โครงการด้านความมั่นคงปลอดภัยทางไซเบอร์
ชื่อโครงงาน สปายแวร์

จัดทำโดย

1 B6320409 น.ส รัตนา สังข์ทอง

2 B6320430 นาย ธนภัทร กันนุลา

3 B6330606 นาย อธิปรัฐ อัมรารัมย์

4 B6333959 น.ส เพลงสกุล ดีพลงาม

5 B6335441 นาย ชานน สัมพันธ์วงศ์

เสนอ

รองศาสตราจารย์ ดร. ศิรปัฐช์ บุญครอง

โครงงานนี้เป็นส่วนหนึ่งของรายวิชา 1101201

Foundation in Information and Network Security

สาขาเทคโนโลยีสารสนเทศ สำนักวิชาเทคโนโลยีสังคม

มหาวิทยาลัยเทคโนโลยีสุรนารี

บทคัดย่อ

รายงานเล่มนี้ทำการจัดทำขึ้นมาเพื่อแก้ไขปัญหาทางคอมพิวเตอร์ ที่ได้มีการโดนโจมตีด้วย Spyware ทางเราจึงได้ทำการศึกษาหาค้นคว้าวิธีการป้องกันและกำจัด Spyware ให้สำหรับคอมพิวเตอร์ เราได้ค้นพบว่า Spyware นั้นสามารถทำการโจมตีคอมพิวเตอร์ได้ในหลากหลายรูปแบบ และทางเราได้ทำการออกแบบกระบวนการการป้องกันและกำจัด Spyware ไว้ด้วย ตามวัตถุประสงค์ดังนี้ และรายงานเล่มนี้ได้จัดทำขึ้นตามวัถตุประสงค์ที่ทางเราได้ตั้งไว้คือ (1)เพื่อศึกษาหลักการทำงานของ Spyware ว่ามีหลักการทำงานกี่ประเภท (2)เพื่อออกแบบกระบวนการการกำจัดและป้องกัน Spyware และนอกจากนี้ขอบเขตของการทำโครงงานนี้มีดังนี้ (1)เพื่อศึกษาและหาวิธีป้องกัน Spyware ไม่ให้ Spyware สามารถเข้ามาในเครื่องเราได้ (2)เพื่อออกแบบกระบวนการป้องกันการโจมตีของ Spyware

ผลลัพธ์ของโครงงานพบว่าทางเราค้นคว้าต่อไปเราค้นพบว่าไม่ใช่แค่ Spyware ที่สามารถโจมตีคอมพิวเตอร์ได้ ยังมี Malware ตัวอื่นๆ อีกที่สามารถโจมตีได้เช่น ไวรัส เป็นต้น ทางเราจึงได้ทำการออกแบบโครงสร้างของโปรแกรมที่สามารถทำการกำจัด Malware ทั้งหมดได้ โดยการใช้ MD5 ที่เป็น Hash ฟังชันส์ที่สามารถเช็คความถูกต้องของข้อมูล เข้าทำการสแกนหาความผิดปกติในคอมพิวเตอร์และส่งข้อมูลไปประมวลผลบน Cloud และทำการกำจัด Malware ทั้งหมดได้ เราจึงได้ผลลัพธ์มาดังต่อไปนี้ (1)าสามารถกำจัดและป้องกัน Spyware ได้ (2)เพื่อเป็นการศึกษากระบวนการทำงานของ Spyware และวิธีป้องกันการโดนโจมตีของ Spyware

สารบัญ

1ข้อเสนอโครงการด้านความมั่นคงปลอดภัยทางไซเบอร์

1. ชื่อโครงงาร (ภาษาไทย)

สปายแวร์

2. ชื่อโครงงาน (ภาษาอังกฤษ) (ถ้ามี)

spyware

3. รายชื่อผู้จัดทำโครงงาน

3.1 B6320409 น.ส รัตนา สังข์ทอง

3.2 B6320430 นาย ธนภัทร กันนุลา

3.3 B6330606 นาย อธิปรัฐ อัมรารัมย์

3.4 B6333959 น.ส เพลงสกุล ดีพลงาม

3.5 B6335441 นาย ชานน สัมพันธ์วงศ์

4. ที่มาและความสำคัญของปัญหา

อธิบายปัญหา

สปายแวร์เป็นซอฟต์แวร์ที่มีความสามารถในการสังเกตการณ์ ดักจับข้อมูล หรือควบคุมอุปกรณ์อิเล็กทรอนิกส์ของใครก็ตามที่อาจจะเผลอไปติดตั้งหรือดาวน์โหลดมันมาไว้ในอุปกรณ์ของตัวเอง

อธิบายผลกระทบของปัญหา

สปายแวร์สามารถเก็บเกี่ยวข้อมูลต่าง ๆ ในอุปกรณ์ของเราได้ ไม่ว่าจะเป็นข้อความ SMS, เบอร์ติดต่อในสมุดโทรศัพท์, ประวัติการโทร, ปฏิทิน, อีเมล, ประวัติการท่องอินเทอร์เน็ตทั้งหมด และโปรแกรมที่เป็นของสปายแวร์เมื่อเราโหลดลงเครื่องคอมพิวเตอร์ก็จะทำให้เครื่องไม่ปลอดภัย สามารถเกิดการขโทยหรือทำลายข้อมูลได้

ข้อมูลพื้นฐาน หรือข้อมูลสนับสนุน เช่น ข้อมูลเชิงสถิติ การสอบถาม ข้อมูลจากข่าวหรือบทความ

อ้างอิงมาจาก

ข้อมูลรั่วไหล! “เพกาซัส” สปายแวร์อันตรายที่หลายประเทศใช้จับตาประชาชน

เมื่อวันที่ 18 ก.ค. สำนักข่าวใหญ่ 17 สำนัก จับมือกันรายงานข่าวกรณีพบข้อมูลรั่วไหวครั้งใหญ่ โดยพบว่า “มีรัฐบาลหลายประเทศใช้สปายแวร์ ‘เพกาซัส (Pegasus)’ แอบสอดส่องและขโมยข้อมูลจากโทรศัพท์มือถือของบุคคลจากหลายประเทศทั่วโลก”

สิ่งที่มันทำได้ถือเป็นการรุกล้ำสิทธิส่วนบุคคลขั้นร้ายแรง เพราะมันจะรู้ว่าคุณโทรหาใคร แชตหาใคร คุยกันเรื่องอะไร เข้าถึงไฟล์หรือรูปภาพทั้งหมด รู้ว่าคุณอยู่ที่ไหน และที่ร้ายกว่านั้น มันสามารถเปิดกล้องและไมค์บันทึกเสียงเพื่อดูว่าคุณกำลังทำอะไรอยู่ได้ด้วย

เพกาซัสถูกพัฒนาและขายแก่รัฐบาลทั่วโลกโดยบริษัท NSO Group ของอิสราเอล มีความสามารถในการแพร่ระบาดในโทรศัพท์ที่ใช้ระบบปฏิบัติการ iOS หรือ Android

เพกาซัสเวอร์ชันแรกสุดถูกตรวจพบในปี 2016 โดยพบในโทรศัพท์ที่ติดไวรัสหลังมีการกดลิงก์ในข้อความหรืออีเมลที่หลอกล่อให้เป้าหมายกดคลิกเข้าไปดู

