บทที่ 4

ผลการวิจัย

การศึกษาและวิจัยครั้งนี้มีวัตถุประสงค์ เพื่อศึกษาและวิเคราะห์หาความผิดปกติและโอกาสการถูกโจมตีจากการใช้เครือข่ายสังคมออนไลน์ ศึกษาและวิเคราะห์การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ พัฒนาตัวแบบในการสืบค้นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ พร้อมทั้งพัฒนาตัวแบบในการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า รวมทั้งการพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ เพื่อที่จะค้นหากลยุทธ์การติดตามภัยจากการใช้เครือข่ายสังคมออนไลน์ ซึ่งการทราบถึงเหตุการณ์ปัจจุบันและประเมินหาการเชื่อมโยงในเครือข่ายสังคมออนไลน์เป็นประโยชน์มากในการวิเคราะห์ และความเข้าใจในเครือข่ายสังคมออนไลน์ดังกล่าว สามารถนำไปสู่การดำเนินงานที่มีประสิทธิภาพของเครื่องมือในการสืบค้นผู้กระทำผิดปกติหรือมีพฤติกรรมการโจมตี การค้นหาเป้าหมายที่อาจจะได้รับผลกระทบจากการโจมตีนั้นๆ รวมทั้งการระบุกลุ่มที่ซ่อนอยู่หรือการหาสมาชิกที่หายไปของกลุ่ม ฯลฯ ในเครือข่ายสังคมออนไลน์ ซึ่งเป็นปัญหาที่พบบ่อยที่สุดในการรักษาความมั่นคงปลอดภัยและการสอบสวนทางอาญา

ผู้วิจัยได้ทำการทดลองเบื้องต้นเพื่อเปรียบเทียบเทคนิคที่เลือกใช้ในกรอบแนบคิดในการวิจัย (บทที่ 3 รูปที่ 3.2) ดังนี้

1. เทคนิคการวิเคราะห์ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์

งานวิจัยการวิเคราะห์ความผิดปกติและการถูกโจมตีในเครือข่ายสังคม (Social Networks Anomaly and Attack Patterns Analysis) [76] และการวิเคราะห์ความผิดปกติและการถูกโจมตีในเครือข่ายสังคมด้วยการสร้างกฎความสัมพันธ์ (Social Networks Anomaly and Attack Patterns Analysis with Association Rules) [78] เป็นงานวิจัยเพื่อค้นหาเทคนิคการวิเคราะห์ความผิดปกติและการถูกโจมตีในเครือข่ายสังคม โดยผู้วิจัยได้ทำการเปรียบเทียบเทคนิคการรวมกลุ่ม

(Cluster Algorithm) เพื่อทำการวิเคราะห์ความผิดปกติของการถูกโจมตีในเครือข่ายสังคมออนไลน์ด้วยการคำนวณการวัดระยะทาง (Distance Measure) และ K-Means Algorithm เปรียบเทียบกับเทคนิคกฎความสัมพันธ์ (Association Rules) พบว่างานวิจัย 2 ชิ้นดังกล่าวให้ผลการวิเคราะห์ความผิดปกติและการถูกโจมตีในเครือข่ายสังคมไม่แตกต่างกัน แต่เทคนิคการรวมกลุ่ม (Cluster Algorithm) จะทำให้เกิดการจัดกลุ่มข้อมูลซึ่งสนับสนุนให้งานในลำดับถัดไปคือการวิเคราะห์เครือข่ายสังคมมีระบบการจัดการกลุ่มที่ดี

2. เทคนิคการวิเคราะห์รูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์

งานวิจัยการแสดงภาพวิชวลไลเซชันของการแพร่กระจายในเครือข่ายสังคม (Visualization of Information Diffusion in Social Networks) [75] เป็นการศึกษาการนำเทคนิคทางทฤษฎีกราฟ (Graph-based Structure) มาทำการวิเคราะห์ปัจจัยสนับสนุนต่างๆ ได้แก่ ค่าความเป็นศูนย์กลาง (Centrality), ค่าการรับข้อมูลข่าวสารหรือผลการกระทำผิดปกติและการโจมตีในเครือข่ายสังคมออนไลน์ (In-Degree), ค่าการกระจายข้อมูลข่าวสารหรือผลการกระทำผิดปกติและการโจมตีในเครือข่ายสังคมออนไลน์ (Out-Degree) เป็นต้น เพื่อค้นหารูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ และการนำเสนอภาพของการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ด้วย Minimum Spanning Tree ของ Prim's Algorithm

3. เทคนิคการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์

งานวิจัยการติดตามโหนดที่มีอิทธิพลต่อการเกิดความผิดปกติและการถูกโจมตีในเครือข่ายสังคม(Tracking the Influencing Nodes of Anomaly and Attack Patterns in Social Networks) [73] เป็นการศึกษาการนำเทคนิคทางทฤษฎีกราฟมาทำการวิเคราะห์ปัจจัยสนับสนุนต่างๆ ได้แก่ ค่าความเป็นศูนย์กลาง (Centrality), ค่าการรับข้อมูลข่าวสารหรือผลการกระทำผิดปกติและการโจมตีในเครือข่ายสังคมออนไลน์ (In-Degree), ค่าการกระจายข้อมูลข่าวสารหรือผลการกระทำผิดปกติและการโจมตีในเครือข่ายสังคมออนไลน์ (Out-Degree) เป็นต้น เพื่อค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ และการนำเสนอภาพของการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm

4. เทคนิคการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์

งานวิจัยการทำนายความเชื่อมโยงในเครือข่ายสังคมด้วยเทคนิคการวิเคราะห์เครือข่ายสังคมและเทคนิคการเรียนรู้แบบมีผู้สอน (Links Prediction in Social Networks by SNA and Supervised Learning) [74] ด้วยเทคนิคการเรียนรู้แบบมีผู้สอน (Supervised Learning, Classification Analysis, J48, oneR, Naïve Bay) เพื่อศึกษาถึงเทคนิคการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ พบว่าวิธี oneR มีประสิทธิภาพทางเวลาและการทำนายที่แม่นยำกว่าวิธีการ J48 และ Naïve Bays ดังนั้นเทคนิคการพัฒนาตัวแบบการพยากรณ์และการจำแนก ณ เวลาอนาคต (Classification for Prediction) ผู้วิจัยได้ทำการเลือกใช้วิธี oneR ในกรอบแนวคิดในการวิจัยต่อไป และนำเสนอภาพของเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ ด้วยเทคนิคการวิเคราะห์เครือข่ายสังคม (Social Network Analysis: SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm

จากวัตถุประสงค์และผลการทดลองเบื้องต้นของงานวิจัยที่กล่าวไว้ ผู้วิจัยได้กำหนดกรอบแนวคิดในการวิจัย ดังแสดงไว้ในบทที่ 3 รูปที่ 3.2 ซึ่งในการวิจัยนี้ได้นำฐานข้อมูลความผิดปกติ (Anomaly) และการถูกโจมตี (Attack) ของการใช้เครือข่ายสังคมออนไลน์และฐานข้อมูลความสัมพันธ์ของสมาชิกที่ได้รับความผิดปกติ(Anomaly) และการถูกโจมตี (Attack) เมื่อใช้งานเครือข่ายสังคมออนไลน์ขององค์กรที่ต้องการความมั่นคงปลอดภัยในระดับสูง เนื่องจากต้องป้องกันความเสี่ยงต่อข้อมูลและระบบสารสนเทศขององค์กรที่รองรับระบบงานทางด้านสุขภาพในระดับประเทศ (Public Health Sector in Thailand) จำนวน 2 ประเทศคือประเทศไทย และประเทศที่ร่วมทดสอบ จำนวน 4 ชุดคือชุดข้อมูลในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เข้าทดสอบการทดลองเพื่อนำไปสู่การสรุปผลและการประเมินตัวแบบของการวิจัยที่แม่นยำ

โดยผู้วิจัยวางแผนการเลือกตัวอย่างฐานข้อมูลความผิดปกติ (Anomaly) และการถูกโจมตี (Attack) ของการใช้เครือข่ายสังคมออนไลน์ซึ่งเป็น Traffic Log ด้วยหลักการของการเลือกตัวอย่างตามความน่าจะเป็น (Probability Sampling) ดังนี้

1. การเลือกตัวอย่างแบบกลุ่ม (Cluster Sampling)

การเลือกตัวอย่างแบบกลุ่ม (Cluster Sampling) เป็นการเลือกตัวอย่างที่ภายในแต่ละกลุ่มมีลักษณะที่สนใจทุกลักษณะ หรือมีลักษณะที่แตกต่างคละกัน ดังนั้นการเลือกตัวอย่างแบบกลุ่มจึงเป็นการเลือกตัวอย่างเพียงบางกลุ่มมาทำการศึกษาเท่านั้น โดยผู้วิจัยได้กำหนดกลุ่มย่อย (Cluster Factor) ตามเดือน

2. การเลือกตัวอย่างสุ่มแบบง่าย (Simple Random Sampling)

เป็นการเลือกตัวอย่างที่ให้แต่ละหน่วยในประชากรมีโอกาสถูกเลือกเท่าๆกันในแต่ละครั้งของการเลือก โดยผู้วิจัยได้ทำการเลือกตัวอย่างแบบง่ายจากการเลือกตัวอย่างแบบกลุ่มได้เดือนเมษายน และธันวาคม

เนื่องจากงานวิจัยนี้ได้ทำการศึกษาตั้งแต่พฤศจิกายน 2554-2556 จึงทำการเลือกตัวอย่าง โดยกำหนดขอบเขตการสุ่มตัวอย่างฐานข้อมูลความผิดปกติ (Anomaly) และการถูกโจมตี (Attack) ของการใช้เครือข่ายสังคมออนไลน์ของ 2 ประเทศ คือ ประเทศไทย และประเทศที่เข้าร่วมทดสอบ ในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 โดยผู้วิจัยจะขอนำเสนอผลการวิจัยแยกออกเป็น 6 ส่วน ดังนี้

1. ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์
2. รูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์
3. การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์
4. การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์
5. การทดสอบประเมินความแม่นยำของการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ และการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %
6. ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ

4.1 ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์

จากวัตถุประสงค์งานวิจัยข้อที่ 1 ซึ่งผู้วิจัยได้ทำการศึกษาและวิเคราห์ฐานข้อมูลเพื่อค้นพบความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ของประเทศไทยและประเทศที่ร่วมทดสอบ ด้วยหลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm)

ทั้งนี้ ในทุกการทดลองของชุดฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ของประเทศไทยและประเทศที่ร่วมทดสอบ นั้น ผู้วิจัยได้สรุปประเด็นรวมความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทยและประเทศที่ร่วมทดสอบ จำนวน 20 ประเด็น เพื่อแสดงสัดส่วนการเกิดเหตุการณ์ต่างๆ ดังนี้

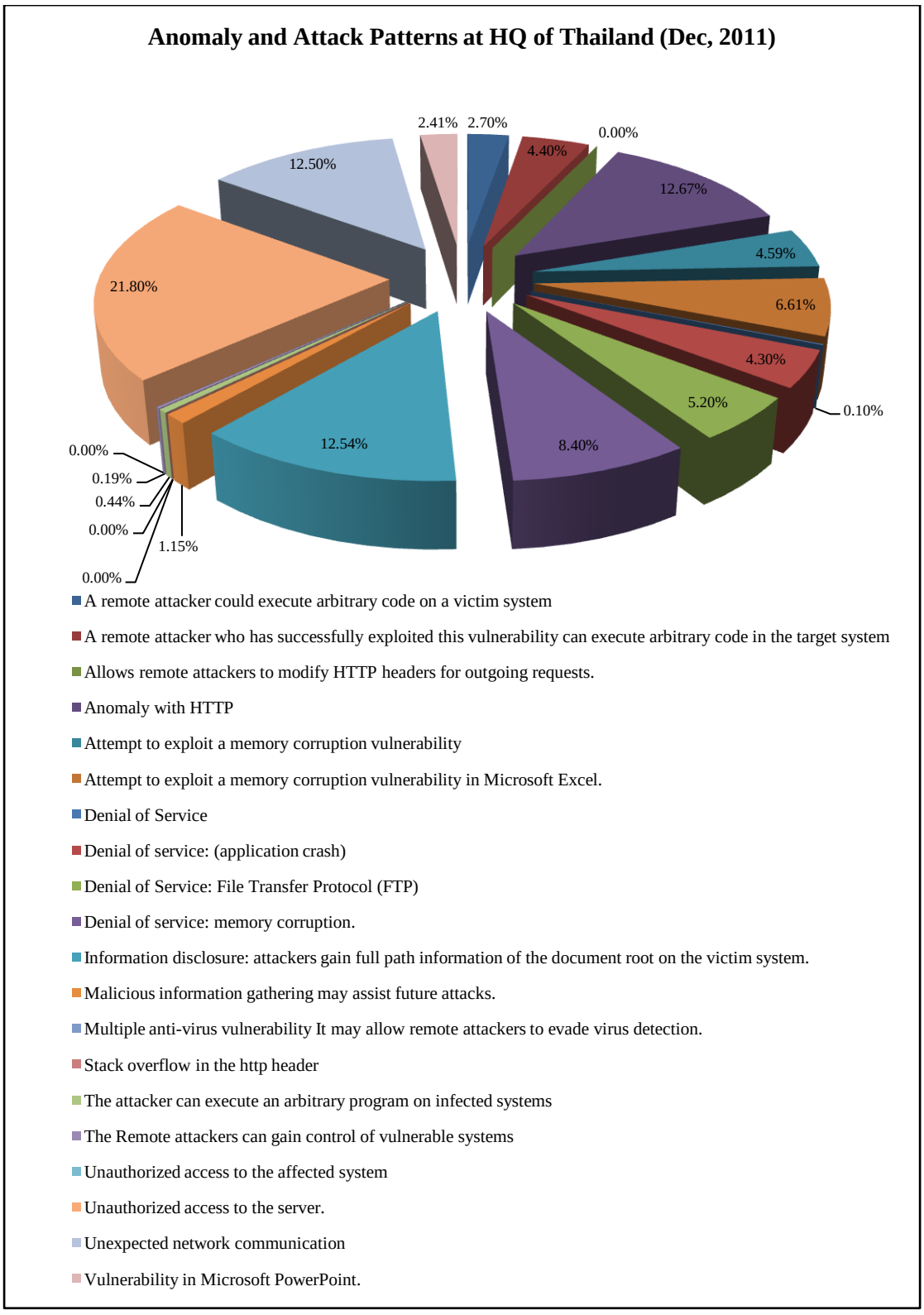
1. A remote attacker could execute arbitrary code on a victim system.
2. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system.
3. Allows remote attackers to modify HTTP headers for outgoing requests.
4. Anomaly with HTTP
5. Attempt to exploit a memory corruption vulnerability
6. Attempt to exploit memory corruption vulnerability in Microsoft Excel.
7. Denial of Service
8. Denial of service: (application crash)
9. Denial of Service: File Transfer Protocol (FTP)
10. Denial of service: memory corruption.
11. Information disclosure: attackers gain full path information of the document root on the victim system.
12. Malicious information gathering may assist future attacks.
13. Multiple anti-virus vulnerability, It may allow remote attackers to evade virus detection.
14. Stack overflow in the http header.
15. The attacker can execute an arbitrary program on infected systems.

16. The Remote attackers can gain control of vulnerable systems.
17. Unauthorized access to the affected system.
18. Unauthorized access to the server.
19. Unexpected network communication.
20. Vulnerability in Microsoft PowerPoint.

ผู้วิจัยสามารถนำเสนอความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ โดยมีข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทย ดังแสดงในตารางที่ 4.1-4.4 และรูปประกอบที่ 4.1-4.6 และข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบ ดังแสดงในตารางที่ 4.5-4.8 และรูปประกอบที่ 4.7-4.12 ดังนี้

ตารางที่ 4.1 ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนธันวาคม 2554 (ประเทศไทย)

Anomaly and Attack Patterns at HQ of Thailand (Dec, 2011)	
Attack Pattern	**Percentage**
A remote attacker could execute arbitrary code on a victim system.	2.70
A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system.	4.38
Allows remote attackers to modify HTTP headers for outgoing requests.	0.00
Anomaly with HTTP.	12.67
Attempt to exploit memory corruption vulnerability.	4.59
Attempt to exploit memory corruption vulnerability in Microsoft Excel.	6.61
Denial of Service.	0.10
Denial of service: (application crash).	4.28
Denial of Service: File Transfer Protocol (FTP).	5.20
Denial of service: memory corruption.	8.40
Information disclosure: attackers gain full path information of the document root on the victim system.	12.54
Malicious information gathering may assist future attacks.	1.15
Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection.	0.00
Stack overflow in the http header.	0.00
The attacker can execute an arbitrary program on infected systems.	0.44
The Remote attackers can gain control of vulnerable systems.	0.19
Unauthorized access to the affected system.	0.00
Unauthorized access to the server.	21.80
Unexpected network communication.	12.50
Vulnerability in Microsoft PowerPoint.	2.41
Total	100.00



รูปที่ 4.1 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนธันวาคม 2554 (ประเทศไทย)

จากตารางที่ 4.1 และรูปที่ 4.1 แสดงให้เห็นว่าข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทยในเดือนธันวาคม 2554 นั้น พบความผิดปกติและโอกาสการถูกโจมตีที่หลากหลายทั้งสิ้น 16 ประเด็น ดังนี้

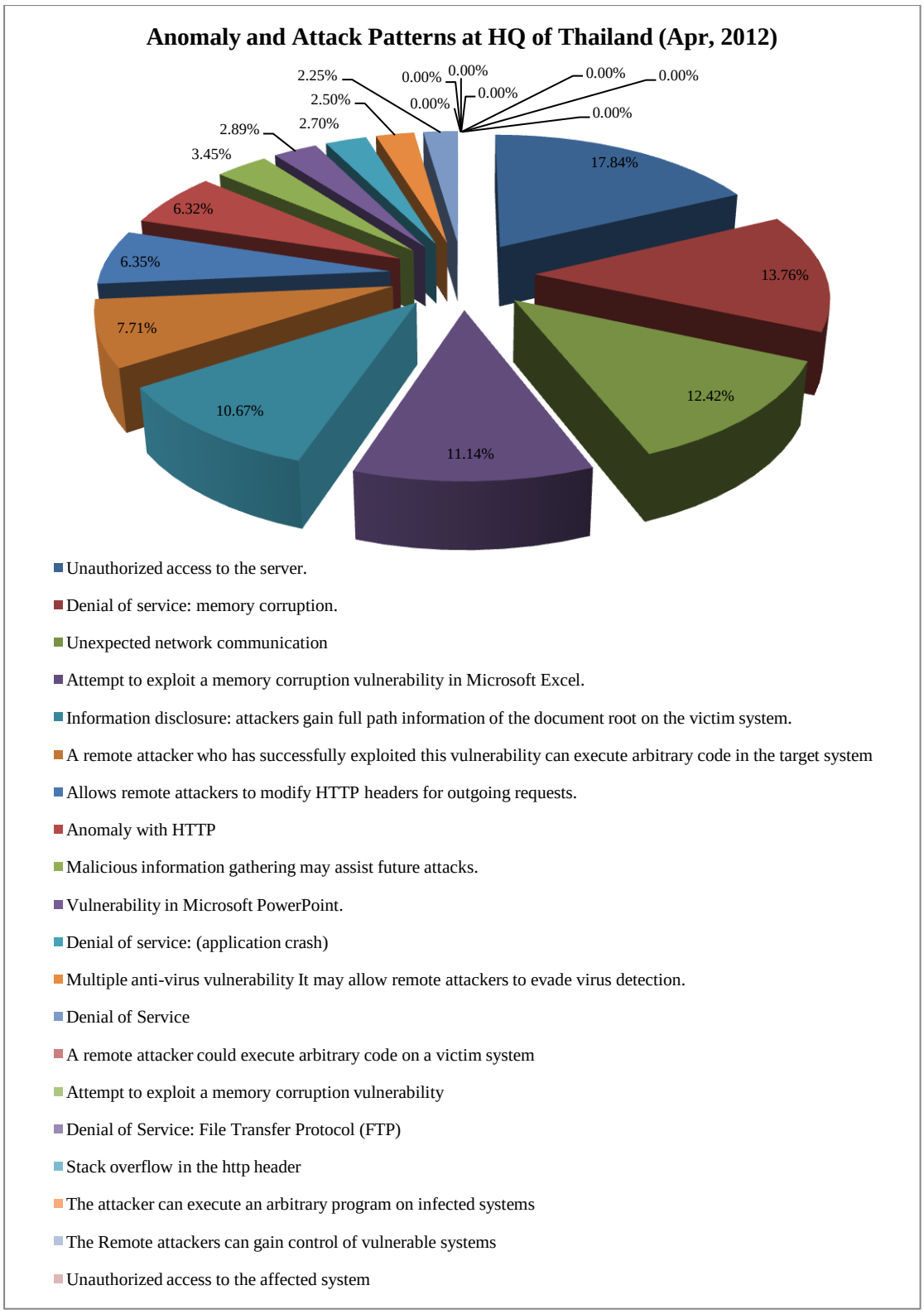
1. Unauthorized access to the server 21.80%
2. Anomaly with HTTP 12.67%
3. Information disclosure: attackers gain full path information of the document root on the victim system 12.54%
4. Unexpected network communication 12.50%
5. Denial of service: memory corruption 8.40%
6. Attempt to exploit a memory corruption vulnerability in Microsoft Excel 6.61%
7. Denial of Service: File Transfer Protocol (FTP) 5.20%
8. Attempt to exploit a memory corruption vulnerability 4.59%
9. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system 4.40%
10. Denial of service: (application crash) 4.30%
11. A remote attacker could execute arbitrary code on a victim system 2.70%
12. Vulnerability in Microsoft PowerPoint 2.41%
13. Malicious information gathering may assist future attacks 1.15%
14. The attacker can execute an arbitrary program on infected systems 0.44%
15. The Remote attackers can gain control of vulnerable systems 0.19%
16. Denial of Service 0.10%

โดยข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทยที่ไม่พบในเดือนธันวาคม 2554 ทั้งสิ้น 4 ประเด็น ดังนี้

1. Allows remote attackers to modify HTTP headers for outgoing requests.
2. Multiple anti-virus vulnerability, It may allow remote attackers to evade virus detection.
3. Stack overflow in the http header.
4. Unauthorized access to the affected system.

ตารางที่ 4.2 ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนเมษายน 2555 (ประเทศไทย)

Anomaly and Attack Patterns at HQ of Thailand (Apr, 2012)	
Attack Pattern	**Percentage**
A remote attacker could execute arbitrary code on a victim system.	0.00
A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system.	7.71
Allows remote attackers to modify HTTP headers for outgoing requests.	6.35
Anomaly with HTTP.	6.32
Attempt to exploit memory corruption vulnerability.	0.00
Attempt to exploit memory corruption vulnerability in Microsoft Excel.	11.14
Denial of Service.	2.25
Denial of service: (application crash).	2.70
Denial of Service: File Transfer Protocol (FTP).	0.00
Denial of service: memory corruption.	13.76
Information disclosure: attackers gain full path information of the document root on the victim system.	10.67
Malicious information gathering may assist future attacks.	3.45
Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection.	2.50
Stack overflow in the http header.	0.00
The attacker can execute an arbitrary program on infected systems.	0.00
The Remote attackers can gain control of vulnerable systems.	0.00
Unauthorized access to the affected system.	0.00
Unauthorized access to the server.	17.84
Unexpected network communication.	12.42
Vulnerability in Microsoft PowerPoint.	2.89
Total	100.00



รูปที่ 4.2 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศไทย)

จากตารางที่ 4.2 และรูปที่ 4.2 แสดงให้เห็นว่าข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทยในเดือนเมษายน 2555 นั้น พบความผิดปกติและโอกาสการถูกโจมตีที่หลากหลายทั้งสิ้น 13 ประเด็น ดังนี้

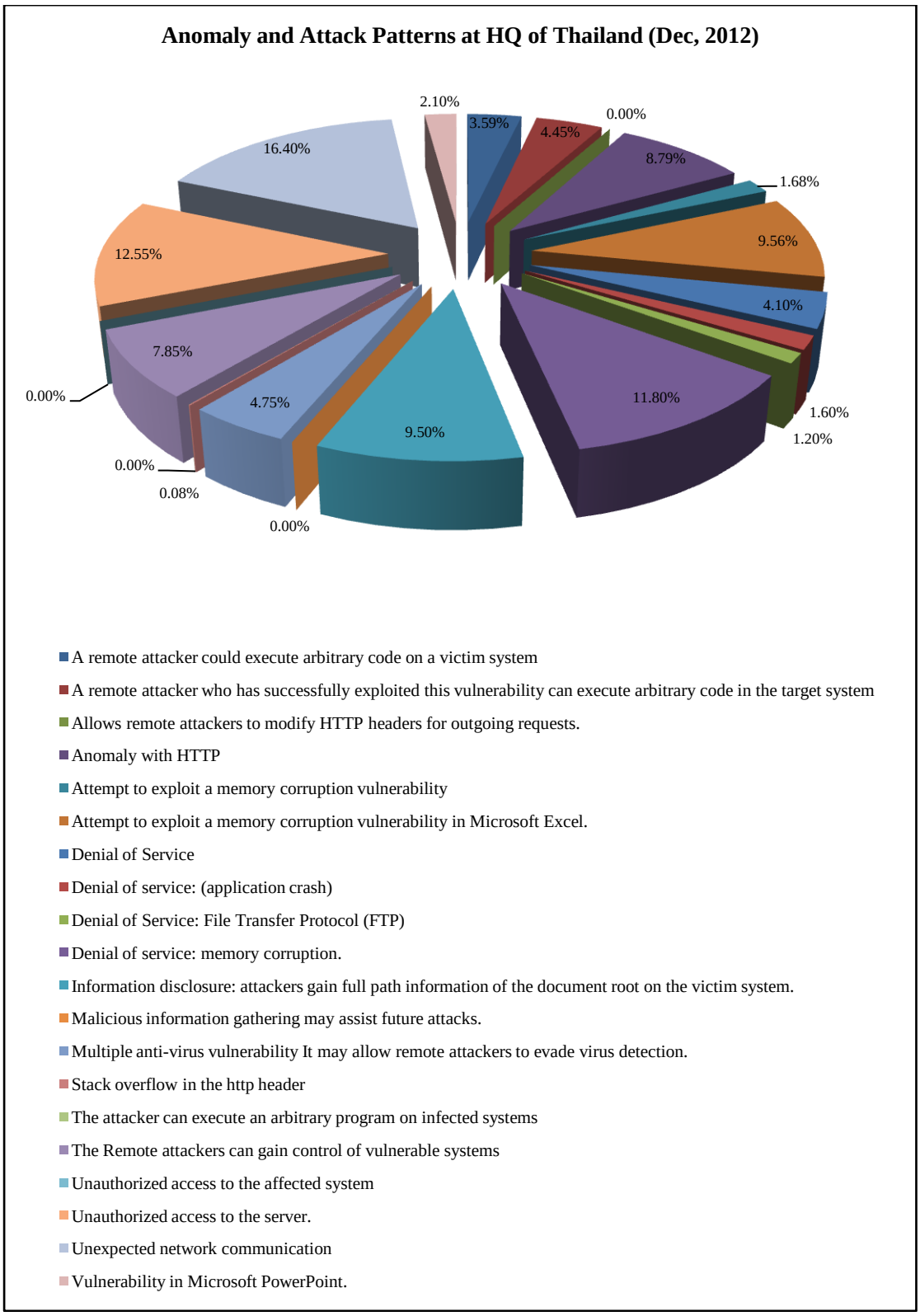
1. Unauthorized access to the server 17.84%
2. Denial of service: memory corruption 13.76%
3. Unexpected network communication 12.42%
4. Attempt to exploit a memory corruption vulnerability in Microsoft Excel 11.14%
5. Information disclosure: attackers gain full path information of the document root on the victim system 10.67%
6. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system 7.71%
7. Allows remote attackers to modify HTTP headers for outgoing requests 6.35%
8. Anomaly with HTTP 6.32%
9. Malicious information gathering may assist future attacks 3.45%
10. Vulnerability in Microsoft PowerPoint 2.89%
11. Denial of service: (application crash) 2.70%
12. Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection 2.50%
13. Denial of Service 2.25%

โดยข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทยที่ไม่พบในเดือนเมษายน 2555 ทั้งสิ้น 7 ประเด็น ดังนี้

1. A remote attacker could execute arbitrary code on a victim system.
2. Attempt to exploit memory corruption vulnerability.
3. Denial of Service: File Transfer Protocol (FTP).
4. Stack overflow in the http header.
5. The attacker can execute an arbitrary program on infected systems.
6. The Remote attackers can gain control of vulnerable systems.
7. Unauthorized access to the affected system.

ตารางที่ 4.3 ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนธันวาคม 2555 (ประเทศไทย)

Anomaly and Attack Patterns at HQ of Thailand (Dec, 2012)	
Attack Pattern	**Percentage**
A remote attacker could execute arbitrary code on a victim system.	3.59
A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system.	4.43
Allows remote attackers to modify HTTP headers for outgoing requests.	0.00
Anomaly with HTTP.	8.79
Attempt to exploit memory corruption vulnerability.	1.68
Attempt to exploit memory corruption vulnerability in Microsoft Excel.	9.56
Denial of Service.	4.10
Denial of service: (application crash)	1.60
Denial of Service: File Transfer Protocol (FTP).	1.20
Denial of service: memory corruption.	11.80
Information disclosure: attackers gain full path information of the document root on the victim system.	9.50
Malicious information gathering may assist future attacks.	0.00
Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection.	4.75
Stack overflow in the http header.	0.08
The attacker can execute an arbitrary program on infected systems.	0.00
The Remote attackers can gain control of vulnerable systems.	7.85
Unauthorized access to the affected system.	0.00
Unauthorized access to the server.	12.55
Unexpected network communication.	16.40
Vulnerability in Microsoft PowerPoint.	2.10
Total	100.00



รูปที่ 4.3 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศไทย)

จากตารางที่ 4.3 และรูปที่ 4.3 แสดงให้เห็นว่าข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทยในเดือนธันวาคม 2555 นั้น พบความผิดปกติและโอกาสการถูกโจมตีที่หลากหลายทั้งสิ้น 16 ประเด็น ดังนี้

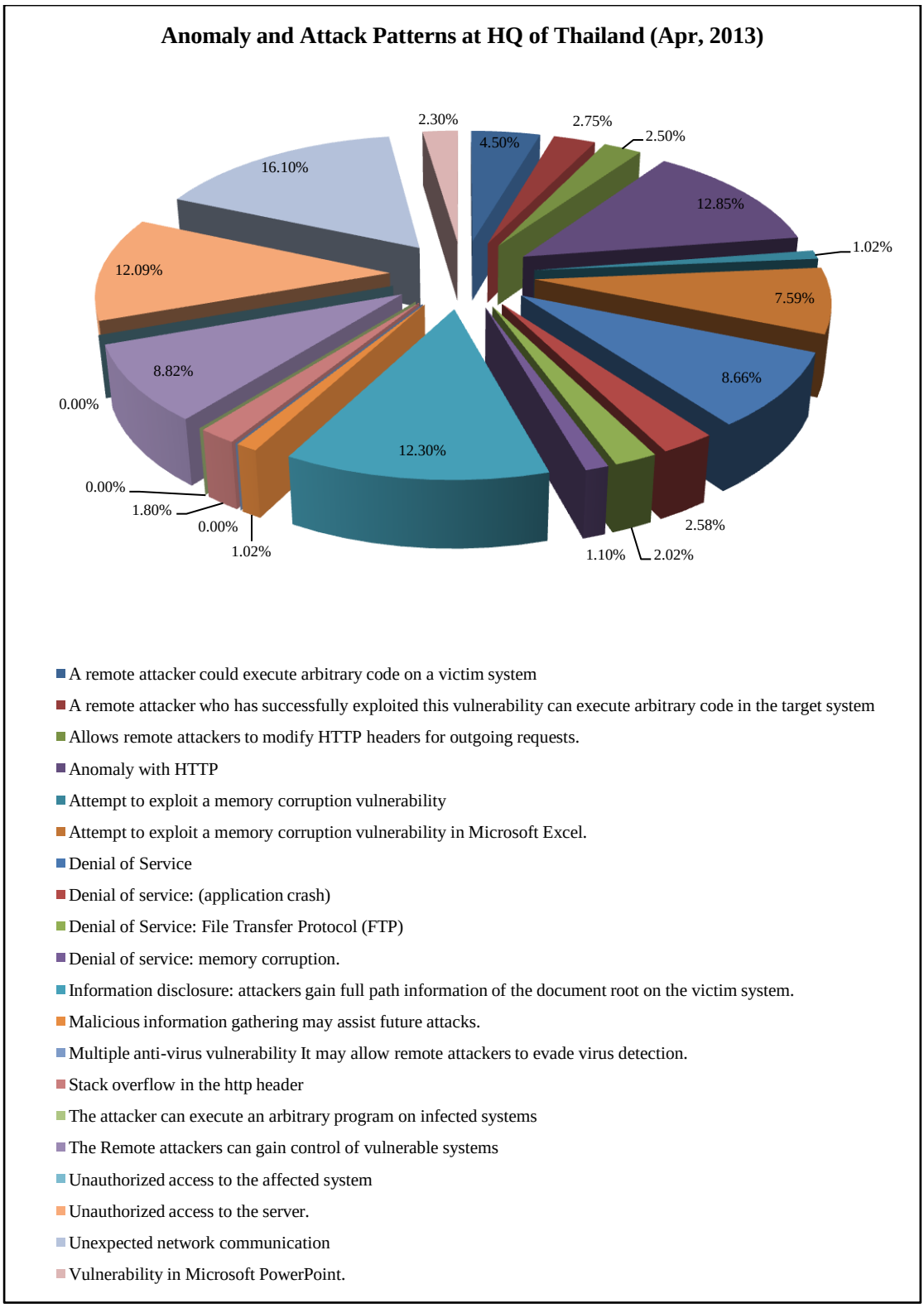
1. Unexpected network communication 16.40%
2. Unauthorized access to the server 12.55%
3. Denial of service: memory corruption 11.80%
4. Attempt to exploit a memory corruption vulnerability in Microsoft Excel 9.56%
5. Information disclosure: attackers gain full path information of the document root on the victim system 9.50%
6. Anomaly with HTTP 8.79%
7. The Remote attackers can gain control of vulnerable systems 7.85%
8. Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection 4.75%
9. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system 4.45%
10. Denial of Service 4.10%
11. A remote attacker could execute arbitrary code on a victim system 3.59%
12. Vulnerability in Microsoft PowerPoint 2.10%
13. Attempt to exploit a memory corruption vulnerability 1.68%
14. Denial of service: (application crash) 1.60%
15. Denial of Service: File Transfer Protocol (FTP) 1.20%
16. Stack overflow in the http header 0.08%

โดยข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทยที่ไม่พบในเดือนธันวาคม 2555 ทั้งสิ้น 4 ประเด็น ดังนี้

1. Allows remote attackers to modify HTTP headers for outgoing requests.
2. Malicious information gathering may assist future attacks.
3. The attacker can execute an arbitrary program on infected systems.
4. Unauthorized access to the affected system.

