วันที่ 4 กรกฎาคม 2568

แรนซัมแวร์ DEVMAN ตัวใหม่จาก DragonForce พุ่งเป้าโจมตีผู้ใช้ Windows 10 และ 11

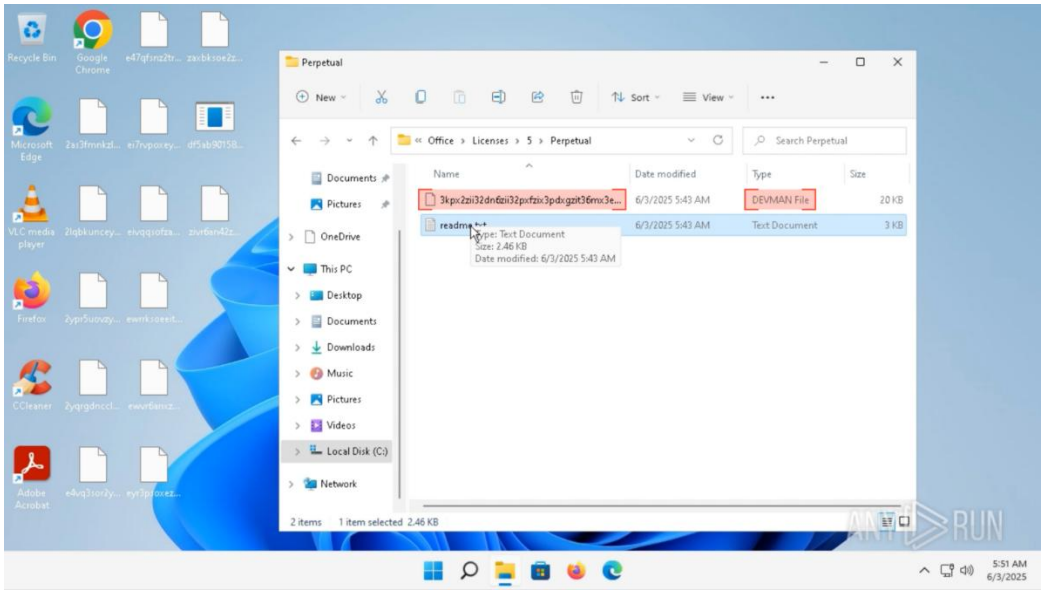
โลกของภัยคุกคามไซเบอร์ได้ต้อนรับแรนซัมแวร์สายพันธุ์ใหม่ที่ถูกขนานนามว่า DEVMAN ซึ่งแสดงให้เห็นถึงที่มาที่ซับซ้อน และเชื่อมโยงกับตระกูลมัลแวร์ชื่อดังอย่าง DragonForce และ Conti

DEVMAN ถูกสร้างขึ้นบนโค้ดพื้นฐานของทั้งสองตระกูลนี้ แต่ก็มีการเพิ่มเติมเอกลักษณ์เฉพาะตัวเข้ามา เช่น การตั้งนามสกุลไฟล์ที่ถูกเข้ารหัสเป็น .DEVMAN และมีพฤติกรรมการทำงานบางอย่างที่แตกต่างออกไป แต่ก็ยังคงลักษณะสำคัญเหมือนกับรุ่นก่อนหน้า

มัลแวร์สายพันธุ์ลูกผสมนี้ ซึ่งเพิ่งถูกนำมาวิเคราะห์ในสภาพแวดล้อมจำลองเพื่อความปลอดภัยของ ANY.RUN มีเป้าหมายโจมตีระบบ Windows 10 และ 11 โดยจะเข้ารหัสไฟล์อย่างรวดเร็วและพยายามแพร่กระจายไปยังเครื่องอื่นในเครือข่ายผ่านทาง SMB