แต่ในช่วงหลัง ความสามารถในการโจมตีของเพกาซัส มีความก้าวหน้ามากขึ้น โดยเพกาซัสสามารถเจาะเข้าอุปกรณ์ต่าง ๆ ได้ผ่านการโจมตีที่เรียกว่า “Zero-Click” ซึ่งหมายความว่า แม้ไม่คลิกลิงก์หรือตอบโต้ข้อความที่น่าจะเป็นไวรัส อุปกรณ์ก็ยังถูกเพกาซัสบุกได้อยู่ดี โดยการใช้ประโยชน์จากช่องโหว่ (Vulnerability) ที่มีอยู่ในซอฟแวร์หรือระบบปฏิบัติการซึ่งไม่มีใครทราบและไม่สามารถแก้ไขได้

ในปี 2019 WhatsApp เปิดเผยว่าซอฟต์แวร์เพกาซัสของ NSO ถูกใช้กับโทรศัพท์มากกว่า 1,400 เครื่อง เพียงแค่โทรผ่านไปยังอุปกรณ์เป้าหมาย เพกาซัสก็สามารถติดตั้งตัวเองบนโทรศัพท์ได้ แม้ว่าเป้าหมายจะไม่รับสายก็ตาม

ไม่นานมานี้ NSO ได้เริ่มใช้ประโยชน์จากช่องโหว่ในซอฟต์แวร์ iMessage ของ Apple ทำให้สามารถเข้าถึง iPhone หลายร้อยล้านเครื่องอย่างลับ ๆ ได้ Apple กล่าวว่า กำลังอัปเดตซอฟต์แวร์อย่างต่อเนื่องเพื่อป้องกันการโจมตีดังกล่าว

สปายแวร์โจมตีผู้ใช้แมคฯที่ชอบของฟรี

เตือน!!! ผู้ใช้แมคฯที่ชอบดาวน์โหลดซอฟต์แวร์ฟรีอย่างเช่น สกรีนเซฟเวอร์ (screensaver) หรือโปรแกรมแปลงฟอร์แมตวิดีโอ (video converter) จากเว็บไซต์ดังๆ เพราะคุณอาจจะได้ติดตั้งสปายแวร์เข้าไปในเครื่องเรียบร้อยแล้ว ซึ่งผลร้ายที่จะเกิดขึ้นตามมาคือ เครื่องแมคฯของคุณจะไม่ปลอดภัย เนื่องจากโปรแกรม back door ที่แอบเปิดช่องสื่อสาร (8254) เพื่อขโมยข้อมูลส่งให้กับผู้ไม่หวังดีที่อยู่บนเน็ต

Intego บริษัทผู้เชี่ยวชาญระบบรักษาความปลอดภัยกล่าวว่า สปายแวร์ทีกำลังแพร่กระจายในหมู่ผู้ใช้แมคฯอยู่ในขณะนี้พบนี้ชื่อว่า OSX/OpinionSpy ซึ่งมันได้รับการติดตั้งเข้าไปในระบบของผู้ใช้ที่ตกเป็นเหยื่อทีดาวน์โหลด สกรีนเซฟเวอร์ (มีอยู่ประมาณ 30 ตัวที่มีสปายแวร์) ที่พัฒนาโดยบริษัท 7art นอกจากนี้ยังมีแอพพลิเคชันแปลงไฟล์วิดีโอที่ชื่อ MishInc FLV to MP3 ที่มีสปายแวร์แฝงอยู่ด้วย โดยรายชื่อของเว็บไซต์ที่ให้บริการดาวน์โหลดซอฟต์แวร์อันตรายได้ ถูกรวบรวมโดยบริษัท Intego แล้ว ทั้งนี้ซอฟต์แวร์แมคฯที่ติดสปายแวร์นั้นจะพบได้บนเว็บไซต์ดาวน์โหลดชั้นนำ อย่างเช่น Softpedia, MacUpdate และ VersionTracker ของ CNET

เนื่องจากเราได้พบข่าวที่รัฐบาลหลายประเทศใช้เพกาซัส แอบสอดส่องและขโมยข้อมูลจากโทรศัพท์มือถือของบุคคลจากหลายประเทศทั่วโลก และ ข่าวที่สปายแวร์โจมตีผู้ที่โหลดโปรแกรมสกรีนเซฟเวอร์ (screensaver) หรือโปรแกรมแปลงฟอร์แมตวิดีโอ (video converter) ซึ่งผลร้ายที่จะเกิดขึ้นตามมาคือเครื่องแมคฯของคุณจะไม่ปลอดภัย เนื่องจากโปรแกรม back door ที่แอบเปิดช่องสื่อสารเพื่อขโมยข้อมูลส่งให้กับผู้ไม่หวังดีที่อยู่บนเน็ต

5. วัตถุประสงค์ของโครงงาน

5.1 เพื่อศึกษาหลักการทำงานของ spyware ว่ามีหลักการทำงานมีกี่ประเภท

5.2 เพื่อออกแบบกระบวนการการกำจัดและป้องกัน spyware

6. ขอบเขตของโครงงาน

6.1 เพื่อศึกษาและหาวิธีป้องกัน spyware ไม่ให้ spyware สามารถเข้ามาในเครื่องเราได้

6.2 เพื่อออกแบบกระบวนการป้องกันการโจมตีของ spyware

7. ผลลัพธ์ของโครงงาน

7.1 สามารถกำจัดและป้องกัน spyware ได้

7.2 เพื่อเป็นการศึกษากระบวนการทำงานของ spyware และวิธีป้องการป้องกันการโดนโจมตีของ spyware

8. แผนการดำเนินงาน

กิจกรรม	สัปดาห์ที่											
	1	2	3	4	5	6	7	8	9	10	11	12
1. ค้นหาปัญหา	●											
2. กำหนดวัถตุประสงค์และข้อมูลต่างๆภายในโครงการ		●	●									
3. ศึกษาการทำงานของ spyware				●	●							
4. ออกแบบการป้องกันและกำจัด spyware						●	●	●	●			
5. วิเคราะห์และประเมินผลของกระบวนการที่ออกแบบ										●		
6. สรุปผลทุกหัวข้อของโครงงาน											●	
7. ปิดโครงงาน												●

9. ประโยชน์ของโครงงาน

9.1 ทำให้เครื่องคอมพิวเตอร์ของเราไม่มี spyware ที่คอยสอดส่องและส่งโฆษณามาให้เรากวนใจ

9.2 ทำให้สามารถป้องกันการเชื่อต่อฮาร์ดแวร์ และเครือข่ายของคุณช้าลง โดยการลักลอบเปลี่ยนการตั่งค่าซอฟแวร์ และเว็บบราวเวอร์ของคุณ สำหรับ spyware บางชนิด

9.3 ทำให้สามารถป้องกันการปิดช่องโหว่ บนบราวเซอร์ของระบบไม่ให้ spyware เข้ามาสอดส่องหรือทำการเติมข้อมูลอัตโนมัติ

2. ศึกษาการทำงานของสปายแวร์

สปายแวร์คืออะไร (Spyware)

