ฟอร์ติการ์ดแล็ปส์จากฟอร์ติเน็ตคาดแนวโน้มภัยคุกคามเครือข่ายปี 2013

แนวโน้มเป็นการคุกคามต่อเนื่อง บนไอพีวี 6 และรวมถึงการสื่อสารระหว่างอุปกรณ์

แคลิฟอร์เนีย, 20 พฤศจิกายน 2555 – Fortinet® (NASDAQ: FTNT) – ฟอร์ติเน็ตผู้นำโลกในอุตสาหกรรมความปลอดภัยเครือข่ายประสิทธิภาพ – ประกาศถึงแนวโน้มภัยคุกคามเครือข่ายปี 2013 ที่ควรจับตามอง 6 ประเภทด้วยกัน

1. APT มุ่งเป้าหมายเป็นรายบุคคลทางโมบาย

APT หรือ Advanced Persistent Threats คือประเภทหนึ่งของอาชญากรรมทางคอมพิวเตอร์ที่มีเป้าหมายเพื่อโจมตีเหยื่อที่มีข้อมูลสำคัญมีเป้าหมายที่แน่ชัดพยายาม ใช้ทุกวิถีทางเพื่อให้การโจมตีสำเร็จผล และที่ค้นพบล่าสุด เช่น โทรจัน Stuxnet, Flame และ Gauss ในปีค.ศ. 2013 นี้ คาดว่ารูปแบบการโจมตีแบบ APT จะมุ่งโจมตีมีเป้าหมายที่เป็นคนดังที่ร่ำรวยมีชื่อเสียง ผู้บริหารระดับซีอีโอ และนักการเมืองที่มีชื่อเสียง เมื่อแฮกเกอร์ได้ข้อมูลที่ต้องการแล้วมักจะค่อยๆ ถอนมัลแวร์จากอุปกรณ์นั้นอย่างเงียบๆ ก่อนที่เหยื่อจะรู้ตัว จึงทำให้คาดการณ์ได้ยาก เนื่องจากเมื่อเกิดเหตุขึ้นเหยื่อมักไม่ได้แจ้งข่าวให้ชัดเจนเนื่องจากเห็นว่าไม่ใช้เรื่องสำคัญ อย่างไรก็ตาม แฮกเกอร์มักมองหาข้อมูลสำคัญที่นำมาก่ออาชญากรรมภายหลัง อาทิ การขู่กรรโชก การขู่เปิดโปง หากมิจ่ายเงินให้ตามต้องการ

2. การพิสูจน์ตัวตน 2 ด้านจะแทนการถามพาสเวิร์ดเพียงครั้งเดียว

การพิสูจน์ตัวตนก่อนเข้าระบบด้วยวิธีการถามพาสเวิร์ดเพียงครั้ง (Single Password Sign on) จะหมดไป และการพิสูจน์ตัวตน 2 ด้าน (Two Factor Authentication) จะเข้ามาแทนที่ เนื่องจากในปัจจุบันมีทูลส์ที่สามารถดาวน์โหลดอย่างง่ายๆ ที่ช่วยในการหารหัสผ่านได้ภายในไม่กี่นาที เช่น หากผู้โจมตีใช้ทูลส์ในการเจาะหารหัสผ่านจากคลาวด์และจ่ายเพียง 20 เหรียญสหรัฐ จะสามารถป้อนรหัสได้ 300 ล้านรหัสที่ต่างกันได้เพียงในแค่ 2- นาที ยิ่งไปกว่านั้น ผู้โจมตีสมัยนี้มีความเชี่ยวชาญมาก สามารถเจาะหารหัสผ่านที่เป็นตัวอักษรและตัวเลขที่ซับซ้อนได้ใน

ระยะเวลาไม่ถึงชั่วโมง เป้าหมายที่เป็นที่ต้องการมักเป็นข้อมูลสำคัญในดาต้าเบส (อาจแฮกผ่านทาง Web portals และช่องโหว่ SQL injection) และ Wireless security (WPA2) ผ่านบริการคลาวด์ ฟอร์ติเน็ตคาดว่า ปีหน้าองค์กรจะให้พนักงานและลูกค้าตั้งระบบการพิสูจน์ตัวตน 2 ด้าน เช่น ข้อมูลเกี่ยวกับสิ่งที่เป็น และสิ่งที่มีเมื่อต้องใช้อุปกรณ์โทรศัพท์มือถือเข้ามาทำธุรกรรม ถึงแม้เราได้เคยเห็นว่า ในปีค.ศ. 2011 บอทเน็ท Zitmo สามารถแฮกอุปกรณ์แอนดรอยด์และโทเคน SecurID ของ RSA ได้สำเร็จถึงแม้ใช้วิธีการพิสูจน์ตัวตน 2 ด้านแล้วก็ตาม แต่วิธีนี้ยังเป็นวิธีที่นิยมสำหรับระบบออนไลน์อยู่ต่อไป

