แคสเปอร์สกี้ แลป เปิดโปงโครงสร้างปฏิบัติการ “Crouching Yeti” ตัวการผู้จ้องป่วนภาคอุตสาหกรรม

แคสเปอร์สกี้ แลป เปิดโปงโครงสร้างการปฏิบัติการของกลุ่ม Crouching Yeti หรือรู้จักกันอีกชื่อว่า Energetic Bear ใช้ภาษารัสเซีย เป็นกลุ่มที่รวบรวมเซิร์ฟเวอร์ที่มีช่องโหว่ทั่วโลก จากข้อมูลการวิจัยพบว่า ตั้งแต่ปี 2016 เป็นต้นมามีเซิร์ฟเวอร์ในหลายประเทศถูกโจมตี เพื่อใช้เป็นทางผ่านไปยังเป้าหมายอื่น หรือบางครั้งเจาะเข้าเซิร์ฟเวอร์ที่โฮสต์เว็บไซต์ภาษารัสเซียเพื่อกระจายมัลแวร์ (watering holes)

Crouching Yeti เป็นกลุ่ม APT (advanced persistent threat) ที่ใช้ภาษารัสเซีย ที่ทางแคสเปอร์สกี้ แลปเฝ้าดูพฤติกรรมมาตั้งแต่ปี 2010 เป็นที่รู้กันดีว่ามีเป้าหมายที่กลุ่มอุตสาหกรรมทั่วโลก โดยเฉพาะเน้นที่ระบบด้านพลังงาน มุ่งโจรกรรมข้อมูลมีค่าจากระบบของเหยื่อ เทคนิคการโจมตีที่ใช้ คือ watering hole ด้วยการโจมตีเว็บไซต์ที่เป็นที่นิยมมีคนเข้าใช้งานเยอะ จากนั้นกระจายลิ้งก์ที่นำโยงผู้ใช้เว็บไปยังเซิร์ฟเวอร์ของผู้ร้าย

เมื่อเร็วๆ นี้ แคสเปอร์สกี้ แลปได้ค้นพบเซิร์ฟเวอร์จำนวนหนึ่งที่ถูกโจมตี เป็นขององค์กรในรัสเซีย สหรัฐอเมริกา ตุรกี และประเทศในยุโรป ข้อมูลจากนักวิจัยระบุว่ามีการโจมตีช่วงปี 2016 และ 2017 ด้วยจุดประสงค์ต่างกันไป นอกจากโจมตีผ่านเว็บไซต์แล้ว (watering hole) ในบางกรณี จะใช้เป็นทางผ่านไปยังเป้าหมายที่แท้จริงต่อไป

ในการวิเคราะห์เซิร์ฟเวอร์ที่ติดเชื้อนั้น นักวิจัยได้พบว่ามีเว็บไซต์รวมทั้งเซิร์ฟเวอร์ในรัสเซีย อเมริกา ยุโรป และละตินอเมริกา ที่ถูกสแกนด้วยทูลหลายแบบ น่าที่จะเพื่อหาเซิร์ฟเวอร์ที่เหมาะจะโฮสต์ทูลเอาไว้ เพื่อพัฒนามาเป็นการโจมตีภายหลัง บางเว็บไซต์ที่ถูกสแกนอาจจะถูกเก็บไว้เป็นตัวเลือกสำหรับใช้เป็น waterhole ทั้งนี้ ประเภทของเว็บไซต์และเซิร์ฟเวอร์ที่ผู้ร้ายสนใจนั้นมีหลากหลายแบบ นักวิจัยของแคสเปอร์สกี้ แลป พบว่าผู้บุกรุกสแกนเว็บไซต์ประเภทต่างๆ จำนวนมาก เช่น ร้านค้าและบริการออนไลน์ หน่วยงานราชการ เอ็นจีโอ ธุรกิจการผลิต เป็น

ผู้เชี่ยวชาญยังพบด้วยว่ากลุ่มนี้ได้ใช้ทูลที่มีอยู่แพร่หลายทั่วไปในการกระทำการอีกด้วย ซึ่งทูลพวกนี้ออกแบบสำหรับการวิเคราะห์เซิร์ฟเวอร์ สำหรับค้นหาและจัดเก็บข้อมูล และยังพบไฟล์ sshd ที่ปรับแต่งให้มีแบคดอร์อีกด้วย ซึ่งถูกใช้แทนที่ไฟล์ตั้งต้นและอาจที่จะได้รับสิทธิ์ด้วย ‘master password’

