ระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach

Cybersecurity Threat Detection System in the form of Data Breach

ปณิธาน วสุวัต

บุญฑริกกา นิซัน

โครงงานวิจัยระดับปริญญาตรีนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตร์บัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ปีการศึกษา 2565

RMUTT-2021-SC-IT-002-XXX

ระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach

Cybersecurity Threat Detection System in the form of Data Breach

ปณิธาน วสุวัต

บุญฑริกกา นิซัน

โครงงานวิจัยระดับปริญญาตรีนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ปีการศึกษา 2565

RMUTT-2021-SC-IT-002-XXX

ใบรับรองโครงงานวิจัยระดับปริญญาตรี ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

หัวข้อโครงงานระดับปริญญาตรี	ระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach (Cybersecurity Threat Detection System in the form of Data Breach)
ชื่อนักศึกษา	**ปณิธาน วสุวัต** 116210906008-4 **บุญฑริกกา นิซัน** 116210906015-9
ปริญญา	วิทยาศาสตร์บัณฑิต (เทคโนโลยีสารสนเทศ)
อาจารย์ที่ปรึกษาโครงงาน	ดร. สันติ พัฒนะวิชัย

คณะกรรมการสอบโครงงานวิจัย	ลายมือชื่อ
อาจารย์ ดร. สันติ พัฒนะวิชัย	
อาจารย์ ผศ.ดร. อนุชา ตุงคัษฐาน	
อาจารย์ สุเทพ เชาว์สนิท	
อาจารย์ วุฒิพล วรรณทรัพย์	

วัน/เดือน/ปี ที่สอบ 9 เมษายน 2566
สถานที่สอบ ห้อง SC1XXX คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

สาขาวิชาเทคโนโลยีสารสนเทศ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

หัวข้อปริญญานิพนธ์	ระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach (Cybersecurity Threat Detection System in the form of Data Breach)
นักศึกษา	ปณิธาน วสุวัต 116210906003-5
	บุญฑริกกา นิซัน 116210906015-9
อาจารย์ที่ปรึกษาโครงงานวิจัย	ดร. สันติ พัฒนะวิชัย
ระดับการศึกษา	ปริญญาตรี
สาขาวิชา	เทคโนโลยีสารสนเทศ
ปีการศึกษา	2565

บทคัดย่อ

โครงงานวิจัยระดับปริญญาตรีเรื่อง ระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach (Cybersecurity Threat Detection System in the form of Data Breach) สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อพัฒนาระบบที่ใช้ในการตรวจจับ และไวรัสเรียกค่าไถ่ต่าง ๆ บนระบบปฏิบัติการ Windows และเพื่อเพิ่มระดับความปลอดภัยของระบบปฏิบัติการ Windows โดยการเขียนโปรแกรมสร้างโปรแกรมสแกนไวรัสขึ้นมา สามรถใช้งานได้โดยการเลือกโฟลเดอร์ที่ต้องการตรวจสอบ และตรวจสอบด้วยวิธีการ Signature Based ระบบจะแสดงผลการตรวจจับให้ทราบว่าไฟล์ใดในโฟลเดอร์ที่ตรวจสอบนั้นเป็นมัลแวร์เรียกค่าไถ่ และสามารถกำจัดไฟล์ที่เป็นไวรัสที่ตรวจเจอออกจากอุปกรณ์ได้ในทันที เป็นการยกระดับการรักษาความปลอดภัย

กิตติกรรมประกาศ

โครงงานวิจัยระดับปริญญาตรี เรื่องระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach (Cybersecurity Threat Detection System in the form of Data Breach) สำเร็จลุล่วงได้ด้วยความกรุณาของอาจารย์ที่ปรึกษาโครงงานวิจัย ดร.สันติ พัฒนะวิชัย รวมถึงอาจารย์ประจำสาขาวิชาเทคโนโลยีสารสนเทศทุกท่านที่ได้ให้คำปรึกษา แนะนำ และชี้แนะแนวทางในการศึกษาค้นคว้า ขั้นตอนและวิธีจัดทำโครงงานวิจัยจนสำเร็จลุล่วงได้ด้วยดี คณะผู้จัดทำโครงงานวิจัยตระหนักถึงความทุ่มเทและเอาใจใส่ของอาจารย์ที่ปรึกษา รวมถึงอาจารย์ทุกท่านในสาขาวิชาเทคโนโลยีสารสนเทศ

สุดท้ายนี้ ผู้วิจัยใคร่ขอขอบพระคุณผู้มีส่วนเกี่ยวข้องทุกท่าน ที่มีส่วนร่วมในการให้ข้อมูลและเป็นที่ปรึกษาในการทำโครงงานวิจัยนี้จนเสร็จสมบูรณ์ ตลอดจนดูแลขณะปฏิบัติงาน ขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ผู้วิจัย

ปณิธาน วสุวัต

บุญฑริกกา นิซัน

สารบัญ

เรื่อง **หน้า**

บทคัดย่อ.....ก

กิตติกรรมประกาศ.....ข

สารบัญ.....ค

สารบัญตาราง.....จ

สารบัญรูป.....ฉ

บทที่ 1 บทนำ.....1

1.1 ความเป็นมาและความสำคัญของปัญหา.....1

1.2 วัตถุประสงค์.....2

1.3 ขอบเขต.....2

1.4 เครื่องมือและอุปกรณ์ที่ใช้.....3

1.5 เครื่องมือและอุปกรณ์ที่ใช้.....3

1.6 วิธีการดำเนินงาน.....3

1.7 ประโยชน์ที่คาดว่าจะได้รับ.....4

1.8 โครงสร้างและเนื้อหาของวิจัย.....4

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง.....5

2.1 ภาษา Python.....5

2.2 Ransomware มัลแวร์เรียกค่าไถ่.....10

2.3 Microsoft Visual Studio.....11

2.4 งานวิจัยที่เกี่ยวข้อง.....12

บทที่ 3 วิธีดำเนินการโครงงาน.....18

3.1 แผนการดำเนินงาน.....18

สารบัญ (ต่อ)

เรื่อง **หน้า**

3.2 การดำเนินงานการออกแบบและพัฒนาระบบ 21
3.3 เครื่องมือที่ใช้ 22
3.4 สรุปขั้นตอนการดำเนินงาน 23
บทที่ 4 ผลการดำเนินงานวิจัย 24
4.1 ผลการดำเนินงาน 24
บทที่ 5 สรุปผลโครงงานและข้อเสนอแนะ 41
5.1 สรุปผลการดำเนินการ 41
5.2 ปัญหาที่พบในการศึกษา 42
5.3 ข้อเสนอแนะ 42
บรรณานุกรม 43
ภาคผนวก 48
ภาคผนวก ก ขั้นตอนการติดตั้งโปรแกรม Visual Studio Code 49
ภาคผนวก ข คู่มือการใช้งาน 55
ภาคผนวก ค Source code 64
ภาคผนวก ง ประวัติผู้จัดทำ 119

สารบัญตาราง

ตารางที่ **หน้า**

ตารางที่ 1 ตารางแผนการดำเนินงาน 18

สารบัญรูป

รูปที่ หน้า

รูปที่ 1 โลโก้ของภาษา python 8
รูปที่ 2 ตัวอย่างข้อความ "เรียกค่าไถ่" 11
รูปที่ 3 Microsoft Visual Studio..... 12
รูปที่ 4 แผนผัง Flowchart แสดงระบบการจัดการมัลแวร์เรียกค่าไถ่..... 19
รูปที่ 5 แผนผัง Flowchart แสดงระบบการจัดการมัลแวร์เรียกค่าไถ่..... 20
รูปที่ 6 แผนผัง Flowchart แสดงระบบการกักกันและการกำจัดมัลแวร์เรียกค่าไถ่ 21
รูปที่ 7 หน้าจอหลักของโปรแกรม 24
รูปที่ 8 แสดงหน้าต่างให้เลือกโฟลเดอร์ภายในเครื่องคอมพิวเตอร์ของผู้ใช้..... 25
รูปที่ 9 แสดงผลลัพธ์การเลือกโฟลเดอร์ 26
รูปที่ 10 Source Code Select Directory (2) 27
รูปที่ 11 โปรแกรมาแจง้เตือนใหเลือกโฟลเดอร์ที่ต้องการสแกนก่อน 27
รูปที่ 12 ผลลัพธ์แสดงการสแกนโฟลเดอร์ที่ไม่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ 28
รูปที่ 13 ผลลัพธ์ของการสแกนโฟลเดอร์ที่มีไวรัสเรียกค่าไถ่ 28
รูปที่ 14 Source Code Scan 29
รูปที่ 15 Source Code Scan(2).....29
รูปที่ 16 แสดงผลลัพธ์การกำจัดไฟล์ได้สำเร็จ.....30
รูปที่ 17 Source Code Delete Ransomware (1).....30
รูปที่ 18 Source Code Delete Ransomware (2.....31
รูปที่ 19 ผลลัพธ์ของการกักกันไฟล์ไวรัสเรียกค่าไถ่ได้สำเร็จ.....31
รูปที่ 20 Source Code Quarantine (1).....32

สารบัญรูป(ต่อ)

