บทความวิชาการ

มัลแวร์ในระบบปฏิบัติการมือถือบน IOS และ Android

MALWARE INOPERATION SYSTEM ON IOS AND ANDROID

เบญจภัค จงหมื่นไวย์
Benjapuk Jongmuenwai
มหาวิทยาลัยราชภัฏนครราชสีมา
จังหวัดนครราชสีมา

บทคัดย่อ

วัตถุประสงค์ของการศึกษาครั้งนี้เพื่อ 1) ศึกษาข้อมูลเกี่ยวกับมัลแวร์ 2) การเพิ่มขึ้นของมัลแวร์สำหรับแนวโน้มการใช้งานมือถือในปัจจุบันและการสื่อสารโทรคมนาคมรวมไปถึงการได้รับ e-mail ดังนั้นการใช้งานอุปกรณ์เคลื่อนที่ต้องตรวจสอบและระบุชื่อผู้ใช้พร้อมทั้งรหัสผ่าน ปัจจุบันโทรศัพท์มือถือได้พบปัญหาเกี่ยวกับมัลแวร์บนระบบปฏิบัติการ IOS และ Android ที่มีปริมาณเพิ่มมากขึ้นซึ่งการใช้งานสำหรับโทรศัพท์มือถือและแท็บเล็ตเป็นสิ่งที่สำคัญต่อชีวิตประจำวันของมนุษย์ ทั้งนี้ โทรศัพท์มือถือและแท็บเล็ตสามารถอำนวยความสะดวกการทำงานให้กับผู้ใช้งานรวมไปถึงความเร็วของอินเทอร์เน็ต ต้องมีการวัดประสิทธิภาพในการใช้งาน ทั้งนี้โทรศัพท์มือถือเป็นอุปกรณ์พกพาแบบเคลื่อนที่และต้องมีระบบปฏิบัติการที่เน้นการโจมตีสำหรับมัลแวร์ได้

ในบทความนี้ เป็นการแนะนำเกี่ยวกับมัลแวร์และวิธีการที่สำคัญในการแก้ปัญหาเมื่อถูกโจมตีจากนั้นการสำรวจพบว่ามัลแวร์ในโทรศัพท์มือถือบนระบบปฏิบัติการ Android มากกว่า IOS ถึง 97% และระบบปฏิบัติ IOS ออกแบบเพื่อเน้นความปลอดภัยมากกว่าระบบปฏิบัติ Android ดังนั้นทั้งสองระบบปฏิบัติการต้องมีการป้องกันภัยจากมัลแวร์

คำสำคัญ : ระบบปฏิบัติการ IOS, ระบบปฏิบัติการ Android, มัลแวร์

ABSTRACT

The purposes of this study were1) to study the learning malware 2) to study mobile trend is malware increasing of telecommunication and receivee-mail. Thus, the mobility have to checking identify by using username and password. Currently, mobile devices have to become part of malware problem on operation IOS and Android mobile more than increasing.

The mobile and tablet are using for everyday life of population and to facilitate every day of work, so the user is likely to have important information of goal in store.Thus, the effective is used for working very high. The mobile is device and developedof malware attack the highlight to operating system.

In this paper, I introduce is about of malware. There are important methodology to solve the problem. Then, the survey found that mobile malware for it. The malware is attack android operating system more than 97% of the competitor for ios operating system is design emphasize safety over the android operating system. Therefore, two operating systemwith compareispreventionof malware.

Keyword : IOS operating system, Android operating system, Malware

บทนำ

ปัจจุบันอุปกรณ์เคลื่อนที่ได้เป็นส่วนหนึ่งในชีวิตประจำวันของมนุษย์ ที่มีแนวโน้มเพิ่มมากขึ้นและช่องทางการสื่อสารหรือการรับส่งอีเมลล์ พัฒนาต่อเนื่องมาจากการใช้อุปกรณ์เคลื่อนที่เป็นส่วนใหญ่ ทั้งนี้อุปกรณ์เคลื่อนที่ทุกชนิดที่นำมาใช้ต้องมีการตรวจสอบตัวตนหรือพิสูจน์ตัวตนโดยใช้รหัสผ่านทั้งสิ้นและในปัจจุบันปัญหามัลแวร์ในระบบปฏิบัติการบนอุปกรณ์เคลื่อนที่สำหรับ IOS และ Android มีจำนวนเพิ่มมากขึ้นอย่างต่อเนื่อง โดยเฉพาะการใช้งานโทรศัพท์มือถือและแท็บเล็ตเพื่ออำนวยความสะดวกในชีวิตประจำวันเกี่ยวข้องกับการทำงานและเรื่องส่วนตัว พร้อมทั้งการติดต่อผ่านระบบอินเทอร์เน็ตเป็นช่องทางหนึ่งที่สามารถติดมัลแวร์ได้ [4]

ระบบปฏิบัติการ IOS มีความปลอดภัยจากมัลแวร์มากกว่าระบบปฏิบัติการ Android สาเหตุหลัก เนื่องจากตัวระบบปฏิบัติการ IOS ถูกออกแบบมาให้เน้นเรื่องความมั่นคงปลอดภัยมากกว่า Android จากตัวอย่างมาตรการการรักษาความมั่นคงปลอดภัยของอุปกรณ์ IOS เช่นการติดตั้งแอพพลิเคชันซึ่งผู้ใช้ทั่วไปจะไม่สามารถดาวน์โหลดแอพพลิเคชันจากแหล่งภายนอกมาติดตั้งเองได้ดังนั้นต้องดาวน์โหลดจาก App Store เท่านั้น ซึ่งแตกต่างจากระบบปฏิบัติการ Android ที่ยินยอมให้ผู้ใช้งานสามารถติดตั้งแอพพลิเคชันจากไฟล์ที่ดาวน์โหลดได้

