BangkokBizNews.com
กรุงเทพธุรกิจ

ปีที่ 29 ฉบับที่ 9967 วันพุธที่ 6 มกราคม พ.ศ. 2559 หน้า 30

'โรงเรียน-ไอโฟน-ไอโอที' เป้าใหญ่'แฮคเกอร์'ปีวอก

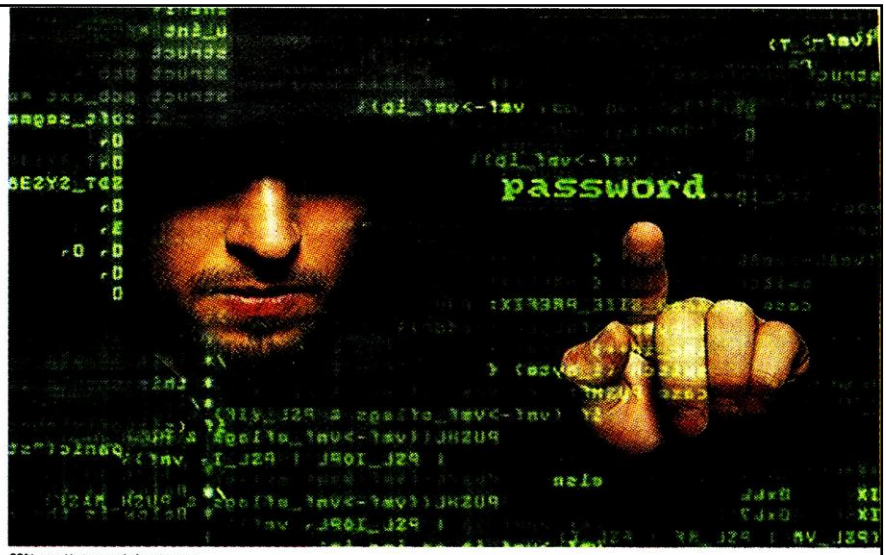
'วอทช์การ์ด' ประเมินภัยคุกคามความปลอดภัยปี 2559 อาจครอบคลุมตั้งแต่ อีเมลหลอกลวง เว็บไซต์ปลอม ไปจนถึงเทคโนโลยีไอโอที และมัลแวร์ที่แฝงตัวมากับโฆษณา

วอทช์การ์ด เทคโนโลยีส์ เผยรายงานการคาดการณ์ความปลอดภัยของข้อมูลประจำปี 2559 ชี้ให้เห็นถึงกระแสภัยคุกคามรูปแบบใหม่ๆ ได้แก่ ไวรัสเรียกค่าไถ่ขึ้นสูงที่จะถูกปล่อยเข้าไปอยู่ในแพลตฟอร์มต่างๆ การโจมตีซึ่งพุ่งเป้าไปที่ระบบปฏิบัติการไอโอเอสมากขึ้น รวมถึงช่องทางใหม่ สำหรับคนร้ายในการขโมยข้อมูลส่วนตัวเพื่อนำไปแอบอ้างตัวตน

นายโครีย์ แนชเรเนอร์ ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีของวอทช์การ์ด กล่าวว่า ภัยคุกคามความปลอดภัยมีการเปลี่ยนแปลงอยู่ตลอดเวลา เนื่องจากอาชญากรไซเบอร์ใช้วิธีการทั้งเก่าและใหม่เพื่อขยายขอบเขตการเข้าถึง แสวงหาประโยชน์ และล้วงข้อมูลสำคัญจากผู้ใช้

ทั้งนี้ วอทช์การ์ด แนะว่า เพื่อสร้างเกราะป้องกันให้ดีขึ้น ควรฝึกอบรมพนักงานเกี่ยวกับภัยคุกคามและเทคนิคทางจิตวิทยาอย่าง โซเชียล เอ็นจิเนียริ่ง หรือการอาศัยช่องโหว่จากพฤติกรรมของผู้ใช้เฉพาะกลุ่ม ตลอดจนการใช้เทคโนโลยีความปลอดภัยเครือข่ายใหม่ล่าสุด เพื่อให้องค์กรสามารถบ่งชี้ปัญหาความปลอดภัยได้ทันที จะช่วยสกัดการโจมตีส่วนใหญ่ที่คาดการณ์ว่าจะเกิดขึ้นในปี 2559 นี้

