การตระหนักรู้เท่าทันภัยคุกคามจากการใช้อินเทอร์เน็ต: กรณีจำลองการโจมตีด้วยการคาดเดารหัสผ่าน (Password Attack)

Awareness of Threat Internet: A case of Password Attack

สุภาพร พันธ์ยา[1], คริชณะ ฉิมมณี[2] และ ราชศักดิ์ สมยานนทนากุล[3]
Supaporn Punya, Krishana Chimmanee and Rachasak Somyanonthanakul
Corresponding author, E-mail : ratchasak.s@rsu.ac.th

Received : *April 15, 2023*
Revised : *June 16, 2023*
Accepted : *June 25, 2023*

บทคัดย่อ

การใช้อินเทอร์เน็ตมีบทบาทในชีวิตประจำวันเป็นอย่างมาก ทั้งในด้านการติดต่อสื่อสาร การศึกษา และการดำเนินธุรกิจ ผู้คนเริ่มเข้าถึงการใช้อินเทอร์เน็ต (Internet) เพิ่มขึ้นในทุกปี และเนื่องด้วยสถานการณ์โควิด-19 ทำให้บริษัทส่วนใหญ่ในหลาย ๆ แห่ง มีนโยบายให้ทำงานที่บ้าน หรือสถานศึกษามีการจัดการเรียนการสอนออนไลน์มากขึ้น เราจึงมีการใช้อินเทอร์เน็ตเพิ่มขึ้น ไม่ว่าจะเป็นการใช้ไวฟาย (WiFi) หรือใช้ฮอตสปอตส่วนบุคคลในการกระจายสัญญาณ อีกทั้งยังมีบริการให้ใช้อินเทอร์เน็ตฟรีตามสถานที่ต่าง ๆ เช่น ร้านกาแฟ โรงเรียน หรือร้านอาหาร การใช้อินเทอร์เน็ตในที่สาธารณะค่อนข้างเสี่ยงต่อการถูกโจมตีหรือขโมยข้อมูลส่วนตัว ซึ่งรูปแบบการโจมตีมีหลากหลายประเภท ในบทความนี้เป็นการจำลองการโจมตีด้วยรูปแบบคาดเดารหัสผ่าน (Password Attack) เพื่อแสดงให้เห็นว่า หากมีการตั้งรหัสผ่านที่ง่าย ก็เสี่ยงต่อการถูกโจมตีได้ง่ายเช่นกัน ซึ่งหลังจากที่ได้ทำการโจมตีรหัสผ่านของผู้ที่ใช้ฮอตสปอตส่วนบุคคลในการกระจายสัญญาณไวฟาย โดยใช้เครื่องมือที่ชื่อว่า แอร์แคร็ก (Aircrack-ng) และ เฟิร์นไวฟาย แคร็กเกอร์ (Fern WiFi Cracker) ในการโจมตี พบว่า ทั้ง 2 เครื่องมือสามารถถอดรหัสผ่านออกมาได้ไม่ถึง 1 นาที จากผลการทดสอบ ผู้ใช้ควรตั้งรหัสผ่านให้ยากต่อการคาดเดา ไม่ว่าจะเป็นการตั้งรหัสผ่านเข้าใช้งานเว็บไซต์ต่าง ๆ หรือ ใช้ฮอตสปอตส่วนบุคคลในการกระจายสัญญาณไวฟาย เพื่อเพิ่มความยากต่อการถูกโจมตี

ดังนั้น บทความนี้เป็นการนำเสนอรูปแบบภัยคุกคามที่เกิดขึ้น เพื่อยกระดับความตระหนักรู้ทันภัยคุกคามทางไซเบอร์ในรูปแบบอื่น ๆ และหากมีการป้องกันที่ดี ก็ย่อมช่วยให้เราใช้งานได้อย่างปลอดภัยมากขึ้น

คำสำคัญ: โจมตีรหัสผ่าน, การตระหนักรู้, ภัยคุกคาม

Abstract

The internet plays a significant role in our daily lives, particularly in communication, education, and business operations. People are increasingly accessing the internet each year, and due to the COVID-19 situation, many companies have implemented work-from-home policies, and educational institutions have shifted to online learning. Consequently, our internet usage has increased, whether through Wi-Fi or personal

[1,2,3] วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต
College of Digital Innovation Technology Rangsit University

hotspots for signal distribution. Additionally, there are various places that offer free internet access, such as coffee shops, schools, or restaurants. However, using the internet in public places poses risks of being attacked or having personal data stolen. There are numerous types of attacks, and this article simulates a password attack to demonstrate that if passwords are easy to guess, they are susceptible to attacks. After conducting password attacks on individuals using personal Wi-Fi hotspots, using tools such as Aircrack-ng and Fern WiFi Cracker, it was found that both tools were able to crack the passwords in less than a minute. Based on the test results, users should set difficult passwords to make them harder to guess, whether it's for accessing various websites or using personal hotspots for WiFi distribution, in order to increase the difficulty of being attacked.

Therefore, this article presents the threat landscape to raise awareness about cybersecurity threats in various forms. With proper prevention measures in place, we can enhance our safety and security while using the internet.