กระบวนการตรวจสอบแอพพลิเคชันที่จะถูกส่งขึ้นบนApp Store เป็นการตรวจสอบโดยมนุษย์ [7] ซึ่งมีการตรวจสอบทั้งคุณภาพของแอพพลิเคชันและความปลอดภัยในการใช้งาน ดังนั้นจึงมีโอกาสน้อยที่แอพพลิเคชันอันตรายจะหลุดขึ้นมาอยู่บน App Store ได้เหมือนกับที่เคยเกิดขึ้นใน Play Store ของระบบปฏิบัติการ Android ที่ใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบ [9] ความเข้มงวดในการจำกัดสิทธิ์การเข้าถึงข้อมูลสำคัญของผู้ใช้งานแอพพลิเคชันเมื่อต้องการเข้าถึงข้อมูลสำคัญหรือต้องการใช้ความสามารถที่อาจละเมิดความเป็นส่วนตัว เช่น เปิดใช้งานกล้องถ่ายรูป อัดเสียง ดูภาพที่ถ่าย ดูข้อมูลปฏิทิน ดูตำแหน่ง GPS จำเป็นต้องได้รับการอนุญาตจากผู้ใช้ก่อนเสมอ โดยจะมีหน้าต่างแจ้งเตือนการขออนุญาตแสดงขึ้นมาในครั้งแรกที่ผู้ใช้งานเรียกใช้ความสามารถนั้น ซึ่งจะต่างจากระบบปฏิบัติการ Android

ที่แอพพลิเคชันจะต้องขอสิทธิ์ทุกอย่างตั้งแต่แรก และหากผู้ใช้จะติดตั้งแอพพลิเคชันจะต้องยอมมอบสิทธิ์ทั้งหมดที่แอพพลิเคชันนั้นร้องขอโดยไม่สามารถเลือกว่าจะอนุญาตให้แอพพลิเคชันมีสิทธิ์แค่อย่างใดอย่างหนึ่งได้

แอพพลิเคชันที่ติดตั้งอยู่ในเครื่องจะไม่สามารถเข้าถึงข้อมูลของแอพพลิเคชันอื่นได้ นอกจากผู้ใช้จะเป็นผู้กำหนดข้อมูลที่ต้องการแชร์ระหว่างแอพพลิเคชันต่างๆระบบการจัดการแอพพลิเคชันของ IOS แอพพลิเคชันที่รันเป็น Background (ไม่ถูกเรียกขึ้นมาแสดงผล) จะถูกจำกัดความสามารถในการทำงานไม่สามารถใช้ทรัพยากรของระบบได้มากเท่า Android เช่น แอพพลิเคชันของ IOS ที่รันเป็น Background จะสามารถรับข้อความแจ้งเตือนเพื่อมาแสดงผลได้เท่านั้น ไม่สามารถอัดเสียงหรือประมวลผลงานอื่นที่ทำค้างอยู่ได้ [14] [12]

Charlie Miller (2011). ได้ทดลองส่งแอพพลิเคชันขึ้น App Store โดยลักษณะภายนอกเป็นแอพพลิเคชันธรรมดาแต่ตั้งค่าไว้ว่าเมื่อผู้ใช้ติดตั้งแอพพลิเคชันนี้ลงในเครื่องแล้วจะแอบไปดาวน์โหลดโค้ดของมัลแวร์มาทำงานทีหลัง แอพพลิเคชันตัวนี้สามารถผ่านการตรวจสอบจาก Apple และหลุดขึ้นมาอยู่บน App Store ได้ [6] [11]

Georgia Tech (2013) ได้ใช้เทคนิคใหม่ที่ทำให้สามารถส่งแอพพลิเคชันที่เป็นมัลแวร์ขึ้นไปอยู่บน App Store ได้อีกครั้งเหตุการณ์เหล่านี้ก็เป็นเครื่องพิสูจน์ที่ดีว่าถึงแม้จะใช้คนตรวจแล้วก็ตามแต่ก็ไม่อาจไว้ใจเรื่องความปลอดภัยได้ 100% [15]

มัลแวร์ใน IOSสามารถหลุดขึ้นไปอยู่บน App Store และมีผู้ใช้ได้รับความเสียหาย โดยในปี 2010 พบมัลแวร์ตัวแรกปรากฏอยู่บน App Store เป็นมัลแวร์ที่โทรศัพท์ไปยังหมายเลขปลายทางที่คิดค่าบริการในราคาแพง [20] และอีกครั้งในปี 2012 เป็นมัลแวร์ที่ส่งรายชื่อคนใน Contact List ออกไปทาง SMS [23] มัลแวร์ทั้งสองตัวนี้หลังจากที่ถูกค้นพบก็ถูกลบออกจาก App Store ในเวลาอันรวดเร็ว

ดังนั้นผู้เขียนจึงได้เขียนบทความวิจัยชิ้นนี้ เพื่อศึกษาและให้แนวคิดเกี่ยวกับข้อมูลของมัลแวร์บนระบบปฏิบัติการ IOS และ Android และเปรียบเทียบหาความแตกต่างระหว่างประสิทธิภาพของมัลแวร์และการใช้งานบนอินเทอร์เน็ตสำหรับมือถือบนอุปกรณ์พกพาโทรศัพท์เคลื่อนที่

