเปลี่ยนแปลงดังกล่าวให้ได้มีประสิทธิภาพก็เป็นไปได้ยากขึ้นเท่านั้น โดยไม่ได้จำกัดที่ระดับปัจเจกบุคคลแต่จะส่งผลถึงการเตรียมความพร้อมในระดับองค์กรอีกด้วย ผู้ไม่ประสงค์ดีโดยเฉพาะที่เป็นภัยคุกคามทางไซเบอร์ก็มักจะใช้ช่องว่างของความเข้าใจสภาพการณ์ที่เปลี่ยนแปลงเร็วนี้ ในการโจมตี หลอกขโมยข้อมูล หรือฝังตัวในองค์กรเพื่อรอโอกาสที่เหมาะสมต่อไป

ระดับความรุนแรงของเหตุการณ์การโจมตีทางไซเบอร์นั้น มีแนวโน้มที่จะมีความซับซ้อนมากขึ้น จากที่ทาง TB-CERT ได้มีการเก็บข้อมูลและเฝ้าระวังจะเห็นได้ว่า รูปแบบการโจมตีในหลายครั้งจะใช้เทคนิคแบบผสมผสานซึ่งอาจจะหมายถึงมีความร่วมมือหรือแลกเปลี่ยนข้อมูลระหว่างกลุ่มผู้โจมตี หากติดตามเหตุการณ์ต่าง ๆ ทั่วโลกจะเห็นว่าเป้าหมายที่สำคัญในช่วงปีที่ผ่านมาแนวโน้มมุ่งไปที่หน่วยงานที่มีความสำคัญทางสารสนเทศของประเทศหรือที่เรียกกันว่า CII – Critical Information Infrastructure อีกทั้งยังมุ่งไปที่การขโมยข้อมูล ซึ่งนอกจากจะสร้างผลกระทบกับเจ้าของข้อมูลแล้วยังกระทบกับภาพพจน์ชื่อเสียงขององค์กรนั้น ๆ อีกด้วย นี่เป็นปัจจัยสำคัญหนึ่งที่ประเทศไทยพยายามผลักดันกฎหมายสำคัญ 2 ฉบับซึ่งมีความสำคัญมากในการที่ประเทศไทยจะก้าวสู่ยุคดิจิทัลและเป็นช่วงเวลาที่สำคัญในการสร้างความมั่นใจให้กับคนไทยและประเทศอื่น ๆ ที่จะต้องมีการเชื่อมต่อและทำธุรกรรมทั้งภาครัฐและภาคเอกชน นั่นคือ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ซึ่งได้ประกาศลงในราชกิจจานุเบกษาในวันที่ 27 พฤษภาคม 2562 โดยพ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์นั้น มีวัตถุประสงค์เพื่อที่จะสนับสนุนให้หน่วยงาน CII มีมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สูงขึ้น มีความพร้อมรับมือภัยไซเบอร์ด้วยตนเอง อีกทั้งยังจะสร้างเครือข่ายความร่วมมือระหว่าง CII เพื่อสามารถที่จะติดต่อสื่อสารแลกเปลี่ยนข้อมูลแจ้งเตือนไปจนถึงร่วมมือกันรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดย TB-CERT ถือว่ามีบทบาทที่สำคัญภายใต้ พ.ร.บ.ฉบับนี้ในการที่จะช่วยประสานงานกับหน่วยงานภาคการเงินและหน่วยงานที่เกี่ยวข้องเพื่อเตรียมความพร้อม อีกทั้งวิเคราะห์แนวทางการรับมือหรือลดความเสียหายจากภัยคุกคามทางไซเบอร์ ส่วน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ถือเป็นข้อกำหนดที่จำเป็นในการที่จะยกสิทธิให้เจ้าของข้อมูลในการป้องกันดูแลข้อมูลของตนเองที่ถูกนำไปใช้เพื่อประโยชน์เพื่อความสะดวกในการใช้บริการของเจ้าของข้อมูลเอง และยังเป็นการเพิ่มสิทธิในการควบคุมไม่ให้ถูกละเมิดได้ ในขณะเดียวกันก็เป็นการกำหนดมาตรการดูแลข้อมูลส่วนบุคคลให้กับหน่วยงานที่เก็บรักษาข้อมูลส่วนบุคคลนั้นให้สูงขึ้น นั่นก็หมายความว่าจะเป็นการเสริมสร้างมาตรการป้องกันดูแลข้อมูลให้กับทุกหน่วยงานในประเทศ

ด้วยเหตุนี้ การสร้างให้องค์กรมี resilience หรือมีความยืดหยุ่นรับมือกับภัยทางไซเบอร์จึงมีความสำคัญยิ่งยวด โดยเฉพาะในช่วงสภาพการณ์ที่มีความเปลี่ยนแปลงอย่างรวดเร็ว (disruption) ภัยคุกคามทางไซเบอร์มีรูปแบบที่ยากที่จะคาดเดาได้ องค์กรจะต้องมีการเตรียมพร้อมตั้งแต่ระดับนโยบาย การกำหนดบทบาทหน้าที่ความรับผิดชอบ การพัฒนาแผนการรับมือหากเกิดภัยทางไซเบอร์ขึ้น รวมไปถึงจะต้องนำแผนการรับมือนั้นไปซ้อมภายใต้สถานการณ์ต่าง ๆ เพื่อให้ผู้ที่เกี่ยวข้องตั้งแต่ผู้บริหารระดับสูงจนถึงผู้ปฏิบัติงานมีความคุ้นเคยในการตอบสนองรับมือต่อสถานการณ์ภัยคุกคามทางไซเบอร์โดยไม่ตระหนกจนเกินไป ผู้ปฏิบัติงานที่เกี่ยวข้องจะต้องมีทักษะในการจัดการกับปัญหาที่ไปในแนวทางเดียวกัน ผู้บริหารจะต้องสามารถกำหนดทิศทางขององค์กรภายใต้สถานการณ์การคุกคามทางไซเบอร์ได้ ส่งผลให้องค์กรสามารถปรับตัวรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพมากขึ้น

ในปี 2561 TB-CERT ได้เน้นยกระดับในเรื่องของ Incident Response ซึ่งถือเป็นกรอบการดำเนินการตอบสนองต่อเหตุการณ์อย่างมีมาตรฐาน ส่วนกิจกรรมในปี 2562 TB-CERT ได้เน้นที่จะช่วยธนาคารสมาชิกในการเตรียมความพร้อมรับมือภัยไซเบอร์ ให้มี resilience ในระดับขององค์กร ผ่านกิจกรรมที่หลากหลายต่อเนื่องทั้งปี ไม่ว่าจะเป็นการเตรียมความพร้อมให้กับผู้ปฏิบัติงานให้มีทักษะทางเทคนิคในเชิงลึกจากการจัด hands on workshop ไปจนถึงการจัดการแข่งขัน cyber combat และงานสัมมนาที่มุ่งเน้นไปในหัวข้อหลักในเรื่องของการพัฒนา organizational resilience โดยจะเห็นว่าภาคการธนาคารในภาพรวมมีความพร้อมมากขึ้น และด้วยการสนับสนุนจากทางธนาคารแห่งประเทศไทยทำให้เกิดการสร้างตระหนักรู้หรือการให้ความสำคัญในการเตรียมความพร้อมรับมือภัยไซเบอร์ในระดับผู้บริหารระดับสูง ซึ่งเป็นการเติมเต็มองค์ประกอบสำคัญของ organizational resilience development

นอกจากนั้น TB-CERT ยังมีการขยายความร่วมมือกับองค์กรนอกภาคการเงิน ไม่ว่าจะเป็นหน่วยงานด้าน telecommunication หน่วยงานด้านความมั่นคง โดยการเชิญเข้าร่วมกิจกรรมของ TB-CERT เพื่อเสริมสร้างความสัมพันธ์ที่ดี และช่วยกันยกระดับความพร้อมในการเตรียมการป้องกันภัยคุกคามทางไซเบอร์ในวงกว้างขึ้น ซึ่งนอกจากจะเป็นการสนับสนุน พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์แล้ว ยังเป็นการสร้างเครือข่ายของความร่วมมือระหว่างอุตสาหกรรมต่าง ๆ ในประเทศไทย ด้วยภัยทางไซเบอร์มีแนวโน้มที่จะไม่จำกัดขอบเขตเฉพาะอุตสาหกรรมใดอุตสาหกรรมหนึ่ง แต่จะสร้างผลกระทบเชื่อมโยงข้ามอุตสาหกรรมอย่างหลีกเลี่ยงไม่ได้ ฉะนั้นการพัฒนา organizational resilience จึงมีความจำเป็นที่จะต้องขยายขอบเขตสู่ country wide resilience เพื่อให้มีความพร้อมรับมือภัยไซเบอร์ในระดับประเทศต่อไป

ดร.กิตติ โฆษะวิสุทธิ์
ประธานกรรมการ TB-CERT

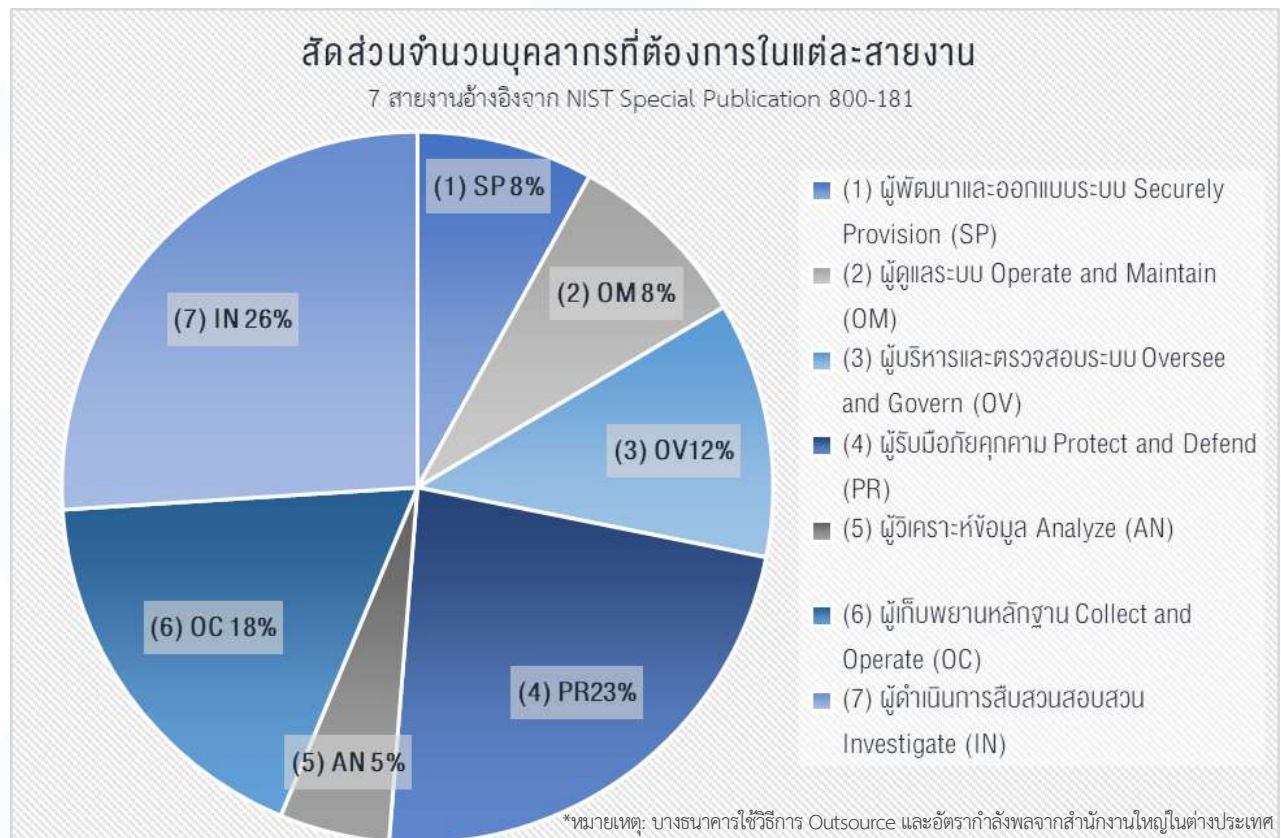
บทวิเคราะห์บุคลากรด้าน Cybersecurity ภาคการธนาคาร

ปัญหาเรื่องการขาดแคลนบุคลากรด้านไอที ไม่ว่าจะเป็นไอทีทั่วไป หรือเจาะลึกไปถึงไอทีซีเคียวริตี้ มีเพิ่มมากขึ้น เนื่องจากความต้องการของตลาดที่เพิ่มขึ้นอย่างก้าวกระโดด ซึ่งคงเป็นผลสืบเนื่องมาจากการที่สังคมในปัจจุบันได้ก้าวเข้าสู่ยุคดิจิทัลและการพัฒนาเทคโนโลยีก็รุดหน้าไปมาก ทำให้หลาย ๆ องค์กร เริ่มมีการปรับตัวเพื่อให้ทันยุคทันสมัย สร้างความสะดวกสบายให้กับลูกค้า และเพิ่มประสิทธิภาพการทำงานบริษัทลูกค้า สำหรับธนาคารเองก็เช่นกัน บางธนาคารได้ปรับโครงสร้างองค์กรใหม่ เช่น ให้มีหน่วยงานที่ดูแลเกี่ยวกับดิจิทัลโดยเฉพาะ ส่งผลให้บุคลากรด้านไอทีและไอทีซีเคียวริตี้ในตลาดขาดแคลน



TB-CERT ได้ร่วมกับธนาคารแห่งประเทศไทย จัดทำการสำรวจความต้องการงานบุคลากรในด้าน ไอทีและไอทีซีเคียวริตี้ รวมถึง Cybersecurity ด้วย จากผลสำรวจพบว่า ภาคการธนาคารต้องการบุคลากรในด้าน ไอทีและ Cybersecurity เป็นจำนวนมาก ในขณะที่ทักษะที่ทางภาคการธนาคารต้องการนั้น ในมหาวิทยาลัยยังไม่มีหลักสูตรรองรับ จึงทำให้เด็กที่จบใหม่ด้านคอมพิวเตอร์ และวิศวกรรมคอมพิวเตอร์ ICT ยังไม่สามารถทำงานได้เลยทันทีหลังเรียนจบ ประกอบกับงานด้านนี้ในสถาบันการเงินมีความซับซ้อนและมีความสำคัญกับบริการโดยตรงภายใต้สภาพการแข่งขันทางธุรกิจที่เร่งรัด จึงมีความต้องการบุคลากรที่มีประสบการณ์ หนึ่งในภารกิจหลักของ TB-CERT จึงจำเป็นต้องพัฒนาบุคลากรทั้งที่ทำงานแล้วและจบใหม่ให้มีศักยภาพและรองรับความต้องการของตลาดได้ แม้จะยังไม่ตอบโจทย์ในปัจจุบันได้ทันทีแต่ก็จะช่วยพัฒนาบุคลากรเข้าสู่งานสายไอทีของภาคการธนาคารได้ทันความต้องการของตลาดในอนาคต

จากการสำรวจ ความต้องการบุคลากรด้านไอทีและ Cybersecurity จากธนาคารสมาชิก TB-CERT จำนวน 22 ธนาคาร พบว่าอัตราความต้องการบุคลากรเทียบกับที่มีในปัจจุบันเพิ่มขึ้นคิดเป็น 12% โดยได้แบ่งหมวดหมู่ของกลุ่มสายงานตาม NIST Special Publication 800-181 เป็น 7 สายงาน และผลสำรวจ 3 ลำดับแรกที่มีความต้องการมากที่สุด ได้แก่ (1) ผู้ดำเนินการสืบสวนสอบสวน (IN) 26% (2) ผู้รับมือภัยคุกคาม Protect and Defend (PR) 23% และ (3) ผู้เก็บพยานหลักฐาน Collect and Operate (OC) 18% ตามลำดับ



