

ภัยคุกคามในระบบสารสนเทศ

Threat information system



Threat information system

ภัยคุกคามในระบบสารสนเทศ

ประเภทของภัยคุกคาม
Rootkit

ประเภทของภัยคุกคาม	ตัวอย่างภัยคุกคาม
<ul style="list-style-type: none"> ● ความผิดพลาดที่เกิดจากบุคคล Human Error/Failure ● ภัยร้ายต่อทรัพย์สินทางปัญญา Compromises to Intellectual Property ● การจารกรรมหรือการรุกล้ำ Espionage or Trespass ● การกรรโชกสารสนเทศ Information Extortion 	<ul style="list-style-type: none"> ● อุบัติเหตุ ความเข้าใจผิดของพนักงาน ● การละเมิดลิขสิทธิ์ ● การเข้าถึงหรือการรวบรวมข้อมูลโดยไม่ได้รับอนุญาต ● การ Backmail การเผยแพร่สารสนเทศที่เป็นความลับ



1. ความผิดพลาดที่เกิดจากบุคคล

Human Error/Failures

เป็นความผิดพลาดที่เกิดจากพนักงานหรือบุคคลที่ได้รับอนุญาตให้เข้าถึงสารสนเทศขององค์กร ได้อาจเกิดจากความไม่ได้ตั้งใจ เนื่องจากไม่มีประสบการณ์ หรือขาดการฝึกอบรม หรือคาดเดา เป็นต้น ป้องกันภัยคุกคาม โดยการให้ความรู้ด้านความมั่นคงปลอดภัยของสารสนเทศ การฝึกอบรมอย่างสม่ำเสมอ มีมาตรการควบคุม

Threat information system

ภัยคุกคามในระบบสารสนเทศ

ประเภทของภัยคุกคาม (ต่อ)

Rootkit



2. ภัยร้ายต่อทรัพย์สินทางปัญญา Comromises to Intellectual Property

ทรัพย์สินทางปัญญา Intellectual Property คือทรัพย์สินที่จับต้องไม่ได้ ที่ถูกสร้างขึ้นโดยบุคคลหรือองค์กรใด ๆ หากต้องการนำทรัพย์สินทางปัญญาของผู้อื่น ไปใช้ อาจต้องเสียค่าใช้จ่าย และจะต้องระบุแหล่งที่มาของทรัพย์สิน ดังกล่าวไว้อย่างชัดเจน

ในทางกฎหมาย การให้สิทธิในความเป็นเจ้าของทรัพย์สินทางปัญญา มี 4 ประเภทคือ ลิขสิทธิ์ (copyrights) ความลับทางการค้า(Trade Secrets) เครื่องหมายการค้า (Trade Marks) สิทธิบัตร(Patents)

Threat information system

ภัยคุกคามในระบบสารสนเทศ

ประเภทของภัยคุกคาม (ต่อ)

Rootkit



Threat information system

ภัยคุกคามในระบบสารสนเทศ

การละเมิดความคุ้มครองทรัพย์สินทางปัญญาที่มากที่สุดคือ การละเมิดลิขสิทธิ์ซอฟต์แวร์

(Software Piracy)

สามารถหาความรู้เพิ่มเติม เรื่อง ทรัพย์สินทางปัญญาได้ที่ www.ipthailand.org

ประเภทของภัยคุกคาม (ต่อ)

Rootkit

DIP กรมทรัพย์สินทางปัญญา
DEPARTMENT OF INTELLECTUAL PROPERTY

กลุ่มงานประชาสัมพันธ์	44100 ถนนนนทบุรี 1 ตำบลบางกระพ้อ อำเภอเมือง จังหวัดนนทบุรี 11000 โทรศัพท์ / โทรสาร 0-2547-4696
สำนักงานเลขานุการกรม	44100 Nonthaburi 1Rd., Tumbon Bangkrasor, Amphur Muang, Nonthaburi 11000 Tel/Fax 0-2547-4696



