Vol 2 No 12 (16 June 2005)
IT Digest
By R&D Strategy Development, NECTEC.
Email: it-digest@nectec.or.th
ISSN 1686-7602
A biweekly newsletter from NECTEC to information technology leaders in Thailand.

เรื่องประจำฉบับ

แฮกเกอร์บนโลกไซเบอร์ (21201)

ภาพจาก BusinessWeek.com

ในช่วงไม่กี่สัปดาห์ที่ผ่านมาบริษัท มาสเตอร์การ์ด อินเตอร์เนชันแนล อิงค์ (Mastecard International Inc.) ซึ่งเป็นผู้ให้บริการบัตรเครดิตรายใหญ่ของโลกจากประเทศสหรัฐอเมริกา ให้เปิดเผยข้อมูลว่าได้มีผู้ไม่ประสงค์ดีเจาะเข้าไปในเครือข่ายของการ์ดซิสเตมส์ โซลูชั่น อิงค์ (CardSystem Solution Inc.) ซึ่งให้บริการด้านการชำระเงินต่างๆ ให้แก่บริษัทบัตรเครดิตและธนาคารพาณิชย์ การเจาะระบบดังกล่าวทำให้ข้อมูลทางการเงินบางอย่างของลูกค้าบัตรเครดิตเกิดการสูญหาย แต่ข้อมูลส่วนตัวอื่นๆ อาทิ เลขที่บัตรประกันสังคมและวันเดือนปีเกิดยังปลอดภัยอยู่

ข่าวดังกล่าวสร้างความตื่นตะหนกและก่อให้เกิดความเคลื่อนไหวในการตรวจสอบข้อเท็จจริงรวมทั้งความเสียหายที่เกิดขึ้น ภายหลังการตรวจสอบพบว่ามีลูกค้าของมาสเตอร์การ์ดเพียง 68,000 ราย จากทั้งหมด 40 ล้านรายเท่านั้นที่ได้รับผลกระทบจากเหตุการณ์ดังกล่าว บริษัทฯ เชื่อว่าความเสียหายที่เกิดขึ้นน่าจะมาจากความ ผิดพลาดของการทำงานของระบบมากกว่าเป็นการกระทำของบุคคลที่ไม่ประสงค์ดี หรือแฮกเกอร์ (Hacker) ขณะที่หน่วยสืบสวนกลางสหรัฐ หรือเอฟบีไอ (The FBI) เร่ง ตรวจสอบว่า เป็นฝีมือของแฮกเกอร์หรือไม่

ที่ผ่านมา บรรดาแฮกเกอร์ทั้งหลายใช่ว่าจะไม่เคยถูกจับมาลงโทษ เมื่อปีที่แล้ว (เดือนตุลาคม 2547) กลุ่มแฮกเกอร์ชื่อ Shadow Crew.com ซึ่งเป็นหนึ่งในเครือข่ายแฮกเกอร์รายใหญ่ ได้ถูกจับกุมโดย U.S. Secret Service ในการจับกุมดังกล่าว สมาชิกของกลุ่ม Shadow Crew ถึง 28 คนถูกจับพร้อมด้วยของกลางคือ คอมพิวเตอร์ 12 เครื่อง หมายเลขบัตรเครดิตจำนวน 1.7 ล้านหมายเลขและ e-mail account ถึง 18 ล้านชื่อ กลุ่ม ShadowCrew นี้มีสมาชิกกระจายอยู่ทั่วโลกจำนวนมากถึง 4,000 ราย ไม่ว่าเป็นอเมริกา บราซิล อังกฤษ รัสเซีย และสเปน