คำจำกัดความโดยทั่วไปของสปายแวร์สามารถอธิบายอย่างง่ายๆ คือ สปายแวร์จะทำหน้าที่เหมือนสายลับในภาพยนตร์ที่คุณเคยดู แต่แทนที่จะบุกเข้าไปในอาคาร และติดตั้งสายดักฟัง พวกมันจะเจาะเข้าไปในคอมพิวเตอร์ หรืออุปกรณ์มือถือของคุณ กล่าวอีกนัยหนึ่งก็คือสปายแวร์เป็นหนึ่งในประเภทของมัลแวร์นั่นเอง

สปายแวร์ ก็คือ โปรแกรมเล็ก ๆ ที่ถูกเขียนขึ้นมาสอดส่อง (สปาย) การใช้งานเครื่องคอมพิวเตอร์ของคุณ อาจจะเพื่อโฆษณาสินค้าต่าง ๆ สปายแวร์บางตัวก็สร้างความรำคาญเพราะจะเปิดหน้าต่างโฆษณาบ่อย ๆ แต่บางตัวร้ายกว่านั้น คือ ทำให้คุณใช้อินเตอร์เน็ตไม่ได้เลย ไม่ว่าจะไปเว็บหน ก็จะโชว์หน้าต่างโฆษณา หรืออาจจะเป็นเว็บประเภทลามกอนาจาร พร้อมกับป๊อปอัพหน้าต่างเป็นสิบ ๆ หน้าต่าง

สปายแวร์ทำงานอย่างไร?

วิธีการทำงานของสปายแวร์นั้น สามารถอธิบายได้ง่ายที่สุดจากตัวอย่างของระบบปฏิบัติการ Windows ซึ่งมีหลายส่วน (สาขา) ในรีจิสทรีของ Windows (นั่นคือฐานข้อมูลสำหรับการกำหนดค่า) ที่มีข้อมูลเกี่ยวกับโปรไฟล์ผู้ใช้แอปพลิเคชันที่ติดตั้งคุณสมบัติโฟลเดอร์ ไอคอน ข้อมูลฮาร์ดแวร์ และพอร์ตที่ใช้ ในทางกลับกันสาขาเหล่านี้จะถูกแบ่งออกเป็นคีย์ย่อยๆ และค่าในรีจิสทรีด้วยชุดไฟล์สนับสนุน การแก้ไขค่าคีย์เหล่านี้โดยสปายแวร์จะช่วยให้สปายแวร์เริ่มทำงานโดยอัตโนมัติ และเมื่อระบบเริ่มทำงาน นี่คือด่านแรกที่ช่วยให้สปายแวร์หลบหนีจากโปรแกรมที่พยายามลบพวกมันออกไป

สปายแวร์มักจะเชื่อมต่อกับตำแหน่งในรีจิสทรีที่อนุญาตให้ทำงานได้ สปายแวร์มีความฉลาดที่จะตรวจสอบความเสียหายของลิงก์ได้เองเป็นระยะๆ หากพบ “ช่องโหว่” มันจะทำการเติมข้อมูลโดยอัตโนมัติ นั่นเป็นเหตุผลว่าทำไมจึงค่อนข้างยากที่จะต่อสู้กับสปายแวร์ แม้ว่าการเชื่อมต่อบางส่วน หรือแม้กระทั่งส่วนใหญ่จะถูกลบออกไป แต่สปายแวร์ก็ยังคงเริ่มทำงานอยู่เสมอ เมื่อระบบปฏิบัติการได้เริ่มทำงานนั่นเอง

สปายแวร์มักจะใช้ประโยชน์อย่างเต็มที่จากความไม่รู้ของผู้ใช้งานเอง และมักจะเป็นข้อสันนิษฐานที่ไม่เหมาะสมของผู้พัฒนาระบบปฏิบัติการ และส่วนเสริมต่าง ๆ โปรแกรมสปายแวร์จำนวนมากใช้ช่องโหว่ในเบราว์เซอร์บนระบบ และใช้ประโยชน์ (ช่องโหว่) ใน JavaScript เพื่อเข้าถึงข้อมูลโดยไม่ได้รับความยินยอมและความรู้จากผู้ใช้งาน

1.ประเภทของสปายแวร์

สปายแวร์สามารถแบ่งออกเป็น 4 กลุ่มหลัก ได้แก่ แอดแวร์ (ซอฟต์แวร์โฆษณา) คุกกี้ โทรจัน และระบบเฝ้าระวัง เราสามารถเพิ่มประเภทอื่นๆในกลุ่มเหล่านี้ได้ ส่วนใหญ่เราจะพบสปายแวร์ได้ในกลุ่มเหล่านี้

สปายแวร์และโปรแกรมแอนตี้สปายแวร์แตกต่างกันอย่างไร?

ในขณะที่สปายแวร์พยายามขโมยข้อมูลส่วนตัวของคุณและตรวจสอบกิจกรรมของคุณ โปรแกรมป้องกันสปายแวร์จะป้องกันไม่ให้สปายแวร์ทำเช่นนั้นได้ การป้องกันสปายแวร์ไม่เพียงแต่ป้องกันผลกระทบที่เป็นอันตรายของสปายแวร์เท่านั้น แต่ยังตรวจจับและลบออกจากระบบได้อีกด้วย แล้วโปรแกรมป้องกันสปายแวร์เหมือนกับโปรแกรมป้องกันไวรัสหรือไม่?

ซอฟต์แวร์ป้องกันสปายแวร์ตอนแรกมีอยู่เป็นแอปพลิเคชันแยกต่างหาก หลังจากนั้นมุ่งเน้นไปที่โปรแกรมที่เป็นอันตรายประเภทอื่น ๆ อย่างไรก็ตามมีการสันนิษฐานว่าเราใช้คำว่าแอนติไวรัสต่อสู้กับมัลแวร์ทุกรูปแบบ ดังนั้นโปรแกรมป้องกันสปายแวร์จึงมักรวมอยู่ในโปรแกรมป้องกันไวรัสยอดนิยมอย่างเช่น Bitdefender Antivirus เพื่อให้แน่ใจว่าการติดตั้งโปรแกรมป้องกันไวรัส จะปกป้องคุณจากการโจมตีของสปายแวร์ ตรวจสอบว่าโปรแกรมป้องกันไวรัสที่คุณเลือกนั้น มีคุณสมบัติป้องกันสปายแวร์ที่ทำงานแบบเรียลไทม์หรือไม่ น่าเสียดายที่โปรแกรมป้องกันไวรัสจำนวนมากโดยเฉพาะรุ่นพื้นฐานที่สุด มักไม่มีโมดูลดังกล่าว

Mac สามารถติดสปายแวร์ได้หรือไม่?