ตารางที่ 4.4 ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนเมษายน 2556 (ประเทศไทย)

Anomaly and Attack Patterns at HQ of Thailand (Apr, 2013)	
Attack Pattern	**Percentage**
A remote attacker could execute arbitrary code on a victim system.	4.50
A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system.	2.75
Allows remote attackers to modify HTTP headers for outgoing requests.	2.50
Anomaly with HTTP.	12.85
Attempt to exploit memory corruption vulnerability.	1.02
Attempt to exploit memory corruption vulnerability in Microsoft Excel.	7.59
Denial of Service.	8.66
Denial of service: (application crash).	2.58
Denial of Service: File Transfer Protocol (FTP).	2.02
Denial of service: memory corruption.	1.10
Information disclosure: attackers gain full path information of the document root on the victim system.	12.30
Malicious information gathering may assist future attacks.	1.02
Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection.	0.00
Stack overflow in the http header.	1.80
The attacker can execute an arbitrary program on infected systems.	0.00
The Remote attackers can gain control of vulnerable systems.	8.82
Unauthorized access to the affected system .	0.00
Unauthorized access to the server.	12.09
Unexpected network communication.	16.10
Vulnerability in Microsoft PowerPoint.	2.30
Total	100.00



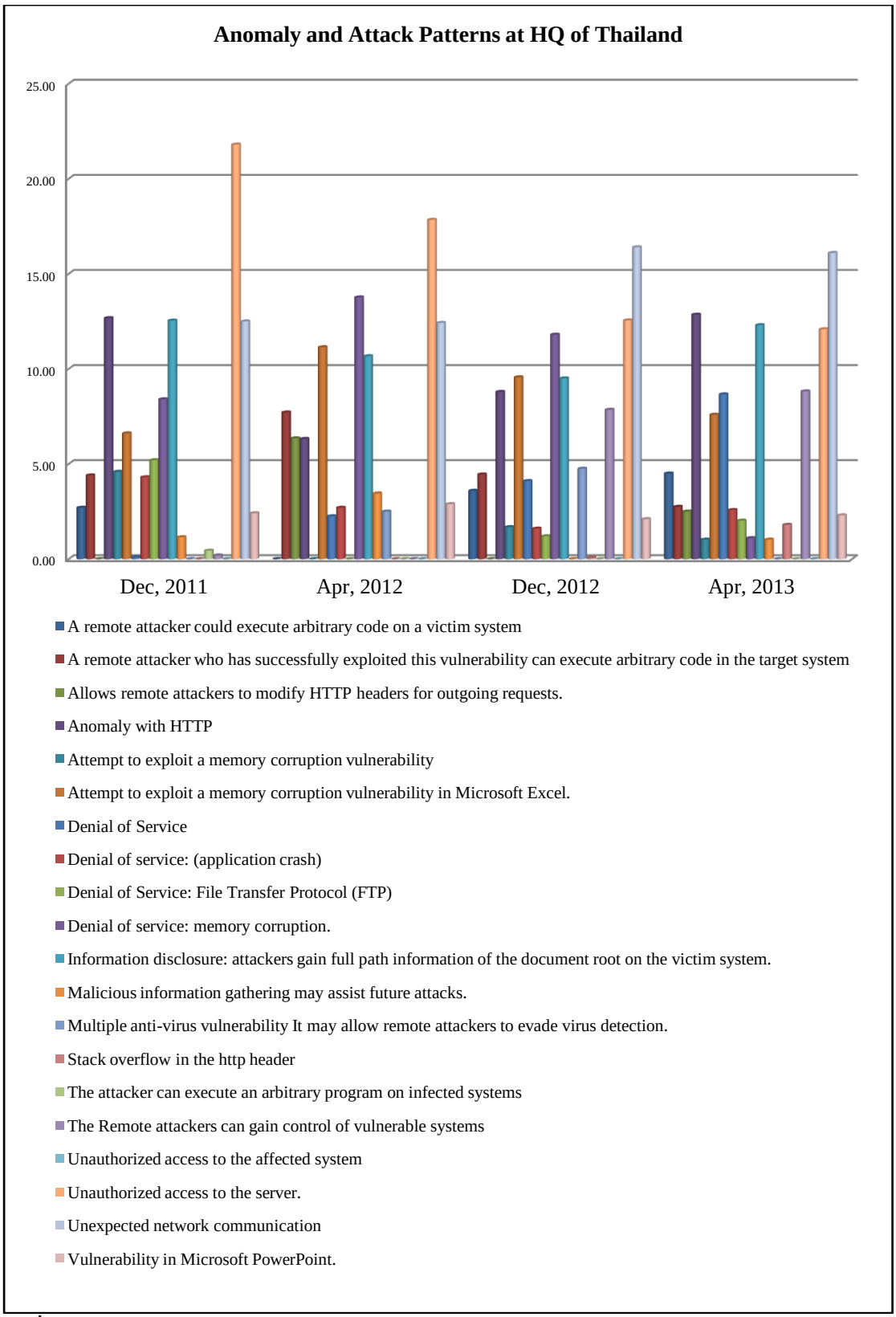
รูปที่ 4.4 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศไทย)

จากตารางที่ 4.4 และรูปที่ 4.4 แสดงให้เห็นว่าข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทยในเดือนเมษายน 2556 นั้น พบความผิดปกติและโอกาสการถูกโจมตีที่หลากหลายทั้งสิ้น 17 ประเด็น ดังนี้

1. Unexpected network communication 16.10%
2. Anomaly with HTTP 12.85%
3. Information disclosure: attackers gain full path information of the document root on the victim system 12.30%
4. Unauthorized access to the server 12.09%
5. The Remote attackers can gain control of vulnerable systems 8.82%
6. Denial of Service 8.66%
7. Attempt to exploit a memory corruption vulnerability in Microsoft Excel 7.59%
8. A remote attacker could execute arbitrary code on a victim system 4.50%
9. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system 2.75%
10. Denial of service: (application crash) 2.58%
11. Allows remote attackers to modify HTTP headers for outgoing requests 2.50%
12. Vulnerability in Microsoft PowerPoint 2.30%
13. Denial of Service: File Transfer Protocol (FTP) 2.02%
14. Stack overflow in the http header 1.80%
15. Denial of service: memory corruption 1.10%
16. Attempt to exploit a memory corruption vulnerability 1.02%
17. Malicious information gathering may assist future attacks 1.02%

โดยข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศไทยที่ไม่พบในเดือนเมษายน 2556 ทั้งสิ้น 3 ประเด็น ดังนี้

1. Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection.
2. The attacker can execute an arbitrary program on infected systems.
3. Unauthorized access to the affected system.



รูปที่ 4.5 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูลประเทศไทย เดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556

จากรูปที่ 4.5 แสดงให้เห็นประเด็นความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ที่ไม่เคยเกิดขึ้นเลยในประเทศไทยคือ Unauthorized access to the affected system

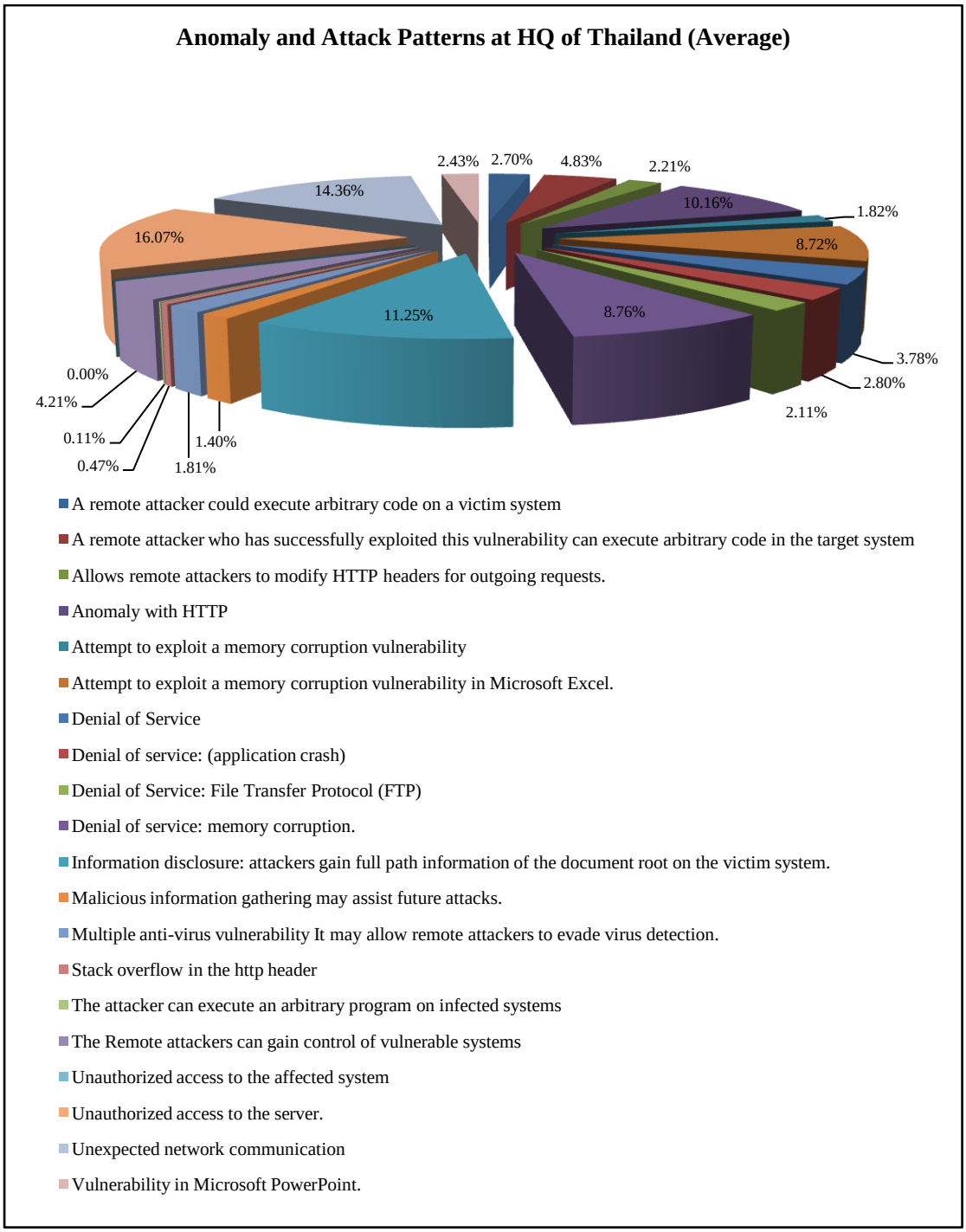
ประเด็นความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์เฉลี่ยในฐานข้อมูลเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ที่เกิดขึ้นในประเทศไทยทุกชุดข้อมูล ทั้งสิ้น 10 ประเด็น เรียงตามลำดับได้ดังนี้

1. Unauthorized access to the server ด้วยอัตรา 16.07%
2. Unexpected network communication ด้วยอัตรา 14.34%
3. Information disclosure: attackers gain full path information of the document root on the victim system ด้วยอัตรา 11.25%
4. Anomaly with HTTP ด้วยอัตรา 10.16%
5. Denial of service: memory corruption ด้วยอัตรา 8.77%
6. Attempt to exploit a memory corruption vulnerability in Microsoft Excel ด้วยอัตรา 8.73%
7. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system ด้วยอัตรา 4.83%
8. Denial of Service ด้วยอัตรา 3.78%
9. Denial of service: (application crash) ด้วยอัตรา 2.80%
10. Vulnerability in Microsoft PowerPoint ด้วยอัตรา 2.43%

จากรูปที่ 4.6 แสดงให้เห็นว่าความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์เฉลี่ยในฐานข้อมูลเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 (ประเทศไทย) สูงสุด 5 อันดับแรกคือ

1. Unauthorized access to the server ด้วยอัตรา 16.07%
2. Unexpected network communication ด้วยอัตรา 14.34%
3. Information disclosure: attackers gain full path information of the document root on the victim system ด้วยอัตรา 11.25%
4. Anomaly with HTTP ด้วยอัตรา 10.16%
5. Denial of service: memory corruption ด้วยอัตรา 8.77%

และประเด็นความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์เฉลี่ยในฐานข้อมูลเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ที่ไม่เคยเกิดขึ้นเลยในประเทศไทยคือ Unauthorized access to the affected system



รูปที่ 4.6 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูลแบบเฉลี่ย (ประเทศไทย)

ตารางที่ 4.5 ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนธันวาคม 2554 (ประเทศที่ร่วมทดสอบ)

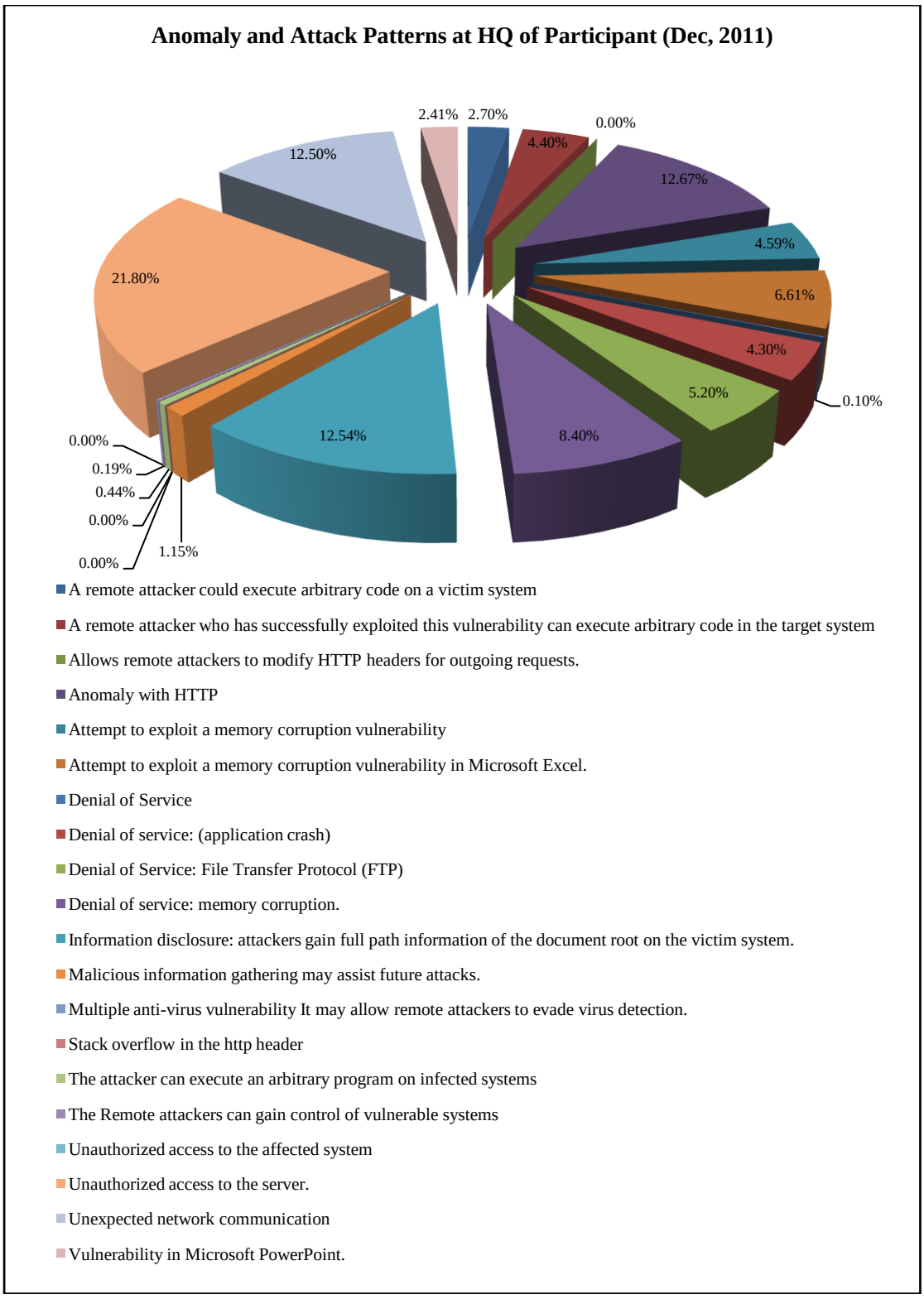
Anomaly and Attack Patterns at HQ of Participant (Dec, 2011)	
Attack Pattern	**Percentage**
A remote attacker could execute arbitrary code on a victim system.	2.70
A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system.	6.50
Allows remote attackers to modify HTTP headers for outgoing requests.	0.00
Anomaly with HTTP.	15.50
Attempt to exploit memory corruption vulnerability.	8.50
Attempt to exploit memory corruption vulnerability in Microsoft Excel.	0.00
Denial of Service.	0.10
Denial of service: (application crash).	4.28
Denial of Service: File Transfer Protocol (FTP).	5.20
Denial of service: memory corruption.	12.40
Information disclosure: attackers gain full path information of the document root on the victim system.	0.00
Malicious information gathering may assist future attacks.	1.15
Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection.	0.00
Stack overflow in the http header.	15.02
The attacker can execute an arbitrary program on infected systems.	0.44
The Remote attackers can gain control of vulnerable systems.	0.19
Unauthorized access to the affected system.	0.00
Unauthorized access to the server.	15.50
Unexpected network communication.	12.50
Vulnerability in Microsoft PowerPoint.	0.00
Total	100.00

จากตารางที่ 4.5 และรูปที่ 4.7 แสดงให้เห็นว่าข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2554 นั้น พบความผิดปกติและโอกาสการถูกโจมตีที่หลากหลายทั้งสิ้น 14 ประเด็น ดังนี้

1. Anomaly with HTTP 15.50%
2. Unauthorized access to the server 15.50%
3. Stack overflow in the http header 15.02%
4. Unexpected network communication 12.50%
5. Denial of service: memory corruption 12.40%
6. Attempt to exploit a memory corruption vulnerability 8.50%
7. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system 6.50%
8. Denial of Service: File Transfer Protocol (FTP) 5.20%
9. Denial of service: (application crash) 4.30%
10. A remote attacker could execute arbitrary code on a victim system 2.70%
11. Malicious information gathering may assist future attacks 1.15%
12. The attacker can execute an arbitrary program on infected systems 0.44%
13. The Remote attackers can gain control of vulnerable systems 0.19%
14. Denial of Service 0.10%

โดยข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบที่ไม่พบในเดือนธันวาคม 2554 ทั้งสิ้น 6 ประเด็น ดังนี้

1. Allows remote attackers to modify HTTP headers for outgoing requests.
2. Attempt to exploit memory corruption vulnerability in Microsoft Excel.
3. Information disclosure: attackers gain full path information of the document root on the victim system.
4. Multiple anti-virus vulnerability, It may allow remote attackers to evade virus detection.
5. Unauthorized access to the affected system.
6. Vulnerability in Microsoft PowerPoint.



รูปที่ 4.7 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนธันวาคม 2554 (ประเทศที่ร่วมทดสอบ)

ตารางที่ 4.6 ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนเมษายน 2555 (ประเทศที่ร่วมทดสอบ)

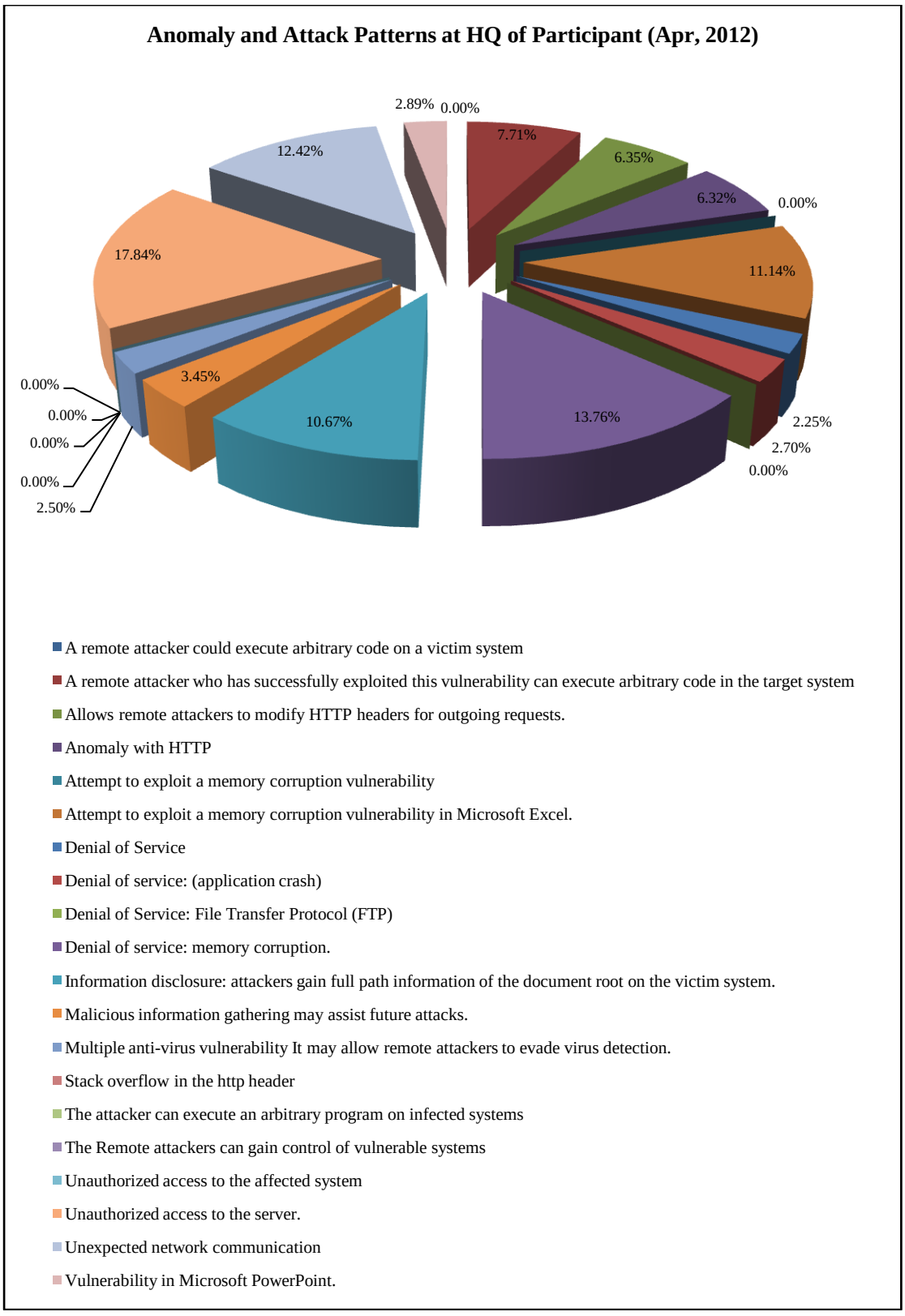
Anomaly and Attack Patterns at HQ of Participant (Apr, 2012)	
Attack Pattern	**Percentage**
A remote attacker could execute arbitrary code on a victim system.	3.50
A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system.	7.71
Allows remote attackers to modify HTTP headers for outgoing requests.	0.00
Anomaly with HTTP.	17.90
Attempt to exploit memory corruption vulnerability.	7.50
Attempt to exploit memory corruption vulnerability in Microsoft Excel.	0.00
Denial of Service.	2.25
Denial of service: (application crash).	2.70
Denial of Service: File Transfer Protocol (FTP).	0.00
Denial of service: memory corruption.	13.76
Information disclosure: attackers gain full path information of the document root on the victim system.	0.00
Malicious information gathering may assist future attacks.	2.20
Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection.	2.50
Stack overflow in the http header.	12.14
The attacker can execute an arbitrary program on infected systems.	0.00
The Remote attackers can gain control of vulnerable systems.	0.00
Unauthorized access to the affected system.	0.00
Unauthorized access to the server.	17.84
Unexpected network communication.	10.00
Vulnerability in Microsoft PowerPoint.	0.00
Total	100.00

จากตารางที่ 4.6 และรูปที่ 4.8 แสดงให้เห็นว่าข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบในเดือนเมษายน 2555 นั้น พบความผิดปกติและโอกาสการถูกโจมตีที่หลากหลายทั้งสิ้น 12 ประเด็น ดังนี้

1. Anomaly with HTTP 17.90%
2. Unauthorized access to the server 17.84%
3. Denial of service: memory corruption 13.76%
4. Stack overflow in the http header 12.14%
5. Unexpected network communication 10.00%
6. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system 7.71%
7. Attempt to exploit a memory corruption vulnerability 7.50%
8. A remote attacker could execute arbitrary code on a victim system 3.50%
9. Denial of service: (application crash) 2.70%
10. Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection 2.50%
11. Denial of Service 2.25%
12. Malicious information gathering may assist future attacks 2.20%

โดยข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบที่ไม่พบในเดือนเมษายน 2555 ทั้งสิ้น 8 ประเด็น ดังนี้

1. Allows remote attackers to modify HTTP headers for outgoing requests.
2. Attempt to exploit memory corruption vulnerability in Microsoft Excel.
3. Denial of Service: File Transfer Protocol (FTP).
4. Information disclosure: attackers gain full path information of the document root on the victim system.
5. The attacker can execute an arbitrary program on infected systems.
6. The Remote attackers can gain control of vulnerable systems.
7. Unauthorized access to the affected system.
8. Vulnerability in Microsoft PowerPoint.



รูปที่ 4.8 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนเมษายน 2555 (ประเทศที่ร่วมทดสอบ)

ตารางที่ 4.7 ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนธันวาคม 2555 (ประเทศที่ร่วมทดสอบ)

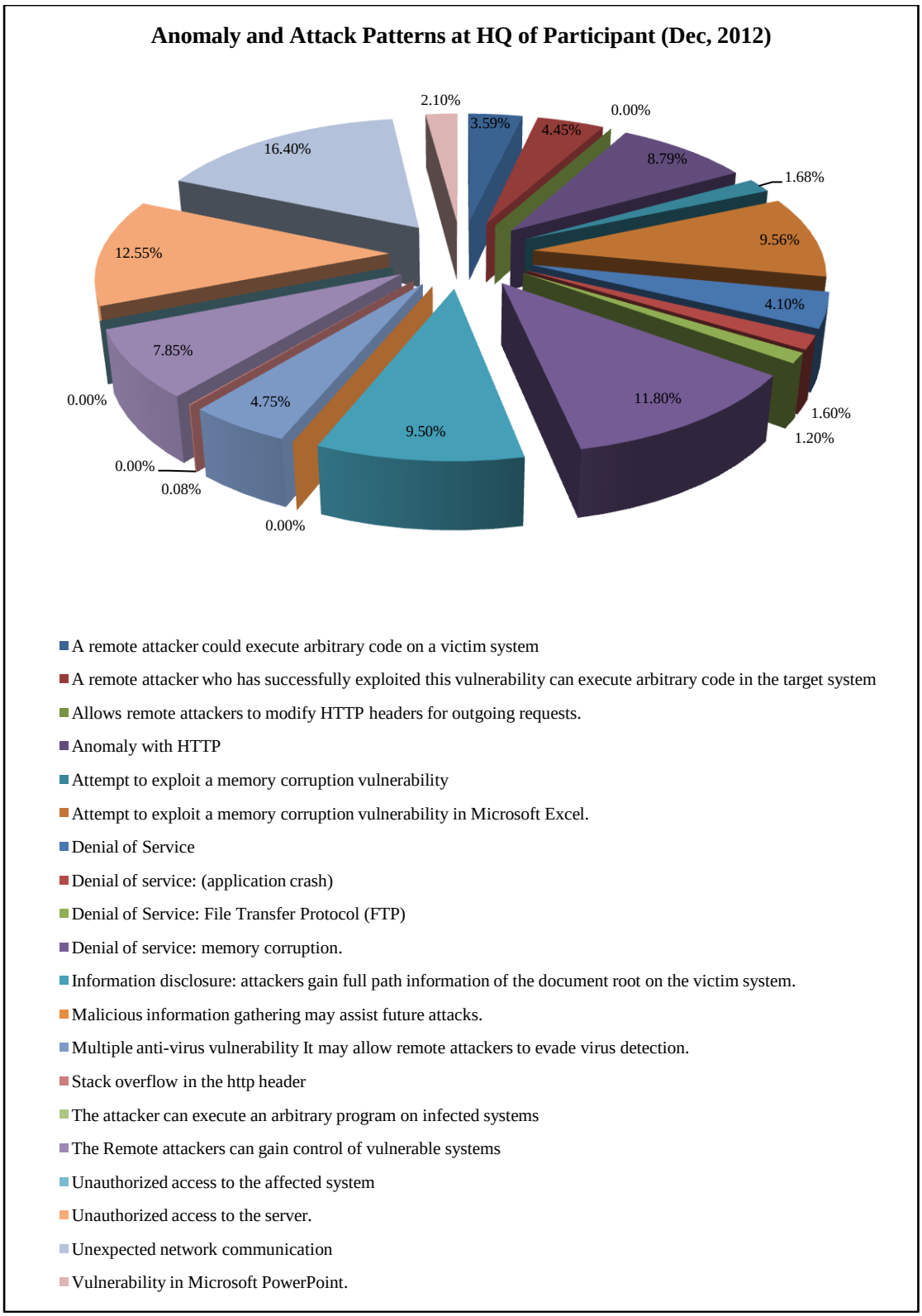
Anomaly and Attack Patterns at HQ of Participant (Dec, 2012)	
Attack Pattern	**Percentage**
A remote attacker could execute arbitrary code on a victim system.	3.59
A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system.	8.50
Allows remote attackers to modify HTTP headers for outgoing requests.	0.00
Anomaly with HTTP.	16.80
Attempt to exploit memory corruption vulnerability.	6.50
Attempt to exploit memory corruption vulnerability in Microsoft Excel.	0.00
Denial of Service.	4.10
Denial of service: (application crash).	1.60
Denial of Service: File Transfer Protocol (FTP).	1.20
Denial of service: memory corruption.	11.80
Information disclosure: attackers gain full path information of the document root on the victim system.	0.00
Malicious information gathering may assist future attacks.	2.10
Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection.	4.75
Stack overflow in the http header.	9.16
The attacker can execute an arbitrary program on infected systems.	0.00
The Remote attackers can gain control of vulnerable systems.	7.85
Unauthorized access to the affected system.	0.00
Unauthorized access to the server.	12.55
Unexpected network communication.	9.50
Vulnerability in Microsoft PowerPoint.	0.00
Total	100.00

จากตารางที่ 4.7 และรูปที่ 4.9 แสดงให้เห็นว่าข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2555 นั้น พบความผิดปกติและโอกาสการถูกโจมตีที่หลากหลายทั้งสิ้น 14 ประเด็น ดังนี้

1. Anomaly with HTTP 16.80%
2. Unauthorized access to the server 12.55%
3. Denial of service: memory corruption 11.80%
4. Unexpected network communication 9.50%
5. Stack overflow in the http header 9.16%
6. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system 8.50%
7. The Remote attackers can gain control of vulnerable systems 7.85%
8. Attempt to exploit a memory corruption vulnerability 6.50%
9. Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection 4.75%
10. Denial of Service 4.10%
11. A remote attacker could execute arbitrary code on a victim system 3.59%
12. Malicious information gathering may assist future attacks 2.10%
13. Denial of service: (application crash) 1.60%
14. Denial of Service: File Transfer Protocol (FTP) 1.20%

โดยข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบที่ไม่พบในเดือนธันวาคม 2555 ทั้งสิ้น 6 ประเด็น ดังนี้

1. Allows remote attackers to modify HTTP headers for outgoing requests.
2. Attempt to exploit memory corruption vulnerability in Microsoft Excel.
3. Information disclosure: attackers gain full path information of the document root on the victim system.
4. The attacker can execute an arbitrary program on infected systems.
5. Unauthorized access to the affected system.
6. Vulnerability in Microsoft PowerPoint.



รูปที่ 4.9 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนธันวาคม 2555 (ประเทศที่ร่วมทดสอบ)

ตารางที่ 4.8 ความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนเมษายน 2556 (ประเทศที่ร่วมทดสอบ)

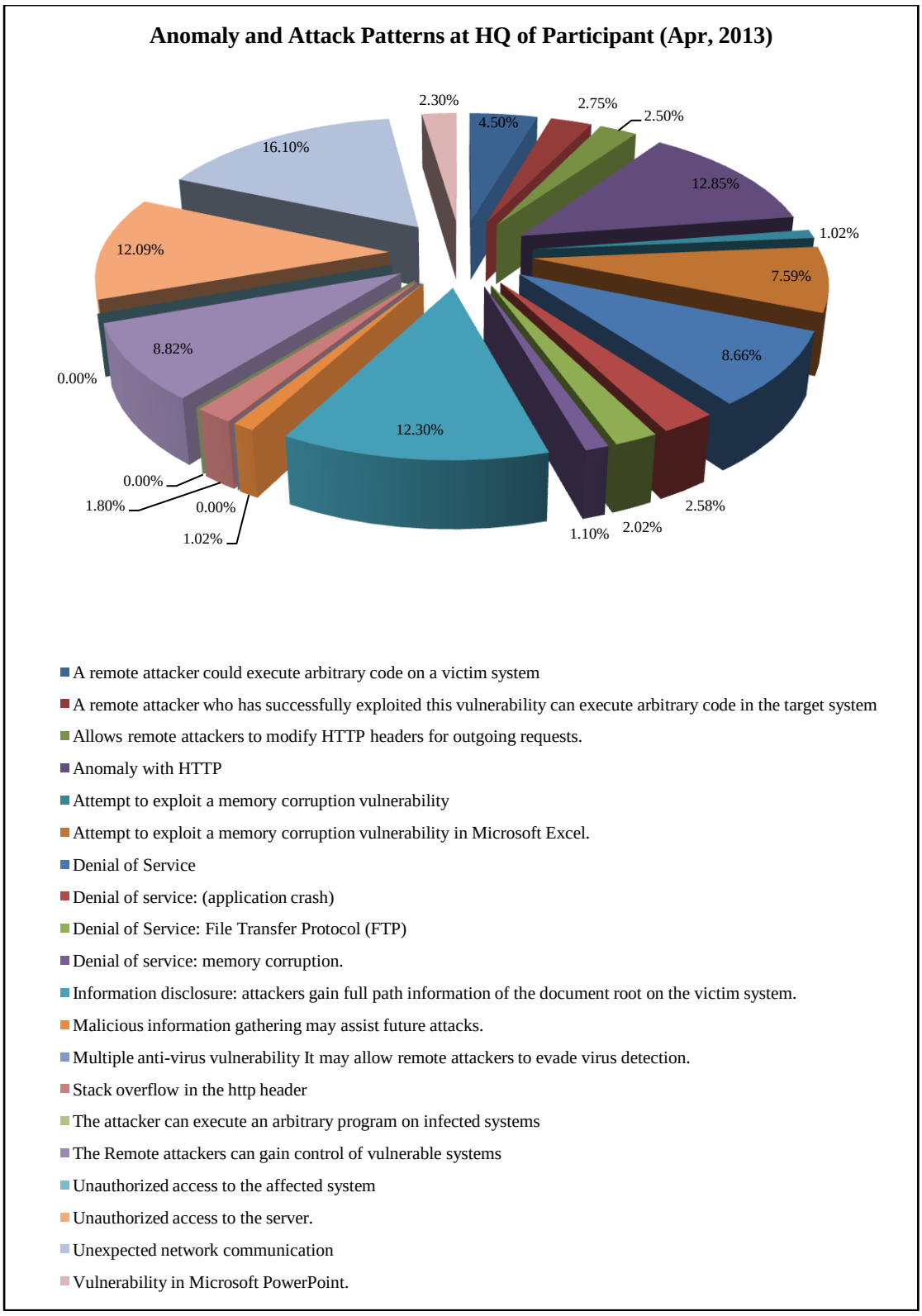
Anomaly and Attack Patterns at HQ of Participant (Apr, 2013)	
Attack Pattern	**Percentage**
A remote attacker could execute arbitrary code on a victim system.	4.50
A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system.	7.00
Allows remote attackers to modify HTTP headers for outgoing requests.	0.00
Anomaly with HTTP.	15.50
Attempt to exploit memory corruption vulnerability.	7.00
Attempt to exploit memory corruption vulnerability in Microsoft Excel.	0.00
Denial of Service.	8.66
Denial of service: (application crash).	2.58
Denial of Service: File Transfer Protocol (FTP).	2.02
Denial of service: memory corruption.	1.10
Information disclosure: attackers gain full path information of the document root on the victim system.	0.00
Malicious information gathering may assist future attacks.	1.90
Multiple anti-virus vulnerability It may allow remote attackers to evade virus detection.	0.00
Stack overflow in the http header.	20.83
The attacker can execute an arbitrary program on infected systems.	0.00
The Remote attackers can gain control of vulnerable systems.	8.82
Unauthorized access to the affected system.	0.00
Unauthorized access to the server.	12.09
Unexpected network communication.	8.00
Vulnerability in Microsoft PowerPoint.	0.00
Total	100.00

จากตารางที่ 4.8 และรูปที่ 4.10 แสดงให้เห็นว่าข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบในเดือนเมษายน 2556 นั้น พบความผิดปกติและโอกาสการถูกโจมตีที่หลากหลายทั้งสิ้น 13 ประเด็น ดังนี้

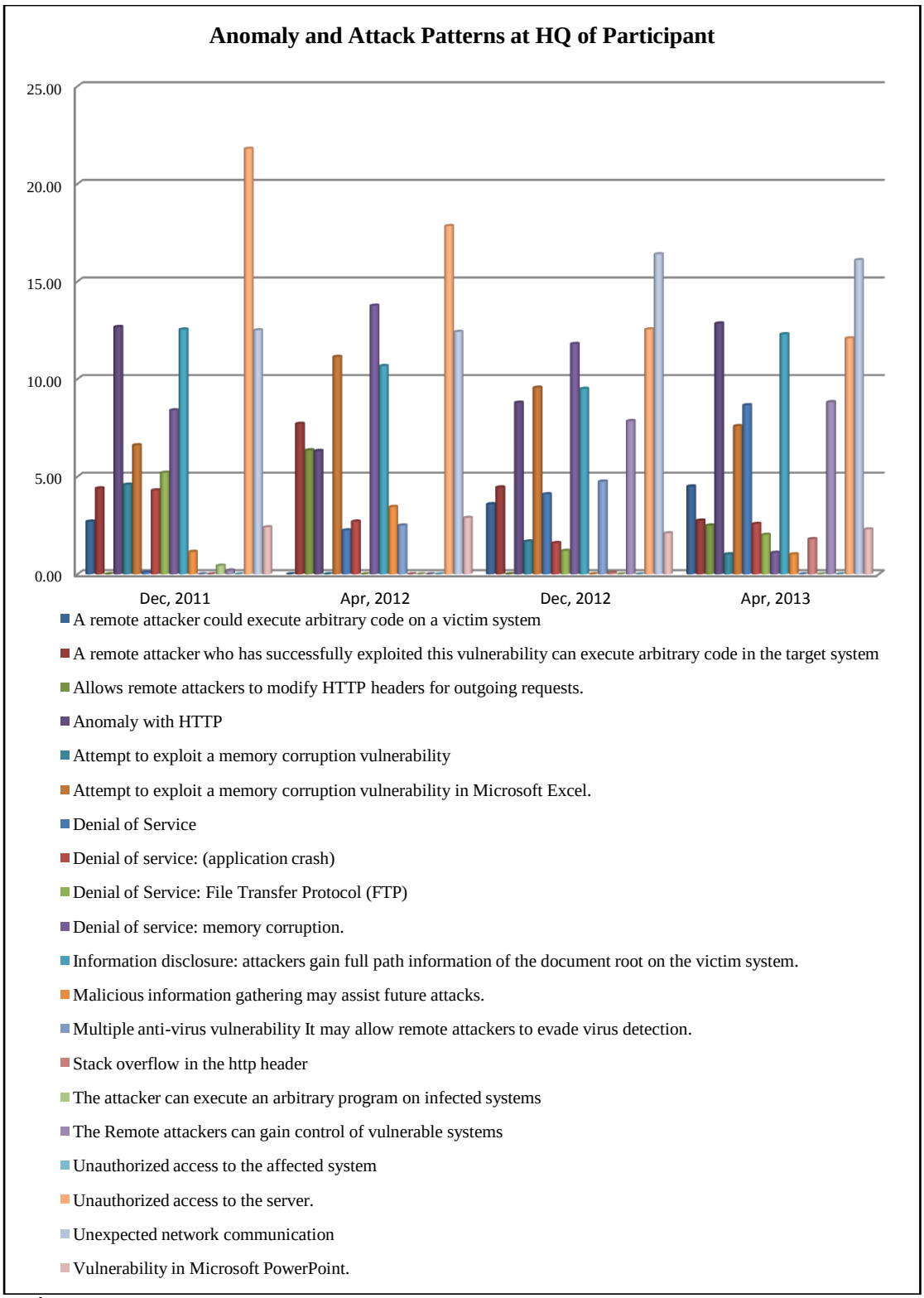
1. Stack overflow in the http header 20.83%
2. Anomaly with HTTP 15.50%
3. Unauthorized access to the server 12.09%
4. The Remote attackers can gain control of vulnerable systems 8.82%
5. Denial of Service 8.66%
6. Unexpected network communication 8.00%
7. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system 7.00%
8. Attempt to exploit a memory corruption vulnerability 7.00%
9. A remote attacker could execute arbitrary code on a victim system 4.50%
10. Denial of service: (application crash) 2.58%
11. Denial of Service: File Transfer Protocol (FTP) 2.02%
12. Malicious information gathering may assist future attacks 1.90%
13. Denial of service: memory corruption 1.10%

โดยข้อมูลความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบที่ไม่พบในเดือนเมษายน 2556 ทั้งสิ้น 7 ประเด็น ดังนี้

1. Allows remote attackers to modify HTTP headers for outgoing requests.
2. Attempt to exploit memory corruption vulnerability in Microsoft Excel.
3. Information disclosure: attackers gain full path information of the document root on the victim system.
4. Multiple anti-virus vulnerability, It may allow remote attackers to evade virus detection.
5. The attacker can execute an arbitrary program on infected systems.
6. Unauthorized access to the affected system.
7. Vulnerability in Microsoft PowerPoint.



