Matichon Online
วันที่ 2 พฤษภาคม พ.ศ. 2552
http://www.matichon.co.th/

ระวังไวรัสหน้าใหม่ร้ายและเร็ว

แคสเปอร์สกี้ แล็บ ผู้นำด้านแอนตี้ไวรัสระดับโลก ประกาศแจ้งเตือนไวรัสตัวใหม่ เวอร์ชั่นใหม่ของ Kido (หรือที่รู้จักในชื่อ Conficker และ Downandup) ที่ออกมาอาละวาดในช่วงคืนวันที่ 8 และ 9 เมษายน คอมพิวเตอร์ที่ติดไวรัส Trojan-Downloader.Win32.Kido หรือ Conficker.c นี้จะทำการเชื่อมต่อกันผ่านแบบเครื่องต่อเครื่อง (P2P) เพื่อกระจายตัวด้วยการทำดาวน์โหลดตัวเองได้อัตโนมัติและปลุกปีศาจ Kido ให้ระบาดผ่านเครือข่ายบอตเน็ต

Kido ในเวอร์ชั่นใหม่ต่างจากเวอร์ชั่นเก่าและร้ายกาจกว่าเดิม เนื่องจากมัลแวร์ตัวนี้ได้แปลงมาเป็นเวิร์มและมีพฤติกรรมเช่นนั้นในการแพร่ระบาด การวิเคราะห์ในเบื้องต้นชี้ว่ามัลแวร์นี้มีข้อจำกัดด้านเวลา โดยคาดว่าจะอาละวาดก่อความเสียหายจนถึงวันที่ 3 พฤษภาคม 2552 นอกจากมัลแวร์ Kido จะแพร่กระจายด้วยการดาวน์โหลดตัวเองได้แล้ว ยังดาวน์โหลดไฟล์มัลแวร์พ่วงมาอีกถึง 2 ไฟล์ไปยังเครื่องที่ติดไวรัส ได้แก่ ระบบแอนตี้ไวรัสปลอม (ตรวจจับได้ในชื่อ FraudTool. Win32.SpywareProtect2009.s) โดยมีไซต์ต้นตออยู่ที่ยูเครน เมื่อโปรแกรมเริ่มรันจะทำทีเป็นแจ้งเตือนให้กดปุ่มเพื่อซื้อโปรแกรมกำจัดไวรัสในราคา 1,750 บาท และไฟล์ที่สอง คือ Worm. Win32.Iksmas.atz. หรือที่รู้จักกันในนาม Waledac วายร้ายตัวนี้จะขโมยข้อมูลและส่งสแปมกลับมาหาคุณ ถูกตรวจจับได้ครั้งแรกในเดือนมกราคม 2552 ผู้เชี่ยวชาญด้านไอทีมากมายสังเกตเห็นความเหมือนระหว่าง Kido และ Iksmas และรูปแบบการแพร่ระบาดของ Kido เปรียบเสมือนกระจกเงาของการแพร่ระบาดของ Iksmas

นายอเล็กซ์ โกซเตฟ หัวหน้าฝ่ายวิจัย แคสเปอร์สกี้ แล็บ กล่าวว่า "ช่วงเวลากว่า 12 ชั่วโมงที่ Iksmas เข้ายึดการเชื่อมโยงกับศูนย์บริหารข้อมูลส่วนกลางได้ทั่วโลก พบว่ามีคำสั่งให้ส่งอี-เมลสแปมออกเป็นจำนวนถึง 42,298 ข้อความ และในทุกอี-เมลพบโดเมนเนมที่มีลักษณะ ฉพาะที่จงใจทำขึ้นเพื่อหลีกเลี่ยงให้พ้นจากการถูกตรวจจับการส่งอี-เมลปริมาณมหาศาลขนาดนั้นด้วยคุณสมบัติการทำงานของตัวฟิลเตอร์ของโปรแกรมแอนตี้สแปมที่ใช้วิธีวิเคราะห์ความถี่ของโดเมนเนม โดยรวมแล้ว เราตรวจจับการใช้โดเมนระดับ 3 ได้ถึง 40,542 และ 33 สำหรับโดเมนระดับที่สอง ในความเป็นจริงแล้วไซต์ต่างๆ เหล่านี้อยู่ที่ประเทศจีนและลงทะเบียนไว้ในชื่อหลากหลายคน จากรายงานพบว่า Iksmas ส่งอี-เมลกว่า 80,000 ครั้งภายใน 1 วัน ซึ่งคาดเดาได้ว่ามีกว่า 5 ล้านเครื่องที่ติดไวรัส และยังมีความสามารถในการส่งสแปมมากกว่า 4000 ล้าน ข้อความภายใน 24 ชั่วโมง"