เมื่อความนิยมของระบบ Mac เพิ่มขึ้น ความสนใจของอาชญากรไซเบอร์ในทรัพยากรที่รวบรวมโดยผู้ใช้ฮาร์ดแวร์ของ Apple ก็เพิ่มขึ้น ตามมาด้วยสปายแวร์ โดยเฉพาะอย่างยิ่งตั้งแต่ปี 2017 พบว่ามีจำนวนการโจมตีเพิ่มขึ้นบนระบบ Mac ปกติวิธีการและอาการติดสปายแวร์จะคล้ายคลึงกับที่ระบบ Windows อย่างไรก็ตามสำหรับ Mac แฮกเกอร์มักใช้การขโมยรหัสผ่านเป็นหลัก หรือใช้รหัสผ่านรีดไถผ่านแป็คดอร์ (ช่องโหว่) ถ่ายภาพหน้าจอ สกัดกั้น และถ่ายโอนไฟล์ หรือบันทึกการกดแป้นพิมพ์

นอกจากนี้ยังมีสปายแวร์ที่ถูกต้องบน Mac ของคุณที่ผู้ใช้งานแทบทุกคนสามารถซื้อ และหาดาวน์โหลดได้ มีวิธีที่ผู้ปกครองใช้ความสามารถของแอปในการตรวจสอบบุตรหลาน หรือวิธีที่เป็นที่นิยมในการตรวจสอบการทำงานของพนักงาน

อุปกรณ์เคลื่อนที่และสปายแวร์

เช่นเดียวกับ Macs เป็นอุปกรณ์พกพาที่ได้รับความนิยมเพิ่มมากขึ้น มีการขยายการใช้สปายแวร์ สปายแวร์ทำงานได้อย่างกว้างขวางตั้งแต่การขโมยข้อความ รายการโทร รายชื่อติดต่อ รูปภาพ อีเมล และประวัติของเบราว์เซอร์ที่ใช้งาน นอกจากนี้สปายแวร์ในสมาร์ทโฟนของคุณ ยังสามารถใช้ไมโครโฟนกล้องแป้นพิมพ์ (แม้กระทั่งสัมผัสนี้!) และเครื่องส่งสัญญาณ GPS มีซอฟต์แวร์ทำงานอยู่เบื้องหลังโดยไม่ต้องสร้างไอคอนหรือทางลัดใด ๆ โดยส่วนใหญ่มักจะส่งข้อมูลที่ได้มาทางอีเมล หรือส่งไปยังเซิร์ฟเวอร์ระยะไกล

แฮกเกอร์โจมตีทั้งผู้บริโภคทั่วไป และองค์กรขนาดใหญ่ที่ใช้สมาร์ทโฟนและแท็บเล็ตในที่ทำงาน แม้แต่ทีมไอทีที่เชี่ยวชาญอาจมีปัญหาในการตรวจจับสปายแวร์บนอุปกรณ์มือถือ แล้วแฮกเกอร์เข้าสู่อุปกรณ์มือถือของคุณได้อย่างไร?

1. การทำงานของ Adware

แอดแวร์คือแอปพลิเคชั่นซอฟต์แวร์ใด ๆ ที่มีการแสดงแบนเนอร์โฆษณา ขณะที่โปรแกรมกำลังทำงาน ผู้เขียนแอปพลิเคชันเหล่านี้ มีรหัสเพิ่มเติมที่จะแสดงโฆษณา ซึ่งสามารถดูได้ผ่านหน้าต่างป๊อปอัพ หรือผ่านแถบที่ปรากฏบนหน้าจอคอมพิวเตอร์ แอดแวร์สร้างรายได้ให้กับผู้พัฒนา จากสร้างโฆษณาออนไลน์โดยอัตโนมัติ ในส่วนต่อประสานผู้ใช้งานของซอฟต์แวร์ หรือบนหน้าจอที่แสดงต่อผู้ใช้งาน ระหว่างกระบวนการติดตั้ง

2. การทำงานของ Dialer

Dialer คือ แอพพลิเคชั่นที่ทำงานโดยการสั่งให้โมเด็ม ตัดการเชื่อมต่อจากผู้ให้บริการอินเตอร์เน็ตโดยหมุนหมายเลขไปยังผู้ให้บริการในต่างประเทศ ทำให้มีค่าโทร์สักท์ที่สูงขึ้น แต่ในปัจจุบันปัญหาเกี่ยวกับ Dialer ได้ลดจำนวนจนแทบไม่พบแล้ว

3. การทำงานของ Hijacker

Browser Hijacker เกิดมาจาก malware หรือ spyware ได้ทำการเปลี่ยน Start page , Error page หรือ Search page ที่มีอยู่ให้เปลี่ยนไปจากเดิม ด้วยวิธีการต่างๆที่เจ้าของไม่ยินยอม

Session Hijacking คือ การขโมย เซสชั่น จากผู้ใช้ มาใช้งานซึ่ง hacker จะมีสิทธิเท่ากับเจ้าของเดิมเลย หาก session admin โดนขโมยไปก็เท่ากับว่า เว็บตกไปเป็นของ hacker แล้ว

4. การทำงานของ BHO (Browser Helper Object)

BHO (Browser Helper Object) เป็นสปายแวร์ที่ยัดเยียดฟังก์ชั่นที่ไม่พึงประสงค์ให้บนเว็บบราวเซอร์ Toolbar บางอย่างก็จัดเป็นสปายแวร์ที่ยัดเยียดเครื่องมือที่ไม่พึงประสงค์ให้บนเว็บบราวเซอร์ด้วย

5. สาเหตุที่คอมพิวเตอร์ของคุณติดสปายแวร์

คอมพิวเตอร์ของคุณสามารถติดสปายแวร์ได้จากหลายๆ ช่องทาง อย่างไรก็ตามแหล่งที่ติดไวรัสมากที่สุดคือโปรแกรมที่มีไวรัสแอบแฝงมาด้วย โดยปกติแล้วโปรแกรมจะติดตั้งตัวเองอย่างเงียบๆ ควบคู่กับโปรแกรม (ที่ปกติแล้วน่าเชื่อถือ) ที่คุณเลือกดาวน์โหลด

เราทุกคนต่างมีความผิดในการดาวน์โหลดเกมหรือแอปฟรีให้ทำงานเล็ก ๆ น้อยๆ ทางออนไลน์ให้กับเรา แต่หากสิ่งเหล่านี้ไม่ได้รับการตรวจสอบอน่างเหมาะสม มันก็อาจเป็นสาเหตุของการติดไวรัสได้

ช่องทางอื่นๆ ที่จะสัมผัสกับสปายแวร์ได้ยังมี:

- การคลิกโฆษณาหรือป๊อปอัพที่ติดไวรัส
- การเยี่ยมชมเว็บไซต์หรือโดเมนที่ติดไวรัส
- การดาวน์โหลดซอฟต์แวร์จากแหล่งข้อมูลที่ไม่น่าเชื่อถือ
- การเปิดเอกสารแนบอีเมลจากผู้ส่งที่ไม่รู้จัก
- การดาวน์โหลดมีเดียจากทอร์เรนต์

6. วิธีป้องกันไม่ให้เครื่องคอมพิวเตอร์ติดสปายร์แวร์

1. ใช้ชุดความปลอดภัยแอนตี้ไวรัสที่มีเครื่องมือแอนตี้สปายแวร์
2. อย่าคลิกโฆษณาไม่พึงประสงค์
3. อ่านรีวิวก่อนดาวน์โหลดซอฟต์แวร์
4. ปรับแต่งความปลอดภัยเบราว์เซอร์ของคุณ
5. หลีกเลี่ยงการคลิกป๊อปอัพโดยบังเอิญเมื่อปิดมัน
6. ใช้ไฟวอล
7. ให้ความรู้กับครอบครัวของคุณเกี่ยวกับความเสี่ยง

7. ข้อดีและข้อเสียของแต่ละโปรแกรม Anti Spyware ที่ติดท็อป 4

1. Bitdefender Antivirus

ข้อดี

- ติดตั้งง่าย ป้องกันไวรัสทุกสายพันธ์รวมถึง Spyware ด้วย
- มีการอัพเดทความเคลื่อนไหวของ Antivirus ใหม่อยู่เสมอ
- สแกนหาและลบไวรัสและรวมถึง spyware ได้
- สามารถหาและลบไฟล์ที่ไม่จำเป็นสำหรับเครื่องได้