รูปที่ 4.10 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล เดือนเมษายน 2556 (ประเทศที่ร่วมทดสอบ)



รูปที่ 4.11 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.11 แสดงให้เห็นประเด็นความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ที่ไม่เคยเกิดขึ้นเลยในประเทศที่ร่วมทดสอบคือ

1. Allows remote attackers to modify HTTP headers for outgoing requests.
2. Attempt to exploit memory corruption vulnerability in Microsoft Excel.
3. Information disclosure: attackers gain full path information of the document root on the victim system.
4. Unauthorized access to the affected system.
5. Vulnerability in Microsoft PowerPoint.

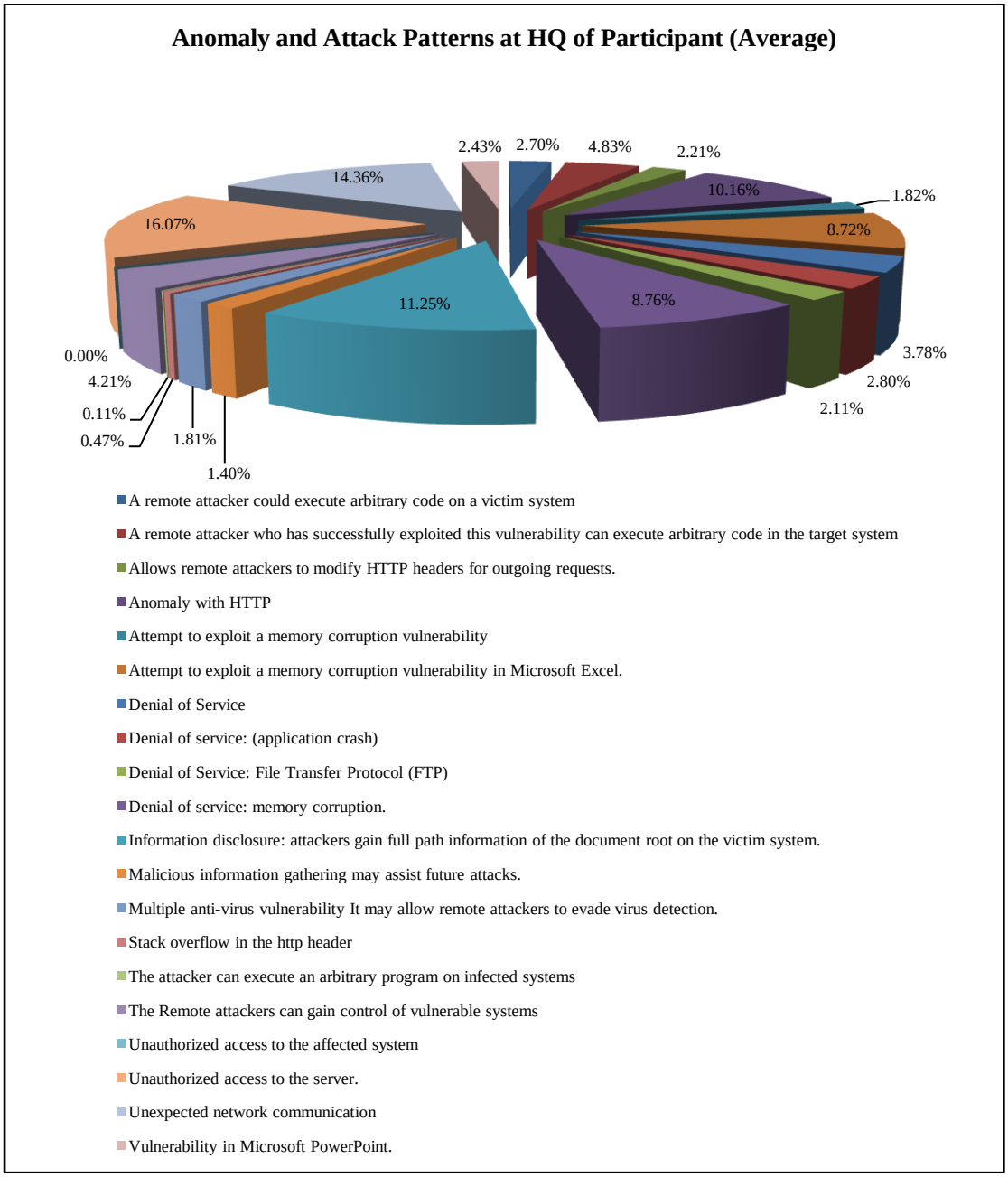
ประเด็นความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์เฉลี่ยในฐานข้อมูลเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ที่เกิดขึ้นในประเทศที่ร่วมทดสอบทุกชุดข้อมูล เรียงตามลำดับได้ดังนี้

1. Anomaly with HTTP ด้วยอัตรา 16.43%
2. Unauthorized access to the server. ด้วยอัตรา 14.50%
3. Stack overflow in the http header ด้วยอัตรา 14.27%
4. Unexpected network communication ด้วยอัตรา 10.00%
5. Denial of service: memory corruption. ด้วยอัตรา 9.77%
6. A remote attacker who has successfully exploited this vulnerability can execute arbitrary code in the target system ด้วยอัตรา 7.43%
7. Attempt to exploit a memory corruption vulnerability ด้วยอัตรา 7.38%
8. Denial of Service ด้วยอัตรา 3.78%
9. A remote attacker could execute arbitrary code on a victim system ด้วยอัตรา 3.57%
10. Denial of service: (application crash) ด้วยอัตรา 2.80%
11. Malicious information gathering may assist future attacks ด้วยอัตรา 1.84%

จากรูปที่ 4.12 แสดงให้เห็นประเด็นความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์เฉลี่ยในฐานข้อมูลเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 (ประเทศที่ร่วมทดสอบ) สูงสุด 5 อันดับแรก ดังนี้

1. Anomaly with HTTP ด้วยอัตรา 16.43%

2. Unauthorized access to the server. ด้วยอัตรา 14.50%
3. Stack overflow in the http header ด้วยอัตรา 14.27%
4. Unexpected network communication ด้วยอัตรา 10.00%
5. Denial of service: memory corruption. ด้วยอัตรา 9.77%



รูปที่ 4.12 กราฟความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูลแบบเฉลี่ย (ประเทศที่ร่วมทดสอบ)

โดยประเด็นความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์เฉลี่ยในฐานข้อมูลเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ที่ไม่เคยเกิดขึ้นเลยในประเทศที่ร่วมทดสอบคือ

1. Allows remote attackers to modify HTTP headers for outgoing requests.
2. Attempt to exploit memory corruption vulnerability in Microsoft Excel.
3. Information disclosure: attackers gain full path information of the document root on the victim system.
4. Unauthorized access to the affected system.
5. Vulnerability in Microsoft PowerPoint.

4.2 รูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์

จากวัตถุประสงค์ข้อที่ 2 ซึ่งผู้วิจัยได้ทำการศึกษาและวิเคราะห์ฐานข้อมูลเพื่อค้นหารูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูล 2 ประเทศ คือประเทศไทยและประเทศที่ร่วมทดสอบ ด้วยข้อมูล 4 ชุด คือชุดข้อมูลในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังรูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ด้วยหลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm) โดยสามารถนำเสนอความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ และแสดงภาพการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ด้วยหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm โดยมีข้อมูลดังแสดงในรูปประกอบที่ 4.13-4.16 ซึ่งเป็นข้อมูลของประเทศไทยในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 และ 4.17-4.20 ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ตามลำดับ ดังนี้

1. ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ของสมาชิกที่ได้รับความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ของประเทศไทยในเดือนธันวาคม 2554 จำนวน 6,994 โหนด (Nodes) และเส้นความสัมพันธ์ (Edges) จำนวน 21,345 ดังแสดงในรูปที่ 4.13

2. ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ของสมาชิกที่ได้รับความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ของประเทศไทยในเดือนเมษายน 2555 จำนวน 7,035 โหนด (Nodes) และเส้นความสัมพันธ์ (Edges) จำนวน 25,774 ดังแสดงในรูปที่ 4.14

3. ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ของสมาชิกที่ได้รับความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ของประเทศไทยในเดือนธันวาคม 2555 จำนวน 6,939 โหนด (Nodes) และเส้นความสัมพันธ์ (Edges) จำนวน 24,225 ดังแสดงในรูปที่ 4.15

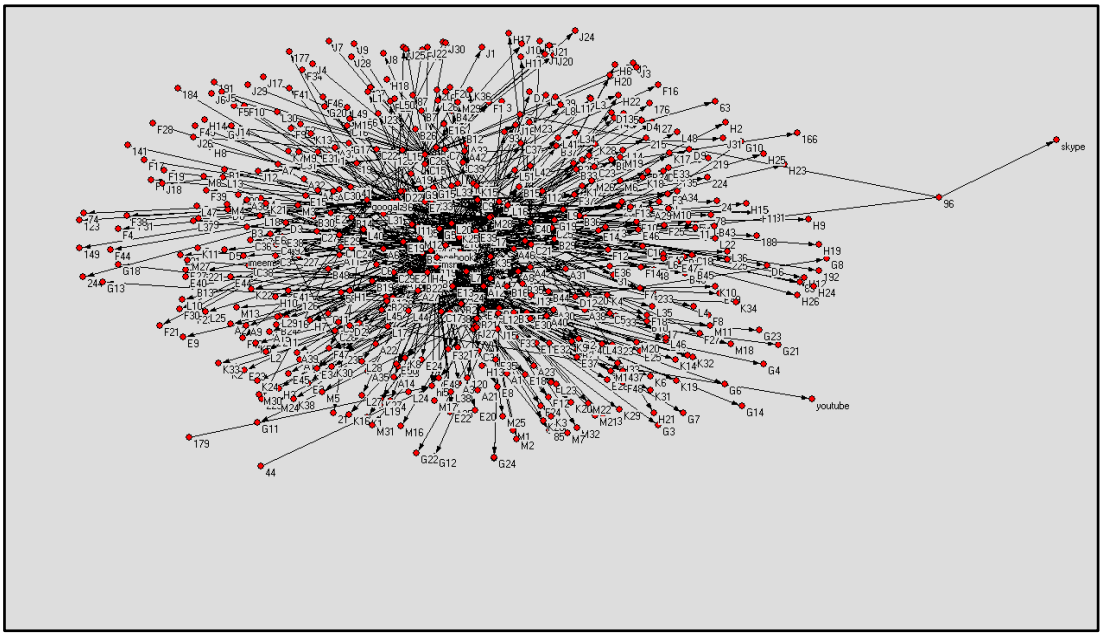
4. ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ของสมาชิกที่ได้รับความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ของประเทศไทยในเดือนเมษายน 2556 จำนวน 8,012 โหนด (Nodes) และเส้นความสัมพันธ์ (Edges) จำนวน 26,106 ดังแสดงในรูปที่ 4.16

5. ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ของสมาชิกที่ได้รับความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2554 จำนวน 8,935 โหนด (Nodes) และเส้นความสัมพันธ์ (Edges) จำนวน 26,779 ดังแสดงในรูปที่ 4.17

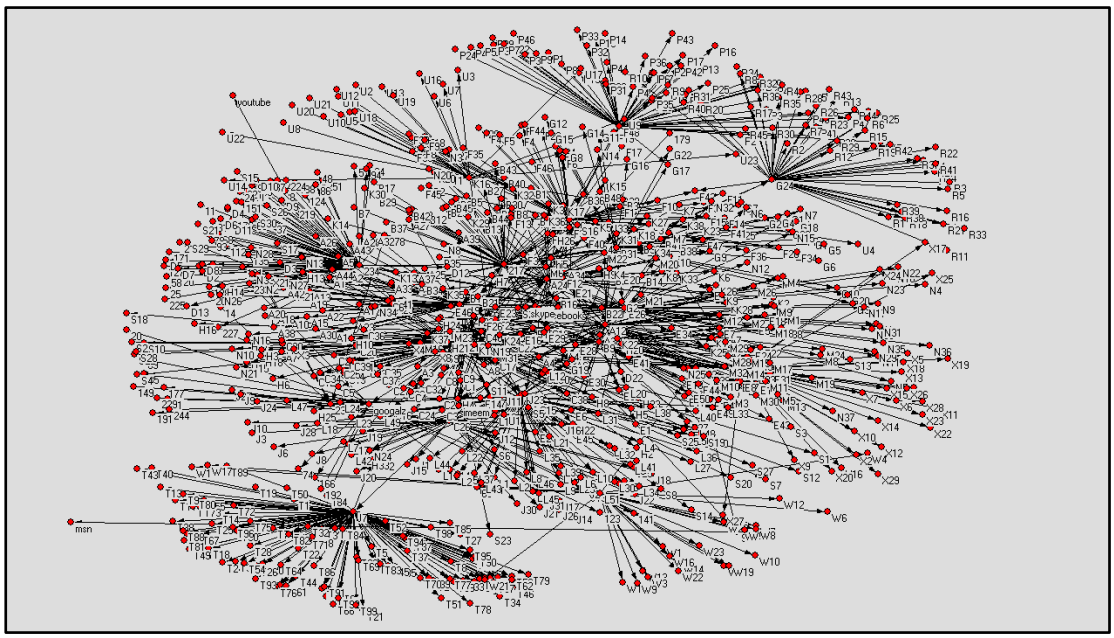
6. ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ของสมาชิกที่ได้รับความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบในเดือนเมษายน 2555 จำนวน 7,935 โหนด (Nodes) และเส้นความสัมพันธ์ (Edges) จำนวน 29,003 ดังแสดงในรูปที่ 4.18

7. ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ของสมาชิกที่ได้รับความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2555 จำนวน 7,845 โหนด (Nodes) และเส้นความสัมพันธ์ (Edges) จำนวน 28,067 ดังแสดงในรูปที่ 4.19

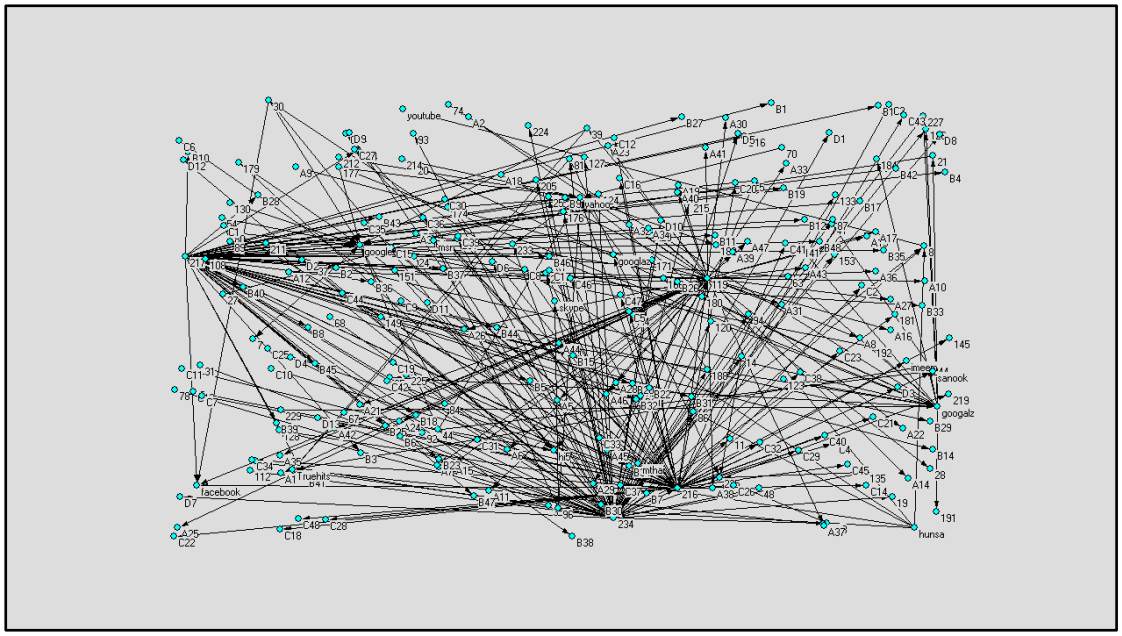
8. ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ของสมาชิกที่ได้รับความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ของประเทศที่ร่วมทดสอบในเดือนเมษายน 2556 จำนวน 7,567 โหนด (Nodes) และเส้นความสัมพันธ์ (Edges) จำนวน 29,432 ดังแสดงในรูปที่ 4.20



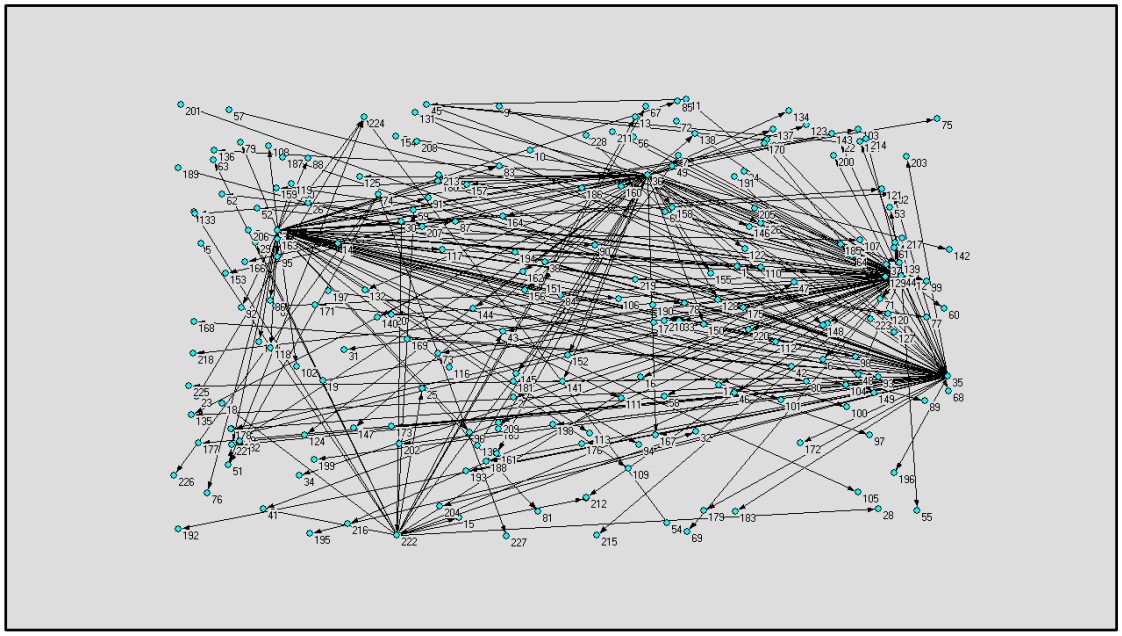
รูปที่ 4.13 ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 (ประเทศไทย)



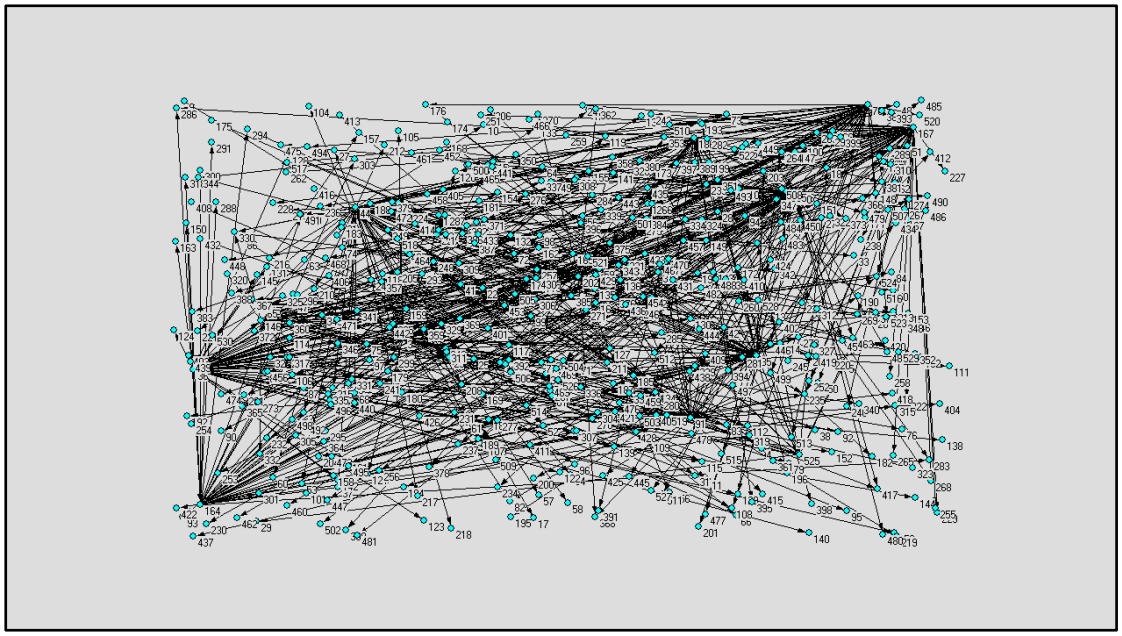
รูปที่ 4.14 ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศไทย)



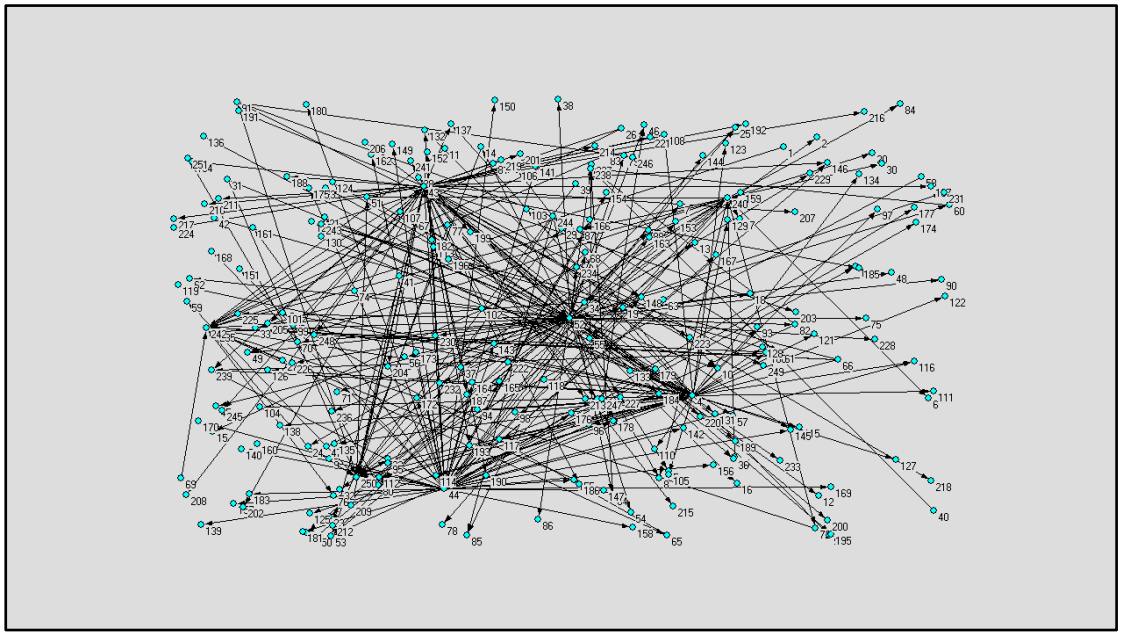
รูปที่ 4.15 ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศไทย)



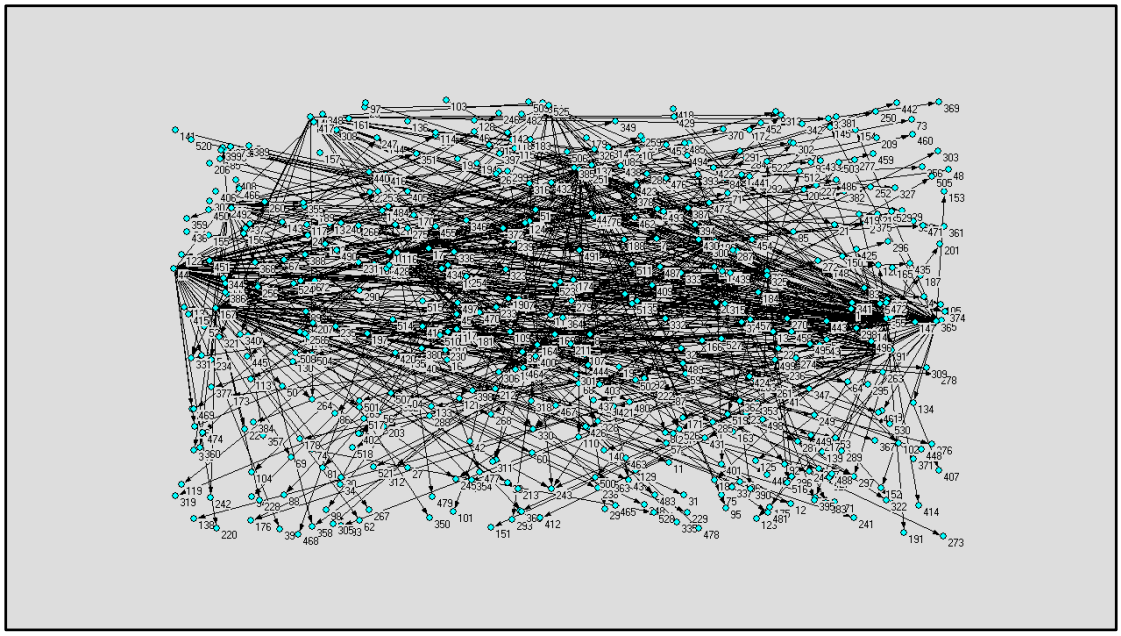
รูปที่ 4.16 ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศไทย)



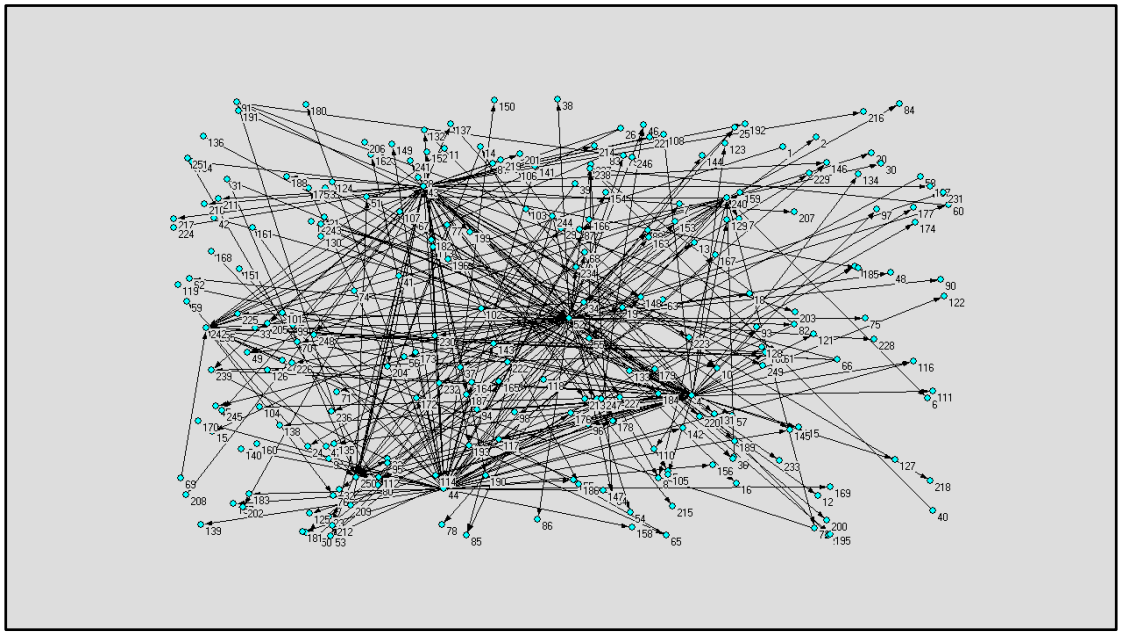
รูปที่ 4.17 ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 (ประเทศที่ร่วมทดสอบ)



รูปที่ 4.18 ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศที่ร่วมทดสอบ)



รูปที่ 4.19 ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศที่ร่วมทดสอบ)



รูปที่ 4.20 ความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศที่ร่วมทดสอบ)

โดยการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีข้อมูลดังแสดงในรูปประกอบที่ 4.21-4.24 ซึ่งเป็นข้อมูลของประเทศไทยในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 และ 4.25-4.28 ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ตามลำดับ

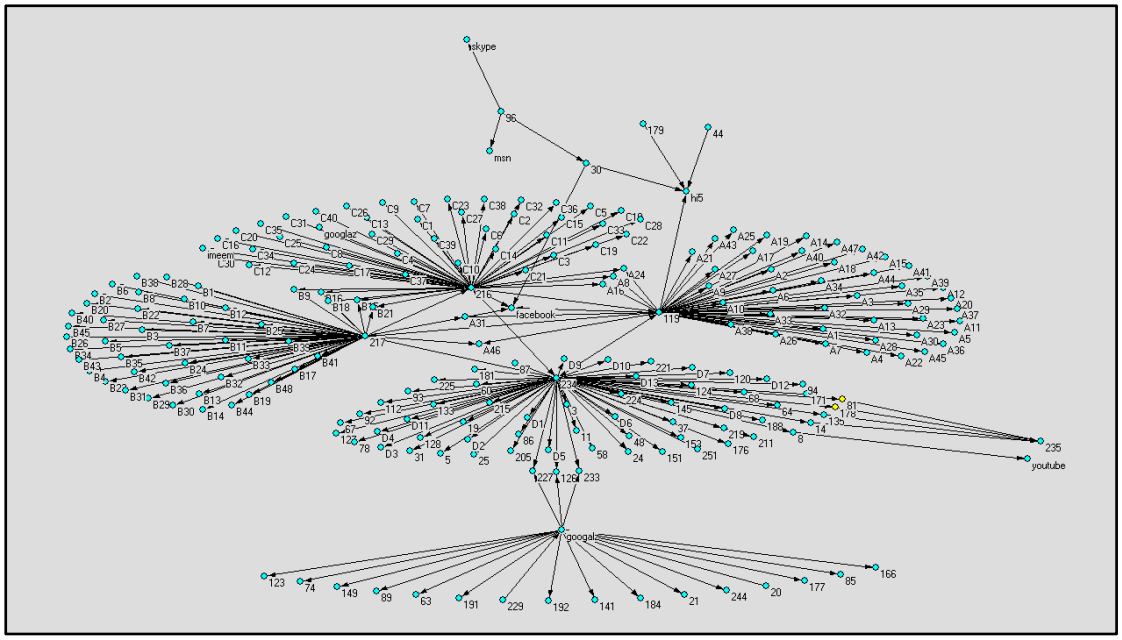
จากรูปที่ 4.21 แสดงให้เห็นการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนธันวาคม 2554 ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) สูงสุด 5 อันดับแรก คือ โหนดหมายเลข 60, 87, 3, 229 และ 224 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) l205, 75, 90, 120, และ 80 หน่วย ตามลำดับ

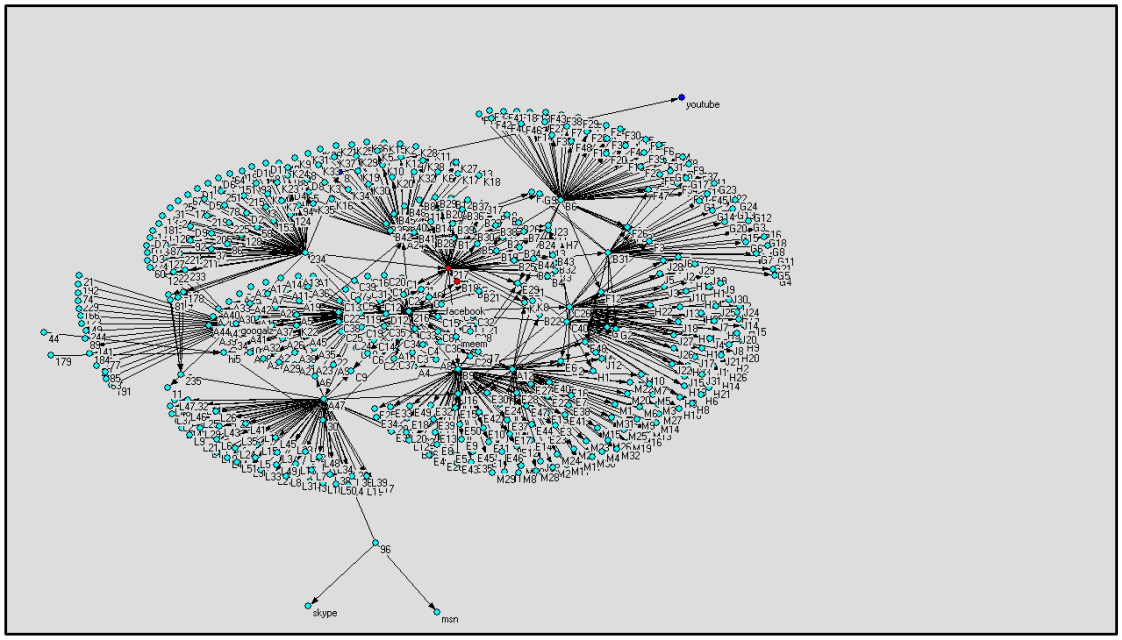
2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) สูงสุด 5 อันดับแรก คือโหนดหมายเลข 234, 99, 217, 229 และ 216 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 1400, 100, 95, 60 และ 75 หน่วย ตามลำดับ

3. โหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารและโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข 99, 119, 217, 216 และ 234 ด้วยค่า Closeness Measure 8.305, 8.436, 8.413, 8.301 และ 8.293 หน่วย ตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 (ประเทศไทย) หากโหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) คือ โหนดหมายเลข 60, 87, 3, 229 และ 224 ได้รับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสมาจากโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 99, 119, 217, 216 และ 234 หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข 234, 99, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 99, 119, 217, 216 และ 234 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes)



รูปที่ 4.21 การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 (ประเทศไทย)



รูปที่ 4.22 การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศไทย)

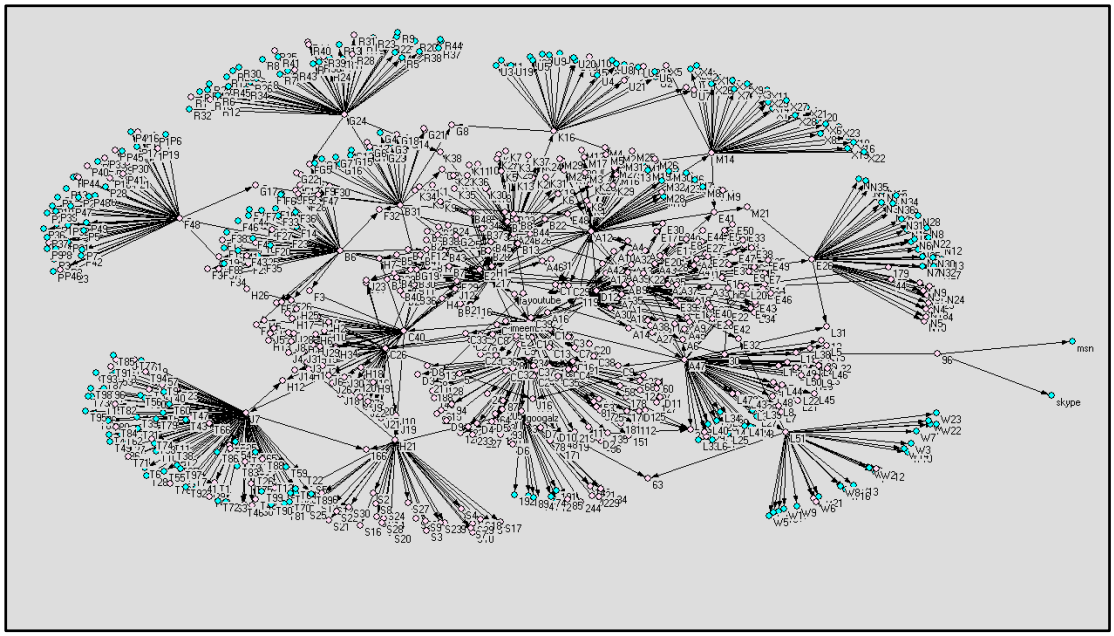
จากรูปที่ 4.22 แสดงให้เห็นการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนเมษายน 2555 ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข 60, 87, 3, googalz และ 224 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) l109, 109, 107, 72, และ 60 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข 234, J7, 217, 229 และ 216 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 1451, 101, 75, 68 และ 61 หน่วย ตามลำดับ

3. โหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ด้วยค่า Closeness Measures 8.456, 8.436, 8.413, 8.301 และ 8.293 หน่วย ตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศไทย) หากโหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) คือ โหนดหมายเลข 60, 87, 3, googalz และ 224 ได้รับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสมาจากโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 119, 217, 216, 171 และ 234 หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข 234, J7, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes)



รูปที่ 4.23 การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศไทย)

จากรูปที่ 4.23 แสดงให้เห็นการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนธันวาคม 2555 ดังนี้

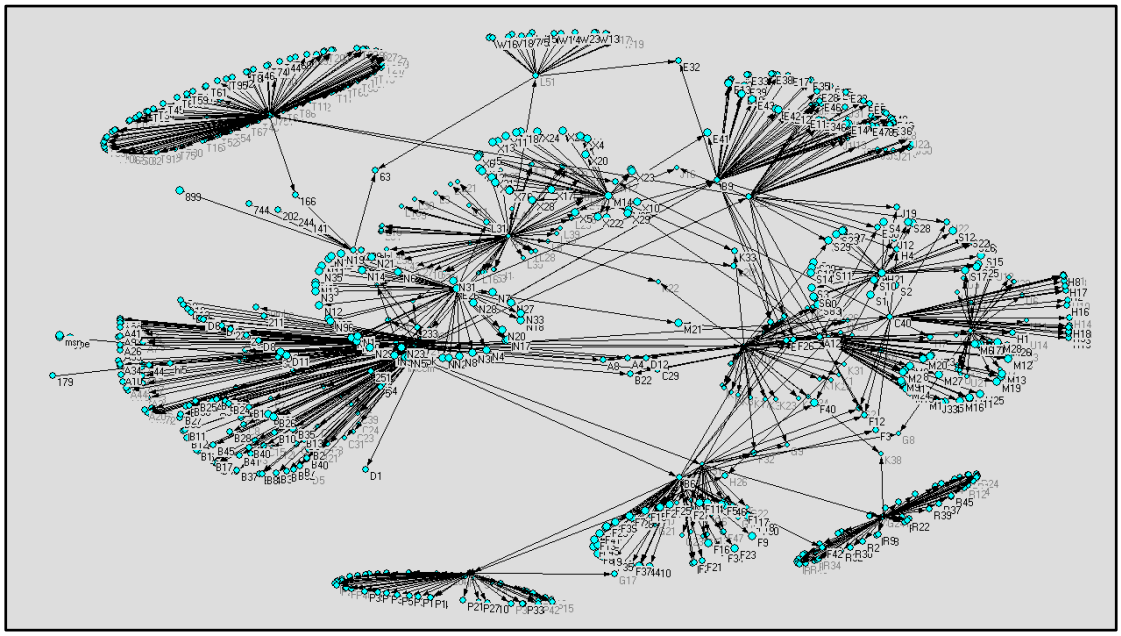
1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข 60, 87, 3, 90 และ 224 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 90, 129, 79, 72, และ 90 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข 234, 90, 217, 229 และ 216 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 1200, 501, 275, 168 และ 55 หน่วย ตามลำดับ

3. โหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ด้วยค่า Closeness Measures 8.293 , 8.436, 8.301, 8.413 และ 8.456 หน่วย ตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศไทย) หากโหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) คือ โหนดหมายเลข 60, 87, 3, 90 และ 224 ได้รับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคม

ออนไลน์มีโอกาสมาจากโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 119, 217, 216, 171 และ 234 หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข 234, 90, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes)



รูปที่ 4.24 การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศไทย)

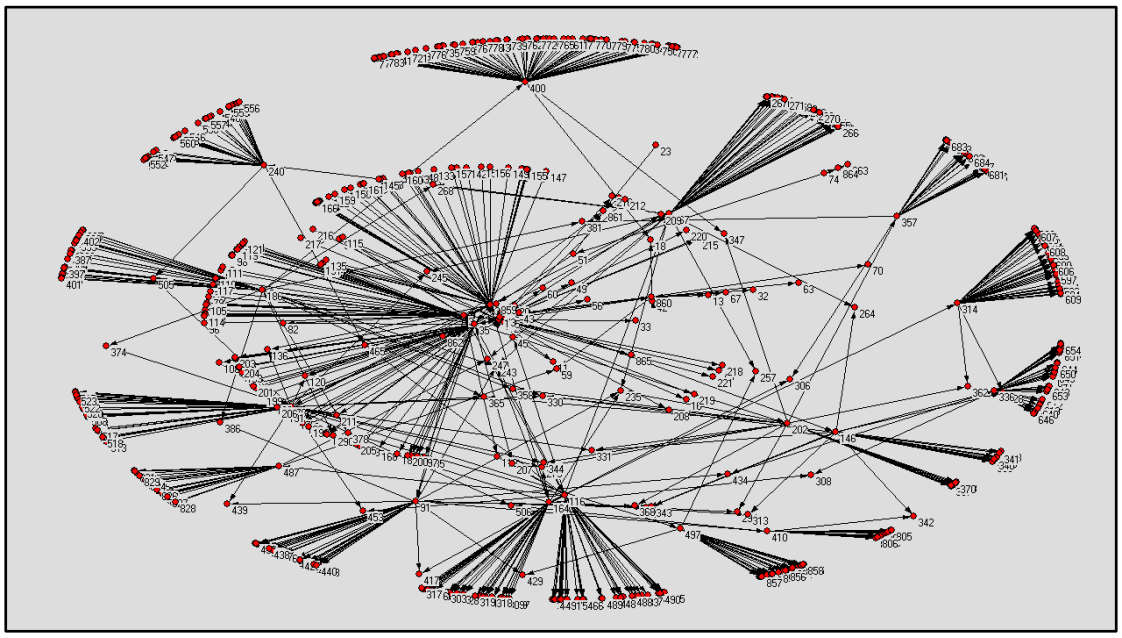
จากรูปที่ 4.24 แสดงให้เห็นการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนเมษายน 2556 ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข 129, 87, 3, 90 และ 224 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 105, 79, 99, 102, และ 85 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือ โหนดหมายเลข 234, 90, 217, 229 และ 216 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 200, 51, 75, 78 และ 95 หน่วย ตามลำดับ

3. โหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ด้วยค่า Closeness Measures 8.301, 8.436, 8.293, 8.456 และ 8.413 หน่วย ตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศไทย) หากโหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) คือ โหนดหมายเลข 129, 87, 3, 90 และ 224 ได้รับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสมาจากโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 119, 217, 216, 171 และ 234 หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข 234, 90, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes)



รูปที่ 4.25 การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 (ประเทศที่ร่วมทดสอบ)

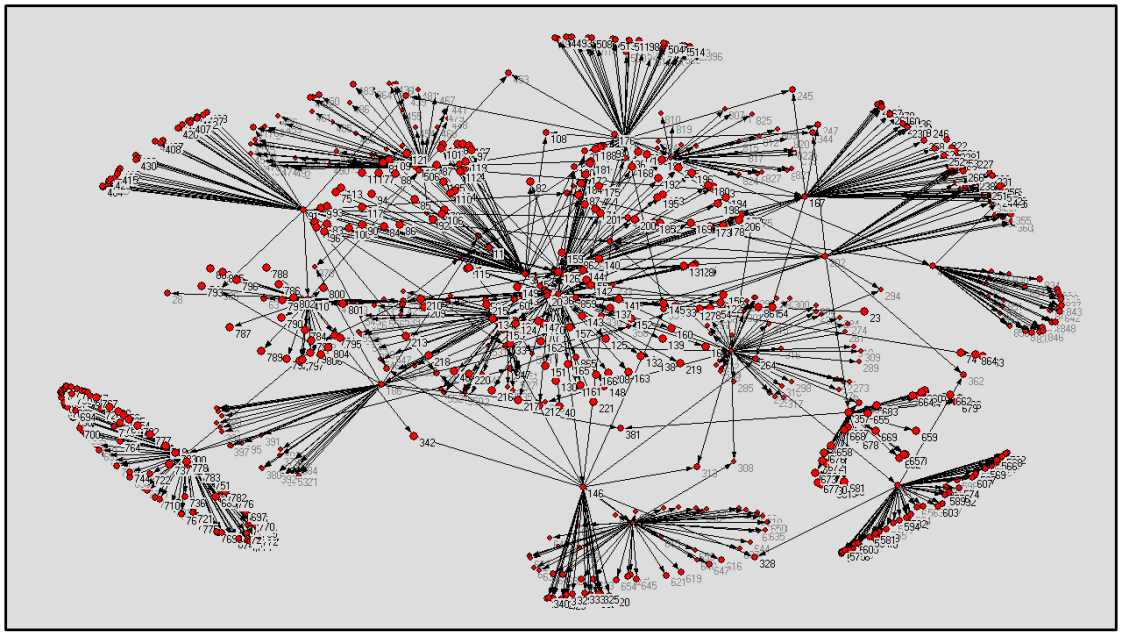
จากรูปที่ 4.25 แสดงให้เห็นการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2554 ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A146, A43, A78, A116 และ A20 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 79, 99, 102, 55 และ 85 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A164, A20, A39, A91 และ A42 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 95, 20, 105, 95 และ 88 หน่วย ตามลำดับ

3. โหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข A275, A374, A186, A243 และ A167 ด้วยค่า Closeness Measures 8.293, 8.351, 8.736, 8.450 และ 8.493 หน่วย ตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลธันวาคม 2554 (ประเทศที่ร่วมทดสอบ) หากโหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) คือ โหนดหมายเลข A146, A43, A78, A116 และ A20 ได้รับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสมาจากโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข A275, A374, A186, A243 และ A167 หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข A164, A20, A39, A91 และ A42 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข A275, A374, A186, A243 และ A167 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes)



รูปที่ 4.26 การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.26 แสดงให้เห็นการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนเมษายน 2555 ดังนี้

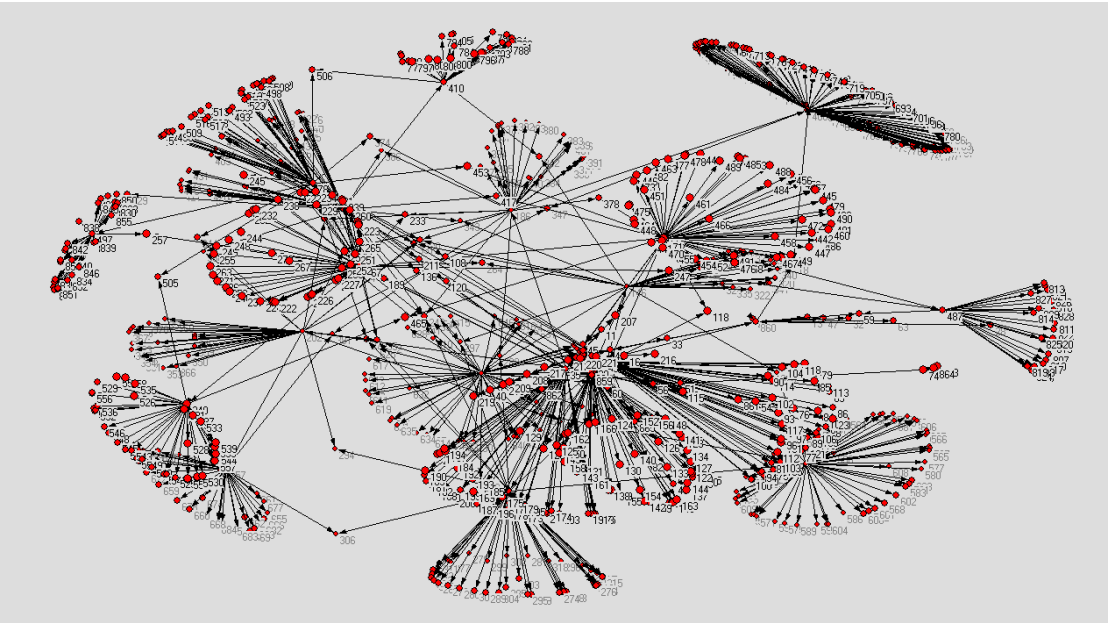
1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A421, A44, A257, A69 และ A250 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 109, 95, 72, 57 และ 102 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A165, A672, A925, A469 และ A52 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 105, 60, 95, 55 และ 108 หน่วย ตามลำดับ

3. โหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข A249, A69, A80, A260 และ A250 ด้วยค่า Closeness Measures 8.103, 8.351, 8.700, 8.159 และ 8.223 หน่วย ตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเมษายน 2555 (ประเทศที่ร่วมทดสอบ) หากโหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) คือ โหนดหมายเลข A421, A44, A257, A69 และ A250 ได้รับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่าย

สังคมออนไลน์มีโอกาสมาจากโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข A249, A69, A80, A260 และ A250 หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือ โหนดหมายเลข A165, A672, A925, A469 และ A52 กระจายข้อมูลข่าวสารหรือพบความผิดปกติ และการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข A249, A69, A80, A260 และ A250 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes)



รูปที่ 4.27 การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศที่ร่วมทดสอบ)

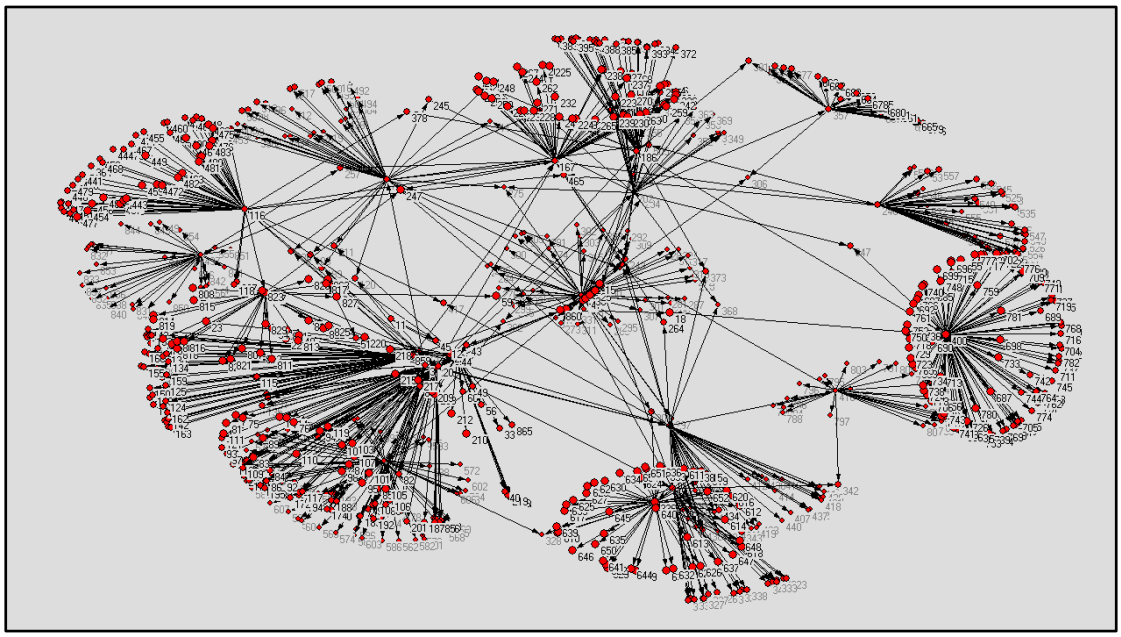
จากรูปที่ 4.27 แสดงให้เห็นการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2555 ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A66, A30, A272, A69 และ A250 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 89, 55, 102, 107 และ 92 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือ โหนดหมายเลข A84, A38, A257, A69 และ A1232 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 95, 160, 105, 75 และ 88 หน่วย ตามลำดับ

3. โหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข A1249, A69, A80, A460 และ A250 ด้วยค่า Closeness Measures 8.403, 8.051, 8.753, 8.959 และ 8.258 หน่วย ตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลธันวาคม 2555 (ประเทศที่ร่วมทดสอบ) หากโหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) คือ โหนดหมายเลข A66, A30, A272, A69 และ A250 ได้รับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสมาจากโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข A1249, A69, A80, A460 และ A250 หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือ โหนดหมายเลข A84, A38, A257, A69 และ A1232 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข A1249, A69, A80, A460 และ A250 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes)



รูปที่ 4.28 การแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.28 แสดงให้เห็นการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนเมษายน 2556 ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A77, A175, A198, A1169 และ A4782 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 109, 155, 102, 97 และ 102 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A1184, A738, A957, A169 และ A232 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 105, 60, 115, 105 และ 128 หน่วย ตามลำดับ

3. โหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข A1249, A69, A80, A460 และ A250 ด้วยค่า Closeness Measures 8.423, 8.151, 8.053, 8.259 และ 8.288 หน่วย ตามลำดับ

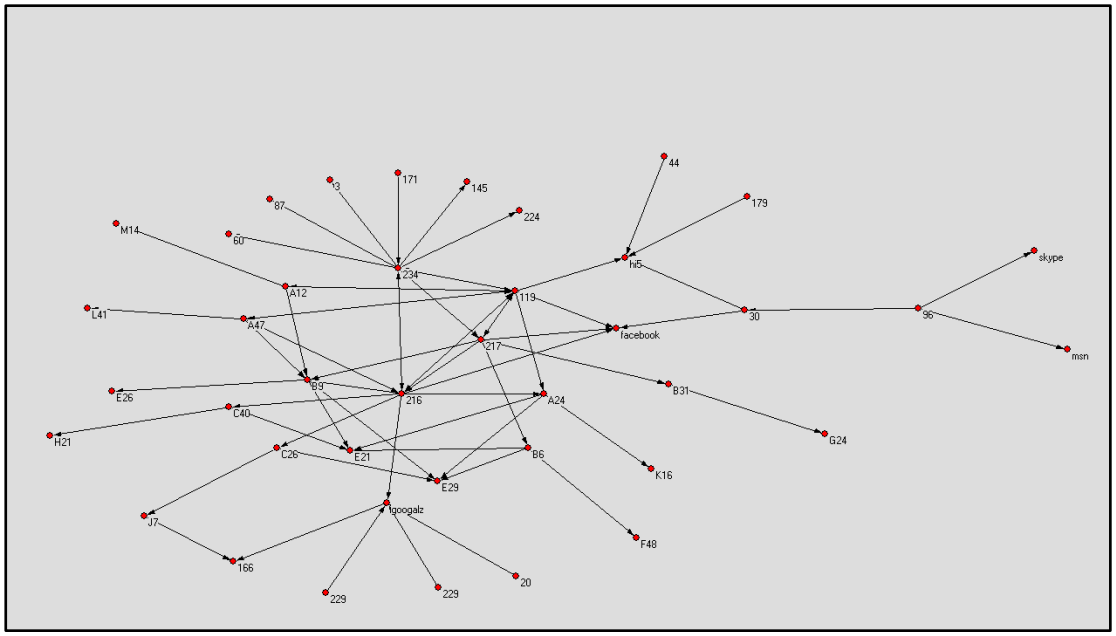
จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเมษายน 2556 (ประเทศที่ร่วมทดสอบ) หากโหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) คือ โหนดหมายเลข A77, A175, A198, A1169 และ A4782 ได้รับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสมาจากโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข A1249, A69, A80, A460 และ A250 หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข A1184, A738, A957, A169 และ A232 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนด A1249, A69, A80, A460 และ A250 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes)

4.3 การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์

จากวัตถุประสงค์ข้อที่ 3 ซึ่งผู้วิจัยได้ทำการศึกษาและวิเคราห์ฐานข้อมูลเพื่อสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูล 2 ประเทศ คือประเทศไทยและประเทศที่ร่วมทดสอบ ด้วยข้อมูล 4 ชุด คือชุดข้อมูลในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังการวิเคราะห์หาวิธีการสืบค้นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อ

ใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Social Network Analysis (SNA) ด้วย Degree Centrality, Betweenness Centrality, Closeness Centrality ซึ่งเป็นการแสดงภาพผู้มีอิทธิพล (Influencing Node)

รวมทั้งพัฒนาตัวแบบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm โดยการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์มีข้อมูลดังแสดงในรูปประกอบที่ 4.29-4.32 ซึ่งเป็นข้อมูลของประเทศไทยในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 และ 4.33-4.36 ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ตามลำดับ ดังนี้



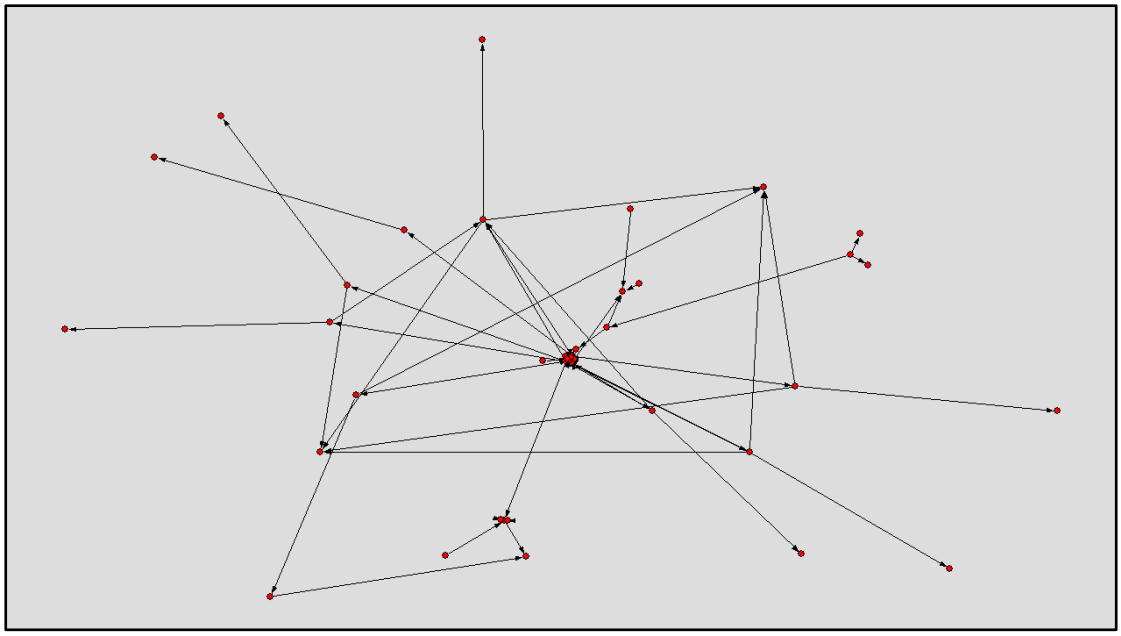
รูปที่ 4.29 การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 (ประเทศไทย)

จากรูปที่ 4.29 แสดงให้เห็นภาพการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือน

ธันวาคม 2554 โดยโหนดที่มีโอกาสเป็นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์คือ

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) สูงสุด 5 อันดับแรก คือ โหนดหมายเลข 60, 87, 3, 229 และ 224 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) l205, 75, 90, 120, และ 80 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) สูงสุด 5 อันดับแรก คือโหนดหมายเลข 234, 99, 217, 229 และ 216 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 1400, 100, 95, 60 และ 75 หน่วย ตามลำดับ

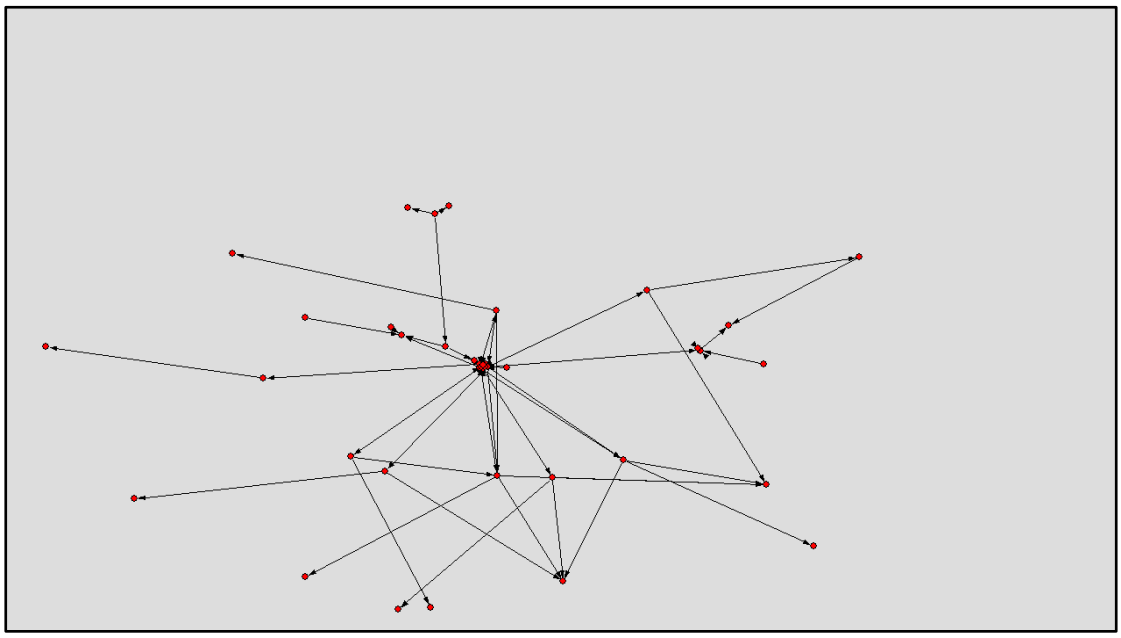


รูปที่ 4.30 การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศไทย)

จากรูปที่ 4.30 แสดงให้เห็นภาพการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนเมษายน 2555 โดยโหนดที่มีโอกาสเป็นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข 60, 87, 3, googalz และ 224 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) l 109, 109, 107, 72, และ 60 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข 234, J7, 217, 229 และ 216 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 1451, 101, 75, 68 และ 61 หน่วย ตามลำดับ

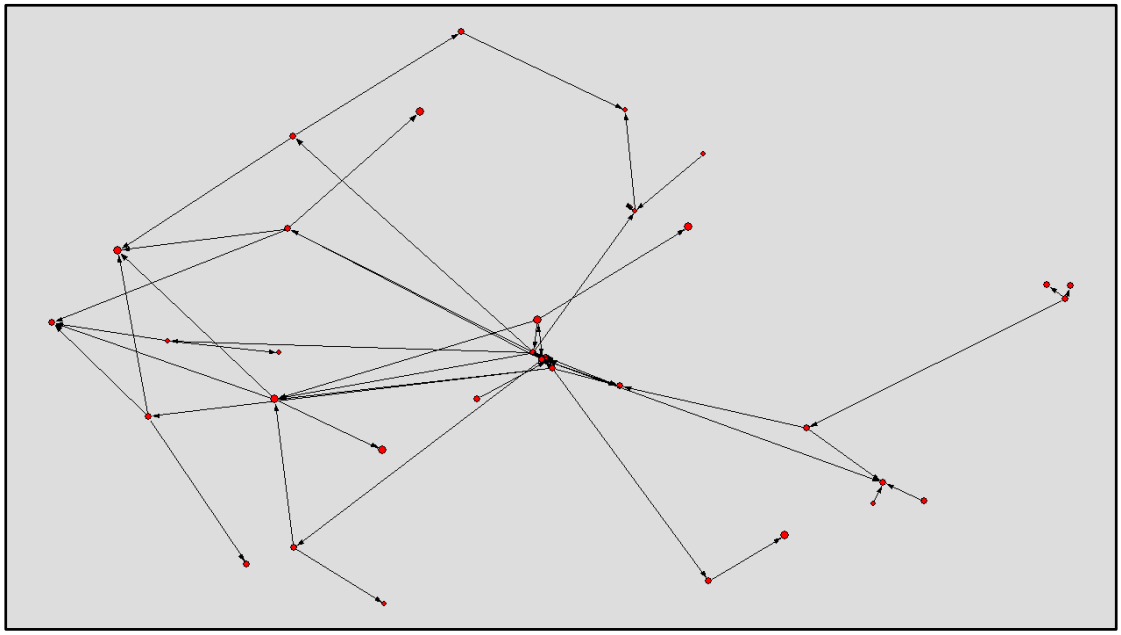


รูปที่ 4.31 การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศไทย)

จากรูปที่ 4.31 แสดงให้เห็นภาพการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนธันวาคม 2555 โดยโหนดที่มีโอกาสเป็นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์คือ ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข 60, 87, 3, 90 และ 224 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 90, 129, 79, 72, และ 90 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือ โหนดหมายเลข 234, 90, 217, 229 และ 216 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 1200, 501, 275, 168 และ 55 หน่วย ตามลำดับ

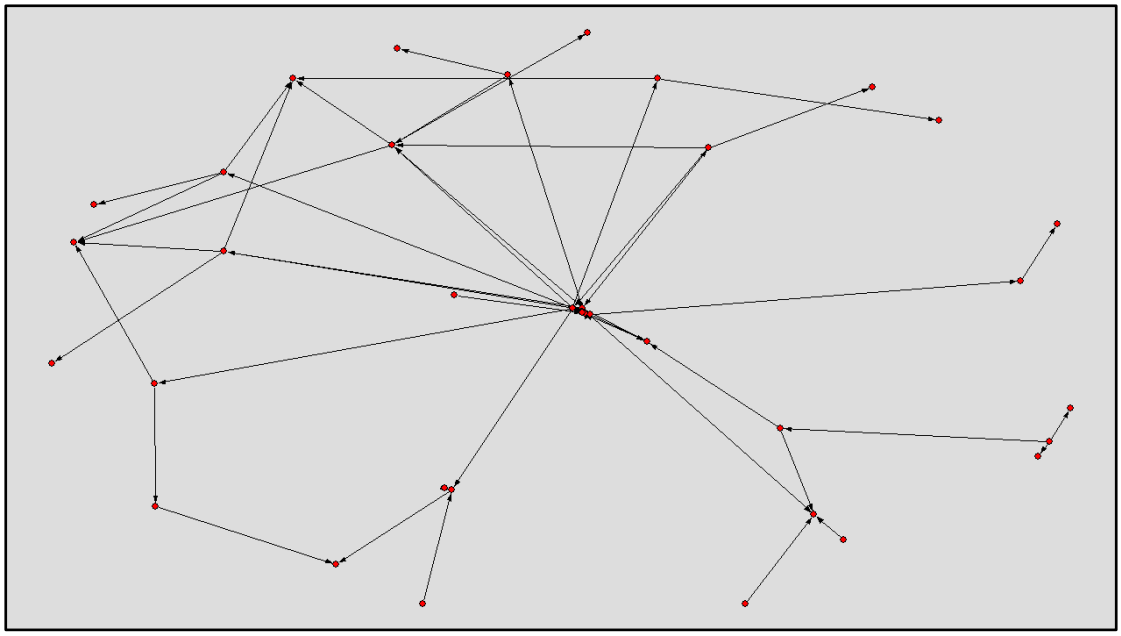


รูปที่ 4.32 การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศไทย)

จากรูปที่ 4.32 แสดงให้เห็นภาพการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนเมษายน 2556 โดยโหนดที่มีโอกาสเป็นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์คือ ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข 129, 87, 3, 90 และ 224 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 105, 79, 99, 102, และ 85 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือ โหนดหมายเลข 234, 90, 217, 229 และ 216 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 200, 51, 75, 78 และ 95 หน่วย ตามลำดับ

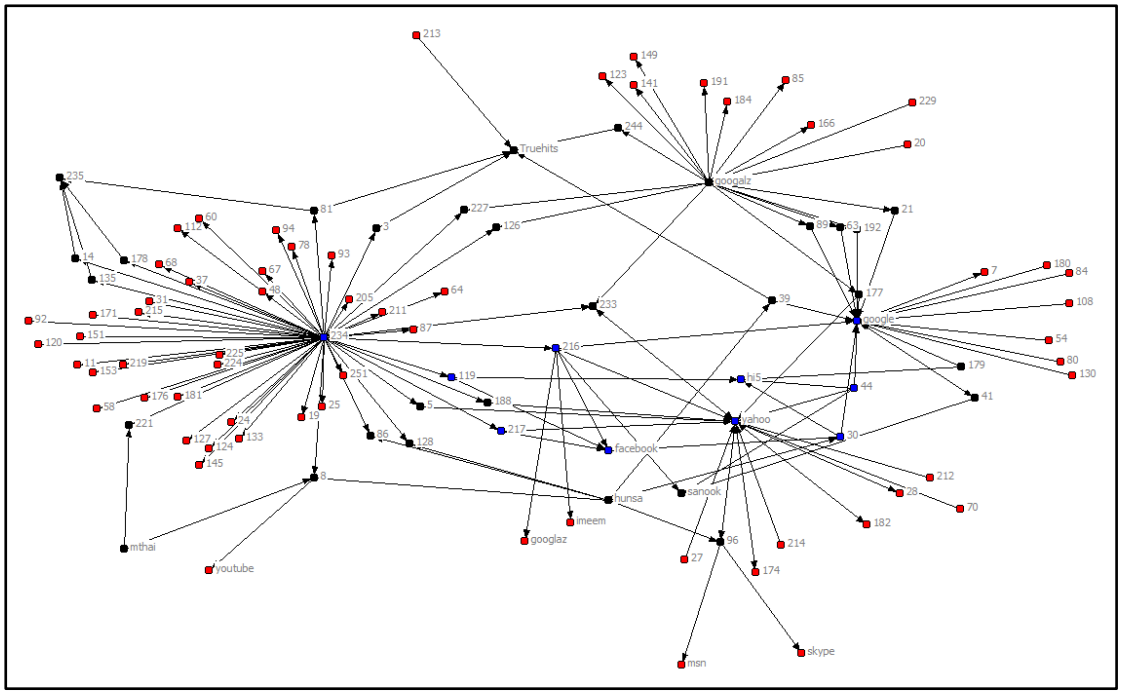


รูปที่ 4.33 การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.33 แสดงให้เห็นภาพการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2554 โดยโหนดที่มีโอกาสเป็นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์คือ ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A146, A43, A78, A116 และ A20 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 79, 99, 102, 55 และ 85 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A164, A20, A39, A91 และ A42 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 95, 20, 105, 95 และ 88 หน่วย ตามลำดับ

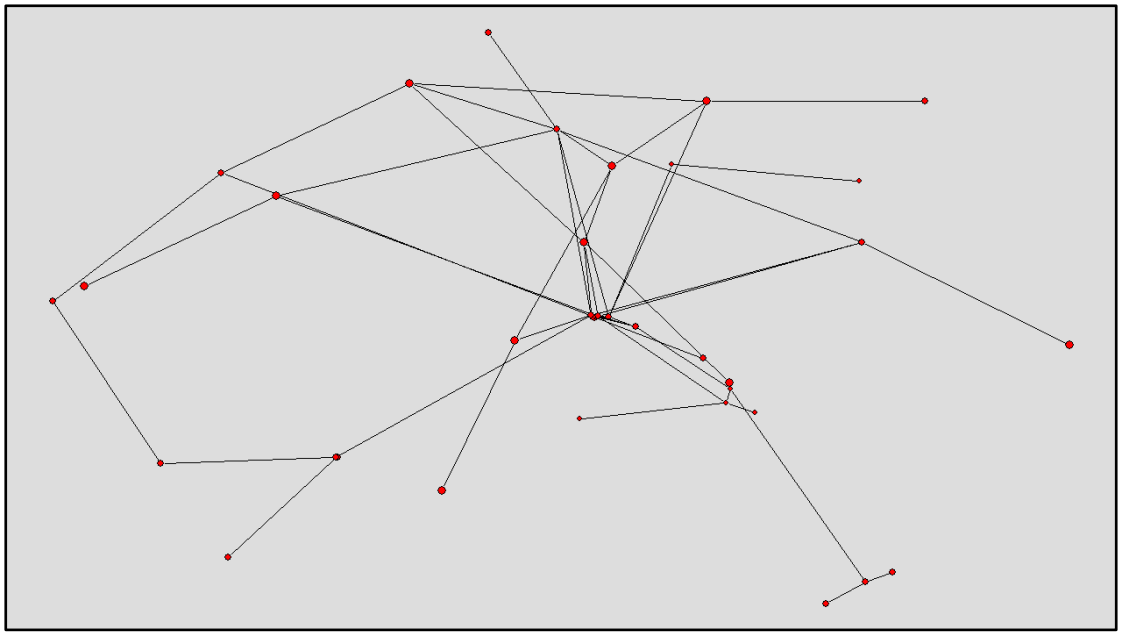


รูปที่ 4.34 การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.34 แสดงให้เห็นภาพการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนเมษายน 2555 โดยโหนดที่มีโอกาสเป็นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์คือ ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A421, A44, A257, A69 และ A250 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 109, 95, 72, 57 และ 102 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A165, A672, A925, A469 และ A52 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 105, 60, 95, 55 และ 108 หน่วย ตามลำดับ

