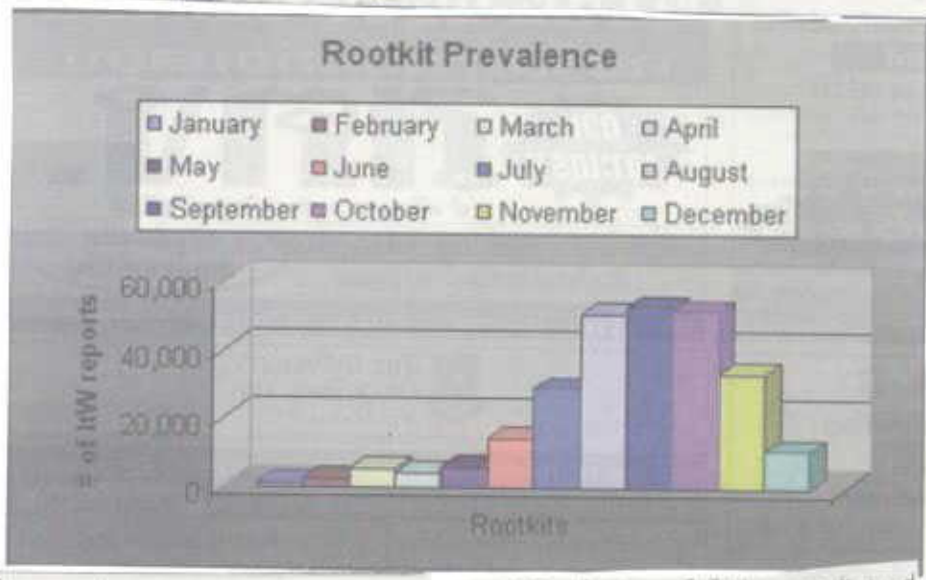
มติชน
ปีที่ 29 ฉบับที่ 10219 วันศุกร์ที่ 3 มีนาคม พุทธศักราช 2549

ก 6713

# รับมือ ภัยจู่โจมโลกไซเบอร์




ในรอบปีที่ผ่านมาอุตสาหกรรมด้านความปลอดภัยและป้องกันไวรัสมีความเปลี่ยนแปลงไม่มากนัก แต่มีแนวโน้มว่าภัยคุกคามรูปแบบใหม่กำลังเริ่มปรากฏขึ้น ไม่ว่าจะใช้เป็นช่องทางก่อโฆษณาสินค้า จนถึงการก่ออาชญากรรมขโมยหมายเลขบัญชีธนาคารของผู้บริโภค

ก่อนหน้านี้ บริษัท เทรนด์ ไมโคร ได้คาดการณ์ว่า ภัยคุกคามปี 2548 จะมาในรูปผสมผสานของมัลแวร์หลากชนิด ตั้งแต่การแพร่ระบาดของ WORM_BAGLE.BE สแปมโทรจัน การเพิ่มจำนวนของมัลแวร์ในตระกูล AGOBOT และแตกสายพันธุ์มากมาย การโจมตีผู้ใช้ในรูปของไฟล์ WMF (Windows Meta File)

ด้านภัยคุกคามที่เกี่ยวกับโปรแกรม IRC และ P2P มีจำนวนมากขึ้น 16% ส่วนสแปมและฟิชชิ่งก็ยังคงเป็นปัญหาใหญ่ที่ผู้ใช้ทั้งองค์กรและผู้ใช้ตามบ้านต้องเผชิญในรอบปีที่ผ่านมา ที่สำคัญ สแปมไม่ได้มาในรูปของภาษาอังกฤษอีกต่อไป มีหลากหลายภาษาทยอยออกมาโจมตีผู้ใช้ตามภูมิภาคมากขึ้นเรื่อยๆ หรือจะเป็นการขโมยรหัสผ่าน และหนอนบ็อตที่อาละวาด ส่วนสปายแวร์และแอดแวร์ก็ยังคงซุกซ่อนตัวเองอยู่หลังหน้าเว็บต้องสงสัยทั่วไปบนโลกอินเตอร์เน็ต

เพื่อการรับมือและป้องกันภัยคุกคามคอมพิวเตอร์และเครือข่ายนี้ เริ่มตั้งแต่ ภัยคุกคาม จากสปายแวร์, แอดแวร์, แบ็คดอร์, รูทคิตส์, และบ็อต ซึ่งเทรนด์ ไมโคร เตือนภัยมัลแวร์ พร้อมกับภัยคุกคาม 15 อันดับจากปี 2548 วัดจำนวนคอมพิวเตอร์ติดเชื้อไว้ว่า...