ภาพจาก: BusinessWeek.com

ShadowCrew หรือที่รู้จักกันในนามแฝงว่า "Scarface" ก่อตั้งมาตั้งแต่ปี 2002 โดย Mr. David Appleyard อายุ 45 ปี และ Mr. Andrew Mantovani ซึ่งมีอายุเพียง 23 ปี ทั้งคู่เปิดเว็บไซต์บังหน้าโดยจะดำเนินการเสมือนว่าเป็นเว็บไซต์ของบริษัทที่ทำธุรกรรมเกี่ยวกับการเคลียร์เงินระหว่างประเทศ ทั้งนี้เพื่อขโมยหมายเลขบัตรเครดิตและรหัสส่วนตัว ส่วนใหญ่แฮกเกอร์เหล่านี้จะเริ่มทำงานในตอนกลางคืนของวันอาทิตย์ในช่วง 22.00 – 02.00 นาฬิกา และมุ่งไปที่ลูกค้าบัตรเครดิตที่มียอดวงเงินสูง โดยการลักลอบขโมยข้อมูลที่สำคัญต่างๆ ของลูกค้า อาทิ ข้อมูลส่วนบุคคล รหัสจากบัตรเครดิต เพื่อทำการปลอมแปลงบัตร หรือทำการนัดพบแบบออนไลน์เพื่อแลกเปลี่ยนข้อมูลหรือซื้อ-ขายข้อมูลที่ขโมยมากับแฮกเกอร์อื่นๆ และที่สำคัญในเว็บไซต์นี้ยังมีการแนะนำเทคนิคและวิธีการต่างๆ ในการเจาะเข้าระบบเพื่อขโมยข้อมูลด้วย ก่อนหน้านี้เคยมีการระบุว่า "Scarface" สามารถขายบัตรเครดิตที่ขโมยข้อมูลมาได้ถึง 115,695 ข้อมูลต่อวัน และมีการคาดการณ์กันว่า ภายในระยะเวลาเพียง 2 ปี Shadow Crew สามารถทำรายได้ถึง 4.3 ล้านเหรียญสหรัฐ ซึ่งมาจากการลักลอบเอาข้อมูลจากบัตรเครดิตและทำการซื้อขายข้อมูลนี้ผ่านระบบการประมูลออนไลน์ (Online Auction) นอกจากนั้น ยังมีรายได้อื่นๆ จากการรับทำเอกสารสำคัญปลอม เช่น พาสปอร์ต บัตรประจำตัว และขายข้อมูลส่วนตัวของลุกค้าบัตรเครดิตที่สำคัญต่างๆ

ตัวอย่างที่ยกมาข้างต้นเป็นเพียงบางส่วนของภัยจากการเจาะระบบ และการขโมยข้อมูลเพื่อฉ้อโกงของกลุ่มมิจฉาชีพหรือแฮกเกอร์บนอินเตอร์เน็ตที่นับวันได้ทวีจำนวนและความรุนแรงมากขึ้น สถิติจาก BusinessWeek แสดงไว้ว่าในปี 2547 ที่ผ่านมาภัยจากแฮกเกอร์ทางอินเตอร์เน็ตมีถึง 207,449 กรณี และสร้างความเสียหายถึง 17.5 พันล้านเหรียญสหรัฐ ซึ่งเพิ่มมากกว่าปี 2546 ถึง 30%

ปัจจุบันเอฟบีไอ (FBI) ได้จัดลำดับภัยอันตรายโดยมีภัยคุกคามทางอิเล็กทรอนิกส์ (e-crime) อยู่ในอันดับที่ 3 รองมาจากภัยก่อการร้าย (Terrorism) และ การสอดแนมจากฝ่ายตรงข้าม (Counter Intelligence) อย่างไรก็ตาม การจับกุมบรรดาแฮกเกอร์ไม่ใช่เรื่องง่าย ส่วนหนึ่งน่าจะมีสาเหตุมาจากการที่กลุ่มแฮกเกอร์ล้วนเป็นผู้ที่มีความสนใจและเชี่ยวชาญด้านคอมพิวเตอร์เป็นอย่างมาก จึงมีความสามารถในการพัฒนาเทคนิคใหม่ๆ ที่หลากหลายรูปแบบมาโจมตีเครือข่ายอินเทอร์เน็ตได้ในเวลาสั้น เช่น Phishing Pharming WI-Phishing และ Typosquatting (ดูคำอธิบายตอนท้าย) ในอีกด้านหนึ่งทางเอฟบีไอถึงแม้จะมีหน่วยที่ดูแลเกี่ยวกับภัยทางอินเตอร์เน็ตแต่ก็ยังขาดงบประมาณเพื่อการสนับสนุนทักษะด้านเทคโนโลยีให้กับเหล่ามือปราบไซเบอร์ นอกจากนั้น ตัวบทกฎหมายก็เป็นปัจจัยสำคัญอีกประการซึ่งถือได้ว่าเป็นอีกรูรั่วหนึ่งที่เปิดโอกาสให้แฮกเกอร์หนีการจับกุมมาลงโทษไปได้ เนื่องจากหลายประเทศยังไม่มีบทกฎหมายเกี่ยวกับอาชญากรรมทางอิเล็กทรอนิกส์ หรือถ้ามีแล้วบทลงโทษก็ไม่รุนแรงพอที่จะทำให้เหล่าแฮกเกอร์กลัว จึงไม่น่าแปลกใจเลยว่าทำไมอัตราภัยคุกคามทางอินเทอร์เน็ตจึงได้เพิ่มขึ้นทุกปี