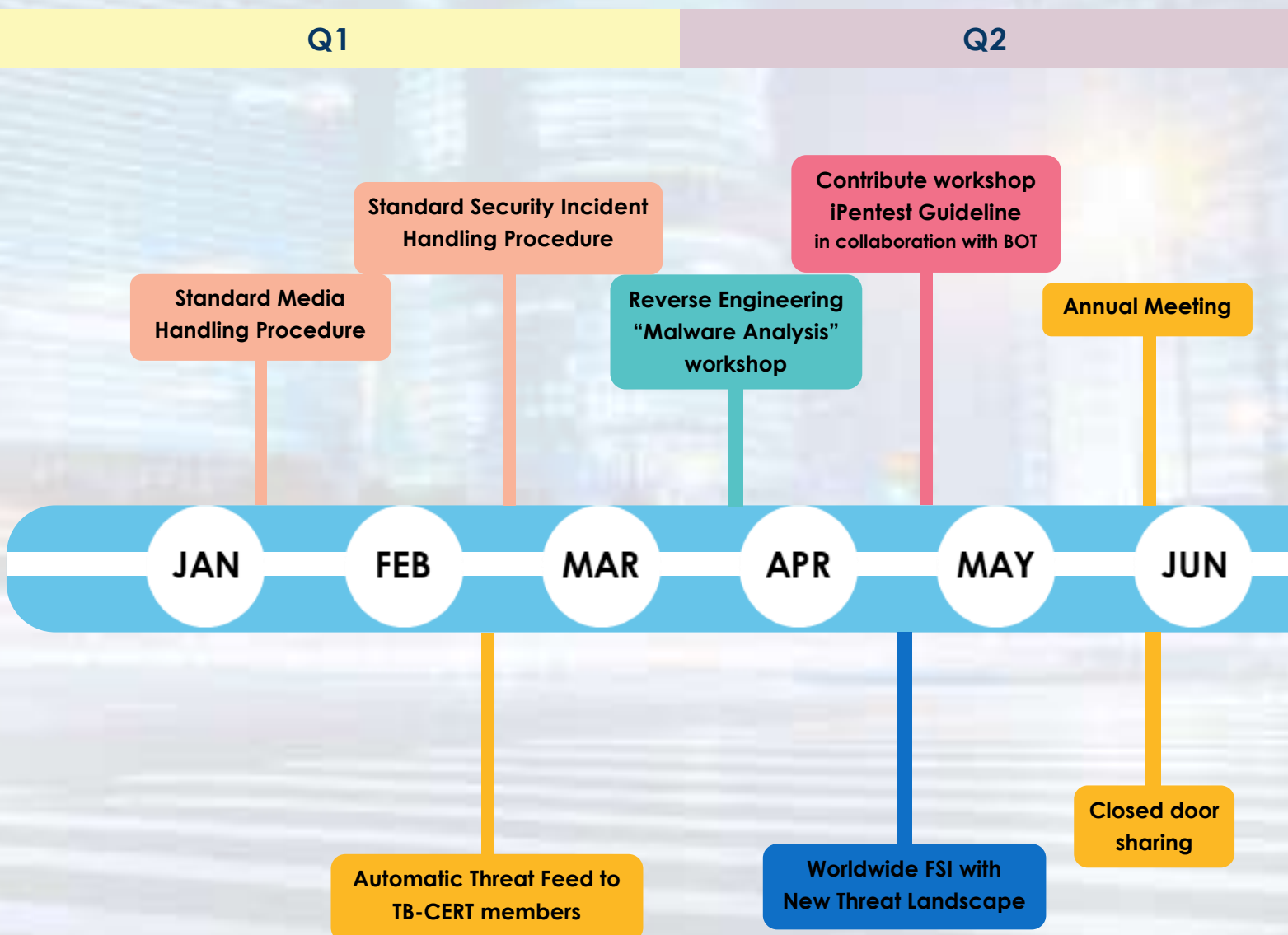
รูปที่ 1 แสดงสัดส่วนจำนวนบุคลากรที่ต้องการในแต่ละสายงาน



รูปที่ 2 แสดงประเภทสายงานด้าน Cybersecurity ตาม NIST Special Publication 800-181

กิจกรรมในปี 2562

ตลอด 3 ปี ที่ผ่านมา TB-CERT พัฒนาศักยภาพของสมาชิกอย่างต่อเนื่อง เราได้เน้นการสร้างรากฐานของ TB-CERT ให้มีความมั่นคงแข็งแรงเพื่อให้สมาชิกมีกรอบในการแลกเปลี่ยนข้อมูลอย่างไว้วางใจซึ่งกันและกัน รวมถึงการยกระดับความมั่นคงปลอดภัยไซเบอร์ให้กับทุกภาคส่วนของหน่วยงานสมาชิก โดยการพัฒนาศักยภาพ สร้างความตระหนักรู้ให้กับสาธารณะ สร้างมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้ทุกภาคส่วนมีหลักการหลักปฏิบัติร่วมกัน และพยายามสร้างพลักดันการสร้างวัฒนธรรมองค์กรให้มี Resilience ผ่านกิจกรรมต่าง ๆ ดังนี้





People Development: การพัฒนาบุคลากรด้าน Cybersecurity ของภาคธนาคาร อาทิ การจัดอบรม การชักจูง
รับมือภัยไซเบอร์



Standardize: การกำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคธนาคาร



Awareness: การสร้างความตระหนักถึงภัยคุกคามด้าน Cybersecurity แก่สมาชิก ผู้บริหารของหน่วยงานสมาชิก
ลูกค้า และสื่อมวลชน



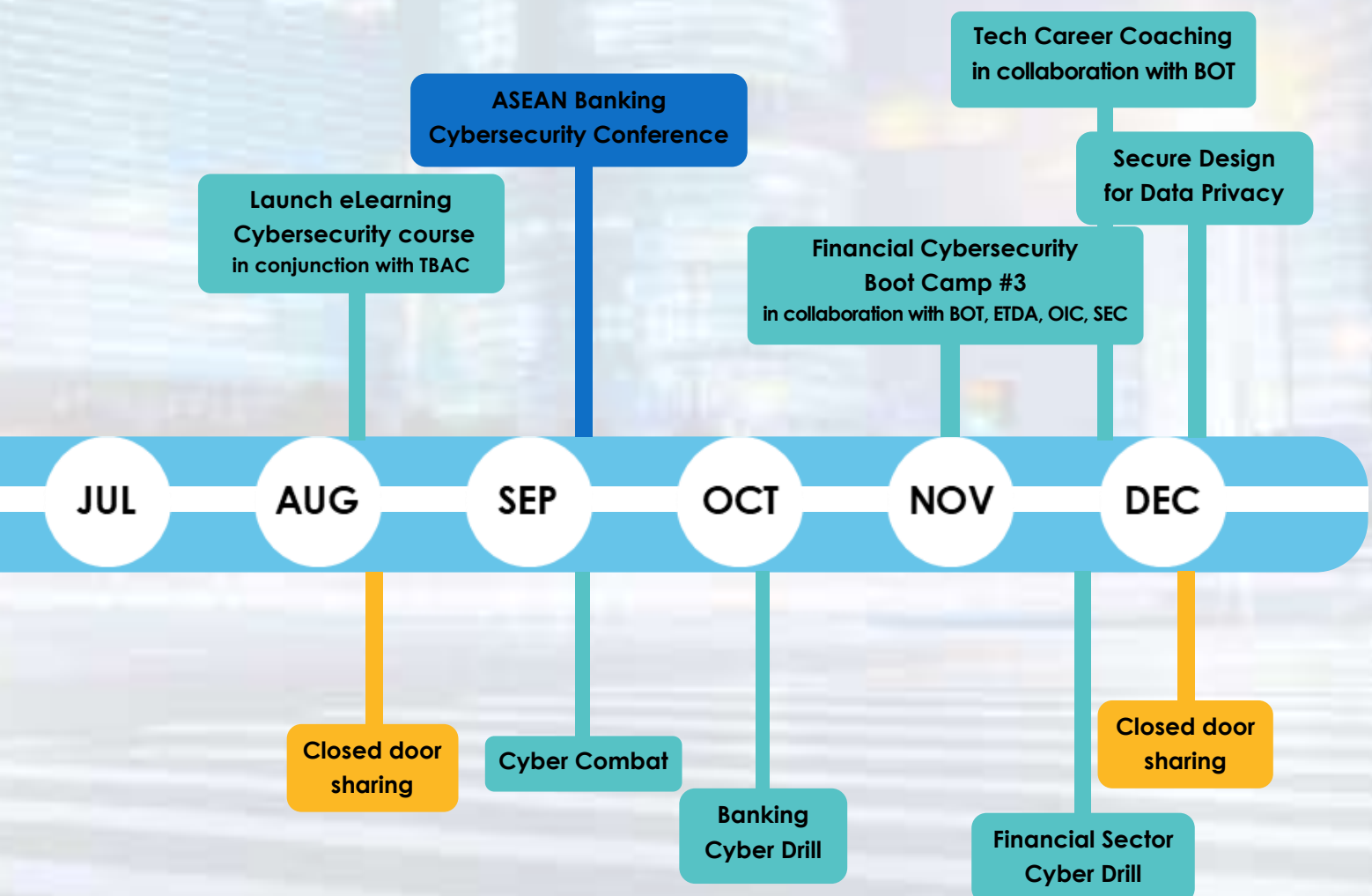
Research & Development: การบริหารจัดการและสร้างองค์ความรู้ด้าน Cybersecurity



Services: Alert & Warning, Incident Handling Recommendation, Incident Response Coordination

Q3

Q4



TB-CERT Activities 2019

การพัฒนาบุคลากร (Human Resource Development)



Cybersecurity Development Program

Reverse Engineering “Malware Analysis” workshop

28-29 March 2019, Bangkok Bank Rama 3

Reverse Engineering “Malware Analysis” เป็นการอบรมเชิงปฏิบัติการต่อเนื่อง 2 วัน โดยวิทยากรบริษัท Group IB Mr. Vitaliy Trifonovs ในวันแรกผู้เข้าอบรมได้เรียนรู้เกี่ยวกับ Theory of Reverse Engineering และวันที่สองเป็นการลงมือปฏิบัติในหัวข้อ Dynamic and Static Malware Analysis

Cybersecurity Development Program



Secure Design for Data Privacy

17 December 2019, National Credit Bureau Head Office

การสัมมนา Secure Design for Data Privacy TB-CERT ได้รับเกียรติจากวิทยากร คุณณฤศม รุ่งศิริวงศ์ ผู้อำนวยการอาวุโส หัวหน้าฝ่าย IT Security ธนาคารเกียรตินาคิน ที่ได้มาให้ความรู้เกี่ยวกับแนวคิด Privacy by Design แนวทางในการออกแบบเพื่อการจัดเก็บข้อมูลส่วนบุคคล เพื่อให้รองรับกับกรอบของกฎหมายคุ้มครองข้อมูลส่วนบุคคล และ GDPR พื้นฐานการออกแบบด้าน Information Security รวมทั้ง Design Pattern ที่สามารถนำไปใช้ได้

TB-CERT Cyber Combat



Cyber Combat

6 September 2019, The Athenée—A Luxury Collection Hotel

การแข่งขันการแข่งขัน Cyber Combat จัดขึ้นต่อเนื่องเป็นครั้งที่ 2 เพื่อพัฒนาทักษะของผู้ปฏิบัติงานด้านการป้องกันภัยไซเบอร์โดยมีผู้เข้าแข่งขันจากภาคการธนาคาร โทรคมนาคม และหน่วยงานความมั่นคง รวม 30 ทีม



Banking Cyber Drill Hybrid Exercise

Banking Cyber Drill

2 October 2019, Bank of Thailand Learning Center

การซ้อมรับมือภัยไซเบอร์ภาคการธนาคาร หรือ Banking Cyber Drill จัดขึ้นต่อเนื่องเป็นครั้งที่ 4 มีวัตถุประสงค์ดังนี้

- เพื่อยกระดับการซ้อมรับมือภัยไซเบอร์ ให้ผู้บริหารได้มีปฏิสัมพันธ์กับผู้ปฏิบัติงาน โดยจำลองสถานการณ์การซ้อมให้มีการร่วมกันตัดสินใจแก้ไขสถานการณ์
- เพื่อประเมินทักษะในการวิเคราะห์การโจมตีทางไซเบอร์ การประเมินแนวทางแก้ไขและป้องกันเหตุ
- เพื่อซักซ้อมการตอบสนองต่อเหตุการณ์แจ้งเตือนภัยคุกคามที่ได้รับจากระบบ Threat Intelligence
- เพื่อซักซ้อมขั้นตอนการตอบสนองต่อเหตุการณ์ผิดปกติจากการโจมตีทางไซเบอร์ กระบวนการประสานงาน ทั้งภายในหน่วยงาน ระหว่างหน่วยงานกับ TB-CERT หรือกับหน่วยงานภายนอกและสาธารณะ
- เพื่อพัฒนาระบบการรับมือภัยไซเบอร์ให้มีประสิทธิภาพ เหมาะสมกับภาคการธนาคาร รวมทั้งเสริมสร้างความร่วมมือระหว่างธนาคารสมาชิกและ TB-CERT

โดยในปีนี้เป็น การซักซ้อมในรูปแบบ Hybrid Exercise แบ่งการซักซ้อมออกเป็น 2 ส่วน คือ

1. ช่วงเช้า เป็นการฝึกซ้อมของทีมปฏิบัติงาน มีผู้เข้าร่วมงาน 124 คนจากองค์กรสมาชิก TB-CERT
2. ช่วงบ่าย เป็นการฝึกซ้อมของทีมบริหาร มีผู้เข้าร่วมงาน 131 คนจากองค์กรสมาชิก TB-CERT และหน่วยงานที่เกี่ยวข้อง

#FincybersecTH2019

Financial Cybersecurity Boot Camp #3

1-3 November 2019,
Bank of Thailand Learning Center

TB-CERT สมาคมธนาคารไทย ร่วมกับหน่วยงานภายใต้บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจ การเงิน การลงทุน และการประกันภัย ได้แก่ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จัดโครงการ Financial Cybersecurity Boot Camp ครั้งที่ 3 โดยมีวัตถุประสงค์เพื่อเพิ่มโอกาสในการพัฒนาทักษะด้าน Cybersecurity และเป็นการสร้างเครือข่ายบุคลากรรุ่นใหม่ที่มีความสนใจงานด้าน Cybersecurity ในภาคการเงิน รวมทั้งฝึกทักษะผ่านการแข่งขันทั้งในด้านการโจมตีและป้องกันระบบ ซึ่งในปีนี้มีผู้เข้าร่วมโครงการจำนวน 17 ทีม รวมทั้งสิ้น 64 คน ส่วนใหญ่กำลังศึกษาระดับปริญญาตรีชั้นปีที่ 3 และปีที่ 4 จากผู้สมัครทั้งสิ้น 30 ทีม รวม 109 คน



Tech Career Coaching

30 November 2019, Krungsri Ploenchit Office

TB-CERT ร่วมกับธนาคารแห่งประเทศไทย และฝ่ายบุคลากรของ 15 ธนาคารสมาชิกสมาคมธนาคารไทย ในการจัดงานแนะแนวอาชีพด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นโครงการต่อเนื่องจาก Financial Cybersecurity Boot Camp โครงการ Tech Career Coaching ได้จัดขึ้นเป็นครั้งแรก มีวัตถุประสงค์เพื่อให้องค์กรภาคการเงินได้มีโอกาสให้ข้อมูลด้านวิชาชีพ การฝึกงาน และทุนการศึกษาด้าน IT และเป็นการสร้างเครือข่ายระหว่างฝ่ายบุคลากรขององค์กรภาคการเงินในการสร้างบุคลากรใหม่ด้าน IT เข้าสู่ภาคการเงินร่วมกัน ผ่านเวทีเสวนา และบูธให้คำปรึกษาจากองค์กรภาคการเงิน การจัดงานดังกล่าวได้รับการตอบรับเป็นอย่างดีจากผู้เข้าร่วมงานกว่า 250 คน ซึ่งมาจากผู้เข้าร่วมโครงการ Financial Cybersecurity Boot Camp จำนวน 24 คน

#TechCareerCoaching



การสร้างความตระหนักรู้และเข้าใจภัยไซเบอร์ (Awareness Building)

Executive Banking Forum: Worldwide FSI with New Threat Landscape

25 April 2019, Intercontinental Hotel Bangkok



งานสัมมนา Worldwide FSI with New Threat Landscape ในครั้งนี้ ได้จัดขึ้นสำหรับผู้บริหารสายงานเทคโนโลยี รวมทั้งหัวหน้าฝ่ายด้านการรักษาความปลอดภัยของระบบและข้อมูลของหน่วยงานสมาชิก โดยได้รับเกียรติจากผู้เชี่ยวชาญบริษัท FireEye ซึ่งเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ มาบรรยายแลกเปลี่ยนมุมมองด้านความซับซ้อนของภัยคุกคามในปัจจุบัน แนวทางในการป้องกัน ตรวจสอบ และรับมือกับภัยคุกคาม รวมทั้งกรณีศึกษาจากธนาคารต่างประเทศ

Building A Resilient Organizational Culture

ASEAN Banking Cybersecurity Conference

6 September 2019, The Athenae Hotel-A Luxury Collection Hotel

งานสัมมนาประจำปี ASEAN Banking Cybersecurity Conference จัดขึ้นภายใต้หัวข้อหลัก “Building A Resilient Organizational Culture” เพื่อเป็นการพัฒนาบุคลากรให้มีความตระหนักในเรื่องของ Cyber Resilience โดยแบ่งการจัดงาน