รูปที่ หน้า

รูปที่ 21 Source Code Quarantine (2).....32

รูปที่ 22 แสดงผลลัพธ์การกักกันไฟล์ไปไว้ที่โฟลเดอร์ QuarantineFolder.....33

รูปที่ 23 หน้าจอหลักของระบบกักกันไฟล์ไวรัสเรียกค่าไถ่.....34

รูปที่ 24โปรแกรม แสดงผลลัพธ์การเลือกโฟลเดอร์อื่น 35

รูปที่ 25 โปรแกรมแสดงผลลัพธ์ในการเลือกโฟลเดอร์ QuarantineFolder.....36

รูปที่ 26 Source Code Select Directory (1).....37

รูปที่ 27 Source Code Directory (2).....37

รูปที่ 28 แสดงการเลือกไฟล์ที่สามารถเลือกได้มากกว่าหนึ่งไฟล์.....38

รูปที่ 29 Source Code listbox (1).....38

รูปที่ 30 Source Code listbox (2).....39

รูปที่ 31 แสดงการแจ้งเตือนการกำจัดไฟล์สำเร็จ.....39

รูปที่ 32 โปรแกรมแสดงผลลัพธ์ให้ทราบว่าไฟล์ที่เลือกถูกกำจัดเสร็จสิ้นแล้ว.....40

รูปที่ 33 หน้าเว็บไซต์แสดงให้เลือกการติดตั้ง.....48

รูปที่ 34 สอบถามการยอมรับเงื่อนไข.....49

รูปที่ 35 แสดงหน้าต่าง Setup.....50

รูปที่ 36 หน้าต่างแสดงความพร้อมในการติดตั้ง.....51

รูปที่ 37 หน้าต่างแสดงการติดตั้ง.....52

รูปที่ 38 หน้าต่างแจ้งเตือนการติดตั้งสำเร็จ.....53

รูปที่ 39 หน้าโปรแกรมหลังติดตั้งเสร็จเรียบร้อย.....54

สารบัญรูป(ต่อ)

รูปที่ หน้า

รูปที่ 40 ทางลัดสำหรับการเปิดใช้โปรแกรม.....54

รูปที่ 41 หน้าจอหลักของโปรแกรม.....56

รูปที่ 42 หน้าต่างให้เลือกโฟลเดอร์ภายในเครื่องคอมพิวเตอร์.....56

รูปที่ 43 แสดงผลลัพธ์การเลือกโฟลเดอร์.....57

รูปที่ 44 โปรแกรมแจ้งเตือนให้เลือกโฟลเดอร์ก่อนการสแกน.....58

รูปที่ 45 แสดงผลลัพธ์การสแกนโฟลเดอร์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ 58

รูปที่ 46 แสดงผลลัพธ์การลบไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่.....59

รูปที่ 47 แสดงผลลัพธ์การกักกันไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่.....60

รูปที่ 48 การตรวจสอบการกักกันไฟล์.....60

รูปที่ 49 หน้าจอหลักของระบบกักกันและกำจัดไฟล์.....61

รูปที่ 50 แสดงรายการไฟล์ในโฟลเดอร์ QuarantineFolder.....61

รูปที่ 51 แสดงการเลือกไฟล์ที่สามารถเลือกได้มากกว่าหนึ่งไฟล์.....62

รูปที่ 52 แสดงการแจ้งเตือนการกำจัดไฟล์สำเร็จ.....62

รูปที่ 53 โปรแกรมแสดงผลลัพธ์ให้ทราบว่าไฟล์ที่เลือกถูกกำจัดเสร็จสิ้นแล้ว.....63

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันนี้บนโลกออนไลน์มีโปรแกรมหลากหลายที่เอาไว้เพื่ออำนวยความสะดวกในด้านต่าง ๆมากมายซึ่งบางโปรแกรมก็อาจจะมีภัยคุกคามโดยที่ไม่รู้ตัวหรือเผลอติดตั้งที่ส่งผลกระทบกับคอมพิวเตอร์ได้ ดังนั้นความปลอดภัยของเครื่องคอมพิวเตอร์คือสิ่งที่ควรให้ความสำคัญเป็นอย่างมากเพื่อให้ไม่ตกเป็นเหยื่อหรือมีภัยคุกคามทางคอมพิวเตอร์เกิดขึ้น

ไวรัสคอมพิวเตอร์ (Computer virus) คือโปรแกรมคอมพิวเตอร์ที่บุกรุกเข้าไปในเครื่องคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากผู้ใช้ส่วนมากมักจะมีประสงค์ร้ายและสร้างความเสียหายให้กับระบบของเครื่องคอมพิวเตอร์นั้นๆ ในเชิงเทคโนโลยีความมั่นคงของระบบคอมพิวเตอร์นั้นไวรัสเป็นโปรแกรมคอมพิวเตอร์ที่สามารถทำสำเนาของตัวเองเพื่อแพร่ออกไป โดยการสอดแทรกตัวสำเนาไปในรหัสคอมพิวเตอร์ส่วนที่สามารถปฏิบัติการได้หรือข้อมูลเอกสาร เช่นการติดไวรัส (infection) แฟ้มข้อมูลที่ติดไวรัสนี้จะเรียกว่าโฮสต์ (host) ไวรัสนั้นเป็นประเภทหนึ่ง ของโปรแกรมประเภทมัลแวร์ (malware) หรือโปรแกรมที่มีประสงค์ร้ายในความหมายที่ใช้กันทั่วไป

มัลแวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ (Malware) ในรูปแบบหนึ่ง ที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่น ๆ กล่าวคือ ไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้อื่นแต่อย่างใด คือ Malware (มัลแวร์) ในรูปแบบหนึ่ง ที่อาชญากรไซเบอร์ (Cyber Criminal) ใช้เพื่อโจมตีข้อมูลส่วนตัวบนคอมพิวเตอร์ของผู้ใช้งาน หรือ องค์กรต่างๆ เพื่อเรียกค่าไถ่ (Ransom) แต่คอมพิวเตอร์จะถูกเข้ารหัส หรือบล็อกการเข้าถึงข้อมูลบนดิสก์ของคุณ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วีดีโอ ทันทีที่หลังจากเครื่องเป้าหมายติดมัลแวร์ดังกล่าว ผู้ใช้งานจะไม่สามารถเปิดหรือเข้าถึงไฟล์เหล่านั้นได้ ดังนั้นผู้ใช้จะต้องทำการจ่ายเงินตามข้อความเรียกค่าไถ่ เพื่อปลดล็อคกู้ข้อมูลคืนมา โดยข้อมูลหรือข้อความเรียกค่าไถ่จะแสดงหลังไฟล์ถูกเข้ารหัสเรียบร้อยแล้ว จำนวนเงินค่าไถ่จะแตกต่างกันไปและการชำระเงินต้องชำระผ่านระบบที่มีความยากต่อการตรวจสอบหรือติดตาม แต่อย่างไรก็ตาม

การชำระเงินก็ไม่ได้หมายความว่าผู้ไม่หวังดีจะส่งคีย์ที่ใช้ในการปลดล็อคไฟล์ให้กับผู้ใช้งานข้อมูลของผู้อื่นแต่อย่างใด

โดยปกติแล้วมัลแวร์เรียกค่าไถ่ มักจะแพร่กระจายผ่านทางสแปม หรือฟิชชิ่งอีเมล แต่ยังมีการค้นพบว่า สามารถแพร่กระจายผ่านทางเว็บไซต์ หรือการดาวน์โหลดโดยไดรฟ์เพื่อติดมัลแวร์ดังกล่าวผ่านอุปกรณ์ปลายทาง และการเจาะเครือข่าย เมื่อมัลแวร์เรียกค่าไถ่ได้เข้ามาแล้ว มันจะทำการล็อคไฟล์ทั้งหมดที่สามารถเข้าถึงได้ โดยใช้การเข้ารหัสที่ค่อนข้างรัดกุม ในที่สุดมัลแวร์ดังกล่าวก็จะทำการเรียกค่าไถ่ (โดยปกติจะให้จ่ายเป็น Bitcoins) เพื่อถอดรหัสไฟล์ที่ถูกเข้ารหัส และกู้คืนการทำงานเต็มรูปแบบไปยังระบบไอทีที่ได้รับผลกระทบ ในบางกรณีซอฟต์แวร์ของมัลแวร์เรียกค่าไถ่จะติดตั้งพร้อมกับโทรจัน เพื่อควบคุมอุปกรณ์ของเหยื่ออีกด้วย

ดังนั้นทางผู้จัดทำจึงได้จัดทำระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์รูปแบบ Data breach ขึ้นมาทำการตรวจจับโฟลเดอร์ เพื่อหาไฟล์ที่มีมัลแวร์เรียกค่าไถ่แฝงตัวอยู่ด้วยการตรวจจับแบบเทคนิค Signature-based detection โดยหากไฟล์นั้นกำลังประมวลผลอยู่ก็จะหยุดการประมวลผล และทำการสั่งกักกันหรือลบไฟล์นั้นทันที เพื่อไม่ให้เกิดการเข้ารหัสและยึดไฟล์ภายในระบบคอมพิวเตอร์ของผู้ใช้งานต่อไป

1.2 วัตถุประสงค์

1.2.1 เพื่อพัฒนาระบบที่สามารถจัดการระบบความปลอดภัยทางด้านมัลแวร์เรียกค่าไถ่

1.2.2 เพื่อสร้างเครื่องมืออีกทางเลือกในการจัดการกับความปลอดภัยทางด้านมัลแวร์เรียกค่าไถ่

