การตรวจจับพฤติกรรมและป้องกันมัลแวร์บนโทรศัพท์มือถือแอนดรอยด์

Behavior Detection and Prevention Malware on Android Mobiles

สุวรรณี ธูปจีน*, ระดม เจือจันทร์ และศิรปัฐช์ บุญครอง

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ถนนประชาราษฎร์ 1 แขวงวงศ์สว่าง เขตบางซื่อ กรุงเทพเทพมหานคร 10800

Suwannee Thoobjeen*, Radom Juajan and Siraput Boonkrong

Faculty of Information Technology, King Mongkut's University of Technology North Bangkok,

Pracharat 1 Road, Wongsawang, Bangsue, Bangkok 10800

บทคัดย่อ

ในปัจจุบันโทรศัพท์มือถือมาพร้อมกับสารพัดประโยชน์ที่ช่วยอำนวยความสะดวกให้แก่ผู้ใช้งานทำให้ได้รับความนิยมแพร่หลายไปทั่วโลก และได้กลายมาเป็นส่วนหนึ่งในชีวิตประจำวันของผู้คนในยุคแห่งเทคโนโลยี ด้วยเหตุนี้จึงทำให้ตกเป็นเป้าหมายการโจมตีจากผู้ไม่หวังดีในการพยายามพัฒนาและสร้างมัลแวร์รูปแบบใหม่ ๆ ขึ้นมา โดยเฉพาะการโจมตีบนระบบปฏิบัติการแอนดรอยด์ที่ต้องเผชิญกับภัยคุกคามจากมัลแวร์และไวรัสต่าง ๆ ซึ่งพบว่าการแพร่กระจายของมัลแวร์ได้มีอัตราการเพิ่มขึ้นส่งผลกระทบต่อผู้ใช้งานและความปลอดภัยของข้อมูล ดังนั้นในบทความนี้จึงได้นำเสนอวิธีการตรวจจับพฤติกรรมของมัลแวร์ ตัวอย่างลักษณะอาการและบริเวณพื้นที่ที่เกิดผลกระทบจากสายพันธุ์มัลแวร์ที่สามารถตรวจสอบหรือสังเกตเห็นได้โดยผู้ใช้เอง พร้อมทั้งแนะนำวิธีการใช้งานโทรศัพท์มือถือให้ปลอดภัยจากมัลแวร์เพื่อลดความเสี่ยงในความปลอดภัยของข้อมูล

คำสำคัญ : โทรศัพท์มือถือ; แอนดรอยด์; มัลแวร์

Abstract

Nowadays, smartphones have provided conveniences to users and, therefore, have gained popularity around the globe. It cannot be denied that they have also become a part of everyday's life. It is, therefore, inevitable that smartphones, especially those with Android, are now targets for attackers. Android smartphones are now facing with various types of malware and viruses, which can affect the users and their privacy of information. This paper discusses methods of detecting behaviours of malware, describes the characteristics of malware and how each type

***ผู้รับผิดชอบบทความ :** Thoobjeen@gmail.com

of malware can be detected by user's own observations. Moreover, the paper also introduces ways of using Android smartphones so that the risk of the infected can be mitigated.

Keywords: mobiles; android; malware

1. บทนำ

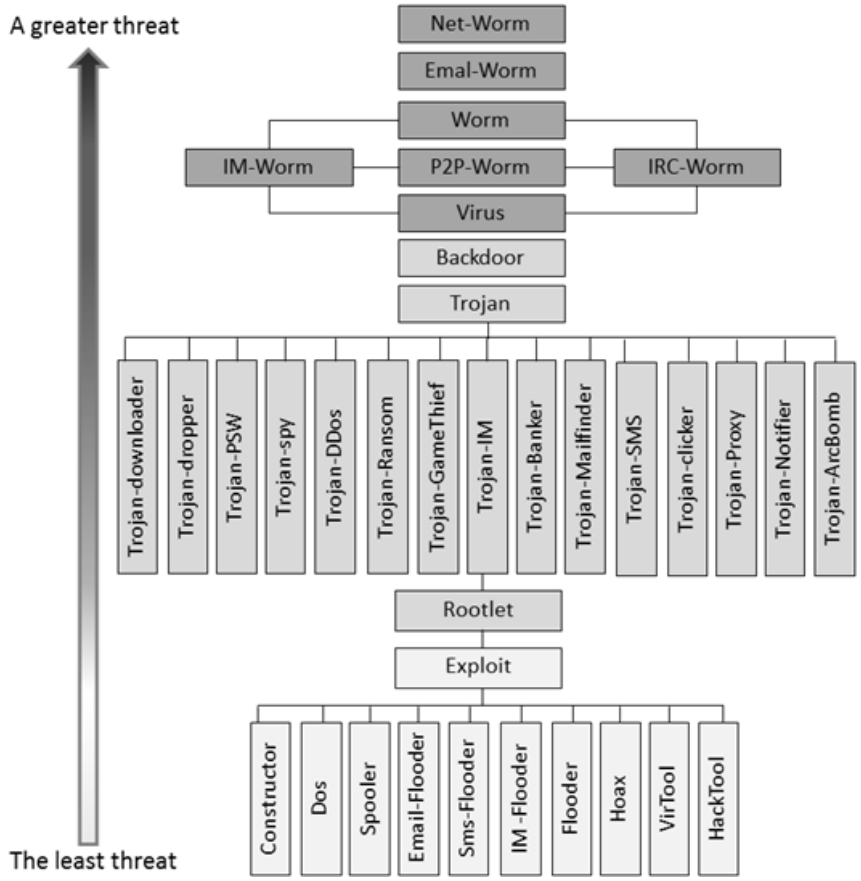
ปัจจุบันโทรศัพท์มือถือมาพร้อมกับประโยชน์ที่ช่วยอำนวยความสะดวกให้แก่ผู้ใช้งานเป็นอย่างดี เช่น สามารถเชื่อมต่ออินเทอร์เน็ตและสามารถติดตั้งแอพพลิเคชั่นต่าง ๆ ลงบนเครื่องได้ จึงทำให้ได้รับความนิยมแพร่หลายไปทั่วโลกและได้กลายมาเป็นส่วนหนึ่งในชีวิตประจำวันของผู้คนในยุคแห่งเทคโนโลยี จะเห็นได้จากการเติบโตทางธุรกิจที่มีอัตราการเพิ่มขึ้นอยู่อย่างต่อเนื่อง [1]