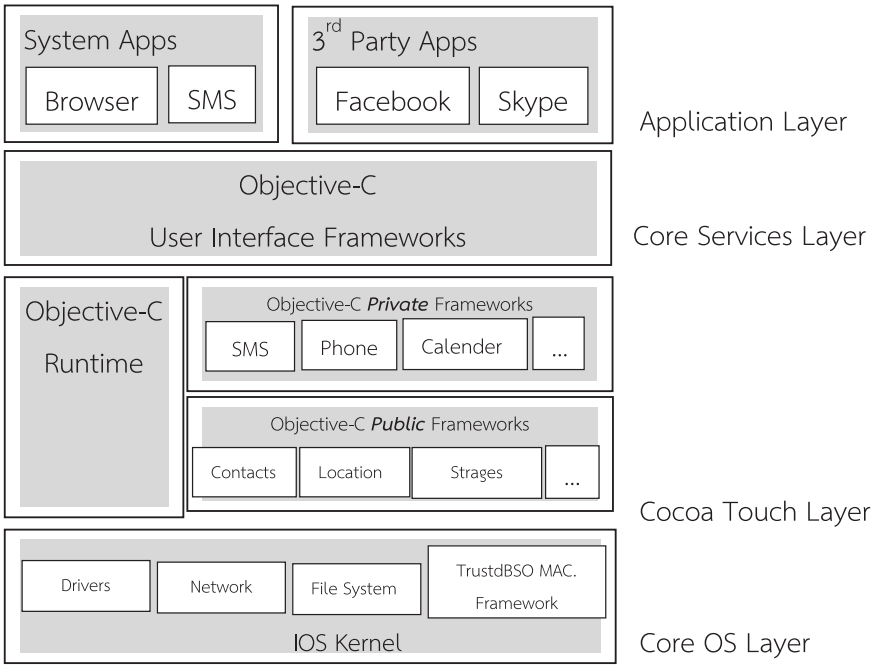
สำหรับส่วนที่เหลือของบทความจะอภิปรายเกี่ยวกับเรื่องต่างๆ ดังนี้ ส่วนที่ 2เป็นการนำเสนอโครงสร้างระบบปฏิบัติการ IOS และ Android ส่วนที่ 3 นำเสนอประเภทมัลแวร์ส่วนที่ 4 นำเสนอเกี่ยวกับประสิทธิภาพของมัลแวร์และส่วนสุดท้ายคือ บทสรุปและข้อเสนอแนะเกี่ยวกับบทความและงานที่เกี่ยวข้องในอนาคต

โครงสร้างระบบปฏิบัติการ IOS และ Android

ระบบปฏิบัติการบนโทรศัพท์เคลื่อนที่ หมายถึงโปรแกรมหรือซอฟต์แวร์ระบบที่ทำหน้าที่ควบคุมการทำงานของอุปกรณ์และโปรแกรมประยุกต์ต่างๆ ที่อยู่ภายในอุปกรณ์ เช่น เครื่องคอมพิวเตอร์มีการใช้ระบบปฏิบัติการWindows 8 และมีการลงโปรแกรม Microsoft Word ซึ่งเป็นโปรแกรมประยุกต์เพื่อใช้งาน

ดังนั้นปัจจุบันนอกจากระบบปฏิบัติการที่อยู่บนเครื่องคอมพิวเตอร์แล้ว ยังมีการนำไปใช้ในโทรศัพท์เคลื่อนที่เพื่อเพิ่มประสิทธิภาพให้สามารถทำงานได้มากกว่าโทรศัพท์มือถือ ซึ่งเรียกว่า Smart Phone ที่มีระบบปฏิบัติการบรรจุไว้ภายในโทรศัพท์เคลื่อนที่ โดยระบบปฏิบัติที่ใช้งานอยู่มีหลายชนิด แบ่งตามบริษัทผู้ผลิตและอุปกรณ์ เช่น Bada OS, Android และ IOS เป็นต้น [2]

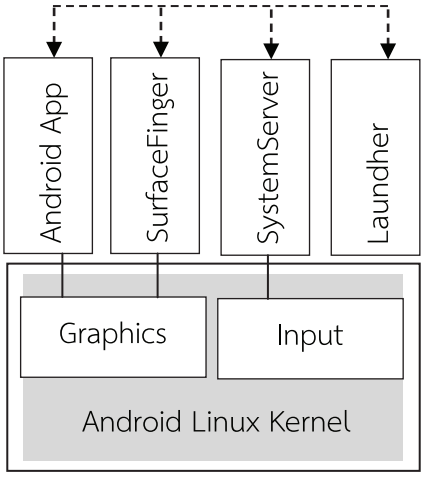
โครงสร้างของสถาปัตยกรรมซอฟต์แวร์ IOS ประกอบไปด้วยชั้นของ Media layer ซึ่งไม่รวมกันโดยพื้นฐานแล้ว โครงสร้างของสถาปัตยกรรม IOS มี 4 ชั้น คือ 1) ชั้นของแอพพลิเคชัน 2) ชั้นที่สองเรียกว่า Cocoa ซึ่งเป็นการจัดเก็บข้อมูลให้อยู่ในรูปแบบออบเจ็กต์เพื่อนำเสนอในรูปแบบของแอพพลิเคชัน 3) เรียกว่าชั้น Core Service เป็นส่วนหลักของการกำหนดโครงสร้างในการเข้าถึงโทรศัพท์ เป็นการอำนวยความสะดวกในการใช้งาน และชั้นที่ 4) ชั้น Core OS layer (แกนหลัก) เป็นส่วนที่ใช้ในการจัดหาสิ่งที่อำนวยความสะดวกให้กับระบบประกอบไปด้วย อุปกรณ์ในการเชื่อมต่อและระบบของไฟล์ข้อมูล ดังแสดงในภาพที่ 1



ภาพที่ 1 โครงสร้างสถาปัตยกรรมซอฟต์แวร์สำหรับ IOS
ที่มา : Tim Werthmann, Ralf Hund, Lucas Davi et, al. (2013).

โครงสร้างของสถาปัตยกรรมซอฟต์แวร์ Android ประกอบไปด้วย ชั้นของ Android Linux ซึ่งเป็นแกนหลัก และสามารถรันบนระบบ ARM CPUs. ดังนั้นโครงสร้างสถาปัตยกรรมซอฟต์แวร์ Android ประกอบด้วยตัวเลขสำหรับการให้บริการของระบบและไลบารี่เพื่อให้บริการแอพพลิเคชันเน้นภาพกราฟิก การใส่ข้อมูลลงบนอุปกรณ์ ตัวอย่างเช่น เริ่มต้นสำหรับการใช้งานระบบเซิฟเวอร์ จุดเริ่มต้นที่ Launcher

การกลับไปสู่จุดเริ่มต้นที่เป็นแบบโฮมสกรีนถือเป็นแอพพลิเคชันบน Android และการสแกนลายนิ้วมือ รวมไปถึงรูปแบบของการใช้งานสำหรับผู้ใช้ ท้ายสุดเป็นการแสดงผลออกมาในรูปแบบข้อมูลที่อยู่บนหน้าจอรายละเอียดข้อมูล ดังแสดงในภาพที่ 2



ภาพที่ 2 โครงสร้างสถาปัตยกรรมซอฟต์แวร์สำหรับ Android
ที่มา : Jeremy Andrus et.,al. (2014).

