ระวัง "โทรจัน" จากอีเมลโอลิมปิก

นำเสนอเมื่อ : 24 ก.ค. 2551

เทรนด์ ไมโคร เตือนผู้ใช้ระวังภัยร้ายโทรจัน ก่อนเปิดไฟล์ข้อมูลกีฬาโอลิมปิก 2008

ศูนย์วิจัยเทรนด์แล็บส์ ของบริษัท เทรนด์ ไมโคร อิงค์ เปิดเผยว่า ผู้สร้างมัลแวรกำลังหาทางโจมตีมหกรรมกีฬาโอลิมปิกภาคฤดูร้อน ที่กำลังจะมีขึ้นในวันที่ 8-24 ส.ค. นี้ โดยมีรายงานพบ **ช่องโหว่ซีโร่เดย์ของโปรแกรม MS Word** (ซีโร่เดย์ คือช่วงเวลาที่มีการพบช่องโหว่ในซอฟต์แวร์แต่ยังไม่มีโปรแกรมซ่อมแซมออกมาอุดช่องโหว่ดังกล่าว) ที่กระทบต่อ Microsoft Word 2000, 2002 และ 2003 รวมทั้งเวอร์ชันแพทช์ (ซ่อมแซม) ของโปรแกรมประมวลผลคำยอดนิยมโปรแกรมนี้ใน MS Office บางเวอร์ชันด้วย เมื่อมีการใช้ประโยชน์จากช่องโหว่จะทำให้แฮคเกอร์สามารถเข้าควบคุมระบบที่มีช่องโหว่นี้ได้ทั้งหมดหรือทำให้แอพพลิเคชันล่มได

ผู้เชี่ยวชาญของเทรนด์แล็บส์ยืนยันว่า สิ่งนี้เป็นอันตราย เนื่องจากไฟล์ .DOC มีการใช้งานอย่างแพร่หลาย โดยให้สังเกตว่า: จะมีการใช้มหกรรมกีฬาโอลิมปิกที่กำลังจะจัดขึ้นเป็นตัวชักชวนให้ผู้ใช้คลิกไฟล์ร้ายดังกล่าว ตัวอย่างของโทรจัน TROJ_MDROPPER.ZT ที่เทรนด์แล็บส์ได้ตรวจพบนั้น มีอยู่ในไฟล์ที่มีชื่อดังต่อไปนี้:

attachment .doc

appeal_letter_of_fttj.doc

attend_the_opening_ceremony_of_

the_29th_olympic_games_in_beijing.doc

five_resolutions.doc

lingotto_con_fiat.doc

รูปตัวอย่างของไฟล์โทรจัน :

ไฟล์เหล่านี้เป็นช่องโหว่ซีโร่เดย์ในกลุ่ม CVE-2008-2244 (ฐานข้อมูลช่องโหว่ที่มีการตรวจพบ)

นอกจากไฟล์ Word ที่มีโทรจันแล้ว เทรนด์แล็บส์ยังพบตัวอย่างของโทรจันในไฟล์ .XLS และ .PPT ด้วยโดยทั้งหมดใช้เรื่องมหกรรมโอลิมปิกและความขัดแย้งในธิเบตมาเป็นตัวหลอกล่อผู้ใช้ นั่นคือความขัดแย้งที่เกี่ยวกับมหกรรมโอลิมปิกจากการที่กลุ่มชนชาวธิเบตเรียกร้องให้คว่ำบาตรกีฬาโอลิมปิกที่จีนเ

ปีนเจ้าภาพ

รูปตัวอย่างไฟล์เพาเวอร์พ้อยท์ที่มีโทรจัน

นอกจากนี้ ยังมีไฟล์ Excel ที่เป็นโทรจันอันตราย เช่น TROJ_MDROPPER.ZY และไฟล์ PowerPoint เช่น TROJ_PPDROP.M แม้ว่าไฟล์เหล่านี้จะยังไม่ได้รับการยืนยันว่ามีช่องโหว่ซีโร่เดย์ แต่ควรติดตามและทำการอัพเดทโปรแกรมป้องกันไว้เสมอ

ทั้งนี้ ในมหกรรมการแข่งขันกีฬาโอลิมปิกคาดว่าจะมีนักกีฬา 10,500 คนเข้าร่วมแข่งขันในกีฬา 28 ประเภท และจากความสนใจในมหกรรมโอลิมปิกจากผู้ชมทั่วโลก คาดว่าจะมีกองทัพมัลแวร์ในรูปของเทคนิควิศวกรรมทางสังคมจากผู้ประสงค์ร้ายออกมาก่อกวนเป็นจำนวนมาก

ที่มา **เดลินิวส์**

http://www.dailynews.co.th/web/html/popup_news/Default.aspx?Newsid=171263&NewsType=1&Template=1