เมื่อโทรศัพท์มือถือได้รับความนิยมอย่างแพร่หลายจึงตกเป็นเป้าหมายในการโจมตีจากผู้ไม่หวังดีในการพยายามพัฒนาและสร้างมัลแวร์รูปแบบใหม่ ๆ ขึ้นมาโจมตีระบบปฏิบัติการบนโทรศัพท์มือถือโดยเฉพาะระบบปฏิบัติการแอนดรอยด์มีโอกาสถูกโจมตีสูงกว่าระบบปฏิบัติการอื่น ๆ [2] อาจเป็นเพราะว่ากูเกิลเพลย์ (Google Play) เป็นระบบที่เปิดกว้างสามารถให้ผู้พัฒนาสร้างแอพพลิเคชั่นมาติดตั้งได้เองโดยไม่ต้องผ่านการตรวจสอบจากระบบ ทำให้ผู้ใช้ทั่วไปสามารถดาวน์โหลดแอพพลิเคชั่นผ่านการแชร์ลิงค์โดยไม่ต้องผ่านกูเกิลเพลย์ จึงทำให้เกิดความเสี่ยงในการดาวน์โหลดแอพพลิเคชั่นที่เป็นมัลแวร์ได้อย่างง่ายดาย มัลแวร์เป็นแอพพลิเคชันที่ถูกเขียนขึ้นมาเพื่อรบกวนการทำงานของระบบ ได้แก่ ทำให้ระบบโทรศัพท์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูล หรือเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องได้จากภายนอก เป็นต้น นอกจากการทำงานข้างต้นแล้ว พฤติกรรมของมัลแวร์โดยส่วนใหญ่จะมีส่วนที่คล้าย ๆ กันคือ หลบซ่อนตัวเองจากการตรวจจับ โหลดมัลแวร์ตัวอื่นมาลงเพิ่ม ปิดการทำงานของระบบรักษาความปลอดภัยหรือฝังตัวเองในระบบเพื่อให้ยังสามารถกลับมาทำงานต่อได้เมื่อรีสตาร์ทเครื่อง [3]

ดังนั้นในบทความนี้จึงได้นำเสนอวิธีการตรวจจับพฤติกรรมของมัลแวร์ที่สามารถตรวจสอบหรือสังเกตเห็นได้โดยผู้ใช้เอง ด้วยการวิเคราะห์ตัวอย่างของสายพันธุ์มัลแวร์ที่ส่งผลให้เกิดความเสียหายต่อผู้ใช้และแนะนำวิธีการป้องกันมัลแวร์ ซึ่งอาจจะเป็นประโยชน์สำหรับผู้ใช้ทั่วไปในการป้องกันมัลแวร์บนโทรศัพท์มือถือเพื่อลดความเสี่ยงในความปลอดภัยของข้อมูล

2. มัลแวร์กับระบบปฏิบัติการแอนดรอยด์

มัลแวร์ (malware) ย่อมาจาก malicious software หมายถึงซอฟต์แวร์ไม่พึงประสงค์ที่ถูกสร้างขึ้นเพื่อทำลายระบบหรือรบกวนการทำงานของระบบ ซึ่งโดยทั่วไปจะรู้จักกันในรูปแบบต่าง ๆ เช่น โทรจัน ไวรัส เวิร์ม พฤติกรรมการทำงานของมัลแวร์หนึ่งตัวอาจมีหลายอย่าง จึงอาจถูกจัดให้อยู่ในได้หลายประเภทหลายสายพันธุ์ รูปที่ 1 แสดงตัวอย่างการแบ่งประเภทพฤติกรรมของมัลแวร์ [4] ที่ก่อให้เกิดภัยคุกคามต่อระบบโทรศัพท์มือถือ โดยมัลแวร์แต่ละประเภทนั้นจะถูกแบ่งกลุ่มตามระดับความรุนแรงที่ส่งผลให้เกิดความเสียหายต่อระบบจากน้อยไปมาก จากตัวอย่างจะเห็นได้ว่า Email-Worm มีพฤติกรรมของระดับความรุนแรงมากกว่า P2P-Worm และ Trojan-Mailfinder นอกจากนี้พฤติกรรมของมัลแวร์โดยส่วนใหญ่จะมีลักษณะคล้ายคลึงกัน เช่น หลบซ่อนจากการถูกตรวจจับ ปิดการทำงานของระบบความปลอดภัย โหลดมัลแวร์ตัวอื่นลงเพิ่ม เป็นต้น