ออกเป็น 2 ส่วน ได้แก่ งานสัมมนาเชิงวิชาการ ประกอบด้วยหัวข้อสัมมนาทั้งด้าน Technical และ Management รวมถึงการแสดงผล solution จากบริษัทผู้สนับสนุน ซึ่งมีผู้สนใจเข้าร่วมงานกว่า 400 คน จากภาคการเงินการธนาคาร ทั้งในประเทศไทยและอาเซียน รวมทั้งหน่วยงานด้านการลงทุนและการประกันภัย



กล่าวต้อนรับและกล่าวเปิดงานโดย คุณชาติศิริ โสภณพนิช ที่ปรึกษาสมาคมธนาคารไทย และ ดร.วิโรฒ สันติประภพ ผู้ว่าการธนาคารแห่งประเทศไทย



การวิจัยและการพัฒนามาตรฐานด้านไซเบอร์ (Research and Development)

iPentest Guideline Workshop

26 April 2019, Bank of Thailand Learning Center



TB-CERT ร่วมกับธนาคารแห่งประเทศไทย ในการจัดทำแนวปฏิบัติการทดสอบเจาะระบบแบบ Intelligence-led (Intelligence-led Penetration Testing Guideline: iPentest) ซึ่งเป็นการทดสอบเจาะระบบในลักษณะเสมือนจริงหรือ Red Teaming ตามมาตรฐานสากล เพื่อยกระดับความพร้อมของสถาบันการเงินในการป้องกันและรับมือภัยคุกคามไซเบอร์ ให้มีการป้องกันที่แข็งแกร่ง ตรวจสอบภัยคุกคามทางไซเบอร์ได้ทันการณ์ สามารถตอบสนองต่อเหตุการณ์และกู้คืนระบบและบริการได้รวดเร็ว รวมทั้งได้จัดให้มีการอบรมเพื่อสร้างความรู้ความเข้าใจในเรื่องดังกล่าว

การแชร์ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์และสร้างความสัมพันธ์ระหว่างสมาชิก

Annual Meeting

24-26 May 2019, Siam Commercial Bank Training Center, Chonburi



TB-CERT ได้จัดงานประชุมสมาชิกประจำปี ซึ่งเป็นกิจกรรมกลุ่มสัมพันธ์เชิงวิชาการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นการระดมสมองและวางแผนงานประจำปีของ TB-CERT การแชร์ความรู้ทางเทคนิค ให้สมาชิกได้มีโอกาสนพบปะ ทำกิจกรรม และเสริมสร้างความสัมพันธ์ระหว่างสมาชิกอีกด้วย



**THE MOMENT
WE SHARE**

เหตุการณ์สำคัญด้านภัยไซเบอร์ในปี 2562



สรุปเหตุการณ์โลกที่น่าสนใจตามทวีปต่าง ๆ ในปี 2562

America

8 กุมภาพันธ์ บริษัท Credit Union หลายแห่งใน US ถูกโจมตีด้วย Spear phishing โดยหลอกลวงส่งมาจากเจ้าหน้าที่ compliance จาก Credit Union อื่น และส่งมาในลักษณะของไฟล์ PDF ที่แนบลิงก์อันตราย อย่างไรก็ตามไม่พบรายงานว่าได้รับความเสียหายจากอีเมลดังกล่าว

13 พฤษภาคม ธนาคาร FirstBank ในโคลราโด ประสบเหตุการณ์ข้อมูลบัตรเครดิตของลูกค้ารั่วไหล ส่งผลให้มีการยกเลิกและแจกจ่ายบัตรเครดิต

24 พฤษภาคม First American Financial Corp. ถูกขโมยข้อมูลเอกสารจำนวน 885 ล้านไฟล์ ที่เกี่ยวข้องกับโฉนดที่ดิน และข้อมูลส่วนบุคคล

29 กรกฎาคม ข้อมูลใบสมัครบัตรเครดิตของ Capital One ประมาณ 100 ล้านใบ รั่วไหล เนื่องจากการถูกแฮกเซิร์ฟเวอร์บนคลาวด์

25 กรกฎาคม ข้อมูลส่วนบุคคลและข้อมูลทางการเงินของสถาบันการเงิน Banco Pan ในบราซิลรั่วไหล ขนาดไฟล์ 250 GB ซึ่งทางสถาบันการเงินได้ประกาศว่าข้อมูลดังกล่าวพอร์ทเนอร์ทางการเงินเป็นเจ้าของข้อมูล

20 มิถุนายน ข้อมูลส่วนบุคคลสมาชิกสหกรณ์ที่ให้บริการด้านการเงินของ Desjardins Group แคนาดา จำนวน 2.9 ล้านรายรั่วไหล โดยอดีตพนักงานขโมยออกไป

4 เมษายน หน่วยงานบังคับใช้กฎหมายเม็กซิโกจับกุมกลุ่มอาชญากรชาวโรมาเนีย ผู้อยู่เบื้องหลังปฏิบัติการ ATM Skimming ในเม็กซิโก

10 มกราคม Redbanc เครือข่าย ATM ของประเทศชิลีถูกโจมตีโดยหลอกลวงให้พนักงานดาวน์โหลดมัลแวร์ระหว่างการสัมภาษณ์งาน หลอกลวงผ่าน Skype

จากเหตุการณ์แนวโน้มการโจมตีสถาบันการเงินในทวีปอเมริกา เป็นการโจมตีเพื่อขโมยข้อมูลเป็นสำคัญ โดยส่วนใหญ่จะเป็นข้อมูลส่วนบุคคลของลูกค้าโดยเทคนิคของ social engineering เช่น phishing หรือการส่งไฟล์แนบที่มีมัลแวร์ไปกับอีเมลก็ยังเป็นเทคนิคที่ยังคงใช้งานได้ดี อีกทั้งในบางเหตุการณ์นั้นเกิดจากผู้ดูแลระบบปรับแต่งค่าการป้องกันการเข้าถึงที่ผิดพลาด ทำให้แฮกเกอร์สามารถเข้าถึงฐานข้อมูลที่อยู่กับผู้ให้บริการคลาวด์ภายนอกได้อย่างง่ายดาย ส่วนเหตุการณ์การโจมตีบริการ ATM ก็ยังพบอยู่แต่จะมีวิธีการที่เปลี่ยนแปลงไป โดยหันไปมุ่งโจมตีไปยังบริษัทผู้ให้บริการเครือข่าย ATM โดยมีเหตุการณ์หนึ่งที่เกิดขึ้นในประเทศชิลีซึ่งเป็นฝีมือของกลุ่มแฮกเกอร์ Lazarus จุดเริ่มต้นของการโจมตีอยู่ที่พนักงานของบริษัท Redbanc ได้ทำการสมัครงานผ่าน LinkedIn ในตำแหน่ง Developer พนักงานดังกล่าวถูกหลอกลวงให้ดาวน์โหลดและเปิดไฟล์แนบชื่อ ApplicationPDF.exe โดยถูกหลอกลวงว่าเป็นแอปพลิเคชันที่ช่วยในการสร้าง Resume ในรูปแบบของบริษัทที่สมัครงาน ซึ่งภายหลังมีการวิเคราะห์พบว่าเป็นมัลแวร์ชื่อ PowerRatankba และมัลแวร์นี้ได้รวบรวมข้อมูลต่าง ๆ ในเครื่องและส่งกลับไปยังเซิร์ฟเวอร์ ได้แก่ รายละเอียดของระบบปฏิบัติการ การตั้งค่า Proxy รายการ Process ปัจจุบัน การเชื่อมต่อ RPC และ SMB รวมถึงสถานะของการเชื่อมต่อ RDP ด้วย หลังจากนั้นเมื่อแฮกเกอร์สามารถเข้าถึงเครื่องดังกล่าวได้แล้วได้ดำเนินการในขั้นตอนต่อ ๆ ไปเพื่อขโมยเงิน

Europe

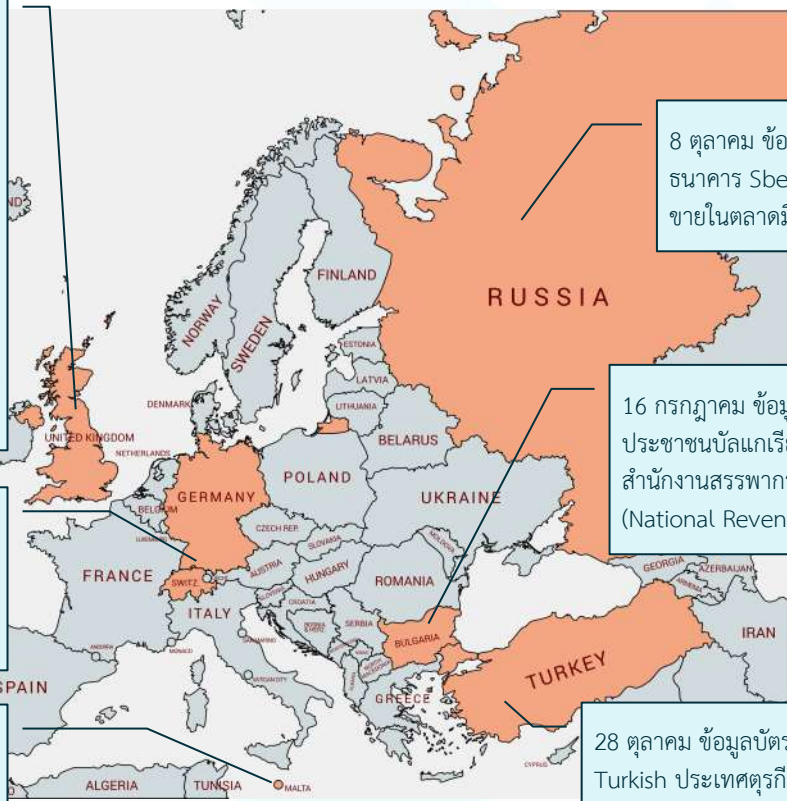
2 กุมภาพันธ์ ธนาคาร Metro ถูกดักข้อความผ่านโปรโตคอล SS7 สำหรับยืนยันตัวตน 2 ปัจจัย ที่ใช้ยืนยันธุรกรรมของลูกค้า

22 มีนาคม บัญชีลูกค้าของ Royal Bank of Scotland (RBS) มีข้อบกพร่องด้านความปลอดภัยหลังจากแนะนำบริการรักษาความปลอดภัยลูกค้าใหม่

14 สิงหาคม ข้อมูลไบโอเมทริกซ์ เช่น ลายนิ้วมือ และใบหน้าของผู้ใช้จำนวน 27.8 ล้านรายการ สำหรับควบคุมการเข้าออกอาคารของบริษัท Suprema รัสเซีย

2 พฤษภาคม แบงค์กิงโทรจัน Retefe ระบาดในประเทศสวิตเซอร์แลนด์และเยอรมนี โดยเครื่องที่ติดแบงค์กิงโทรจันนี้จะถูกติดตั้ง TOR และเชื่อมต่อไปยังเว็บไซต์ปลอมของธนาคาร

13 กุมภาพันธ์ ธนาคาร Bank of Valletta (BOV) ประเทศ Malta หยุดทำงานหลังจากถูกพยายามขโมยเงินกว่า 13 ล้านยูโร



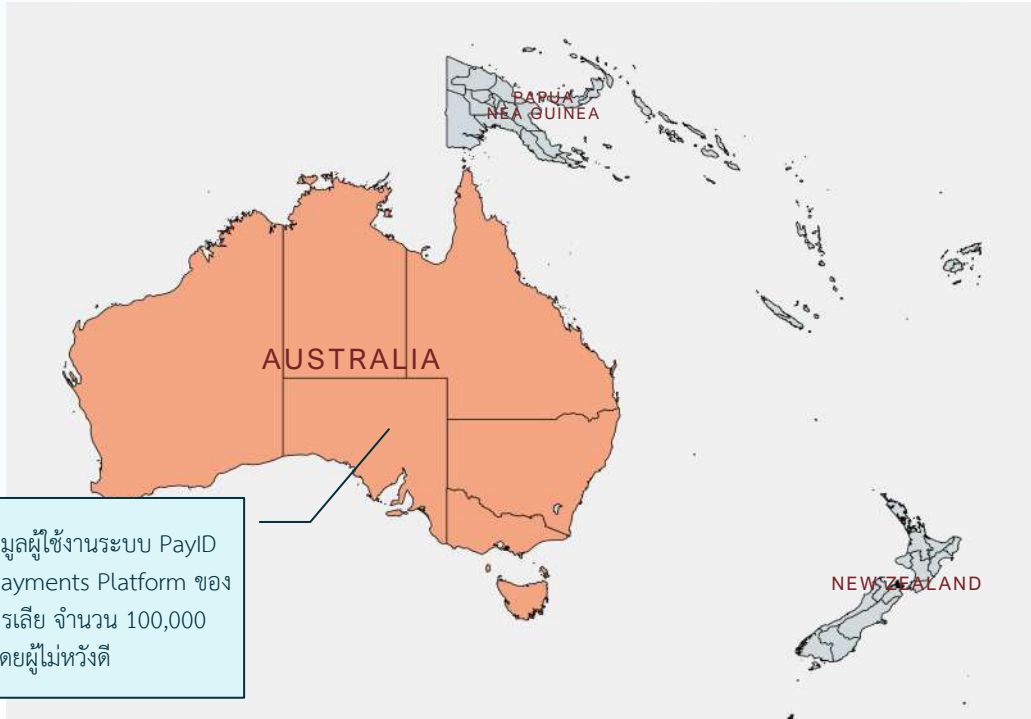
8 ตุลาคม ข้อมูลของลูกค้าธนาคาร Sberbank รัสเซีย และขายในตลาดมืดกว่า 60 ล้านราย

16 กรกฎาคม ข้อมูลด้านการเงินของประชาชนบัลแกเรียรั่วไหลจากสำนักงานสรรพากรแห่งชาติบัลแกเรีย (National Revenue Agency)

28 ตุลาคม ข้อมูลบัตรเครดิตธนาคาร Turkish ประเทศตุรกี จำนวน 460,000 รายการถูกขายบน Darkweb

เหตุการณ์ด้านความปลอดภัยสารสนเทศที่พบในทวีปยุโรปส่วนใหญ่เป็นภัยคุกคามที่เกี่ยวข้องกับข้อมูลรั่วไหล เช่นกันกับทวีปอเมริกา แม้ว่าจะมีเหตุการณ์ที่ข้อมูลถูกขโมยจากระบบคลาวด์น้อยกว่าของทวีปอเมริกาก็ตาม ข้อมูลส่วนบุคคลของลูกค้าสถาบันการเงินที่ถูกขโมยแล้ว ยังมีข้อมูล Biometrics เช่น ลายนิ้วมือและใบหน้ารั่วไหลอีกด้วย ซึ่งข้อมูลประเภทนี้ต้องให้ความสำคัญเนื่องจากข้อมูลดังกล่าวไม่สามารถถูกเปลี่ยนแปลงได้ โดยใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562 ของไทยหรือ GDPR – General Data Protection Regulation ของ EU ยังระบุให้ข้อมูล Biometrics นี้เป็นข้อมูลประเภทอ่อนไหว (Sensitive information) ต้องให้การคุ้มครองป้องกันเป็นพิเศษเพื่อมิให้เกิดผลกระทบกับเจ้าของข้อมูล นอกจากนี้ยังมีเหตุการณ์ที่แฮกเกอร์พยายามขโมยเงินจากธนาคาร Bank of Valletta (BOV) ประเทศ Malta จำนวน 13 ล้านยูโร ถึงแม้ว่าความพยายามครั้งนี้จะไม่ประสบความสำเร็จ แต่ก็ทำให้ธนาคารหยุดให้บริการ ซึ่งสร้างความเสียหายให้แก่ธนาคาร