ภัยคุกคามลูกผสมที่แตกตัวจากโค้ดของ DragonForce

อย่างไรก็ตาม การโจมตีของมันดูเหมือนจะยังอยู่ในช่วงทดลอง เนื่องจากมีข้อบกพร่องร้ายแรง เช่น การเข้ารหัสไฟล์เรียกค่าไถ่ของตัวเอง ซึ่งทำให้ประสิทธิภาพของมันลดลง แม้ว่าโปรแกรมแอนตี้ไวรัสส่วนใหญ่จะตรวจจับ DEVMAN เป็น DragonForce หรือ Conti แต่การวิเคราะห์ในเชิงลึกเผยให้เห็นว่า DEVMAN มีโครงสร้างพื้นฐานแยกเป็นของตัวเอง ซึ่งรวมถึง เว็บไซต์สำหรับเผยแพร่ข้อมูลที่ขโมยมาโดยเฉพาะ (Dedicated Leak Site - DLS) ในชื่อ “Devman’s Place” ที่อ้างว่าเกือบ 40 ราย ส่วนใหญ่อยู่ในเอเชียและแอฟริก



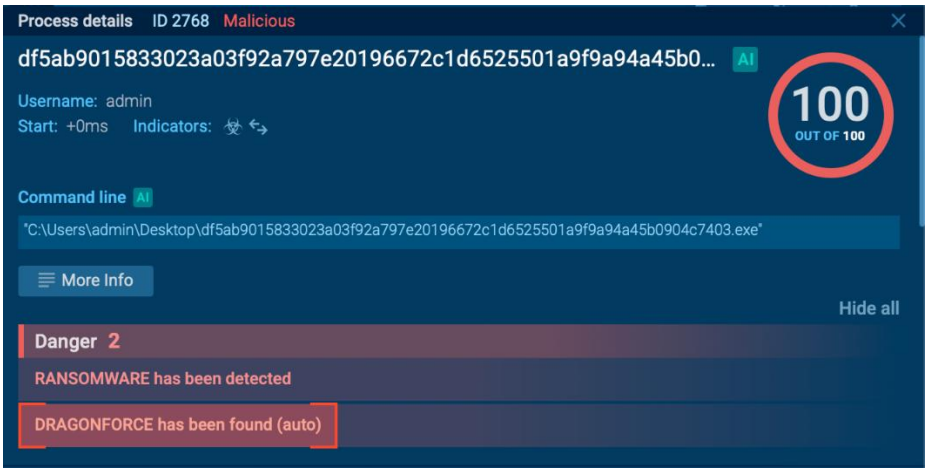
พฤติกรรมของ DEVMAN ยังแสดงให้เห็นถึงความไม่สอดคล้องกันที่น่าสนใจในระบบปฏิบัติการและสภาพแวดล้อมการทำงานที่แตกต่างกัน บน Windows 10 แรนซัมแวร์ตัวนี้สามารถเปลี่ยนภาพพื้นหลังหน้าจอเดสก์ท็อปเพื่อแสดงข้อความเรียกค่าไถ่ได้สำเร็จ แต่กลับล้มเหลวในการทำแบบเดียวกันบน Windows 11 ด้วยเหตุผลที่ยังไม่แน่ชัด

กระบวนการเข้ารหัสของมันนั้นนับว่าดุดันพอสมควร โดยมีให้เลือกถึงสามโหมด คือ แบบเต็ม (full), แบบเฉพาะส่วนหัวไฟล์ (header-only), และแบบกำหนดเอง (custom) ซึ่งเปิดโอกาสให้ผู้โจมตีเลือกระหว่างความเร็วในการเข้ารหัสกับความเสียหายที่ต้องการสร้าง

ความท้าทายในการปฏิบัติการและข้อบกพร่อง

ข้อบกพร่องที่น่าทึ่งในการสร้างมัลแวร์ คือ การที่มันเข้ารหัสไฟล์เรียกค่าไถ่ของตัวเอง ทำให้ไฟล์นั้นไม่สามารถอ่านได้ และเป็นการตัดช่องทางการสื่อสารเพื่อแจ้งขั้นตอนการจ่ายเงินไปโดยปริยาย ความผิดพลาดครั้งใหญ่นี้ ประกอบกับการเปลี่ยนชื่อไฟล์ที่คาดเดาได้ (เช่น ไฟล์เรียกค่าไถ่จะถูกเปลี่ยนชื่อเป็น “e47qfsnz2trbkhnt.devman” เสมอ) ชี้ให้เห็นว่า DEVMAN อาจยังอยู่ในขั้นตอนการทดสอบมากกว่าที่จะเป็นภัยคุกคามที่พร้อมใช้งานจริง