รูปที่ 1 ตัวอย่างการแบ่งประเภทมัลแวร์ [4]

ภัยคุกคามจากมัลแวร์บนระบบปฏิบัติการแอนดรอยด์นั้น อาจเกิดจากผู้ไม่หวังดีพยายามพัฒนาแอพพลิเคชั่นมัลแวร์ แล้วปล่อยให้ผู้ใช้ทั่วไปดาวน์โหลดแอพพลิเคชั่นผ่านการแชร์ลิงค์ได้โดยง่าย และจากรายงานของ Mobile threat report เมื่อประมาณต้นปี พ.ศ. 2556 โดย F-Secure Labs ได้ทำการสำรวจจำนวนมัลแวร์ที่เพิ่มขึ้นซึ่งพบว่าการตรวจพบแอพพลิเคชั่นมัลแวร์บนระบบปฏิบัติการแอนดรอยด์เพิ่มขึ้นมีจำนวนมากถึง 275 สายพันธุ์ [5] และจากมัลแวร์ที่ตรวจพบส่วนใหญ่เป็นประเภทโทรจันที่รบกวนการทำงานของโทรศัพท์มือถือ และส่วนใหญ่จะมุ่งเป้าหมายไปที่ระบบ mobile banking หรือการทำธุรกรรมออนไลน์บนโทรศัพท์มือถือ โดยเข้าไปค้นหาข้อมูลส่วนตัวของผู้ใช้งานและจะแฝงตัวในรูปแบบของ SMS spy และพยายามทำให้ผู้ใช้งานเชื่อว่านั่นคือการตรวจสอบความปลอดภัยของธนาคารแต่ความจริงแล้วคือการขโมยข้อมูลส่วนตัว

3. การวิเคราะห์และตรวจจับพฤติกรรมมัลแวร์

การวิเคราะห์มัลแวร์มีจุดประสงค์เพื่อศึกษาพฤติกรรมและขั้นตอนการทำงานของมัลแวร์ ตรวจสอบผลกระทบจากความเสียหาย รวมถึงศึกษาวิธีการป้องกันและแก้ไขปัญหาหลังจากเครื่องโทรศัพท์ติดมัลแวร์ ปัจจุบันมัลแวร์ได้มีการพัฒนาสายพันธุ์และเพิ่มจำนวนขึ้นอยู่เสมอ ดังนั้นจึงได้มีกลุ่มนักวิจัยได้คิดค้นวิธีการวิเคราะห์และตรวจจับพฤติกรรม

ของมัลแวร์ เพื่อเป็นประโยชน์สำหรับผู้ใช้งานโทรศัพท์ในการป้องกันการดาว์นโหลดมัลแวร์ ดังนี้