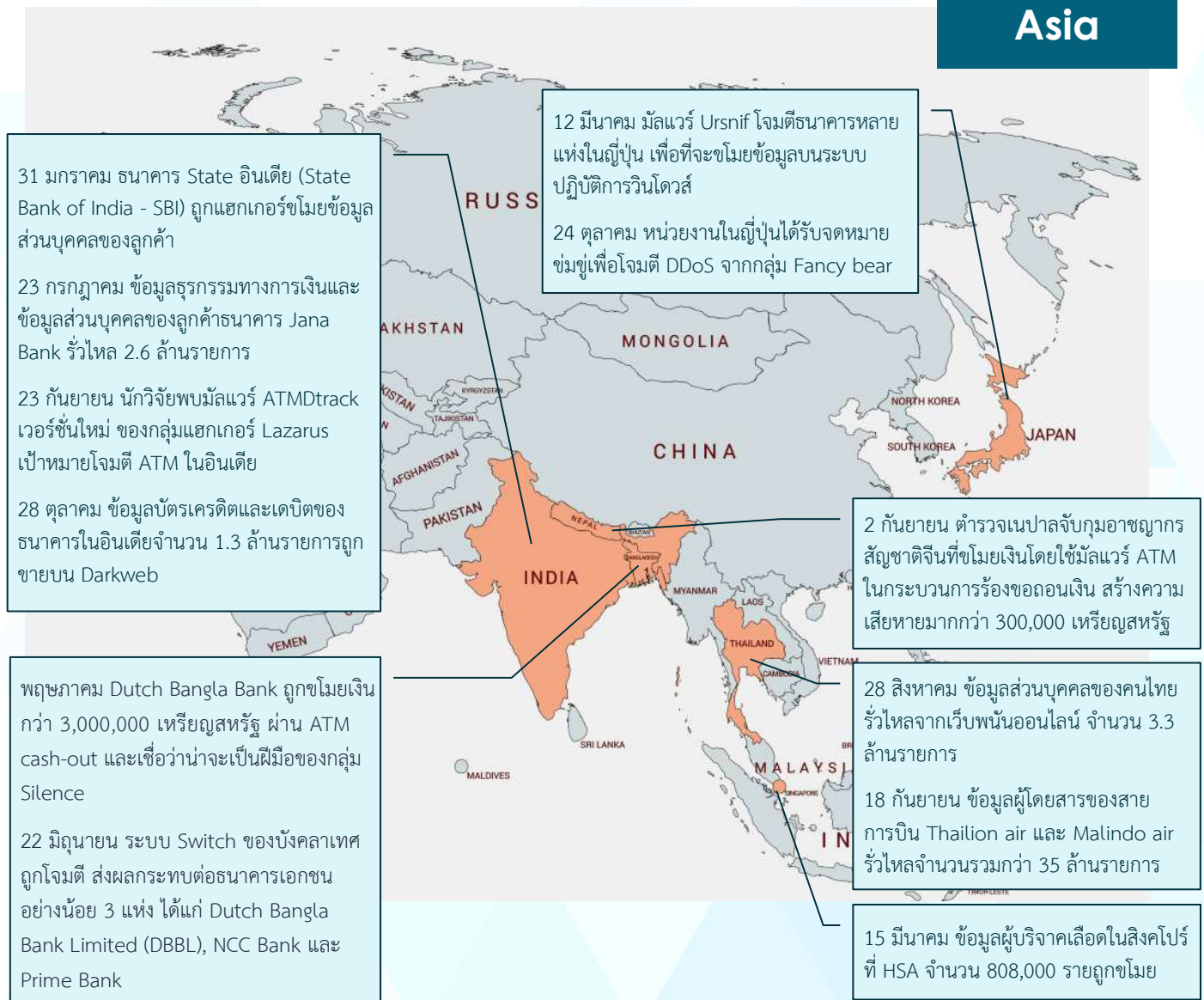
Australia



3 มิถุนายน ข้อมูลผู้ใช้งานระบบ PayID ซึ่งเป็น New Payments Platform ของประเทศออสเตรเลีย จำนวน 100,000 ราย ถูกเข้าถึงโดยผู้ไม่หวังดี

ในประเทศออสเตรเลียพบเหตุการณ์ข้อมูลผู้ใช้งาน PayID ซึ่งเป็นแพลตฟอร์มการโอนเงินของประเทศออสเตรเลีย (New Payments Platform - NPP) ที่อนุญาตให้โอนเงินด้วยหมายเลขโทรศัพท์หรืออีเมล (คล้ายกับระบบพร้อมเพย์ของประเทศไทย) โดยผู้ไม่หวังดีจะทำการโอนเงินโดยใช้หมายเลขโทรศัพท์หรืออีเมลที่ต้องการทราบข้อมูล จากนั้นระบบจะแจ้งข้อมูลส่วนบุคคลของผู้ที่รับโอนเงินกลับมา อย่างไรก็ตามทางธนาคาร CUA – Credit Union Australia ได้ประกาศถึงผลกระทบว่า ข้อมูลชื่อเต็ม หมายเลขโทรศัพท์มือถือ และเลขบัญชีธนาคารถูกเข้าถึงด้วยวิธีดังกล่าว จากข้อมูลที่ถูกเก็บรวบรวมด้วยวิธีดังกล่าวผู้ไม่หวังดีจะใช้ข้อมูลนั้นมาใช้ในการส่งอีเมล phishing หรือโทรติดต่อเพื่อหลอกข้อมูลอื่น ๆ เพิ่มเติมก่อนดำเนินการสร้างความเสียหายในรูปแบบอื่น ๆ ต่อไป

Asia



ในปี 2562 ที่ผ่านมา หน่วยงานและสถาบันการเงินในทวีปเอเชียถูกโจมตีจากกลุ่มแฮกเกอร์ต่าง ๆ โดยแฮกเกอร์มักจะเลือกเป้าหมายโจมตีเป็นประเทศอินเดีย โดยส่วนใหญ่จะเป็นการขโมยข้อมูลด้วยการสร้างมัลแวร์ ATMDtrack เพื่อโจมตี ATM นอกจากนี้ธนาคารในบังคลาเทศเองก็ถูกขโมยเงินกว่า 3,000,000 เหรียญสหรัฐผ่านตู้ ATM ซึ่งเชื่อว่าเป็นฝีมือของกลุ่มแฮกเกอร์ที่ชื่อ Silence ส่วนในประเทศญี่ปุ่นพบมัลแวร์ Ursnif ที่โจมตีธนาคารหลายแห่งและมีเหตุการณ์ที่กลุ่มแฮกเกอร์ Fancy Bear ส่งอีเมลข่มขู่เพื่อที่จะโจมตีแบบ DDoS หากไม่จ่ายเงินด้วย ในเหตุการณ์นั้นทำให้ JPCERT/CC (CERT ประเทศญี่ปุ่น) ได้ออกมาประกาศแจ้งเตือน แต่ในเหตุการณ์ครั้งนั้นไม่ได้รับรายงานแจ้งความเสียหาย

สำหรับประเทศไทยนั้น ถึงแม้ว่าธนาคารและสถาบันการเงินในประเทศไทยจะไม่เกิดเหตุการณ์ถูกโจมตีจนทำให้เกิดผลกระทบโดยตรง แต่ก็มีเหตุการณ์ข้อมูลรั่วไหลจากเว็บพนันออนไลน์ และเว็บสายการบิน ซึ่งเป็นข้อมูลส่วนบุคคลที่รั่วไหลออกไปและบุคคลเหล่านั้นก็เป็นลูกค้าธนาคาร จึงอาจจะทำให้มีผู้ไม่หวังดีใช้ข้อมูลดังกล่าวแอบอ้างเพื่อหลอกลวงเป็นเจ้าของข้อมูลและมาทำธุรกรรมกับธนาคาร ซึ่งถือเป็นการสร้างผลกระทบทางอ้อมแก่ธนาคาร

วิเคราะห์เหตุการณ์ในปี 2562 เทียบกับปี 2561



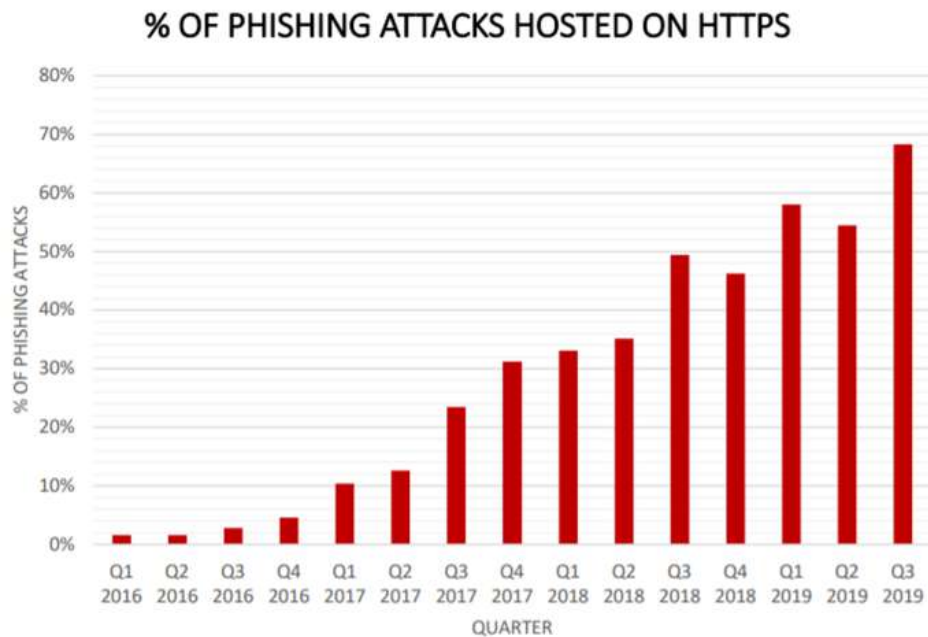
ในปี 2562 มีเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับภาคการธนาคารทั่วโลก โดยเมื่อเปรียบเทียบกับปี 2561 มีความเปลี่ยนแปลงดังนี้

1. พิชชิ่งที่ตรวจจับและปิดกั้นได้ยากขึ้น

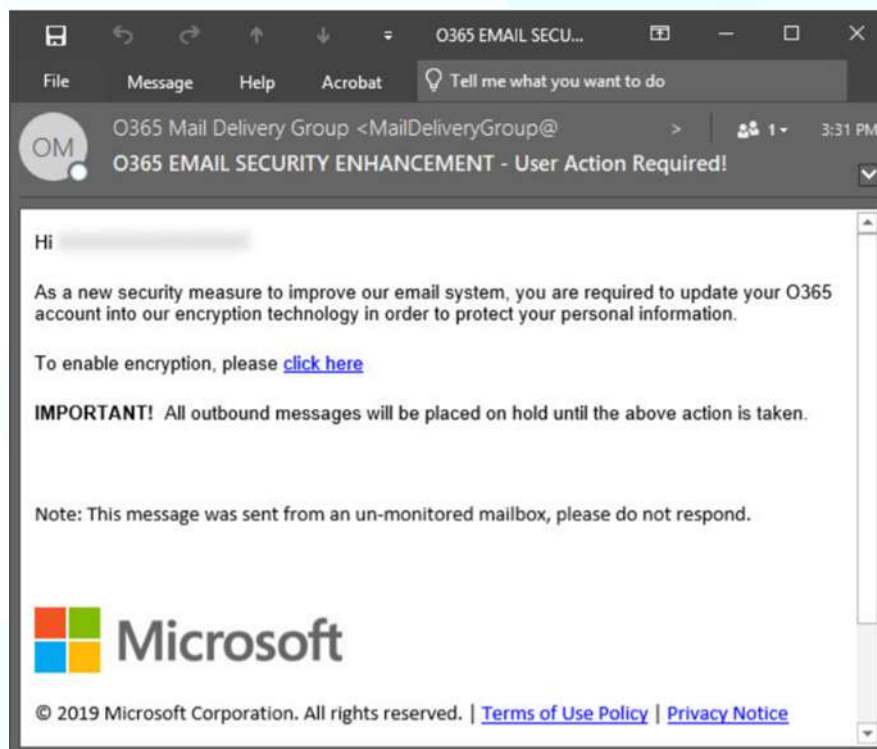
จากรายงานเหตุการณ์พิชชิ่งที่เกี่ยวข้องกับธนาคารในประเทศไทยที่ TB-CERT ได้รับแจ้งมานั้นพบว่าปริมาณเว็บไซต์พิชชิ่งที่มีการใช้ https เพื่อให้เว็บไซต์นั้นดูน่าเชื่อถือมากขึ้น มีมากถึง 77% ดังรูปที่ 1 และเมื่อเปรียบเทียบกับสัดส่วนจากรายงานสถิติพิชชิ่งทั่วโลกจาก AntiPhishing Working Group (APWG) พบว่าในช่วงไตรมาสที่ 3 ของปีนี้มีปริมาณเว็บพิชชิ่งที่ใช้ HTTPS ถึง 68% [1] ดังรูปที่ 2 ซึ่งมีความสอดคล้องกับสถิติเว็บพิชชิ่งที่เกี่ยวข้องกับธนาคารในประเทศไทยที่ TB-CERT ได้รับแจ้ง และยังมีแนวโน้มเพิ่มขึ้นในทุก ๆ ไตรมาสอีกด้วย อีกทั้งแฮกเกอร์จะเลือกใช้ผู้ให้บริการรับฝากเว็บไซต์กับบริษัทเล็กหรือก่อตั้งใหม่ เนื่องจากบริษัทเหล่านี้จะมีช่วงเวลาการให้บริการไม่ตลอด 24 ชั่วโมง และบางบริษัทติดต่อยาก หรือไม่สนใจในการแก้ไขปัญหาดีพอ และเมื่อพบเว็บไซต์พิชชิ่งถูกจัดเก็บที่โฮสติ้งดังกล่าว ทำให้ takedown ได้ช้า นอกจากนี้ในปี 2562 พบพิชชิ่งที่หลอกลวงว่าเป็นระบบอื่น นอกจากระบบของธนาคาร เช่น O365 Facebook รวมถึงบัญชีผู้ใช้ Line ปลอม เพื่อใช้หลอกลามข้อมูลส่วนตัวด้วย [2] ดังตัวอย่างในรูปที่ 3 ซึ่งในปัจจุบันบัญชีของระบบต่าง ๆ อาจจะมีการเชื่อมโยงกัน เช่น ใช้อีเมล office จาก O365 ไปสมัครใช้งาน Facebook หรือเครือข่ายสังคมออนไลน์ต่าง ๆ นอกจากนี้ผู้ใช้งานบางคนยังมีการใช้ชื่อบัญชีและรหัสผ่านเดียวกันในทุกระบบอีกด้วย ทำให้เมื่อแฮกเกอร์สามารถขโมยรหัสผ่านของระบบใดระบบหนึ่งได้ก็จะสามารถยึดครองทุกบัญชีผู้ใช้งานของเหยื่อได้ด้วย ดังนั้นผู้ใช้งานควรเพิ่มมาตรการป้องกัน เช่น การใช้ระบบยืนยันตัวด้วยหลายปัจจัย (Multi factors authentication) ใช้รหัสผ่านที่แตกต่างกันในแต่ละบัญชี รวมถึงการไม่ใช้อีเมลขององค์กรไปสมัครใช้งานเครือข่ายสังคมออนไลน์ เป็นต้น



รูปที่ 1 แสดงปริมาณร้อยละการใช้ HTTPS บนเว็บไซต์พิชชิ่งเทียบกับ HTTP ที่ TB-CERT ได้รับแจ้งทั้งหมดในปี 2562



รูปที่ 2 แสดงปริมาณร้อยละของเว็บไซต์ฟิชชิ่งที่ใช้ HTTPS ทั่วโลก โดย Anti-Phishing Working Group (APWG)



