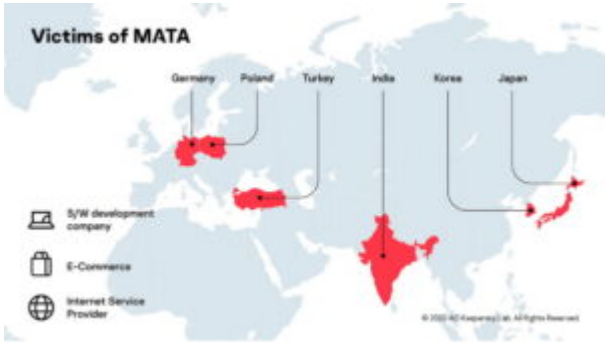
# แคสเปอร์สกี้พบ MATA มัลแวร์ขั้นสูงเชื่อมโยงกลุ่ม Lazarus


นักวิจัยแคสเปอร์สกี้ได้ค้นพบการเข้าโจมตีที่ใช้มัลแวร์เฟรมเวิร์กขั้นสูง ในชื่อ MATA มีเป้าหมายระบบปฏิบัติการ Windows, Linux และ macOS เริ่มใช้มาตั้งแต่ต้นปี 2018 โดยเฟรมเวิร์กนี้พบว่ามีส่วนเชื่อมโยงกับกลุ่มลาซารัส (Lazarus) ชื่อดังที่หนุนหลังโดยเกาหลีเหนือ

ทูลเซ็ตอันตรายที่ใช้ในการทะลวงเป้าหมายหลากหลายแพลตฟอร์มนั้นเป็นสายพันธุ์ที่หายาก ต้องใช้เงินในการลงทุนสูงกับผู้พัฒนา จึงมักใช้งานระยะยาวถึงจะคืนทุน เพิ่มกำไรให้แก่ผู้ก่อภัยคุกคามได้ โดยใช้งานในการโจมตีหลายๆ ครั้งในช่วงเวลาต่างกันไป กรณีที่แคสเปอร์สกี้เป็นผู้ค้นพบนั้นคือ MATA เฟรมเวิร์กสามารถโจมตีเป้าหมายบนสามแพลตฟอร์ม ได้แก่ Windows, Linux และ macOS ได้เลย แสดงว่าผู้ร้ายได้วางแผนการใช้งานไว้หลายวัตถุประสงค์ ตัวเฟรมเวิร์กประกอบขึ้นด้วยคอมโพเน้นท์ อาทิ โหลดเดอร์ (loader) ออร์เคสเตรเตอร์ (orchestrator ทำหน้าที่จัดการและประสานงานระหว่างขั้นตอนเมื่อใดก็ตามที่อุปกรณ์นั้นกลายมาเป็นเหยื่อ) และปลั๊กอิน (plugins)

ข้อมูลจากนักวิจัยแคสเปอร์สกี้ชี้ว่า ชิ้นส่วนแรกที่พบความเกี่ยวโยงกับ MATA ถูกใช้ในช่วงเดือนเมษายน 2018 โดยประมาณ และตั้งแต่นั้นมาผู้ก่อภัยคุกคามเบื้องหลังมัลแวร์เฟรมเวิร์กขั้นสูงตัวนี้ก็รุกหนักเพื่อเจาะเข้าองค์กรทั่วโลก และพบว่าถูกใช้ในการโจมตีอีกหลายครั้ง โดยมีเป้าหมายอยู่ที่การโจรกรรมฐานข้อมูลลูกค้า และเพื่อแพร่กระจายแรนซัมแวร์ ซึ่งเป็นซอฟต์แวร์ที่ออกแบบมาเพื่อบล็อกการเข้าระบบคอมพิวเตอร์จนกว่าจะยอมจ่ายค่าไถ่

จากข้อมูลของแคสเปอร์สกี้ชี้ว่า พบเหยื่อของ MATA ตามที่ต่างๆ ในโปแลนด์ เยอรมนี ตุรกี เกาหลี ญี่ปุ่น และอิน

เดีย แปลว่าผู้ก่อภัยคุกคามมิได้เน้นพื้นที่ใดเป็นพิเศษ และพบว่าลาซารัสเข้ารุกล้ำระบบคอมพิวเตอร์ของอุตสาหกรรมหลากหลายประเภท แม้แต่บริษัทที่ทำด้านพัฒนาซอฟต์แวร์ บริษัทอีคอมเมิร์ซ และผู้ให้บริการอินเทอร์เน็ตก็โดนด้วยเช่นกัน