-

3. มุ่งโจมตีการสื่อสารระหว่างอุปกรณ์กับอุปกรณ์

การสื่อสารระหว่างอุปกรณ์กับอุปกรณ์ หรือ Machine-to-machine (M2M) หมายถึงเทคโนโลยีที่อนุญาตให้อุปกรณ์ในระบบตามสายและไร้สายได้สื่อสารกันด้วยศักยความสามารถที่เท่ากัน อาจเป็นตู้เย็นสื่อสารกับเซิร์ฟเวอร์เพื่อเตือนให้เจ้าของบ้านซื้อนมและไข่ อาจเป็นกล้องที่สนามบินถ่ายภาพหน้าผู้เดินทางและสื่อสารกับดาต้าเบสเพื่อตรวจสอบประวัติอาชญากรรม หรือเป็นอุปกรณ์การแพทย์ที่ให้ออกซิเจนกับผู้ประสบอุบัติเหตุและยังสามารถส่งสัญญาณเตือนถึงระดับการเต้นของหัวใจที่ต่ำลงให้กับทีมแพทย์ที่โรงพยาบาลได้ ในขณะที่มีความพยายามที่จะพัฒนา M2M เพื่อลดความผิดพลาดของมนุษย์แต่ยังมีการพูดถึงวิธีการสร้างความปลอดภัยที่ดีที่สุดให้กับระบบนี้ เราคาดว่าปีหน้าเราจะได้เห็นงการแฮก M2M ครั้งแรกและน่าจะเกี่ยวข้องกับความมั่นคงของชาติ เช่น อุปกรณ์ที่อำนวยความสะดวกการพัฒนาอาวุธ โดยมีแนวโน้มว่าน่าจะเป็นการให้ข้อมูลที่สามารถบิดเบือนการทำงานของ M2M และทำให้เครื่องหนึ่งทำผิดข้อมูล จึงสร้างช่องโหว่และเข้าโจมตีที่จุดเสี่ยงนี้

4. พฤติกรรมหลีกเลี่ยงแซนบ๊อกซ์มากขึ้น

Sandboxing คือ วิธีการให้การกรองแยกโปรแกรมและแอปพลิเคชั่น จึงไม่สามารถโอนโค้ดที่แปลกปลอมเข้ามาได้ เช่น จากการอ่านเอกสารไปยังระบบปฏิบัติการ โดยมีผู้ค้าหลายรายเช่น Adobe และ Appleได้ใช้วิธีการนี้ เมื่อมีเทคโนโลยีแล้ว แฮกเกอร์มักจะหลีกเลี่ยงไป ฟอร์ติการ์ดแล็ปส์เองเคยเห็นการรุกรานนี้ในแซนบ๊อกซ์ของอุปกรณ์เสมือน (Virtual machine – VM) อาทิ ในช่องโหว่ของ Adobe Reader X มาแล้ว และในปีหน้า เราคาดว่าจะเห็นรหัสแบบใหม่ที่ได้รับการออกแบบมาเพื่อหลีกเลี่ยง Sandbox ใช้โดยเฉพาะกับอุปกรณ์รักษาความปลอดภัยและอุปกรณ์มือถือ

5. บอทเน็ทคุกคามข้ามแพลทฟอร์ม

ในปีค.ศ. 2012 ฟอร์ติการ์ดแล็ปส์ได้ติดตามโมบายบอทเน็ท เช่น Zitmo และพบว่ามีคุณลักษณะและการทำงานคล้ายบอทเน็ทของเครื่องพีซี ในปีหน้านี้ ฟอร์ติการ์ดแล็ปส์คาดว่าเราน่าจะได้เห็นรูปแบบใหม่ของภัย Denial of

Service (DoS) ที่คุกคามทั้งเครื่องพีซีและอุปกรณ์มือถือในเวลาพร้อมๆ กัน อาทิ เครื่องพีซีและอุปกรณ์มือถือที่ใช้เซิร์ฟเวอร์การควบคุมและคำสั่ง Command and Control (C&C) เดียวกันเกิดติดเชื้อ จะจู่โจมโปรโตคอลและกระทำเหมือนกันในเวลาเดียวกัน ซึ่งยิ่งทำให้บอทเน็ทนั้นแพร่กระจาย แต่เดิมบอทเน็ททำงานแยกกันเช่น บนเครื่องคอมพิวเตอร์และระบบปฏิบัติการมือถือ (เช่น Android) ปัจจุบันนี้จะกลายเป็นบอทเน็ทที่แข็งแกร่ง สามารถปฏิบัติข้ามแพลทฟอร์มได้

6. มัลแวร์บนโมบายจะโตไล่ตามมัลแวร์บนเดสท้อปและแล็ปท้อป

แต่เดิมที่ผ่านมา ผูลิตมัลแวร์จะผลิตมัลแวร์เพื่อมุ่งโจมตีเดสท้อปและแล็ปท้อปเนื่องจากเป็นอุปกรณ์ที่มีจำนวนมาก ในปัจจุบันนี้ จะผลิตมัลแวร์เพื่อทั้งบนโมบายและเดสท้อปแล็ปท้อป ฟอร์ติการ์ดแล็ปส์ได้พบตัวอย่างมัลแวร์บนโมบายกว่า 50,000 ชนิดในขณะที่พีซีมีนับล้านๆ ชนิด นักวิจัยสังเกตุเห็นว่าจำนวนของมัลแวร์บนโมบายโตขึ้นมาก เนื่องจากมีจำนวนมือถือใช้งานมากขึ้นกว่าเดสท้อปและแล็ปท้อปนั่นเอง อาจใช้เวลาหลายปีกว่ามัลแวร์บนโมบายจะโตไล่ทันมัลแวร์บนเดสท้อปและแล็ปท้อปเนื่องจากอุปกรณ์โมบายจะซับซ้อนกว่าพีซีแบบเดิมๆ มาก