ตัวอย่างวิธีการเจาะข้อมูลของแฮกเกอร์

เทคนิค	วิธีการ
PHISHING	แฮกเกอร์ทำการสร้างเว็บไซต์ปลอมที่มีเนื้อหาเหมือนเว็บไซต์ของจริง (อาทิ เว็บไซต์ที่เกี่ยวกับการเงินหรือเว็บไซต์ที่เกี่ยวกับการซื้อของออนไลน์) โดยทำการส่งอี-เมล์ เพื่อหลอกลวงให้ผู้รับอี-เมล์ ให้เปิดเผยข้อมูลทางด้านการเงินและข้อมูลส่วนบุคคลอื่นๆ เช่น ข้อมูลของหมายเลขบัตรเครดิต ชื่อผู้ใช้ รหัสผ่าน เป็นต้น
PHARMING	แฮกเกอร์จะทำการโจมตีไปที่ระบบ DNS Server ของผู้ให้บริการอินเตอร์เน็ต (ISP) หรือของบริษัทต่างๆ โดยตรง หรืออีกวิธีการหนึ่งเรียกว่า DNS Hijacking คือทำให้ผู้ใช้บริการคิดว่าได้เข้าไปใน URL ที่ถูกต้องจริงๆ และทำการ "Redirect" URL นั้นไปยังเว็บไซต์ปลอมที่ทำรอไว้ให้เหยื่อหลงเข้าไปติดกับ
WI-PHISHING	แฮกเกอร์จะทำการแสกน หาตำแหน่งของ จุดเชื่อมต่อ (Access Poin) ที่เปิดใช้วายฟาย (Wi-Fi) อย่างไม่ระมัดระวังเรื่องความปลอดภัย เช่น มีการใช้ค่า Default SSID หรือไม่มีการเข้ารหัสด้วยเว็บคีย์ ทำให้แฮกเกอร์สามารถเข้ามาใช้งานระบบทันที เมื่อมีการต่ออินเทอร์เน็ต โดยแฮกเกอร์ก็จะทำการขโมยรหัสผ่านและข้อมูลสำคัญต่างๆของเหยื่อไป
TYPOSQUATTING	แฮกเกอร์จะตั้งเว็บไซต์ที่มีชื่อคล้ายกับเว็บดังๆ แต่จงใจให้มีตัวสะกดผิดเพี้ยนไปนิดหน่อย ดังนั้นเมื่อผู้ใช้อินเทอร์เน็ตพิมพ์ตัวอักษรผิดจากชื่อเว็บไซต์จริง จะทำให้เกิดการเชื่อมต่อไปที่เว็บไซต์ปลอม และถูกโหลดไวรัสเข้าเครื่องโดยอัตโนมัติ

ที่มา : BusinessWeek.com และสำนักข่าวไทย, ธันวาคม 2547

ดิจิทัลพลาสเตอร์ (21202)

"ดิจิทัลพลาสเตอร์" ได้ถูกออกแบบให้มีขนาดเล็กและประหยัดพลังงานมากที่สุด (ภาพจาก: BBC NEWS)

พลาสเตอร์ไฮเทคที่มีอุปกรณ์อิเล็กทรอนิกส์ชิ้นเล็กๆ ติดอยู่นี้ พัฒนาขึ้นโดยนักวิทยาศาสตร์จากมหาวิทยาลัยอิมพีเรียลคอลเลจ ลอนดอน ประเทศอังกฤษ ภายใต้บริษัททูมาซ์ (Toumaz) ซึ่งแยกตัวออกไปจากมหาวิทยาลัย เป็นเครื่องมือที่ใช้ตรวจเช็คสัญญาณที่สำคัญๆ ของสุขภาพ เช่น อุณหภูมิร่างกาย ความดันโลหิต ระดับน้ำตาลในเลือด ฯลฯ หลังจากนั้นจะส่งผลการตรวจวัดไปยังเครื่องคอมพิวเตอร์เพื่อคำนวณหาค่าความผิดปกติของร่างกายที่จำเป็นต้องควบคุมและทำการรักษา ซึ่งเทคโนโลยีใหม่นี้ คาดว่าจะถูกนำมาใช้อย่างแพร่หลายในอีกไม่กี่เดือนข้างหน้า