Keywords: Password Attack, Awareness, Threat

บทนำ

อินเทอร์เน็ตเข้ามามีบทบาทในชีวิตประจำวัน ในด้านการติดต่อสื่อสาร การศึกษา และการทำธุรกิจ ทำให้ประสิทธิภาพของการรับส่งข้อมูล มีความสะดวก รวดเร็วมากขึ้น ซึ่งทำให้การใช้อินเทอร์เน็ตกว้างขวางมากทั้ง ทั้งใช้อินเทอร์เน็ตส่วนตัวและอินเทอร์เน็ตแบบเครือข่ายไร้สาย หรือที่เรียกว่าไวฟาย เนื่องจากระบบเครือข่ายไร้สายได้ถูกออกแบบมาให้มีความง่ายต่อการใช้งานและลดความซับซ้อนในการติดตั้ง ผู้ใช้งานจึงสามารถเข้าถึงอินเทอร์เน็ตได้ง่าย สามารถใช้ระบบเครือข่ายไร้สายผ่านเครื่องคอมพิวเตอร์โน๊ตบุ๊ค และอุปกรณ์อิเล็กทรอนิกส์อื่น ๆ ได้ง่ายขึ้น แต่ในการเข้าถึงอินเทอร์เน็ตได้ง่าย จึงส่งผลให้การโจมตีบนระบบไวฟาย ถูกดำเนินการได้โดยง่าย และยากต่อการตรวจจับป้องกัน (เดชพสิษฐ์, 2564) ดังนั้น จึงทำให้แฮกเกอร์ (Hacker) ใช้ประโยชน์จากช่องโหว่ด้านความมั่นคงปลอดภัยทางเทคโนโลยีในการติดตั้งและเจาะระบบคอมพิวเตอร์หรือล้วงข้อมูลส่วนตัวไปได้

ในปี 2565 ที่ผ่านมามีการทำงานที่บ้าน (Work from home) เนื่องด้วยสถานการณ์โควิด-19 ทำให้จำนวนการใช้อินเทอร์เน็ตมากขึ้น ทั้งการใช้อินเทอร์เน็ตส่วนตัว หรือใช้ฮอตสปอตส่วนบุคคลในการกระจายสัญญาณให้กับคอมพิวเตอร์เพื่อทำงาน พูดคุยสนทนา แลกเปลี่ยนข้อมูล หรือการเข้าใช้งานในโปรแกรมต่าง ๆ ทั้งนี้ หลายบริษัท กำหนดนโยบายให้ทำงานที่บ้าน หรือสถานศึกษาให้มีการเรียนออนไลน์มากขึ้น ทำให้มีการเข้าถึงอินเทอร์เน็ตมากขึ้น รวมทั้งมีไวฟายให้ใช้บริการฟรีตามสถานที่สาธารณะต่าง ๆ เช่น ร้านกาแฟ โรงเรียน หรือร้านอาหาร เป็นต้น ซึ่งการเชื่อมต่อไวฟายสาธารณะบางแห่งอาจไม่มีการเข้ารหัส (Encryption) ทำให้มีความเสี่ยงในการถูกโจมตีหรือขโมยข้อมูลส่วนตัวไปได้ ซึ่งผู้ใช้งานไวฟายไม่อาจทราบได้ว่ามีผู้ไม่หวังดีหรือมุ่งร้ายต่อข้อมูลสำคัญระหว่างการใช้ไวฟายด้วยหรือไม่ ดังนั้น หากผู้ใช้งานมีมาตรการป้องกันที่ดี ย่อมช่วยให้การใช้งานและเชื่อมต่อได้อย่างปลอดภัยมากขึ้น

จากข้อมูลที่ได้เผยแพร่ผลสำรวจการเชื่อมต่อไวฟายสาธารณะ โดยสำรวจข้อมูลจากกลุ่มผู้ใช้งานในประเทศสหรัฐอเมริกา พบว่า 71% ไม่ได้ตระหนักหรือมีความกังวลเรื่องความมั่นคงปลอดภัยในการใช้งานไวฟายฟรี มีผู้ใช้ไวฟายเพียง 25% เท่านั้นที่มีความตระหนักถึงการใช้งานไวฟายฟรีในที่สาธารณะ ซึ่งจากข้อมูลเหล่านี้จะเห็นได้ว่า ผู้ใช้ส่วนใหญ่มีความเสี่ยงสูงที่จะถูกขโมยข้อมูล (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร, 2562) อย่างไรก็ดี หนึ่งในภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ค่อนข้างสำคัญและมีความน่าสนใจก็คือ โจมตีในรูปแบบคาดเดารหัสผ่าน ซึ่งเป็นวิธีการที่ผู้ไม่ประสงค์ดีพยายามเจาะระบบด้วยวิธีการทดสอบสุ่มเดารหัสผ่านทุกค่า โดยลองทุก ๆ ความเป็นไปได้ของรหัสผ่านจนกว่าจะพบคำตอบที่ถูกต้อง วิธีการนี้เป็นการพยายามใช้ความเป็นไปได้ที่จะคาดเดารหัสผ่าน การโจมตีรูปแบบนี้ มักใช้เวลานานและใช้ทรัพยากรในกระบวนการค่อนข้างมาก ส่วนใหญ่วิธีนี้จะใช้ได้ผล หากผู้ถูกโจมตีตั้งรหัสผ่านที่ง่ายต่อการคาดเดา และหากผู้ใช้งานไม่ตระหนักถึงภัยคุกคาม อาจเสี่ยงต่อการถูกเจาะเข้าระบบและส่งผลกระทบต่อองค์กรธุรกิจและหน่วยงานทั่วโลก จนได้รับความเสียหายในหลาย ๆ ด้าน