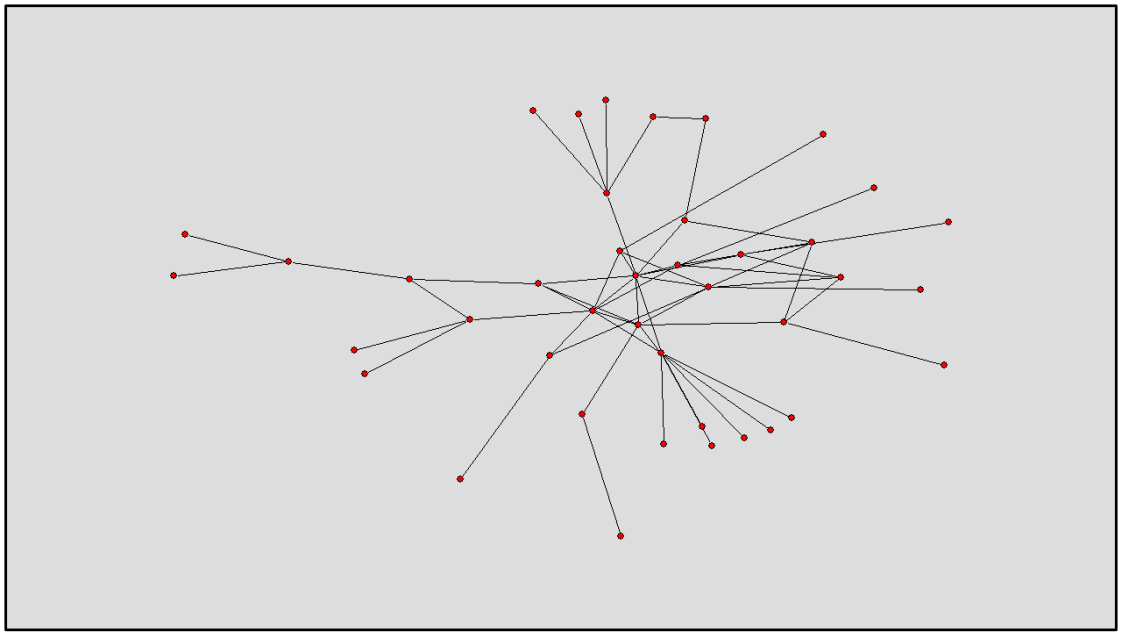


รูปที่ 4.35 การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.35 แสดงให้เห็นภาพการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2555 โดยโหนดที่มีโอกาสเป็นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์คือ ดังนี้

1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A66, A30, A272, A69 และ A250 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 89, 55, 102, 107 และ 92 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A84, A38, A257, A69 และ A1232 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 95, 160, 105, 75 และ 88 หน่วย ตามลำดับ



รูปที่ 4.36 การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.36 แสดงให้เห็นภาพการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนเมษายน 2556 โดยโหนดที่มีโอกาสเป็นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์คือ ดังนี้

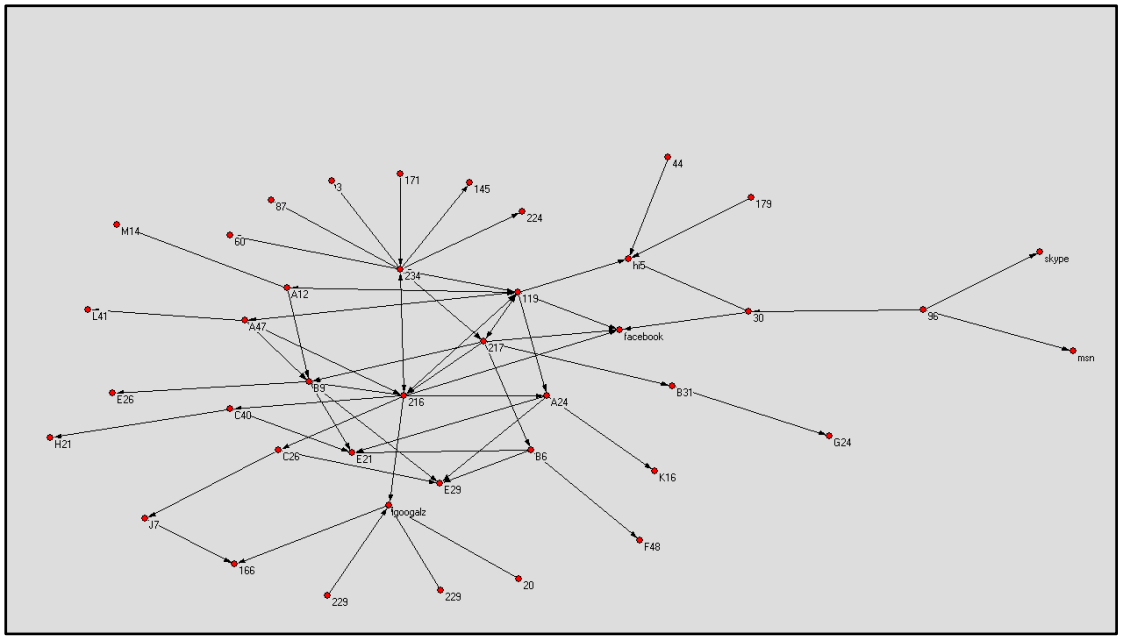
1. โหนดศูนย์กลางการรับข้อมูลข่าวสาร (In-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A77, A175, A198, A1169 และ A4782 ด้วยค่าศูนย์กลางรับข้อมูลข่าวสาร (In-Degree) 109, 155, 102, 97 และ 102 หน่วย ตามลำดับ

2. โหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) 5 อันดับแรก คือโหนดหมายเลข A1184, A738, A957, A169 และ A232 ด้วยค่าศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree) 105, 60, 115, 105 และ 128 หน่วย ตามลำดับ

4.4 การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์

จากวัตถุประสงค์ข้อที่ 4 ซึ่งผู้วิจัยได้ทำการศึกษาและวิเคราห์ฐานข้อมูลเพื่อทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูล 2 ประเทศ คือประเทศไทยและประเทศที่ร่วมทดสอบ ด้วยข้อมูล 4 ชุด คือชุดข้อมูลในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังการวิเคราะห์หาวิธีการหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ในหลักการของ Data Mining (Supervised Learning, Classification Analysis, oneR Algorithm)

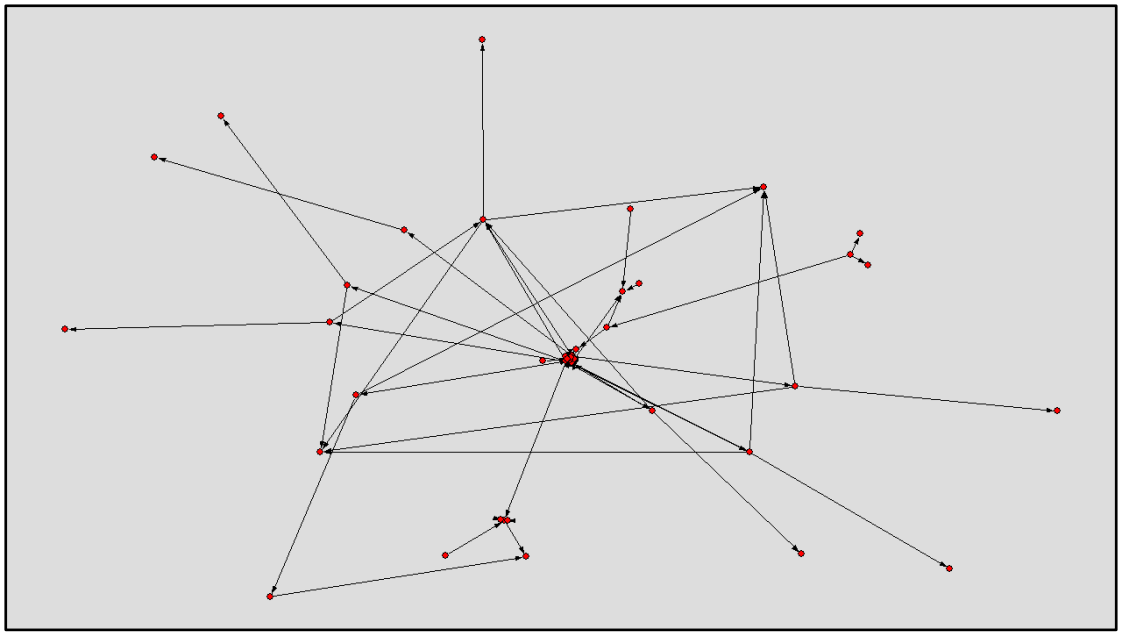
พร้อมทั้ง พัฒนาตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ในหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm โดยการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์มีข้อมูลดังแสดงในรูปประกอบที่ 4.37-4.40 ซึ่งเป็นข้อมูลของประเทศไทยในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 และ 4.41-4.44 ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ตามลำดับ ดังนี้



รูปที่ 4.37 การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ฐานข้อมูลเดือนธันวาคม 2554 (ประเทศไทย)

จากรูปที่ 4.37 แสดงให้เห็นภาพการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนธันวาคม 2554 โดยโหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารและโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข 99, 119, 217, 216 และ 234 ด้วยค่า Closeness Measure 8.305, 8.436, 8.413, 8.301 และ 8.293 หน่วย ตามลำดับ

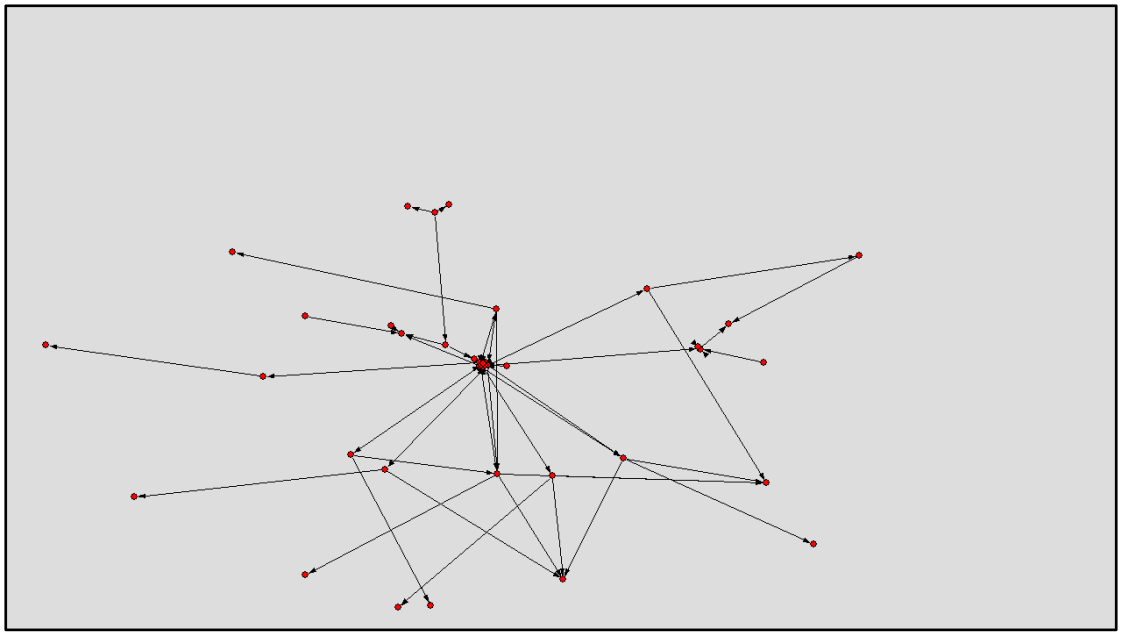
จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 (ประเทศไทย) หากโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข 234, 99, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 99, 119, 217, 216 และ 234 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes) หรือโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์



รูปที่ 4.38 การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ฐานข้อมูลเดือนเมษายน 2555 (ประเทศไทย)

จากรูปที่ 4.38 แสดงให้เห็นภาพการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนเมษายน 2555 โดยโหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ด้วยค่า Closeness Measures 8.456, 8.436, 8.413, 8.301 และ 8.293 หน่วย ตามลำดับ

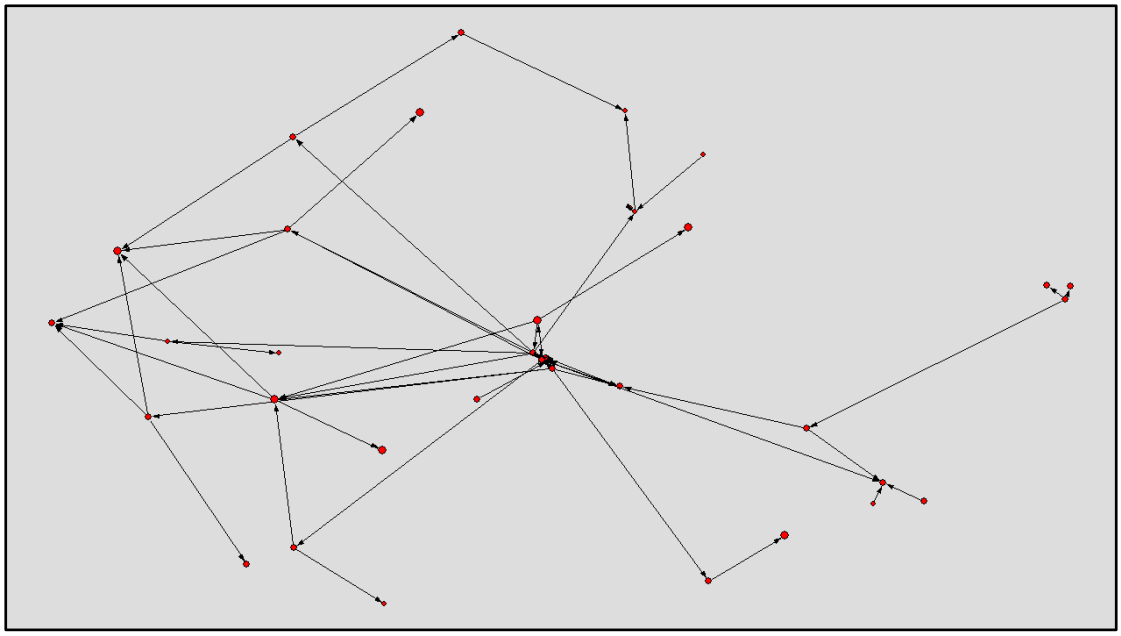
จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศไทย) หากโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข 234, J7, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes) หรือโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์



รูปที่ 4.39 การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ฐานข้อมูลเดือนธันวาคม 2555 (ประเทศไทย)

จากรูปที่ 4.39 แสดงให้เห็นภาพการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนธันวาคม 2555 โดยโหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ด้วยค่า Closeness Measures 8.293 , 8.436, 8.301, 8.413 และ 8.456 หน่วย ตามลำดับ

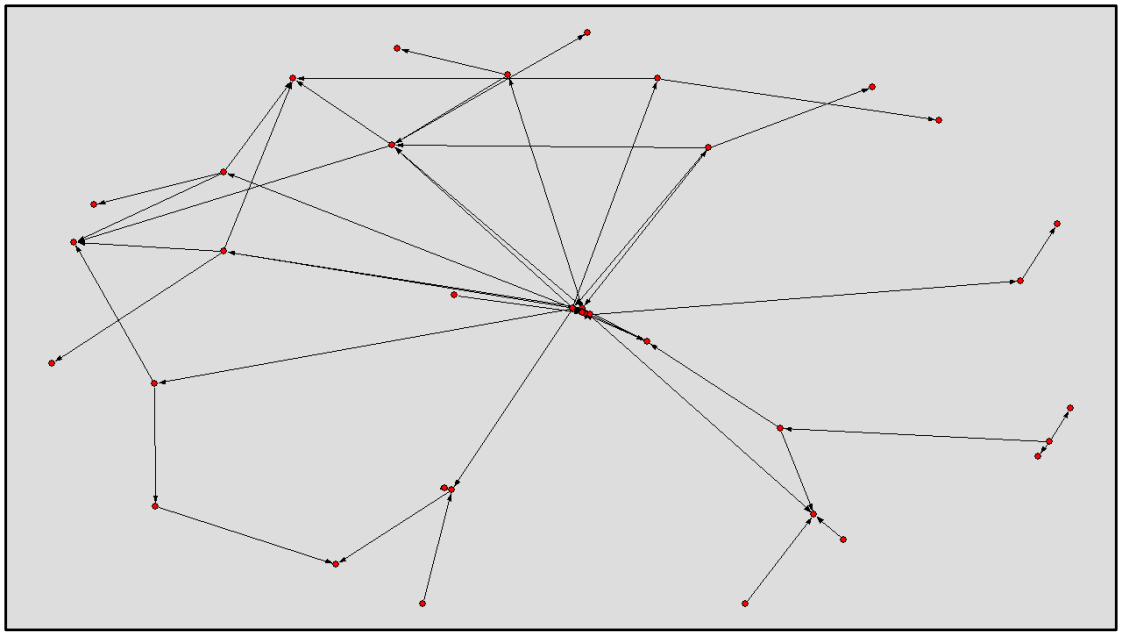
จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศไทย) หากโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข 234, 90, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes) หรือโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์



รูปที่ 4.40 การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ฐานข้อมูลเดือนเมษายน 2556 (ประเทศไทย)

จากรูปที่ 4.40 แสดงให้เห็นภาพการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศไทยในเดือนเมษายน 2556 โดยโหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ด้วยค่า Closeness Measures 8.301, 8.436, 8.293, 8.456 และ 8.413 หน่วย ตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศไทย) หากโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข 234, 90, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้โหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes) หรือโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์

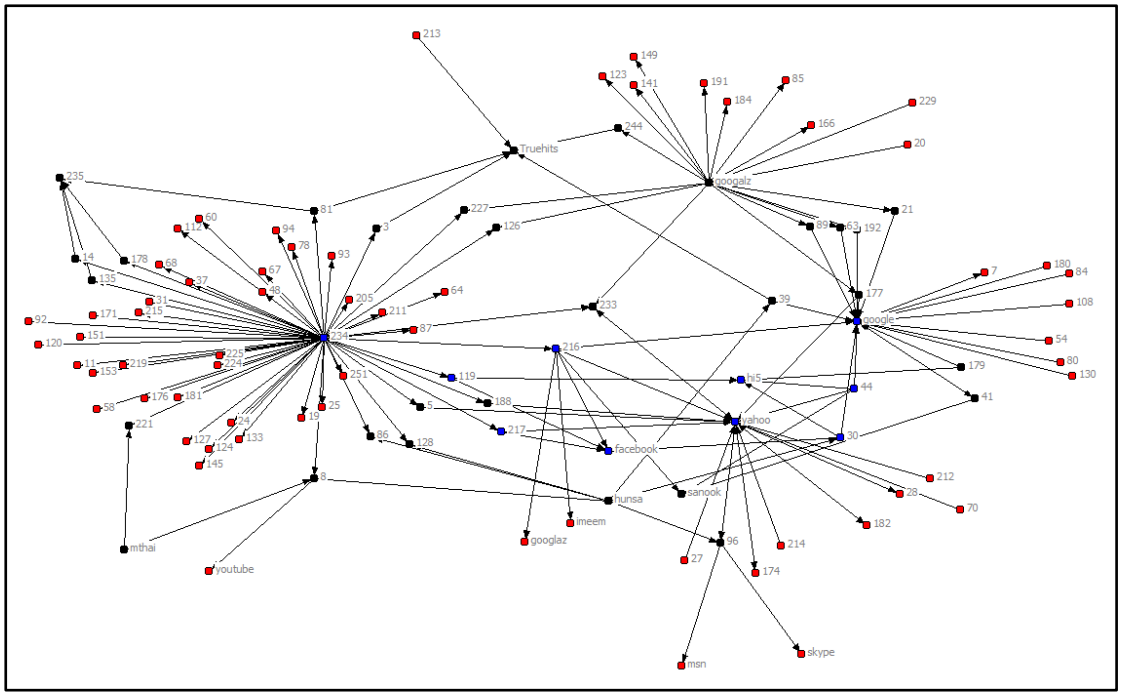


รูปที่ 4.41 การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีฯ ฐานข้อมูลเดือนธันวาคม 2554 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.41 แสดงให้เห็นภาพการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2554 โดยโหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข A275, A374, A186, A243 และ A167 ด้วยค่า Closeness Measures 8.293, 8.351, 8.736, 8.450 และ 8.493 หน่วยตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2554 (ประเทศที่ร่วมทดสอบ) หากโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข A164, A20, A39, A91 และ A42 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข A275, A374, A186, A243 และ A167 ทำให้โหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes) หรือโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับ

ผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์

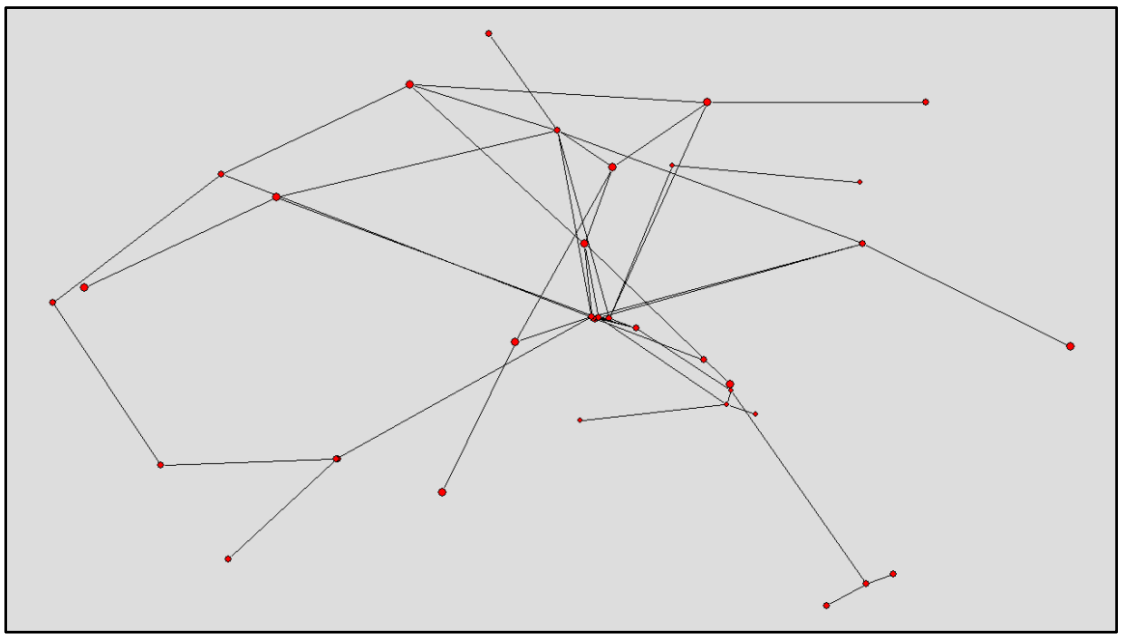


รูปที่ 4.42 การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีฯ ฐานข้อมูลเดือนเมษายน 2555 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.42 แสดงให้เห็นภาพการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนเมษายน 2555 โดยโหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข A249, A69, A80, A260และ A250 ด้วยค่า Closeness Measures 8.103, 8.351, 8.700, 8.159 และ 8.223 หน่วยตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2555 (ประเทศที่ร่วมทดสอบ) หากโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข A165, A672, A925, A469 และ A52 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนด

หมายเลข A249, A69, A80, A260และ A250 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes) หรือโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์

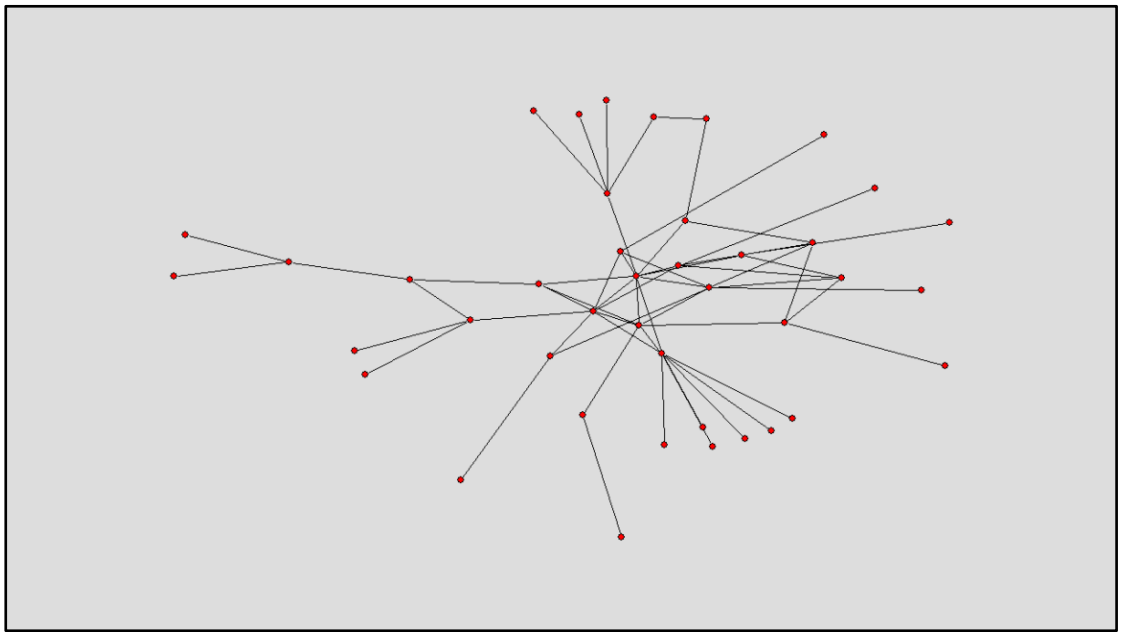


รูปที่ 4.43 การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีฯ ฐานข้อมูลเดือนธันวาคม 2555 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.43 แสดงให้เห็นภาพการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนธันวาคม 2555 โดยโหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข A1249, A69, A80, A460 และ A250 ด้วยค่า Closeness Measures 8.403, 8.051, 8.753, 8.959 และ 8.258 หน่วยตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนธันวาคม 2555 (ประเทศที่ร่วมทดสอบ) หากโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนดหมายเลข A84, A38, A257, A69 และ A1232 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการ

ถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือโหนดหมายเลข A1249, A69, A80, A460 และ A250 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes) หรือโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์



รูปที่ 4.44 การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีฯ ฐานข้อมูลเดือนเมษายน 2556 (ประเทศที่ร่วมทดสอบ)

จากรูปที่ 4.44 แสดงให้เห็นภาพการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นข้อมูลของประเทศที่ร่วมทดสอบในเดือนเมษายน 2556 โดยโหนดที่ใกล้ชิดกับโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร 5 อันดับแรก คือโหนดหมายเลข A1249, A69, A80, A460 และ A250 ด้วยค่า Closeness Measures 8.423, 8.151, 8.053, 8.259 และ 8.288 หน่วยตามลำดับ

จากความสัมพันธ์ในเครือข่ายสังคมออนไลน์ในฐานข้อมูลเดือนเมษายน 2556 (ประเทศที่ร่วมทดสอบ) หากโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร (Out-Degree Nodes) คือโหนด

หมายเลข A1184, A738, A957, A169 และ A232 กระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์มีโอกาสส่งไปยังโหนดที่ใกล้ชิด (Closeness Nodes) คือ โหนด A1249, A69, A80, A460 และ A250 ทำให้เป็นโหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (Attacked Nodes) หรือโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์

4.5 การทดสอบประเมินความแม่นยำของตัวแบบ

ผู้วิจัยได้ทำการพัฒนาตัวแบบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ และพัฒนาตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ซึ่งเป็นองค์ประกอบส่วนหนึ่งของตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟซึ่งผู้วิจัยดำเนินการประเมินความแม่นยำของตัวแบบดังกล่าวด้วยสถิติทดสอบ Wilcoxon Rank Sum Test

เมื่อ n_A คือขนาดตัวอย่างของกลุ่มตัวอย่างทดสอบที่ 1

และ n_B คือขนาดตัวอย่างของกลุ่มตัวอย่างทดสอบที่ 2

โดย $n = n_A + n_B$ และกำหนดสถิติทดสอบด้วยวิธี Wilcoxon Rank Sum Test คือ T_A

ดังนั้น ค่าเฉลี่ย $E(T_A)$ และค่าความแปรปรวน $V(T_A)$ เป็นดังนี้

$$E(T_A) = \frac{n_A(n_A+n_B+1)}{2} = \frac{n_A(n+1)}{2} \quad (4.1)$$

$$V(T_A) = \frac{n_A(n_A+n_b+1)}{2} = \frac{n_A(n+1)}{2} \quad (4.2)$$

สถิติทดสอบ $Z = \frac{T_A - n_A(n+1)/2}{\sqrt{n_A n_B(n+1)/12}}$ (4.3)

และเขตปฏิเสธ $|Z| > Z_{1-\alpha_{/2}}$

โดยที่ Z มีการแจกแจงแบบปกติมาตรฐาน ที่มีค่าเฉลี่ย =0 และ ค่าความแปรปรวน=1

สถิติทดสอบดังกล่าวข้างต้นเป็นสถิติทดสอบสมมติฐานที่ไม่ใช้พาราเตอร์ (Nonparametric Tests) เนื่องจากไม่สามารถหาการแจกแจง มีตัวอย่างขนาดเล็ก และข้อมูลอยู่ในรูปลำดับที่หรือความถี่ โดยการทดสอบสมมติฐานที่ไม่ใช้พาราเตอร์ (Nonparametric Tests) แต่ละวิธีเป็นการทดสอบระหว่างข้อมูลที่เกิดขึ้นจริงในอนาคตและข้อมูลที่ได้จากการประเมินหรือทำนายหาบนฐานข้อมูลในปัจจุบัน 2 ประเทศ คือประเทศไทยและประเทศที่ร่วมทดสอบ ด้วยข้อมูล 4 ชุด คือ ชุดข้อมูลในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 % ดังต่อไปนี้

4.5.1 ตัวแบบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์

H_0: โหนดที่ค้นพบจากตัวแบบ=โหนดที่เกิดขึ้นจริงในอนาคต หรือ
(ลักษณะที่สนใจศึกษาของประชากรทั้งสองไม่แตกต่างกัน)

H_1: โหนดที่ค้นพบจากตัวแบบ≠โหนดที่เกิดขึ้นจริงในอนาคต หรือ
(ลักษณะที่สนใจศึกษาของประชากรทั้งสองแตกต่างกัน)

การทดสอบสมมติฐานของการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูล (ประเทศไทย) มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

จะได้ว่า $Z_{1-\alpha_{/2}} = 1.96$

ตารางที่ 4.9 ตารางสถิติทดสอบความแม่นยำของตัวแบบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงในฐานข้อมูลประเทศไทย

ชุดข้อมูลประเทศไทย	$Z_{\text{คำนวณ}}$	ผลการทดสอบ
เดือนธันวาคม 2554	1.85	ไม่สามารถปฏิเสธ H_0
เดือนเมษายน 2555	1.75	ไม่สามารถปฏิเสธ H_0
เดือนธันวาคม 2555	1.90	ไม่สามารถปฏิเสธ H_0
เดือนเมษายน 2556	1.93	ไม่สามารถปฏิเสธ H_0

จากผลการทดสอบสมมติฐาน จึงไม่สามารถปฏิเสธ H_0 นั่นคือ โหนดที่ค้นพบจากตัวแบบ=โหนดที่เกิดขึ้นจริงในอนาคต (ทุกชุดข้อมูล) หรือตัวแบบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

ตารางที่ 4.10 ตารางสถิติทดสอบความแม่นยำของตัวแบบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงในฐานข้อมูลประเทศที่ร่วมทดสอบ

ชุดข้อมูลประเทศที่ร่วมทดสอบ	$Z_{\text{คำนวณ}}$	**ผลการทดสอบ**
เดือนธันวาคม 2554	1.80	ไม่สามารถปฏิเสธ H_0
เดือนเมษายน 2555	1.84	ไม่สามารถปฏิเสธ H_0
เดือนธันวาคม 2555	1.95	ไม่สามารถปฏิเสธ H_0
เดือนเมษายน 2556	1.90	ไม่สามารถปฏิเสธ H_0

จากผลการทดสอบสมมติฐาน จึงไม่สามารถปฏิเสธ H_0 นั่นคือ โหนดที่ค้นพบจากตัวแบบ=โหนดที่เกิดขึ้นจริงในอนาคต (ทุกชุดข้อมูล) หรือตัวแบบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

4.5.2 ตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์

H_0: โหนดที่ค้นพบจากตัวแบบ＝โหนดที่เกิดขึ้นจริงในอนาคต หรือ
(ลักษณะที่สนใจศึกษาของประชากรทั้งสองไม่แตกต่างกัน)

H_1: โหนดที่ค้นพบจากตัวแบบ≠โหนดที่เกิดขึ้นจริงในอนาคต หรือ
(ลักษณะที่สนใจศึกษาของประชากรทั้งสองแตกต่างกัน)

การทดสอบสมมติฐานของการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือน

ล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูล (ประเทศไทย) มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

จะได้ว่า $Z_{1-\alpha_{/2}} = 1.96$

ตารางที่ 4.11 ตารางสถิติทดสอบความแม่นยำของตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในฐานข้อมูลประเทศไทย

ชุดข้อมูลประเทศไทย	$Z_{\text{คำนวณ}}$	**ผลการทดสอบ**
เดือนธันวาคม 2554	1.83	ไม่สามารถปฏิเสธ H_0
เดือนเมษายน 2555	1.85	ไม่สามารถปฏิเสธ H_0
เดือนธันวาคม 2555	1.91	ไม่สามารถปฏิเสธ H_0
เดือนเมษายน 2556	1.90	ไม่สามารถปฏิเสธ H_0

จากผลการทดสอบสมมติฐาน จึงไม่สามารถปฏิเสธ H_0 นั่นคือ โหนดที่ค้นพบจากตัวแบบ=โหนดที่เกิดขึ้นจริงในอนาคต (ทุกชุดข้อมูล) หรือตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคม มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

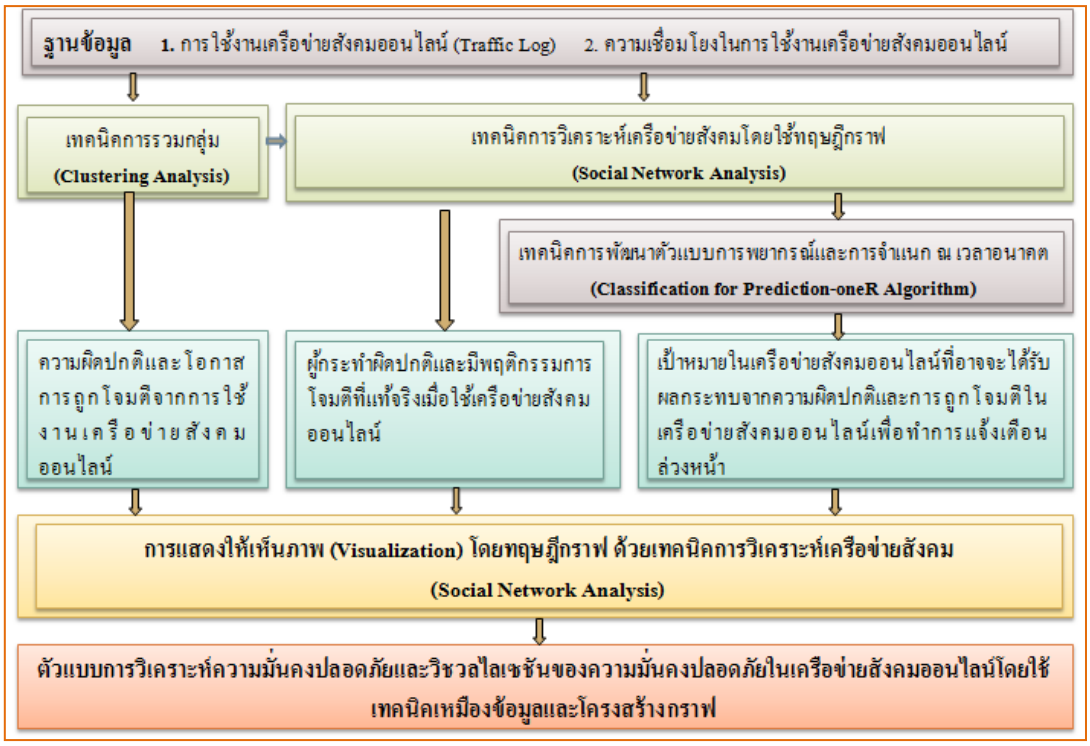
ตารางที่ 4.12 ตารางสถิติทดสอบความแม่นยำของตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในฐานข้อมูลประเทศที่ร่วมทดสอบ

ชุดข้อมูลประเทศที่ร่วมทดสอบ	$Z_{\text{คำนวณ}}$	**ผลการทดสอบ**
เดือนธันวาคม 2554	1.89	ไม่สามารถปฏิเสธ H_0
เดือนเมษายน 2555	1.85	ไม่สามารถปฏิเสธ H_0
เดือนธันวาคม 2555	1.92	ไม่สามารถปฏิเสธ H_0
เดือนเมษายน 2556	1.90	ไม่สามารถปฏิเสธ H_0