ภัยมัลแวร์แพร่ระบาดไปไม่น้อย ครองสัดส่วนที่ 16% ถูกออกแบบเนื้อหาให้คล้ายกับสแปม

ช่วง 3 ปีที่ผ่านมา นักวิจัยของเทรนด์ ไมโคร เตือนผู้ใช้ออนไลน์ว่าไวรัสร้ายที่ใช้ช่องทางผ่านทางโปรแกรมสนทนาออนไลน์ (ไอเอ็ม) กำลังเพิ่มจำนวนขึ้น พบหนอน KELVIR, FATSO และ BROPIA ออกมาอาละวาดระบาดผ่านทางโปรแกรม MSN แม้ผู้ใช้ ผู้ค้า ผู้ติดตั้งระบบและองค์กรตรวจสอบอี-เมลหาทางป้องกัน แต่สุดท้ายมัลแวร์ก็เอาคืนด้วยการเขียนมัลแวร์ด้วยเทคนิคที่ซับซ้อนยิ่งขึ้น เช่น ใช้ลิงค์ยูอาร์แอลลวงตา หรือหลอกให้ผู้ใช้ดาวน์โหลดโปรแกรมที่แฝงโทรจันไปติดตั้งไว้ในเครื่องอย่างง่ายดาย เทคนิคที่ใช้ไม่ได้ยึดติดว่าต้องมาพร้อมกับอี-เมล เท่านั้น แต่สามารถผ่านการดาวน์โหลดไฟล์ทั่วไปบนโลกอินเตอร์เน็ต โดยผู้ใช้ไม่รู้ตัวว่าไฟล์ร้ายถูกฝังลงในเครื่องด้วยเทคนิคดังกล่าว และคาดว่าเทคนิคนี้จะได้รับความนิยมเพิ่มมากขึ้นไปอีก

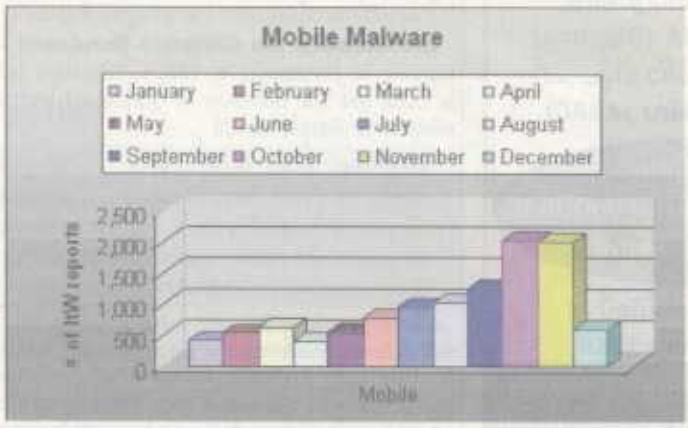
ส่วน ฟิชชิ่ง วิธีการลวงด้วยแอดเดรสบาร์ ครองอันดับหนึ่ง 81% มักเลือกจู่โจมผู้ใช้เบราเซอร์อินเตอร์เน็ตเอ็กซ์พลอเรอร์ (ไออี) ที่มีมากเกือบ 90%

[ต่อด้านหลัง]

ของผู้ใช้ที่ติดตั้งระบบปฏิบัติการวินโดวส์

ขณะที่ รูทคิตส์ (rootkits) ชุดโปรแกรมที่บรรดาแฮกเกอร์จะแอบทิ้งไว้ในเครื่องหลังจากรู้โจมได้สำเร็จแล้ว เพื่อใช้เป็นเครื่องมือในการหาประโยชน์ใส่ตัวในภายหลัง โปรแกรมประเภทรูทคิตส์จะพยายามหลบซ่อนตัวเองให้หลุดรอดจากการตรวจจับของเจ้าของระบบ ทำให้สามารถฝังรากแน่นอยู่ในระบบชนิดยากจะพบ แม้ว่าในรอบปีที่ผ่านมารูทคิตส์อาจมีไม่มากนัก แต่เทรนด์ ไมโคร คาดว่าแนวโน้มของภัยคุกคามรูปแบบนี้จะยังคงเกิดขึ้นต่อเนื่องไปจนถึงปี2549

ไม่เฉพาะโลกบนเน็ต แม้แต่โทรศัพท์มือถือหนอนมือถือตัวแรกถูกค้นพบในเดือนสิงหาคม 2547 ชื่อว่า SYMBOS_CABIR แพร่ระบาดตัวเองไปยังมือถือเครื่องอื่นๆ บนระบบปฏิบัติการซิมเบียน 60 ผ่านทางเทคโนโลยีบลูทูธ และพบว่าหนอนมือถือกำลังทวีจำนวนเพิ่มมากขึ้น มีความสามารถรู้โจมมากขึ้นนำไปสู่เทคโนโลยีมือถือใหม่ๆ




โดยเฉพาะช่องสัญญาณส่งผ่านข้อมูลที่เพิ่มขึ้นในการเชื่อมต่ออินเตอร์เน็ต เช่น ไว-ไฟ, เอจ/จีพีอาร์เอส, 3จี/ยูเอ็มทีเอส และแม้แต่ไวแมคซ์ที่กำลังจะเกิดขึ้น ก็เป็นเป้าหมายที่ต้องคอยระมัดระวังเช่นกัน