ผลสำรวจพบว่า ในปี 2565 มีภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบคอมพิวเตอร์ เช่น ไวรัส, วอร์ม, โทรจัน และสปายแวร์ (Malicious Code) 54%, ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ (Availability)

18%, การล่อลวงหรือใช้เล่ห์กลต่าง ๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Information Garthering) 16%, การพยายามบุกรุกเจาะระบบด้วยวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force) หรือวิธีการเดาสุ่มข้อมูล (Intrusion Attempt) 12% (NT cyfence, 2566)

จากข้อมูลสถิติภัยคุกคามที่ได้กล่าวมา ผู้เขียนจึงขอนำเสนอรูปแบบการโจมตีทางไซเบอร์ต่าง ๆ รวมถึงจำลองการโจมตีด้วยรูปแบบคาดเดารหัสผ่าน และวิธีการสร้างความตระหนักรู้ เพื่อให้เป็นแนวทางป้องกันภัยที่จะเกิดขึ้นกับผู้ใช้งานในอนาคต

รูปแบบการโจมตีทางไซเบอร์

ภัยคุกคามที่เกิดจากการใช้อินเทอร์เน็ตมีมากมายหลายรูปแบบยกตัวอย่างเช่น การโจมตีทางไซเบอร์ ซึ่งแต่ละประเภทของภัยคุกคามจะมีลักษณะการโจมตีเป็นลักษณะเฉพาะตัว (Signature) ซึ่งอาจจะมีการทำงานที่คล้ายคลึงกันก็ตาม ดังนั้นผู้เขียนได้รวบรวมการโจมตีที่เป็นที่นิยมในโลกออนไลน์จำนวน 10 รูปแบบ (SCB, 2565) ดังนี้

1. มัลแวร์ (Malware: Malicious Software) โปรแกรมที่พัฒนาขึ้นมาเพื่อขโมยข้อมูลหรือรบกวนระบบคอมพิวเตอร์ เครือข่าย หรือ เซิร์ฟเวอร์ (Server) โดยแฮกเกอร์ (Hacker) ทำงานโดยล่อลวงเป้าหมายด้วยวิธีการต่าง ๆ เพื่อให้นำมัลแวร์ฝังลงไปในอุปกรณ์ โดยการเปิดทางเข้าถึงข้อมูลหรือเข้าควบคุมระบบของเป้าหมายได้ มัลแวร์มีหลายประเภท ยกตัวอย่างเช่น ไวรัสคอมพิวเตอร์ (Virus) หนอนคอมพิวเตอร์ (Worms) ม้าโทรจัน (Trojan horse) สปายแวร์ (Spyware) และมัลแวร์เรียกค่าไถ่ (Ransomware) (สุรชัย, 2563)

2. ฟิชชิ่ง (Phishing) เป็นภัยคุกคามทางไซเบอร์ที่มีลักษณะการทำงานคล้ายกับการจับปลาในบึงหรือทะเลสาบที่แม้จะมีโอกาสตกปลาได้จำนวนไม่มาก แต่ถ้าตกได้ปลาตัวใหญ่ก็ถือว่าคุ้มค่า โดยแฮกเกอร์มักใช้การแอบอ้างเป็นบุคคลอื่น ๆ เพื่อขอข้อมูลสำคัญด้วยวิธีการต่าง ๆ เช่น อีเมลปลอม ข้อความหลอกลวง หรือเว็บไซต์ปลอม เมื่อเหยื่อหลงเชื่อและทำการเปิดไฟล์เหล่านั้นโปรแกรมมัลแวร์ จะถูกติดตั้งและพร้อมโจมตีทันที

3. Man-in-the-Middle (MitM) เป็นวิธีการที่แฮกเกอร์เข้ามาแทรกกลางระหว่างการสนทนา หรือแทรกระหว่างทำธุรกรรมออนไลน์ของผู้ซื้อกับผู้ขาย และทำหน้าที่เป็นตัวกลางแทรกเข้าไประหว่างการรับส่งข้อมูลโดยที่ทั้งคู่สนทนา หรือผู้ซื้อผู้ขายไม่รู้ว่ามีคนมาแทรกตรงกลาง โดยทั่วไปแล้วผู้โจมตีแบบ MitM มักจะอาศัยช่องโหว่จากเครือข่ายไวฟายสาธารณะ เพื่อหลอกเอาข้อมูลสำคัญ นอกจากนั้นแฮกเกอร์หลายรายมักใช้วิธี MitM เพื่อส่งต่อฟิชชิ่งหรือมัลแวร์อีกด้วย

4. Denial of Service (DOS) เป็นการโจมตีระบบคอมพิวเตอร์ด้วยวิธีส่งคำขอ (Request) เข้าไปเครื่องแม่ข่ายจำนวนมากจน ทำให้ระบบปฏิบัติการหรือแอปพลิเคชันทำงานล่าช้า หรือหยุดชะงักชั่วคราวเพราะต้องทำงานรองรับคำขอจำนวนมาก เพียงแต่การโจมตีแบบ DoS นั้น เป็นการส่งคำขอเข้าระบบคอมพิวเตอร์จำนวนมากจากคอมพิวเตอร์แค่เครื่องเดียว แต่ DOS จะส่งคำขอจำนวนมากด้วยเครื่องคอมพิวเตอร์หลายเครื่อง ซึ่งในระหว่างการโจมตีนั้น แฮกเกอร์อาจฝังมัลแวร์ เพื่อเจาะเข้าระบบหรือเอาข้อมูลสำคัญขององค์กรได้อีกด้วย