3. การจารกรรมหรือการรुकล้ำ

Espionage or Trespass

การจารกรรมหรือการรुकล้ำ (Espionage or Trespass)

การจารกรรม Espionage เป็นการที่กระทำซึ่งใช้อุปกรณ์อิเล็กทรอนิกส์ หรือตัวบุคคลในการจารกรรมสารสนเทศ ที่เป็นความลับผู้จารกรรมจะใช้วิธีการต่าง ๆ เพื่อให้ถึงซึ่งสารสนเทศที่จัดเก็บไว้ และรวบรวมสารสนเทศนั้น โดยไม่ได้รับอนุญาต Industrial Espionage วิธีนี้เป็นการใช้เทคนิคที่ถูกกฎหมายแต่ก้ำกึ่งความไม่ชอบธรรม เพื่อรวบรวมสารสนเทศที่สำคัญหรือความลับทางการค้าของคู่แข่งเพื่อนำมาหาผลประโยชน์

Threat information system

ภัยคุกคามในระบบสารสนเทศ

ประเภทของภัยคุกคาม (ต่อ)

Rootkit



ความแตกต่างระหว่าง Hacker / Cracker

Hacker มีเป้าหมายเพื่อทดสอบความสามารถหรือต้องการทำร้ายโดยการเจาะระบบให้สำเร็จ



Threat information system

ภัยคุกคามในระบบสารสนเทศ

ประเภทของภัยคุกคาม (ต่อ)

Rootkit



ความแตกต่างระหว่าง Hacker / Cracker

Cracker มีจุดประสงค์คือ ต้องการทำลายระบบความมั่นคง ปลอดภัยของระบบคอมพิวเตอร์หรือระบบสารสนเทศ



Threat information system

ภัยคุกคามในระบบสารสนเทศ

ประเภทของภัยคุกคาม (ต่อ)

Rootkit



Threat information system

ภัยคุกคามในระบบสารสนเทศ

หนอนคอมพิวเตอร์
Computer Worm

หนอนคอมพิวเตอร์ (Computer Worm)

คือ หน่วยย่อยลงมาจากไวรัสคอมพิวเตอร์ ปกติแล้ว หนอนคอมพิวเตอร์จะแพร่กระจายโดยไม่ผ่านการใช้งานของผู้ใช้ โดยมันจะคัดลอกและกระจายตัวมันเองข้ามเครือข่าย เช่น ระบบเครือข่าย หรือ อินเทอร์เน็ต เป็นต้น หนอนคอมพิวเตอร์สามารถทาลายข้อมูลและแบนด์วิธ สร้างความเสียหายให้กับคอมพิวเตอร์รวมถึงการทำให้คอมพิวเตอร์หยุดทำงาน



Threat information system

ภัยคุกคามในระบบสารสนเทศ

มัลแวร์
Malware

มัลแวร์ (Malware)

คือความไม่ปกติทางโปรแกรม ที่สูญเสีย C (Confidentiality), I (Integrity) และ A (Availability) อย่างไม่อย่างหนึ่ง หรือทั้งหมด จนเกิดเป็นไวรัส เวิร์ม โทรจัน สปายแวร์ Backdoor และ Rootkit

- การสูญเสีย C (Confidentiality) คือ สูญเสียความลับทางข้อมูล
- การสูญเสีย I (Integrity) คือ สูญเสียความไม่เปลี่ยนแปลงของข้อมูล นั่นคือ ข้อมูลถูกเปลี่ยนแปลงแก้ไข โดยเฉพาะส่วนสำคัญที่เกี่ยวข้องกับระบบภายในระบบปฏิบัติการ
- การสูญเสีย A (Availability) คือ สูญเสียเสถียรภาพของระบบปฏิบัติการ



Threat information system

ภัยคุกคามในระบบสารสนเทศ

โทรจัน (Trojan)