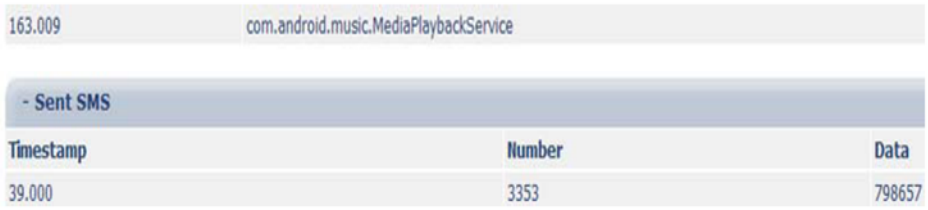
Mirco และคณะ ได้เสนอสถาปัตยกรรมแบบกระจายในการร่วมมือเพื่อจัดการกับมัลแวร์ ทั้งนี้มีการนำพฤติกรรมของมัลแวร์ เช่น การแพร่กระจายของมัลแวร์ การโจมตีผ่านเครือข่าย การกระจายการโจมตี การค้นหา IP address ที่น่าสงสัย และการค้นหาเครื่องแม่ข่ายที่ดาว์นโหลดมัลแวร์เข้าไป สถาปัตยกรรมมี 3 ชั้น ชั้นลึกสุดเป็นเซนเซอร์ประเภท IDS (intrusion detection system) และ Honey pot ที่นำมาใช้ตรวจจับการบุกรุกของมัลแวร์ต่าง ๆ ซึ่งจะทำการหลอกล่อให้มัลแวร์เข้ามาติดตั้ง ซึ่งเมื่อทำการตรวจจับมัลแวร์ได้แล้วจะมีกระบวนการทำงานที่สามารถระบุได้ว่ามัลแวร์อยู่ที่ใดในระบบ [6] Zarni และ Xinyuan เสนอสถาปัตยกรรมแบบเครื่องจักรเรียนรู้ (machine learning) ในการตรวจจับมัลแวร์ในแอพพลิเคชั่นที่ดาวน์โหลดเข้าไปในโทรศัพท์มือถือแอนดรอยด์ ทั้งนี้ระบบการเรียนรู้จะจำแนกแยกแยะระหว่างแอพพลิเคชั่นปกติและแอพพิลเคชั่นที่มีมัลแวร์ฝังอยู่ [7] Markus และ Ari เสนอสถาปัตยกรรมเครือข่ายที่ใช้การวิเคราะห์ Server/Could-base Post-Mortem detection กับร่องรอยของมัลแวร์ เพราะการเกิดผลร้ายจากมัลแวร์จะมีร่อยรอยใน Log file ได้แก่ มีการ call มีการ download มีการติดตั้ง เป็นต้น ระบบนี้ทำงานภายใต้สมมุติฐานว่า Log file จะไม่เสียหายจากมัลแวร์ [8] Sai และคณะ เสนอวิธีใช้ลายเซ็นของไวรัสในการตรวจจับมัลแวร์ (signature) ซึ่งพบว่ามัลแวร์จะมีลักษณะเฉพาะบางส่วนที่ตายตัว ซึ่งเมื่อมัลแวร์มีวิวัฒนาการทางสายพันธุ์ มัลแวร์ตัวใหม่จะมีลักษณะเฉพาะในส่วนนี้อยู่ด้วย งานวิจัยนี้จะสร้างลายเซ็นที่เป็นลักษณะเฉพาะของมัลแวร์ทั้งตระกูล เพียงลายเซ็นเดียวเพื่อใช้ในการเปรียบเทียบ และการทดสอบวิธีการนี้พบว่าสามารถตรวจจับมัลแวร์ใหม่ ๆ ในตระกูลเดียวกัน [9] Liu และคณะ ได้เสนอวิธีการตรวจจับมัลแวร์ โดยใช้ความร่วมมือทางสังคมและการสร้างระบบฐานข้อมูลมัลแวร์ที่เกิดขึ้นบ่อย แล้วกระจายข้อมูลดังกล่าวไปยังโทรศัพท์มือถือทุกเครื่อง จากผลการทดลองพบว่าสามารถลดการแพร่กระจายของมัลแวร์ได้ [10]

นอกจากนี้วิธีโดยทั่ว ๆ ไปที่สามารถใช้วิเคราะห์พฤติกรรมของมัลแวร์ในระบบปฏิบัติการแอนดรอยด์สามารถใช้วิธีวิศวกรรมย้อนกลับ (reverse engineering) ซึ่งเป็นกระบวนการตรวจสอบย้อนกลับเพื่อค้นหาต้นแบบเทคโนโลยีของอุปกรณ์ วัตถุ หรือระบบผ่านการวิเคราะห์โครงสร้าง ฟังก์ชันและการทำงานของอุปกรณ์นั้น เช่น เมื่อทำการวิเคราะห์จากโค้ดของแอพพลิเคชั่นอาจจะสามารถรู้ถึงจุดประสงค์ของมัลแวร์ที่มีต่อระบบ ดังรูปที่ 2 เป็นตัวอย่างของโค้ดมัลแวร์ที่สั่งให้ส่งข้อความไปที่เบอร์โทรศัพท์ 3354 [11]

นอกจากนี้วิธีการวิเคราะห์มัลแวร์จากเว็บไซต์ที่ให้บริการเครื่องมือ Online malware scan ที่ใช้วิธีการอัพโหลดไฟล์ขึ้นไปเพื่อให้ antivirus ค่ายต่าง ๆ ช่วยสแกน เช่น http//Anubis.iseclab.org ก็อาจจะช่วยให้สามารถทราบถึงจุดประสงค์ของมัลแวร์ที่มีผลต่อระบบได้ แสดงตัวอย่างดังรูปภาพที่ 3 [11]

```
82      invoke-virtual/range {v0 .. v5}, Landroid/telephony/SmsManager;->sendTextMessage
83      :try_end_2d
84      .catch Ljava/lang/Exception; {:try_start_2a .. :try_end_2d} :catch_44
85
86      .line 63
87      :goto_2d
88      const-string v1, "3354"
```

