มาแล้ว! มัลแวร์จารกรรมข้อมูลภาคอุตสาหกรรม แคสเปอร์สกี้พบทูลเซ็ตใหม่อำพรางตัวได้นาน

นักวิจัยของแคสเปอร์สกี้ได้ค้นพบชุดของการโจมตีที่มีเป้าหมายเป็นภาคอุตสาหกรรมย้อนหลังไปถึงปี 2018 ซึ่งหาได้ยากมากในโลกของภัยคุกคามต่อเนื่องขั้นสูง (APT) ที่ผู้ก่อภัยคุกคามมักเน้นโจมตีหน่วยงานการทูตและผู้มีบทบาททางการเมืองระดับสูง ชุดเครื่องมือที่ใช้ซึ่งเดิมชื่อ MT3 ตั้งโดยผู้เขียนมัลแวร์ ได้รับการขนานนามใหม่จากแคสเปอร์สกี้ว่า“MontysThree” ใช้เทคนิคต่างๆ เพื่อหลบเลี่ยงการตรวจจับ รวมถึงการโฮสต์การสื่อสารกับเซิร์ฟเวอร์ควบคุมบนบริการคลาวด์สาธารณะ และการซ่อนโมดูลที่เป็นอันตรายหลักโดยใช้วิธีอำพรางข้อมูล (Steganography)

หน่วยงานของรัฐบาล หน่วยงานการทูต และผู้ให้บริการโทรคมนาคมมักจะเป็นเป้าหมายของกลุ่ม APT เนื่องจากบุคลากรและสถาบันเหล่านี้มักมีข้อมูลที่เป็นความลับและมีความอ่อนไหวทางการเมืองเป็นจำนวนมาก ที่พบยากกว่าคือการเป้าหมายแคมเปญจารกรรมที่เป็นหน่วยงานภาคอุตสาหกรรม แต่เช่นเดียวกับการโจมตีวงการอื่นๆ คือสามารถส่งผลร้ายแรงต่อธุรกิจได้ ด้วยเหตุนี้เมื่อสังเกตเห็นกิจกรรมของ MontysThree นักวิจัยของแคสเปอร์สกี้จึงบันทึกกิจกรรมร้ายได้อย่างรวดเร็ว

ในการดำเนินการจารกรรม MontysThree ใช้โปรแกรมมัลแวร์ซึ่งประกอบด้วยโมดูลสี่โมดูล ตัวโหลดแรกแพร่กระจายโดยใช้ไฟล์ RAR SFX (ไฟล์อาร์ไคฟ์ที่แยกออกมาเอง) ซึ่งมีรายชื่อผู้ติดต่อของพนักงาน เอกสารทางเทคนิค และผลวิเคราะห์ทางการแพทย์ เพื่อหลอกให้พนักงานดาวน์โหลดไฟล์ ซึ่งเป็นเทคนิคสเปียร์ฟิชชิงทั่วไป ตัวโหลดมีหน้าที่หลักในการทำให้ไม่สามารถตรวจพบมัลแวร์ในระบบได้ ในการทำเช่นนี้จะใช้เทคนิคที่เรียกว่าการอำพรางข้อ

มูล (Steganography)

ผู้ก่อภัยคุกคามใช้การอำพรางข้อมูลเพื่อซ่อนการแลกเปลี่ยนข้อมูล ในกรณีของ MontysThree เพย์โหลดที่เป็นอันตรายหลักจะปลอมเป็นไฟล์บิตแมป (เป็นรูปแบบสำหรับจัดเก็บภาพดิจิทัล) หากป้อนคำสั่งที่ถูกต้อง ตัวโหลดจะใช้อัลกอริทึมที่สร้างขึ้นเองเพื่อถอดรหัสเนื้อหาจากอาร์เรย์พิกเซล และเรียกใช้เพย์โหลดที่เป็นอันตราย

เพย์โหลดตัวหลักที่เป็นอันตรายจะใช้เทคนิคการเข้ารหัสหลายอย่างเพื่อหลบเลี่ยงการตรวจจับ ได้แก่ การใช้อัลกอริทึม RSA เพื่อเข้ารหัสการสื่อสารกับเซิร์ฟเวอร์ควบคุม และถอดรหัส “งาน” หลักที่ได้รับมอบหมายจากมัลแวร์ ซึ่งรวมถึงการค้นหาเอกสารที่มีนามสกุลเฉพาะและในไดเรกทอรีของบริษัท MontysThree ถูกออกแบบมาเพื่อพุ่งเป้าหมายไปที่เอกสาร Microsoft และ Adobe Acrobat โดยเฉพาะ นอกจากนี้ยังสามารถจับภาพหน้าจอและ “ลายนิ้วมือ” (เช่น รวบรวมข้อมูลเกี่ยวกับการตั้งค่าเครือข่าย ชื่อโฮสต์ ฯลฯ) เพื่อดูว่าน่าสนใจหรือไม่