"ดิจิทัลพลาสเตอร์" นี้ ประกอบด้วยซิลิคอนชิปขนาด 3 คูณ 5 มิลลิเมตร ซึ่งมีระบบเซ็นเซอร์อยู่ภายในหลายตัวทำหน้าที่ตรวจวัดและแสดงปริมาณของอาการผิดปกติที่เกิดขึ้นในร่างกายมนุษย์ได้ โดยในการทำงานนี้เซ็นเซอร์ตัวหนึ่งจะทำหน้าที่ตรวจวัดคลื่นหัวใจและแสดงผลออกมาให้เห็นถ้ามีอาการผิดปกติ ขณะเดียวกันเซ็นเซอร์ตัวอื่นๆ ก็ทำหน้าที่ตรวจวัดจุดอื่นในร่างกายไปพร้อมๆ กัน เช่น อุณหภูมิร่างกาย ความดันโลหิตและระดับน้ำตาลในเลือด เป็นต้น ข้อมูลต่างๆ ที่ได้จากการตรวจวัดจะถูกจัดการส่งต่อโดยเซ็นเซียมซิลิคอนชิป (Sensium Silicon Chip) ซึ่งรับพลังงานจากแบตเตอรี่ขนาดเล็ก (เท่ากับที่ใช้ในนาฬิกาข้อมือ) และข้อมูลต่างๆ ที่วัดได้จากดิจิทัลพลาสเตอร์นี้สามารถแสดงผลโดยส่งผ่านทางโทรศัพท์มือถือหรือเครื่องคอมพิวเตอร์มือถือ (PDA) ไปยังเครื่องคอมพิวเตอร์ที่ใช้เป็นฐานข้อมูลเพื่อทำการตรวจวัดเปรียบเทียบตามเกณฑ์ของค่าปกติที่ได้ตั้งไว้ รวมทั้งวิเคราะห์ผลว่าร่างกายอยู่ในภาวะถึงขีดอันตรายหรือไม่ การวิเคราะห์สุขภาพในเบื้องต้นจากผลที่อ่านได้ ช่วยให้แพทย์สามารถรับรู้อาการผิดปกติที่เกิดกับคนไข้ได้อย่างทันท่วงที

นาย Keith Errey ผู้บริหารของบริษัททูมาซ์ กล่าวว่า ดิจิทัลพลาสเตอร์นี้ยังสามารถที่จะติดตั้งเซ็นเซอร์วัดความเคลื่อนไหว เพิ่มเติมลงไปให้ทำหน้าที่เหมือนกับ "พี่เลี้ยงคนชรา" เพื่อคอยส่งสัญญาณบอกเมื่อคนชราหกล้มหรือเป็นลมหมดสติไป โดยขณะนี้ทางบริษัทได้พยายามที่จะพัฒนาและผลิตดิจิทัลพลาสเตอร์ให้มีขนาดเล็กและใช้พลังงานน้อยที่สุดเท่าที่จะทำได้

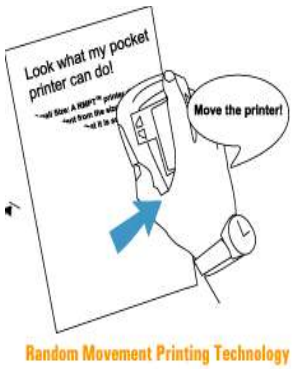
เครื่องพิมพ์ขนาดเล็กที่สุดในโลก (21203)

ภาพ PrintBrush(tm) ซึ่งเป็นเครื่องพิมพ์ที่มีขนาดเล็กที่สุดในโลก
ภาพจาก: www.pdacortex.com

ปัจจุบันได้มีการคิดค้นเทคโนโลยีและนวัตกรรมใหม่ๆ เพื่อนำมาใช้ในการผลิตเครื่องพิมพ์ (printer) ให้มีขนาดที่เล็กลงเพื่อให้สามารถพกพาไปในที่ต่างๆ ได้โดยสะดวกและใช้งานง่าย และเมื่อเร็วๆ นี้ได้มีการเปิดตัวของ PrintBrush (tm) ซึ่งเป็นเครื่องพิมพ์ที่มีขนาดเล็กที่สุดในโลก