ข้อเสีย

- ความต้องการใช้ทรัพยากรภายในเครื่องเยอะ
- สามารถใช้ได้แค่กับคอมพิวเตอร์ส่วนตัวเท่านั้น ไม่สามารถนำมาใช้ในระบบขององค์กรได้
- ไม่สามารถสแกนเครื่องแบบเจาะจงหรือกำหนดเองได้
- ไม่เหมาะกับคอมพิวเตอร์เก่าที่สเปคไม่ถึงและไม่เหมาะกับความเร็วกินเทอร์เน็ตที่ช้า

ข้อมูลเพิ่มเติม

- สามารถลงได้กับระบบปฏิบัติการ Window ทุกรุ่นและสำหรับ MacOS กับ Android สามารถติดตั้งได้ฟรี
- ซอฟแวร์นี้มีตัวสแกนที่สามารถสแกนลิงค์เพื่อดูว่าเว็ปนี้เรากำลังทำธุรกรรมทางการเงินอยู่นี้เป็นเว็ปที่พยายามจะฟิชชิ่งบัตรเกครดิทของเราหรือไม่

2. TotalAV Antivirus

ข้อดี

- สามารถสแกนทั้งโปรแกรมและเว็ปไซต์ภายในเครื่องว่าสามารถที่จะสร้างอันตรายให้กับคอมพิวเตอร์ของคุณได้หรือไม่
- สามารถสแกนได้อย่างละเอียดและสามารถกำจัด Spyware และมัลแวร์อื่นๆภายในเครื่องได้อย่างมีประสิทธิภาพ
- ระบบยังสามารถเปิดเครื่องมีเพื่อปิดกันโฆษณาและเครื่องมือสำหรับตรวจจับการรั่วไหลของข้อมูล
- สามารถใช้ VPN เพื่อเข้าเว็ปไซต์ในโหมดไม่ระบุตัวตนได้และมีเครื่องมือในการรักษาความปลอดภัยของคุณจากการขโมยข้อมูล

- มีระบบการสแกนแบบรวดเร็วภายในเวลาไม่เกิน 15 นาที

ข้อเสีย

- มีระบบในการสแกนอย่างรวดเร็วเพียงแค่ 15 นาทีก็สามารถสแกนเครื่องคล้าวๆได้ นั้นทำให้ไม่มีความระเอียดในการค้นหาไฟล์ต่างๆภายในเครื่อง
- ในขณะที่ทำการสแกนเครื่องอยู่นั้นจะมีโฆษณาต่างๆข้องตัวโปรแกรมโผล่ขึ้นมาสิ่งนั้นทำให้ผู้ใช้งานนั้นลำคาญได้
- โปรแกรมนี้จะทำการเปิดใช้งานเองโดยอัตโนมัติทำให้เวลาบูสเครื่องคอมพิวเตอร์ก็จะช้าลง

3. McAfee Antivirus

ข้อดี

- สามารถตรวจจับและปิดกั้น Spyware และมัลแวร์ตัวอื่นๆได้ 100%
- ใช้เวลาในการตรวจาสอบรายการมากกว่า 10,200 รายการโดบใช้เวลาน้อยกว่า 5 นาที
- เมื่อพบไฟล์ที่น่าสงสัยจะทำการส่งไฟล์ดังกล่าวไปยังพื้นที่กักกันโดยอัตโนมัติ
- ปิดกั้นการพยายามฝัง Spyware หรือมัลแวร์ต่างๆลงบนอุปกรณ์เพื่อขุดเหรียญโดยอัตโนมัติได้
- มีการป้องกันการเชื่อมต่อทั้วหมดรวมถึง VPN

ข้อเสีย

- ตัวโปรแกรมไม่ได้มีฟีเจอร์ที่โดดเด่นมากมายเท่ากับ Antivirus ตัวอื่นๆ
- มี UI ที่ซับซอนกว่า Antivirus ตัวอื่นๆ
- ตัวโปรแกรมทำงานได้เป็นอย่างดี แต่ยังไม่สมบูรณ์แบบกับเครื่องมือ WebAdvisor และฟีเจอร์เพิ่มประสิทธิภาพนั้นค่อนข้างน่าผิดหวัง

4. Norton Antivirus

ข้อดี

- สามารถใช้ได้กับระบบปฏิบัติการทุกรูปแบบ เช่น Window, MacOS และ Android
- สามารถป้องกัน Spyware และมัลแวร์ที่จะทำการโจมตีทางอินเทอร์เน็ตอื่นๆ
- หน้าตาสีสันสวยงาม
- มีการ Insight ตรวจสอบไฟล์อยู่เรื่อยๆ
- มีระบบ Cloud ซึ่งสามารถเก็บไฟล์ต่างๆมีขนาดถึง 25GB
- บล็อคเว็ปไซต์ที่ไม่ปลอดภัยและป้องกันการดาวน์โหลดที่น่าสงสัย

ข้อเสีย

- เนื่องจากโปรมแกรมสามารถทำหน้าได้หลากหลายจึงทำให้การใช้พื้นที่ภายในเครื่องเยอะ
- มีป็อปอัพที่เป็นโฆษณาหรือป็อปอัพที่ไม่พึงประสงค์เยอะจนน่ารำคาญ
- ถอนการติดตั้งยาก
- ตัวโปรแกรมราคาแพง

สรุป

จากการสำรวจตัวโปรแกรม Antivirus ทั้ง 4 ตัวเพื่อการนำไปปรับแก้ไขให้เป็นรูปแบบของเราเอง สรุปได้ว่าทุกตัวสามารถกำจัด Spyware ได้ทั้งหมดและยังรวมไปถึงการกำจัดมัลแวร์ตัวอื่นๆ และในบางโปรมแกรมยังสามารถตรวจสอบเว็ปไซต์ที่ผู้ใช้งานเข้าไปดูว่าเว็ปไซต์นั้นปลอดภัยหรือไม่ หรือเว็ปไซต์นั้นมีตัว Spyware หรือมัลแวร์ตัวอื่นๆอยู่หน้าเว็ปไซต์นั้นหรือไม่และยังสามารถป้องกันการดาวน์โหลดที่อาจจะทำให้เกิดอันตรายต่อเครื่องได้

ผลสรุปข้างต้นในการตรวจสอบและทำการออกแบบรูปแบบการป้องกันและกำจัด Spyware ไปจากเครื่องคอมพิวเตอร์นั้น เราจะนำข้อดีต่างๆของแต่ละโปรแกรมนำมาประยุคให้เข้ากับรูปแบบที่เราต้องการจะสร้าง

3. ออกแบบการป้องกันและกำจัด spyware

1. แนวทางการทำงานของโปรแกรม

โปรมแกรมของเราจะสามารถทำการกำจัด Spyware และ Malware ตัวอื่นๆได้เพราะนอกจาก Spyware แล้ว Malware ตัวอื่นๆ ก็เป็นภัยกับเครื่องคอมพิวเตอร์เช่นกัน จึงท าให้กลุ่มเราเลือกที่จะท าให้โปรแกรมชองเราท าได้ นอกเหนือจากแค่จัดการกับ Spyware