หมายถึง โปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปในคอมพิวเตอร์ เพื่อลักลอบเก็บข้อมูลของคอมพิวเตอร์เครื่องนั้น เช่น ข้อมูลชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคล อื่น ๆ โดยส่วนใหญ่แฮคเกอร์จะส่งโปรแกรมเข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนำไปใช้ในการเจาะระบบเพื่อโจมตีคอมพิวเตอร์, เซิร์ฟเวอร์, หรือระบบเครือข่ายอีกที ซึ่งเป็นที่รู้จักกันในชื่อการโจมตีเพื่อ "ปฏิเสธการให้บริการ" (Denial of Services)

Trojan Horse

ม้าโทรจัน



Threat information system

ภัยคุกคามในระบบสารสนเทศ

Backdoor

Backdoor

ในทางความมั่นคงของระบบคอมพิวเตอร์ หมายถึง รูรั่วของระบบรักษาความมั่นคง ที่ผู้ออกแบบหรือผู้ดูแลใจทิ้งไว้ โดยเป็นกลไกลัดทางซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ข้ามผ่านการควบคุมความมั่นคง แต่อาจเปิดทางให้ผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบและก่อความเสียหายได้



Threat information system

ภัยคุกคามในระบบสารสนเทศ

Rootkit

Rootkit

เป็นโปรแกรมที่ออกแบบมาเพื่อซ่อนอ็อบเจกต์ต่างๆ เช่น กระบวนการ ไฟล์ หรือ ข้อมูลใน Registry แม้จะเป็นโปรแกรมที่อาจไม่เป็นอันตรายเสมอไป แต่ก็ถูกนำมาใช้ในการซ่อนกิจกรรมที่เป็นอันตรายมากขึ้นในปัจจุบัน ทำให้คอมพิวเตอร์ใดๆ สามารถส่งสแปมหรือทำการโจมตีคอมพิวเตอร์เครื่องอื่นๆ ได้โดยที่ผู้ใช้เป้าหมายไม่สามารถล่วงรู้และ โปรแกรมด้านความปลอดภัยทั่วไปไม่สามารถตรวจจับได้



Threat information system

ภัยคุกคามในระบบสารสนเทศ

BOTNET

BOTNET

เป็นเครือข่ายหุ่นรบที่เป็นสะพานเชื่อมภัยคุกคามทางเครือข่ายคอมพิวเตอร์ ด้วยมัลแวร์ทั้งหลายเพื่อต่อยอดความเสียหาย และทำให้ยากแก่การควบคุมมากขึ้น ตัวนำทางที่วานี้ก็คือ Botnet ซึ่งก่อให้เกิดภัยคุกคามที่ไม่สามารถเกิดขึ้นได้เองโดยลำพัง เช่น Spam, DoS/DDoS และ Phishing เป็นต้น





Spam

สแปม สแปม สแปมที่น่ารังเกียจ เปรียบได้กับเมลขยะอิเล็กทรอนิกส์บนพรหมเช็ดเก้าคุณ เป็นผู้นำด้านความน่ารำคาญในยุคของอินเทอร์เน็ตเลยทีเดียว อ่านคำแนะนำของเราเกี่ยวกับความอันตรายของสแปม และวิธีป้องกันกล่องจดหมายของคุณให้ปราศจากสแปม

Spam Mail

หรืออีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ antispam หรือหากใช้ฟรีอีเมล เช่น hotmail, yahoo ก็จะมีโปรแกรมคัดกรองอีเมลขยะในชั้นหนึ่งแล้ว

Spam Mail



Threat information system

ภัยคุกคามในระบบสารสนเทศ

Phishing



Phishing

อาจจะไม่ใช่ปลาหรือคนเบ็ดให้เห็น แต่บ่อยครั้งที่มี "การตกขอรวัน" สำหรับอาชญากรด้วยการใช้เทคนิคนี้ พวกเขาสามารถทำการขโมยโดยใช้การหลอกลวงทางอินเทอร์เน็ตและอีเมล เพื่อให้ผู้ใช้งานทำการเปิดเผยข้อมูลส่วนตัวของพวกเขาเหล่านั้น

Phishing

คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือ หมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซ็นเจอร์