5. SQL Injection Attack ระบบฐานข้อมูลที่ใช้ภาษา (SQL: Structure Query Language) เพื่อใช้เพื่อจัดการฐานข้อมูลของตนเอง เว็บไซต์ส่วนใหญ่ใช้ระบบฐานข้อมูลที่ใช้ภาษา SQL จัดการฐานข้อมูลเพื่อจัดเก็บข้อมูลสำคัญ เช่น บัญชีผู้ใช้, รหัสผ่าน และข้อมูลบัญชี ดังนั้น แฮกเกอร์อาศัยช่องโหว่ของโปรแกรมหรือเว็บไซต์ใส่ SQL เข้าไป เพื่อหลอกระบบฐานข้อมูลให้ดึงข้อมูลออก การโจมตีวิธีนี้ทำให้อาชญากรไซเบอร์เปิดการโจมตีไปที่ SQL จึงทำให้ส่งผลกระทบต่อระบบเซิร์ฟเวอร์โดยตรง (monster, 2564)

6. Zero-day Exploit & Attack Zero-day Exploit เป็นการโจมตีระบบด้วยการนำปล่อยโปรแกรมมัลแวร์ผ่านช่องโหว่ที่มีอยู่ที่ในซอฟต์แวร์ ระบบเครือข่ายคอมพิวเตอร์ หรือ ฮาร์ดแวร์ โดยผู้พัฒนาหรือเจ้าของซอฟต์แวร์เองก็ไม่รู้ตัว ส่วน Zero-day Attack หมายถึงการที่แฮกเกอร์ใช้ Zero-day Exploit สร้างความเสียหายหรือโจรกรรมข้อมูลจากอุปกรณ์ที่มีช่องโหว่มีตัวอย่างที่ บริษัทเทคโนโลยีขนาดใหญ่ อย่างเช่น Microsoft, Google, และ Apple มีการรายงานว่าเคยแก้ข้อผิดพลาด หรือช่องโหว่ในระบบมาแล้วทั้งนั้น

7. Password Attack เป็นการโจมตีทางไซเบอร์ ด้วยการเดารหัสผ่าน หรือใช้วิธีการล่อลวงให้เป้าหมายเปิดเผยรหัสผ่าน โดยทั่วไปแล้ว มี 3 รูปแบบ ได้แก่

- 7.1 Password Spraying Attack: เป็นการโจมตีกลุ่มเป้าหมายที่ใช้รหัสผ่าน ที่คาดเดาง่ายและเป็นที่นิยมอย่าง “123456” หรือ “abcdfgh” แล้วไล่โจมตีบัญชีที่มีอยู่ทีละบัญชี
- 7.2 Brute Force Attack: เป็นการสุ่มรหัสผ่านแบบลองผิดลองถูกไปเรื่อย ๆ จนกว่าจะได้รหัสผ่านที่ตรงกับบุคคลหรือองค์กรเป้าหมาย

7.3 Social Engineering: เป็นวิธีการที่แฮกเกอร์ใช้หลักจิตวิทยาหลอกล่อเป้าหมายให้บอกรหัสผ่าน เช่น การแจ้งเตือนผ่านแอปพลิเคชันหลอกล่อให้ใส่บัญชีผู้ใช้และรหัสผ่าน หรือ call center ที่โทรมาหลอกให้ทำธุรกรรมการเงิน เป็นต้น

8. Drive-by Attack โดยทั่วไปแล้วการโจมตีทางไซเบอร์ส่วนมากจะสำเร็จได้นั้นต้องให้เป้าหมายดำเนินการบางอย่าง เช่น กดคลิกลิงก์ หรือกดดาวน์โหลดไฟล์เอกสารแนบ แต่ Drive-by Attack นั้นจะแทรกคำสั่งพิเศษที่เป็นอันตรายไปยังเว็บไซต์ที่ถูกต้อง ซึ่งอาจอยู่ในรูปแบบของเว็บลิงก์ เพียงแค่คลิกเปิดลิงค์ขึ้นมา ก็ถูกติดตั้งมัลแวร์โดยไม่รู้ตัว

9. Internet of Things Attacks (IoT Attacks) การเชื่อมโยงในระบบอินเทอร์เน็ตที่มีปริมาณมากขึ้นทำให้อุปกรณ์ไฟฟ้าที่ใช้ในชีวิตประจำวันมีการเชื่อมต่อในระบบอินเทอร์เน็ต เช่น ลำโพงอัจฉริยะ สมาร์ททีวี หรือแม้แต่กล้องวงจรปิด อุปกรณ์ดังกล่าวล้วนแล้วแต่เป้าหมายของแฮกเกอร์ โดยทั่วไปแล้วอุปกรณ์ IoT ส่วนใหญ่ไม่มีการอัปเดตซอฟต์แวร์ ป้องกันไวรัส (antivirus) ทำให้การติดตั้งมัลแวร์ และควบคุมจากระยะไกลทำได้ง่าย