1.3 ขอบเขต

ขอบเขตเชิงเนื้อหา

- มีการตรวจจับ Ransomware ภายในไฟล์
- มีการกักกันไฟล์ที่มี Ransomware
- มีการกำจัดไฟล์ที่มี Ransomware

ขอบเขตเชิงเทคนิค

- ใช้เทคนิค Signature-based detection ในการตรวจจับ

- ตรวจจับได้เฉพาะ Ransomware ที่มี md5hash ตรงกับข้อมูลที่รวบรวมมาเท่านั้น

1.4 เครื่องมือและอุปกรณ์ที่ใช้

1.4.1 ฮาร์ดแวร์ที่ใช้ในโครงงาน

- Laptop Dell Vostro 15 3000
- Laptop Asus ZenBook
- Computer Asus Vivo Book s14

1.4.2 ซอฟต์แวร์ที่ใช้ในโครงงาน

- ระบบปฏิบัติการ Windows 10
- โปรแกรม Microsoft visual studio
- ภาษา Python

1.5 เครื่องมือและอุปกรณ์ที่ใช้

ผู้ใช้งานทั่วไป

1.6 วิธีการดำเนินงาน

1.6.1 ศึกษาความเป็นไปได้เกี่ยวกับการจัดทำระบบ รวบรวมข้อมูลที่ประเภทของการตรวจจับไวรัสเรียกค่าไถ่ และวิธีในการตรวจจับเพื่อพัฒนาโปรแกรม

1.6.2 วิเคราะห์และออกแบบระบบจากข้อมูลที่รวบรวมมา และวางแผนการดำเนินงานเพื่อกำหนดรูปแบบและลักษณะระบบ เช่น อุปกรณ์ที่ต้องใช้ ภาษาที่ใช้ในการเขียนคำสั่ง libraryที่ต้องใช้งานในการพัฒนาระบบ

1.6.3 เขียนโปรแกรมและพัฒนาระบบ นำแผนการพัฒนาทั้งหมดมาดำเนินการเพื่อเขียนคำสั่งควบคุมการทำงานของระบบ เพื่อให้ตัวระบบสามารถตรวจสอบไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงเข้ามาได้

1.6.4 ทดสอบระบบ นำไฟล์ตัวอย่างทั้งไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงอยู่ และไฟล์ทั่วไปนำมาสแกนเพื่อตรวจสอบโดยการเลือกโฟล์เดอร์ที่ต้องการ แซะสามารถลบไฟล์ได้ตามที่ออกแบบ ซึ่งทดสอบโดยทีมพัมนาระบบ

1.6.5 สรุปผลและนำเสนอผลโครงงาน ระบบที่นำไปทดสอบนั้นมีประสิทธิภาพในสแกนหา ไวรัสเรียกค่าไถ่ หรือไม่

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1.2.1. ได้ระบบที่สามารถจัดการระบบความปลอดภัยทางด้านไวรัสเรียกค่าไถ่

1.2.2. ได้เครื่องมืออีกทางเลือกในการจัดการกับความปลอดภัยทางด้านไวรัสเรียกค่าไถ่

1.8 โครงสร้างและเนื้อหาของวิจัย

การพัฒนาสารนิพนธ์ฉบับนี้สามารถแบ่งเนื้อหาออกเป็น 5 บท ดังนี้

- บทที่ 1 เป็นการกล่าวถึงที่มาและความสำคัญ แนวทางการแก้ปัญหา วัตถุประสงค์ ขอบเขต เครื่องมือที่ใช้ และผลที่คาดว่าจะได้รับ ของการจัดทำงานวิจัยนี้
- บทที่ 2 เป็นการกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้องซึ่งเป็นความรู้พื้นฐานต่างๆ ของโปรแกรมที่เกี่ยวข้องกับการนำมาใช้ในการทำงานวิจัย
- บทที่ 3 เป็นการกล่าวถึงแผนการดำเนินงาน ลำดับขั้นตอน แผนผังการทำงานของระบบในการจัดทำงานวิจัยนี้
- บทที่ 4 เป็นการกล่าวถึงการดำเนินงานการทำงานเครื่องมือที่ใช้ และผลการดำเนินงานในการจัดทำระบบ
- บทที่ 5 เป็นการสรุปผลการดำเนินงานในการจัดทำงานวิจัย ปัญหาที่พบและข้อเสนอแนะ

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในการดำเนินโครงการแอพพลิเคชั่นตรวจจับและกำจัด Adware สำหรับมือถือ Android ผู้พัฒนาได้ทำการศึกษา ค้นคว้าเกี่ยวกับแนวคิด ทฤษฎี และเอกสารที่เกี่ยวข้อง เพื่อแสวงหาความรู้ที่จะนำมาใช้กำหนดกรอบแนวคิดสำหรับการศึกษาโดยมีรายละเอียดดังนี้

2.1 ภาษา Python

2.2 Ransomware มัลแวร์เรียกค่าไถ่

2.3 Microsoft Visual Studio

2.4 งานวิจัยที่เกี่ยวข้อง

2.1 ภาษา Python [4]

ภาษาโปรแกรม Python คือภาษาโปรแกรมคอมพิวเตอร์ระดับสูง โดยถูกออกแบบมาให้เป็นภาษาสคริปต์ที่อ่านง่าย โดยตัดความซับซ้อนของโครงสร้างและไวยกรณ์ของภาษาออกไป ในส่วนของการแปลงชุดคำสั่งที่เราเขียนให้เป็นภาษาเครื่อง Python มีการทำงานแบบ Interpreter คือเป็นการแปลชุดคำสั่งทีละบรรทัด เพื่อป้อนเข้าสู่หน่วยประมวลผลให้คอมพิวเตอร์ทำงานตามที่เราต้องการ นอกจากนั้นภาษาโปรแกรม Python ยังสามารถนำไปใช้ในการเขียนโปรแกรมได้หลากหลายประเภท โดยไม่ได้จำกัดอยู่ที่งานเฉพาะทางใดทางหนึ่ง (General-purpose language) จึงทำให้มีการนำไปใช้กันแพร่หลายในหลายองค์กรใหญ่ระดับโลก เช่น Google, YouTube, Instagram, Dropbox และ NASA เป็นต้น

ประวัติของภาษาโปรแกรม Python ได้เริ่มต้นขึ้นในเดือนธันวาคมปี 1989 โดยนาย Guido van Rossum โปรแกรมเมอร์ชาวดัตช์ ในตอนนั้นทำงานอยู่ที่สถาบันวิจัยแห่งชาติ Centrum Wiskunde & Informatica (CWI) ซึ่งเป็นสถาบันวิจัยทางด้านคณิตศาสตร์และวิทยาการคอมพิวเตอร์ในเมืองอัมสเตอร์ดัม ประเทศเนเธอร์แลนด์ ในเวลานั้น Guido ต้องพัฒนาโปรแกรมสำหรับผู้ดูแลระบบ เพื่อใช้ในโครงการ Amoeba ซึ่งเป็นโครงการเกี่ยวกับระบบปฏิบัติการแบบกระจาย (Distributed operating system) อย่างไรก็ตามเขารู้สึกว่าภาษาโปรแกรม ABC, C และ Bourne shell มีข้อจำกัดมากมาย ทั้งเรื่องใช้เวลาในการพัฒนานานมากและไม่สามารถตอบโจทย์หลายประการ ดังนั้น Guido จึงได้ตัดสินใจเริ่มพัฒนาภาษาโปรแกรมระดับสูงขึ้นมาใหม่เพื่อใช้งานเองเป็นงานอดิเรก โดยนำเอาสิ่งที่ชอบในภาษา ABC มาพัฒนาลงไปในภาษาโปรแกรม Python รวมถึงได้พัฒนาส่วนอื่น ๆ เพิ่มเติมเข้าไป และในเวลา

ต่อมาจึงได้เผยแพร่ Python 1.0 เวอร์ชันแรกในปี 1994 หากเทียบกับภาษา Java ที่ได้ทำการเผยแพร่เวอร์ชันแรกในปี 1996 จะเห็นได้ว่าภาษา Python มีอายุมากกว่าภาษา Java ถึง 2 ปี

ภาษา Python มีกรณีการใช้งานหลายอย่างในการพัฒนาแอปพลิเคชัน ซึ่งรวมถึงตัวอย่างดังต่อไปนี้

การพัฒนาเว็บฝั่งเซิร์ฟเวอร์

การพัฒนาเว็บฝั่งเซิร์ฟเวอร์ประกอบด้วยฟังก์ชันแบ็คเอนด์ที่ซับซ้อนซึ่งเว็บไซต์ดำเนินการเพื่อแสดงข้อมูลต่อผู้ใช้ ตัวอย่างเช่น เว็บไซต์ต้องโต้ตอบกับฐานข้อมูล สื่อสารกับเว็บไซต์อื่น และปกป้องข้อมูลเมื่อส่งข้อมูลผ่านเครือข่าย Python มีประโยชน์สำหรับการเขียนโค้ดฝั่งเซิร์ฟเวอร์ เนื่องจากมีไลบรารีจำนวนมากที่ประกอบด้วยโค้ดที่เขียนไว้ล่วงหน้าสำหรับฟังก์ชันแบ็คเอนด์ที่ซับซ้อน นักพัฒนายังใช้เฟรมเวิร์ก Python ที่หลากหลายซึ่งมีเครื่องมือที่จำเป็นทั้งหมดเพื่อสร้างเว็บแอปพลิเคชันได้เร็วขึ้นและง่ายขึ้นอีกด้วย ตัวอย่างเช่น นักพัฒนาสามารถสร้างโครงสร้างเว็บแอปพลิเคชันได้ภายในไม่กี่วินาที เนื่องจากไม่จำเป็นต้องเขียนขึ้นใหม่ทั้งหมด จากนั้นนักพัฒนาสามารถทดสอบได้โดยใช้เครื่องมือทดสอบของเฟรมเวิร์ก โดยไม่ต้องพึ่งพาเครื่องมือทดสอบภายนอก