นักวิจัยจากแคสเปอร์สกี้สามารถตรวจพบการเชื่อมโยง MATA ไปยังกลุ่มลาซารัสได้ แม้ตามที่รู้กันว่าการปฏิบัติงานของกลุ่มจะมีความซับซ้อนอย่างมาก โยงใยกับเกาหลีเหนือ มีความเกี่ยวข้องกับปฏิบัติการจารกรรมไซเบอร์และการโจมตีใดๆ ที่เป็นเป้าหมายทางการเงิน มีนักวิจัยจำนวนหนึ่งรวมทั้งจากแคสเปอร์สกี้ ได้เคยออกรายงานเกี่ยวกับกลุ่มนี้ว่ามีเป้าหมายที่ธนาคารและสถาบันองค์กรการเงินขนาดใหญ่ รวมทั้งการโจมตี ATMDtrack และแคมเปญ AppleJeus อีกด้วย ชุดการโจมตีล่าสุดชี้ว่าผู้ก่อภัยคุกคามยังคงรูปแบบการปฏิบัติการในแนวนี้อย่างต่อเนื่อง

นายซองซู ปาร์ค นักวิจัยอาวุโสของแคสเปอร์สกี้ กล่าวว่า “ชุดการโจมตีนี้แสดงว่ากลุ่มลาซารัสเต็มใจที่จะจ่ายเงินลงทุนกับการพัฒนาทูลเซ็ตนี้ขึ้นมา เพื่อเปิดทางรุกเข้าสู่กลุ่มเป้าหมายให้ได้ โดยเฉพาะอย่างยิ่งในการตามล่าเงินและข้อมูล ยิ่งไปกว่านั้น การเขียนมัลแวร์สำหรับ Linux และ macOS ชี้ว่าผู้ร้ายคิดว่าตนเองมีทูลมากมายเพื่อใช้โจมตี Windows ซึ่งคนส่วนใหญ่นิยมใช้ วิธีการนี้พบโดยมากในกลุ่ม APT ที่มีความเก๋าในตัว เราคาดว่า MATA จะมีพัฒนาการต่อยอดอีกมาก และขอแนะนำองค์กรต่างๆ ให้ใส่ใจให้ความสำคัญกับความปลอดภัยของข้อมูล ซึ่งเป็นทรัพยากรสำคัญอันมีค่าที่จะรับผลกระทบ”

อ่านเกี่ยวกับ MATA ได้จาก Securelist.com

MATA: Multi-platform targeted malware framework

คำแนะนำจากนักวิจัยของแคสเปอร์สกี้เพื่อหลีกเลี่ยงการตกเป็นเหยื่อของมัลแวร์แบบมัลติแพลตฟอร์มดังต่อไปนี้:

- ติดตั้งผลิตภัณฑ์เพื่อความปลอดภัยไซเบอร์สำหรับเครื่องเอ็นด์พอยต์บนระบบ Windows, Linux และ MacOS อาทิ Kaspersky Endpoint Security for Busines เพื่อป้องกันให้พ้นภัยไซเบอร์ทั้งที่มีอยู่และที่จะมาใหม่ และยังให้ฟีเจอร์ในการควบคุมดูแลด้านความปลอดภัยไซเบอร์ของแต่ละระบบปฏิบัติการได้อีก
- จัดหาแหล่งข้อมูลวิเคราะห์เชิงลึกให้แก่ทีมงาน SOC (Threat Intelligence) เพื่อช่วยให้มีข้อมูลที่ทันสมัย รู้จักทูล เทคนิคและกลเม็ดใหม่ๆ ที่ผู้ก่อภัยคุกคามนำมาใช้โจมตี
- สำรองข้อมูลธุรกิจอยู่เสมอในที่ๆ สามารถเรียกใช้งานได้ทันท่วงที เพื่อการกู้คืนข้อมูลที่อาจจะเสียหาย สูญหาย หรือถูกล็อกไว้กรณีถูกเรียกค่าไถ่โดยแรนซัมแวร์ เป็นต้น