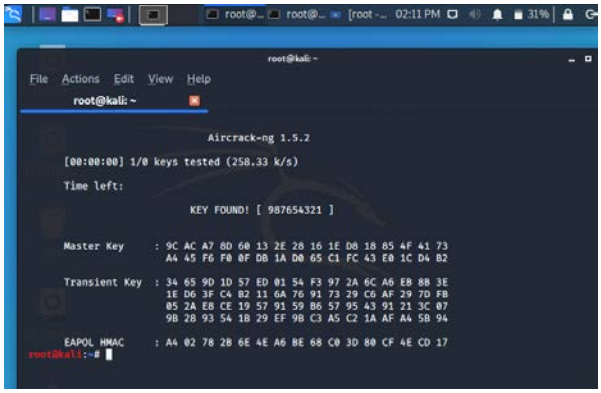
10. DNS Spoofing (Domain Name System Spoofing) เป็นกระบวนการปลอมแปลง domain name เพื่อนำเส้นทางที่พยายามเข้าเว็บไซต์ที่ถูกต้องส่งต่อไปยังเว็บไซต์ปลอมหรือเว็บไซต์มัลแวร์ หน้าตาของเว็บไซต์หลอกจะคล้ายกับเว็บไซต์จริงมาก เพื่อหลอกให้ผู้ใช้งานป้อนข้อมูลส่วนตัวที่สำคัญ เช่น เปลี่ยนเส้นทางเว็บไซต์ขององค์กรไปยังเว็บไซต์อนาจารเพื่อสร้างความอับอาย เป็นต้น (SCB, 2565)

ตามที่ได้ยกตัวอย่างการโจมตีในโลกออนไลน์จะเห็นได้ว่าทั้งหมดเป็นภัยที่เกิดจากการเชื่อมต่อของ เครื่องคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ กับระบบอินเทอร์เน็ต เพื่อใช้งานในการติดต่อสื่อสาร หรือ ใช้งานในกิจกรรมต่าง ๆ ที่ส่งผลร้ายแรงต่างกัน ขึ้นอยู่กับว่าระบบที่ถูกโจมตีจะทำให้เกิดการสูญเสียหรือมีข้อมูลสำคัญมากเพียงใด ซึ่งการโจมตีนั้นจะใช้เครื่องมือเพื่อโจมตีในแต่ละรูปแบบภัยคุกคามแตกต่างกันไป

การจำลองการโจมตีด้วยรูปแบบคาดเดารหัสผ่านและผลการศึกษา

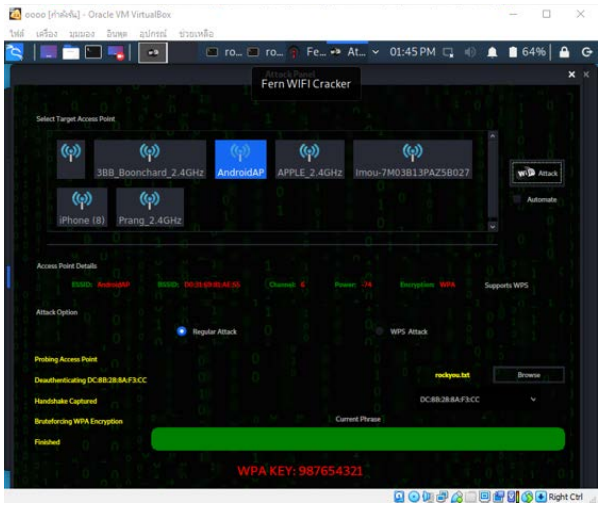
ผู้เขียนได้ดำเนินการจำลองการโจมตีด้วยรูปแบบคาดเดารหัสผ่าน โดยใช้เครื่องมือโจมตีที่ชื่อว่า แอร์แคร็ก และเฟิร์นวายฟาย แคร็กเกอร์ ที่มีอยู่ในระบบปฏิบัติการณ์กาลีลินุกซ์ โดยมีอุปกรณ์ที่ถูกทดสอบ คือ โทรศัพท์มือถือ โดยทำการเปิดฮอตสปอตส่วนบุคคลเพื่อการกระจายสัญญาณไวฟาย ซึ่งแบ่งการโจมตี ออกเป็น 2 เครื่องมือ ดังนี้

1. แอร์แคร็ก คือ เครื่องมือที่ใช้ค้นหาสัญญาณระบบเครือข่าย และใช้สำหรับดักจับข้อมูลของเครือข่ายไรสาย (Wireless LAN) คุณสมบัติสำคัญคือสามารถใช้ถอดรหัสข้อมูลทั้งในรูปแบบของ WEP และ WPA2 ได้ นอกจากนี้ยังเป็นเครื่องมือเพื่อใช้วิเคราะห์เครือข่ายไร้สายตามมาตรฐาน 802.11 (Chin-Ling Chen, 2564) โดยทำงานร่วมกับการ์ดแลนแบบไร้สาย (Wireless Card) หลายรุ่น ซึ่งแอร์แคร็กอยู่ในระบบปฏิบัติการกาลีลินุกซ์ ในระบบปฏิบัติการนี้มีเครื่องมือแอร์แคร็กให้ใช้งานได้อยู่แล้ว ไม่จำเป็นต้องติดตั้งเพิ่ม (CHAVIT, 2562) และเป็นเครื่องมือที่ใช้ทดสอบการเจาะรหัส ในรูปแบบ WEP และ WAP2 จุดประสงค์ของเครื่องมือนี้คือเพื่อกู้คืนหรือโจมตีรหัสผ่านไวฟาย โดยทำการค้นหารหัสในไฟล์ที่นำมาใช้ในการถอดรหัส ซึ่งมีรายการรหัสผ่านอยู่ในไฟล์ที่นำมาใช้พอสมควร (Parvathi Vinod, 2562) จากภาพที่ 1 จะเห็นได้ว่าสามารถถอดรหัสไวฟายออกมาได้สำเร็จในเวลาเพียง 0 วินาที