แคสเปอร์สกี้ แล็บ ให้ความสำคัญเป็นอย่างมากกับเรื่องนี้พร้อมทั้งยังดำเนินการวิเคราะห์การแปลงรูปไปในลักษณะต่างๆ ของไวรัสดังกล่าว ผู้ใช้แคสเปอร์สกี้ แล็บ คลายความกังวลไปได้เลยเนื่องจากเวอร์ชั่นใหม่ของไวรัสตัวนี้ (Net-Worm.Win32. Kido.js) ได้ถูกตรวจจับได้แล้วตั้งแต่เริ่มต้น (ในชื่อ HEUR: Worm.Win32.Generic) ซึ่งมีการแปลงรูปของ Iksmas ที่ดาวน์โหลดมา

มติชนรายวัน วันที่ 02 พฤษภาคม พ.ศ. 2552 ปีที่ 32 ฉบับที่ 11375 หน้า 18

ที่มา : http://www.matichon.co.th/matichon/view_news.php?newsid=01tec070205552&sectionid=0143&day=2009-05-02

เปิดตัว "TSP E-Newsletter" บริการข่าวออนไลน์ฟรี ข้อมูลวงการวิจัยไทย

อุทยานวิทยาศาสตร์ประเทศไทย (ซายน์พาร์ค) ศูนย์บริหารจัดการเทคโนโลยี (TMC) เป็นนิคมเพื่อการวิจัยและพัฒนาที่สำคัญในวงการวิจัยไทย เปิดตัว TSP E-Newsletter หรือบริการข่าวออนไลน์ฉบับปฐมฤกษ์เพื่อนำเสนอนวัตกรรม ความก้าวหน้า ข้อมูลข่าวสาร และความเคลื่อนไหวในวงการวิจัยและพัฒนาของไทย มุ่งเน้นเพื่อเป็นแหล่งให้ข้อมูลที่ควรรู้แก่องค์กรที่มีความตื่นตัวต่อการดำเนินธุรกิจบนฐานของวิทยาศาสตร์และเทคโนโลยี

โดย TSP E-Newsletter ฉบับแรกนี้จะนำเสนอเรื่องราวที่เป็นประโยชน์เกี่ยวกับการวิเคราะห์ทดสอบเพื่อความปลอดภัยทางด้านอาหาร อาทิ สถานะของการวิเคราะห์ทดสอบทางด้านอาหารของประเทศ รวมทั้งแนวโน้มการปรับตัวในอนาคต จากผู้บริหารระดับแนวหน้าของบริษัท ศูนย์วิทยาศาสตร์

เบทาโกร จำกัด และ บริษัท ทูฟชูด พีเอสบี ประเทศไทย จำกัด ซึ่งเป็นผู้เช่ารายแรกของซายน์พาร์คยังได้แนะนำบริการวิเคราะห์ทดสอบของบริษัท พร้อมแสดงวิสัยทัศน์ในการพัฒนาศักยภาพบริการให้มีประสิทธิภาพและสามารถตอบสนองความต้องการที่เพิ่มขึ้นของผู้ผลิตไทย

TSP E-Newsletter ฉบับเปิดตัวครั้งนี้ยังอัดแน่นด้วยข้อมูลที่มีประโยชน์เกี่ยวกับปัญหาที่เกิดจาก Foodborne Pathogen ซึ่งพบมากในผลิตภัณฑ์อาหารแถบภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยนักวิจัยจากศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติ (BIOTEC)

พร้อมกันนี้ยังได้เพิ่มเติมเนื้อหาสาระและข้อมูลที่เป็นประโยชน์แก่ผู้ประกอบการธุรกิจเทคโนโลยี หรือผู้ที่ต้องการทราบข่าวสาร ข้อมูล กิจกรรม การฝึกอบรม รวมทั้งบริการด้านการวิจัยและพัฒนาต่างๆ ที่ซายน์ปาร์คมีให้แก่ภาคเอกชน

โดยผู้ที่สนใจทั่วไปสามารถเข้าไปดูข้อมูลและสมัครสมาชิก TSP E-Newsletter ได้ฟรี ผ่านเว็บไซต์ www.sciencepark.or.th

มติชนรายวัน วันที่ 02 พฤษภาคม พ.ศ. 2552 ปีที่ 32 ฉบับที่ 11375 หน้า 20

ที่มา : http://www.matichon.co.th/matichon/view_news.php?newsid=01tec08020552&sectionid=0143&day=2009-05-02