รูปที่ 3 แสดงตัวอย่างฟิชชิ่งที่หลอกลวงว่าเป็น O365

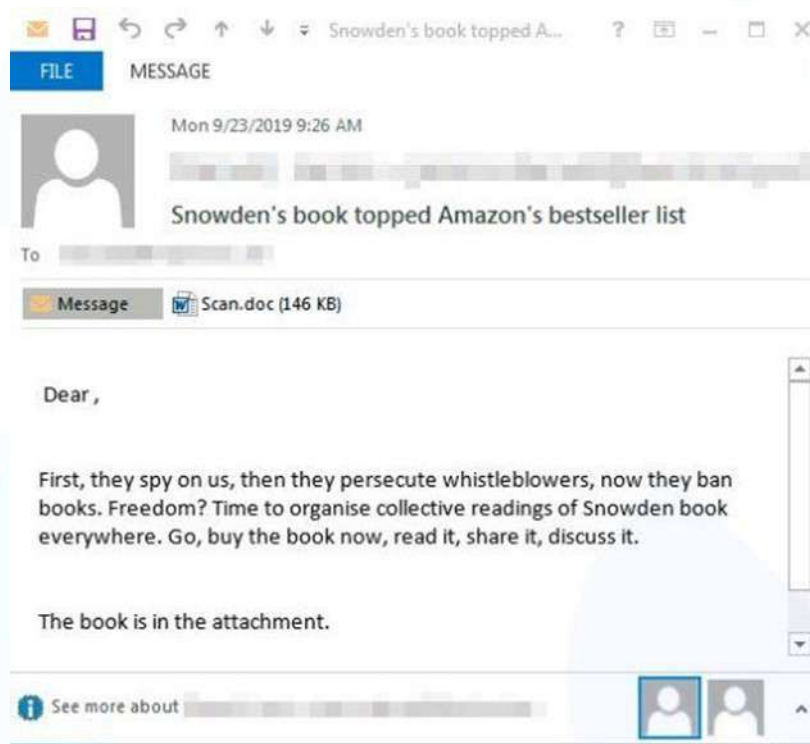


2. มัลแวร์ไร้ไฟล์ (Fileless Malware) กลายเป็นเทคนิคหลักที่แฮกเกอร์นิยมใช้

ในปีที่กลุ่มแฮกเกอร์ส่วนใหญ่มักสร้างมัลแวร์ไร้ไฟล์เพื่อใช้ในการโจมตี ซึ่งสอดคล้องกับการคาดการณ์ในปีที่ผ่านมาของ TB-CERT โดยการเปลี่ยนแปลงที่พบคือมีการเปลี่ยนเทคนิคจาก Script-base (คือใช้ powershell script ฝังในไฟล์) เปลี่ยนมาเป็นการใช้เทคนิคฝังในหน่วยความจำโดยตรง หรือ Memory code injection [3] มากขึ้น โดยไม่จำเป็นต้องเขียนไฟล์มัลแวร์ลงในฮาร์ดดิสก์ ส่งผลทำให้โปรแกรมป้องกันมัลแวร์ตรวจจับได้ยากขึ้นกว่าเดิม นอกจากนี้ยังมีการสร้างมัลแวร์ไร้ไฟล์ที่ทำงานบนระบบปฏิบัติการอื่นที่ไม่ใช่ Windows อีกด้วย โดยแฮกเกอร์กลุ่ม Lazarus ได้สร้างมัลแวร์ไร้ไฟล์บนระบบปฏิบัติการ MacOS เพื่อขโมยข้อมูลบนหน่วยความจำ ยังมีการพัฒนา Framework สำหรับสร้างมัลแวร์ไร้ไฟล์บน Linux ชื่อ FireELF [4] และแจกจ่ายอยู่บนอินเทอร์เน็ตด้วย ทำให้มีโอกาสที่แฮกเกอร์จะสามารถสร้างมัลแวร์ไร้ไฟล์บน Linux ได้ง่ายขึ้น อย่างไรก็ตามถึงแม้ว่าจะไม่พบรายงานความเสียหายเกิดขึ้นแต่ก็ต้องให้ความสนใจเพื่อเตรียมการป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นในอนาคตได้

3. มัลแวร์ที่ผสมผสานความสามารถในการโจมตี

ในปี 2562 มีการค้นพบมัลแวร์ที่มีความสามารถในการโจมตีที่หลากหลาย เห็นได้ชัดเจนจากการกลับมาของมัลแวร์ Emotet [5][6] ในเดือนกันยายน ซึ่งก่อนหน้านี้ Emotet เป็นแบคคิงโทรจัน แต่ครั้งนี้เพิ่มขีดความสามารถของตัวเองให้มีความสามารถทั้งการเป็นโทรจัน และบ็อตเน็ต นอกจากนี้ในบางสายพันธุ์ยังเป็นมัลแวร์เรียกค่าไถ่ (Ransomware) อีกด้วย โดย Emotet จะใช้เทคนิคการแพร่กระจายตัวผ่านทางอีเมล ซึ่งอาจจะส่งเป็นไฟล์แนบ หรือลิงก์ให้ดาวน์โหลดได้ จากตัวอย่างของ Emotet ในปี 2562 นี้ เป็นแคมเปญหลอกลวงว่ามีการแจกหนังสือ “Permanent Record” ที่ถูกสั่งห้ามขาย ของ Edward Snowden อดีตที่ปรึกษาทางเทคนิคให้กับสำนักงานความมั่นคงแห่งชาติของสหรัฐ (NSA-National Security Agency) เมื่อเหยื่อหลงเชื่อดาวน์โหลดและเปิดไฟล์แนบแล้ว มัลแวร์จะทำการขโมยข้อมูลการล็อกอินใช้งานอีเมลและส่งอีเมลต่อไปตามรายชื่อผู้ติดต่อที่พบในเครื่องอีกด้วย นอกจากนี้จากสถิติของเว็บไซต์ที่ให้บริการวิเคราะห์พฤติกรรมมัลแวร์ (Sandbox) ชื่อ ANY.RUN พบว่า Emotet ยังเป็นมัลแวร์ที่พบมากที่สุดในรอบปี 2562 [7] อีกด้วย ดังรูปที่ 5



รูปที่ 4 ตัวอย่างอีเมลที่แนบไฟล์มัลแวร์ Emotet [6]



รูปที่ 5 สถิติแสดงจำนวน sample ที่ถูกวิเคราะห์ใน Any.run ซึ่งเป็น sandbox ที่ใช้วิเคราะห์พฤติกรรมของมัลแวร์



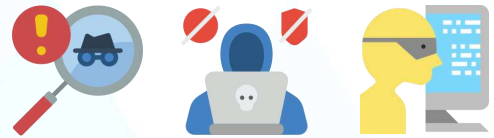
4. ข้อมูลรั่วไหลจากคลาวด์และฐานข้อมูล

ในปี 2562 ที่ผ่านมามีข้อมูลส่วนบุคคลเป็นเป้าหมายของแฮกเกอร์ ยิ่งในปีนี้มีประกาศใช้งาน GDPR-General Data Protection Regulation และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562 ยิ่งทำให้ประเด็นนี้ยิ่งน่าสนใจมากยิ่งขึ้น ถึงแม้ว่าข้อมูลส่วนบุคคลนั้นไม่ได้รั่วไหลจากสถาบันการเงิน แต่ข้อมูลดังกล่าวสามารถถูกนำมาใช้ในการแอบอ้างเพื่อการฉ้อโกงสถาบันการเงินได้ จากข่าวเหตุการณ์การโจมตีเพื่อขโมยข้อมูลจากหน่วยงานต่าง ๆ นั้น พบว่ามีเหตุการณ์การขโมยข้อมูลที่ใช้บริการคลาวด์ เช่น S3 bucket เป็นต้น อีกทั้งฐานข้อมูลที่ถูกแฮกให้เข้าถึงจากสาธารณะ เช่น Elasticsearch และ MongoDB เป็นต้น ซึ่งสาเหตุหลักนั้นมาจากผู้ดูแลระบบปรับแต่งค่า configuration ไม่ดีเพียงพอ ทำให้บุคคลภายนอกสามารถเข้าถึงได้โดยไม่ต้องได้รับอนุญาต อีกทั้งไม่ได้ใช้การเข้ารหัสข้อมูลในการจัดเก็บ ทำให้เมื่อมีผู้ไม่หวังดีขโมยข้อมูลออกไปได้ก็สามารถเห็นข้อมูลได้ทั้งหมด ดังนั้นการปรับแต่ง ตรวจสอบ configuration สำหรับควบคุมการเข้าถึงระบบฐานข้อมูล ไม่ว่าจะเป็นระบบที่อยู่ในดาต้าเซ็นเตอร์หรือระบบคลาวด์และการอัปเดตซอฟต์แวร์ที่ใช้ต่าง ๆ จะช่วยลดความเสี่ยงจากการถูกขโมยข้อมูลได้อย่างมีประสิทธิภาพ

5. การขโมยข้อมูลไบโอเมตริกซ์ (Biometrics)

ในปี 2562 มีเหตุการณ์ที่น่าสนใจเกี่ยวกับการขโมยข้อมูลไบโอเมตริกซ์ ได้แก่ ข้อมูลลายนิ้วมือ และข้อมูลระบบจดจำใบหน้าของผู้ใช้จำนวน 27.8 ล้านรายการ ซึ่งถูกใช้สำหรับควบคุมการเข้าออกอาคารของบริษัท Suprema นอกจากนี้ยังมีเหตุการณ์ที่มีแฮกเกอร์พยายามขโมยข้อมูลของลูกค้าบริษัท Veritas Genetics ซึ่งเป็นผู้ให้บริการทดสอบ DNA อย่างไรก็ตามทางบริษัทได้มาประกาศแล้วว่าข้อมูลที่รั่วไหลนั้น ไม่มีข้อมูลที่ sensitive เช่น ชื่อ นามสกุล หรือ รหัสพันธุกรรม (DNA) เป็นต้น ยิ่งไปกว่านั้นมีการนำเอาข้อมูลไบโอเมตริกซ์มาใช้ในการยืนยันตัวตนเพิ่มมากขึ้นอย่างมาก ดังนั้นหน่วยงานที่จะเก็บข้อมูลไบโอเมตริกซ์จะต้องใช้ความระมัดระวังให้มาก เนื่องจากว่าข้อมูลเหล่านี้เป็นข้อมูลที่ Sensitive อีกทั้งเจ้าของข้อมูลไม่สามารถเปลี่ยนข้อมูลนี้ได้อีกด้วย

เทคนิคของกลุ่มแฮกเกอร์สถาบันการเงินที่น่าสนใจ



1. Lazarus

กลุ่มแฮกเกอร์สัญชาติเกาหลีเหนือ Lazarus เป็นกลุ่มแฮกเกอร์ที่พุ่งเป้าโจมตีสถาบันการเงินในหลายประเทศ ในปีนี้แฮกเกอร์กลุ่มนี้ได้สร้างมัลแวร์ประเภทไร้ไฟล์ (Fileless Malware) สายพันธุ์ใหม่ที่มีผลกระทบบนระบบปฏิบัติการ MacOS ซึ่งทำงานอยู่ในหน่วยความจำ และไม่ต้องติดตั้งลงฮาร์ดดิสก์ ทำให้สามารถหลบเลี่ยงการตรวจจับของโปรแกรมป้องกันมัลแวร์ได้ โดยมีจุดประสงค์ในการขโมยข้อมูลที่อยู่ในหน่วยความจำ นอกจากนี้ยังมีการสร้างมัลแวร์ที่มุ่งขโมยเงินจากตู้ ATM โดยการนำโทรจัน DTrack มาผสมผสาน ซึ่งมัลแวร์ DTrack จัดอยู่ในประเภทโทรจันที่ถูกควบคุมได้จากระยะไกล (Remote Access Trojan – RAT) ที่มีความสามารถในการเรียกดูข้อมูลที่อยู่ในหน่วยความจำ (Memory Dump) ได้ ซึ่งมัลแวร์ ATMDTrack นั้นจึงมีความสามารถอ่านและเก็บข้อมูลในบัตรที่ใช้บริการจากตู้ที่ถูกมัลแวร์ดังกล่าวคุกคามได้

2. TA505

กลุ่มแฮกเกอร์ TA505 เป็นกลุ่มแฮกเกอร์ที่พุ่งเป้าโจมตีสถาบันการเงินในหลายประเทศ เช่น สหราชอาณาจักร ฝรั่งเศส ญี่ปุ่น อินเดีย ฟิลิปปินส์ และอาร์เจนตินา เป็นต้น อย่างไรก็ตามประเทศไทยเองก็ตกเป็นเป้าหมายด้วยเช่นกัน แต่ได้รับผลกระทบน้อยมาก ในปี 2562 นี้แฮกเกอร์กลุ่มนี้สร้างมัลแวร์หลากหลายสายพันธุ์ โดยส่วนใหญ่จะมีลักษณะคล้ายกันคือส่งอีเมลพร้อมไฟล์แนบที่มีนามสกุล .xls เมื่อเหยื่อหลงเชื่อเปิดไฟล์ .xls ดังกล่าว มัลแวร์จะดาวน์โหลดไฟล์มัลแวร์ที่จะทำอันตรายผ่านลิงค์บน Dropbox และการสร้าง Tunnel ผ่านทางโปรโตคอล Remote Desktop เป็นต้น โดยมีวัตถุประสงค์เพื่อฝังตัว ขโมยข้อมูลสำคัญ และควบคุมเครื่องคอมพิวเตอร์ที่ถูกมัลแวร์คุกคามจากระยะไกลได้

3. Cobolt

กลุ่มแฮกเกอร์ Cobalt ในปีนี้มีเทคนิคที่น่าสนใจคือการอาศัยการหลอกลวงโดยใช้ไฟล์ PDF แล้ว Redirect ไปยัง Google App Engine ผ่านทางโปรโตคอล HTTPS ทำให้เหยื่อเข้าใจว่ากำลังเข้าถึงข้อมูลจาก Google จริงๆ จากนั้นจะดาวน์โหลดไฟล์ Word ที่ฝังมาโครเพื่อจะโจมตีต่อไป นอกจากนี้แฮกเกอร์กลุ่มนี้ยังได้สร้างมัลแวร์เรียกค่าไถ่ชื่อ PureLocker ที่มีจุดเด่นด้านความสามารถในการเข้ารหัสไฟล์และทำงานได้บนทุกระบบปฏิบัติการหลัก ได้แก่ Windows, Linux, และ MacOS

4. Fancy Bear

ในปีนี้อีกแฮกเกอร์สัญชาติรัสเซียอย่าง Fancy Bear (APT28) ส่งอีเมลข่มขู่เพื่อเรียกค่าไถ่จากหน่วยงานในสถาบันการเงิน หน่วยงานราชการ และกลาโหม เป็นต้น ซึ่งเหตุการณ์นี้เกิดขึ้นในหลายประเทศ อย่างไรก็ตามยังไม่พบอีเมลข่มขู่ในประเทศไทย เทคนิคที่แฮกเกอร์กลุ่มนี้ใช้โจมตีเป็นลักษณะการทำ DDoS โดยโจมตีผ่านโปรโตคอลต่าง ๆ ได้แก่ DNS NTP และ CLDAP รวมไปถึงโปรโตคอล WS Discovery (UDP/3702 multicast address 239.255.255.250) และ ARMS-Apple Remote Management Service (UDP/3283) ด้วย ซึ่งโปรโตคอล WS Discovery (UDP/3702 multicast address 239.255.255.250) เคยพบการเพิ่มปริมาณทราฟฟิกได้ถึง 15,300%

5. Silence

กลุ่มแฮกเกอร์ Silence กลุ่มแฮกเกอร์สัญชาติรัสเซีย และมีเป้าหมายโจมตีสถาบันการเงินในรัสเซียเป็นหลัก ในปีนี้ได้ใช้เทคนิคการส่งอีเมลฟิชซิงและหลอกลวงว่าเป็นอีเมลตอบกลับอัตโนมัติ เพื่อรวบรวมบัญชีอีเมลที่ยังมีการใช้งานอยู่ อีกทั้งยังเป็นการยืนยันอีเมลของเหยื่อด้วย ซึ่งจากรายงานพบว่าการส่งอีเมลถึง 170,000 ฉบับ ทั้งในทวีปยุโรป เอเชีย และประเทศในกลุ่มสหภาพโซเวียต ในจำนวนนี้ส่งมายังทวีปเอเชียถึง 80,000 ฉบับใน 12 ประเทศ ซึ่ง TB-CERT ไม่ได้รับรายงานผลกระทบดังกล่าวของกลุ่มการเงินในประเทศไทย เมื่อมัลแวร์ดังกล่าวสามารถคุกคามเครื่องคอมพิวเตอร์ในสถาบันการเงินได้แล้วจะพยายาม Lateral movement ไปยังเครื่องคอมพิวเตอร์ที่ประมวลผลข้อมูลบัตร อีกทั้งยังพยายามควบคุม ATM โดยไม่จำเป็นต้องติดตั้งมัลแวร์ในตัว ATM เพื่อที่จะขโมยเงินอีกด้วย

6. FIN7

กลุ่มแฮกเกอร์ FIN7 สัญชาติรัสเซีย ที่มีเป้าหมายหลักในการโจมตีสถาบันการเงินในยุโรปและสหรัฐอเมริกา แม้ประเทศไทยจะไม่ใช่มเป้าหมาย แต่ในปีนี้มีเทคนิคของมัลแวร์ที่น่าสนใจ คือมัลแวร์ BOOSTWRITE เป็น dropper ที่ทำงานในหน่วยความจำเท่านั้น (หรือเป็นมัลแวร์ประเภทไร้ไฟล์) และสามารถถอดรหัส payload ที่ฝังตัวมาด้วยกุญแจที่ได้รับจากเซิร์ฟเวอร์ นอกจากนี้ยังมี RDFSNIFFER ซึ่งเป็น payload ของมัลแวร์นี้ จะถูกโหลดเข้ากับโปรเซสเดียวกันกับโปรเซสของ NCR Aloha Command ซึ่งเป็นซอฟต์แวร์ที่ใช้บริหารจัดการและแก้ไขปัญหาของการประมวลผลการชำระเงินผ่านบัตร ในลักษณะของ DLL เพื่อควบคุมระบบบริหารจัดการดังกล่าว