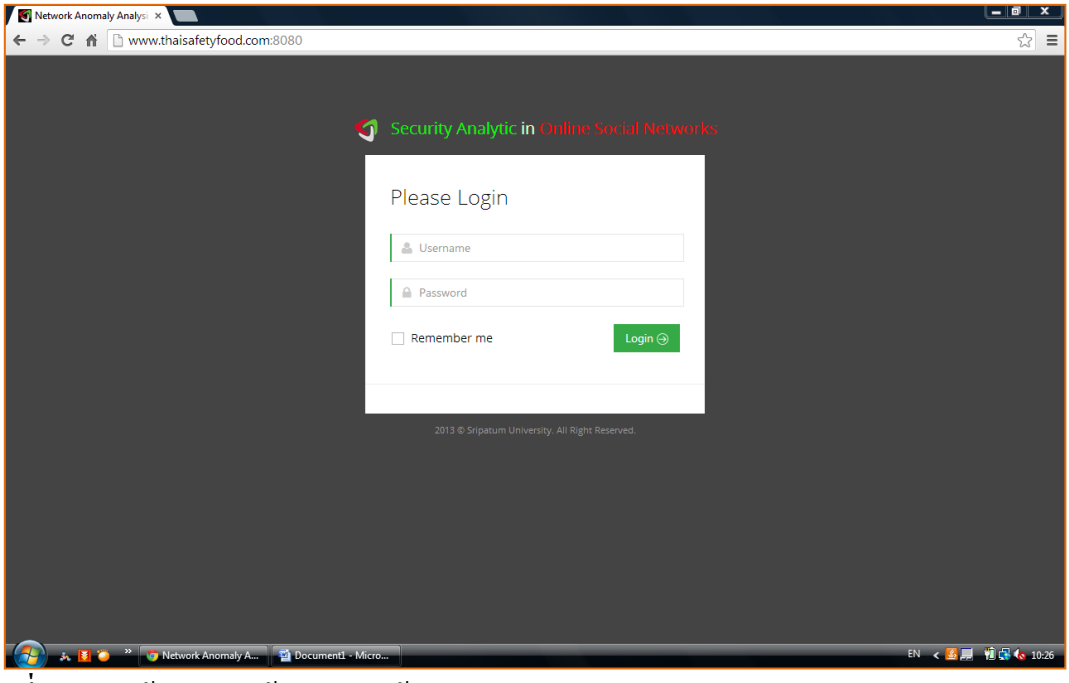
จากผลการทดสอบสมมติฐาน จึงไม่สามารถปฏิเสธ H_0 นั่นคือ โหนดที่ค้นพบจากตัวแบบ=โหนดที่เกิดขึ้นจริงในอนาคต (ทุกชุดข้อมูล) หรือตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคม มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

4.6 ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ

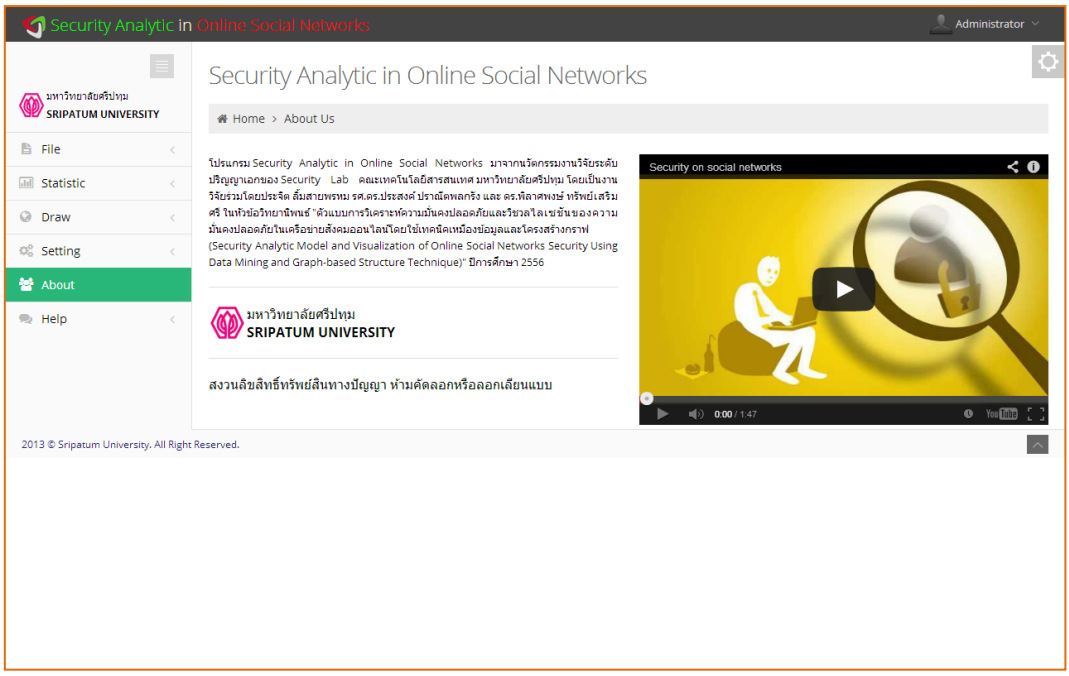
ผู้วิจัยได้ทำการทดสอบประเมินความแม่นยำของตัวแบบที่ได้ คือ ตัวแบบการประเมินหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ และตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ด้วยการทดสอบสมมติฐานระหว่างข้อมูลที่เกิดขึ้นจริงในอนาคตและข้อมูลที่ได้จากการประเมินหรือทำนายหาบนฐานข้อมูลในปัจจุบัน โดยใช้เกณฑ์ความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 % และได้สรุปผลการทดลองและนำเสนอตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ (Security Analytics Model and Visualization of Online Social Networks Security Using Data Mining and Graph-based Structure Technique) ดังตัวแบบต่อไปนี้



รูปที่ 4.44.1 ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ



รูปที่ 4.45 หน้าจอการใช้รหัสการใช้งาน (Username) และรหัสลับ (Password) ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



รูปที่ 4.46 หน้าจอรายการหลักโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์

จากหน้าจอหลักโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application) จะประกอบด้วยรายการย่อย (Sub Menu) ดังนี้ File, Statistic, Draw, Setting, About และ Help ดังแสดงในรูปที่ 4.47

1. รายการย่อยของ **File** มีดังนี้

   1.1 **Create** รองรับการสร้างข้อมูลนำเข้าโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application) ดังแสดงในรูปที่ 4.48 และ 4.49 สามารถเก็บในรูปแบบของแฟ้มข้อมูล Excel File, CSV File และ โดยมีแบบของข้อมูลนำเข้าเรียงตามลำดับดังนี้

   1.1.1 Date หมายถึงวันที่ของการเกิดเหตุการณ์

   1.1.2 Time หมายถึงเวลาของการเกิดเหตุการณ์

   1.1.3 Attack_ID หมายถึงหมายเลขความผิดปกติและโอกาสการถูกโจมตี

1.1.4 Severity หมายถึงระดับความเสี่ยงของความผิดปกติและโอกาสการถูกโจมตี

1.1.5 Source IP หมายถึงหมายเลขเครื่องคอมพิวเตอร์เริ่มต้นจากการเกิดความผิดปกติและโอกาสการถูกโจมตี

1.1.6 Source Port หมายถึงหมายเลข Port ของเครื่องคอมพิวเตอร์เริ่มต้นจากการเกิดความผิดปกติและโอกาสการถูกโจมตี

1.1.7 Destination IP หมายถึงหมายเลขเครื่องคอมพิวเตอร์ปลายทางของการเกิดความผิดปกติและโอกาสการถูกโจมตี

1.1.8 Destination Port หมายเลข Port ของเครื่องคอมพิวเตอร์ปลายทางของการเกิดความผิดปกติและโอกาสการถูกโจมตี

1.1.9 Message หมายถึงคำอธิบายการเกิดความผิดปกติและโอกาสการถูกโจมตีของ Attack_ID

1.2 **Open** รองรับการเปิดแฟ้มข้อมูลที่จะนำเข้าโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application) ดังแสดงในรูปที่ 4.50 และ 4.51 สามารถเลือกเปิดแฟ้มข้อมูลได้ใน 2 รูปแบบคือ Excel File และ CSV File

1.3 **Import** รองรับการนำเข้าข้อมูลจากฐานข้อมูล Log File ใดๆ เพื่อเข้าสู่โปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application) ดังแสดงในรูปที่ 4.52 และ 4.53 โดยผู้ใช้จะต้องกำหนด Mapping Table ของฐานข้อมูล Log File ใดๆ และรูปแบบของข้อมูลของโปรแกรมฯ

1.4 **Close** รองรับการปิดใช้แฟ้มข้อมูลโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application)

1.5 **Exit** รองรับการออกจากโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security

Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application)

2. รายการย่อยของ Statistic ดังแสดงในรูปที่ 4.54 และ 4.55 ดังนี้

2.1 Anomaly and Attack Patterns ดังแสดงในรูปที่ 4.56

รองรับการแสดงสถิติการวิเคราะห์ความมั่นคงปลอดภัยในมิติของความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ โดยแสดงข้อความการวิเคราะห์ด้านล่างของตารางสถิติ ในหลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm)

2.2 Information Diffusion ดังแสดงในรูปที่ 4.57

รองรับการแสดงสถิติการวิเคราะห์ความมั่นคงปลอดภัยในมิติของการแพร่กระจายความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm) และหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm โดยแสดงข้อความการวิเคราะห์ด้านล่างของตารางสถิติ

2.3 Tracking Influencing Nodes ดังแสดงในรูปที่ 4.58

รองรับการแสดงสถิติการวิเคราะห์ความมั่นคงปลอดภัยในมิติของผู้ที่มีอิทธิพลต่อการแพร่กระจายความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Social Network Analysis (SNA) ด้วย Degree Centrality, Betweenness Centrality, Closeness Centrality เพื่อค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ (Influencing Nodes) และหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm เพื่อแสดงภาพผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ โดยแสดงข้อความการวิเคราะห์ด้านล่างของตารางสถิติ

2.4 Predicting Attacked Nodes ดังแสดงในรูปที่ 4.59

รองรับการแสดงสถิติการวิเคราะห์ความมั่นคงปลอดภัยในมิติของผู้ที่อาจได้รับผลกระทบจากความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Data Mining (Supervised Learning, Classification

Analysis, oneR Algorithm) และหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm เพื่อแสดงภาพเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ โดยแสดงข้อความการวิเคราะห์ด้านล่างของตารางสถิติ

3. รายการย่อยของ Draw ดังแสดงในรูปที่ 4.60 และ 4.61 มีดังนี้

   3.1 Anomaly and Attack Patterns ดังแสดงในรูปที่ 4.62 และ 4.62.1 รองรับการแสดงภาพการวิเคราะห์ความมั่นคงปลอดภัยในมิติของความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm) โดยแสดงข้อความการวิเคราะห์ด้านล่างของภาพ

   3.2 Information Diffusion ดังแสดงในรูปที่ 4.63 และ 4.63.1-4.63.4 รองรับการแสดงภาพการวิเคราะห์ความมั่นคงปลอดภัยในมิติของการแพร่กระจายความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm) และแสดงภาพด้วยหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm โดยแสดงข้อความการวิเคราะห์ด้านล่างของภาพ

   3.3 Tracking Influencing Nodes ดังแสดงในรูปที่ 4.64 และ 4.64.1-4.64.4 รองรับการแสดงภาพการวิเคราะห์ความมั่นคงปลอดภัยในมิติของผู้ที่มีอิทธิพลต่อการแพร่กระจายความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในหลักการของ Social Network Analysis (SNA) ด้วย Degree Centrality, Betweenness Centrality, Closeness Centrality เพื่อค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ (Influencing Nodes) และแสดงภาพด้วยหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm เพื่อแสดงภาพผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ โดยแสดงข้อความการวิเคราะห์ด้านล่างของภาพ

3.4 Predicting Attacked Nodes ดังแสดงในรูปที่ 4.65 และ 4.65.1-4.65.4

รองรับการแสดงภาพการวิเคราะห์ความมั่นคงปลอดภัยในมิติของผู้ที่อาจได้รับผลกระทบจากความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Data Mining (Supervised Learning, Classification Analysis, oneR Algorithm) และแสดงภาพด้วยหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm เพื่อแสดงภาพเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ โดยแสดงข้อความการวิเคราะห์ด้านล่างของภาพ

4. รายการย่อยของ Setting ดังแสดงในรูปที่ 4.66 มีดังนี้

4.1 Mapping Table ดังแสดงในรูปที่ 4.67

เป็นหน้าจอเพื่อให้ผู้ใช้ระบุความสัมพันธ์ระหว่าง File ที่เรามี และไปหยอดใส่รูปแบบที่โปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application) สามารถใช้ประมวลผลได้ คือ Item- Date, Time, Attack ID, Severity, Source IP, Destination IP, Source Port, Destination Port and Message (เลือก column ของแฟ้มข้อมูลที่ผู้ใช้มี เพื่อ map กับ Date, Time, Attack ID, Severity, Source IP, Destination IP, Source Port, Destination Port and Message)

4.2 Web 2.0 ดังแสดงในรูปที่ 4.68

เป็นหน้าจอแบบ Excel sheet 3 column (URL, Start IP Addresses, End IP Adresses) เพื่อให้ผู้ใช้ระบุข้อมูลเพื่อให้โปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application) รู้ว่า IP อะไรบ้างที่เป็น Web 2.0

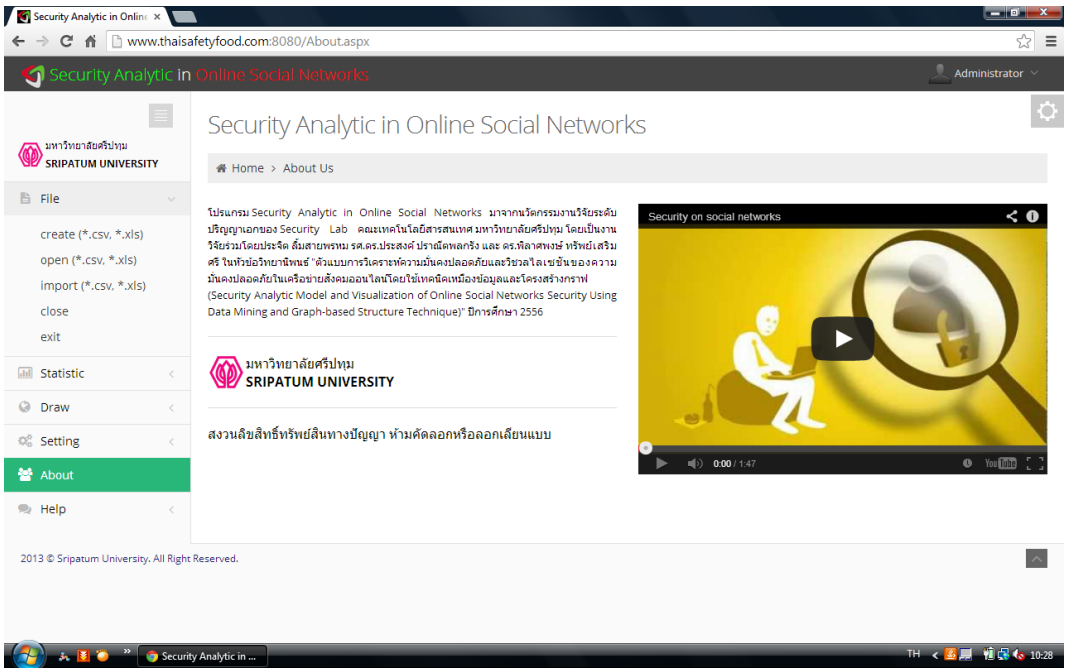
4.3 Database ดังแสดงในรูปที่ 4.69

เป็นหน้าจอเพื่อให้ผู้ใช้ระบุ Path ของ destination ของการประมวลผลจากฐานข้อมูลของ Log File ที่องค์กรมี กับโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์

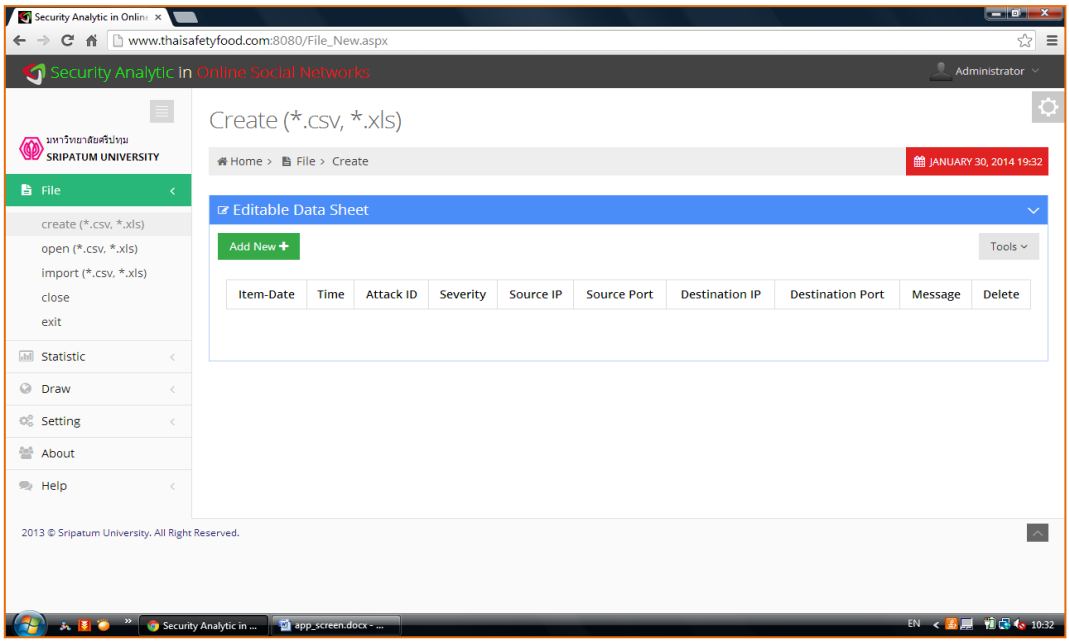
(Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application)

5. รายการย่อยของ About ดังแสดงในรูปที่ 4.70 เพื่อบอกข้อมูลของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application)
6. รายการย่อยของ Help ดังแสดงในรูปที่ 4.71 มีดังนี้
   6.1 Create Data Sheet ดังแสดงในรูปที่ 4.72
   เป็นหน้าจอแนะนำการใส่ข้อมูลที่ File-Create และ File-Open โดยต้องใส่เรียงตาม Item- Date, Time, Attack ID, Severity, Source IP, Destination IP, Source Port, Destination Port and Message
   6.2 How to Import Data ดังแสดงในรูปที่ 4.73 เพื่อแนะนำการ import data โดยมี 2 วิธี
      6.2.1 ทำการ Create Data Sheet ที่โปรแกรมอื่นๆ แล้วเก็บเป็น (*.csv, *.xls) ที่ประกอบด้วย Item- Date, Time, Attack ID, Severity, Source IP, Destination IP, Source Port, Destination Port and Message จากนั้นใช้ File-Open
      6.2.2 เลือก import data โดยต้องทำการ setting Mapping Table ความสัมพันธ์ระหว่าง file ที่เรามี และไปหยอดใส่ใน Item- Date, Time, Attack ID, Severity, Source IP, Destination IP, Source Port, Destination Port and Message จากนั้นเลือก File-Import
   6.3 Mapping Table ดังแสดงในรูปที่ 4.74 เป็นหน้าจอสร้างความสัมพันธ์ระหว่าง file ที่เรามี และไปหยอดใส่ใน Item- Date, Time, Attack ID, Severity, Source IP, Destination IP, Source Port, Destination Port and Message ที่โปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application) สามารถนำไปประมวลผลได้
   6.4 Trouble Shooting ดังแสดงในรูปที่ 4.75 เพื่อแนะนำการแก้ปัญหาต่างๆ ของการใช้งานโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการ

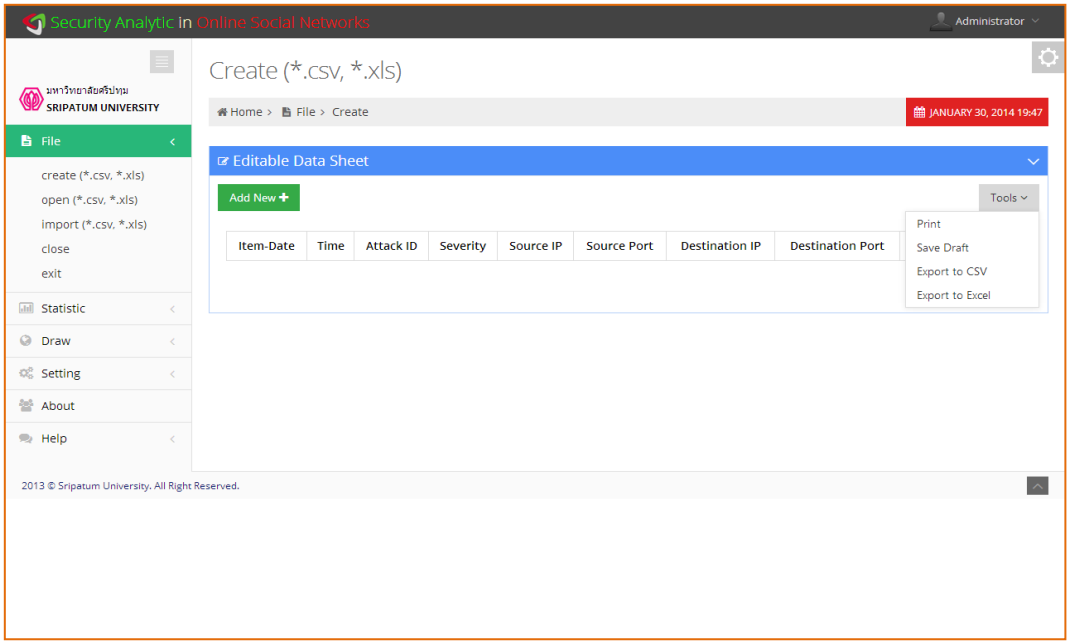
ถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ (Security Analytic Model for Anomaly and Attack Patterns in Online Social Networks Application)



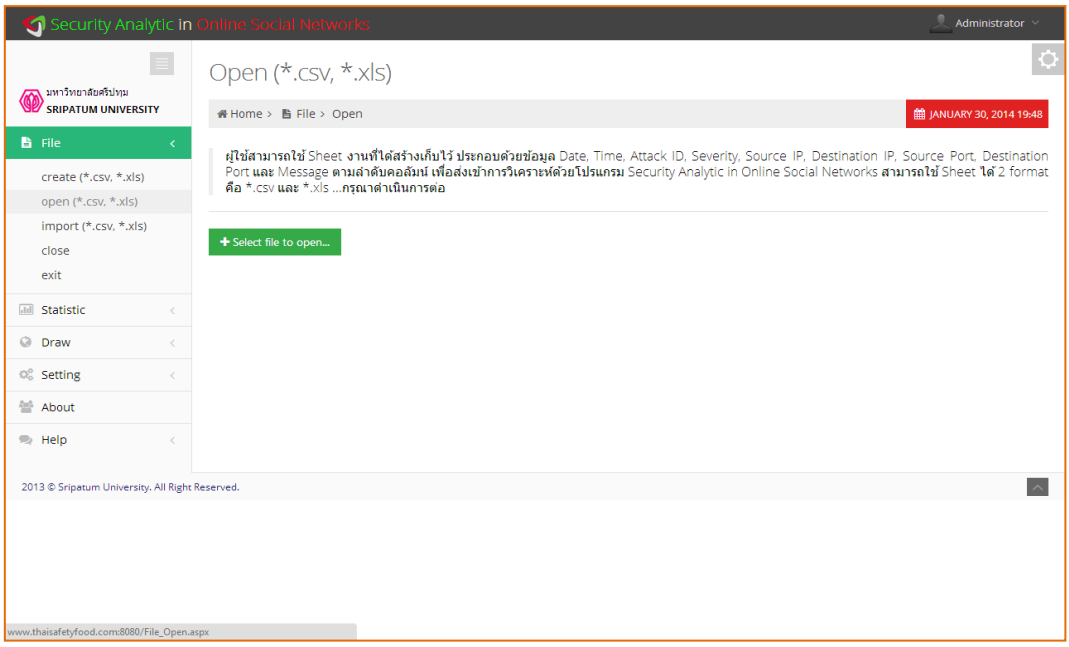
รูปที่ 4.47 หน้าจอรายการย่อย File ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



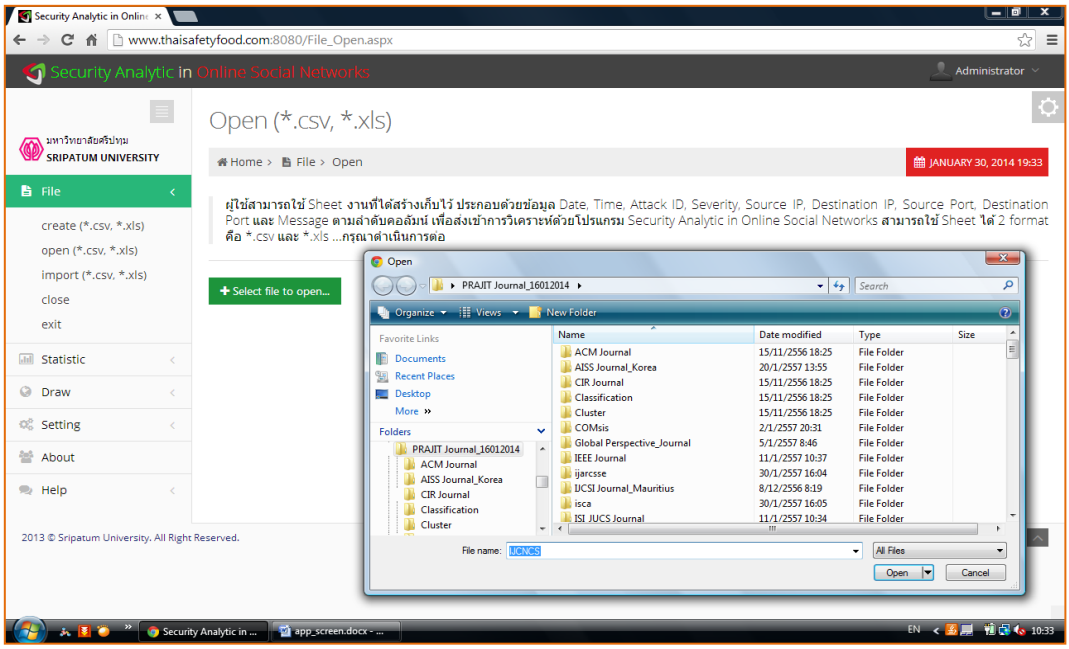
รูปที่ 4.48 หน้าจอรายการย่อย File-Create ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



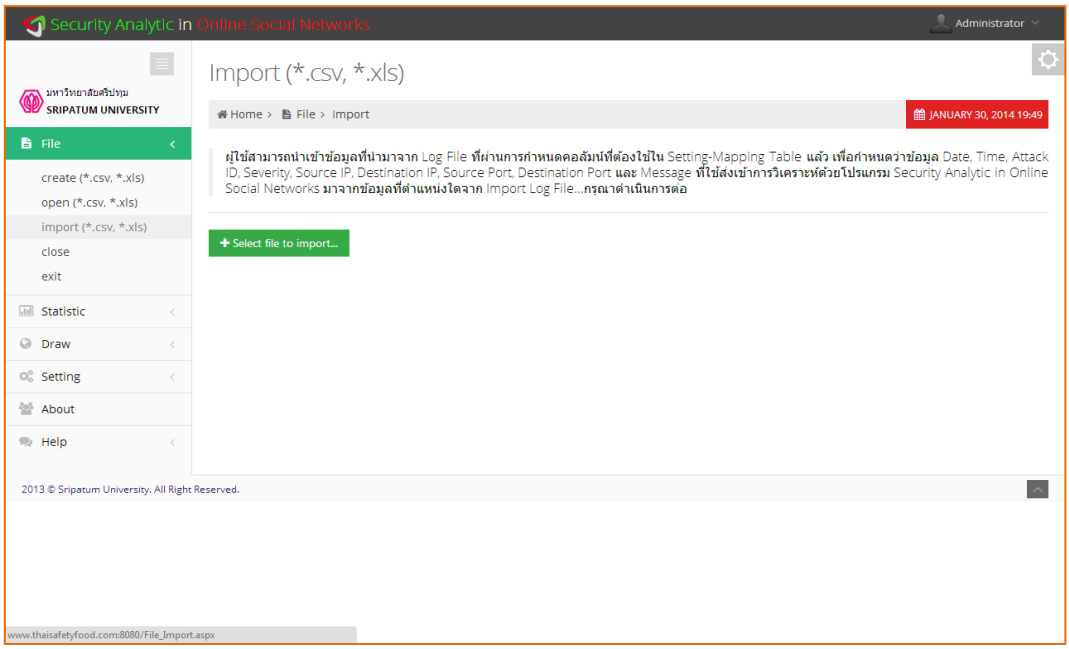
รูปที่ 4.49 หน้าจอรายการย่อย File-Create-Tools ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



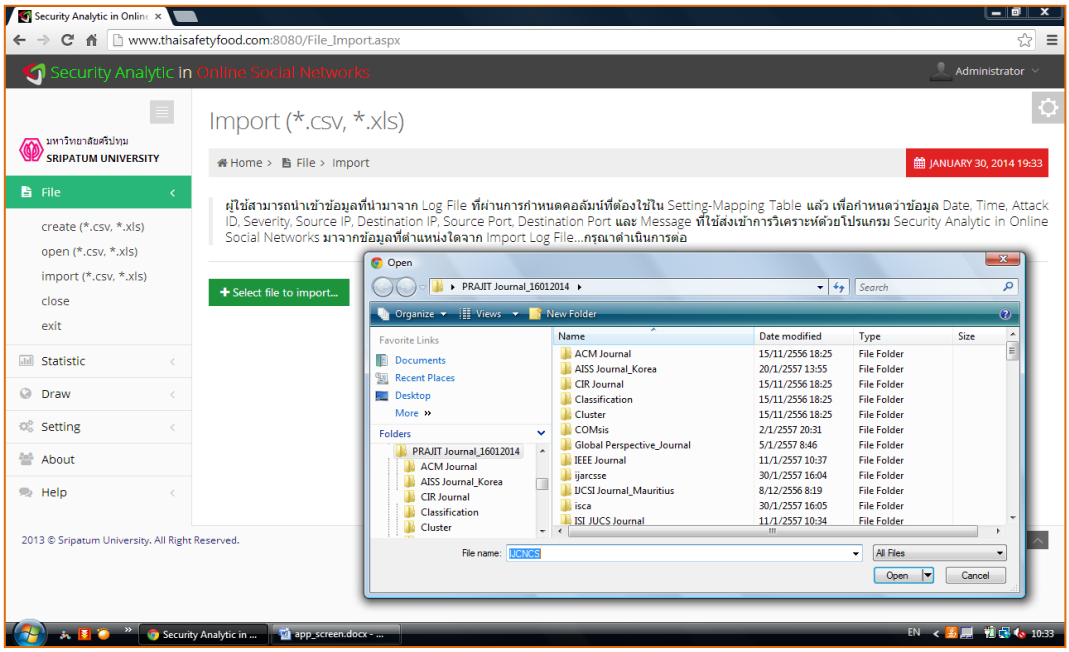
รูปที่ 4.50 หน้าจอรายการย่อย File-Open ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



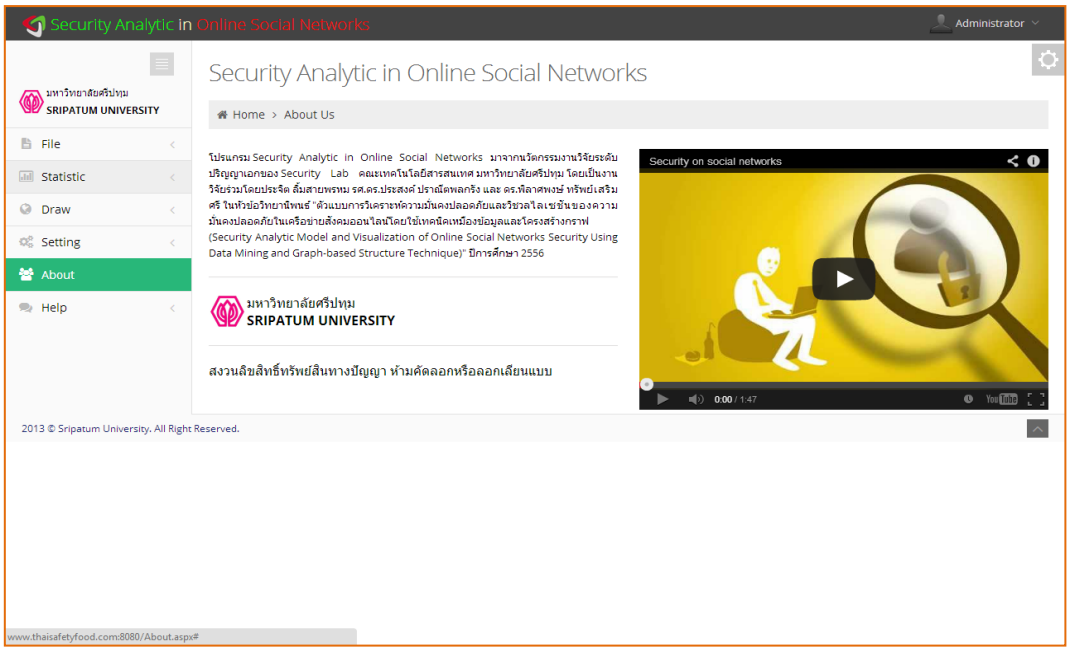
รูปที่ 4.51 หน้าจอรายการย่อย File-Open-Select ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



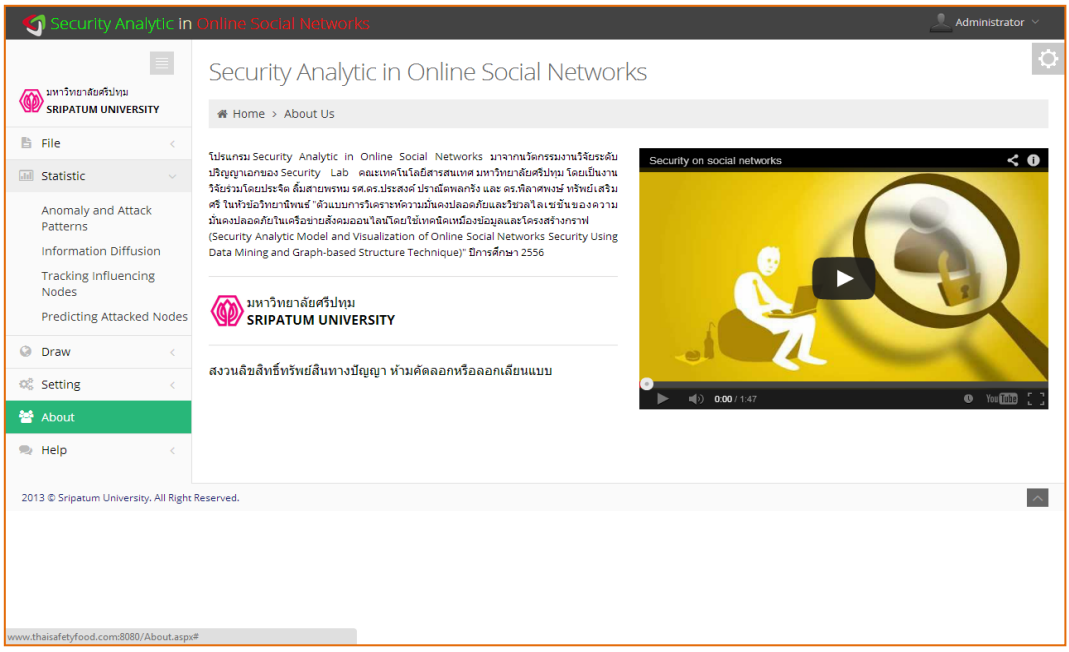
รูปที่ 4.52 หน้าจอรายการย่อย File-Import ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



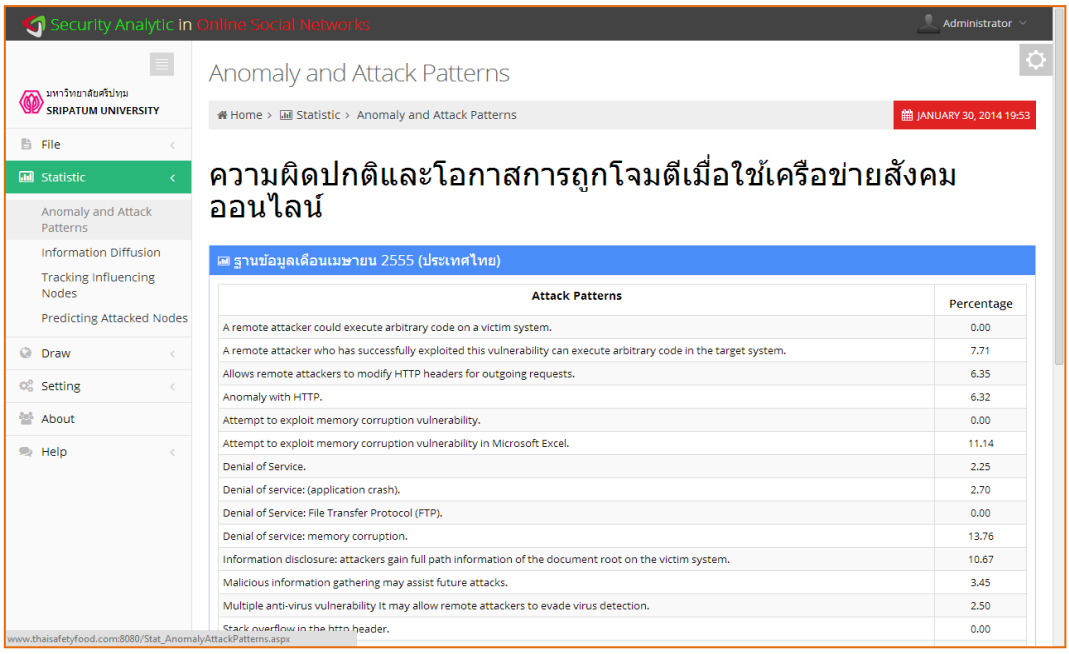
รูปที่ 4.53 หน้าจอรายการย่อย File-Import-Select ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