ในปี 2003 บริษัท PrintDreams ได้พัฒนาสินค้าภายใต้ชื่อ RMPT: Random Movement Printing Technology และได้ประกาศเปิดตัว PrintBrush(tm) ซึ่งเป็นเครื่องพิมพ์ที่มีขนาดเล็กที่สุดในโลก เครื่องพิมพ์ขนาดพกพานี้มีความยาวประมาณปากกาลูกลื่นธรรมดาทั่วไป ในขณะที่มีความกว้างและสูงเท่ากับโทรศัพท์เคลื่อนที่รุ่นใหม่ๆ ในปัจจุบันและมีน้ำหนักประมาณ 350 กรัม เท่านั้น นอกจากนี้ บริษัทฯ ยังได้พัฒนาเทคโนโลยีเซ็น เซอร์ OptoNav ซึ่งมีความเที่ยงตรงสูง เพื่อทำให้ผลลัพธ์ที่ได้จากการพิมพ์มีคุณภาพคมชัดมากยิ่งขึ้น

หลักการทำงานของ PrintBrush(tm) คือ ผู้ใช้สามารถทำการดาวน์โหลดข้อมูลหรือรูปภาพที่ได้จากที่ต่างๆ เช่น อินเทอร์เน็ต หรือ SMS มาไว้ยังเครื่อง PrintBrush(tm) โดยผ่านทาง PDA โทรศัพท์เคลื่อนที่หรือคอมพิวเตอร์โน้ตบุ๊ค ซึ่งผ่านการเชื่อมต่อแบบไร้สายโดยใช้บูทูธ (Bluetooth) หลังจากนั้นนำเครื่องพิมพ์มาวางที่กระดาษพร้อมกับใช้มือลากเครื่องพิมพ์ไปบนกระดาษที่ต้องการจะพิมพ์ ทั้งนี้กระดาษที่ใช้จะเป็นชนิดใดก็ได้ และไม่จำกัดว่าจะมีรูปร่างอย่างไร ขนาดใหญ่หรือเล็ก หลังจากนั้นข้อความที่ต้องการจะปรากฏขึ้นมาทันทีหลังจากที่ลากเครื่องพิมพ์ผ่านไปบนกระดาษ โดยเครื่องพิมพ์นี้จะมีระบบกลไกที่สามารถตรวจสอบการเคลื่อนไหวของมือ การหมุนและการเปลี่ยนความเร็วโดยฉับพลัน ทำให้ผลลัพธ์การพิมพ์ที่ได้จากการดาวน์โหลดข้อมูลหรือรูปภาพจะมีลักษณะเหมือนกับต้นฉบับแทบทุกประการ ทั้งนี้ บริษัทฯ คาดว่าจะสามารถทำการผลิตและออกวางจำหน่ายในตลาดได้ในเร็วๆ นี้ (ปี 2005) ภายใต้ชื่อ RMPT(tm)



ภาพจาก: pdacortex.com

ที่มา: 21201: http://newsvote.bbc.co.uk/go/pr/fr/-/2/hi/americas/4107236.stm
2005, 6 June. "Hacker Hunters; a global force takes on the dark side of Computing." BusinessWeek (Asian Edition). Page 46-54.
21202: http://news.bbc.co.uk/2/hi/health/4617633.stm
http://www.tehrantimes.com/Description.asp?Da=6/19/2005&Cat=7&Num=7
21203: http://www.pdacortex.com/printdreams.htm
http://www.printdreams.com

IT Digest เป็นวารสารอิเล็กทรอนิกส์ ที่จัดทำขึ้นเผยแพร่โดยไม่คิดค่าใช้จ่าย หากท่านสนใจเป็นสมาชิก หรืออ่านบทความย้อนหลัง โปรดติดต่อเราได้ที่เว็บไซต์ http://www.nectec.or.th/pub/itdigest/ หรือทางไปรษณีย์อิเล็กทรอนิกส์ it-digest@nectec.or.th

ที่ปรึกษา: ทวีศักดิ์ กออนันตกูล และ ชฎามาศ ธุวะเศรษฐกุล บรรณาธิการบริหาร: กัลยา อุดมวิทิต
กองบรรณาธิการ: จิราภรณ์ แจ่มชัดใจ, ถวิดา มิตรพันธ์, พรรณี พนิตประชา, อภิญญา กมลสุข, อลิสา คงทน , พิสิฐจรรย์ แพทย์เจริญ และ จินตนา พัฒนาธรชัย