### แนวโน้มภัยคุกคามปี? 2549

เทรนด์ ไมโครคาดว่าสิ่งที่พบเจอในรอบปีที่ผ่านมาจะยังคงเกิดขึ้นต่อเนื่องในปี2549:

-สปาย-ฟิชชิ่ง ยังคงเพิ่มขึ้นอย่างต่อเนื่อง

-บ็อต จะใช้รูทคิตส์ในการเพิ่มความสามารถให้กับตัวเอง

-สเปียร์-ฟิชชิ่ง (Spear-phishing) จะสร้างความกังวลใจให้กับองค์กรธุรกิจต่างๆไม่น้อย

-สแปมจะมาในรูปภาษาท้องถิ่นมากขึ้น

-มัลแวร์จะมาในรูปของการเข้ารหัสและแบ่งย่อยตัวเองมากขึ้นเพื่อหลบเลี่ยงการตรวจจับ

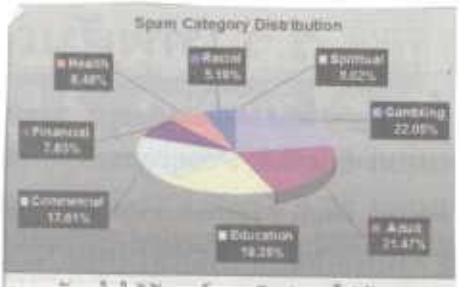
-โปรแกรมสนทนาออนไลน์ อย่าง IRC, IM, และ P2P จะยังคงเป็นช่องทางแพร่ไวรัสอยู่

-ช่องโหว่ของระบบปฏิบัติการวินโดว์สยังคงเป็นเป้าหมายไม่หยุดหย่อน

-เกรย์แวร์และมัลแวร์เริ่มแยกกันไม่ออก แต่ก็ส่งผลดีต่อผู้ค้าผลิตภัณฑ์รักษาความปลอดภัยที่จะสามารถกำจัดภัยร้ายนี้ได้ง่ายขึ้น

-บ็อตและบ็อตเน็ตส์เพิ่มจำนวนขึ้น

-แอดแวร์และสปายแวร์ยังคงแพร่ระบาดอยู่




### ข้อแนะนำสำหรับผู้ใช้รับมือมัลแวร์ปี 2549

สำหรับผู้ใช้องค์กร:

-หมั่นใช้ระบบสแกนหาไวรัสทางอินเตอร์เน็ตให้เหมือนกับระบบสแกนอี-เมลที่ใช้กันมานานแล้ว

-ปิดกั้นการเข้าถึงเครือข่ายองค์กรของโปรโตคอลที่ไม่จำเป็น โดยเฉพาะโปรแกรมสนทนาออนไลน์ทั้งหลาย

-ใช้ซอฟต์แวร์สแกนช่องโหว่ในเครือข่าย

-อย่าให้สิทธิพิเศษแก่ผู้ใช้งานในองค์กร จำกัดสิทธิการใช้งานเป็นนโยบายออกมาเลย

-ใช้ระบบสแกนสปายแวร์องค์กร

-ให้ความรู้กับผู้ใช้ และกำหนดนโยบายการใช้งานเครือข่ายองค์กรอย่างเข้มงวด

**สำหรับผู้ใช้ตามบ้าน:**

-ระวังเว็บไซต์ ที่มีข้อแม้ให้คุณต้องติดตั้งซอฟต์แวร์ลงในคอมพิวเตอร์ และอย่าติดตั้งซอฟต์แวร์ใหม่จากเว็บไซต์แปลกหน้า นอกจากคุณจะมั่นใจว่าเว็บไซต์หรือเจ้าของซอฟต์แวร์นั้นน่าเชื่อถือจริง

-สแกนโปรแกรมที่ดาวน์โหลดทางอินเตอร์เน็ตด้วยซอฟต์แวร์ป้องกันสปายแวร์และไวรัสที่ได้รับการอัพเดตแล้ว ไม่ว่าจะดาวน์โหลดจากเครือข่าย P2P ผ่านเว็บไซต์ หรือแหล่งอื่นใดก็ตาม

-ระวังอี-เมลหน้าตาแปลกๆ อย่าเปิดไฟล์แนบท้ายหรือคลิกลิงค์ที่มาพร้อมกับอี-เมลไม่น่าไว้ใจ

-ตั้งค่า "Automatic Update" ในระบบปฏิบัติการวินโดว์สของคุณไว้ และอัพเดตใหม่ทันทีที่มีการประกาศให้เข้าไปอัพเดต

**-ต้องใช้บริการสแกนไวรัสแบบเรียลไทม์ เพื่อช่วยให้การท่องโลกออนไลน์ปลอดภัยไร้กังวล**