ระบบอัตโนมัติด้วยสคริปต์ Python

ภาษาการเขียนสคริปต์คือภาษาการเขียนโปรแกรมที่ทำให้งานที่มนุษย์ทำตามปกติเป็นไปโดยอัตโนมัติ โปรแกรมเมอร์จึงใช้สคริปต์ Python อย่างแพร่หลายเพื่อทำให้งานประจำวันหลายอย่างดังต่อไปนี้เป็นไปโดยอัตโนมัติ การเปลี่ยนชื่อไฟล์จำนวนมากพร้อมกัน การแปลงไฟล์เป็นไฟล์ประเภทอื่น การลบคำที่ซ้ำกันในไฟล์ข้อความ การดำเนินการทางคณิตศาสตร์ขั้นพื้นฐาน การส่งข้อความอีเมล การดาวน์โหลดเนื้อหา การดำเนินการวิเคราะห์บันทึกพื้นฐาน การค้นหาข้อผิดพลาดในหลายไฟล์

วิทยาศาสตร์ข้อมูลและแมชชีนเลิร์นนิง

วิทยาศาสตร์ข้อมูลดึงความรู้อันมีคุณค่าจากข้อมูล และแมชชีนเลิร์นนิง (ML) จะสอนคอมพิวเตอร์ให้เรียนรู้จากข้อมูลโดยอัตโนมัติและทำนายได้อย่างแม่นยำ นักวิทยาศาสตร์ข้อมูลใช้ Python สำหรับงานด้านวิทยาศาสตร์ข้อมูลต่างๆ ดังต่อไปนี้

การแก้ไขและลบข้อมูลที่ไม่ถูกต้อง ซึ่งเรียกว่าการทำความสะอาดข้อมูล

การแยกและเลือกคุณสมบัติต่างๆ ของข้อมูล

การระบุประเภทข้อมูล ซึ่งเป็นการเพิ่มชื่อที่มีความหมายสำหรับข้อมูล

การค้นหาสถิติต่างๆ จากข้อมูล

การแสดงข้อมูลด้วยภาพโดยใช้แผนภูมิและกราฟ เช่น แผนภูมิเส้น กราฟแท่ง ฮิสโทแกรม และแผนภูมิวงกลม นักวิทยาศาสตร์ข้อมูลใช้ไลบรารี Python ML เพื่อฝึกฝนโมเดล ML และสร้างตัวจำแนกที่จำแนกประเภทข้อมูลได้อย่างแม่นยำ บุคคลในแวดวงต่างๆ ใช้ตัวจำแนกแบบ Python เพื่อทำงานด้านการจำแนกประเภท เช่น การจำแนกประเภทรูปภาพ ข้อความ และการรับส่งข้อมูลทางเครือข่าย การรู้จำเสียง และการจดจำใบหน้า นักวิทยาศาสตร์ข้อมูลยังใช้ Python สำหรับดีปเลิร์นนิ่ง ซึ่งเป็นเทคนิค ML ขั้นสูง

การพัฒนาซอฟต์แวร์

นักพัฒนาซอฟต์แวร์มักใช้ Python สำหรับงานด้านการพัฒนาและการประยุกต์ใช้ซอฟต์แวร์ต่างๆ ดังนี้ การติดตามบักในโค้ดของซอฟต์แวร์ การสร้างซอฟต์แวร์โดยอัตโนมัติ การดูแลการจัดการโครงการด้วยซอฟต์แวร์ การพัฒนาต้นแบบซอฟต์แวร์

การพัฒนาแอปพลิเคชันบนเดสก์ท็อปโดยใช้ไลบรารีส่วนติดต่อผู้ใช้แบบกราฟิก (Graphical User Interface หรือ GUI)การพัฒนาเกมที่ใช้ข้อความแบบง่ายๆ ไปจนถึงวิดีโอเกมที่ซับซ้อนมากขึ้น

ระบบทดสอบซอฟตแวร์อัตโนมัติ

การทดสอบซอฟต์แวร์เป็นกระบวนการตรวจสอบว่าผลลัพธ์จริงจากซอฟต์แวร์ตรงกับผลลัพธ์ที่คาดหวังหรือไม่ เพื่อให้แน่ใจว่าซอฟต์แวร์ไม่มีข้อผิดพลาด

โดยนักพัฒนาใช้เฟรมเวิร์กการทดสอบหน่วย Python เช่น Unittest, Robot และ PyUnit เพื่อทดสอบการทำงานที่เขียนขึ้น ผู้ทดสอบซอฟต์แวร์ใช้ Python เพื่อเขียนกรณีที่ใช้ในการทดสอบสำหรับสถานการณ์การทดสอบต่างๆ ตัวอย่างเช่น ผู้ทดสอบใช้เพื่อทดสอบอินเทอร์เฟซผู้ใช้ของเว็บแอปพลิเคชันส่วนประกอบซอฟต์แวร์หลายตัว และคุณสมบัติใหม่ นักพัฒนาสามารถใช้เครื่องมือหลายอย่างเพื่อเรียกใช้สคริปต์ทดสอบได้โดยอัตโนมัติ โดยเครื่องมือเหล่านี้เรียกว่าเครื่องมือรวบรวม/ปรับใช้อัตโนมัติ (Continuous Integration/Continuous Deployment หรือ CI/CD) ทั้งนี้ผู้ทดสอบและนักพัฒนาซอฟต์แวร์ใช้เครื่องมือ CI/CD เช่น Travis CI และ Jenkins เพื่อทำให้การทดสอบเป็นไปโดยอัตโนมัติ เครื่องมือ CI/CD จะเรียกใช้สคริปต์ทดสอบ Python โดยอัตโนมัติ และรายงานผลการทดสอบทุกครั้งที่นักพัฒนานำการเปลี่ยนแปลงโค้ดใหม่มาใช้

*รูปที่ 1 โลโก้ของภาษา **python***

*(ที่มา : **https://www.python.org/community/logos/**)*

ไลบรารี Python คือชุดของโค้ดที่ใช้บ่อยซึ่งนักพัฒนาสามารถใช้ในโปรแกรม Python เพื่อหลีกเลี่ยงการเขียนโค้ดขึ้นใหม่ทั้งหมด ตามค่าเริ่มต้นแล้ว Python จะมาพร้อมกับไลบรารีมาตรฐาน ซึ่งมีฟังก์ชันที่นำกลับมาใช้ใหม่ได้มากมาย นอกจากนี้ยังมีไลบรารี Python มากกว่า 137,000 รายการสำหรับการประยุกต์ใช้ต่างๆ รวมถึงการพัฒนาเว็บ วิทยาศาสตร์ข้อมูล และแมชชีนเลิร์นนิง (ML) ไลบรารี Python ยอดนิยม ได้แก่

Matplotlib นักพัฒนาซอฟต์แวร์ใช้ Matplotlib เพื่อลงจุดข้อมูลในกราฟิกสองมิติและสามมิติ (2D และ 3D) คุณภาพสูง ซึ่งมักจะใช้ในงานทางวิทยาศาสตร์ Matplotlib ช่วยให้คุณสามารถแสดงข้อมูลเป็นภาพโดยแสดงผลในแผนภูมิต่างๆ เช่น แผนภูมิแท่งและแผนภูมิเส้น คุณยังสามารถลงจุดแผนภูมิได้หลายรายการพร้อมกัน และกราฟิกสามารถใช้งานได้ในทุกแพลตฟอร์มอีกด้วย

Pandas มีโครงสร้างข้อมูลที่ปรับให้เหมาะสมและยืดหยุ่น ซึ่งคุณสามารถใช้เพื่อจัดการชุดข้อมูลเวลาและข้อมูลที่มีโครงสร้าง เช่น ตารางและอาร์เรย์ ตัวอย่างเช่น คุณสามารถใช้ Pandas เพื่ออ่าน เขียน ผสานรวม กรอง และจัดกลุ่มข้อมูลได้ หลายคนจึงใช้สำหรับงานด้านวิทยาศาสตร์ข้อมูล การวิเคราะห์ข้อมูล และ ML

NumPy เป็นไลบรารียอดนิยมที่นักพัฒนาใช้เพื่อสร้างและจัดการอาร์เรย์ จัดการรูปร่างเชิงตรรกะ และดำเนินการคำนวณพีชคณิตเชิงเส้นได้อย่างง่ายดาย โดย NumPy รองรับการทำงานร่วมกับภาษาต่างๆ มากมาย เช่น C และ C++

