KHONKAEN UNIVERSITY

Real-Time OTP Phishing Demonstration

การพัฒนาและสาธิตระบบดักจับรหัส OTP แบบเรียลไทม์

หลักการและเหตุผล

ปัจจุบันการโจมตีแบบ Phishing ได้พัฒนาเป็นการโจมตีแบบ Real-time ที่สามารถข้ามระบบความปลอดภัยอย่าง OTP ได้ โดยมิจฉาชีพมักสร้างหน้า Login ปลอมเลียนแบบบริการยอดนิยม เช่น TrueID เพื่อหลอกขโมยข้อมูลผู้ใช้

โครงงานนี้จึงศึกษากระบวนการโต้ตอบระหว่างผู้โจมตีและเหยื่อแบบเรียลไทม์ เพื่อแสดงให้เห็นว่าแม้มีระบบ OTP หากผู้โจมตีควบคุมหน้าจอเหยื่อได้ ก็สามารถขโมยข้อมูลได้ทันที ผลการศึกษาจะช่วยสร้างความตระหนักและแนวทางสังเกตความผิดปกติให้กับผู้ใช้งาน

สรุปผลการดำเนินงาน

จากการศึกษาพบว่า การโจมตีแบบ Real-time OTP Phishing เป็นเทคนิคที่มีความซับซ้อนและสามารถหลีกเลี่ยงระบบความปลอดภัยแบบ OTP ได้ หากผู้ใช้งานถูกหลอกให้กรอกข้อมูลผ่านเว็บไซต์ปลอมที่มีลักษณะคล้ายกับเว็บไซต์จริง

ในการทดลองจำลองกระบวนการโจมตีผู้โจมตีสามารถนำข้อมูล Username, Password และรหัส OTP ที่ผู้ใช้กรอกบนเว็บไซต์ปลอมไปใช้เข้าสู่ระบบจริงได้ทันทีในขณะที่เซสชันยังคงใช้งานอยู่ ส่งผลให้การโจมตีประสบความสำเร็จแม้ว่าระบบจะมีการยืนยันตัวตนแบบสองขั้นตอนก็ตาม

วัตถุประสงค์

1. จำลองการโจมตีแบบ Real-time OTP Phishing ผ่านหน้าเว็บเลียนแบบของ TrueID
2. ศึกษาช่องโหว่ของระบบยืนยันตัวตนสองชั้น (2FA) และการข้ามรหัส OTP
3. ทดสอบการทำงานระหว่างหน้าเว็บปลอมกับระบบควบคุมของผู้โจมตีแบบ Real-time
4. สรุปแนวทางป้องกันและสร้างความตระหนักด้านความปลอดภัยให้ผู้ใช้ TrueID

วิธีการใช้งาน

1. ผู้ใช้งานกรอกข้อมูลบนเว็บไซต์ปลอม
2. ข้อมูลที่ได้รับถูกนำไปใช้เข้าสู่ระบบเว็บไซต์จริง
3. ระบบของเว็บไซต์จริงส่งรหัส OTP ให้ผู้ใช้งาน
4. ผู้ใช้งานกรอกรหัส OTP บนเว็บไซต์ปลอม
5. รหัส OTP ถูกนำไปยืนยันตัวตนบนเว็บไซต์จริง
6. ผู้ใช้งานถูก redirect ไปยังเว็บไซต์จริง
7. การโจมตีประสบความสำเร็จ

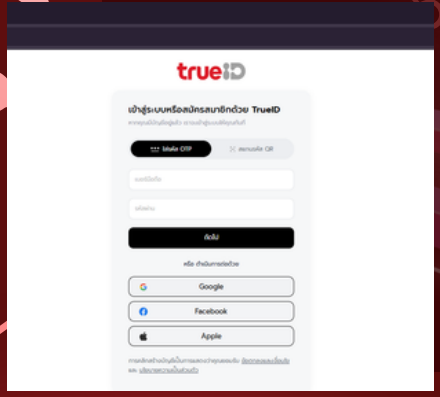
ขอบเขตงาน

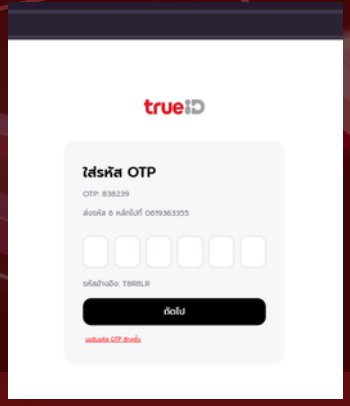
โครงงานนี้มุ่งศึกษาแนวคิดของการโจมตีแบบ Real-time OTP Phishing โดยจำลองหน้าเข้าสู่ระบบที่มีลักษณะคล้ายกับ TrueID เพื่อสาธิตกระบวนการหลอกล่อผู้ใช้ให้กรอก Username, Password และ OTP ผ่านเว็บไซต์ปลอม จากนั้นนำข้อมูลไปใช้เข้าสู่ระบบเว็บไซต์จริงในเวลาเดียวกัน เพื่อแสดงให้เห็นว่าระบบ OTP หรือ 2FA ยังสามารถถูกโจมตีได้หากผู้ใช้กรอกข้อมูลผ่านเว็บไซต์ที่ไม่น่าเชื่อถือ

เอกสารอ้างอิง

https://www.ijtsrd.com/papers/ijtsrd75061.pdf
https://www.usenix.org/system/files/sec21-ulqinaku.pdf

เครื่องมือที่ใช้พัฒนา





เสนอ
ศ. ดร.จักรชัย โสอินทร์
อ. ดร.ชาติชาย ปุณริบูรณ์
ผศ. ดร.สาธิต กระเวนกิจ

SC362006
Information& Communication Technology Security
หลักสูตร เทคโนโลยีสารสนเทศ
คณะ วิทยาลัยการคอมพิวเตอร์
พ.ศ.2569

สมาชิกในกลุ่ม

นายสามารถ มงคลฤกษ์	663380498-4
นายปวริศ สายโยค	663380635-0
นางสาวกานติมา สุคำภา	673380204-8
นางสาวจริญญา บุญแสน	673380205-6
นางสาวธีร์จุฑา ศรีทะบาล	673380221-8
นางสาวณัฐชนน จันทร์โสม	673380215-3
นายภูเบศ น้อยวัน	673380504-6