รูปแบบของโปรแกรมที่นำมาใช้

รูปแบบของโปรแกรมที่นำมาใช้ได้แก่ระบบการประมวนผลแบบ Cloud Computing หรือก็คือการที่ให้ติดตั้ง โปรแกรมส่วนเล็กๆ ไว้ภายในเครื่องคอมพิวเตอร์ของแล้วก็ใช้ Cloud มาเป็นตัวช่วยประมวลผลว่าไฟล์ไหนบ้างในเครื่อง ของเรานั้นเป็น Spyware หรือ Malware บ้าง

เหตุผลที่เลือก Cloud เพราะว่า

1. ตัวโปรแกรมนั้นจะได้มีขนาดเล็กและไม่เปลืองพื้นที่
2. ลดการใช้ทรัพยากรณ์ของเครื่องคอมพิวเตอร์
3. สามารถอัพเดทได้อย่างรวดเร็ว

ขั้นตอนการทำงานของโปรแกรม

1. Scanning

– จะทำการเข้าไปค้นหาไฟล์ที่ถูกบ่งบอกว่าถูกไวรัสแฝงตัวอยู่ในหน่วยความจำ

- จะมีการดึงเอาโปรแกรมบางส่วนของตัวไวรัสมาเก็บไว้เป็นฐานข้อมูล

- ใช้หลังการ checksum – ถ้าไฟล์ถูกไวรัสแฝงตัวจะทำให้ค่า Checksum ที่คำนวณได้จะไม่เท่ากับค่า Checksum ที่เป็นข้อมูลของ ไฟล์ดังกล่าว

2. Integrity Checking

- จะตรวจสอบความคงอยู่ (Integrity Checker) ที่เก็บข้อมูลความคงอยู่ (Integrity Information) - เอาข้อมูลไฟล์ไว้เพื่อเปรียบเทียบ.

- ตัวอย่างข้อมูลไฟล์ที่ใช้เช่น ขนาดไฟล์ เวลาแก้ไขครั้งล่าสุด และค่า Checksum - ถ้าพบไฟล์มีการเปลี่ยนแปลงที่มีสาเหตุจากไวรัส ระบบจะแจ้งให้ผู้ใช้งานทราบถึงความผิดปกติ

- ผู้ใช้งานสามารถกู้ไฟล์ข้อมูลดังกล่าวคืนไปเป็นไฟล์ก่อนที่จะติดไวรัสได้

3. Heuristic

- เปรียบเทียบการทำงานของไวรัสกับกฎ Heuristic

- ชุดกฎ Heuristic ถูกพัฒนาให้สามารถแยกแยะพฤติกรรมการทำงานว่าเป็นการทำงานของไวรัสหรือไม่

- มีการเก็บข้อมูลของไวรัสที่รู้จักเพื่อใช้ในการจับคู่แพตเทิร์น

- สามารถระบุว่าเป็นพฤติกรรมการทำงานของไวรัสชนิดใด

4. Interception

- โปรแกรมป้องกันไวรัสจะสร้าง virtual machine ที่มีความอ่อนแอไว้ภายในเครื่อง
- ทำหน้าที่คอยล่อให้โปรแกรมประเภทไวรัสโจมตีและมีหน้าที่เฝ้าดูว่ามีไวรัสหรือโปรแกรมใดบ้างที่มีพฤติกรรมผิดปกติน่าสงสัยเข้ามาทำงานใน virtual machine

2. Checksum

Checksums ใช้เพื่อรับรองความถูกต้องของไฟล์หลังจากส่งจากอุปกรณ์เก็บข้อมูลหนึ่งไปยังอุปกรณ์อื่น สิ่งนี้สามารถผ่านอินเทอร์เน็ตหรือระหว่างคอมพิวเตอร์สองเครื่องบนเครือข่ายเดียวกัน ไม่ว่าจะด้วยวิธีใดหากคุณต้องการให้แน่ใจว่าไฟล์ที่ส่งนั้นเหมือนกับไฟล์ต้นฉบับคุณสามารถใช้ checksum.

การตรวจสอบจะคำนวณโดยใช้ฟังก์ชั่นแฮชและโดยปกติจะโพสต์พร้อมกับการดาวน์โหลด ในการตรวจสอบความสมบูรณ์ของไฟล์ผู้ใช้จะทำการคำนวณ checksum โดยใช้โปรแกรม checksum calculator และเปรียบเทียบทั้งสองส่วนเพื่อให้แน่ใจว่าตรงกัน เช็คซัมใช้ให้แน่ใจว่าไฟล์ไม่ถูกดัดแปลง เมื่อใช้อัลกอริทึมการตรวจสอบแม้จะเปลี่ยนแปลงเล็กน้อย

เช็คซัมที่พบมากที่สุดคือ MD5 และ SHA-1.

ความแตกต่างระหว่างผลรวม MD5, SHA-1 และ SHA-256

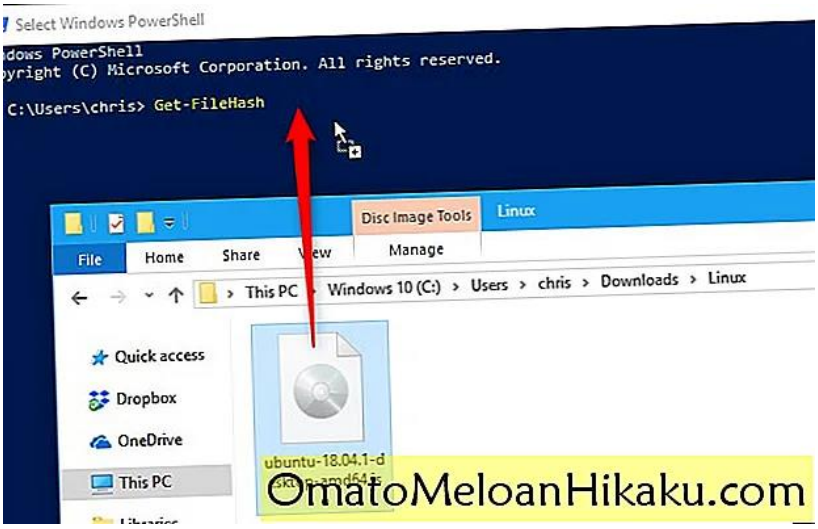
ฟังก์ชัน MD5 และ SHA-1 กล่าวอีกนัยหนึ่งก็คือพวกเขาพบไฟล์ 2 ไฟล์ที่สร้างแฮช MD5 หรือ SHA-1 เหมือนกัน แต่ต่างกัน สิ่งนี้ไม่น่าจะเกิดขึ้นโดยบังเอิญ แต่ผู้โจมตีสามารถใช้เทคนิคนี้เพื่อปลอมไฟล์ที่เป็นอันตรายให้เป็นไฟล์ที่ถูกต้อง นั่นคือเหตุผลที่คุณไม่ควรใช้ผลรวม MD5 หรือ SHA-1 ในการตรวจสอบว่าไฟล์เป็นของจริงเพียงเพื่อตรวจสอบความเสียหาย ยังไม่มีรายงานใด ๆ เกี่ยวกับการชนกันของ SHA-256 ซึ่งเป็นสาเหตุที่ตอนนี้แอปพลิเคชันสร้างผลรวม