อ้างอิง

1. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf
2. <https://www.cisco.com/c/dam/en/us/products/collateral/security/2019-threats-of-the-year-cybersecurity-series-dec-2019.pdf>
3. <https://resources.infosecinstitute.com/malware-spotlight-fileless-malware/>
4. <https://kalilinuxtutorials.com/fireelf/>
5. <https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-exploring-emetet-elaborate-everyday-enigma/>
6. <https://fossbytes.com/top-malware-2019/>
7. <https://any.run/malware-trends/emetet>
8. [https://www.globenewswire.com/news-release/2019/11/12/1945147/0/en/October-2019-s-Most-Wanted-Malware-the-Divine of-Cryptominers-Continues-as-Emotet-Botnet-Expands-Rapidly.html](https://www.globenewswire.com/news-release/2019/11/12/1945147/0/en/October-2019-s-Most-Wanted-Malware-the-Divine-of-Cryptominers-Continues-as-Emotet-Botnet-Expands-Rapidly.html)
9. <https://securelist.com/biometric-data-processing-and-storage-system-threats/95364/>
10. <https://www.pcsecurity-99.com/2019/12/07/infamous-lazarus-apt-hackers-group-attack-mac-computers-with-fileless-malware/>
11. <https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf>
12. <https://securelist.com/kaspersky-security-bulletin-2019-statistics/95475/>

คาดการณ์แนวโน้มการโจมตีในปี 2563

จากการรวบรวมข้อมูลเหตุการณ์ที่เกิดขึ้นในปีที่ผ่านมาประกอบกับการวิเคราะห์สถานการณ์และแนวโน้มจากรายงานหลายแหล่ง TB-CERT จึงได้ทำการคาดการณ์แนวโน้มรูปแบบการโจมตีทางไซเบอร์ สำหรับปี 2563 นี้ ดังนี้

1. การขโมยข้อมูลบัตรที่ใช้ชำระเงินผ่านช่องทางอิเล็กทรอนิกส์ (e-skimming)

การซื้อขายของออนไลน์เป็นที่นิยมอย่างมากในปัจจุบัน และนับวันยิ่งจะมีปริมาณการใช้บริการซื้อขายของออนไลน์มากขึ้น ทำให้แฮกเกอร์นั้นพยายามที่จะขโมยข้อมูลบัตรที่ใช้ชำระเงิน ไม่ว่าจะเป็นบัตรเครดิตและบัตรเดบิตหรือบัตรในรูปแบบอื่น ๆ ที่ต่างพัฒนาให้มีความสะดวกในการใช้งานมากขึ้น โดยการฝังมัลแวร์ไว้ที่เครื่องคอมพิวเตอร์ที่ทำหน้าที่ Point of Sale (POS) หรือระบบคอมพิวเตอร์ของร้านค้าที่ให้บริการขายของออนไลน์ เพื่อที่จะดักรับข้อมูลบัตรของผู้ถือบัตร ที่ชำระเงินผ่านเครื่อง POS หรือ ผ่านเว็บไซต์ e-commerce ที่แฮกเกอร์เจาะระบบแล้วฝังมัลแวร์ไว้ได้ ดังนั้นเจ้าของร้านค้าที่ใช้งาน POS และเจ้าของเว็บไซต์ e-commerce ต่าง ๆ ต้องระมัดระวัง ตรวจสอบความปลอดภัยของระบบอย่างสม่ำเสมอ จึงมีความพยายามที่จะผลักดันมาตรฐาน PCI DSS หรือ Payment Card Industry Data Security Standard มาอย่างต่อเนื่องเพื่อให้เกิดแนวปฏิบัติที่ให้องค์กร ผู้ให้บริการ และร้านค้ามีการดูแลป้องกันการบริหารจัดการความมั่นคงปลอดภัยข้อมูลของลูกค้าที่มีประสิทธิภาพมากขึ้น

2. ระบบปฏิบัติการ MacOS, Linux และ Unix เป็นเป้าหมายมากขึ้น

จากเดิมที่กลุ่มแฮกเกอร์ต่าง ๆ มักจะอาศัยช่องโหว่บนระบบปฏิบัติการ Windows และซอฟต์แวร์ต่าง ๆ ดังนั้นผู้ดูแลระบบจึงให้ความสนใจกับเครื่องที่ติดตั้งระบบปฏิบัติการ Windows มากกว่า แต่มีงานวิจัยของผู้ผลิตโปรแกรมป้องกันไวรัสบางแห่งรายงานว่า ในปี 2562 พบว่ามีมัลแวร์ที่แพร่กระจายตัวบนระบบปฏิบัติการ MacOS เพิ่มมากขึ้น อีกทั้งเมื่อปลายปี 2562 กลุ่มแฮกเกอร์เกาหลีเหนืออย่าง Lazarus ก็ได้สร้างมัลแวร์ที่แพร่กระจายบนระบบปฏิบัติการ MacOS ด้วย ดังนั้นในองค์กรที่มีการใช้งานระบบปฏิบัติการอื่นที่นอกเหนือจาก Windows แล้วต้องให้ความสำคัญในการรักษาความปลอดภัยมากขึ้น

3. การแฮกระบบ IoT – Internet of Things

ปัจจุบันเทคโนโลยีที่เกี่ยวข้องกับ IoT ได้พัฒนาไปอย่างมาก อีกทั้งราคาก็ลดลง ทำให้เครื่องใช้ไฟฟ้า อุปกรณ์อำนวยความสะดวก อุปกรณ์เพื่อสุขภาพติดตามตัว รวมถึงของเล่น ส่วนใหญ่จะเริ่มเชื่อมต่อสู่อินเทอร์เน็ตได้แล้ว อย่างเช่นกล้องวงจรปิด สมาร์ททีวี เครื่องซักผ้า อุปกรณ์ช่วยเหลืออัจฉริยะในบ้าน เป็นต้น จึงเป็นแรงจูงใจที่ทำให้แฮกเกอร์พยายามโจมตีอุปกรณ์เหล่านี้ที่ไม่ได้รับการป้องกันที่ดีเพียงพอ ซึ่งผลกระทบที่อาจจะพบได้อย่างเช่นการเผยแพร่ข้อมูลส่วนตัว เช่นภาพจากกล้องวงจรปิดในบ้าน หรือแม้กระทั่งการข่มขู่กรรโชกเพื่อเรียกรansom และทรัพย์สินของเหยื่อ ดังนั้นการใช้เทคโนโลยี IoT จึงควรคำนึงถึงความปลอดภัยและความเป็นส่วนตัวของผู้ใช้งานด้วย รวมถึงการศึกษาคุณสมบัติของอุปกรณ์ที่เลือกใช้ด้วย

4. มัลแวร์เรียกค่าไถ่ (Ransomware) จะผสมผสานการเผยแพร่ข้อมูลที่อ่อนไหว (Extortion) ด้วย

มัลแวร์เรียกค่าไถ่ที่ผ่านมาจะเข้ารหัสข้อมูลไฟล์สำคัญขององค์กร แต่องค์กรส่วนใหญ่ที่ถูกมัลแวร์เรียกค่าไถ่คุกคามนี้มักจะจ่ายเงินค่าไถ่ ดังนั้นแฮกเกอร์จะหาวิธีในการข่มขู่ที่รุนแรงขึ้น เช่นการข่มขู่ว่าจะทำลายข้อมูลที่อ่อนไหวเปิดเผยข้อมูลที่อ่อนไหวขององค์กรสู่สาธารณะ การนำไปขายในตลาดมืด รวมไปถึงการแจ้งไปยังหน่วยงานกำกับขององค์กรนั้น ๆ ได้

5. การใช้คลาวด์สาธารณะ (Public Cloud) ในการโจมตีมากขึ้น

ความสะดวกสบายในการใช้บริการ คลาวด์สาธารณะต่าง ๆ ด้วยเหตุผลด้านความประหยัด ความรวดเร็ว และประสิทธิภาพในการใช้งาน ทำให้แฮกเกอร์ส่วนใหญ่มักจะเลือกลงทุนใช้คลาวด์สาธารณะเป็นฐานในการโจมตี ไม่เพียงเท่านั้นองค์กรส่วนใหญ่ไม่สามารถปิดกั้นการเข้าถึงคลาวด์สาธารณะเหล่านี้ด้วย เนื่องจากจะกระทบการใช้งานของผู้ใช้ขององค์กรได้ ตัวอย่างเช่น แฮกเกอร์เปิดเว็บไซต์ฟิชชิ่งบนผู้ให้บริการคลาวด์สาธารณะ ถ้าผู้ดูแลระบบขององค์กรปิดกั้นการเข้าถึง แฮกเกอร์ก็จะเปลี่ยนแปลงค่าหมายเลขไอพีได้ใหม่ได้อย่างง่ายดาย ทำให้ผู้ดูแลระบบขององค์กรปิดกั้นการเข้าถึงลำบากมากยิ่งขึ้น

6. ข้อมูลรั่วไหลบนเว็บ Repository ต่าง ๆ

เว็บ Repository เป็นเว็บที่มีไว้สำหรับเก็บข้อมูล ควบคุมเวอร์ชันและแชร์โค้ดที่พัฒนาขึ้น เช่น Github และ Pastebin เป็นต้น เพื่อเพิ่มประสิทธิภาพในการทำงานร่วมกันของนักพัฒนาซอฟต์แวร์ต่าง ๆ อย่างไรก็ตามแฮกเกอร์เองก็มักจะอาศัยเว็บเหล่านี้ในการแจกจ่ายโค้ดในการเจาะระบบ หรือแม้แต่การแชร์ข้อมูลความลับต่าง ๆ ที่ขโมยมาได้ เผยแพร่บนเว็บเหล่านั้นได้ ข้อมูลรั่วไหลที่มักพบได้บ่อยบนเว็บ Repository ได้แก่ ชื่อบัญชีผู้ใช้ รหัสผ่าน รวมถึงเลขที่บัตรเครดิต เป็นต้น ดังนั้นการเฝ้าระวังข้อมูลรั่วไหลจึงควรค้นหาข้อมูลจากเว็บเหล่านี้ด้วย

อ้างอิง

1. <https://www.rsa.com/content/dam/en/e-book/20-predictions-for-2020.pdf>
2. <https://documents.trendmicro.com/assets/rpt/rpt-the-new-norm-trend-micro-security-predictions-for-2020.pdf>
3. <https://hello.global.ntt/en-us/insights/future-disrupted-2020-technology-trends>
4. <https://securityintelligence.com/posts/ibm-x-force-security-predictions-for-2020/>
5. <https://www.technologyrecord.com/Article/which-technologies-could-change-enterprise-it-in-2020-101253>
6. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
7. <https://www.crowdstrike.com/blog/4-cyber-threat-predictions-for-2020/>
8. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/11/20151759/KSB2019_APT-predictions-2020_web.pdf
9. https://www.boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/top-9-cybersecurity-trends-for-2020.pdf
10. <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-2020-threats-predictions-report/>
11. <https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/>
12. <https://www2.frost.com/news/press-releases/artificial-intelligence-seen-as-key-technology-game-changer-but-implementation-challenges-remain-finds-frost-sullivan/>

บทสรุป

การเตรียมความพร้อมในการรับมือภัยคุกคามไซเบอร์ จำเป็นต้องมีการพัฒนาบุคลากร กระบวนการรับมือ และการพัฒนามาตรฐานความมั่นคงปลอดภัยอย่างต่อเนื่อง เพื่อให้เกิดการสร้างวัฒนธรรมองค์กรให้มีความเข้าใจในเรื่อง Cyber Resilience และเกิดผลอย่างยั่งยืนในยุคดิจิทัล TB-CERT เล็งเห็นว่าการพัฒนาทักษะความรู้พื้นฐานให้กับหน่วยงานสมาชิกโดยผ่านกิจกรรมการจัดฝึกอบรมทั้งภาคทฤษฎีและปฏิบัติอย่างต่อเนื่องจะเพิ่มความรู้ความเชี่ยวชาญให้กับบุคลากรที่เกี่ยวข้องให้สามารถรับมือภัยไซเบอร์ได้อย่างทันทั่วถึง และเป็นมาตรฐานเดียวกันทั้งอุตสาหกรรม การชักชวนกระบวนการรับมือภัยคุกคามอย่างสม่ำเสมอหรือที่เราเรียกกันว่า Banking Cyber Drill ประจำปีนั้นช่วยให้หน่วยงานสมาชิกได้ฝึกทดสอบประสิทธิภาพของกระบวนการรับมือภัยคุกคามของตนในสถานการณ์ต่าง ๆ นอกจากนั้น การร่วมฝึกซ้อมของสมาชิกในกลุ่มการเงินก็ถือเป็นการชักชวนความเข้าใจของหน่วยงานทั้งอุตสาหกรรม จะช่วยให้หน่วยงานสมาชิกที่อาจจะยังไม่มีกระบวนการชัดเจน สามารถนำผลการฝึกซ้อมไปปรับใช้ได้อย่างมีประสิทธิภาพมากขึ้น และเป็นโอกาสที่ดีที่ทุกหน่วยงานจะได้แลกเปลี่ยนเรียนรู้จากประสบการณ์จากสมาชิกอื่น ๆ อันจะเป็นกระบวนการเรียนรู้แบบอัตราร่วง โดย TB-CERT ได้มีบทบาทในการส่งเสริมการพัฒนาระบบการแลกเปลี่ยนข้อมูลเหตุการณ์การโจมตีในรูปแบบต่าง ๆ ของแฮกเกอร์ ระหว่างหน่วยงานสมาชิกด้วยกัน ให้ทุก ๆ หน่วยงานได้รับข้อมูลเดียวกันอย่างรวดเร็ว ทันต่อเหตุการณ์ เพื่อเป็นการป้องกันภัยที่อาจจะเกิดขึ้นกับหน่วยงานใดหน่วยงานหนึ่งในภาคอุตสาหกรรมได้ทันที ทั้งยังมีการแลกเปลี่ยนข้อมูลจากหน่วยงาน CERT ทั้งในและนอกประเทศภายใต้พันธสัญญาแลกเปลี่ยนข้อมูลซึ่งเป็นแหล่งข้อมูลที่น่าเชื่อถือได้อีกแหล่งหนึ่งให้กับหน่วยงานสมาชิก

นอกจากการผลักดันให้องค์กรมีความเข้าใจและทักษะในการรับมือกับภัยไซเบอร์อย่างยืดหยุ่นแล้วนั้น TB-CERT ยังเน้นการพัฒนามาตรฐานด้าน Cybersecurity ร่วมกันซึ่งจะช่วยให้สมาชิกและหน่วยงานกำกับดูแลมีความเข้าใจบนพื้นฐานเดียวกัน และเป็นส่วนหนึ่งของการทำให้ภาคอุตสาหกรรมธนาคารมีความเข้มแข็งขึ้นอย่างยั่งยืน พร้อมทั้งจะยกระดับให้เป็น resilience industry ได้อย่างมั่นคง

ภาคผนวก

เอกสารเผยแพร่

5/5 สูตรเด็ด รอดพ้นจากฟิชซิง

TLP: WHITE

5 สิ่งที่ต้องทำ

- 1** ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตอยู่เสมอ
- 2** ตรวจสอบแหล่งที่มาของอีเมล ให้แน่ใจก่อนเปิดอ่านอีเมล
- 3** หากพบอีเมลที่สงสัยว่าเป็นฟิชซิงที่เกี่ยวข้องกับธนาคาร ติดต่อธนาคารทันที
- 4** ในกรณีหลงเชื่อและเปิดเผยรหัสผ่านแล้ว ให้ติดต่อธนาคาร เพื่อเปลี่ยนรหัสผ่านทันที
- 5** ติดตามข่าวสารการแจ้งเตือนฟิชซิงจากหน้าเว็บไซต์ของธนาคารอย่างสม่ำเสมอ

5 สิ่งที่ไม่ควรทำ

- 1** โฟสต์บัญชีอีเมลบนเว็บไซต์สาธารณะ
- 2** เปิดอีเมลโดยไม่ตรวจสอบแหล่งที่มา
- 3** คลิกลิงค์ที่มาพร้อมกับอีเมลที่ไม่แน่ใจแหล่งที่มา
- 4** ตอบกลับอีเมลที่น่าสงสัย โดยไม่ไตร่ตรองให้ถี่ถ้วน
- 5** เปิดเผยข้อมูลส่วนบุคคลใด ๆ ผ่านการร้องขอผ่านทางอีเมล หรือ เว็บไซต์ที่น่าสงสัย

TR19-004

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง



TB-CERT
Thailand Banking Sector CERT

เอกสารเผยแพร่

 TB-CERT Thailand Banking Sector CERT	TR19-005 คำแนะนำเกี่ยวกับช่องโหว่หมายเลข CVE-2019-0708 ที่เกี่ยวข้องกับบริการ Remote Desktop ภายในระบบปฏิบัติการวินโดวส์	TLP: WHITE 
--	--	--

คำแนะนำเกี่ยวกับช่องโหว่หมายเลข CVE-2019-0708 ที่เกี่ยวข้องกับบริการ Remote Desktop ภายในระบบปฏิบัติการวินโดวส์