ข้อมูลแสดงการเปรียบเทียบโครงสร้างการทำงานของฮาร์ดแวร์กับระบบปฏิบัติการ

1. Framework & Architect : คือโครงสร้างและการทำงานของฮาร์ดแวร์กับระบบปฏิบัติการ

IOS : เป็นโครงสร้างที่ซับซ้อนในการติดต่อกันระหว่างฮาร์ดแวร์กับซอฟต์แวร์ทำงานเข้ากันได้ดีเพราะผลิตมาเพื่อระบบปฏิบัติการ IOS โดยเฉพาะแต่การทำงานยังด้อยกว่า Android

Android : มีโครงสร้างที่ซับซ้อนอีกชั้นนึงออกแบบให้เอาไปใช้ได้ง่ายกับอุปกรณ์บนมือถือแบบใดก็ได้ส่วนใหญ่แต่ละค่ายมือถือทำได้ดีทำให้มีความหลายหลายของระบบเหนือกว่า IOS และมากกว่า Android

2. Feature : คือฟังก์ชันที่สามารถทำงานได้

IOS : ฟังก์ชันการทำงาน มีฟังก์ชันการทำงานที่หลากหลายน้อยกว่าเพราะ apple เป็นผู้สร้างสรรค์เพียงแหล่งเดียว

Android : ฟังก์ชันการทำงานมีความหลายหลายเพราะระบบปฏิบัติการเป็นโอเพนซอร์สทุกค่ายมือถือจะช่วยกันพัฒนาทาง Google ก็จะนำมาใส่ในระบบปฏิบัติการ Android รุ่นต่อไป

3. Multitasking : การทำงานหลายอย่างพร้อมกัน

Android : Full multitaskคือ แอพพลิเคชันที่มีหลายฟังก์ชันในตัวเดียวกันข้อดีคือเหมือนคอมพิวเตอร์ตั้งโต๊ะที่ทรงพลังสามารถทำงานหลายๆ อย่างได้พร้อมกันเต็มเวลา

IOS : semi multitask คือ จะทำงานเฉพาะแอพที่เปิดอยู่ให้มีความสำคัญสูงสุด แต่แอพหลังฉากส่วนใหญ่จะไม่ทำงานต่อ อยู่ในสถานะ sleep หรือ minimal work เท่าที่จำเป็น ทำให้สามารถทำอะไรได้ทีละอย่าง ไม่สามารถทำอะไรหลายอย่างได้พร้อมกัน [10]

ประเภทมัลแวร์

มัลแวร์ (Malware) ย่อมาจาก “Malicious Software” หมายถึงโปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อระบบคอมพิวเตอร์และเครือข่าย โดยจะเข้ามาบุกรุกเครื่องคอมพิวเตอร์ของเราและสร้างความเสียหายให้กับระบบคอมพิวเตอร์และเครือข่าย นอกจากนั้นแล้ว ถ้ามีโอกาสก็จะทำการแทรกตัวเข้าไประบาดในระบบคอมพิวเตอร์ของเครื่องอื่นและระบบเครือข่าย สาเหตุดังกล่าวอาจจะเกิดจากการนำเอาอุปกรณ์จำพวก ดิสก์ หรือแฟลชไดว์ที่ติดไวรัสจากเครื่องหนึ่งเอาไปใช้งานในอีกเครื่องหนึ่ง อาจจะผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลสามารถทำให้ไวรัสแพร่ระบาดได้[1]

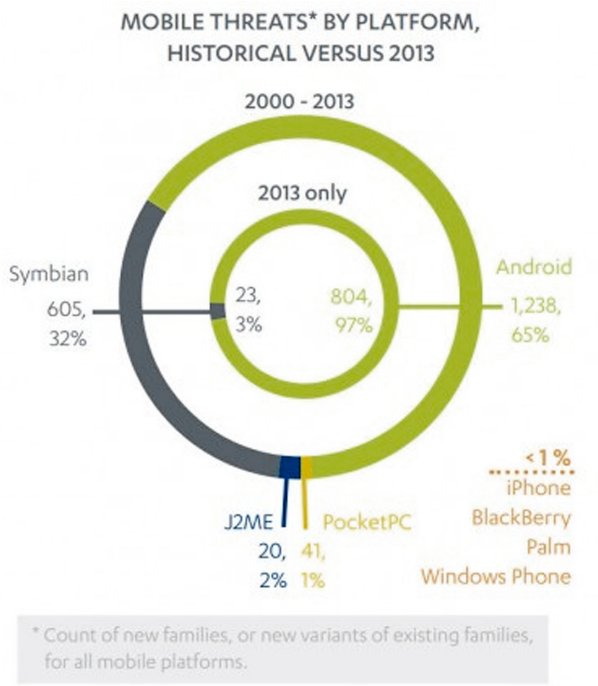
มัลแวร์ คือโปรแกรมที่ถูกออกแบบมาเพื่อโจมตีผู้ใช้เป็นหลักไม่ว่าจะเป็นการขโมยข้อมูลทำให้ระบบเสียหาย แอบดักจับข้อมูลโดยผู้ใช้ ซึ่งมีรูปแบบการหลอกลวงหลายช่องทางจากสถิติของ Symantec ชี้ว่า 97% ของ Malware อยู่บน Android, 3% อยู่บน Symbian ส่วนใน IOS, BlackBerry, Windows Phone รวมกันทั้งหมดยังน้อยกว่า 1% [24]

มัลแวร์ในระบบปฏิบัติการ IOS ตัวแรกสุดถูกค้นพบเมื่อปี 2009 เป็นมัลแวร์ที่มีการส่งต่อ SMS ของผู้ใช้ไปยังบุคคลอื่น หลังจากนั้นก็เริ่มมีการค้นพบมัลแวร์ใน IOS เพิ่มขึ้น โดยมีทั้งแบบที่เป็น Spyware หรือมัลแวร์ขโมยข้อมูลธนาคารออนไลน์ แต่เกือบทั้งหมดมัลแวร์สามารถติดได้เฉพาะเครื่องที่ถูก Jailbreak แล้วดังตารางที่ 1 [3]