วิธีการคำนวณ Checksums

หากคุณทราบการตรวจสอบของไฟล์ต้นฉบับและต้องการตรวจสอบในพีซีของคุณคุณสามารถทำได้อย่างง่ายดาย Windows, macOS และ Linux ล้วนมียูทิลิตี้ในตัวสำหรับสร้างเช็คซัม คุณไม่จำเป็นต้องมียูทิลิตี้ของบุคคลที่สาม บน Windows PowerShell’s คำสั่ง Get-FileHash จะคำนวณเช็คซัมของไฟล์ ในการใช้งานให้เปิด PowerShell ก่อน ใน Windows 10 ให้คลิกขวาที่ปุ่ม Start แล้วเลือก“ Windows PowerShell” คุณยังสามารถเปิดใช้งานได้โดยค้นหาเมนูเริ่มสำหรับ“ PowerShell” แล้วคลิกทางลัด“ Windows PowerShell”

ที่พรอมต์ให้พิมพ์ รับ FileHash แล้วกด Space Bar ของคุณ

พิมพ์เส้นทางของไฟล์ที่คุณต้องการคำนวณการตรวจสอบ หรือเพื่อให้ง่ายขึ้นให้ลากและวางไฟล์จากหน้าต่าง File Explorer ไปยังหน้าต่าง PowerShell เพื่อเติมเส้นทางโดยอัตโนมัติ



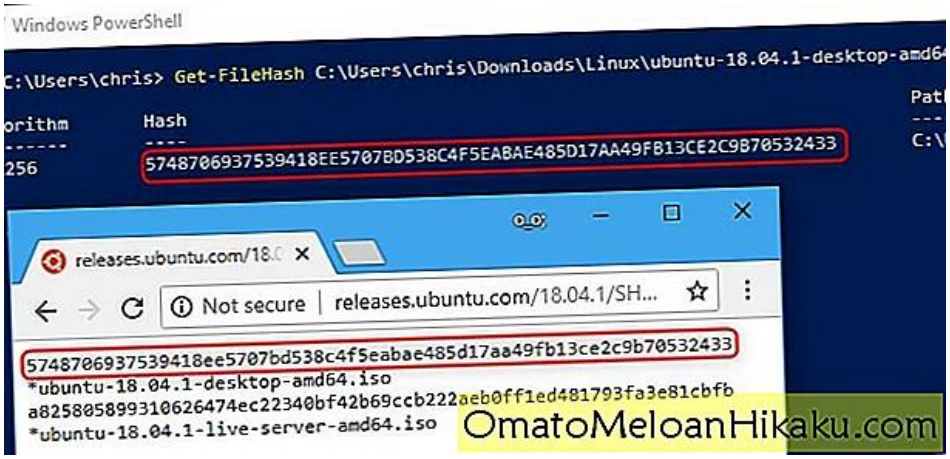
กด Enter เพื่อเรียกใช้คำสั่งและคุณจะเห็นแฮช SHA-256 สำหรับไฟล์ ขึ้นอยู่กับขนาดของไฟล์และความเร็วในการจัดเก็บข้อมูลในคอมพิวเตอร์ของคุณกระบวนการนี้อาจใช้เวลาสองสามวินาที

หากคุณต้องการการตรวจสอบประเภทอื่นให้เพิ่มที่เหมาะสม - ตัวเลือกอัลกอริทึมต่อท้ายคำสั่งดังนี้:

รับ FileHash C: path to file.iso -Algorithm MD5

รับ FileHash C: path to file.iso -Algorithm SHA1

เปรียบเทียบการตรวจสอบที่คำนวณได้กับรายการเดิม คุณไม่ควรมองใกล้เกินไปเนื่องจากจะมีความแตกต่างอย่างมากในการตรวจสอบแม้ว่าไฟล์พื้นฐานจะมีความแตกต่างกันเพียงเล็กน้อยก็ตาม

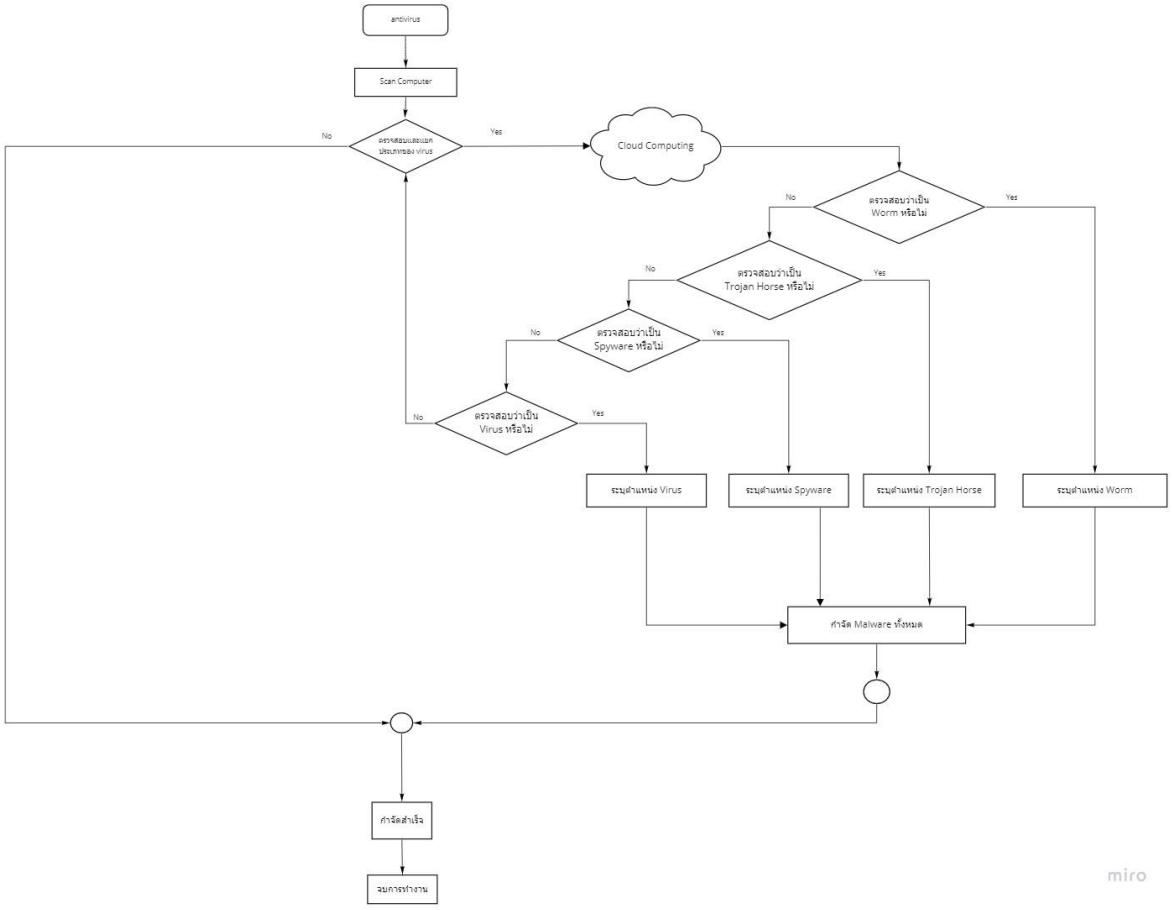


หากการตรวจสอบตรงกันไฟล์จะเหมือนกัน หากไม่เป็นเช่นนั้นอาจเกิดปัญหา - ไฟล์อาจเสียหายหรือคุณกำลังเปรียบเทียบไฟล์สองไฟล์ที่ต่างกัน หากคุณดาวน์โหลดสำเนาของไฟล์และการตรวจสอบไม่ตรงกับสิ่งที่คุณคาดหวังให้ลองดาวน์โหลดไฟล์อีกครั้ง