นอกจากนี้ แรนซัมแวร์ตัวนี้ยังทำงานแบบออฟไลน์เป็นหลัก โดยไม่พบการสื่อสารไปยังเซิร์ฟเวอร์ควบคุมภายนอก (C2) แต่จะอาศัยการตรวจสอบหาช่องทางผ่านโปรโตคอล SMB เพื่อแพร่กระจายตัวเองภายในเครือข่ายแทน



การที่มันใช้ **Windows Restart Manager** เพื่อ Bypass ไฟล์ที่กำลังถูกใช้งานอยู่ และใช้ค่าตายตัว (**Mutex**) อย่าง “hsfjuukjzloqu28oajh727190” เพื่อควบคุมการทำงาน ก็ยิ่งตอกย้ำความเชื่อมโยงกับเทคนิคและขั้นตอนการโจมตี (**TTPs**) ที่มาจาก Conti

มัลแวร์ตัวอย่างนี้ยังแสดงให้เห็นถึงกลไกการคงอยู่รอดในระบบและการหลบหลีกการตรวจจับในระดับพื้นฐาน เช่น การลบรีจิสทรีคีย์ (registry keys) หลังจากการแก้ไข และการตรวจสอบหาไฟล์สำรองของระบบ (Shadow Copies) เพื่อขัดขวางการกู้คืนระบบ

แม้ว่าความซับซ้อนของมันจะไม่ได้ล้ำสมัยนัก แต่ลูกเล่นแปลกๆ เหล่านี้ก็ให้ข้อมูลเชิงลึกที่มีค่าเกี่ยวกับระบบนิเวศของแรนซัมแวร์ในรูปแบบบริการ (**RaaS**) ที่กำลังพัฒนาอยู่ ซึ่งเหล่าผู้ร่วมขบวนการจะนำเฟรมเวิร์กที่มีอยู่แล้วอย่าง DragonForce มาปรับแต่งเพื่อสร้างสายพันธุ์ย่อยของตัวเองขึ้นมา

การปรากฏตัวของ DEVMAN เน้นให้เห็นถึงธรรมชาติของการพัฒนาแรนซัมแวร์ยุคใหม่ที่กระจัดกระจาย ซึ่งการนำโค้ดกลับมาใช้ซ้ำและการตั้งค่าที่ผิดพลาดมักทำให้การระบุตัวตนผู้สร้างทำได้ยากขึ้น

จากรายงาน ทีมรักษาความปลอดภัยที่ใช้เครื่องมืออย่าง Interactive Sandbox ของ ANY.RUN จะสามารถมองเห็นภัยคุกคามประเภทนี้ได้แบบเรียลไทม์ ทำให้สามารถแกะรอยพฤติกรรม ดึงข้อมูลบ่งชี้การบุกรุก (**IOCs**) และปรับปรุงกระบวนการรับมือให้ดียิ่งขึ้นได้ แม้ว่ามัลแวร์จะทำงานผิดพลาดไปบ้างก็ตาม

Indicators of Compromise (IOCs)

Type	Value
MD5	e84270afa3030b48dc9e0c53a35c65aa
SHA256 (Sample 1)	df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403
SHA256 (Sample 2)	018494565257ef2b6a4e68f1c3e7573b87fc53bd5828c9c5127f31d37ea964f8
File Name (Mutex)	hsfjuukjzloqu28oajh727190
File Name (Note)	e47qfsnz2trbkhnt.devman

DEVMAN เป็นแรนซัมแวร์ที่น่าสนใจ เนื่องจากเป็นลูกผสมของตระกูลมัลแวร์ชื่อดัง แม้จะมีข้อบกพร่องในปัจจุบัน แต่ก็เป็นสัญญาณเตือนถึงการพัฒนาอย่างต่อเนื่องในวงการ RaaS ซึ่งอาชญากรไซเบอร์นำโค้ดที่มีอยู่แล้วมาปรับแต่งเพื่อสร้างภัยคุกคามใหม่ๆ การติดตามและวิเคราะห์พฤติกรรมของแรนซัมแวร์เหล่านี้จึงเป็นสิ่งสำคัญในการรับมือกับภัยคุกคามในอนาคต

ข้อมูลอ้างอิง

July 1, 2025 By Aman Mishra

- https://gbhackers.com/new-devman-ransomware-by-dragonforce/