เผยแพร่วันที่ 20 พฤษภาคม 2562

ปรับปรุงล่าสุดวันที่ 20 พฤษภาคม 2562

ไมโครซอฟท์ประกาศแพทช์ CVE-2019-0708 ที่เกี่ยวข้องกับบริการ Remote Desktop ภายในระบบปฏิบัติการวินโดวส์ ซึ่ง Remote Desktop เป็นบริการที่อนุญาตให้ผู้ที่มิสิทธิ์สามารถเข้าถึงและควบคุมเครื่องคอมพิวเตอร์ได้จากระยะไกล โดยการใช้งานนั้นผู้ที่ต้องการจะเข้าถึงจะต้องมีการยืนยันตัวตนด้วยบัญชีผู้ใช้และรหัสผ่าน จึงจะสามารถใช้ในการเข้าถึงได้ บริการ Remote Desktop ถูกติดตั้งมาพร้อมกับระบบปฏิบัติการวินโดวส์ ตั้งแต่ windows XP จนถึงระบบปฏิบัติการวินโดวส์เวอร์ชันล่าสุด

รายละเอียดของช่องโหว่

ช่องโหว่ดังกล่าวสามารถทำให้ผู้โจมตีสามารถเอ็กคิวต์โค้ดได้จากระยะไกล (Remote Code Execution) โดยไม่จำเป็นต้องทำการยืนยันตัวตน (authentication) แต่อย่างใด ซึ่งหมายถึงช่องโหว่นี้ทำให้ระบบปฏิบัติการวินโดวส์สามารถถูกโจมตีโดยไม่จำเป็นต้องทราบ บัญชีผู้ใช้ และรหัสผ่าน และเมื่อโจมตีสำเร็จแล้วสามารถเข้ายึดครองเครื่องได้ ทางไมโครซอฟท์เกรงว่าช่องโหว่ดังกล่าวอาจจะถูกนำไปใช้ในการโจมตีแบบ wormable อย่าง Wannacry ที่โจมตีและแพร่กระจายไปเรื่อยๆ

ระบบที่ได้รับผลกระทบ

ช่องโหว่ดังกล่าวมีผลกระทบต่อระบบปฏิบัติการวินโดวส์ ได้แก่ Windows 7, Windows Server 2008, และ Windows Server 2008 R2 ส่วนระบบปฏิบัติการที่ได้รับผลกระทบแต่ไม่มี support แล้วอย่าง Windows 2003 and Windows XP ให้ดาวน์โหลดแพทช์หมายเลข KB4500705 ไปติดตั้ง ดังรายละเอียดเอกสารอ้างอิงที่ [3]

หมายเหตุ สำหรับระบบปฏิบัติการ Windows 8, Windows 8.1, Windows 10, Windows server 2012, Windows 2012 R2, และ Windows server 2016 ไม่ได้รับผลกระทบจากการแจ้งเตือนครั้งนี้

เอกสารเผยแพร่

 TB-CERT Thailand Banking Sector CERT	TR19-005 คำแนะนำเกี่ยวกับช่องโหว่หมายเลข CVE-2019-0708 ที่เกี่ยวข้องกับบริการ Remote Desktop ภายในระบบปฏิบัติการวินโดวส์	TLP: WHITE 
--	--	--

คำแนะนำ

1. หากจำเป็นต้องใช้งาน Remote Desktop ให้ดำเนินการอัปเดตแพตช์ของระบบปฏิบัติการที่ได้รับผลกระทบตามเอกสารอ้างอิง [1] และ [3] อย่างเร่งด่วน
2. หากไม่จำเป็นต้องใช้งาน Remote Desktop ให้ทำการยกเลิกการใช้งาน ตามเอกสารอ้างอิง [4]
3. ควรปิดกั้นการเข้าถึงพอร์ตที่ไม่จำเป็นจากภายนอก
4. พิจารณาปรับแต่งอุปกรณ์เครือข่าย เพื่อป้องกันหรือเฝ้าระวังการเข้าถึง Remote Desktop โดยตรงจากภายนอก ซึ่งอาจจะพิจารณาเพิ่มการใช้งาน Virtual Private Network (VPN) ด้วย
5. พิจารณาการใช้งาน Network Layer Authentication - NLA ในการปรับแต่งค่าคุณสมบัติของการใช้ Remote Desktop ตามเอกสารอ้างอิง [5] ซึ่งหากไม่สามารถติดตั้งแพตช์หรือปิดกั้นการเข้าถึง Remote Desktop ได้ ให้เปิดใช้งาน NLA เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่ดังกล่าว
6. ติดต่อบริษัทโปรแกรมป้องกันมัลแวร์ที่ใช้งาน เพื่อสอบถามแนวทางในการป้องกันช่องโหว่ดังกล่าว

เอกสารอ้างอิง

1. <https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/>
2. <https://www.bleepingcomputer.com/news/security/microsoft-fixes-critical-remote-desktop-flaw-blocks-worm-malware/>
3. <https://support.microsoft.com/help/4500705>
4. <https://www.lifewire.com/disable-windows-remote-desktop-153337>
5. <https://social.technet.microsoft.com/wiki/contents/articles/5490.configure-network-level-authentication-for-remote-desktop-services-connections.aspx>

เอกสารเผยแพร่

การพิสูจน์และยืนยันตัวตนด้วยหลายปัจจัย (Multi-factor Authentication)

TLP: WHITE

ตอนที่ 1 (1/2)

เผยแพร่วันที่ 11 กรกฎาคม 2562

การพิสูจน์และยืนยันตัวตน (Authentication) คืออะไร

การพิสูจน์และยืนยันตัวตน (Authentication) เป็นกระบวนการที่ใช้ในการตรวจสอบผู้มีสิทธิ์เข้าใช้บริการ ทำธุรกรรม หรือใช้ทรัพยากรที่บุคคลนั้นเป็นเจ้าของจริง ซึ่งโดยทั่วไปมักพบกระบวนการพิสูจน์และยืนยันตัวตนในบริการต่างๆ ผ่านระบบเครือข่ายอินเทอร์เน็ต เช่น การเข้าถึงบัญชีอีเมล หรือบัญชีเครือข่ายสังคมออนไลน์ ส่วนมากจะนิยมใช้ชื่อบัญชี และรหัสผ่าน โดยที่รหัสผ่านที่ใช้นั้น บางครั้งอาจจะสั้นเกินไป ง่ายเกินไป ใช้รหัสผ่านเดิมเป็นระยะเวลานานเกินไป รวมถึงผู้ประสงค์ร้ายอาจจะล่วงรู้หรือเดารหัสผ่านได้ ทำให้บัญชีผู้ใช้ถูกขโมยได้ ดังนั้นการใช้รหัสผ่านเพียงอย่างเดียวในการพิสูจน์และยืนยันตัวตนจึงไม่เพียงพอในการป้องกันบัญชีผู้ใช้ได้

ประเภทของวิธีการพิสูจน์และยืนยันตัวตน

วิธีการพิสูจน์และยืนยันตัวตนแบ่งได้ 3 ประเภท ดังนี้



Something you know

"สิ่งที่คุณรู้" เช่น ชื่อบัญชี รหัสผ่าน รหัส PIN เลขที่บัตรประชาชน หรือคำถามคำตอบความลับ เป็นต้น



Something you have

"สิ่งที่คุณมี" เช่น โทรศัพท์มือถือที่ใช้คู่กับ One-Time password (OTP) หรือ Authenticator App รวมถึง Token และ บัตรต่างๆ เป็นต้น



Something you are

"สิ่งที่คุณเป็น" หรืออัตชีวมิติ (Biometric) เช่น ลายนิ้วมือ ฝ่ามือ ม่านตา ใบหน้า เสียง และรวมถึงพฤติกรรมที่ทำประจำด้วย เป็นต้น

การพิสูจน์และยืนยันตัวตนด้วยหลายปัจจัย คืออะไร

เป็นการเอาสิ่งที่คุณรู้ หรือสิ่งที่คุณมี หรือสิ่งที่คุณเป็น มาใช้ร่วมกันในการพิสูจน์และยืนยันตัวตน เช่น การใช้รหัสผ่านควบคู่กับ OTP หรือ การใช้บัตรคู่กับลายนิ้วมือ เป็นต้น โดยมีจุดประสงค์เพื่อเพิ่มความปลอดภัยในการใช้งานระบบต่างๆ เช่น หากมีผู้ประสงค์ร้ายล่วงรู้รหัสผ่าน แต่จะเข้าถึงระบบไม่ได้หากไม่มี OTP เป็นต้น

TR19-006

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

เอกสารเผยแพร่

การพิสูจน์และยืนยันตัวตนด้วยหลายปัจจัย (Multi-factor Authentication) ตอนที่ 1 (2/2)

TLP: WHITE



เผยแพร่วันที่ 11 กรกฎาคม 2562

ตัวอย่างการใช้การพิสูจน์และยืนยันตัวตนด้วยหลายปัจจัยในบริการของธนาคาร

ระบบการให้บริการด้านการเงินของธนาคารส่วนใหญ่นำระบบการพิสูจน์และยืนยันตัวตนด้วยหลายปัจจัยมาใช้แล้ว เช่น การใช้งานตู้เอทีเอ็ม ลูกค้าจะต้องใช้บัตรเอทีเอ็มควบคู่กับรหัส PIN หรือการใช้งาน Mobile banking ลูกค้าจะต้องใส่ รหัส PIN ควบคู่กับค่า OTP ที่ธนาคารส่งมาให้ผ่านทาง SMS เพื่อทำรายการด้านการเงิน เป็นต้น นอกจากนี้ในปัจจุบันโทรศัพท์มือถือส่วนใหญ่รองรับการพิสูจน์ตัวตนด้วยอัตชีวมิติ เช่น ลายนิ้วมือ หรือใบหน้า เป็นต้น ธนาคารบางแห่งจึงได้นำการพิสูจน์ตัวตนด้วยวิธีนี้ควบคู่กับรหัส PIN ที่ให้ใช้งานตั้งค่าเองอีกด้วย



สิ่งที่ควรปฏิบัติในการใช้การพิสูจน์และยืนยันตัวตนด้วยหลายปัจจัยอย่างปลอดภัย

1. ใช้รหัสผ่านที่แข็งแกร่ง และซับซ้อน ถึงแม้ว่าจะใช้ Multi-factor Authentication แล้วก็ตาม
2. ติดตั้งโปรแกรมป้องกันมัลแวร์ที่โทรศัพท์มือถือและเครื่องคอมพิวเตอร์ เพื่อป้องกันมัลแวร์ประเภทโทรจันขโมยข้อมูล
3. เก็บรักษาโทรศัพท์มือถือ ป้องกันการถูกขโมย
4. หากจำเป็นต้องบอกรหัส PIN หรือรหัสผ่านให้กับผู้อื่นทราบ ให้เปลี่ยนแปลงรหัสดังกล่าวก่อนบอกผู้อื่น เช่น เมื่อต้องส่งโทรศัพท์ซ่อม ให้ทำการเปลี่ยนแปลงรหัส PIN สำหรับปลดล็อกหน้าจอก่อนส่งซ่อม
5. ระงับการล่อลวงให้เปิดเผยข้อมูลส่วนบุคคลโดยเหล่าผู้ประสงค์ร้าย เช่น มีผู้ประสงค์ร้ายโทรศัพท์มาหลอกลวงให้แจ้งรหัส OTP เป็นต้น
6. ไม่ควรเก็บสิ่งที่ใช้ในการยืนยันตัวตนไว้ที่เดียวกัน เช่น ไม่ควรจดรหัส PIN ไว้หลังบัตรเอทีเอ็ม เป็นต้น เพื่อป้องกันเมื่อถูกขโมยแล้วผู้ประสงค์ร้ายจะยังคงไม่สามารถเข้าถึงระบบได้
7. ตรวจสอบอีเมลแจ้งเตือนและรายงานการล็อกอิน ส่วนใหญ่แอปพลิเคชันของธนาคารจะส่งอีเมลแจ้งเตือนการล็อกอิน หากพบการล็อกอินที่ผิดปกติ เช่น ล็อกอินจากสถานที่ที่ไม่ได้ไป หรือช่วงเวลาที่ไม่ได้ใช้งาน ให้สันนิษฐานว่าอาจจะถูกลักลอบล็อกอิน ให้ดำเนินการเปลี่ยนรหัสผ่านทันที

เอกสารเผยแพร่

ข้อบกพร่องบนโทรศัพท์ Samsung ทำให้การตรวจสอบการยืนยันตัวตนด้วยลายนิ้วมือผิดพลาด

TLP: WHITE



เผยแพร่วันที่ 30 ตุลาคม 2562
ปรับปรุงวันที่ 30 ตุลาคม 2562

จากข่าวการค้นพบข้อบกพร่องบนโทรศัพท์มือถือ Samsung ในตระกูล Galaxy Note10 และ S10 ที่ผู้ประสงค์ร้ายสามารถยืนยันตัวตนด้วยลายนิ้วมือได้โดยไม่ต้องลงทะเบียนไว้ก่อน ซึ่งข้อบกพร่องนี้เกิดจากการเลือกใช้งานเคสและฟิล์มป้องกันหน้าจอบางประเภท เช่น ซิลิโคน หรือพลาสติก เป็นต้น ทำให้เกิดช่องว่างรบกวนการสแกนลายนิ้วมือ

ทั้งนี้ธนาคารหลายแห่งในหลายประเทศได้แจ้งการถอนแอป mobile banking ของธนาคารออกจาก Play store และไม่รองรับการใช้งานโทรศัพท์ Samsung ในรุ่นที่ได้รับผลกระทบดังกล่าวด้วย ถึงแม้ว่าในประเทศไทยจะไม่มีประกาศจากธนาคารต่าง ๆ แต่ยังคงต้องให้ความสนใจในการป้องกันผลกระทบอื่นที่อาจตามมาได้

ระบบที่ได้รับผลกระทบ

โทรศัพท์มือถือ Samsung เฉพาะรุ่น Galaxy Note10/10+ และ S10/S10+/S10 5G

วิธีการตรวจสอบ

สำหรับผู้ที่ใช้เคสหรือฟิล์มที่อาจมีความเสี่ยง ให้ทดสอบโดยการปลดล็อกหน้าจอด้วยลายนิ้วมืออื่นที่ไม่ได้ลงทะเบียนไว้ หากสามารถปลดล็อกหน้าจอได้ แสดงว่าฟิล์มหรือเคสนั้นอาจก่อให้เกิดความเสี่ยงที่ผู้ประสงค์ร้ายปลดล็อกหน้าจอได้

ผลกระทบที่อาจเกิดขึ้น

ผู้ประสงค์ร้ายสามารถปลดล็อกโทรศัพท์มือถือที่ใช้วิธีการยืนยันตัวตนด้วยลายนิ้วมือได้ รวมถึงการทำธุรกรรมต่าง ๆ ที่ต้องใช้การยืนยันตัวตนด้วยลายนิ้วมือบนโทรศัพท์รุ่นที่ได้รับผลกระทบ

คำแนะนำสำหรับผู้ใช้งานที่ได้รับผลกระทบ

1. เก็บรักษาโทรศัพท์มือถือไว้ให้ปลอดภัย เพื่อป้องกันผู้ประสงค์ร้ายลักลอบปลดล็อกโทรศัพท์ และแอบอ้างทำธุรกรรมแทนผ่านการยืนยันตัวตนด้วยลายนิ้วมือได้
2. อัปเดตระบบปฏิบัติการ ซึ่งทางบริษัทได้ประกาศว่ามีการปล่อยอัปเดตแล้ว โดยเลือกจากเมนู “อัปเดตซอฟต์แวร์ หรือ Update Software” ในส่วน การตั้งค่า (Settings)
3. เปลี่ยนฟิล์มป้องกันหน้าจอ โดยเลือกผลิตภัณฑ์ที่ผ่านการรับรองของบริษัท พร้อมทั้งลงทะเบียนลายนิ้วมือใหม่
4. ยกเลิกการใช้งานปลดล็อกหน้าจอด้วยไบโอเมตริกซ์ จนกว่าจะติดตั้งอัปเดตจากบริษัท

เอกสารอ้างอิง

1. <https://news.samsung.com/global/statement-on-fingerprint-recognition-issue>
2. <https://www.bleepingcomputer.com/news/security/samsung-galaxy-s10-fingerprint-reader-defeated-by-silicone-case/>
3. https://www.gsmarena.com/samsung_issues_statement_following_reports_of_fingerprint_vulnerability_on_s10_note10-news-39708.php
4. <https://it.toolbox.com/blogs/tomolzak/samsung-galaxy-s10-fingerprint-scanner-hacked-threats-and-vulnerabilities-today-04-10-2019-041019>