ไม่ว่าจะเป็น ไวรัสเรียกค่าไถ่จะถูกปล่อยเข้าไปอยู่ในแพลตฟอร์มต่างๆ, เทคนิค โซเชียล เอ็นจิเนียริ่ง ซึ่งอาศัยช่องโหว่จากพฤติกรรมของผู้ใช้จะเป็นภัยคุกคามใหญ่หลวง, การเจาะระบบรักษาความปลอดภัยของธุรกิจเอสเอ็มบีจะกลับสู่รูปแบบพื้นฐาน, มัลแวร์บนระบบปฏิบัติการไอโอเอสจะพุ่งสูงขึ้น, มัลแวร์ที่แฝงตัวมากับโฆษณาจะเพิ่มขึ้นโดยอาศัยวิธีการเข้ารหัส, ระบบอัตโนมัติจะยกระดับความปลอดภัยไปอีกขั้น, อาชญากรไซเบอร์จะล้วงข้อมูลในสถานศึกษา, เฟิร์มแวร์ปลอมจะมุ่งโจมตีเทคโนโลยีอินเทอร์เน็ต ออฟ ธิงส์, ฟีเจอร์อุปกรณ์ไร้สายที่ "ใช้งานง่าย" จะกลายเป็นช่องโหว่ร้ายแรงของอุปกรณ์ไร้สายในอนาคต และกลุ่มแฮคเกอร์ที่ปฏิบัติการเคลื่อนไหวทางการเมือง หรือ Hacktivist จะเจาะระบบสื่อประเภทกระจายภาพและเสียง



ภาพ : null-byte wonderhowto.com

> มัลแวร์บนระบบปฏิบัติการไอโอเอสจะพุ่งสูงขึ้น

ก่อนหน้านี้แคสเปอร์สกี้ แลป ออกมาระบุว่า ภัยคุกคามบนโมบาย เป็นอีกหนึ่งภัยคุกคามที่น่าจับตา จากนี้จะเห็นเพิ่มมากขึ้น โดยเฉพาะการพยายามขโมยเงินจากบัญชีธนาคารออนไลน์ รวมถึงการโจมตีไซเบอร์แบบพุ่งเป้าก็ยังขยายขอบเขตไปอย่างต่อเนื่อง

โดยเฉพาะแพคเกจที่ประสงค์ร้ายช่วงปีที่ผ่านมา มีจำนวนมากกว่า 1.5 ล้านแพคเกจที่ติดตั้งลงในโมบายดีไวซ์ ซึ่งเพิ่มขึ้นจากเดิมมากกว่า 1.5 เท่า ขณะเดียวกันมีการแจ้งเตือนจำนวน 5.68 ล้านครั้งว่า มีมัลแวร์ที่พยายามขโมยเงินจากยูสเซอร์ผ่านบัญชีธนาคารออนไลน์

ช่วงไตรมาสที่ 3 ของปีที่แล้วยูสเซอร์ในประเทศออสเตรียถูกโจมตีโดยโทรจันแบงก์กิ้งมากกว่าภูมิภาคอื่น ยูสเซอร์ที่ใช้แคสเปอร์สกี้ แลปในออสเตรีย จำนวน 5% เผชิญหน้ากับภัยคุกคามนี้ ขณะที่ประเทศสิงคโปร์ ซึ่งครองอันดับที่ 1 ในไตรมาสที่แล้ว เลื่อนมาเป็นอันดับ 2 หรือ 4.2% และอันดับ 3 คือประเทศตุรกีหรือราว 3%

ประเทศที่ถูกโจมตีใน 10 อันดับแรกส่วนใหญ่มีตัวเลขการใช้งานบัญชีธนาคารออนไลน์ที่โดดเด่นซึ่งจูงใจอาชญากรทางไซเบอร์ ในจำนวนมัลแวร์ที่ใช้ในการพุ่งเป้าไปยังบัญชีธนาคารออนไลน์ของยูสเซอร์ โทรจัน Trojan-Downloader.Win32.Upatre เป็นโทรจันที่พบได้บ่อยมากที่สุด ถูกใช้โจมตีสูงถึง 63.1% ของการโจมตีทั้งหมดเพื่อพยายามขโมยรายละเอียดการใช้จ่ายของยูสเซอร์

ทั้งนี้ แสดงให้เห็นว่าขอบเขตของภัยคุกคามระดับโลกยังคงค่อยๆ เติบโตขึ้นอย่างรวดเร็ว โปรแกรมประสงค์ร้ายต่อโมบายดีไวซ์ยังคงเพิ่มขึ้น และปรากฏในประเทศที่นิยมใช้บัญชีธนาคารออนไลน์ ผู้ใช้จึงมีความเสี่ยงค่อนข้างมากจากโทรจันที่จ้องโจมตีเป้าหมาย พบว่ามีเหตุการณ์พยายามโจมตีและขโมยบัญชีธนาคารออนไลน์จำนวน 5.6 ล้านครั้ง และอาชญากรไซเบอร์ก็พัฒนาการโจมตีให้ซ่ำซองมากยิ่งขึ้น

ดังนั้น การใช้ผลิตภัณฑ์เพื่อความปลอดภัยทางไซเบอร์คุณภาพสูงจึงสำคัญมากเมื่อใช้อินเทอร์เน็ต ทั้งสำหรับบุคคลทั่วไปและองค์กรซึ่งต้องปกป้องตัวเองจากการที่ภัยคุกคามเพิ่มขึ้นอย่างต่อเนื่อง