FireEye เผยการโจมตีไซเบอร์ในประเทศอินเดียและประเทศเพื่อนบ้าน

นิวเดลี, ประเทศอินเดีย–(Marketwired)–21 ส.ค. 2558

– แคมเปญล่าสุดตั้งเป้าไปยังองค์กรต่างๆ ในประเทศบังคลาเทศ เนปาล และปากีสถาน โดยเล็งสืบหาข้อมูลเกี่ยวกับข้อพิพาทชายแดน

FireEye, Inc. (NASDAQ: FEYE) ผู้นำในการหยุดยั้งการโจมตีไซเบอร์ขั้นสูงในปัจจุบัน ได้ทำการเปิดเผยรายละเอียดของแคมเปญการโจมตีขั้นสูง ซึ่งคาดว่ามีเป้าหมายไปยังการขโมยข้อมูลเกี่ยวกับข้อพิพาททางชายแดนและการเจรจาต่อรองเรื่องอื่น ๆ ในภูมิภาค

โดย FireEye เชื่อว่าการโจมตีดังกล่าวมีกลุ่มผู้โจมตีขั้นสูง (APT) ที่มีฐานปฏิบัติการอยู่ในประเทศจีน เป็นผู้อยู่เบื้องหลังการดำเนินการ โดยผู้โจมตีได้ทำการส่งอีเมล์ฟิชชิ่งแบบกำหนดเป้าหมายไว้ พร้อมกับแนบเอกสารไมโครซอฟท์เวิร์ดโดยเอกสารเหล่านี้จะมีเนื้อหาเรื่องการแก้ไขปัญหาในระดับภูมิภาค แต่จะมีการแนบสคริปท์ที่มีชื่อว่า WATERMAIN ซึ่งจะทำการสร้างช่องทางเชื่อมต่อ backdoor ไว้บนเครื่องที่โดนโจมตี ซึ่งการโจมตีของแคมเปญนี้ได้ถูกตรวจพบในเดือนเมษายนปี พ.ศ. 2558 ประมาณหนึ่งเดือนล่วงหน้าก่อนที่นายกรัฐมนตรีอินเดีย Narendra Modi จะเดินทางไปเยือนประเทศจีนเป็นครั้งแรก

FireEye ได้เฝ้าสังเกตกิจกรรม WATERMAIN มาตั้งแต่ปี พ.ศ. 2554 โดยตลอดสี่ปีที่ผ่านมา กลุ่มภัยคุกคามนี้ได้ใช้มัลแวร์ WATERMAIN ในการโจมตีเป้าหมายต่างๆมากกว่า 100 ราย โดยร้อยละ 70 ของกลุ่มเป้าหมายจะอยู่ในอินเดีย และกลุ่มที่ใช้ WATERMAIN นั้นยังมีเป้าหมายอยู่ที่นักเคลื่อนไหวทางการเมืองชาวทิเบตและ องค์กรในชาติอื่นๆ ในเอเชียตะวันออกเฉียงใต้ โดยจะมุ่งเน้นไปที่องค์กรภาครัฐ สถานทูต วิทยาศาสตร์และการศึกษา

“การเก็บข้อมูลข่าวกรองของอินเดียยังคงเป็นเป้าหมายยุทธศาสตร์ที่สำคัญของกลุ่ม APT ที่มีฐานอยู่ในจีน และการโจมตีเหล่านี้ในประเทศเพื่อนบ้านของอินเดียสะท้อนให้เห็นถึงความสนใจที่เพิ่มขึ้นในกิจการระหว่างประเทศ” คำกล่าวของ Bryce Boland หัวหน้าเจ้าหน้าที่ฝ่ายเทคโนโลยี FireEye ประจำภูมิภาคเอเชียแปซิฟิก “องค์กรควรจะเพิ่มความพยายามของพวกเขาในการรักษาความปลอดภัยในโลกไซเบอร์ และให้แน่ใจว่าพวกเขาสามารถป้องกัน ตรวจจับและตอบสนองต่อการโจมตีเพื่อที่จะปกป้องตัวเองได้”

การโจมตีแบบ APT ไปยังองค์กรในอินเดียและประเทศเพื่อนบ้านนั้นเป็นเรื่องที่เกิดขึ้นอยู่บ่อยครั้ง โดยในเดือน

เมษายน ทาง FireEye ได้เปิดเผยรายละเอียดของกลุ่มผู้โจมตีขั้นสูงที่เรียกว่า APT30 ซึ่งเป็นแคมเปญการจารกรรมไซเบอร์นานกว่าหนึ่งทศวรรษ โดยมีผู้ต้องสงสัยคือกลุ่มผู้โจมตีที่มีฐานปฏิบัติการณ์อยู่ในประเทศจีน ซึ่งมีบริษัทด้านการบินและการป้องกันทางการทหารในอินเดีย อยู่ในรายชื่อของกลุ่มเป้าหมายด้วยเช่นกัน

ตราบริษัท
http://release.media-outreach.com/i/Download/3524

เกี่ยวกับ FireEye, Inc.
FireEye ได้คิดค้นแพลตฟอร์มการรักษาความปลอดภัยที่ใช้การวิเคราะห์ผ่านระบบจำลองเสมือน ที่จะช่วยให้การป้องกันภัยคุกคามชั้นสูงได้แบบเรียลไทม์แก่องค์กรและหน่วยงานภาครัฐทั่วโลกจากการโจมตีไซเบอร์รูปแบบใหม่ๆ ซึ่งเป็นการโจมตีที่มีความซับซ้อนสูง และสามารถหลบหลีกการป้องกันแบบดั้งเดิมที่พึ่งพาการใช้ซิกเนเจอร์ เช่น ไฟร์วอลล์รุ่นใหม่, IPS, ป้องกันไวรัสและเกตเวย์ ได้อย่างง่ายดาย โดยแพลตฟอร์มการป้องกันภัยคุกคามของ FireEye สามารถช่วยป้องกันการคุกคามแบบเรียลไทม์โดยไม่ต้องใช้ซิกเนเจอร์ในการป้องกันองค์กร โดยสามารถครอบคลุมถึงการป้องกันการโจมตีผ่านช่องทางหลักๆ และในทุกขั้นตอนของวงจรชีวิตของการโจมตี ด้วยการทำงานร่วมกันของระบบวิเคราะห์ผ่านระบบจำลองเสมือน กับข้อมูลเชิงลึกของการโจมตีทางไซเบอร์ จะช่วยในการตรวจจับและป้องกันการโจมตีในโลกไซเบอร์ได้แบบเรียลไทม์ โดยในปัจจุบัน FireEye มีลูกค้ากว่า 3,700 รายใน 67 ประเทศ ซึ่งรวมถึง 675 องค์กรใน Forbes Global 2000

ข้อมูลการติดต่อ

นักลงทุนติดต่อ
Kate Patterson
FireEye, Inc.
kate.patterson@fireeye.com
408-321-4957

สื่อมวลชนติดต่อ
Patrick Neighorn
FireEye, Inc.
patrick.neighorn@FireEye.com
+65-3158-5732