รูปที่ 2 Malware send a message to phone number 3354



163.009	com.android.music.MediaPlaybackService

- Sent SMS

Timestamp	Number	Data
39.000	3353	798657

รูปที่ 3 An analysis result from website

4. สายพันธุ์มัลแวร์ที่สามารถวิเคราะห์และตรวจพบได้บนสมาร์ทโฟนแอนดรอยด์

สายพันธุ์มัลแวร์ (malware family) ในปัจจุบันบางส่วนสามารถถูกตรวจจับได้โดยโปรแกรมสแกนไวรัสหรือผู้ใช้สามารถสังเกตเห็นได้จากอาการหรือพฤติกรรมที่ผิดปกติบนระบบโทรศัพท์ จากงานวิจัยของ Thanh ได้เก็บตัวอย่างสายพันธุ์มัลแวร์ที่สามารถถูกตรวจจับได้จากบริษัทผู้ผลิตโปรแกรมสแกนไวรัส จำนวน 1,485 มัลแวร์ ได้แบ่งสายพันธุ์มัลแวร์เป็น 58 สายพันธุ์ และผู้เขียนได้เลือกมาเพียงบางส่วนจากจำนวนสายพันธุ์มัลแวร์ทั้งหมดตามตารางที่ 1 และ 3 แสดงพฤติกรรมและสายพันธุ์มัลแวร์และบริเวณพื้นที่ที่เกิดผลกระทบจากสายพันธุ์มัลแวร์ ตารางที่ 2 อธิบายลักษณะของข้อมูลที่ถูกขโมยโดยแอพพลิเคชั่นมัลแวร์ [11]

มัลแวร์เมื่อถูกติดตั้งบนเครื่องโทรศัพท์จะส่งผลให้ระบบเกิดการทำงานที่ผิดปกติ ในการตรวจสอบผู้ใช้โทรศัพท์สามารถสังเกตเห็นได้ถึงลักษณะความเปลี่ยนแปลงที่ผิดปกติในระบบโทรศัพท์ ตารางที่ 3 เป็นตัวอย่างสายพันธุ์มัลแวร์ที่แสดงลักษณะอาการที่ผู้ใช้โทรศัพท์สามารถตรวจสอบโดยผู้ใช้เอง

ตารางที่ 1 ลักษณะของข้อมูลที่ถูกขโมยโดยแอพพลิเคชั่นมัลแวร์

ลำดับ	รายละเอียด
1	ขโมยข้อมูลส่วนบุคคล เช่น รหัสประจำเครื่องโทรศัพท์ (IMEI, IMSI) เบอร์โทรศัพท์
2	ขโมยข้อมูลการใช้เครือข่าย เช่น Bookmarks, APN, IP, MAC
3	ขโมยข้อมูลในเครื่อง เช่น SMS, contacts, account, calls log
4	ขโมยไฟล์ข้อมูล เช่น แก้ไขไฟล์ข้อมูล คัดลอกไฟล์ข้อมูล
5	ขโมยข้อมูลแอพพลิเคชั่น เช่น ดาวน์โหลดและติดตั้งแอพพลิเคชั่น
6	ขโมยข้อมูลตำแหน่งที่ตั้ง เช่น GPS, Google, Country code
7	ส่งข้อมูลออกไปให้ C&C sever เช่น ส่งผ่านข้อความทาง SMS
8	ส่งข้อมูลไปยัง URL โดยการเชื่อมต่อผ่านอินเทอร์เน็ต
9	ขโมยส่งข้อความแบบ Premium-rate ซึ่งเป็นหมายเลขโทรศัพท์ที่เสียค่าบริการแพงกว่าปกติ
10	พยายามเข้าถึง Root ของระบบ เพื่อได้สิทธิ์ควบคุม แก้ไข เปลี่ยนแปลงโทรศัพท์
11	ขโมยรหัสผ่านธนาคาร เช่น รหัส ATM
12	ขโมยรหัส QR code

ตารางที่ 2 ลักษณะอาการและบริเวณพื้นที่ที่เกิดผลกระทบจากสายพันธุ์มัลแวร์

พื้นที่	สายพันธุ์มัลแวร์	ประเภทของอาการ (ดูรายละเอียดในตารางที่ 2)											
		1	2	3	4	5	6	7	8	9	10	11	12
China	AnserverBot	x						x					
	BaseBridge (AdSMS)	x		x				x					
	Pjapps	x	x	x				x					
	CruseWin (CruseWind)							x		x			
	DroidCoupon												
	DreamLight			x				x					
	DroidKungFu (LeNa)	x			x	x		x					
	Smssend (Fakeplayer)							x		x			
	Gamblersms												
	Rootsmart (Bmaster)	x						x			x		
China, Canada	FakeAngry (AnZhu)	x			x			x					
	Faketimer (Oneclickfraud)	x						x		x			
USA, CN, RU	GGTracker	x		x				x		x			
	GoldDream	x		x				x					
	HippoSMS							x		x			
	jSMSHider (Smshider, Xsider)							x	x				
	KMin (ozotshielder)	x					x	x					
	Plankton				x	x	x	x					
	Spitmo	x						x				x	
	Tapsnake						x	x					
	Walkinwat	x		x			x	x					
	Battery Doctor (fakdoc)					x		x					
	CI4					x		x					
Japan	Dougalek	x		x				x					
Eastern, Europe	DropDialer			x				x		x			
Spain	FakeToken	x						x					
Russia	FindAndCall							x					
Russia, Eurrope	Logastrod	x	x					x		x			
	Luckycat				x			x					
	Moghava				x								
Russia	Opfake							x		x			