คำขอ ไลบรารีคำขอมีฟังก์ชันที่เป็นประโยชน์ที่จำเป็นสำหรับการพัฒนาเว็บ โดยคุณสามารถใช้ไลบรารีนี้เพื่อส่งคำขอ HTTP, เพิ่มส่วนหัว, เพิ่มพารามิเตอร์ URL, เพิ่มข้อมูล และทำงานอื่นๆ อีกมากมายเมื่อสื่อสารกับเว็บแอปพลิเคชัน

OpenCV-Python เป็นไลบรารีที่นักพัฒนาใช้ในการประมวลผลรูปภาพสำหรับการประยุกต์ใช้เชิงคอมพิวเตอร์วิทัศน์ ซึ่งมีฟังก์ชันมากมายสำหรับงานประมวลผลภาพ เช่น การอ่านและเขียนรูปภาพพร้อมกัน, การสร้างสภาพแวดล้อม 3 มิติจาก 2 มิติ และการบันทึกภาพและวิเคราะห์ภาพจากวิดีโอ

Keras เป็นไลบรารีนิวรัลเน็ตเวิร์กเชิงลึกของ Python ที่รองรับการประมวลผลข้อมูล การแสดงภาพข้อมูล และอื่นๆ อีกมากมายได้อย่างยอดเยี่ยม Keras รองรับนิวรัลเน็ตเวิร์กมากมาย ซึ่งมีโครงสร้างแบบโมดูลที่ให้ความยืดหยุ่นในการเขียนแอปพลิเคชันด้านนวัตกรรม

2.2 Ransomware มัลแวร์เรียกค่าไถ่ [6]

มัลแวร์เรียกค่าไถ่ (Ransomware) ได้รับการกำหนดโดยกระทรวงยุติธรรมของสหรัฐอเมริกา ในฐานะรูปแบบใหม่ของอาชญากรรมทางไซเบอร์ที่มีศักยภาพ ที่สามารถก่อให้เกิดผลกระทบในระดับโลก นอกจากนี้ยังสามารถสร้างผลกระทบอย่างมาก สามารถขัดขวางการดำเนินธุรกิจ และนำไปสู่การสูญเสียข้อมูลที่สำคัญได้ มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่นๆ คือ ไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้อื่นแต่อย่างใด แต่จะเข้ารหัสหรือล็อคไฟล์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วีดีโอ ผู้ใช้งานจะไม่สามารถเปิดหรือเข้าถึงไฟล์เหล่านั้นได้ ดังนั้นผู้ใช้จะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” เพื่อปลดล็อคกู้ข้อมูลคืนมา

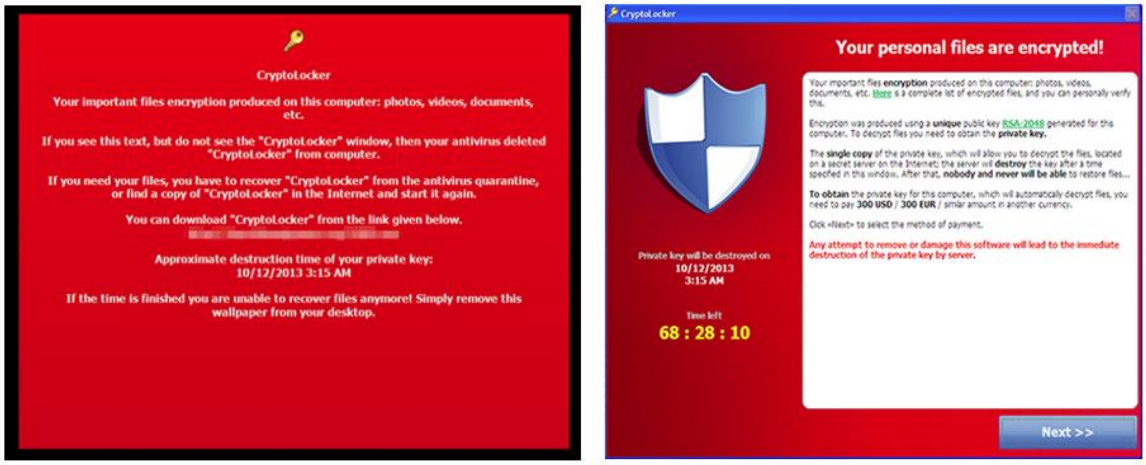
โดยข้อมูลหรือข้อความ “เรียกค่าไถ่” จะแสดงหลังไฟล์ถูกเข้ารหัสเรียบร้อยแล้ว จำนวนเงินค่าไถ่จะแตกต่างกันไป โดยจะมีราคาอยู่ที่ $150 - $500 โดยประมาณและการชำระเงินต้องชำระผ่านระบบที่มีความยากต่อการตรวจสอบหรือติดตาม เช่น การโอนเงินผ่านทางอิเล็กทรอนิกส์, Paysafecard หรือ Bitcoin เป็นต้น แต่อย่างไรก็ตามการชำระเงินก็ไม่ได้หมายความว่าผู้ไม่หวังดีจะส่งคีย์ที่ใช้ในการปลดล็อคไฟล์ให้กับผู้ใช้งาน

Ransomware จะแพร่กระจาย โดยผ่านช่องทางต่าง ๆ ดังนี้

• ในรูปแบบเอกสารแนบทางอีเมล์ Ransomware จะมาในรูปแบบเอกสารแนบทางอีเมล์ โดยอีเมล์ผู้ส่งมักจะเป็นผู้ให้บริการที่เรารู้จักอย่างเช่น ธนาคาร และจะใช้หัวข้อหรือประโยคที่ดูน่าเชื่อถืออย่าง “Dear Value Customer”, “Undelivered Mail Returned to Sender”, “Invitation to connect on LinkedIn.” เป็นต้น ประเภทของไฟล์แนบก็จะเป็น “.doc” หรือ “.xls” ทำให้ผู้ใช้คิดว่าเป็นไฟล์เอกสาร Word หรือ Excel แต่เมื่อตรวจสอบจะเห็นนามสกุล “.exe” ซ่อนอยู่ อย่างเช่น “Paper.doc.exe” แต่ผู้ใช้จะเห็นเฉพาะ “Paper.dac” ทำให้เข้าใจผิดว่าเป็นไฟล์ที่ไม่อันตราย

• ในรูปแบบของโฆษณา (Malvertising) Ransomware อาจมาในรูปแบบของโฆษณา มาว่าจะเป็นที่ฝังมากับซอฟต์แวร์หรือตามหน้าเว็บไซต์ต่าง ๆ

• เชื่อมโยงไปยังเว็บไซต์อันตรายและอาศัยช่องโหว่ของซอฟต์แวร์ ผู้ใช้ยังสามารถกลายเป็นเหยื่อได้โดยไม่ได้ตั้งใจ เพียงเข้าเยี่ยมชมหน้าเว็บที่ถูกผู้ไม่หวังดีเข้ามาควบคุม ตัวอย่างเช่น ถูกดาวน์โหลดโค้ด (Code) ที่เป็นอันตรายผ่านทางโฆษณาแบนเนอร์ใน Flash ดังแสดงในรูปที่ 3 โดย Ransomware มักจะใช้ประโยชน์จากข้อบกพร่องหรือช่องโหว่ด้านความปลอดภัยอื่นๆในเบราว์เซอร์, แอพลิเคชั่น หรือระบบปฏิบัติการ บ่อยครั้งก็มักจะเกิดจากช่องโหว่ในเว็บเบราว์เซอร์, Java และ PDF แต่ช่องโหว่ที่พบมากที่สุดก็คือใน Flash



รูปที่ 2 ตัวอย่างข้อความ "เรียกค่าไถ่"

(ที่มา : trendmicro.com/vinfo/ph/security/definition/ransomware/)

2.3 Microsoft Visual Studio [7]

Microsoft Visual Studio คือ ชุดพัฒนาโปรแกรม (Integrated Development Environment) ประกอบด้วยโปรแกรมหลายๆ ตัวที่ใช้ในการสร้างโปรแกรมสำเร็จรูปบนระบบปฏิบัติการวินโดวส์ หรือใช้สร้างเว็บโปรแกรม สร้างเว็บบริการ จัดการฐานข้อมูล และอื่นๆ อีกมากมาย Visual Studio ได้รวบรวมเครื่องมือพัฒนาต่างๆ ที่ใช้ในการพัฒนาโปรแกรมตั้งแต่ หน้าจอที่ใช้พัฒนาโปรแกรม (Development interface) เครื่องมือในการตรวจหาจุดผิดในโปรแกรม (Debugging tool) ตัวช่วยอัตโนมัติในการเขียนโปรแกรม (Wizard tool) ตัวจัดการฐานข้อมูล (Database management) และส่วนประกอบอื่นๆที่จำเป็นในการพัฒนาโปรแกรม นำมาประกอบกันเป็นชุด เรียกว่า Integrated Development Environment (ชุดพัฒนาโปรแกรม) หรือเรียกย่อๆ ว่า IDE

รูปที่ 3 Microsoft Visual Studio

(ที่มา : http://blog.bru.ac.th/wp-content/uploads/bp-attachments/10774/Chapter-1.pdf)

2.4 งานวิจัยที่เกี่ยวข้อง

2.4.1 งานวิจัยเรื่อง แนวทางการรับมือและการรับแจ้งเหตุของตำรวจต่อกรณีมัลแวร์เรียกค่าไถ่ [2]