Crimeware



Crimeware

ไม่ว่าจะเป็นโทรจัน คีย์ลอคเกอร์หรือสปายแวร์ Crimeware' เป็นตัวแทนของภัยคุกคามชนิดใหม่ต่อความปลอดภัยของเรา กลายเป็นอุปสรรคใหม่ในการต่อสู้กับอาชญากรรมใน ศตวรรษที่ 21 จระวิงไว้ให้ดี

Threat information system

ภัยคุกคามในระบบสารสนเทศ

Crimeware



Threat information system

ภัยคุกคามในระบบสารสนเทศ



Passwords

การเลือกใช้รหัสผ่านที่ดีเป็นสิ่งที่สำคัญในการอยู่อย่างปลอดภัยในโลกออนไลน์เพียงแค่ปฏิบัติตามกฎเหล็กต่างๆ ซึ่งเป็นเรื่องที่น่าตกใจว่ามีคนมากมายกลับละเลย สิ่งเหล่านี้ และ 3 รหัสผ่านที่ถูกใช้มากที่สุดบนอินเทอร์เน็ต? 'password', 'monkey' และ '123456'

Passwords



Threat information system

ภัยคุกคามในระบบสารสนเทศ



Symptoms

เมื่อพวกมัลแวร์พยายามที่จะทำให้คอมพิวเตอร์ของเราติดเชื
 ก็จะใช้วิธีที่แยบยลในการกลบรอยขอพวกมัน แล้วเราจะรู้ได้อย่างไร
 ถ้าคอมพิวเตอร์ของเรานั้นติดไวรัส?

คอมพิวเตอร์ที่ติดเชื้อจะมีอาการอย่างไร?

Symptoms



5 อันดับไวรัสคอมพิวเตอร์ที่สร้างความเสียหายร้ายแรงมากที่สุด



1. Mydoom (2004)



Threat information system

ภัยคุกคามในระบบสารสนเทศ

Threat information system

ภัยคุกคามในระบบสารสนเทศ

สรุป 10 วิธีป้องกันภัยคุกคามทางอินเทอร์เน็ต สำหรับการใช้งานส่วนบุคคล

- ตั้งสติก่อนเปิดเครื่อง
- กำหนด Password ที่ยากแก่การคาดเดา
- สังเกตขณะเปิดเครื่อง
- หมั่นตรวจสอบและอัปเดต OS หรือซอฟต์แวร์ที่ใช้
- ไม่ลงซอฟต์แวร์มากเกินไปจนจำเป็น
- ไม่ควรเข้าเว็บไซต์เสี่ยงภัย
- สังเกตความปลอดภัยของเว็บไซต์ที่ ให้บริการธุรกรรมออนไลน์
- ไม่เปิดเผยข้อมูลส่วนตัวลงบนเว็บ Social Network
- ศึกษาถึงข้อกำหนดเกี่ยวกับการใช้สื่ออินเทอร์เน็ต
- ไม่หลงเชื่อโดยง่าย

สรุป 10 วิธีป้องกันภัยคุกคามทางอินเทอร์เน็ต สำหรับการใช้งานส่วนบุคคล













Threat information system

ภัยคุกคามในระบบสารสนเทศ

2014 BEST

Best Antivirus Software Review

REVIEWS AND COMPARISONS

Gold Award Winner	Rankings								
#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
									
Bitdefender Antivirus Plus	Kaspersky Anti-Virus	Norton AntiVirus	F-Secure Anti-Virus	AVG Anti-Virus	BullGuard Antivirus	G Data AntiVirus	Panda Antivirus Pro	Avast! Pro Antivirus	McAfee AntiVirus Plus
\$29.95	\$59.95	\$39.99	\$39.99	\$34.99	\$29.95	\$29.95	\$35.99	\$39.99	\$39.99
READ REVIEW »	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW	REVIEW
VISIT SITE »	VISIT SITE	VISIT SITE	VISIT SITE	VISIT SITE	VISIT SITE	VISIT SITE	VISIT SITE	VISIT SITE	VISIT SITE

Antivirus 2014

