ยอดผู้ใช้โดนมัลแวร์การเงินโจมตีเพิ่มสูงขึ้น 7% ในครึ่งปีแรก 2562 จำนวน 430,000 ราย

นักวิจัย Kaspersky เปิดเผยว่า มีผู้ใช้กว่า 430,000 ราย
เผชิญปัญหามัลแวร์ที่ต้องการขโมยด้านการเงิน เงินคริปโต
และเว็บไซต์ที่ให้บริการด้านการเงิน ในช่วงครึ่งปีแรกของปี 2562
ซึ่งเพิ่มขึ้นจากช่วงเวลาเดียวกันของปีที่แล้วคิดเป็น 7%
โดยผู้ที่ได้รับมัลแวร์นี้ 30.9% เป็นผู้ใช้ในองค์กร ซึ่งสูงกว่าปีที่แล้วถึง 2
เท่า เพราะปีที่แล้วมีอัตราผู้ติดเชื้ออยู่ที่ 15.3%
มัลแวร์ด้านการเงินนี้ นั่นก็คือโทรจันด้านการเงินการธนาคารนั่นเอง
ที่มีวัตถุประสงค์เพื่อขโมยข้อมูลทางการเงิน
และยังโจมตีผู้ใช้ด้วยการเข้าถึงข้อมูลที่จำเป็น
รวมทั้งทรัพย์สินและเครื่องจักรต่าง ๆ ขององค์กรทางการเงิน
ซึ่งภัยคุกคามดังกล่าวได้ครอบครองส่วนสำคัญของแนวการคุกคามอยู่เสม
อ
เนื่องจากการเงินเป็นแรงจูงใจที่สำคัญต่อพวกอาชญากรไซเบอร์และพวก
ฉ้อโกงต่าง ๆ จากข้อมูลเกี่ยวกับมัลแวร์ใหม่ ๆ ของ Kaspersky
แสดงให้เห็นว่ามัลแวร์เหล่านี้
มีวัตถุประสงค์เพื่อขโมยเงินที่เป็นอันตรายมาก

โดยเฉพาะอย่างยิ่งเมื่อคุกคามไปถึงสภาพแวดล้อมในองค์กร
เนื่องจากเครือข่ายต่าง ๆ
ในองค์กรจะอยู่บนพื้นฐานขององค์กรที่เชื่อมต่อต่าง ๆ
และหากมีอุปกรณ์ตัวใดตัวนึงที่ถูกคุกคามหรือติดมัลแวร์
จะทำให้ทั้งเครือข่ายโดนคุกคามไปด้วย

ข้อมูลแสดงที่ถูกโจมตีโดยมัลแวร์ด้านการเงินในช่วงครึ่งปีแรก 2561

ถึงช่วงครึ่งปีหลัง 2562
แหล่งที่มา Kaspersky

ลักษณะการโจมตีของมัลแวร์นี้จะเป็นการส่งอีเมลสแปมและเว็บไซต์ฟิชชิ่
ง ซึ่งมักจะทำเป็นเว็บไซต์ที่ถูกกฎหมาย
โดยมีเป้าหมายในการขโมยข้อมูลทางการเงิน
ธนาคารและข้อมูลบัตรเครดิต และข้อมูลที่สำคัญต่าง ๆ
โดยในช่วงครึ่งปีแรกของปี 2562 นักวิจัยของ Kaspersky
ได้ตรวจจับกว่า 339,000 ฟิชชิ่ง
ที่เป็นเว็บปลอมที่ปลอมตัวเป็นเว็บไซต์ของธนาคารขนาดใหญ่ต่าง ๆ
นักวิจัยได้รวบรวมรายชื่อของตระกูลโทรจันการเงินที่กำลังโจมตีผู้ใช้ต่าง
ๆ ในองค์กร โดย 40%
ของภัยคุกคามที่โจมตีผู้ใช้ในองค์กรมาจากโทรจันที่ชื่อว่า RTM
ซึ่งเป็นหนึ่งในโทรจันด้านการเงินที่เป็นอันตรายมากสำหรับการเงินและธุ
รกิจในปี 2561 รองลงมาเป็นโทรจัน Emotet คิดเป็น 15%
โดยภัยคุกคามนี้สามารถเป็นอันตรายเมื่อเข้าสู่เครือข่ายขององค์กรได้
ซึ่งสามารถกระจายตัวเองผ่านช่องโหว่ของอุปกรณ์ที่ไม่ได้อัปเดต
จากนั้นจะดาวน์โหลดภัยคุกคามอื่น ๆ มายังอุปกรณ์ที่ตกเป็นเหยื่อ