ภาพที่ 1 หน้าจอแสดงการถอดรหัสผ่านของแอร์แคร็ก
ที่มา: ภาพโดยผู้วิจัย สุภาพร พันธ์ยา

2. เฟิร์นไวฟาย แคร็กเกอร์ เป็นโปรแกรมเพื่อใช้ตรวจสอบความมั่นคงปลอดภัยระบบเครือข่ายไร้สายและเป็นซอฟต์แวร์แบบจียูไอ (GUI: Graphical User Interface) เป็นการใช้ภาพเป็นตัวประสานกับผู้ใช้ ทำให้การใช้เครื่องมือนี้ง่ายขึ้น เครื่องมือนี้ใช้ถอดรหัสผ่านแบบ WEP ได้อย่างง่ายดาย ซึ่งเป็นโปรแกรมที่สามารถถอดรหัสและกู้คืนได้อีกทั้งยังสามารถโจมตีเครือข่ายอื่น ๆ บนเครือข่ายไร้สายได้อีกด้วย (VIJAY KUMAR, 2564) ดังภาพที่ 2 จะเห็นได้ว่าสามารถถอดรหัสไวฟายออกมาได้สำเร็จในเวลาไม่ถึง 25 วินาที



ภาพที่ 2 หน้าจอแสดงการถอดรหัสผ่านของเฟิร์นไวฟาย แคร็กเกอร์
ที่มา: ภาพโดยผู้วิจัย สุภาพร พันธ์ยา

จากผลการศึกษาพบว่า เครื่องมือแอร์แคร็กใช้ระยะเวลาถอดรหัสเพียงแค่ 0 วินาที ถึงแม้ว่าเป็นเครื่องมือที่ใช้งานค่อนข้างยาก จำเป็นต้องพิมพ์คำสั่ง หรือต้องมีทักษะการในเขียนโปรแกรม แต่กลับใช้ระยะเวลาในการถอดรหัสออกมาได้ค่อนข้างไว ส่วนเครื่องมือเฟิร์นไวฟาย แคร็กเกอร์ใช้ระยะเวลาในการถอดรหัส 25 วินาที ถึงแม้ว่ามีการใช้งานที่ง่าย หน้าจอเป็นมิตรกับผู้ใช้งาน แต่ใช้ระยะเวลาในการถอดรหัสออกมาได้ค่อนข้างช้ากว่าเครื่องมือแอร์แคร็ก

ตามที่ผู้เขียนได้ยกตัวอย่างเครื่องมือที่ใช้ในการคุกคามระบบคอมพิวเตอร์บนระบบอินเทอร์เน็ตทั้งสองโปรแกรมจะเห็นได้ว่าถ้ามีการตั้งรหัสที่ง่ายต่อการคาดเดา การโจมตีรหัสผ่านก็ทำได้ง่ายและรวดเร็ว ทำให้ผู้ใช้งานหรือระบบคอมพิวเตอร์ที่ไม่มีการป้องกันภัยคุกคาม มีความเสี่ยงต่อข้อมูลสำคัญในระบบ ดังนั้น เพื่อให้ระบบมีความมั่นคงปลอดภัย ควรเริ่มให้ผู้ใช้งานและเจ้าของระบบคอมพิวเตอร์มีความตระหนักรู้ในเรื่องการป้องกันภัยคุกคาม

วิธีการสร้างความตระหนักรู้ และการป้องกันภัยคุกคาม

การป้องกันระบบคอมพิวเตอร์ที่ดีวิธีหนึ่งคือการให้ผู้ใช้งานระบบคอมพิวเตอร์มีความตระหนักถึงภัยคุกคามที่จะเกิดขึ้น เพราะการติดตั้งโปรแกรมเพื่อป้องกันภัยคุกคามเพียงอย่างเดียวโดยไม่ได้ใช้งานอย่างเหมาะสม ก็อาจเป็นต้นเหตุให้เกิดความเสียหายในระบบคอมพิวเตอร์ได้ ดังนั้น ผู้เขียนขอเสนอแนวทางวิธีการสร้างความตระหนักรู้ และการป้องกันภัยคุกคาม ดังนี้

1. การอัปเดตระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดเสมอ ซึ่งการอัปเดตระบบปฏิบัติการแต่ละครั้งผู้ผลิตจะทำการแก้ไขข้อบกพร่องในการทำงาน และปรับปรุงความมั่นคงปลอดภัยที่ดีขึ้น ซึ่งจะเป็นการป้องกันให้ดีมากขึ้น ทำให้การการเจาะระบบทำได้ยากขึ้น

2. การปิดใช้งานไวฟาย เมื่อไม่ได้ใช้งานคอมพิวเตอร์และไม่เปิดใช้งานการเชื่อมต่อไวฟายอัตโนมัติ เนื่องจากการเปิดไวฟายตลอดเวลาเป็นการเปิดโอกาสที่ระบบจะถูกแฮกเกอร์ติดตั้งแอปพลิเคชันอันตราย และเชื่อมต่ออินเทอร์เน็ตเพื่อแลกเปลี่ยนข้อมูลส่วนตัวของเราได้