มัลแวร์เรียกค่าไถ่เป็นเครื่องมือของคนร้ายไซเบอร์ที่ต้องการขู่กรรโชกทรัพย์เพื่อให้ได้ผลประโยชน์ที่เป็นตัวเงิน แฮกเกอร์สร้างซอฟท์แวร์ประสงค์ร้ายโดยอาศัยเทคโนโลยีรหัสลับผสมผสานกับเทคนิควิธีวิศวกรรมซอฟท์แวร์ วันนาครายและเพทย่าเป็นมัลแวร์ที่สร้างความเสียหายทั่วโลกในช่วงหลายปีที่ผ่านมา มัลแวร์สเปดเพิ่งถูกตรวจพบเมื่อไม่มานานนี้และได้สร้างความเสียหายให้กับโรงพยาบาลสระบุรี สิ่งสำคัญอันดับแรกของการรับมือกับภัยคุกคามเช่นนี้คือการปฏิเสธการจ่ายเงินและเจรจาต่อรองกับคนร้ายทุกช่องทาง โครงการยกเลิกค่าไถ่เป็นทางเลือกหนึ่งให้เหยื่อได้รับคำแนะนำและเครื่องมือถอดถอนมัลแวร์ วันนาคราย เพทย่าและสเปดยังคงถูกจัดอยู่ในกลุ่มภัยคุกคามที่น่าจับตาช่วงทศวรรษนี้ การรับมือเชิงรุกด้วยการปฏิเสธการจ่ายเงินเป็นสิ่งที่ผู้เชี่ยวชาญแนะนำ ตลอดจนการตัดการเชื่อมต่อทันทีเมื่อเกิดเหตุเพื่อลดการแพร่ระบาดในวงกว้าง ส่วนการรับมือเชิงตั้งรับคือการสำรองข้อมูลและปรับปรุงซอฟท์แวร์ระบบปฏิบัติการและโปรแกรมป้องกันไวรัสเป็นประจำ ช่องทางรับแจ้งเหตุร้ายไซเบอร์เป็นที่สิ่งตำรวจทุกประเทศต้องให้ความสำคัญ การเชื่อมโยงข้อมูลจากเหยื่อในฐานะผู้แจ้งเป็นประโยชน์อย่างยิ่งต่อการสืบสวนเพื่อรวบรวมพยานหลักฐานนำไปสู่การพิสูจน์การกระทำผิดของคนร้าย

จากงานวิจัยดังกล่าวเป็นการศึกษาสภาพปัญหาและความรุนแรงของมัลแวร์เรียกค่าไถ่ และนำเสนอแนวทางการรับมือด้วยการรับแจ้งเหตุผ่านระบบการให้บริการของหน่วยงานตำรวจ ซึ่งแสดงให้เห็นถึงความรุนแรงของมัลแวร์เรียกค่าไถ่ในประเภทต่าง ๆ

2.4.2 งานวิจัยเรื่อง แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ในเขตพื้นที่พุทธสถาน กรณีศึกษาเมสแก๊งA Guideline for Ransomware Detection and Prevention at the Buddhist Places : A case study of Maze Gang [1]

เนื่องจากจากการแพร่ระบาดของโรคโควิด ๑๙ ทำให้ตลอดปี ค.ศ. ๒๐๒๐ เป็นช่วงที่การทำงานจากที่บ้าน (Work from home) ได้เข้ามามีบทบาทสำคัญต่อองค์กร ธุรกิจและหน่วยงานทั่วโลก ทำให้ภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ที่เกิดจากการใช้งานอินเทอร์เน็ตเพิ่มมากยิ่งขึ้น โดยเฉพาะภัยจากมัลแวร์เรียกค่าไถ่ จากการสำรวจในปี พ.ศ. ๒๕๖๓ พบว่า มีการโจมตีทางไซเบอร์ด้วยมัลแวร์ประเภทนี้ในเขตพื้นที่พุทธสถาน ดังนั้น งานวิจัยฉบับนี้มีวัตถุประสงค์เพื่อศึกษาแนวทางการป้องกันความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่จากการทบทวนวรรณกรรมที่เกี่ยวข้องจากบทความวิจัยต่างประเทศ และใช้กรณีศึกษาจริงจากการโจมตีทางไซเบอร์จากเมสแก๊ง นอกจากนี้ได้รวบรวมผลการวิเคราะห์ต่าง ๆ มาใช้เป็นแนวทางป้องกันการโจมตีจากเมสแก๊งจากผลการศึกษาขั้นตอนการโจมตีของเมสแก๊งพบว่า มีพฤติกรรมหลายอย่างที่สามารถนำมาสร้างแนวทางในการป้องกันได้ เช่น การแอบฝังตัวอยู่ในระบบโครงข่ายเป็นเวลานานก่อนที่จะลงมือนำข้อมูลที่สำคัญออกมาจากเครือข่ายของเป้าหมายและดำเนินการเข้ารหัสไฟล์ข้อมูล แต่ถ้ามีมาตรการในการเฝ้าระวังระบบเครือข่ายที่ดีเพียงพอ ก็อาจจะสามารถตรวจพบและระงับภัยคุกคามไซเบอร์ที่เกิดขึ้นจาก มัลแวร์เรียกค่าไถ่ได้ เป็นต้น ดังนั้น บทความฉบับนี้จึงได้เสนอแนวทางการป้องกันการโจมตีจากมัลแวร์เรียกค่าไถ่เมสแก๊งบนพื้นฐานกรอบแนวคิดของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติกระทรวงพาณิชย์ สหรัฐฯ ได้แก่ (๑) การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (๒) การปกป้องดูแลทรัพย์สิน

งานวิจัยดังกล่าวศึกษาวิธีการโจมตีของแมสแก๊งจะเป็นลักษณะของมัลแวร์เรียกค่าไถ่แบบใช้คนสั่งการ (Human-operated ransomware) บนระบบปฏิบัติการวินโดวส์ ซึ่งร้อยละ ๙๓ ของมัลแวร์เรียกค่าไถ่เป็นไฟล์นามสกุล exe ซึ่งทำงานบนระบบปฏิบัติการวินโดวส์

2.4.3 งานวิจัยเรื่อง HLMD: a signature-based approach to hardware-level behavioral malware detection and classification [5]

Malicious programs, or malware, often use code obfuscation techniques to make static analysis difficult. To deal with this problem, various behavioral detection techniques have been proposed that focus on runtime behavior to distinguish between benign and

malicious programs. The majority of them are based on the analysis and modeling of system call traces, which are a common type of audit data often used to describe the interaction between programs and the operating system. However, the techniques are not widely used in practice because of high performance overheads. An alternative approach is to perform behavioral detection at the hardware level. The basic idea is to use information that is accessible through hardware performance counters, which are a set of special purpose registers built into modern processors providing detailed information about hardware and software events. In this paper, we pursue this line of research by presenting HLMD, a novel approach that uses behavioral signatures generated from hardware performance counter traces to instantly detect and disable malicious programs at the beginning of their execution. HLMD is especially suitable for independent malicious programs that can be run standalone without having to be attached to a host program. Each behavioral signature is composed of some number of singular values and singular vectors, obtained by applying the singular value decomposition to the hardware performance counter traces of a known malware family. HLMD follows a two-stage heuristic matching strategy to increase the detection performance to an acceptable level while reducing the detection complexity to linear time. The results of our experiments performed on a dataset of benign and malicious programs show that HLMD can achieve an average precision, recall, and F-measure of 95.19%, 89.96%, and 92.50%, respectively.

จากงานวิจัยดังกล่าว มีการศึกษาเกี่ยวกับพฤติกรรมของมัลแวร์ที่ในปัจจุบันนี้มีเทคนิคหลีกเลี่ยงการตรวจจับได้ดี จึงได้คิดค้นหลากหลายวิธีในการตรวจจับ จนได้วิธีการตรวจจับพฤติกรรมที่ระดับฮาร์ดแวร์ ซึ่งเป็นแนวทางใหม่ที่ใช้ลายเซ็นพฤติกรรมที่สร้างขึ้นจากการติดตามตัวนับประสิทธิภาพของฮาร์ดแวร์เพื่อตรวจจับและปิดใช้งานโปรแกรมที่เป็นอันตรายในทันทีเมื่อเริ่มดำเนินการ และผลการทดลองแสดงให้เห็นว่า HLMD นี้มีความแม่นยำในการตรวจจับมัลแวร์สูง

2.4.8 งานวิจัยเรื่อง Ransomware Digital Extortion: A Rising New Age [3]

Threat

Imagine what would happen if you were stopped from accessing your own files or accessing your own computer system.

Now imagine further if to get back the access someone demanded ransom amount from you. Globally increasingly social

interactions and financial transactions involve few critical aspects such as digital data, computing device and the internet.

This is an area where Ransomware has spread and become a major concern against digital extortion in the form of a

new age threat vector to corporates and end users alike. This paper presents the various ways and methods adopted

by cyber criminals against Ransomware and present an anti-malware detection system. Background/Objectives: The

impact of Ransomware has caused immense damage to end users and corporates alike. Access to authorized data being

blocked and being released only after the ransom demand has been mate, is a new age digital extortion has which holds

promise as a viable option against the cyber-attacks on user systems, mobiles and handhelds. Methods/Statistical

Analysis: The authors reviewed existing Crypto and Locker ransomware, studying their propagation, attack techniques

and new emerging threat vectors as file Encryption Ransomware, Screen Lock Ransomware, Windows & Browser Lock,

Pop Advertisements and URL Redirection. The authors also designed and tested cloud-based malware detection system,

performing comparison evaluation with and without the proposed anti-malware solution in form of sandboxes, so even

if the environment got compromised, it could be easily decommissioned and rebuilt from a fresh clean virtual snapshots.