โทรจันอันดับสามคือโทรจัน Trickster คิดเป็น 12%
ของโทรจันทั้งหมดที่ถูกเปิดเผย
ส่วนลักษณะการโจมตีของผู้ใช้ส่วนตัวจะแตกต่างจากผู้ใช้ในองค์กร
รายชื่อมัลแวร์ที่พยายามจะโจมตีนั้นอันดับแรกคือ มัลแวร์ Zbot คิดเป็น
26% ที่เข้ามาขโมยข้อมูลสำคัญ รองลงมาเป็น RTM และ Emotel
ที่ได้กล่าวไปแล้วข้างต้น ซึ่งผลออกมาเป็นที่น่าสนใจ นั่นก็คือในปี 2561

โทรจัน RTM จะตั้งเป้าโจมตีผู้ใช้งานในองค์กร แต่ในปี 2562 นี้ RTM เริ่มคุกคามผู้ใช้ส่วนตัวมากขึ้นด้วย

“เราคาดว่าจะมีจำนวนผู้ใช้ที่โดนโจมตีมากขึ้นในครึ่งปีหลัง 2562 โดยปกติเราจะเห็นกิจกรรมการโจมตีที่เพิ่มสูงขึ้นหลังเทศกาลวันหยุด เพราะในช่วงวันหยุดคนใช้อุปกรณ์น้อยกว่าปกติ และทำให้มีโอกาสน้อยในการถูกโจมตี เราขอแนะนำให้ทุกคนระมัดระวังเป็นพิเศษเมื่อทำธุรกรรมทางการเงินทางออนไลน์” โอเลก คูปรีฟ นักวิจัยด้านความปลอดภัย Kaspersky กล่าว

เพื่อป้องกันองค์กรและธุรกิจของคุณจากมัลแวร์การเงิน ผู้เชี่ยวชาญด้านความปลอดภัยของ Kaspersky ให้คำแนะนำ ดังนี้

 แนะนำการอบรม cybersecurity awareness training สำหรับพนักงาน โดยเฉพาะอย่างยิ่งพนักงานรับผิดชอบด้านบัญชี เพื่อสอนให้พวกเขาสามารถแยกได้ว่าอันไหนคือการโจมตีแบบฟิชชิ่ง ไม่เปิดไฟล์แนบหรือคลิกลิงก์ที่น่าสงสัย

 ติดตั้งการอัปเดตของซอฟต์แวร์ทั้งหมด

 ห้ามติดตั้งโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือหรือแหล่งที่ไม่รู้จัก

 ในการป้องกันปลายทาง การสอบสวนและการแก้ไขอย่างทันท่วงที การใช้โซลูชั่น EDR เช่น Kaspersky Endpoint Detection and Response สามารถตรวจจับมัลแวร์การเงินได้

 บูรณาการ Threat Intelligence เข้ากับระบบควบคุมความปลอดภัย SIEM เพื่อที่จะเข้าถึงข้อมูลภัยคุกคามที่อัปเดตล่าสุด

Kaspersky แนะนำผู้ใช้ส่วนตัว ดังนี้ :

 ควรติดตั้งการอัปเดตความปลอดภัยในทันที

 ไม่ควรติดตั้งซอฟต์แวร์จากแหล่งที่ไม่รู้จัก อุปกรณ์เคลื่อนที่ควรจะปิดตัวเลือกนี้ในการตั้งค่า

 ใช้โซลูชั่นด้านความปลอดภัย เช่น Kaspersky Total Security

อ่านรายงานฉบับเต็มได้ที่ Securelist.com

เกี่ยวกับ Kaspersky

Kaspersky เป็นบริษัทด้านความปลอดภัยบนอินเทอร์เน็ตระดับโลก

ที่ก่อตั้งในปี 1997
ด้วยความเชี่ยวชาญด้านความปลอดภัยที่ได้พัฒนามาอย่างต่อเนื่อง
จนปัจจุบันเปลี่ยนเป็นโซลูชั่นความปลอดภัยยุคใหม่
ที่ให้บริการในการป้องกันสำหรับธุรกิจ โครงสร้างพื้นฐาน
รัฐบาลและลูกค้าทั่วโลก การให้บริการของบริษัทประกอบด้วย
การป้องกันปลายทาง
โซลูชั่นการป้องกันความปลอดภัยแบบพิเศษจำนวนมาก
และบริการเพื่อป้องกันภัยคุกคามดิจิทัล ซึ่ง Kaspersky
ได้ป้องกันความปลอดภัยให้แก่ผู้ใช้กว่า 400 ล้านคน และอีกกว่า
270,000 องค์กร
ที่ป้องกันความปลอดภัยให้กับทุกส่วนที่สำคัญสำหรับลูกค้า
ศึกษาข้อมูลเพิ่มเติมได้ที่ www.kaspersky.com