ตารางที่ 3 รายละเอียดลักษณะอาการของสายพันธุ์มัลแวร์ที่ผู้ใช้โทรศัพท์สามารถสังเกตเห็นได้เมื่อเครื่องติดมัลแวร์

สายพันธุ์มัลแวร์	ลักษณะอาการ	การตรวจสอบโดยผู้ใช้เอง	ไอคอน
AnserverBot	ขึ้นไดอะล็อกบ็อกซ์ว่ากำลังร้องขออัพเกรดแอพพลิเคชั่นแต่ไม่แสดงไอคอนใด ๆ	จำชื่อแอพพลิเคชั่นที่กำลังอัพเกรดและตรวจสอบการแสดงไอคอน	
BaseBridge (AdSMS)	มีการเรียกเก็บค่าบริการอินเทอร์เน็ตที่สูงผิดปกติ (GPRS) และแอพพลิเคชั่นป้องกันความปลอดภัย 360 Safeguard ถูกติดตั้ง	ตรวจสอบค่าบริการโทรศัพท์ ตรวจสอบการแจ้งเตือนข้อผิดพลาดจากแอพพลิเคชั่น 360 Safeguard	
Pjapps	ขออนุญาตเข้าถึงประวัติการใช้งานบุ๊คมาร์กและได้รับข้อความ SMS เมื่อติดตั้ง	ตรวจสอบการขออนุญาตเข้าถึงบุ๊คมาร์กและข้อความที่ได้รับ	
CruseWin (CruseWind)	แสดงหน้าจอสีดำ	ตรวจสอบค่าบริการโทรศัพท์และลักษณะไอคอนของ Flash	
DroidCoupon	ช่องโหว่จากแอนดรอยด์ 2.2 เกิดจากการหลบซ่อนจากแพลตฟอร์มก่อนหน้านี้ดังนั้น จึงเห็นการยากที่จะตรวจสอบได้	โทรศัพท์ได้รับการอัพเกรดเป็นเวอร์ชันใหม่	
DreamLight	บริการ CoreSevice กำลังทำงานเมื่อรับสายโทรศัพท์	ตรวจสอบการทำงานของบริการ CoreSevice	
DroidKungFu (LeNa)	ติดตั้ง Google search หรือ Google Site search	ตรวจสอบลักษณะไอคอนของทั้งสองแอพพลิเคชั่น	
Smssend (Fakeplayer)	แอพพลิเคชั่น Media player ทำงาน	ตรวจสอบค่าบริการโทรศัพท์ ตรวจสอบการตั้งค่าแอพพลิเคชั่น	
Gamblersms	ร้องขอเบอร์โทรศัพท์และอีเมล์	ตรวจสอบเบอร์โทรศัพท์และอีเมล์	
GGTracker	เว็บไซต์เกี่ยวกับแอพพลิเคชั่นแบตเตอรี่โทรศัพท์ battery-monitoring tool	ตรวจสอบแบตเตอรี่โทรศัพท์	

ตารางที่ 3 (ต่อ)

สายพันธุ์มัลแวร์	ลักษณะอาการ	การตรวจสอบโดยผู้ใช้เอง	ไอคอน
GoldDream	ยากในการระบุลักษณะอาการ	ควรติดตั้งแอพพลิเคชั่นรักษาความปลอดภัยบนโทรศัพท์	
HippoSMS	ค่าบริการโทรศัพท์จากเบอร์ 1066	ตรวจสอบค่าบริการโทรศัพท์	
jSMSHider (Smshider, Xsider)	บริการชื่อ “InstallService” แต่ไม่ทำการติดตั้งแอพพลิเคชั่น	ตรวจสอบไอคอน “InstallService”	
KMin (ozotshielder)	เปลี่ยนภาพหน้าจอ	ตรวจสอบไอคอน	
Spitmo	ป๊อปอัพ “Certificate update” หรือ “Security update”	ตรวจสอบการตั้งค่าโทรศัพท์	
Tapsnake	ร้องขอข้อมูลหลังจากคลิ๊กไอคอน	ตรวจสอบค่าบริการโทรศัพท์	
Walkinwat	แอพพลิเคชั่นไม่อนุญาตให้ cracking	ไม่ทำตามข้อเสนอของแอพพลิเคชั่น	
Battery Doctor (fakdoc)	โฆษณาเกี่ยวกับแบตเตอรี่โทรศัพท์	ไม่ติดตั้งแอพพลิเคชั่น	
CI4	ไม่ปรากฏไอคอนหลังจากทำการติดตั้ง		
DropDialer	ลบตัวเองออกจากระบบหลังจากส่งข้อความ	ตรวจสอบไอคอนและค่าโทรศัพท์	
FakeAngry (AnZhu)	ป๊อปอัพแสดง displayed bookmark name/bookmark URL	ปรากฏหน้าจอล็อกออฟหรือล็อกแอพพลิเคชั่น	
Faketimer (Oneclickfraud)	เว็บไซต์ที่มีเนื้อหาไม่สมบูรณ์	ตรวจสอบแอพพลิเคชั่นและลบออกจากระบบ	
FakeToken	ปลอมเว็บไซต์ของธนาคารโดยเลียนแบบโลโก้และสีเหมือนเว็บไซต์ธนาคาร	ตรวจสอบไอคอนของธนาคาร	
FindAndCall	ข้อความสแปม	ตรวจสอบไอคอน ลบออกจากระบบ	
Logastrod	ค่าโทรศัพท์ที่สูงผิดปกติ	ตรวจสอบค่าโทรศัพท์	
Luckycat	ไอคอน “empty” หรือ standard android icon		
Moghava	ขนาดของภาพไฟล์ JPG เพิ่มขึ้น	ตรวจสอบแอพพลิเคชั่นและลบออกจากระบบ	
Opfake	The Opera icon	ตรวจสอบค่าโทรศัพท์	
Rootsmart (Bmaster)	ไอคอนชื่อภาษาจีน	ไอคอนชื่อภาษาจีน	