หลักการทำงานของมัลแวร์คือตัวมัลแวร์จะติดมากับเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Mac OS X หรือ Windows ก่อน จากนั้นจะเฝ้ารอให้ผู้ใช้นำอุปกรณ์ที่ใช้งานระบบปฏิบัติการ IOS มาเชื่อมต่อกับเครื่องผ่านพอร์ต USB แล้วจึงติดตั้งแอพพลิเคชัน IOS อันตรายลงไปในเครื่องเหยื่อเพื่อขโมยข้อมูลนอกจากนี้ยังมีความสามารถเชื่อมต่อไปยังเซิร์ฟเวอร์ของผู้สั่งการมัลแวร์เพื่ออัพเดตความสามารถใหม่เพิ่มเติมเนื่องจากมัลแวร์ตัวนี้แพร่กระจายผ่านการเสียบสายเคเบิลจึงถูกตั้งชื่อว่า WireLurker [8]

มัลแวร์ในระบบปฏิบัติมือถืออยู่บนพื้นฐานของการสแกนลายนิ้วมือ ซึ่งจำนวนไวรัสประเภทของซอฟต์แวร์สำหรับโทรศัพท์มือถือเป็นภัยคุกคามที่จะเข้ามาทำลาย เมื่อวิเคราะห์ข้อมูลประเภทไวรัส เช่นแบบไดนามิกและแบบการวิเคราะห์คงที่ โดยกิจกรรมที่ตอบสนองบนพื้นฐานของผู้บริโภคจะนำเสนอในงานวิจัยชิ้นนี้ คือแนวคิดที่กล่าวถึงหลักความเป็นจริงต้องมีการบรรจุข้อมูลลงในจำนวนข้อมูลทั้งหมด ดังนั้นผู้บริโภคอาจจะไม่จำเป็นต้องมีแอพพลิเคชันที่หลากหลาย เช่น เมื่อผู้บริโภคมีการเรียนรู้การใช้อุปกรณ์เพิ่มเติมในส่วนการใช้งานที่เป็นไปได้ โดยเป็นการประเมินโครงสร้างเกี่ยวกับรูปแบบของสมาร์ทโฟน ซึ่งผลลัพธ์ของ

การทำงานไม่สนับสนุนอุปกรณ์ ดังนั้น ผลการทดสอบความเป็นไปได้สำหรับมัลแวร์ที่อยู่ในระบบปฏิบัติการมีตัวชี้วัดในการเพิ่มความสามารถพื้นฐาน เช่น การใช้แอพพลิเคชันที่มีขนาดเล็กและมีอัตราของการหาค่าความผิดพลาดบนพื้นฐานของเครื่องมือ โดยตลาดของแอพพลิเคชันวันนี้เป็นของสมาร์ทโฟน มากไปกว่านั้น การจัดหาอุปกรณ์และปริมาณสำหรับโครงสร้างหรือเซนเซอร์ ตัวอย่าง การใช้ GPS, WiFi ใช้หน้าจอแบบทัชสกรีนหรือการใช้งานเว็บเบราเซอร์เปรียบเทียบกับสมาร์ทโฟนซึ่งโครงสร้างทั้งหมดนี้ถูกนำเสนอโดยผู้ใช้งาน [22] [16].จากสถิติของ Symantec ชี้ว่า 97% ของ Malware อยู่บน Android, 3% อยู่บน Symbian ส่วนใน IOS, BlackBerry, Windows Phone รวมกันทั้งหมดยังน้อยกว่า 1% [5]



ภาพที่ 3 แสดงข้อมูลพื้นฐานเกี่ยวกับประวัติไวรัสในปี 2013
ที่มา : http://www.macthai.com/2014/04/09/97-percent-of-mobile-malware-is-on-android/

ตารางที่ 1 แสดงข้อมูลรายชื่อมัลแวร์ใน IOS ทั้งหมดที่ค้นพบตั้งแต่เดือนมิถุนายน 2009 ถึงเมษายน 2014

Name	Discovery date	Presumed origin	Devices	Type
IOS/Trapsms/.A!tr.spy	June 2009	Russia?	Jailbroken	SMS Forwarder
Spy/MobileSpy!iPhone OS	Aug 2009	USA	Jailbroken	Spyware
IOS/Eeki.A!worm	Nov 2009	Australia (Ashley Towns)	Jailbroken	Worm Proof of Concept
IOS/Eeki.B!worm	Nov 2009	The Netherlands	Jailbroken	Mobile banking malware
IOS/Toires.A!tr.spy	Nov 2009	Switzerland (Nicolas Seriot)	Any (jailbroken or not)	Rogue application Proof of Concept

ตารางที่ 1 (ต่อ)

Name	Discovery date	Presumed origin	Devices	Type
Adware/LBTM!IOS	Sep 2010	France	Any (jailbroken or not)-Was	Call premium phone number
			found (and removed) in the official AppStore	
Spy/KeyGuard!iPhoneOS	Apr 2011	Czech Rep.	Jailbroken	Keylogger
IOS/FindCall.A!tr.spy	July 2012	Russia ?	Any (jailbroken or not)-Was found (and removed) in the official AppStore	Privacy trojan
Riskware/Killmob!IOS	July 2013	USA	Jailbroken	Spyware
IOS/AdThief.A!tr	Mar 2014	China	Jailbroken	Ad revenue hijacking
IOS/SSLCreds.A!tr.pws	Apr 2014	China	Jailbroken	Password stealer

ที่มา : https://blog.fortinet.com/post/ios-malware-does-exist.