The system comprised of three virtual environments running services for Malware Behavioral Analysis, Malware Code

Analysis and Malware Reporting. Open source and commercial tools were used in each of the three environments. Malware

Behavioral environment for analyzing malware for before and after receiving malware payload files and logs from infected

user devices. Malware Code Analysis gathered assembly code and memory dumps from memory and performed analysis

on malware payload instructions. The Reporting environment analyzed Web URL proactively for malicious sites hosting

malware code or payloads and also checked the user system and devices for before and after analysis logs. Findings:

When comparing to the standard antivirus scanners that rely on signatures, the proposed malware detection and alerting

process has better malware mitigation results and advantages. The Anti-Malware scanning security apart from being a

cloud service with the secure scanners operating from cloud platforms display a high level of resilience. Being a Cloud

application has the standard cloud feature advantages of being elastic, scalable, pay-as-you-use, user driven cloud model.

This model can also help in saving costs by promoting the BYOD concept. Application/Improvements: The Anti-Malware

cloud model can be modified to offer specific payload blocking for different customers even as other customers of that very.

application programs are able to access them and even benefit from experience of the infected customers. This model can

be scale up dynamically as required.

จากงานวิจัยข้างต้น มีการศึกษาวิเคราะห์แรนซัมแวร์ เพื่อนำไปออกแบบและทดสอบระบบตรวจจับมัลแวร์บนคลาวด์ ทำการเปรียบเทียบแบบมีและไม่มีการป้องกันมัลแวร์ในรูปแบบของแซนด์บ็อกซ์ ซึ่งผลการวิจัยนั้นค่อนข้างดีเมื่อเปรียบเทียบกับโปรแกรมสแกนไวรัสมาตรฐานอื่น กล่าวคือ สามารถลดการบุกรุกของไวรัสแรนซัมแวร์ได้ดีกว่า และมีความปลอดภัยสูงกว่า

บทที่ 3

วิธีดำเนินการโครงงาน

ขั้นตอนการดำเนินงานของการสร้างระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์รูปแบบ Data breach เพื่อให้บรรลุวัตถุประสงค์ของโครงการ มีขั้นตอนดังนี้

3.1 แผนการดำเนินงาน

3.2 การดำเนินงานการออกแบบและพัฒนาระบบ

3.3 เครื่องมือที่ใช้

3.4 สรุปขั้นตอนการดำเนินงาน

3.1 แผนการดำเนินงาน

การดำเนินงานและจัดทำการวิจัยนี้ เป็นการสร้างและออกแบบระบบตรวจจับไฟล์ที่แฝงมาด้วยมัลแวร์เรียกค่าไถ่ โดยมีการรวบรวมข้อมูลที่เกี่ยวข้อง รวมไปถึงขั้นตอนของการตรวจจับและกำจัดมัลแวร์เรียกค่าไถ่บนระบบปฏิบัติการวินโดวส์ เพื่อให้การทานของระบบมีประสิทธิภาพและแนวทางในการดำเนินงาน ซึ่งสามารถสรุปขั้นตอนได้ดังนี้

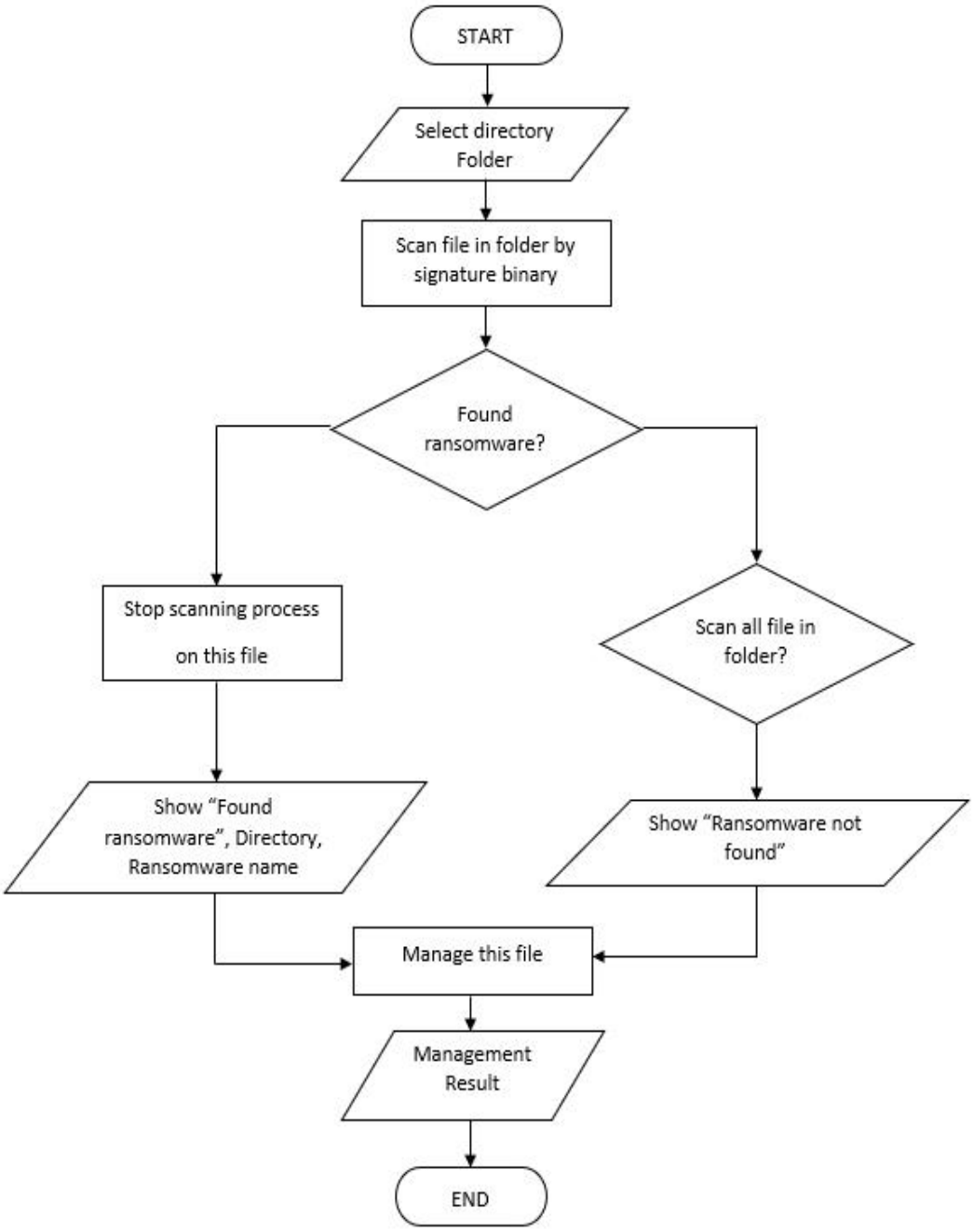
การดำเนินงาน/เดือนปี	พ.ศ. 2565										พ.ศ. 2566	
	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	**********	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.
1.ศึกษาความเป็นไปได้ของโครงงาน						สหกิจศึกษา						
2.วิเคราะห์และออกแบบระบบ												
3.เขียนโปรแกรมและพัฒนาระบบ												
4.ทดสอบระบบ												
5.สรุปผลและนำเสนอ												