3. การใช้ VPN (Virtual Private Network) เพื่อรับ – ส่งข้อมูลสำคัญผ่านระบบเครือข่ายอินเทอร์เน็ตมีความมั่นคงปลอดภัยสูงเพราะว่าข้อมูลจะถูกเข้ารหัส รวมถึงการไม่เปิดเผยตัวตน โดย VPN จะทำหน้าที่เปลี่ยนเส้นทางการรับส่งข้อมูลผ่านเซิร์ฟเวอร์ส่วนตัวที่กระจายไปทั่วหลายภูมิภาค ซึ่งจะทำให้คนกลางจะไม่สามารถเข้าถึงหรือขโมยข้อมูลไปได้ เป็นการเพิ่มความมั่นคงปลอดภัย เนื่องจากมีการเข้ารหัสคุณภาพสูง อาชญากรไซเบอร์จึงต้องใช้เวลาค่อนข้างมากในการเข้าถึงข้อมูล (ไอที 24 ชั่วโมง, 2565)

4. การเข้าใช้งานเว็บไซต์ปลอดภัยโดยสังเกต URL (Uniform Resource Locator) ของเว็บไซต์ ซึ่งควรขึ้นต้นเป็น HTTPS หรือรูปแม่กุญแจล็อก เนื่องจากเว็บไซต์ที่ปลอดภัยจะมีการเข้ารหัสข้อมูลในการรับส่งข้อมูลเพื่อป้องกันการดักจับข้อมูลจากแฮกเกอร์

5. ผู้ใช้งานไม่บันทึกรหัสผ่าน หรือเข้าสู่ระบบเว็บไซต์อัตโนมัติ เพราะถ้าคอมพิวเตอร์เชื่อมต่อกับไวฟายโดยไม่ได้ตั้งใจ อาจทำให้แฮกเกอร์เข้าถึงข้อมูลส่วนตัวและข้อมูลการเข้าสู่ระบบอาจถูกส่งออกทันที (ศูนย์ต่อต้านข่าวปลอมประเทศไทย, 2565)

6. ปิดการใช้งาน Wi-Fi Router เมื่อไม่ได้มีการใช้งานในบ้านหรือสำนักงาน เพื่อช่วยลดความเสี่ยงในการถูกโจมตีและรักษาอายุการใช้งานของอุปกรณ์เมื่อไม่ได้ใช้งาน

7. ตั้งรหัสผ่านให้ยากต่อการคาดเดาและหลากหลาย มีความยาวอย่างน้อย 12-14 ตัวอักษร ประกอบไปด้วย ตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และควรเปลี่ยนรหัสผ่านเป็นประจำทุก 3- 6 เดือน เพื่อป้องกันกรณีที่มีการรั่วไหลของข้อมูลโดยที่เราไม่รู้ตัว (NT cyfence, 2563)

8. ไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากแฮกเกอร์เจาะระบบสำเร็จ อาจทำให้ระบบอื่น ๆ ถูกเจาะได้ง่ายเช่นกัน

9. หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บผิดกฎหมาย และไม่คลิกไฟล์แนบจากผู้ส่งที่ไม่ระบุนาม ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมต่าง ๆ เพื่อหลีกเลี่ยงการติดมัลแวร์

10. ไม่ส่งต่อข่าวปลอมและติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยอยู่เสมอ (สำนักเทคโนโลยีสารสนเทศและการสื่อสาร, 2559)

11. หลีกเลี่ยงการใช้งานไวฟายที่ไม่ระบุผู้ให้บริการในที่สาธารณะ

12. ไม่ควรคลิกลิงก์หรือเปิดไฟล์แนบจากอีเมลที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

13. ควรติดตั้งโปรแกรมป้องกันไวรัสและ อัปเดตอย่างสม่ำเสมอ

สรุป

จากผลการศึกษาพบว่าทั้งเครื่องมือ แอร์แคร็ก และเฟิร์นวายฟาย แคร็กเกอร์ สามารถถอดรหัสผ่านออกมาได้ไม่ถึง 1 นาที ดังนั้น ผู้ใช้ควรตระหนักถึงภัยคุกคามทางไซเบอร์เป็นอย่างมาก จากที่กล่าวมาข้างต้น ทำให้เห็นว่ามีภัยคุกคามหลากหลายรูปแบบและเป็นสิ่งที่อยู่ใกล้ตัวเรา ซึ่งการใช้อินเทอร์เน็ตหรือใช้ไวฟาย เป็นวิธีการที่ง่าย สะดวก รวดเร็วในการเข้าถึงข้อมูล แต่ถ้าหากเรามีวิธีการป้องกันที่ไม่ดี ก็อาจเสี่ยงต่อการที่แฮกเกอร์เจาะระบบเพื่อเอาข้อมูลส่วนตัวไปได้ ทำให้เกิดผลเสียตามมาภายหลัง แต่ถ้าเรามีวิธีการป้องกันที่ดี เช่น ตั้งรหัสผ่านให้ยากต่อการคาดเดาหรือไม่เปิดใช้งานการเชื่อมต่อไวฟายอัตโนมัติ เพียงผู้ใช้ตระหนักถึงความมั่นคงปลอดภัยทางไซเบอร์ ก็สามารถลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยในการใช้งานให้มากขึ้นอีกด้วย

ข้อเสนอแนะ

1. ผู้ใช้งานระบบอินเทอร์เน็ตควรตั้งรหัสผ่านให้ยากต่อการคาดเดา โดยเฉพาะการใช้ฮอตสปอตเคลื่อนที่ (Mobile hotspot) เพื่อแชร์สัญญาณอินเทอร์เน็ตไร้สายผ่านทางโทรศัพท์มือถือ