เนื่องจากบริษัท Apple, Google ได้อนุญาตให้ใช้งานแอพพลิเคชันได้และภาพรวมในส่วนของการตลาดและการส่งสัญญาณไปยังผู้ใช้งานต้องมีความปลอดภัยจากมัลแวร์ ดังนั้นจึงต้องมีการประเมินประสิทธิภาพของเครื่องมือและจัดกลุ่มตัวเลขที่เป็นอันตรายสำหรับเอนดรอยด์ โดยมีการอนุญาตให้ใช้งาน 11 กลุ่ม ซึ่งมัลแวร์ที่ไม่ได้อยู่บนแอพพลิเคชันมีทั้งหมด 956 กลุ่ม ดังแสดงในตารางที่ 2

ตารางที่ 2 จำนวนตัวเลขที่เป็นอันตรายสำหรับเอนดรอยด์ มีการอนุญาตให้ใช้งาน 11 กลุ่มซึ่งมัลแวร์ที่ไม่อยู่บนแอพพลิเคชันมีทั้งหมด 956 กลุ่ม

Number of Dangerous permissions	Number ofnon-malicious applications	Number ofmalicious applications
0	75 (8%)	-
1	154 (16%)	1
2	182 (19%)	1
3	152 (16%)	-
4	140 (15%)	2
5	82 (9%)	1
6	65 (7%)	-
7	28 (3%)	2
8	19 (2%)	1

ตารางที่ 2 (ต่อ)

Number of Dangerous permissions	Number ofnon-malicious applications	Number ofmalicious applications
9	21 (2%)	1
10	10 (1%)	1
11	6 (0.6%)	1
12	7 (0.7%)	-
13	4 (0.4%)	-
14	4 (0.4%)	-
15	2 (0.2%)	-
16	1 (0.1%)	-
17	1 (0.1%)	-
18	-	-
19	-	-
20	1 (0.1%)	-
21	-	-
22	-	-
23	1 (0.1%)	-
24	-	-
25	-	-
26	1 (0.1%)	-

ที่มา : Adrienne Porter Felt, et al. (2011).

การวัดประสิทธิภาพของมัลแวร์

ณ ปัจจุบันรุ่นโทรศัพท์มือถือหรือสมาร์ทโฟนกับผู้ใช้งานมีความจำเป็นสำหรับการใช้งานบนเว็บไซต์ โดยเปรียบเทียบรุ่นโทรศัพท์มือถือที่ใช้กับจำนวนผู้ใช้บริการ ดังแสดงในภาพที่ 4 แหล่งข้อมูลเป็นเสมือนประตูสู่องค์กร ซึ่งเว็บไซต์ได้ปรับเปลี่ยนรูปแบบให้ดูน่าสนใจและมีความปลอดภัยเพิ่มขึ้น การระบุตัวตนผู้ใช้งานที่ดีเช่น การใช้งานเว็บบอร์ด เป็นต้น ซึ่งรหัสการเข้าใช้งานและรหัสผ่านมีความสำคัญสำหรับผู้พัฒนาเว็บไซต์

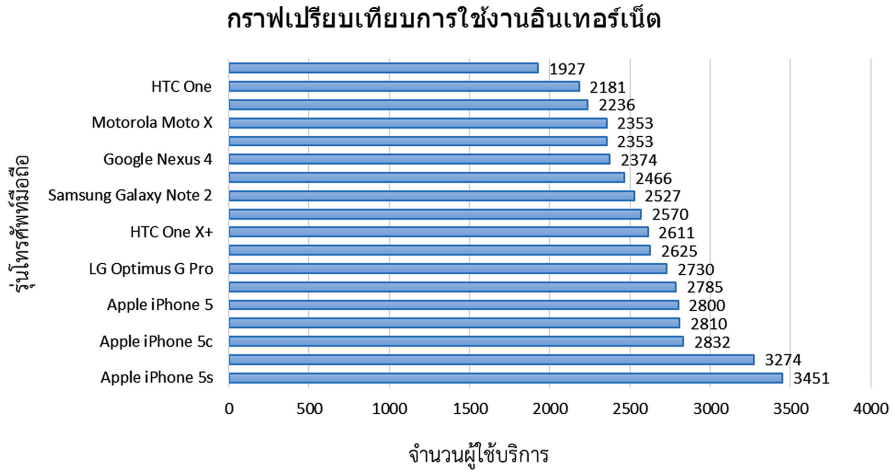
การใช้งานเว็บบอร์ดอาจก่อให้เกิดช่องโหว่ของภัยคุกคามที่มากับเว็บไซต์ได้และอาจสร้างความเสียหายให้กับองค์กรได้ ไม่ว่าจะเป็นทางด้านข้อมูล ด้านชื่อเสียง ซึ่งไม่สามารถประเมินค่าได้ [24], [25] ดังนั้นกระบวนการของการวัดประสิทธิภาพมัลแวร์ต้องมีการเรียนรู้และจัดกลุ่มของมัลแวร์ทั้งหมด ดังนี้

Yajin Zhou และคณะ (2011). ได้กล่าวว่า พื้นฐานการเรียนรู้ตัวอย่างมัลแวร์ ขั้นตอนแรกต้องมีการอนุญาตให้ใช้ข้อมูลเป็นปัจจุบันก่อนและความต้องการสำหรับมัลแวร์ขึ้นอยู่กับรูปแบบของฟังก์ชันที่เปิดใช้งานบนแอพพลิเคชัน ดังตารางที่ 3แสดงประสิทธิภาพในการเรียนรู้เพื่อจัดกลุ่มมัลแวร์ทั้ง 10 ประเภท เพื่ออนุญาตให้การใช้งานมีประสิทธิภาพและรายงานจำนวนตัวเลขของการใช้งานแอพพลิเคชันบนพื้นฐานของการกรองข้อมูล โดยเฉพาะกลุ่มของข้อมูลจำนวน 8 กลุ่ม จะต้องมีอย่างน้อย 6% ของการใช้แอพพลิเคชัน เพื่อนำไปประยุกต์ใช้งาน ในกรณีนี้ จำเป็นต้องมีการลงทะเบียนการกระจายสัญญาณของการรับส่งข้อมูลสำหรับเอนดรอยด์ ดังนั้น ต้องมีการทดสอบเงื่อนไขก่อนให้อยู่ในรูปแบบที่ตรงกัน โดยการลดสัญญาณมีอัตราเฉลี่ยร้อยละ 0.64 [23]

