เอกสารการแจ้งเตือนการป้องกันการโจมตี
การหลีกเลี่ยงการตรวจสอบสิทธิ์หลายปัจจัย (MFA)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี พบการป้องกันการโจมตีการหลีกเลี่ยงการตรวจสอบสิทธิ์หลายปัจจัย (MFA)

Multi-Factor Authentication (MFA) เป็นกระบวนการยืนยันตัวตนที่ต้องใช้ปัจจัยมากกว่าหนึ่งรายการในการตรวจสอบผู้ใช้ก่อนอนุญาตให้เข้าถึงระบบ [1] สามารถแบ่งปัจจัยที่ใช้ใน MFA ได้ดังนี้ [2]

- Knowledge Factor เช่น รหัสผ่าน
- Possession Factor เช่น รหัสผ่านครั้งเดียว One-Time Passwords (OTP)
- Inherence Factor เช่น ลายนิ้วมือหรือการสแกนใบหน้า
- Location-based Factor เช่น ตำแหน่ง หรือเครือข่ายที่ใช้งาน
- Behaviour-based Factor การวิเคราะห์พฤติกรรมผู้ใช้ เช่น รูปแบบการพิมพ์

การโจมตี MFA Bypass คือการทำให้ผู้โจมตีสามารถหลบเลี่ยงการตรวจสอบสิทธิ์ โดยใช้วิธีต่าง ๆ ดังต่อไปนี้ [3]

- การโจมตีแบบ Man-in-the-Middle (MiTM) คือการที่ผู้โจมตีดักจับข้อมูลระหว่างผู้ใช้ และระบบเพื่อขโมยข้อมูลรหัสผ่าน และ MFA
- การโจมตีแบบ MFA Fatigue Attack คือการที่ผู้โจมตีใช้เทคนิคในการส่งการแจ้งเตือน MFA ซ้ำ ๆ จนเหยื่อยอมอนุมัติคำขอด้วยความสับสน
- การโจมตีแบบ Session Hijacking การโจมตีแบบ Session Hijacking คือการขโมยคุกกี้เซสชันเพื่อนำไปใช้ในการล็อกอิน
- การโจมตีแบบ Token Theft คือการขโมยโทเค็น MFA หรือรหัสยืนยันที่ใช้ในกรณีที่ผู้ใช้ลืมรหัสผ่าน

การป้องกัน MFA Bypass มีดังนี้

- การใช้ MFA ที่ป้องกันฟิชชิ่ง เช่น การใช้ FIDO2 Security Keys
- การใช้วิธีการตรวจสอบที่เข้มงวด เช่น โทเค็นฮาร์ดแวร์หรือข้อมูลชีวมิติ
- การจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบ เพื่อป้องกันการโจมตีแบบ Fatigue
- การฝึกอบรมผู้ใช้ ให้ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการจัดการ MFA
- การบันทึกและติดตามการเข้าสู่ระบบ ใช้ระบบ SIEM เพื่อตรวจสอบระบบที่ผิดปกติช่วยในการตรวจจับการโจมตี

ทั้งนี้ สามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Cod

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://www.csa.gov.sg/alerts-advisories/Advisories/2024/ad-2024-020
2. https://jumpcloud.com/blog/different-factors-of-multi-factor-authentication-mfa
3. https://www.beyondtrust.com/resources/glossary/mfa-fatigue-attack