TR19-007

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

เอกสารเผยแพร่

5 Steps เช็ค ข่าวร์ แชร์ !!!

TLP: WHITE



เผยแพร่วันที่ 17 ธันวาคม 2562

ปัจจุบันทุกคนสามารถเข้าถึง สร้าง และแชร์ข่าวสารต่างๆ ได้ อย่างง่ายดายและรวดเร็ว ผ่านช่องทางสื่อสังคมออนไลน์ อีเมล เว็บไซต์ และโปรแกรมสนทนา และช่องทางอื่นๆ อีกมากมาย ทำให้มีข่าวทั้งจริงและข่าวลวงถูกเผยแพร่ในวงกว้าง ที่อาจส่งผลให้เกิดความเสียหายต่อบุคคลที่ถูกกล่าวถึงในข่าวสาร ดังนั้นก่อนจะแชร์ข่าวสารต่างๆ จำเป็นต้องตรวจสอบให้แน่ใจก่อนว่าข่าวนั้นถูกต้องและสามารถแชร์ได้ ซึ่งมีขั้นตอนดังนี้

1. ตั้งสติ คิดไตร่ตรอง

พิจารณาข่าวสารที่ได้รับอย่างเป็นกลาง ว่าสมเหตุสมผล หรือข่าวสารดังกล่าวมีความเป็นไปได้ที่จะเป็นจริงมากน้อยเพียงใด



2. ตรวจสอบแหล่งที่มา และวันที่

ตรวจสอบความน่าเชื่อถือของข้อมูล แหล่งที่มา ผู้เขียน และวันที่ โดยค้นหาจากสำนักข่าวต่างๆ รวมถึงแหล่งอ้างอิงที่เชื่อถือได้



3. ตรวจสอบองค์ประกอบที่น่าสงสัย

ตรวจสอบองค์ประกอบร่วมในข่าวนั้น เช่น คำผิด ตัวสะกด และภาพที่ใช้ประกอบ เป็นต้น ซึ่งหากเป็นข่าวจริงมักไม่มีคำผิดเนื่องจากจะได้รับการตรวจทานและแก้ไขอย่างถี่ถ้วนมาแล้ว

4. ปรึกษาผู้รู้

ติดต่อสอบถามไปยังผู้ที่มีความเชี่ยวชาญ หรือหน่วยงานที่ถูกอ้างอิงในข่าวสารก่อนแชร์ข่าวนั้นๆ ออกไป

5. “ข่าวลวง” ควรรีบเตือนให้ผู้อื่นทราบ

เมื่อพบว่าเป็นข่าวลวง ควรจะบอกให้ผู้อื่นทราบ และห้ามแชร์ต่อ เพื่อป้องกันไม่ให้ข่าวลวงนั้นกระจายออกไป

หมายเหตุ การนำเข้าหรือแชร์ข้อมูลอันเป็นเท็จ มีความผิดทางกฎหมาย มีโทษทั้งจำและปรับ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2560 มาตรา 14

TB19-009

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง



เอกสารเผยแพร่

 TB-CERT Thailand Banking Sector CERT	TR19-008 คำแนะนำเกี่ยวกับการรับมือการโจมตีของ กลุ่มแฮกเกอร์ Fancy Bear (APT28)	
--	---	---

คำแนะนำเกี่ยวกับการรับมือการโจมตีของกลุ่มแฮกเกอร์ Fancy Bear (APT28)

เผยแพร่วันที่ 8 พฤศจิกายน 2562

ปรับปรุงล่าสุดวันที่ 8 พฤศจิกายน 2562

ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (Thailand Banking Sector CERT หรือ TB-CERT) ได้รับข้อมูลจาก JPCERT/CC [1] เรื่องการโจมตีแบบการปฏิเสธการให้บริการ (Distributed Denial of Services หรือ DDoS) ของกลุ่มผู้โจมตีชื่อ APT28 หรือ Fancy Bear ที่มีการส่งอีเมลล์ ช่มชู้ ดังรูปที่ 1 เพื่อเรียกค่าไถ่จากหน่วยงานในสถาบันการเงิน หน่วยงานราชการ และกลาโหม เป็นต้น ซึ่งเหตุการณ์นี้เกิดขึ้นในประเทศหลายประเทศ

กลุ่มแฮกเกอร์นี้โจมตีผ่านโปรโตคอลต่าง ๆ ได้แก่ DNS NTP และ CLDAP รวมไปถึงโปรโตคอล WS Discovery (UDP/3702 multicast address 239.255.255.250) ซึ่งเคยพบการเพิ่มปริมาณทราฟฟิกได้ถึง 15,300% [2] และ ARMS-Apple Remote Management Service (UDP/3283) [3] ด้วย

ลักษณะของอีเมล

Sender: <sender_name>@ctemplar[.]com

--MESSAGE--

We are the Fancy Bear and we have chosen **[redacted]** as target for our next DDoS attack. Please perform a google search for "Fancy Bear" to have a look at some of our previous work. Your network will be subject to a DDoS attack starting at Monday (in 5 days). (This is not a hoax, and to prove it right now we will start a small attack on **[redacted IP]** that will last for 30 minutes. It will not be heavy attack, and will not cause you any damage so don't worry, at this moment.) What does this mean? This means that your website and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation amongst your users / customers. How do I stop this? We will refrain from attacking your servers for a small fee. The current fee is 2 Bitcoin (BTC). The fee will increase by 1 Bitcoin for each day after deadline that passed without payment. Please send Bitcoin to the following Bitcoin address: 1DBm16Z53Z4mfVj6fffxLRdZtWF9vJnCWl. Once you have paid we will automatically get informed that it was your payment. Please note that you have to make payment before the deadline or the attack WILL start! What if I don't pay? If you decide not to pay, we will start the attack on the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution (Cloudflare, Sucuri, Imperva and similar services are useless). We will completely destroy your reputation and make sure your services will remain offline until you pay. Do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again. Please note that Bitcoin is anonymous and no one will find out that you have complied.

--End of MESSAGE--

เอกสารเผยแพร่



Subject: DDoS attack

We are the Fancy Bear and we have chosen XXX as target for our next DDoS attack.

Please perform a google search for "Fancy Bear" to have a look at some of our previous work.

Your network will be subject to a DDoS attack starting at Wednesday (within X days).

(This is not a hoax, and to prove it right now we will start a small attack on a few of your IPs that will last for 30 minutes. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.)

What does this mean?

This means that your website and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your users / customers.

How do I stop this?

We will refrain from attacking your servers for a small fee. The current fee is 2 Bitcoin (BTC). The fee will increase by 1 Bitcoin for each day after deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address:

[illegible]

Once you have paid we will automatically get informed that it was your payment. Please note that you have to make payment before the deadline or the attack WILL start!

What if I don't pay?

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution (Cloudflare, Incapsula and similar services are useless). We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again.

Please note that Bitcoin is anonymous and no one will find out that you have complied.

รูปที่ 1 แสดงลักษณะอีเมลข่มขู่ [1]

เอกสารเผยแพร่

 TB-CERT Thailand Banking Sector CERT	TR19-008 คำแนะนำเกี่ยวกับการรับมือการโจมตีของ กลุ่มแฮกเกอร์ Fancy Bear (APT28)	
--	---	---

Indicator of Compromise (IOC)

[IP]

213.193.124[.]178	77.245.135[.]76	87.251.185[.]197	186.249.85[.]62	173.225.97[.]59
73.222.102[.]43	87.238.149[.]14	43.252.18[.]154	78.96.4[.]97	180.100.133[.]21
141.213.30[.]81	137.99.120[.]107	190.218.75[.]12	1.225.103[.]192	186.233.204[.]15
93.148.227[.]167	184.67.233[.]66	73.215.166[.]26	73.184.131[.]152	194.165.135[.]37
90.79.181[.]162	181.126.191[.]95	186.4.206[.]69	78.96.4[.]97	201.20.109[.]156
128.9.168[.]175	95.180.32[.]125	160.226.137[.]18	1.225.103[.]192	207.99.1[.]106
82.112.195[.]37	181.51.57[.]46	98.242.135[.]12	78.96.4[.]97	216.15.163[.]130
80.219.165[.]93	77.120.40[.]141	181.46.188[.]24	186.249.85[.]62	220.243.237[.]14
179.219.122[.]179	188.0.152[.]204	24.139.113[.]96	62.112.106[.]10	222.216.190[.]151
128.255.242[.]214	195.35.85[.]169	50.206.77[.]90	91.211.245[.]17	24.103.42[.]134
135.23.41[.]7	177.0.33[.]194	161.43.205[.]202	73.184.131[.]152	42.123.67[.]10
141.219.40[.]200	47.51.133[.]130	93.170.188[.]147	179.52.58[.]71	62.32.103[.]141
134.102.89[.]135	92.83.149[.]135	202.160.16[.]144	167.59.10[.]111	69.174.3[.]94
207.61.192[.]156	31.211.144[.]80	220.130.80[.]212	103.63.190[.]66	70.88.196[.]178
96.47.194[.]168	13.94.104[.]145	1.225.103[.]192	54.171.57[.]68	71.71.127[.]49
50.246.36[.]5	78.131.204[.]106	186.249.86[.]98	104.130.2[.]169	77.81.107[.]173
185.44.131[.]72	109.199.51[.]209	81.25.62[.]153	104.225.15[.]131	77.81.107[.]189
1.224.87[.]99	89.218.62[.]12	73.184.131[.]152	107.0.160[.]33	77.81.110[.]208
185.44.128[.]135	54.36.172[.]201	125.75.132[.]53	116.196.93[.]71	77.81.110[.]36
93.190.144[.]101	40.76.194[.]159	162.151.72[.]86	123.56.73[.]58	85.17.68[.]133
89.42.31[.]105	93.107.107[.]147	98.197.252[.]15		

เอกสารเผยแพร่

 TB-CERT Thailand Banking Sector CERT	TR19-008 คำแนะนำเกี่ยวกับการรับมือการโจมตีของ กลุ่มแฮกเกอร์ Fancy Bear (APT28)	
--	---	---

คำแนะนำ

1. หากได้รับอีเมลล์ขู่การโจมตี อย่าจ่ายเงินเด็ดขาด
2. เผื่อระวังหรือพิจารณาปิดกั้นการโจมตีที่อาจมาจากหมายเลขไอพีตามที่แจ้งไว้ในส่วนค่า Indicator of Compromise
3. ประเมินผลกระทบที่อาจเกิดขึ้น และเตรียมรายงานสถานการณ์ต่อผู้บริหาร หากมีเหตุการณ์ดังกล่าวเกิดขึ้น และดำเนินการตามกระบวนการตอบสนองเหตุการณ์ด้านความปลอดภัย (Incident Response Process)
4. ประสานงานกับผู้ให้บริการอินเทอร์เน็ต ในการปิดกั้นทราฟฟิกจากภายนอกสู่เครือข่ายของหน่วยงานตามโปรโตคอล UDP/53 UDP/123 UDP/3702 และ UDP/3283 หากไม่ได้ใช้งาน
5. ประสานงานกับผู้ให้บริการอินเทอร์เน็ต เพื่อเผื่อระวังที่อุปกรณ์เครือข่ายที่เกี่ยวข้อง โดยเฉพาะอุปกรณ์ที่ใช้ในการป้องกัน DDoS หรือ DDoS protection อย่างใกล้ชิด
6. ประสานงานกับผู้ให้บริการอินเทอร์เน็ต เพื่อเตรียมมาตรการรับมือร่วมกัน เช่น การกรองทราฟฟิก (filter traffic) หรือ การบีบแบนด์วิดท์ (shape bandwidth) ที่เข้ามายังเป้าหมายการโจมตี เป็นต้น
7. เผื่อระวังปริมาณแบนด์วิดท์ที่มีลักษณะผิดปกติ หากพบความผิดปกติ ให้วิเคราะห์ประเภทของทราฟฟิกที่ทำให้เกิดความผิดปกตินั้น และแจ้ง TB-CERT ให้รับทราบเพื่อเตรียมการป้องกันต่อไป
8. เตรียมการสื่อสารความกับลูกค้า หากเกิดเหตุการณ์โจมตีจริง

เอกสารอ้างอิง

1. <https://www.jpcert.or.jp/newsflash/2019103001.html>
2. <https://www.wired.com/story/ddos-attack-ws-discovery/>
3. <https://www.netsecscout.com/blog/asert/call-arms-apple-remote-management-service-udp>
4. <https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-ddos-tevekenysegre-figyelmezteto-zsarololevellel-kapcsolatban/>

คณะกรรมการ TB-CERT

ดร.กิตติ โมะวิสุทธ์ ประธานกรรมการ		ธนาคารกรุงเทพ Senior Vice President Head of Security Management	
ชัยวัฒน์ อัครวิวงศ์ รองประธานกรรมการ		บริษัท กลสิกร บิซิเนส-เทคโนโลยี กรุ๊ป Deputy Managing Director Head of IT Security	
ภคพงศ์ จุลวงศาธิลปี กรรมการ	ธนาคารกรุงศรีอยุธยา Senior Vice President Cyber Security Department	นฤตม รุ่งศิริวงศ์ กรรมการ	ธนาคารเกียรตินาคิน Senior Vice President IT Security Head
สมบูรณ์ ทิริญภัทรศิลป์ กรรมการ	ธนาคารสแตนดาร์ด ชาร์เตอร์ด Head Country Technology Management	ประกลกฤษ แสงชูวงศ์ กรรมการ	ธนาคารทหารไทย Team Head of Information Security Detection and Response
ยศ กิมสวัสดิ์ เลขานุการ		สมาคมธนาคารไทย Head of Payment System Office (PSO)	
กิตติศักดิ์ จิรวรรณกุล ผู้ช่วยเลขานุการ	สมาคมธนาคารไทย CERT Manager	ธาวินี วงศ์วิเศษ ผู้ช่วยเลขานุการ	สมาคมธนาคารไทย CERT Relation Manager

สมาชิก TB-CERT



ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
Bank of Agriculture and Agricultural
Cooperatives



ธนาคารเกียรตินาคิน จำกัด (มหาชน)
Kiatnakin Bank Public Company
Limited



ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)
Bank of Ayudhya Public Company Limited
(Krungsri)



ธนาคารกรุงไทย จำกัด (มหาชน)
Krung Thai Bank Public Company Limited



ธนาคารกรุงเทพ จำกัด (มหาชน)
Bangkok Bank Public Company Limited



ธนาคารแลนด์ แอนด์ เฮาส์ จำกัด (มหาชน)
Land and Houses Bank Public
Company Limited



ธนาคารแห่งประเทศไทย
Bank of Thailand



บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด
National Credit Bureau Company
Limited



ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน)
CIMB Thai Bank Public Company Limited



บริษัท ศูนย์ประมวลผล จำกัด
Processing Center Company Limited



ธนาคารซิตีแบงก์
Citibank N.A.



ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
The Siam Commercial Bank Public
Company Limited



ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย
Export-Import Bank of Thailand



ธนาคารสแตนดาร์ดชาร์เตอร์ด (ไทย) จำกัด
(มหาชน)
Standard Chartered Bank (Thai) Public
Company Limited



ธนาคารอาคารสงเคราะห์
Government Housing Bank



ธนาคารธนชาต จำกัด (มหาชน)
Thanachart Bank Public Company Limited



ธนาคารออมสิน
Government Savings Bank



ธนาคารไทยเครดิต เพื่อรายย่อย จำกัด
(มหาชน)
The Thai Credit Retail Bank Public
Company Limited



ธนาคารไอซีบีซี (ไทย) จำกัด (มหาชน)
Industrial and Commercial Bank of China
(Thai) Public Company Limited (ICBC Thai)



ธนาคารทีเอสซี จำกัด (มหาชน)
TISCO Bank Public Company Limited



ธนาคารอิสลามแห่งประเทศไทย
Islamic Bank of Thailand



ธนาคารทหารไทย จำกัด (มหาชน)
TMB Bank Public Company Limited



บริษัท เนชั่นแนล โอทีเอ็มเอ็กซ์ จำกัด
National ITMX Company Limited



ธนาคารยูโอบี จำกัด (มหาชน)
United Overseas Bank (Thai) Public
Company Limited



ธนาคารกสิกรไทย จำกัด (มหาชน)
(KASIKORNBANK Public Company Limited)



บริษัท วีซ่า อินเตอร์เนชั่นแนล ประเทศไทย
จำกัด
Visa International (Thailand) Ltd.

IN COLLABORATION WE TRUST



BUILDING A RESILIENT ORGANIZATIONAL CULTURE





TB-CERT

Thailand Banking Sector CER1



ANNUAL REPORT

2019

Security is not the responsibility for IT alone, It Is belong to
Everyone in your organization that needs to well manage it.



The Thai Bankers' Association
4th Fl., 5/13 Moo 3, Chaengwattana Rd.,
Pakkret, Nonthaburi 11120
Phone: 025587500
Website: www.tba.or.th



TB-CERT
Thailand Banking Sector CERT