ตารางที่ 3 ตารางประสิทธิภาพในการเรียนรู้เพื่อจัดกลุ่มมัลแวร์ทั้ง 10 ประเภท

Malware	Essential Permissions	Apps
ADRD	INTERNET, ACCESS_NETWORK_STATE RECEIVE_BOOT_COMPLETED	10,379 (5.68 %)
Bgserv	INTERNET, RECEIVE_SMS, SEND_SMS	2,880 (1.58 %)
DroidDream	CHANGE_WIFI_STATE	4,096 (2.24 %)
DroidDreamLight	INTERNET,READ_PHONE_STATE	71,095 (38.89 %)
Geinimi	INTERNET, SEND_SMS	7,620 (4.17 %)
jSMSHider	INSTALL_PACKAGES	1,210 (0.66 %)
BaseBridge	NATIVECODE	8,272 (4.52 %)
Pjapps	INTERNET,RECEIVE_SMS	4,637 (2.54 %)
Zsone	RECEIVE_SMS_SEND_SMS	3,204 (1.75 %)
ZHash	CHANGE_WIFI_STATE	4,096 (2.24 %)

ที่มา : Yajin Zhou, Zhiwang, Wu Zhou, Xuxian Jiang (2011).



ภาพที่ 4 แสดงกราฟเปรียบเทียบการใช้งานอินเทอร์เน็ต
ที่มา : Rishi Chandy and Haijiegu (2012).

สำหรับความแตกต่างของโครงสร้างสมาร์ทโฟน เริ่มตั้งแต่ผู้บริโภคหลักต้องมีการตรวจจับซอฟต์แวร์ไวรัสคอมพิวเตอร์ ส่วนการเขียนซอฟต์แวร์สามารถรันและทดสอบโดยการเรียกใช้ฟังก์ชันที่เกี่ยวข้อง มัลแวร์ต้องมีรูปแบบที่มองเห็นชัดเจนเพื่อเป็นการวัดประสิทธิภาพฟังก์ชันทุกฟังก์ชันสามารถที่จะส่งและรับข้อความ เพื่อติดต่อฐานข้อมูลกับข้อความการเข้ารหัสผ่านเครือข่าย การที่จะเข้าถึงข้อมูลได้นั้น ต้องมีตัวเลขของการบันทึกข้อมูล การทดสอบเริ่มโดยการประเมินเพื่อทดสอบการใช้งานของผู้บริโภคโดยมีส่วนประกอบหลัก ดังนี้ การนำเสนอข้อมูลเพื่อทดสอบและให้คำจำกัดความบนพื้นฐานของการทดสอบและเปรียบเทียบข้อมูล รวมไปถึงจำนวนของสมาร์ทโฟนที่ต้องการ โดยข้อมูลสำหรับการติดต่อ Wi-Fi และ 3G ต้องตรวจจับโทรศัพท์มือถือ ซึ่งตารางที่ 4 แสดงระยะเวลาที่ทดสอบระหว่างคาบ 5 นาที หาค่าเฉลี่ยจากผู้ใช้งานสำหรับการติดต่อผ่านระบบ Wifi และตารางที่ 5 แสดงตัวเลขเพื่อกรองข้อมูลของแอพพลิเคชันภายหลังจากมีการรับส่งข้อมูล [21]

ตารางที่ 4 ระยะเวลาที่ทดสอบระหว่างคาบ 5 นาที หาค่าเฉลี่ยจากผู้ใช้งาน สำหรับการติดต่อผ่านระบบ Wifi

Connection	Consumption	CV
WiFi (always on)	51.17 mW	0.87%
WiFi (if screen is on)	51.26 mW	1.14%
3G	68.47 mW	9.49%

ที่มา : Yajin Zhou, Zhi Wang, Wu Zhou, Xuxian Jiang (2011).

ตารางที่ 5 แสดงตัวเลขเพื่อกรองข้อมูลของแอพพลิเคชันภายหลังจากมีการรับส่งข้อมูล

Permission	RECEIVE_SMS	SEND_SMS	RECEIVE_SMS & SEND_SMS
Apps	5,214	8,235	3,204
Percentage	2.85%	4.50%	1.75%

ที่มา : Yajin Zhou, Zhi Wang, Wu Zhou, Xuxian Jiang (2011).

บทสรุปและข้อเสนอแนะ

มัลแวร์ในระบบปฏิบัติการมือถือสำหรับ IOS และ Android ได้เพิ่มขึ้นและพัฒนาอย่างต่อเนื่องโดยเฉพาะแอพพลิเคชันที่อยู่บน Android ถึงแม้ว่าข้อมูลที่อยู่บน Google Play เป็นไวรัสซอฟต์แวร์ที่มีฟังก์ชันการทำงานที่หลากหลายเริ่มตั้งแต่ปีค.ศ. 2012 แต่เป็นการค้นพบที่ยังไม่ได้รับการเปิดเผยและต่อมาได้ให้ความสำคัญเกี่ยวกับผู้ใช้งานและผู้ใช้งานสามารถดาวน์โหลดข้อมูลได้ทุกที่ทุกเวลา

เมื่อเปรียบเทียบกับมัลแวร์ของระบบปฏิบัติการ IOS สามารถดาวน์โหลดได้จาก App Store มีกระบวนการของการทำงานโดยรันบนสคริปต์ ไม่เหมือนกับแอพพลิเคชันทั่วไปที่ควรจะมีฟังก์ชันที่หลากหลาย การค้นพบมัลแวร์ในระบบปฏิบัติการ IOS มีหลายประเภท เช่น สปายแวร์ แอดแวร์เป็นต้น ดังนั้นเมื่อสมาร์ทโฟนมีการถูกJailbreak ผู้ใช้งานสามารถใช้อุปกรณ์เพื่อเข้าถึงข้อมูลได้ โดยแอพพลิเคชันบน IOS สามารถค้นหาได้ที่ App Store