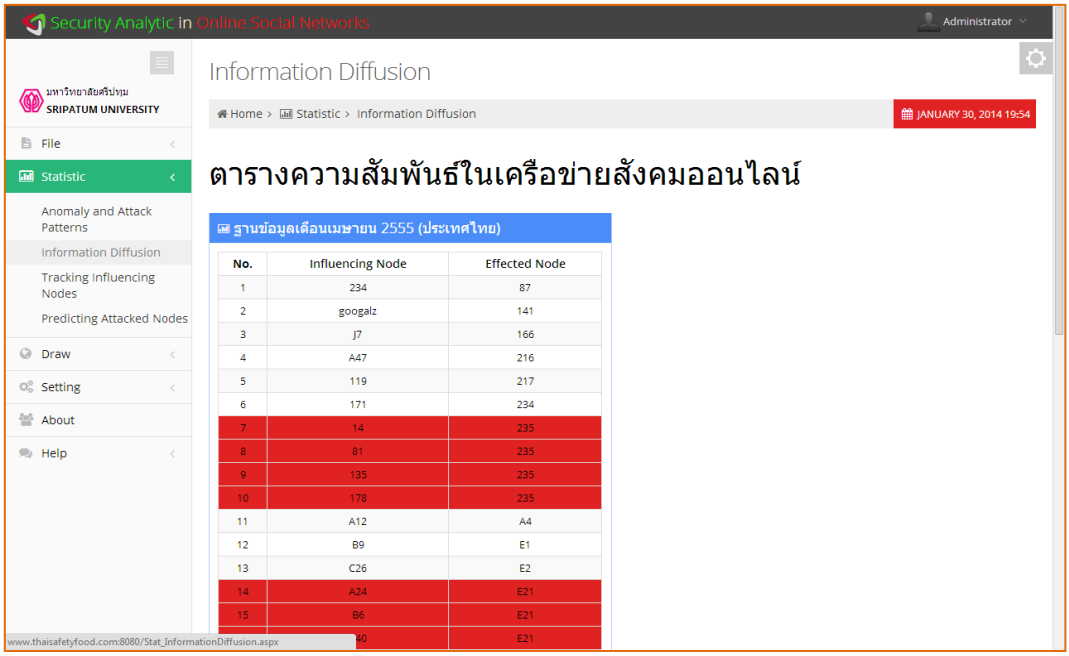
รูปที่ 4.54 หน้าจอรายการย่อย Statistic ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 1



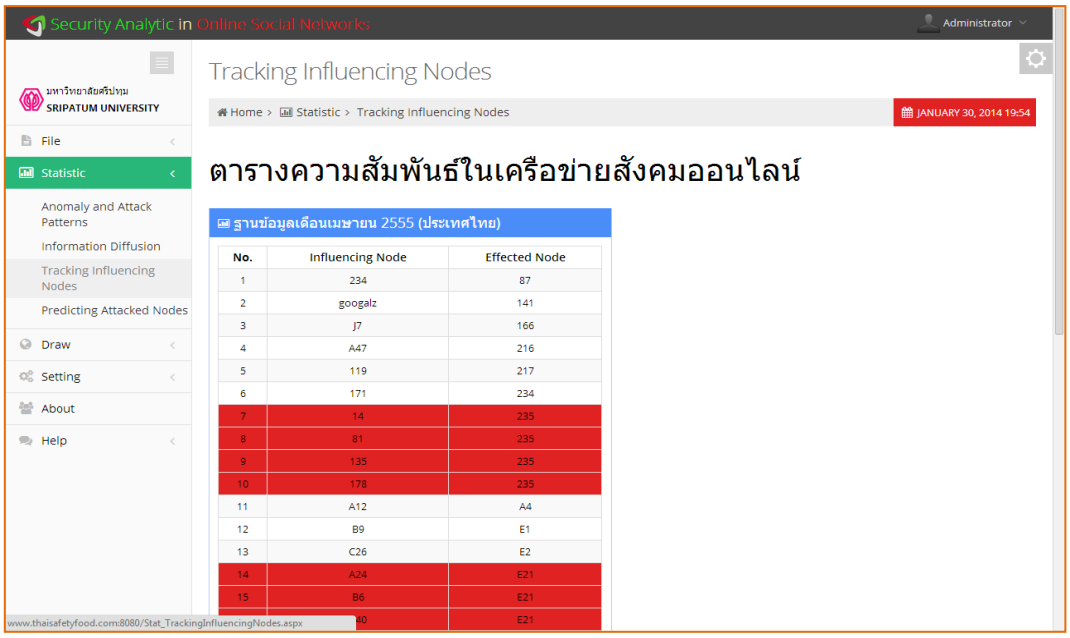
รูปที่ 4.55 หน้าจอรายการย่อย Statistic ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 2



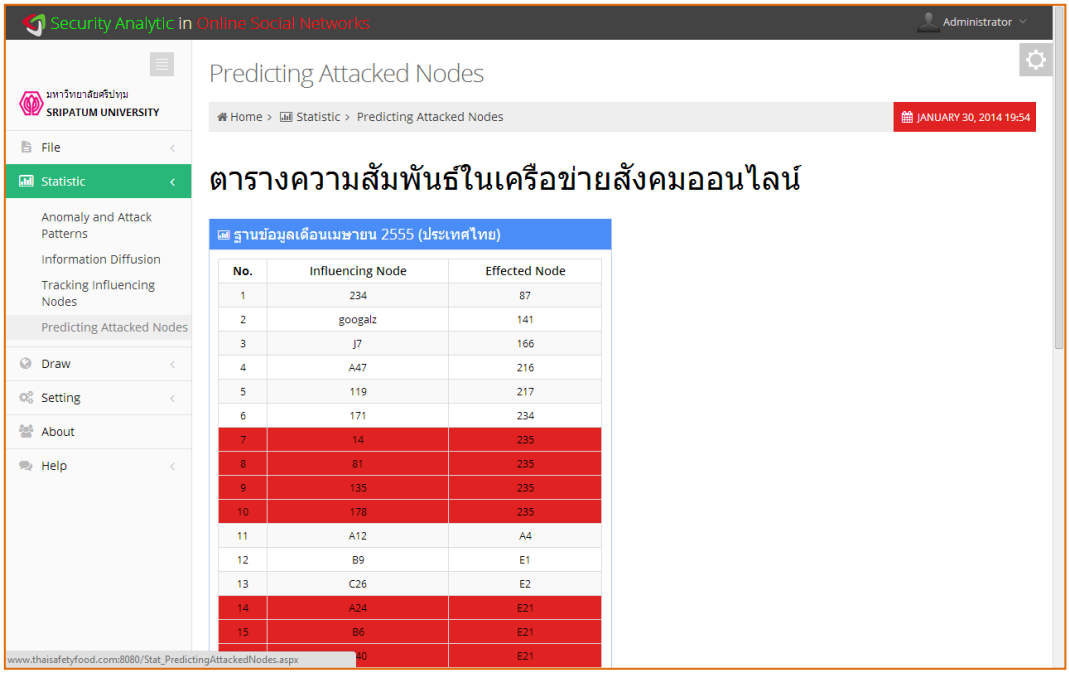
รูปที่ 4.56 หน้าจอรายการย่อย Statistic-Anomaly and Attack Patterns ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



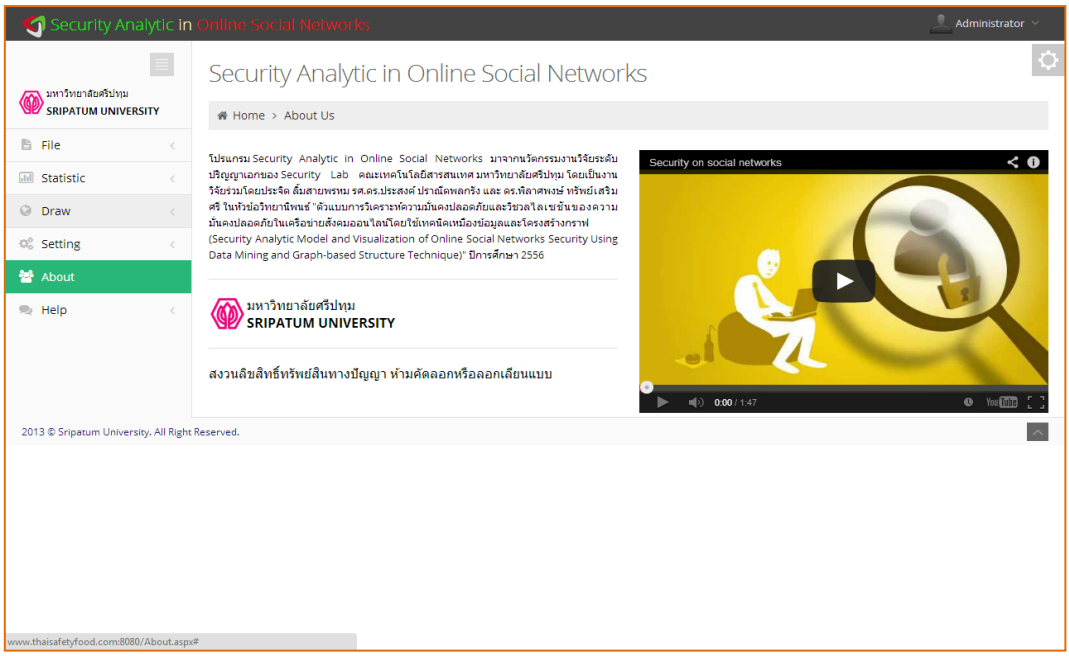
รูปที่ 4.57 หน้าจอรายการย่อย Statistic-Information Diffusion ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



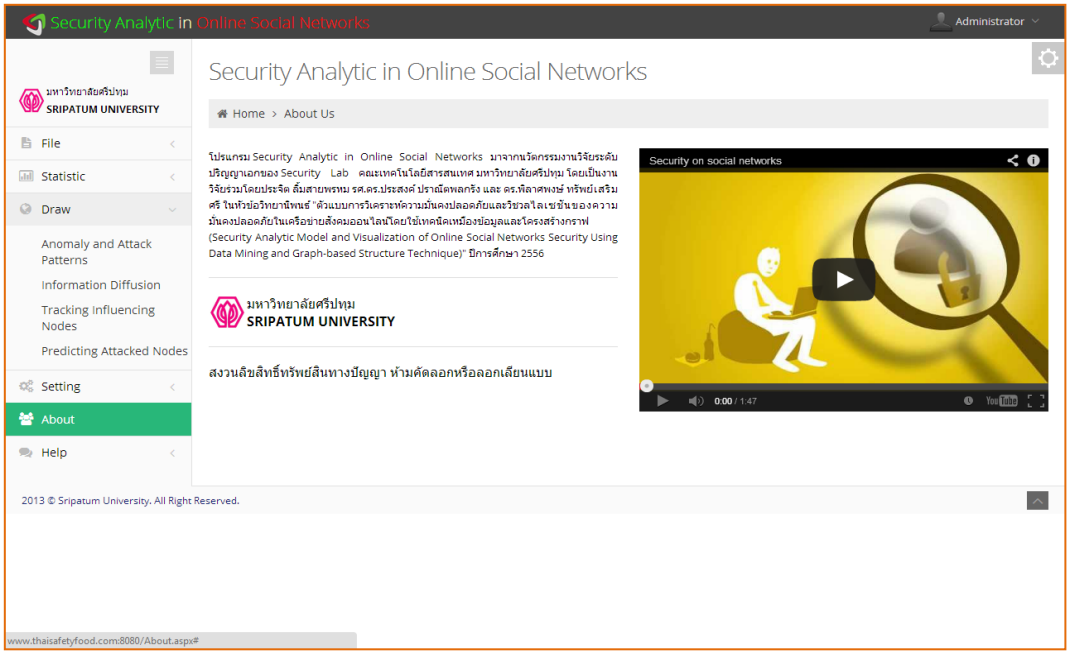
รูปที่ 4.58 หน้าจอรายการย่อย Statistic-Tracking Influencing Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



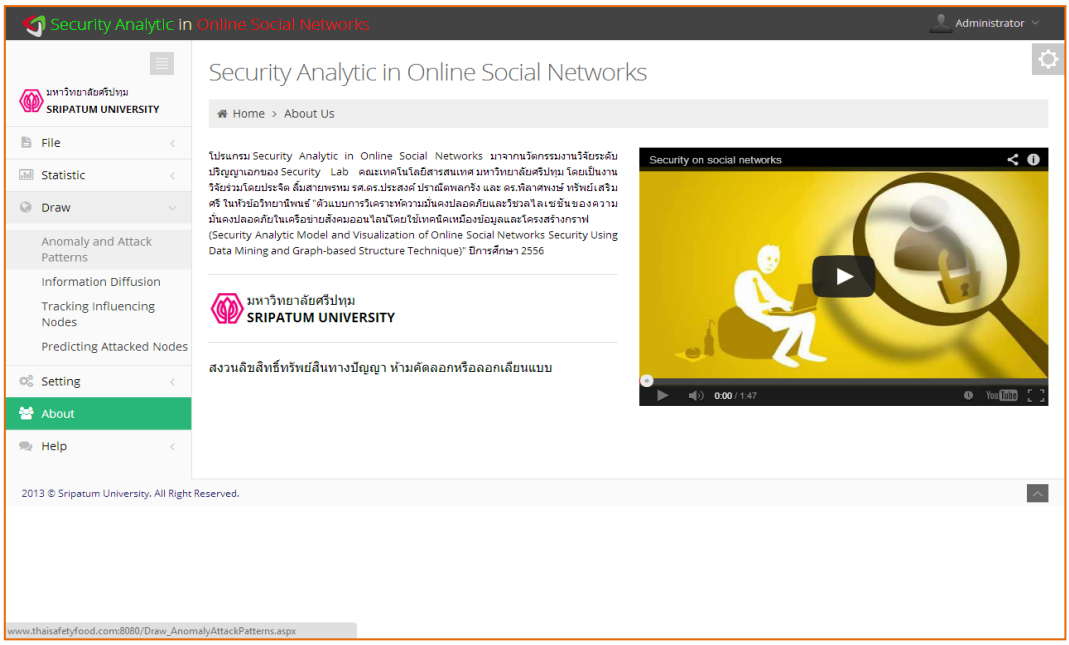
รูปที่ 4.59 หน้าจอรายการย่อย Statistic-Predicting Attacked Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



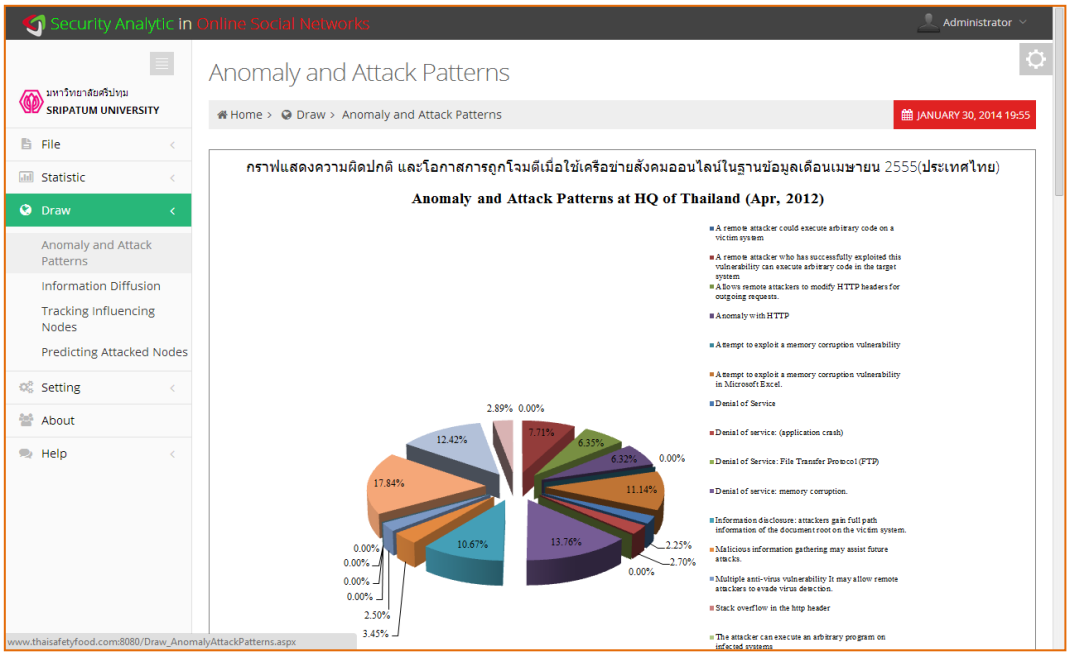
รูปที่ 4.60 หน้าจอรายการย่อย Draw ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 1



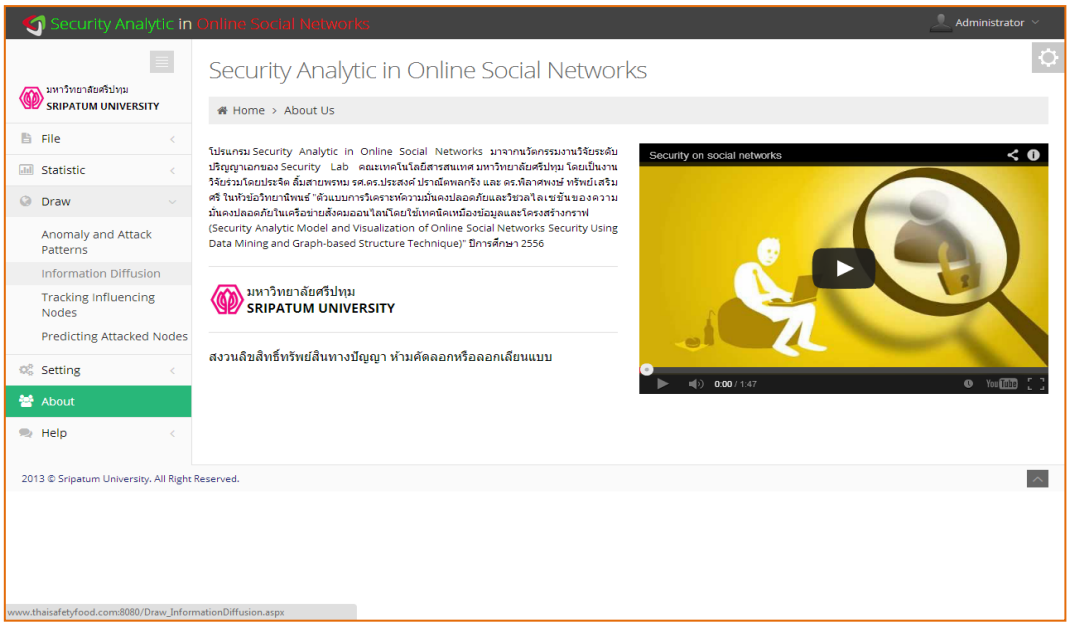
รูปที่ 4.61 หน้าจอรายการย่อย Draw ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 2



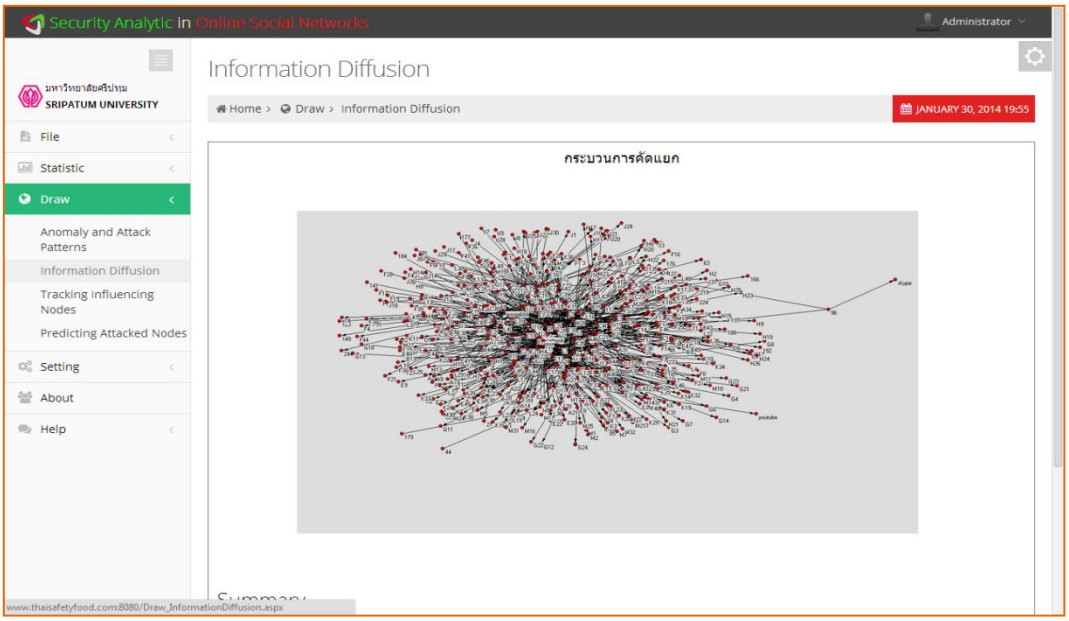
รูปที่ 4.62 หน้าจอรายการย่อย Draw-Anomaly and Attack Patterns ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



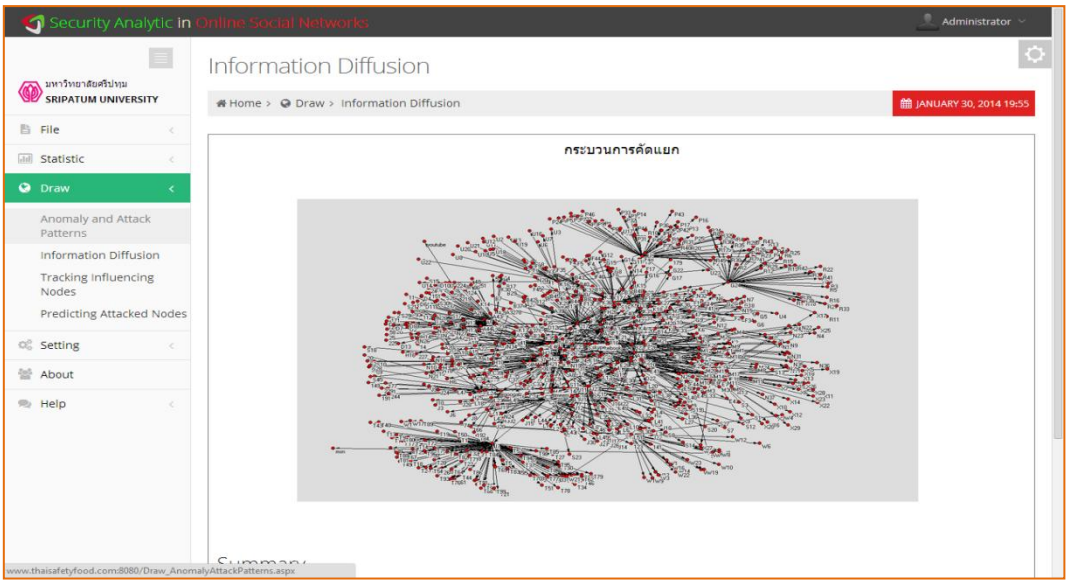
รูปที่ 4.62.1 หน้าจอรายการย่อย Draw-Anomaly and Attack Patterns ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



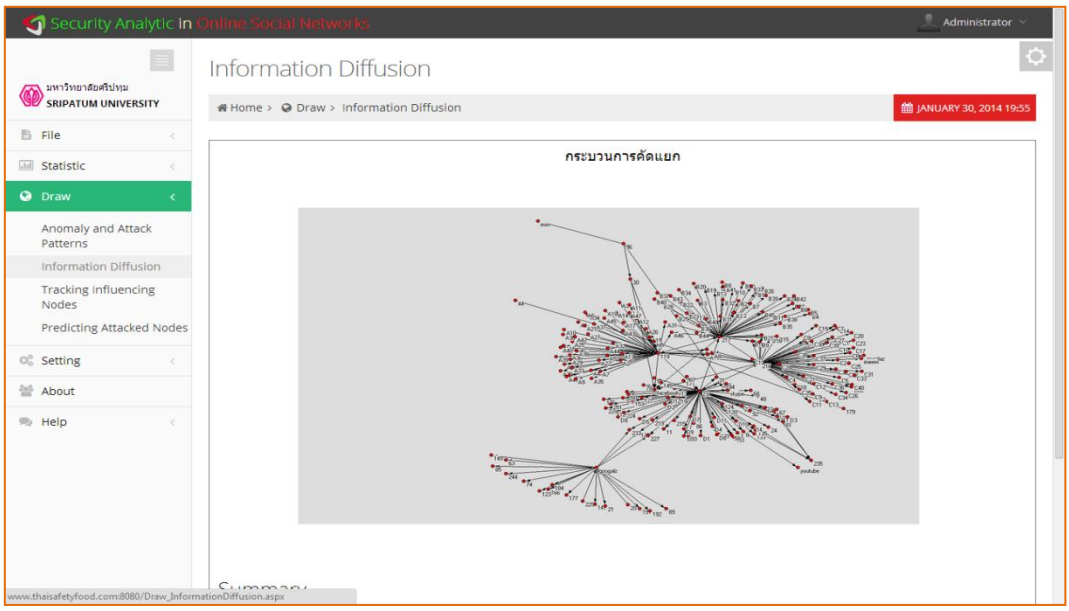
รูปที่ 4.63 หน้าจอรายการย่อย Draw-Information Diffusion ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



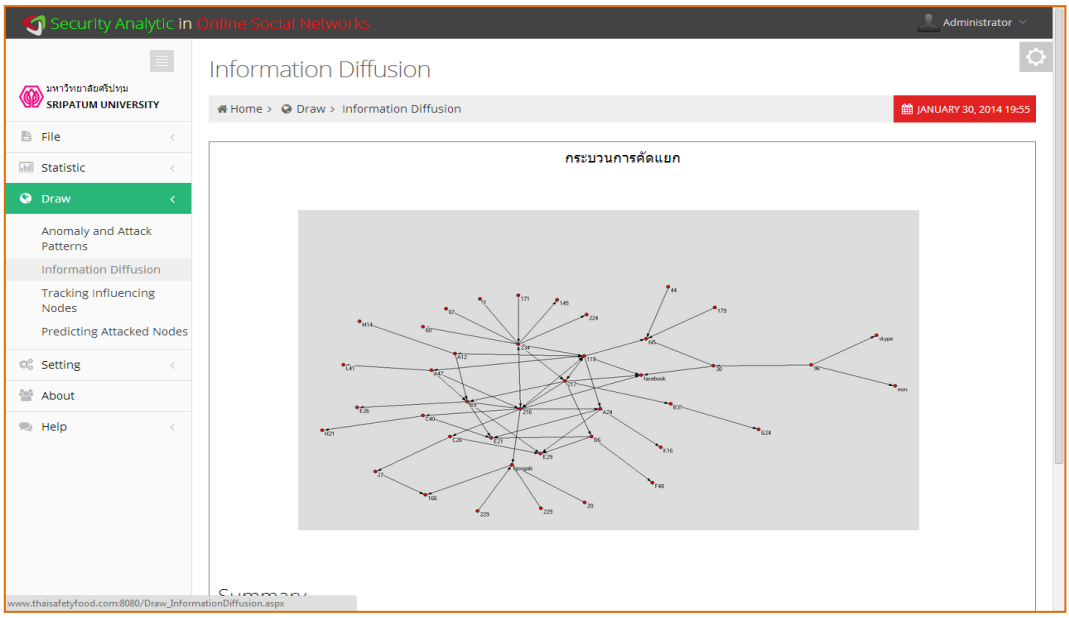
รูปที่ 4.63.1 หน้าจอรายการย่อย Draw-Information Diffusion ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 1



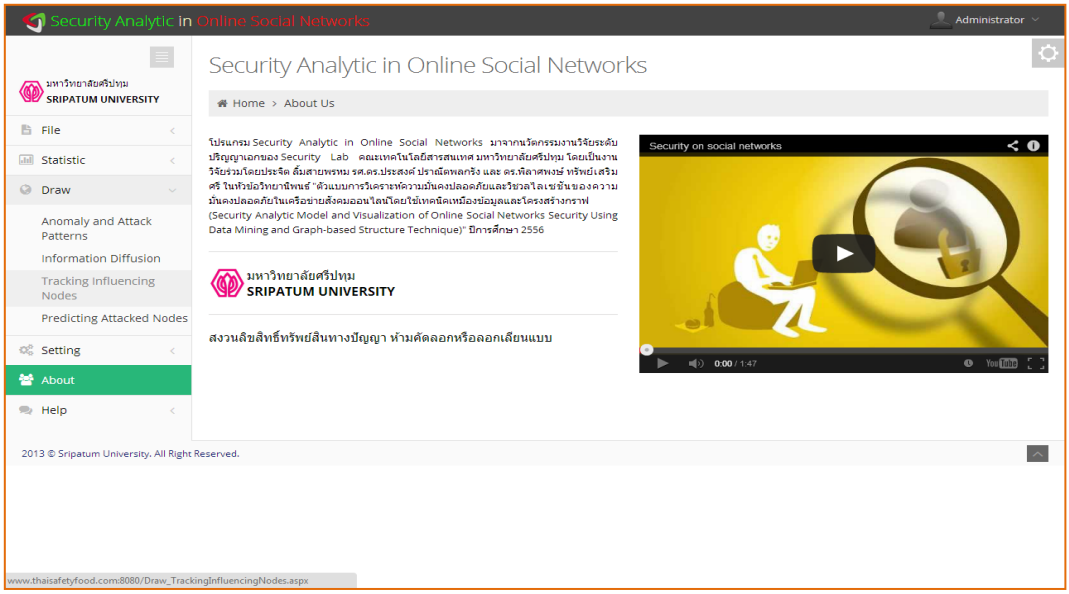
รูปที่ 4.63.2 หน้าจอรายการย่อย Draw-Information Diffusion ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 2



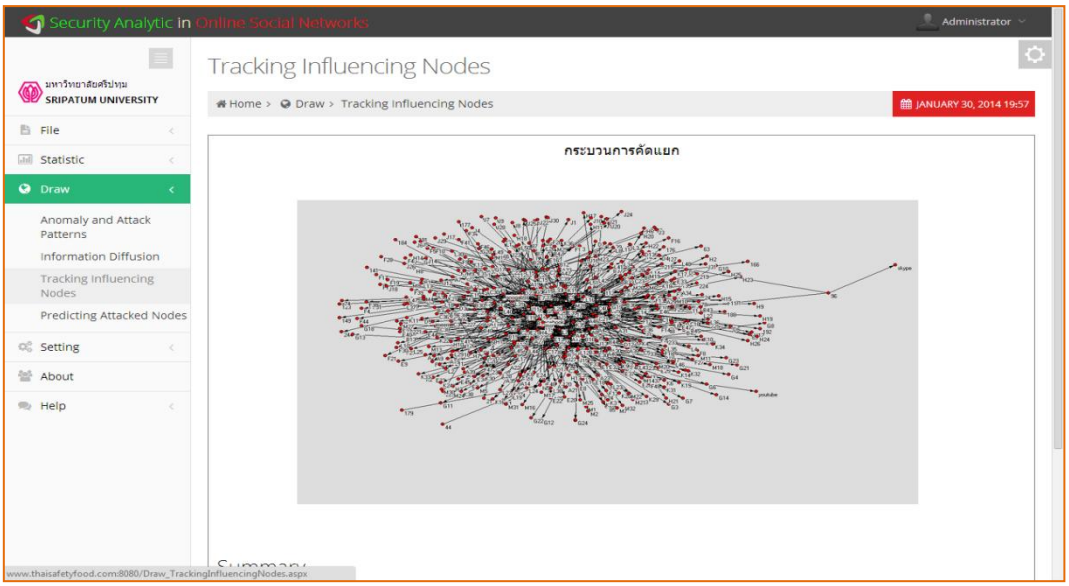
รูปที่ 4.63.3 หน้าจอรายการย่อย Draw-Information Diffusion ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 3



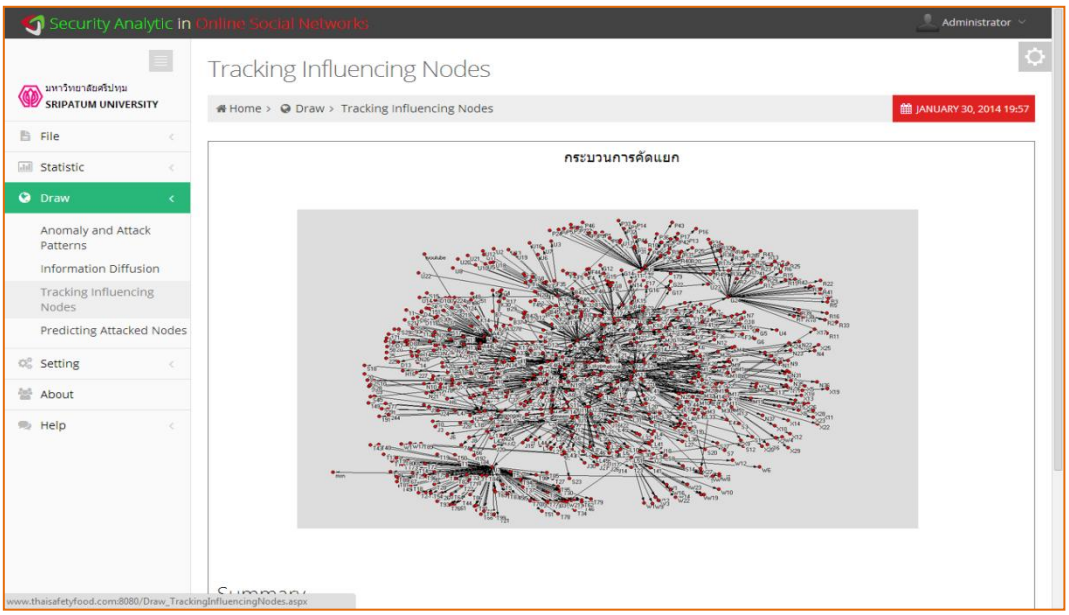
รูปที่ 4.63.4 หน้าจอรายการย่อย Draw-Information Diffusion ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 4



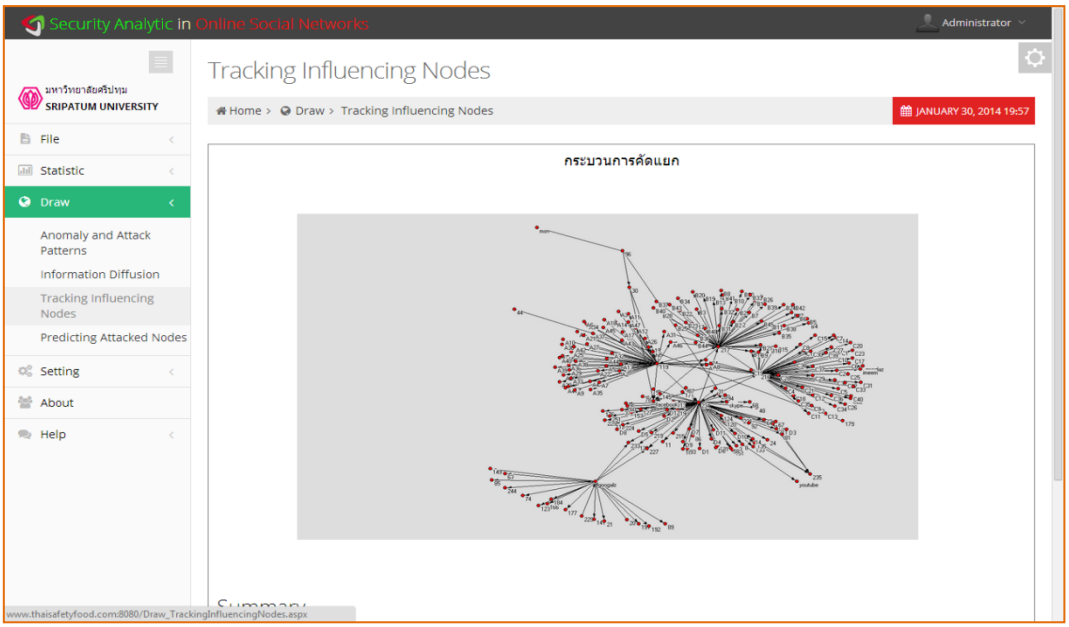
รูปที่ 4.64 หน้าจอรายการย่อย Draw-Tracking Influencing Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



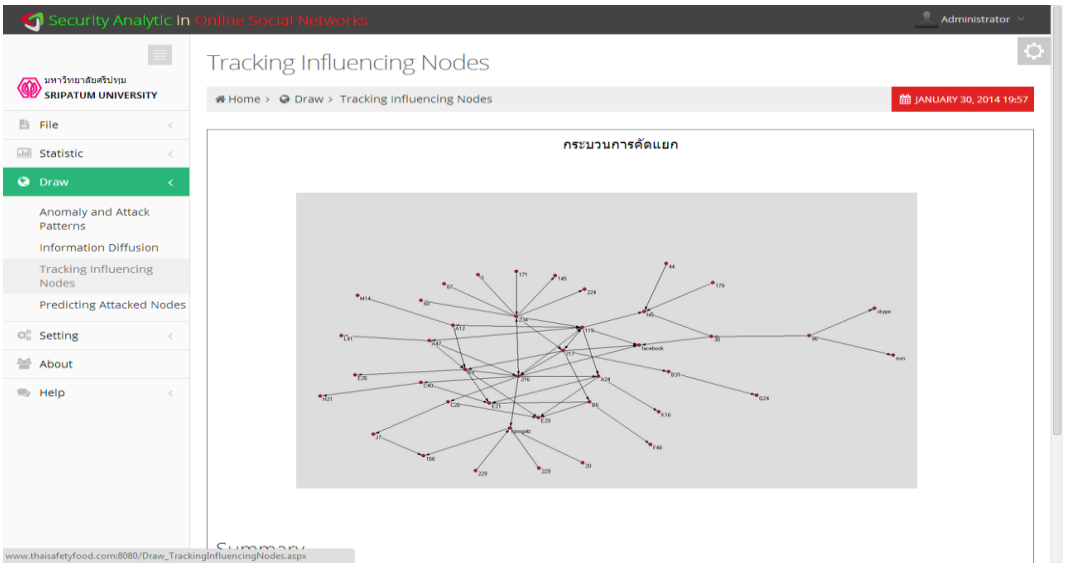
รูปที่ 4.64.1 หน้าจอรายการย่อย Draw-Tracking Influencing Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 1