จากการวิเคราะห์พฤติกรรมของมัลแวร์นั้น มัลแวร์บางสายพันธุ์ผู้ใช้สามารถสังเกตลักษณะอาการที่ส่งผลกระทบต่อระบบการทำงานของโทรศัพท์และสามารถตรวจสอบแก้ไขได้ แต่ก็ยังมีมัลแวร์บางสายพันธุ์ที่ไม่แสดงพฤติกรรมหรือลักษณะอาการที่เป็นภัยต่อระบบ อาจเป็นเพราะความสามารถของมัลแวร์ที่ปรับตัวไม่ให้ถูกตรวจจับได้ง่าย ดังนั้นสิ่งที่สำคัญที่สุดในการป้องกันมัลแวร์ ผู้ใช้ควรลดความเสี่ยงและตระหนักถึงความปลอดภัยในการดาวน์โหลดแอพพลิเคชั่นต่าง ๆ บนมือถือ

5. วิธีการป้องกันสำหรับผู้ใช้งานโทรศัพท์มือถือแอนดรอยด์

วิธีการแพร่กระจายของมัลแวร์ โดยส่วนใหญ่นั้นจะเป็นการหลอกลวงให้ผู้ใช้เป็นผู้ติดตั้งแอพพลิเคชั่นเข้าไปเอง มัลแวร์จะถูกติดตั้งบนโทรศัพท์ได้เกิดจากพฤติกรรมการใช้งานของผู้ใช้ ที่ไม่ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้น เพื่อลดความเสี่ยงที่จะส่งผลให้เกิดความสูญเสียทางการเงินและข้อมูลส่วนตัว จึงขอแนะนำวิธีการป้องกันสำหรับผู้ใช้งาน ดังนี้

5.1 ผู้ใช้ควรระวังตรวจสอบนโยบายความเป็นส่วนตัว และการขออนุญาตการทำงานของแอพพลิเคชั่นก่อนทำการติดตั้งแอพพลิเคชั่น และควรตรวจสอบความสามารถในการเข้าถึงข้อมูลต่าง ๆ ภายในเครื่อง เช่น แอพพลิเคชั่นคำนวณเลข แต่กลับขออนุญาตเข้าถึงไฟล์รูปภาพ หรือเข้าถึงบัญชีผู้ใช้อีเมล ซึ่งพฤติกรรมดังกล่าวไม่ได้เกี่ยวข้องกับการทำงานของแอพพลิเคชั่น เป็นต้น

5.2 ผู้ใช้ควรติดตั้งแอพพลิเคชั่น antivirus ที่สามารถสแกนไวรัสและสปายแวร์ได้ แต่ควรระวังในการติดตั้งหรือดาวน์โหลดแอพพลิเคชั่นในการรักษาความปลอดภัยให้กับเครื่องนั้น ควรเลือกดาวน์โหลดจากแหล่งที่มาที่น่าเชื่อถือ เช่น Google Play Store เพราะในปัจจุบันได้มีผู้พัฒนาแอปพลิเคชั่น antivirus ปลอม เพื่อให้ผู้ใช้สมาร์ทโฟนเกิดความเข้าใจผิดคิดว่าเป็นแอพพลิเคชั่นป้องกันความปลอดภัยจึงดาวน์โหลดไปใช้

5.3 ผู้ใช้ควรตรวจสอบจากการอ่านรีวิว และคอมเมนต์จากผู้ใช้ก่อนทำการติดตั้งแอพพลิเคชั่น เพื่อให้ทราบถึงสิ่งที่ถูกคอมเมนต์นั้นเป็นอย่างไร ได้แก่ มีปัญหาการใช้งานหรือไม่ มีการแจ้งเตือนระวังมัลแวร์หรือไม่ และหากเป็นไปได้สามารถเข้าไปดูเว็ปไซต์บริษัทของผู้พัฒนาแอพพลิเคชั่นก็ควรเข้าไปตรวจสอบ เพื่อเป็นการลดความเสี่ยงที่อาจเกิดขึ้นได้ เป็นต้น