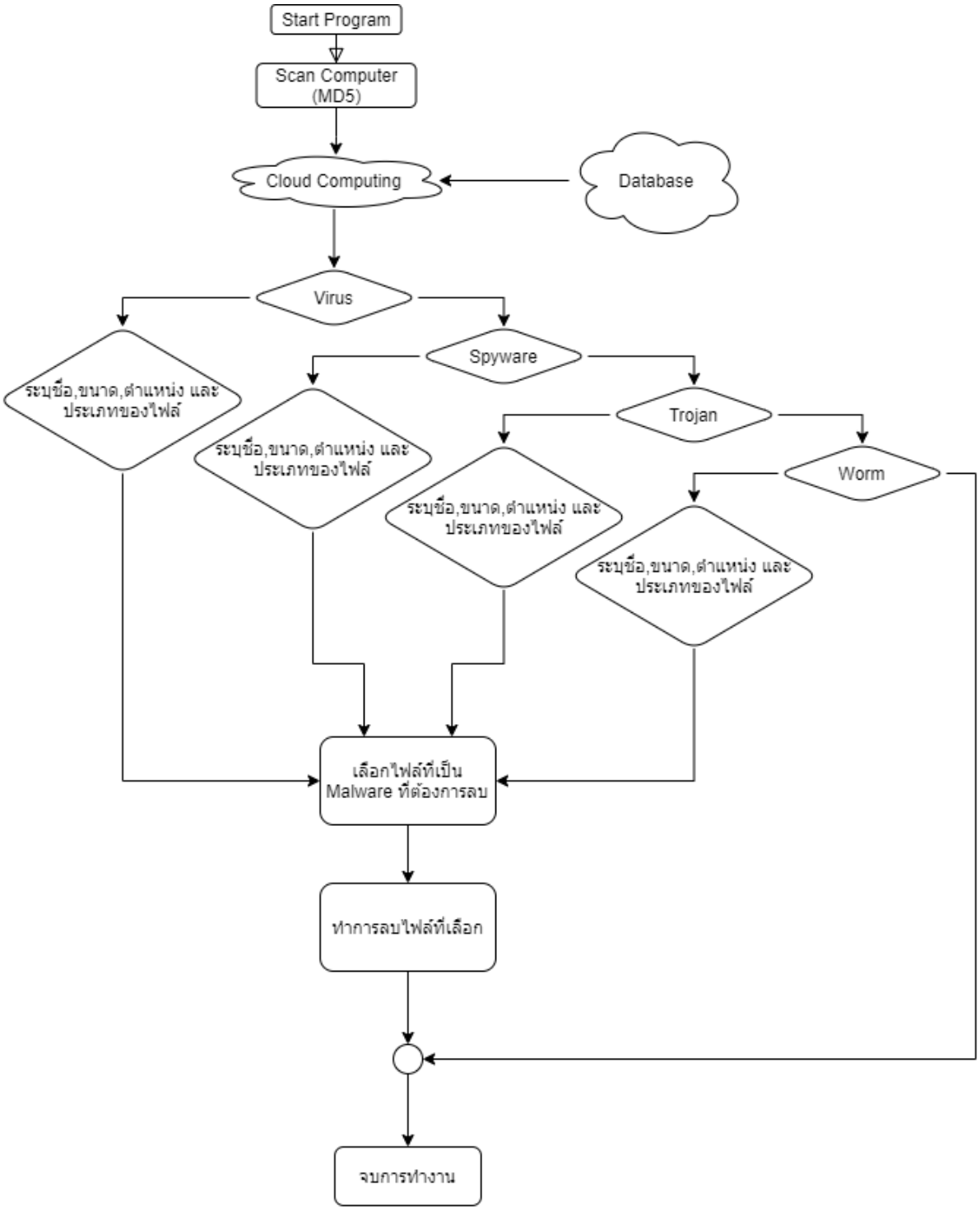
ตารางเปรียบเทียบระหว่างการใช้ Cloud Computing และ Edge Computing

Parameters	Cloud Computing	Edge Computing
Service location	Within the Internet	In the edge network
Distance (number of hops)	Multiple hops	Single hop
Latency	High	Low
Location awareness	No	Yes
Mobility support	Limited	Supported
Data em route attacks	High probability	Very low probability
Target user	General Internet users	Mobile users
Service scope	Globla	Limited
Hardware	Scalable capabilities	Limited capabilities

Flowchart การทำงานของระบบ Antivirus



Flowchart การทำงานของระบบ Antivirus



4. วิเคราะและประเมินผลของกระบวนการที่ออกแบบ

ข้อดี MD5

1. นำไปตรวจสอบความถูกต้องของไฟล์

2. นำไปใช้ในการเก็บข้อมูลที่ไม่ต้องการเปิดเผย เช่น เก็บรหัสผ่านไว้ในฐานข้อมูล|

3. PHP เก่าๆก็ใช้ได้

4. มีความเร็วกว่า SHA-1

ข้อดี SHA-1

1. มีความแข็งแรงกว่า MD5

2. ใช้เพื่อตรวจสอบว่า ไฟล์ไม่ ได้รับการเปลี่ยนแปลง โดยทำ checksum ก่อนที่ไฟล์จะถูกส่งและจากนั้นอีกครั้งเมื่อถึงปลายทาง

1. ตารางวิเคราะห์ข้อมูล

จากการออกแบบตัวโปรแกรมของเรานั้นโปรแกรมสามารถตรวจจับและจัดการกับ Spyware ได้เพราะใช้ MD5 เข้ามาช่วยในการตรวจจับการทำงานของ Spyware ทำให้สามารถตรวจจับได้เร็วมากยิ่งขึ้นอีกทั้งตัวโปรแกรมยังสามารถ ระบุข้อมูลข้อมูลของ spyware ได้ละเอียดอีกด้วย โดยระบบนี้สามารถกำจัด สปายแวร์ได้ แต่ยังไม่สามารถป้องกันได้

2. ตารางประเมินผล

หัวข้อ	เปอร์เซ็น (100%)	หมายเหตุ
1. สามารถ scan ไฟล์บน computer ได้ครบถ้วนกี่เปอร์เซ็น		
2. สามารถตรวจจับ malware ได้กี่เปอร์เซ็น		
3. สามารถระบุไฟล์ ประเภทไฟล์ได้กี่เปอร์เซ็น		
4. สามารถใช้ MD5 ในการอ้างอิงได้กี่เปอร์เซ็น		
5. สามารถลบ malware ออกจากเครื่องได้กี่เปอร์เซ็น		
6. สามารถเก็บข้อมูลไฟล์ส่วนตัวในฐานข้อมูลได้กี่เปอร์เซ็น		
7. ระบบมีประสิทธิภาพในการทำงานทั้งหมดกี่เปอร์เซ็น		