เตือนภัย "Icepack" โปรแกรมติดตั้ง มัลแวร์ผ่านช่องโหว่บนพีซี [1 ส.ค. 50 - 06:06]

ผู้สื่อข่าวรายงานว่า ศูนย์วิจัยแพนด้า แล็ป บริษัท แพนด้า ซอฟต์แวร์ ได้ประกาศถึงการตรวจพบเครื่องมือติดตั้งมัลแวร์ผ่านช่องโหว่ตัวใหม่ เรียกว่า "Icepack" โปรแกรมนี้มีจำหน่ายบนอินเทอร์เน็ตในราคา 400 เหรียญสหรัฐ โดยการตรวจพบเครื่องมือนี้และเครื่องมืออื่นๆ ก่อนหน้านี้เช่น Mpack , XRummer, Zunker, Barracuda, Pinch ฯลฯ ถือเป็นการยืนยันถึงพัฒนาการของธุรกิจบนอินเทอร์เน็ต ที่ทำกำไรด้วยการสร้างและจำหน่ายแอพพลิเคชันสำหรับการนำไปใช้ในทางที่มิชอบ

รายงานข่าวแจ้งว่า Icepack จะเข้าสู่หน้าเว็บที่ได้วาง iframe ที่ชี้ไปยังเซิร์ฟเวอร์ที่ได้ติดตั้งแอพลิเคชันไว้ นวัตกรรมที่สำคัญใน Icepack คือ เครื่องมือเพิ่ม iframe ขณะที่แอพลิเคชันรุ่นเก่าๆ เช่น Mpack จำเป็นต้องมีแฮกเกอร์เข้าสู่หน้าเว็บเพื่อวาง iframe ด้วยตัวเอง และเมื่อผู้ใช้เข้าสู่หน้าเว็บดังกล่าว iframe จะเรียกใช้ Icepack โดยจะมองหาช่องโหว่ในคอมพิวเตอร์ของผู้ใช้ เมื่อพบจะดาวน์โหลดเครื่องมือเจาะช่องโหว่เข้าสู่คอมพิวเตอร์

รายงานข่าวแจ้งต่อว่า ฟีเจอร์สำคัญของ Icepack คือ ความสามารถในการเจาะช่องโหว่ใหม่ๆ ที่เพิ่งปรากฏ เนื่องจากผู้ใช้ยังไม่ทันได้อัพเดทคอมพิวเตอร์ของตัวเองเพื่อแก้ปัญหาดังกล่าว จากนั้น เหล่าอาชญากรจะสามารถดาวน์โหลดมัลแวร์เข้าสู่ระบบได้ทุกประเภท จากราคาของเครื่องมือนี้ เป็นไปได้ว่ามัลแวร์ที่มีการดาวน์โหลดมากที่สุด จะเป็นมัลแวร์ที่นิยมใช้ในการขโมยข้อมูลลับ เพื่อนำไปใช้ในการฉ้อโกงผ่านระบบออนไลน์ เช่น โทรจัน สปายแวร์ และโปรแกรมบ็อต เป็นต้น

นาย หลุยส์ โครอน ผู้อำนวยการด้านเทคนิค ศูนย์วิจัยแพนด้า แล็ป กล่าวว่า เครื่องมือนี้คล้ายกับเครื่องมือติดตั้งมัลแวร์ เช่น Mpack แต่ได้มีการปรับปรุงให้ขึ้น โดยก็เป็นเรื่องมีเหตุผลเพราะมีเงินจำนวนมากเข้ามาเกี่ยวข้อง บรรดาอาชญากรจึงพยายามผูกขาดตลาด ด้วยการนำเสนอผลิตภัณฑ์ที่มีความสามารถสูงขึ้น นวัตกรรมอีกประการของ Icepack คือ การรวมเอาเครื่องมือตรวจสอบ ftps เข้าไว้ด้วยกันกับ iframer โดยเครื่องมือตรวจสอบ ftp ใช้สำหรับดูข้อมูลบัญชีผู้ใช้ FTP ที่ได้จากเครื่องคอมพิวเตอร์ ข้อมูลจากบัญชีผู้ใช้ดังกล่าวจะถูกส่งไปตรวจสอบความถูกต้อง จากนั้นข้อมูลความถูกต้องจะถูกส่งผ่านไปยัง iframe ที่จะแทรกการชี้ตำแหน่ง iframe ไปยัง Icepack เข้าสู่บัญชีนั้น โดยวิธีการนี้ทุกอย่างจะกลับเข้าสู่ " วงรอบ" อีกครั้ง

ผู้สื่อข่าวรายงานต่อว่า ต้าน บริษัท ฟอร์ติเน็ต ผู้บุกเบิกและผู้ให้บริการระบบรักษาความปลอดภัยแบบ multi-threat security ก็ออกประกาศเตือนที่ระบุว่า ประเทศไทยได้รับผลกระทบอย่างรวดเร็วจาก Tibs หรือ aka Storm ที่เป็นพายุไวรัสที่สร้างความเสียหายไปทั่ว ด้วยความรุนแรงระดับสูง โดยการแฝงตัวไปพร้อมกับบัตรอวยพรทางอินเทอร์เน็ต หรือ greeting card ขณะนี้ ประเทศไทยจัดว่าเป็นหนึ่งในประเทศที่ได้รับการโจมตีโดยเฉพาะเจาะจงมาโดยตรง

รายงานข่าวแจ้งอีกว่า ช่วงกลางเดือน ก.ค.2550 ความรุนแรงของ Tibsในประเทศไทย เพิ่มขึ้นอยางรวดเร็วและสูงกว่าประเทศอื่นๆ ที่ตกอยู่ในสถานการณ์เดียวกัน โดยจำนวนที่เข้าจู่โจมสูงถึง 31.5 ล้านครั้ง จากจำนวนไวรัสที่ส่งออกมาทั้งหมด เปรียบเทียบกับปริมาณในประเทศสหรัฐอเมริกาที่สูงถึง 300 ล้านตัว นับว่าเป็นการไหลบ่าของภัยคุกคามที่น่ากลัวมาก เข้าครอบคลุมประเทศที่มีผู้ใช้บริการอินเทอร์เน็ต สัดส่วนอยู่ที่ 1 ใน 10 ของจำนวนทั้งหมด และภายในประเทศมีสัดส่วนการตรวจจับ Tibs อยู่ที่ 10 ต่อ 1 ของไวรัสโดยทั่วไป ทั้งนี้ Tibs ก่อให้ความตึงเครียดอันเกิดจากอีเมล์จำนวนที่มากนับเป็นล้านๆ ฉบับ

ทั้งนี้ ข้อมูลของ "พายุไวรัส" ดูได้ที่รายงานสรุปไวรัสของฟอร์ติเน็ตประจำเดือน ม.ค.2550 (**http://www.fortinet.co.th/news/pr/thai/2007/pr090207.html**) ที่ทางฟอร์ติเน็ตได้ค้นพบ และแจ้งให้ทราบถึงผลกระทบมาต่อเนื่องของ Tibs โดยเหมือนกับว่าความสามารถต่ำกว่าอุปกรณ์ตรวจจับ แต่แท้จริงแล้วไม่เป็นเช่นนั้นเลย นี่อาจเป็นเหตุผลหนึ่งที่มีความเป็นไปได้สูงว่า ทำไมอุปกรณ์ตรวจจับจำนวนมากในประเทศไทย ถึงได้รับไวรัสและติดเชื้อกันไปทั้งระบบ รวมทั้งส่งผลให้ Tibs ลามไปจนทั่วด้วยคลื่นของสแปมเมล์นั่นเอง