ข้อมูลที่รวบรวมได้และการสื่อสารกับเซิร์ฟเวอร์ควบคุมจะถูกโฮสต์บนบริการคลาวด์สาธารณะ เช่น Google, Microsoft และ Dropbox ทำให้ตรวจทราฟฟิกการสื่อสารได้ยากว่าเป็นอันตรายหรือไม่ และเนื่องจากไม่มีโปรแกรมป้องกันไวรัสที่บล็อกบริการเหล่านี้ จึงทำให้เซิร์ฟเวอร์ควบคุมสามารถดำเนินการคำสั่งได้โดยไม่ถูกขัดจังหวะ

MontysThree ยังใช้วิธีง่ายๆ เพื่อให้อยู่ของระบบที่ติดไวรัสได้นาน คือใช้ตัวปรับแต่งสำหรับ Windows Quick Launch ทุกครั้งที่ผู้ใช้เรียกใช้งานแอปพลิเคชันอย่างเบราว์เซอร์ โดยใช้แถบเครื่องมือ Quick Launch ก็เป็นการเรียกใช้โมดูลเริ่มต้นของมัลแวร์ด้วยตัวเองโดยไม่ได้ตั้งใจ

ทั้งนี้แคสเปอร์สกี้ไม่พบความคล้ายคลึงกันในโค้ดที่เป็นอันตรายหรือโครงสร้างพื้นฐานของ MontysThree กับกลุ่ม APT กลุ่มอื่นใดก่อนหน้านี้

นายเดนิส เลเกโซ นักวิจัยความปลอดภัยอาวุโส ทีมวิเคราะห์และวิจัยของแคสเปอร์สกี้ กล่าวว่า “MontysThree มีลักษณะที่น่าสนใจเพราะมีการกำหนดเป้าหมายไปที่ภาคอุตสาหกรรม และเป็นการผสมผสาน TTP ที่ซับซ้อนและขาดทักษะ โดยทั่วไปความซับซ้อนจะแตกต่างกันไปในแต่ละโมดูล แต่ไม่สามารถเปรียบเทียบกับระดับที่ใช้โดย APT ขั้นสูงสุดได้ อย่างไรก็ตาม ผู้ก่อภัยคุกคามใช้มาตรฐานการเข้ารหัสที่แข็งแกร่งและมีการตัดสินใจเชิงเทคโนโลยีบางอย่าง รวมถึงวิธีการอำพรางที่กำหนดเอง ที่สำคัญที่สุดคือชัดเจนว่าผู้โจมตีได้ใช้ความพยายามอย่างมากในการพัฒนาชุดเครื่องมือ MontysThree ซึ่งชี้ถึงความมุ่งมั่นในจุดมุ่งหมายและไม่ใช่แคมเปญที่มีอายุสั้น”

ท่านสามารถอ่านข้อมูลเพิ่มเติมเรื่อง MontysThree ได้ที่ https://securelist.com/montysthree-industrial-espionage/98972/ รายละเอียดเกี่ยวกับตัวบ่งชี้การโจมตีของกลุ่มนี้ รวมถึงการแฮชไฟล์ สามารถเข้าดูได้ที่ Kaspersky Threat Intelligence Portal https://opentip.kaspersky.com/

แคสเปอร์สกี้ขอแนะนำวิธีการเพื่อป้องกันภัยคุกคามอย่าง MontysThree ดังนี้

• จัดให้ทีม SOC สามารถเข้าถึงข้อมูลภัยคุกคามล่าสุด Kaspersky Threat Intelligence Portal เป็นจุดบริการที่ผู้ใช้งานสามารถเข้าถึงสิ่งที่ต้องการได้ทั้งหมด (Single point of access) ซึ่งให้ข้อมูลการโจมตีทางไซเบอร์และข้อมูลเชิงลึกที่แคสเปอร์สกี้รวบรวมมานานกว่า 20 ปี

• สำหรับการตรวจจับ การตรวจสอบและการแก้ไขเหตุการณ์ระดับเอ็นด์พอยต์อย่างทันท่วงที แนะนำให้ใช้โซลูชั่น EDR เช่น Kaspersky Endpoint Detection and Response

• จัดให้พนักงานได้รับการฝึกอบรมด้านสุขอนามัยความปลอดภัยทางไซเบอร์ขั้นพื้นฐาน เนื่องจากการโจมตีแบบกำหนดเป้าหมายจำนวนมากเริ่มต้นด้วยฟิชชิงหรือเทคนิควิศวกรรมสังคมอื่น ๆ

• ใช้ผลิตภัณฑ์รักษาความปลอดภัยเอ็นด์พอยต์ที่มีประสิทธิภาพซึ่งสามารถตรวจจับการใช้เฟิร์มแวร์ เช่น Kaspersky Endpoint Security for Business

• อัปเดตเฟิร์มแวร์ UEFI เป็นประจำและซื้อเฟิร์มแวร์จากผู้ขายที่เชื่อถือได้เท่านั้น