

Group-IB เผยธนาคาร เงินดิจิทัล และโครงสร้างพื้นฐานสำคัญ จะตกเป็นเป้าหมายหลักของแฮกเกอร์ในอนาคตอันใกล้



1. ในปีหน้า ความเสียหายหลักจากการโจมตีทางไซเบอร์สำหรับธนาคารจะไม่ใช้การขโมยเงิน แต่เป็นการทำลายโครงสร้างพื้นฐานไอทีในขั้นตอนสุดท้ายของการเจาะข้อมูล ในอดีตที่ผ่านมา บรรดาธนาคารถูกโจมตีโดยอาชญากรไซเบอร์เท่านั้น แต่ในปัจจุบัน แฮกเกอร์ที่มีความเกี่ยวข้องกับรัฐโจมตีธนาคารถี่กว่าเดิมมาก โดยปกติอาชญากรไซเบอร์จะพยายามปกปิดร่องรอยการโจรกรรม ส่วนแฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐจะสร้างความเสียหายสูงสุดแก่ธนาคารและทำให้การดำเนินงานต้องหยุดชะงักลงด้วยการทำลายโครงสร้างพื้นฐานไอที ซึ่งทั้งสองกรณีนี้ มูลค่าความเสียหายต่อธนาคารอาจสูงกว่ามูลค่าเงินที่ถูกขโมยไป เนื่องจากการให้บริการต้องหยุดชะงัก ขณะที่ความน่าเชื่อถือของธนาคารก็ถูกบั่นทอน

(โลโก้: http://mma.prnewswire.com/media/582503/Group_IB_Logo.jpg)

2. แฮกเกอร์จะโจมตีโรงงานอุตสาหกรรมได้มากขึ้น เนื่องจากเรียนรู้วิธีการจัดการกับ “ตรรกะ” ของโครงสร้างพื้นฐานสำคัญ โดยปกติแล้ว โรงงานจะมีระบบไอทีที่ซับซ้อนและมีเอกลักษณ์ แม้จะเจาะเข้าระบบได้ก็ยังคงต้องมีความรู้เฉพาะเกี่ยวกับหลักการดำเนินงานจึงจะสามารถโจมตีระบบได้ ทว่าในช่วงไม่กี่ปีมานี้ เราสังเกตเห็นว่าแฮกเกอร์มีความสามารถมากขึ้น และสร้างความเสียหายต่อโครงสร้างพื้นฐานสำคัญได้มากขึ้น ดังนั้นเราจึงคาดการณ์ว่า การโจมตีครั้งใหญ่จะพุ่งเป้าไปที่โรงงานอุตสาหกรรมและโครงสร้างพื้นฐานสำคัญที่เกี่ยวข้องมากขึ้น

3. แฮกเกอร์เปลี่ยนเป้าหมายจากธนาคารไปสู่อุตสาหกรรมเงินดิจิทัล (การเสนอขายโทเคนต่อสาธารณชนเป็นครั้งแรก (ICO) กระเป๋าเงินดิจิทัล ตลาดแลกเปลี่ยน และกองทุน) ที่กำลังมีการเพิ่มเงินทุนจำนวนมหาศาลอย่างต่อเนื่องในทางเทคนิคแล้ว การโจมตีผู้ให้บริการในภาคส่วนนี้ไม่ได้ง่ายไปกว่าการโจมตีธนาคาร ทว่าความปลอดภัยข้อมูลและความสมบูรณ์ของบริษัทบล็อกเชนยังต่ำกว่ามาก นอกจากนี้ เทคโนโลยีบล็อกเชนยังไม่มีกระบวนการควบคุมที่เข้มงวดและมีการปกปิดตัวตนมากกว่า บรรดาแฮกเกอร์จึงมองว่ามีโอกาสน้อยกว่าที่จะถูกจับได้ในระหว่างกระทำการ

รับชมรายงานฉบับเต็มได้ที่ <https://www.group-ib.com/2017-report.html>

เกี่ยวกับ Group-IB

Group-IB ช่วยให้องค์กรขนาดใหญ่ตระหนักรู้และสามารถรับมือกับภัยคุกคามออนไลน์ที่มีต้นกำเนิดจากรัสเซีย ยุโรปตะวันออก และศูนย์กลางการโจมตีทางไซเบอร์อื่นๆ โดย Group-IB Threat Intelligence ช่วยให้องค์กรต่างๆ สามารถสร้างเกราะป้องกันการโจมตีทางไซเบอร์ที่ซับซ้อนได้อย่างมีประสิทธิภาพมากขึ้น ทั้งนี้ Group-IB เป็นพันธมิตรอย่างเป็นทางการของ EUROPOL และ INTERPOL ขณะเดียวกัน Gartner, Forrester, IDC, Organization for Security and Co-operation in Europe (OSCE) และองค์กรอีกมากมาย ต่างก็ให้การยอมรับ Group-IB ในฐานะผู้นำด้านการป้องกันการฉ้อโกงออนไลน์ การขโมยเงิน และความเสียด้านชื่อเสียง รับชมข้อมูลเพิ่มเติมได้ที่ <http://www.group-ib.com>

ที่มา: Group-IB