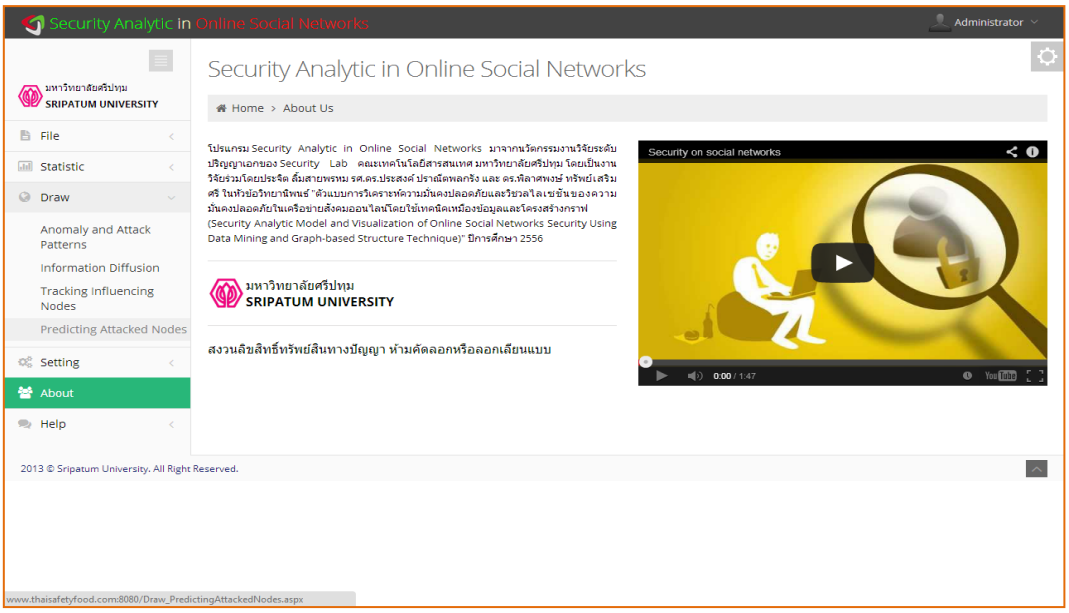
รูปที่ 4.64.2 หน้าจอรายการย่อย Draw-Tracking Influencing Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 2



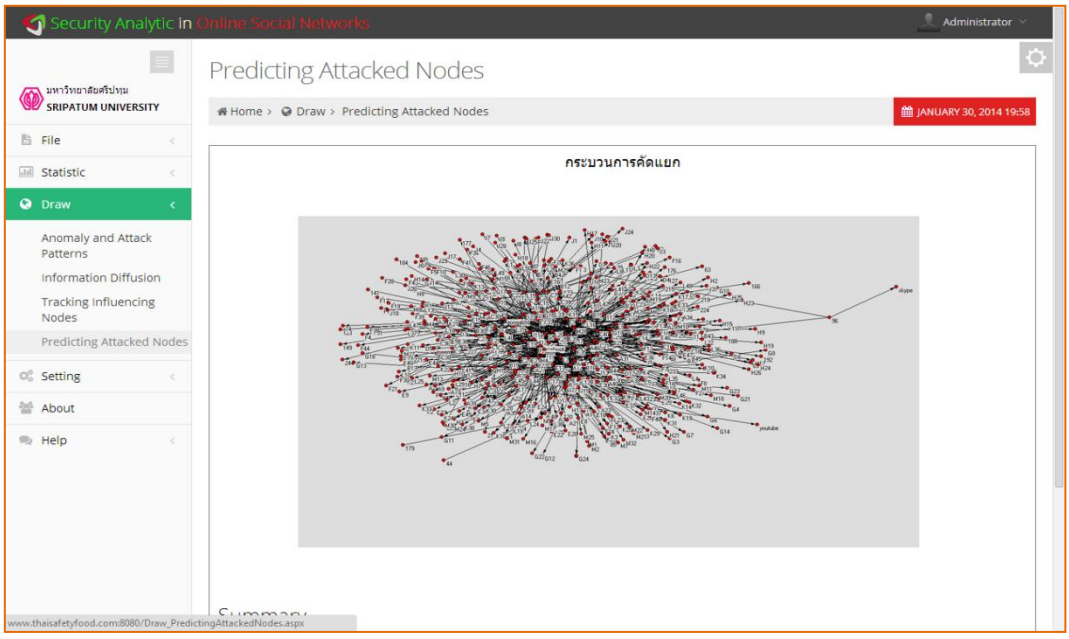
รูปที่ 4.64.3 หน้าจอรายการย่อย Draw-Tracking Inluencing Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 3



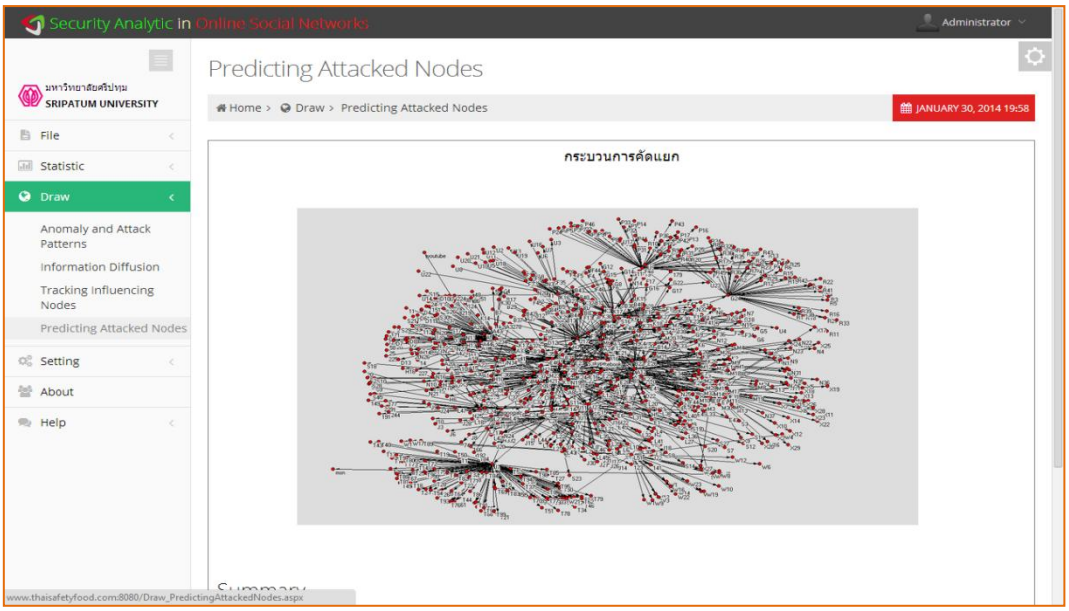
รูปที่ 4.64.4 หน้าจอรายการย่อย Draw-Tracking Influencing Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 4



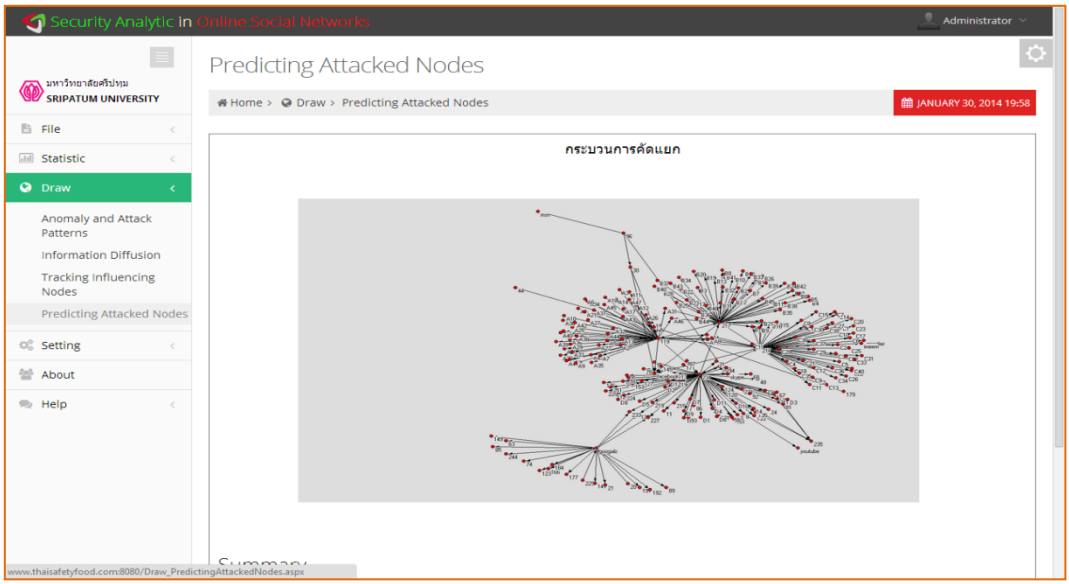
รูปที่ 4.65 หน้าจอรายการย่อย Draw-Predicting Attacked Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



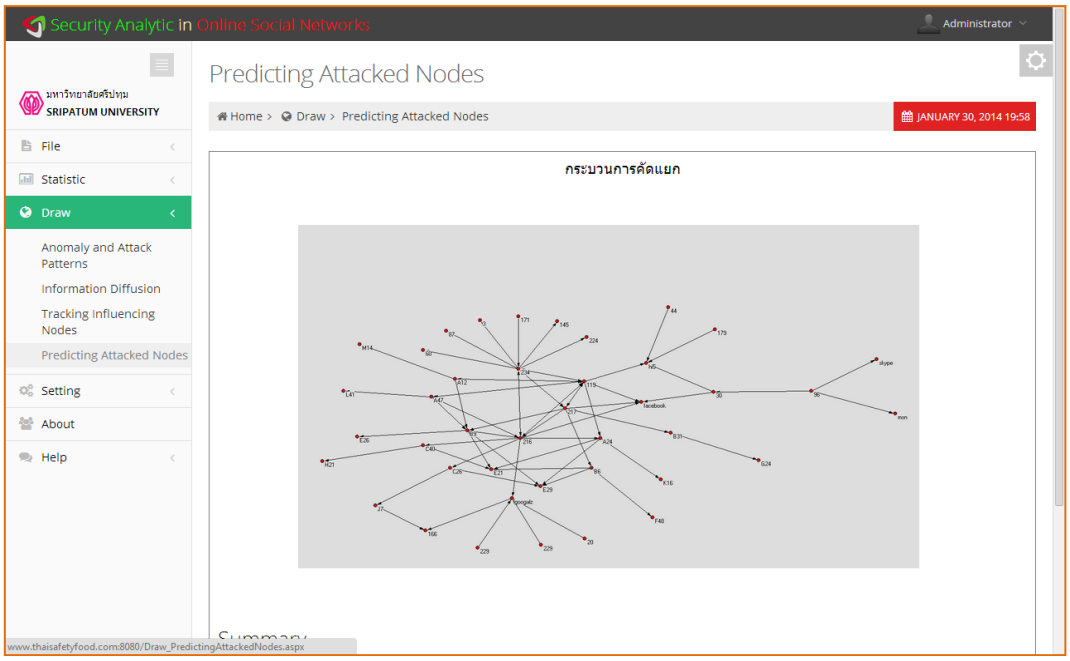
รูปที่ 4.65.1 หน้าจอรายการย่อย Draw-Predicting Attacked Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 1



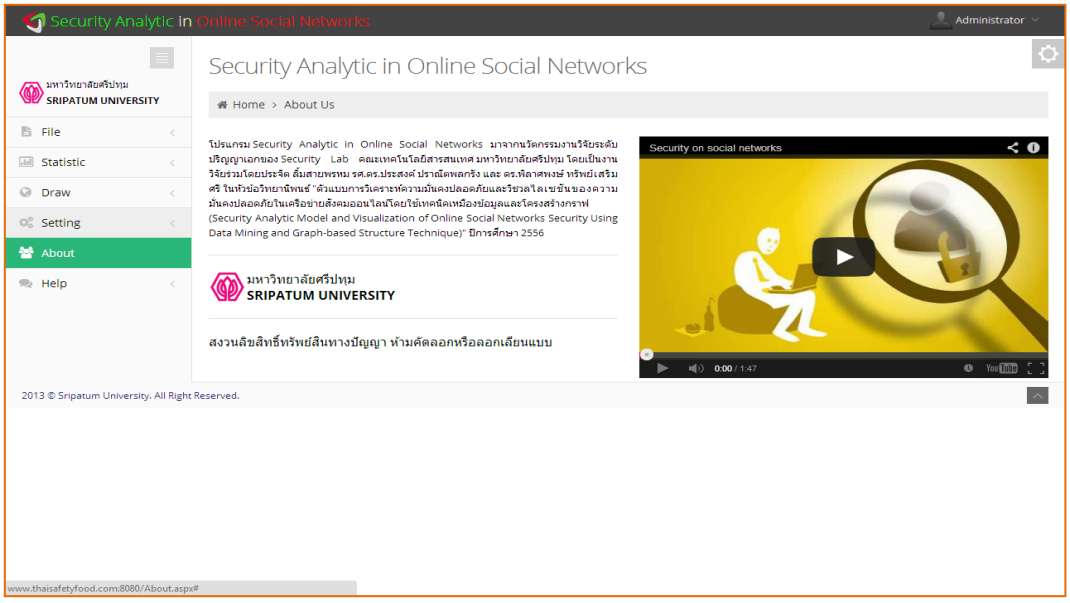
รูปที่ 4.65.2 หน้าจอรายการย่อย Draw-Predicting Attacked Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 2



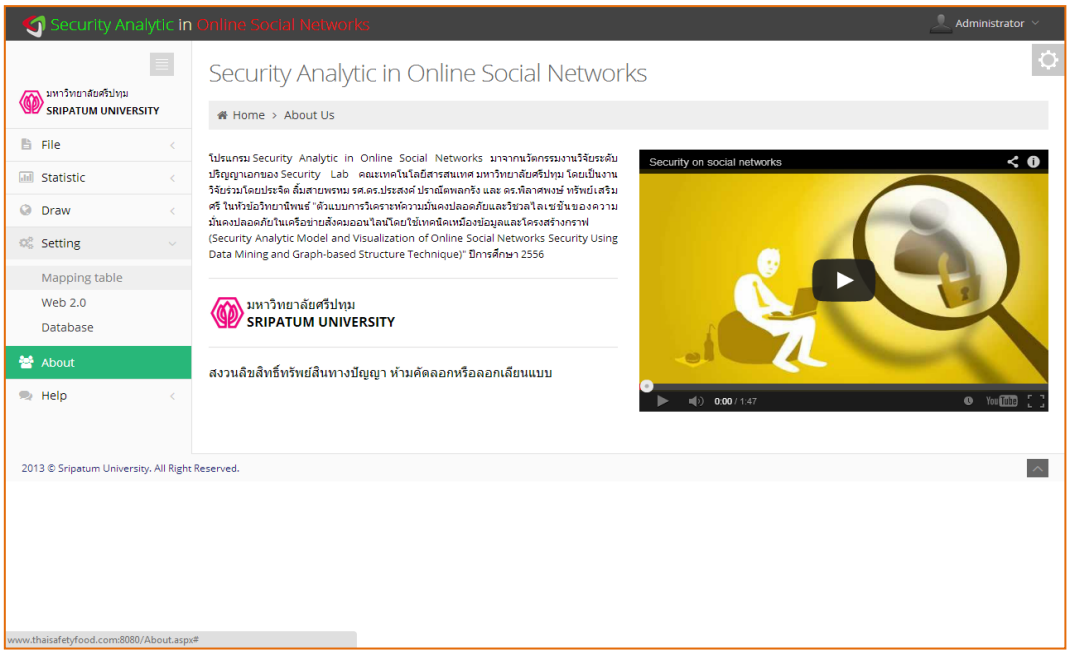
รูปที่ 4.65.3 หน้าจอรายการย่อย Draw-Predicting Attacked Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 3



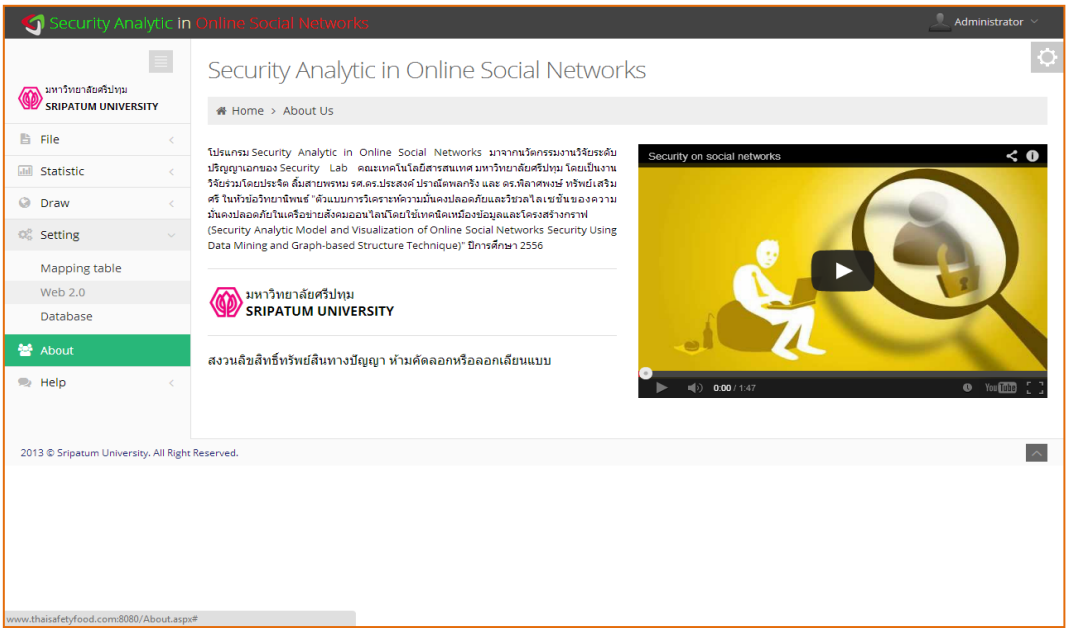
รูปที่ 4.65.4 หน้าจอรายการย่อย Draw-Predicting Attacked Nodes ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ หน้าที่ 4



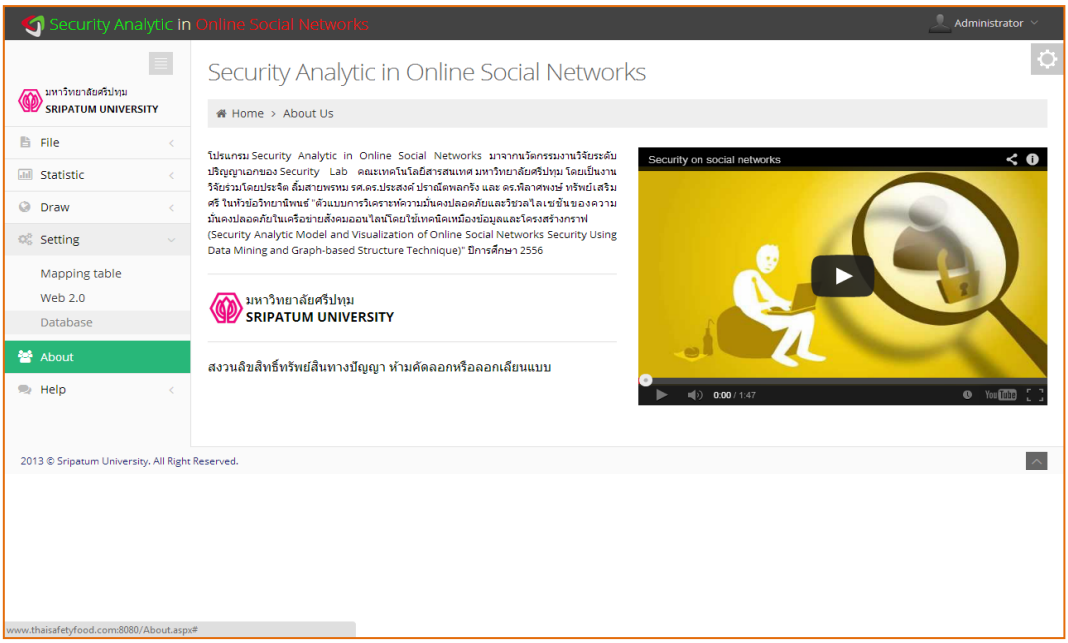
รูปที่ 4.66 หน้าจอรายการย่อย Setting ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



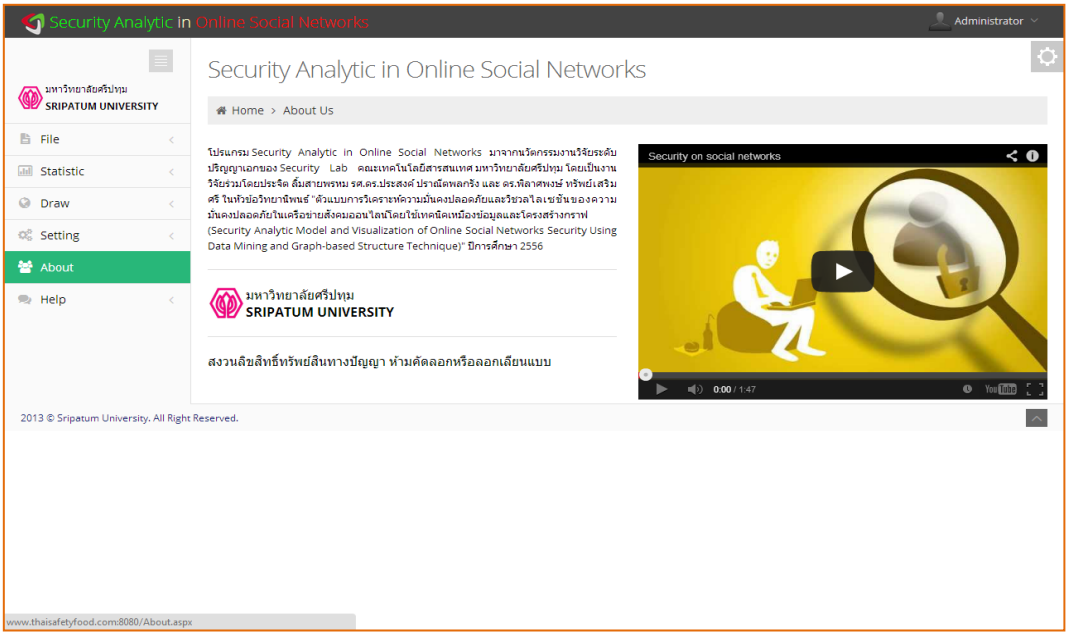
รูปที่ 4.67 หน้าจอรายการย่อย Setting-Mapping Table ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



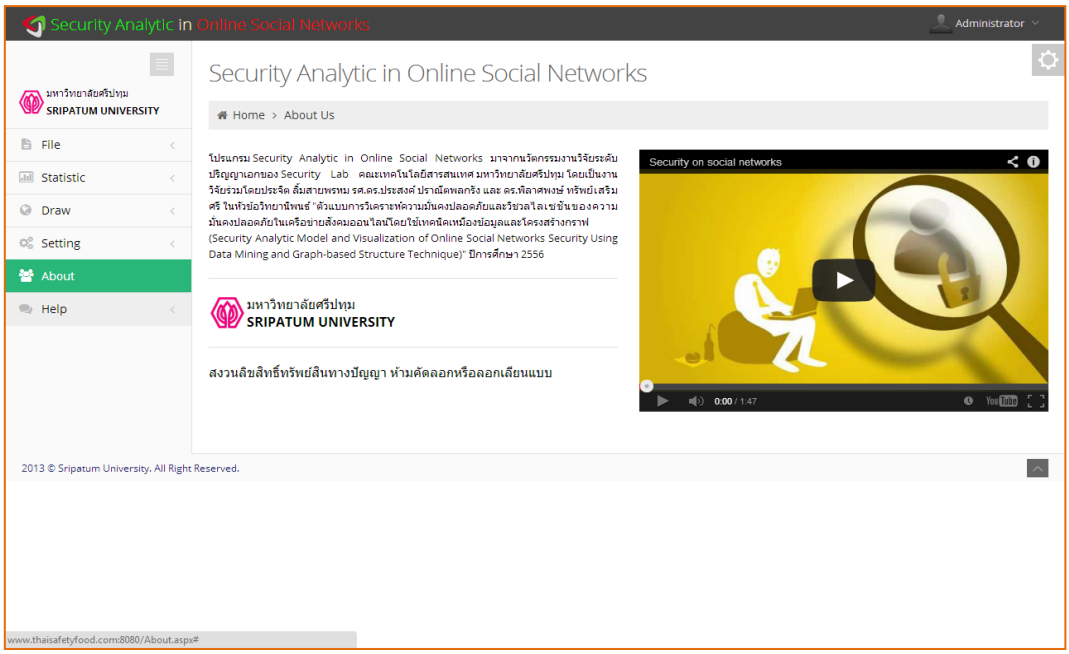
รูปที่ 4.68 หน้าจอรายการย่อย Setting- Online Social Networks ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



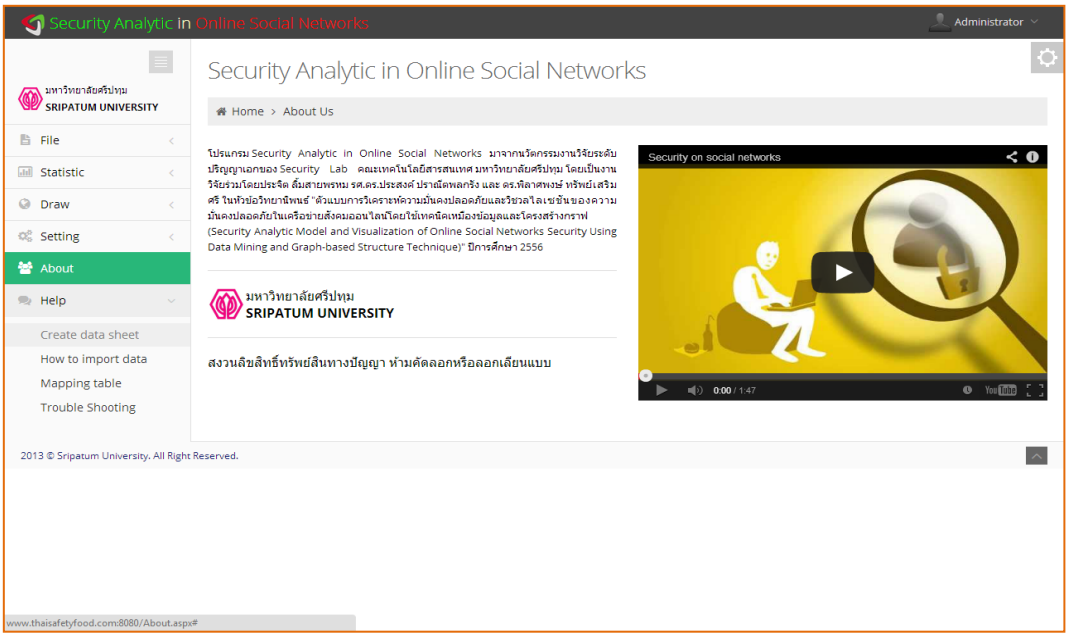
รูปที่ 4.69 หน้าจอรายการย่อย Setting-Database ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



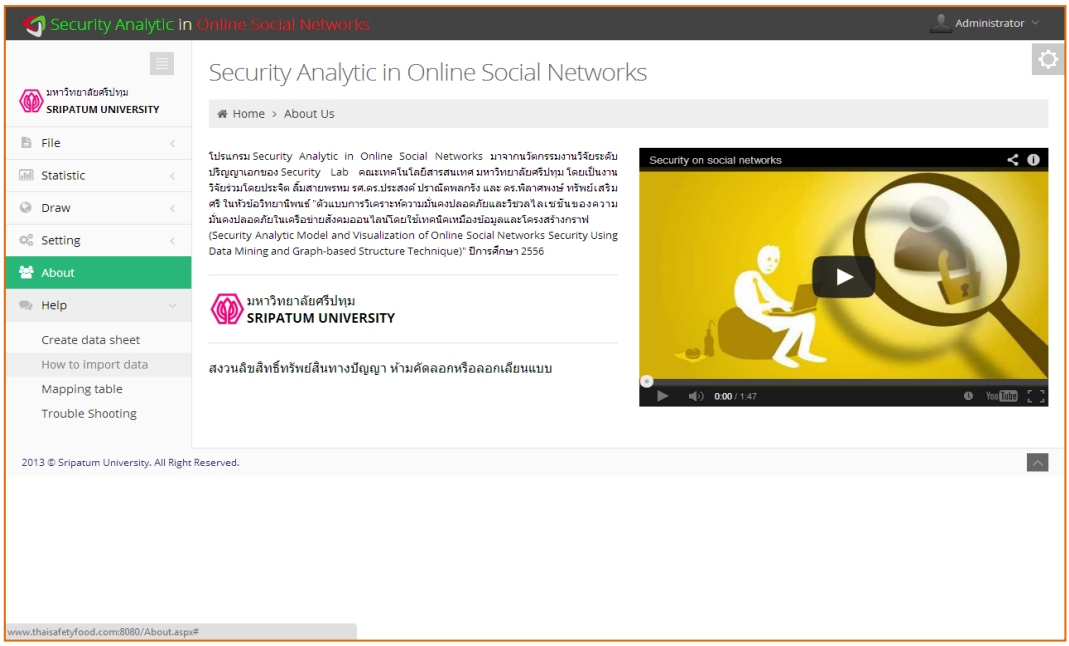
รูปที่ 4.70 หน้าจอรายการย่อย About ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



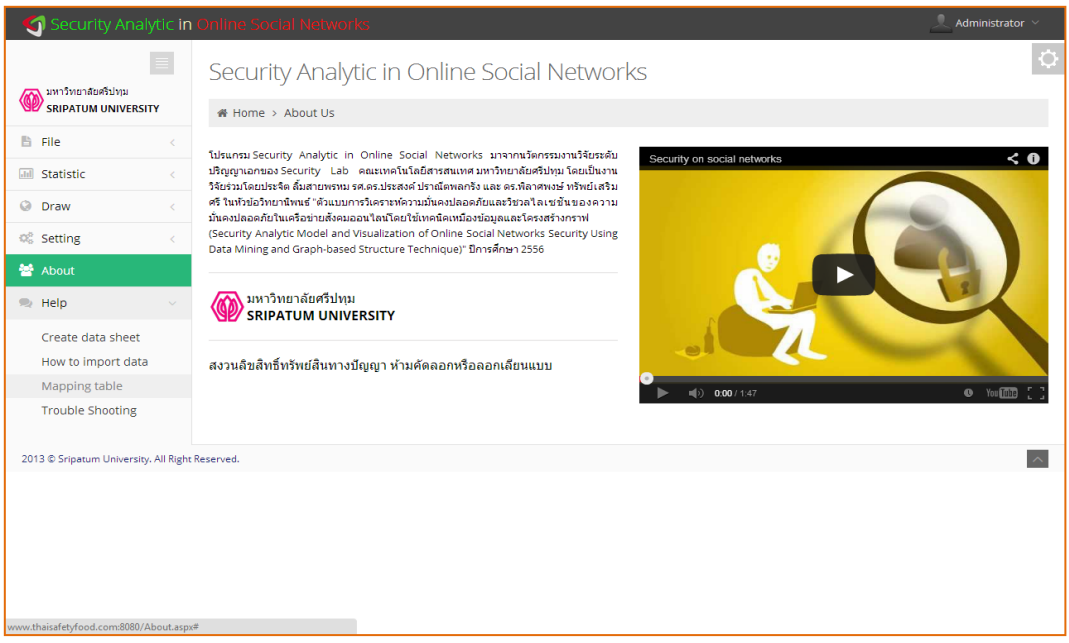
รูปที่ 4.71 หน้าจอรายการย่อย Help ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



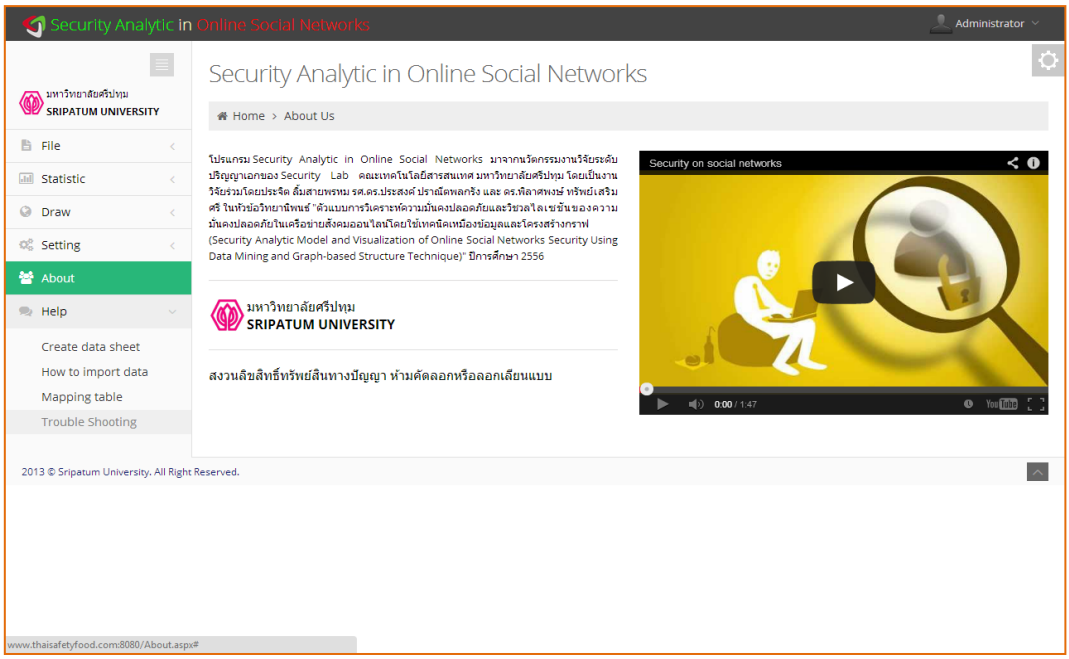
รูปที่ 4.72 หน้าจอรายการย่อย Help-Create Data Sheet ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



รูปที่ 4.73 หน้าจอรายการย่อย Help-How to Import Data ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



รูปที่ 4.74 หน้าจอรายการย่อย Help-Mapping Table ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์



รูปที่ 4.75 หน้าจอรายการย่อย Help-Trouble Shooting ของโปรแกรมวิเคราะห์ความมั่นคงปลอดภัยต่อความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์

4.7 สรุป

เนื้อหาในบทที่ 4 นี้เป็นการนำเสนอผลจากการวิจัย ตามวัตถุประสงค์ของงานวิจัย ซึ่งประกอบด้วย (1) เพื่อทำการวิเคราะห์หาความผิดปกติและโอกาสการถูกโจมตีจากการใช้เครือข่ายสังคมออนไลน์ (2) เพื่อศึกษารูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (3) เพื่อพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟสำหรับรองรับการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริง โดยมีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 % และ (4) เพื่อพัฒนาตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า โดยมีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 % ซึ่งจากผลการวิจัยข้างต้นสามารถสนับสนุนวัตถุประสงค์ของงานวิจัยได้ครบถ้วน ดังนี้

1. สามารถพบความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์โดยตัวอย่างชุดข้อมูลประเทศไทยเดือนเมษายน 2556 พบความผิดปกติและโอกาสการถูกโจมตีสูงสุดด้วยการทำให้ระบบสื่อสารขัดข้องสูงถึง 16.10% รองลงมาเป็นความผิดปกติของ HTTP

12.85% และ การถูกเปิดเผยข้อมูลโดยผู้บุกรุกที่ใช้เส้นทางในการเข้าถึงข้อมูลข่าวสารผ่านทางระบบที่ตกเป็นเหยื่อ 12.30%

2. สามารถค้นหาลักษณะการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ โดยตัวอย่างชุดข้อมูลประเทศไทยเดือนเมษายน 2556 พบรูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ คือ หากโหนดหมายเลข 129, 87, 3, 90 และ 224 ซึ่งเป็นโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร คือโหนดหมายเลข 234, 90, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือกระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ จะมีโอกาสมาจากโหนดที่ใกล้ชิด คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้โหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์

3. สามารถค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ โดยตัวอย่างชุดข้อมูลประเทศไทยเดือนเมษายน 2556 พบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ด้วยโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ คือโหนดหมายเลข 129, 87, 3, 90 และ 224 ส่วนโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร หรือกระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ คือโหนดหมายเลข 234, 90, 217, 229 และ 216

4. สามารถทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าโดยตัวอย่างชุดข้อมูลประเทศไทยเดือนเมษายน 2556 พบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าด้วยโหนดศูนย์กลางการกระจายข้อมูลข่าวสารหรือกระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ คือโหนดหมายเลข 234, 90, 217, 229 และ 216 มีโอกาสส่งไปยังโหนดที่ใกล้ชิด คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้โหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ หรือเป็นโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า

5. สามารถสรุปรวมแนวคิดทั้งหมดตามกรอบการวิจัยเป็น ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ ที่มีความละเอียดถูกต้องอย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 % ในการวิเคราะห์ความสัมพันธ์เชื่อมโยงในเครือข่ายสังคมออนไลน์ที่มีขนาดใหญ่และซับซ้อน