5.4 ผู้ใช้ควรระวังในขณะทำการเชื่อมต่อ Wi-Fi สาธารณะ เมื่อมีความจำเป็นที่ต้องทำการเชื่อมต่ออินเทอร์เน็ตด้วย Android phone ผ่านบริการ Wi-Fi สาธารณะ แนะนำว่าผู้ใช้ควรจะทำกิจกรรมบนอินเทอร์เน็ตเท่าที่จำเป็นและทำการปิดแอพพลิเคชั่นที่ไม่จำเป็นในขณะนั้นทั้งหมด เนื่องจากในปัจจุบันมีสคริปท์ที่เป็นอันตรายคอยดักจับยูสเซอร์เนมและพาสเวิร์ดที่ส่งผ่านการเชื่อมต่อสาธารณะนั้น และไม่ควรดาวน์โหลดแอพพลิเคชั่นหรือทำธุรกรรมบริการธนาคารออนไลน์หรือเฟซบุ๊ก เป็นต้น

5.5 ผู้ใช้ควรทำการอัพเดทแอพพลิเคชั่นให้เป็นเวอร์ชันปัจจุบันอยู่เสมอโดยทำการตรวจสอบให้แน่ใจว่าระบบปฏิบัติการ และแอพพลิเคชั่นต่าง ๆ ภายในเครื่องได้ถูกอัพเดทเป็นเวอร์ชันล่าสุดแล้ว เพื่อเป็นการป้องกันและลดช่องโหว่หรือความเสี่ยงในการใช้แอพพลิเคชั่นนั้น ๆ เป็นต้น

6. สรุป

บทความนี้ได้นำเสนอวิธีการตรวจจับพฤติกรรมของมัลแวร์ที่สามารถตรวจสอบหรือสังเกตเห็นได้โดยผู้ใช้เอง ด้วยการวิเคราะห์ตัวอย่างของสายพันธุ์มัลแวร์ที่ส่งผลให้เกิดความเสียหายต่อระบบและแนะนำวิธีการ

ป้องกันมัลแวร์ ซึ่งอาจจะเป็นประโยชน์สำหรับผู้ใช้ทั่วไปในการป้องกันมัลแวร์บนโทรศัพท์มือถือเพื่อลดความเสี่ยงในความปลอดภัยของข้อมูล เพราะจำนวนมัลแวร์ที่เพิ่มขึ้นในปัจจุบันจะเพิ่มขึ้นตามจำนวนแอพพลิเคชั่นที่ถูกพัฒนาขึ้นจากผู้ไม่หวังดี มัลแวร์บางสายพันธุ์อาจถูกตรวจจับได้ด้วยแอปพลิเคชั่นป้องกันความปลอดภัยหรือผู้ใช้สามารถตรวจสอบเองได้ แต่ก็มีอีกหลายสายพันธุ์ที่ไม่แสดงอาการหรือพฤติกรรมให้ถูกตรวจจับได้ง่าย ดังนั้นการป้องกันที่ดีที่สุดควรเป็นการระวังในการใช้งานของตัวผู้ใช้เอง โดยเฉพาะการดาวน์โหลดหรืออัพเดทแอพพลิเคชั่นและระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดจากแหล่งข้อมูลที่ปลอดภัย และค่อยติดตามข้อมูลข่าวสารการระวังภัยมัลแวร์ที่เกิดขึ้นในปัจจุบันอยู่เสมอ

7. เอกสารอ้างอิง

[1] Gartner, Egham, UK, August 14, 2013, Gartner Says Smartphone Sales Grew 46.5 Percent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First Time, Available Source: http://www.gartner.com/newsroom/id/2573415, October 14, 2014.

[2] Ameya, N., Tomas, P., Mohammad, A. and Kang, Y., 2013, Android mobile platform security and malware server, pp. 2320-7308, IJRET.

[3] Zhou, Y.j. and Jiang, X.X., 2012, Dissecting Android malware: Characterization and evolution, pp. 95-109, IEEE Symposium on Security and Privacy.

[4] Kaspersky, Malware Classifications, Available Source: http://www.kaspersky.com/internet-security-enter/threats/malware-classifications, October 14, 2014.

[5] F-secure, Mobile threat report Q1 2014, Available Source: http://www.fsecure.com/weblog/archives/MobileThreaReport_Q1_2014.pdf, October 14, 2014.

[6] Micro, M., Michele, M. and Michele, C., 2009, Peer-to-Peer architecture for collaborative intrusion and malware detection on a large scale, pp. 475-490, International Conference on Information Security.

[7] Zarni, A. and Win, Z., March 2013, Permission-Based Android malware detection, IJSTR, V.2, pp. 228-234.

[8] Markus, J. and Ari, J., 2009, Server-side detection of malware infection, pp. 11-22, NSPW'09.

[9] Sai S.V., Pankaj, K. and Bezawada, B., 2008, Signature generation and detection of malware families, pp. 336-349, ACISP 2008, LNCS 5107.

[10] Liu, Y., Vinod, G. and Liviu, L., 2011, Enhancing mobile malware detection with social collaboration, pp. 572-576, IEEE Third International Conference on Social Compution.

[11] Thanh, H.L., 2013, Analysis of malware families on android mobile: Detection characteristics recognizable by ordinary phone users and how to fit it, J. Inform. Secur. 4: 213-224.