2. ผู้ใช้งานระบบอินเทอร์เน็ตควรหลีกเลี่ยงการนำข้อมูลส่วนตัว เช่น เบอร์มือถือ วันเดือนปีเกิด เลขบัตรประชาชน หรือข้อมูลส่วนตัวมาตั้งเป็นรหัสผ่าน เนื่องจากข้อมูลดังกล่าวจะโดนนำมาใช้เพื่อการคาดเดารหัสผ่าน ซึ่งอาจเสี่ยงต่อการถูกโจมตีได้ง่าย

3. ผู้ใช้งานระบบอินเทอร์เน็ตควรหลีกเลี่ยงการใช้ไวฟายสาธารณะ เนื่องจากไวฟายสาธารณะส่วนใหญ่มักเข้าถึงได้ง่าย และไม่มีการเข้ารหัส ทำให้แฮกเกอร์สามารถดักจับข้อมูลดังกล่าวบนเครือข่ายไร้สายเพื่อขโมยรหัสผ่านหรือข้อมูลสำคัญต่าง ๆ โดยที่ผู้ใช้บริการไม่รู้ตัว

เอกสารอ้างอิง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. (2562). **สถิติการใช้ WiFi สาธารณะ.** สืบค้นเมื่อ 14 เมษายน 2566, จากhttps://ict.moph.go.th/th/extension/676.

NT cyfence. (2566). **สถิติภัยคุกคาม 2565. (ออนไลน์).** สืบค้นเมื่อ 14 เมษายน 2566, จากhttps://www.cyfence.com/article/2022-threat-statistics-summary-from-csoc-by-nt-cyfence/.

CHAVIT. (2562). **เครื่องมือที่แฮกเกอร์นิยมเจาะระบบคอมพิวเตอร์ผ่านเครือข่ายไร้สายในกาลีลินุกซ์ (Kali linux).** สืบค้นเมื่อ 12 เมษายน 2566, จาก https://medium.com/@6117660003/.

Parvathi Vinod. (2562). **Wifi Password Recovery**. สืบค้นเมื่อ 27 พฤษภาคม 2566, จาก https://nceca.in/2020/NCECA_2020_paper_109.pdf.

เอกสารอ้างอิง

VIJAY KUMAR. (2564). **อันดับเครื่องมือที่แฮกเกอร์นิยมเจาะระบบคอมพิวเตอร์ผ่านเครือข่ายไร้สายในกาลีลินุกซ์.** สืบค้นเมื่อ 27 พฤษภาคม 2566, จาก https://www.cyberpratibha.com/blog/top-5-wifi-hacking-software-to-retrieve-password/.

Chin-Ling Chen and Supaporn Punya. (2564). An enhanced WPA2/PSK for preventing authentication cracking. **International Journal of Informatics and Communication Technology (IJ-ICT)**, 10(2), 85-92.

ไอที 24 ชั่วโมง (2565). **การป้องกันภัยการโจมตีทางไซเบอร์.** สืบค้นเมื่อ 14 เมษายน 2566, จากhttps://www.it24hrs.com/2022/best-way-protect-your-pc-laptop-public-wifi/.

ศูนย์ต่อต้านข่าวปลอม ประเทศไทย. (2565**). การป้องกันภัยจากการใช้ไวฟายสาธารณะ.** สืบค้นเมื่อ 14 เมษายน 2566, จากhttps://www.antifakenewscenter.com/.

NT cyfence. (2563). **การป้องกันภัยจากการถูกโจมตีอินเทอร์เน็ต.** สืบค้นเมื่อ 26 พฤษภาคม 2566, จากhttps://www.cyfence.com/article/7-way-to-secure-your-online-identity/.

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร (2559). **การป้องกันภัยคุกคามทางคอมพิวเตอร์.** สืบค้นเมื่อ 26 พฤษภาคม 2566, จาก https://www.senate.go.th/assets/portals/49/news/87/2_%E0%B8%AA%E0%B8%B3%E0%B8%99%E0%B8%B1%E0%B8%81%E0%B9%80%E0%B8%97%E0%B8%84%E0%B9%82%E0%B8%99%E0%B9%82%E0%B8%A5%E0%B8%A2%E0%B8%B5%E0%B8%AA%E0%B8%B2%E0%B8%A3%E0%B8%AA%E0%B8%99%E0%B9%80%E0%B8%97%E0%B8%A8%E0%B9%81%E0%B8%A5%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%AA%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%AA%E0%B8%B2%E0%B8%A3_km11-59.pdf.

Monster. (2564). **7 รูปแบบทั่วไปของการโจมตี Cybersecurity.** สืบค้นเมื่อ 27 พฤษภาคม 2566, จาก https://monsterconnect.co.th/7-common-types-of-cybersecurity-attacks/.

SCB. (2565). **10 รูปแบบการโจมตีทางไซเบอร์ระดับตัวท็อป.** สืบค้นเมื่อ 27 พฤษภาคม 2566, จาก https://www.scb.co.th/th/personal-banking/stories/tips-for-you/top-10-cyber-attack.html.

สุรชัย ฉัตรเฉลิมพันธุ์ และ เทอดพงษ์ แดงสี. (2564). การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร: กรณีการจำลอง การโจมตีด้วยฟิชชิ่ง. **วารสารมนุษยศาสตร์และสังคมศาสตร์มหาวิทยาลัยธนบุรี**, 4(2), 1-11.