“Crouching Yeti เป็นกลุ่มผู้ร้ายไซเบอร์ที่มีชื่อเสียงร้ายกาจที่ใช้ภาษารัสเซียที่ออกอาละวาดมาหลายปีแล้ว และยัง

ประสบความสำเร็จเรื่อยมาในการเข้าโจมตีเป้าหมายธุรกิจด้านอุตสาหกรรมด้วยเทคนิคการโจมตีแบบ watering hole ที่มักเลือกใช้ และยังค้นพบด้วยว่ากลุ่มนี้เจาะเข้าเซิร์ฟเวอร์ไม่เพียงแต่เพื่อจะแฝงตัวเข้าไปแพร่กระจายเชื้อมัลแวร์เท่านั้น แต่ยังเพื่อคอยสแกนข้อมูลต่อไปอีกด้วย และใช้ทูลแบบโอเพ่นซอร์สที่ทำให้ตามจับตัวได้ยากขึ้นอีกด้วย” วลาดิเมียร์ แดชเชนโก หัวน้ากลุ่มวิจัยช่องโหว่ (Vulnerability Research Group) ประจำ ICS CERT แคสเปอร์สกี้ แลป

“กิจกรรมของกลุ่มนี้ มีอาทิ สอดส่องลอบเก็บข้อมูล โจรกรรมข้อมูลเพื่อการสอบสิทธิ์ในการเข้าใช้ (authentication data) และสแกนข้อมูลต่างๆ ถูกนำมาใช้เพื่อเปิดฉากการโจมตีต่อไป ความหลากหลายของเซิร์ฟเวอร์ที่ติดเชื้อมัลแวร์ และข้อมูลที่ถูกสแกนเป็นตัวบ่งชี้ว่ามีความเป็นไปได้ที่ว่ามีผู้อยู่เบื้องหลังการปฏิบัติการของกลุ่มนี้” วลาดิเมียร์กล่าวเพิ่มเติม

แคสเปอร์สกี้ แลป แนะนำว่าองค์กรต่างๆ ควรที่จะมีกรอบที่ชัดเจนในการป้องกันตนเองจากการคุกคามทางไซเบอร์ ซึ่งประกอบด้วย โซลูชั่นสำหรับความปลอดภัยโดยเฉพาะ ที่ออกแบบเพื่อป้องกันจากการโจมตีแบบตั้งเป้าหมาย พร้อมด้วยฟีเจอร์การตรวจจับและรับมือกับการคุกคาม รวมทั้งบริการคำแนะนำโดยผู้เชี่ยวชาญ และข้อมูลจำเพาะที่เกี่ยวข้อง แพลตฟอร์มเพื่อต้อต้านการคุกคามแบบตั้งเป้าหมายของแคสเปอร์สกี้ แลป นี้เป็นส่วนหนึ่งของ Kaspersky Threat Management and Defense สามารถตรวจจับการคุกคามได้ตั้งแต่ระยะเริ่มแรก ด้วยการวิเคราะห์กิจกรรมที่น่าสงสัยบนเน็ตเวิร์ก และ Kaspersky EDR ช่วยเพิ่มขีดความสามารถในการตรวจดูเอนด์พอยนท์ การตรวจสอบและการรับมือกับภัยคุกคามแบบออโตเมชั่น สนับสนุนด้วยข้อมูลจำเพาะเกี่ยวกับภัยคุกคามจากทั่วโลก รวมทั้งบริการคำแนะนำจากผู้เชี่ยวชาญของแคสเปอร์สกี้ แลป ที่มีความเชี่ยวชาญประสบการณ์เฉพาะทางในการไล่ล่าและจัดการกับภัยไซเบอร์

ท่านสามารถอ่านข้อมูลเพิ่มเติมเกี่ยวกับ Crouching Yeti ได้จากเว็บไซต์ Kaspersky Lab ICS CERT
https://ics-cert.kaspersky.com/reports/2018/04/23/energetic-bear-crouching-yeti-attacks-on-servers/