อย่างไรก็ตามระบบปฏิบัติการมือถือไม่ได้มีความปลอดภัยไปจากมัลแวร์เนื่องจากผลการสำรวจพบว่า การรับส่งแอพพลิเคชันมีอัตราความเร็วเพิ่มขึ้น เนื่องจากระบบอินเทอร์เน็ตเป็นส่วนสำคัญที่นำไปสู่ภัยคุกคามได้ โดยเฉพาะมัลแวร์ดังนั้น ผู้ใช้งานจึงต้องมีวิธีการเรียนรู้และป้องกันตนเองให้ปลอดภัย โดยให้ความสำคัญถึงวิธีและกระบวนการเรียนรู้เพื่อดาวน์โหลดอัพโหลดข้อมูลก่อนที่จะนำมาใช้งานบนสมาร์ทโฟนโดยในอนาคตต้องมีมาตรการป้องกันมัลแวร์เพื่อเข้าถึงระบบปฏิบัติการให้ช้าลงมากกว่าที่เป็นอยู่ ดังนั้นต้องศึกษาถึงปัจจัยและสภาพแวดล้อมที่เกี่ยวข้องทั้งหมด เช่น การใช้งานอินเทอร์เน็ต อัตราความเร็วของการรับส่งข้อมูล เป็นต้น เพื่อให้ได้ผลลัพธ์ที่มีความถูกต้องและชัดเจนต่อการป้องกันมัลแวร์ที่จะเข้าสู่สมาร์ทโฟน

เอกสารอ้างอิง

[1]. ประจักษ์ ธัญวิรภาพ (2536). **รวม 1080 ไวรัสคอมพิวเตอร์**. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

[2]. อรพิน ประวัติบริสุทธิ์. (2551). **คู่มือเรียนระบบปฏิบัติการ** = Operating system.กรุงเทพฯ : โปรวิชั่น.

[3]. เสฏฐวุฒิ แสนนาม(2557). **WireLurkerและ Masque Attack : ผู้ใช้ iOSติดมัลแวร์ได้แม้ไม่** Jailbreak.[ออนไลน์]. ได้จาก : https://www.thaicert.or.th/papers/general/2013/pa2013ge007.html

[4]. Kelly Gordon. (2014). **Report : 97% OfMobile Malware Is On Android. This Is The Easy Way You Stay Safe**. [ออนไลน์]. ได้จาก : http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/.

[5]. **เปรียบเทียบ Android กับ iOS ด้าน OS (ระบบปฏิบัติการ) (2015)**. [ออนไลน์]. ได้จาก : http://androidsogood.blogspot.com/2015/01/android-ios-os.html.

[6]. Claudine Beaumont(2008). **Apple's Jobs confirms iPhone 'kill switch**. [ออนไลน์]. ได้จาก : http://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-kill-switch.html

[7]. App Review Guidelines. (2015). [ออนไลน์]. ได้จาก : https://developer.apple.com/app-store/review/guidelines/.

[8]. Denis Maslennikov. (2012). **Find and Call: Leak and Spam**. [ออนไลน์]. ได้จาก : http://securelist.com/blog/incidents/33544/find-and-call-leak-and-spam-57/

[9]. ValliMeenakshiRamanathan. **(2012). Google Play Store Gets Built-In Malware Scanner; Alerts Users AgainstPossible Threats At Download Stage**. [ออนไลน์]. ได้จาก : http://www.ibtimes.com/google-play-store-gets-built-malware-scanner-alerts-users-against-possible-threats-download-stage

[10]. AxelleApvrille (2014). **iOS Malware Does Exist**. [ออนไลน์]. ได้จาก : https://blog.fortinet.com/post/ios-malware-does-exist.

[11]. Andy Greenberg (2011). **iPhone Security Bug Lets Innocent-Looking Apps Go Bad** [ออนไลน์]. ได้จาก : http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/

[12]. Tim Bray (2010). **Multitasking the Android Way** [ออนไลน์]. ได้จาก : http://android-developers.blogspot.com/2010/04/multitasking-android-way.html

[13]. Josh Lowensohn (2013). **Researchers slip malware onto Apple's App Store, again** [ออนไลน์]. ได้จาก : http://www.cnet.com/news/researchers-slip-malware-onto-apples-app-store-again/

[14]. **Understand multitasking and background activity on your iPhone, iPad, or iPod touch. (2015)**. [ออนไลน์]. ได้จาก : http://support.apple.com/en-us/HT202070.

[15]. Michael Irschick (2012). **Use a website to distribute your iOS app for Beta Testing**. [ออนไลน์]. ได้จาก : http://3qilabs.com/how-to-ad-hoc-distribute-your-ios-app-via-a-website-and-ota/

[16]. Fortinet (2014). **Virus : Adware/LBTM!iPhoneOS**. [ออนไลน์]. ได้จาก : http://www.fortiguard.com/encyclopedia/virus/#id=2102975

[17]. Adrienne Porter Felt et.,al. (2011). **A Survey of Mobile Malware in the Wild**. ACM : 1-12.

[18]. HienThi Thu Truong et.,al. (2014). **The Company You Keep : Mobile Malware Infection Rates and Inexpensive Risk Indicators**. ACM.1-11.

[19]. Jeremy Andrus et.,al. (2014). **Native Execution of IOS Apps on Android**. ACM.1-12.

[20]. Johannes Hoffmannet.,al. (2012). **Mobile Malware Detection Based on Energy Fingerprints – A Dead End?**. ACM : 1-20.

[21]. Rishi Chandy and HaijieGu. (2012). **Indentifying Spam in the IOS App Store**. ACM.1-4.

[22]. Tim Werthmann, Ralf Hund and Lucas Davi. (2013). **PSiOS : Bring Your Own Privacy & Security to IOS Devices**. ASIA CCS' 13.1-12.

[23]. Yajin Zhou, Zhiwang, Wu Zhou, Xuxian Jiang (2011). **Hey, You, Get Off of MyMarket : Detecting Malicious Apps in Official and Alternative Android Markets**. Department of Computer Science.1-13.

[24]. Ying Chen et.,al. (2013). **Is This App Safe for Children? A Comparison Study of Maturity Ratings on Android and IOS Applications**. ACM.1-11.

[25]. ZinaidaBenensonet.,al. (2013). **Android and IOS Users' Differences concerning Security and Privacy**.ACM.1-13.