ตารางที่ 1 ตารางแผนการดำเนินงาน

3.1.1 แผงผัง Flowchart

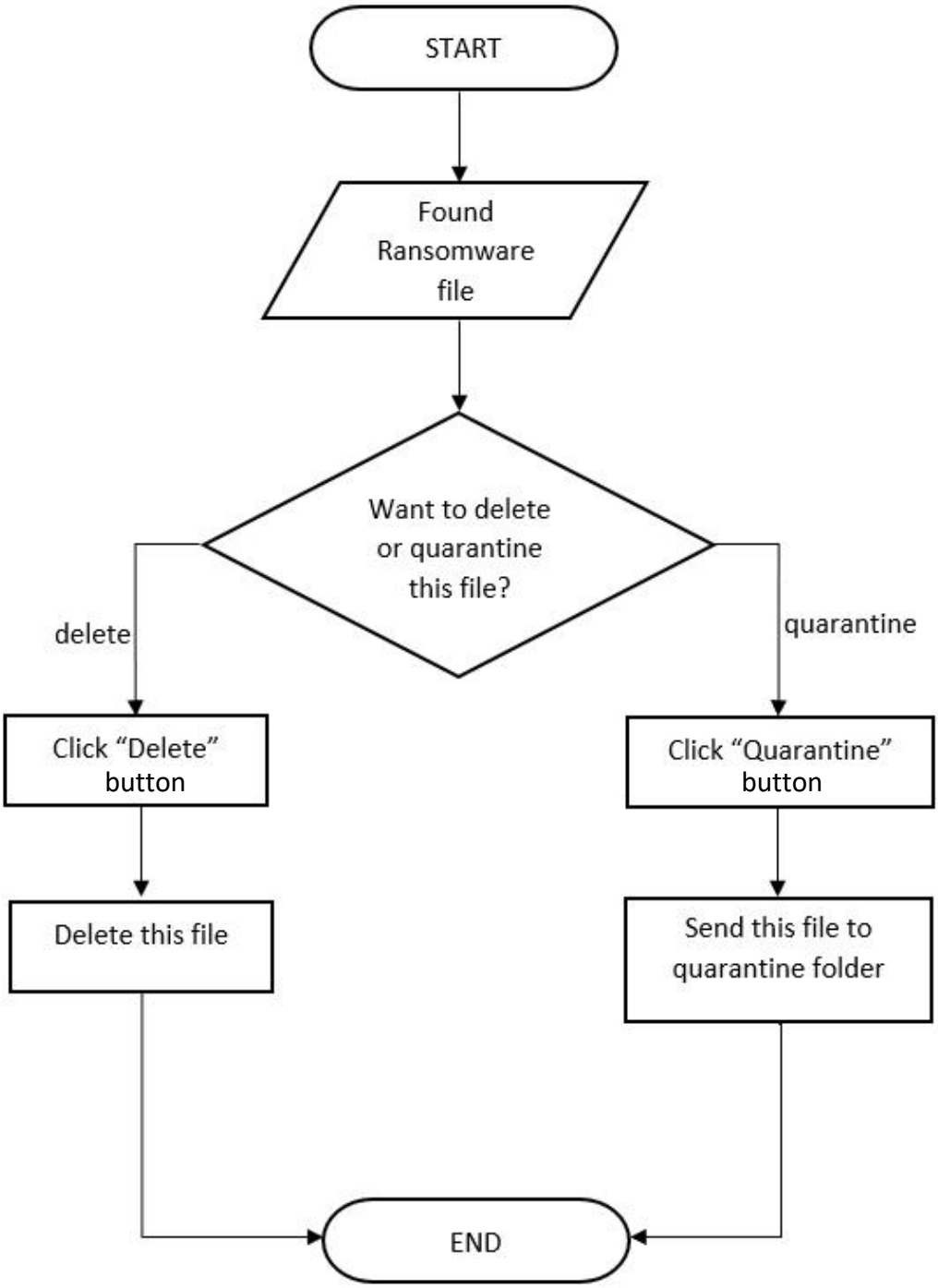
ใช้ในการแสดงขั้นตอนของระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์รูปแบบ Data breach

<u>Flowchart แสดงระบบการตรวจจับมัลแวร์เรียกค่าไถ่</u>



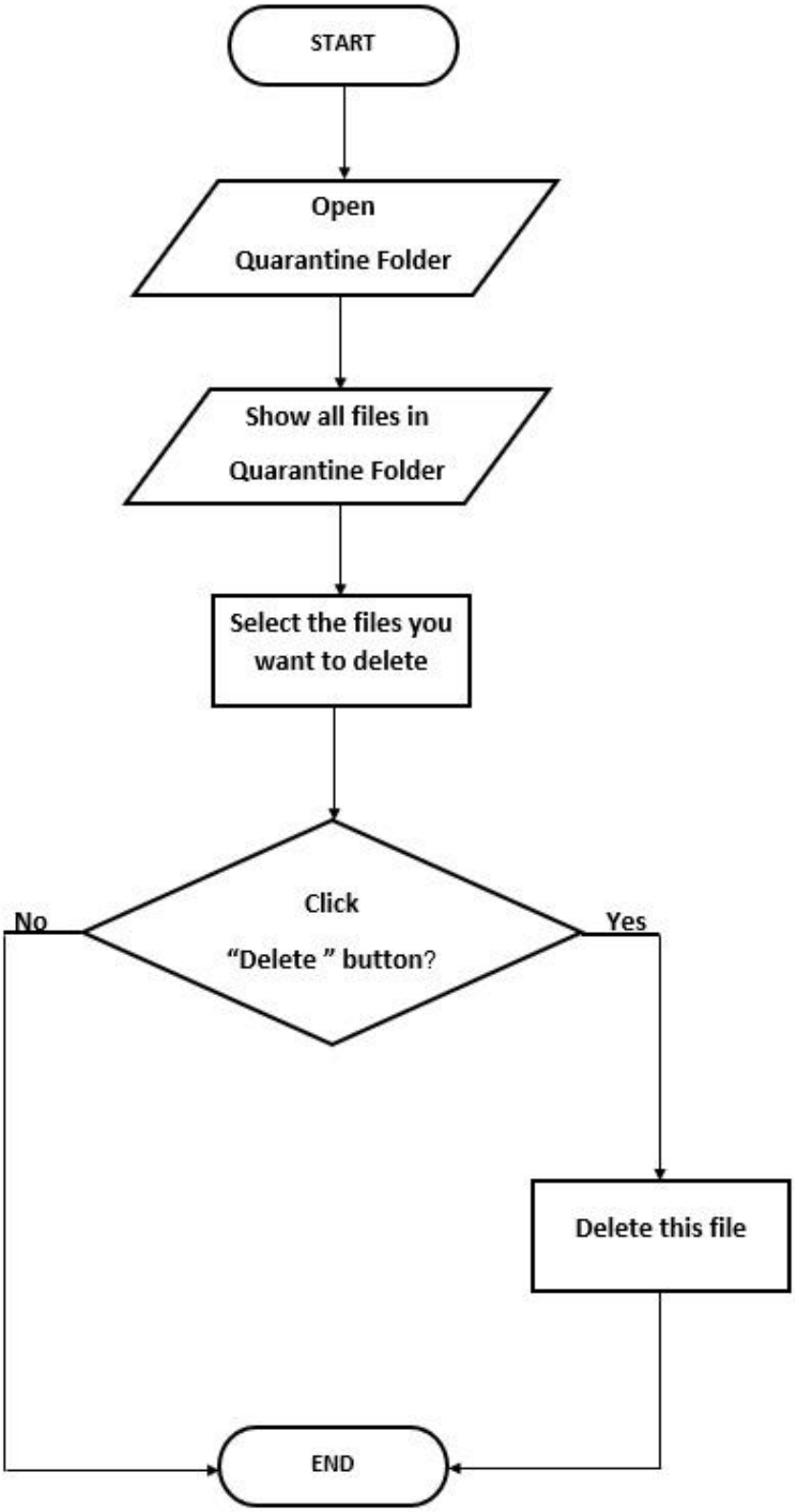
*รูปที่ 4 แผนผัง **Flowchart** แสดงระบบการจัดการมัลแวร์เรียกค่าไถ่*

Flowchart แสดงระบบการตรวจจับมัลแวร์เรียกค่าไถ่



*รูปที่ 5 แผนผัง **Flowchart** แสดงระบบการจัดการมัลแวร์เรียกค่าไถ่*

Flowchart แสดงระบบการกักกันและกำจัดมัลแวร์เรียกค่าไถ่



*รูปที่ 6 แผนผัง **Flowchart** แสดงระบบการกักกันและกำจัดมัลแวร์เรียกค่าไถ่*

3.2 การดำเนินงานการออกแบบและพัฒนาแอพพลิเคชั่น

3.2.1 ศึกษาความเป็นไปได้ของโครงงาน

ศึกษารูปแบบการจัดทำโดยรวบรวมข้อมูลด้านการเขียนโค้ดเพื่อสร้างแบบแผนการดำเนินงานให้สอดคล้องกับการตรวจจับมัลแวร์เรียกค่าไถ่แบบsignature base

3.2.2 วิเคราะห์และออกแบบแอพพลิเคชั่น

นำข้อมูลจากที่รวบรวมมา และนำมาวางแผนขั้นตอนการดำเนินงานเพื่อกำหนดรูปแบบและลักษณะของโปรแกรม

3.2.3 เขียนโปรแกรมและพัฒนาแอพพลิเคชั่น

นำแผนการพัฒนาทั้งหมดมาดำเนินการเพื่อเขียนคำสั่งควบคุมการทำงานของโปรแกรมเพื่อให้ตัวโปรแกรมทำงานได้ตามหลักการ

3.2.4 ทดสอบระบบ

เป็นการนำระบบ มาทดสอบความถูกต้องของระบบ โดยทางทีมผู้พัฒนาจะนำระบบที่ถูกพัฒนาสำเร็จแล้วมาทดสอบว่าระบบ สามารถที่จะตรวจจับได้ว่าภายในโปลเดอร์ที่ต้องการมีไฟล์ที่มีมัลแวร์เรียกค่าไถ่แฝงอยู่หรือไม่ หากมีการตรวจพบก็ทำการกักกันและกำจัดในขั้นตอนถัดไป หากมีความผิดพลาดจะทำการนำกลับไปที่ขั้นตอน (3.2.3) การเขียนโปรแกรมและพัฒนาระบบ

3.2.5 สรุปผลและนำเสนอผลโครงงาน

นำผลจากการทดลองระบบตรวจจับ และกำจัดมัลแวร์เรียกค่าไถ่ สำหรับมือถือ มีประสิทธิภาพในการตรวจจับ และจำกัด ไฟล์มัลแวร์เรียกค่าไถ่ หรือสามารถทำงานได้ตามวัตถุประสงค์ที่ตั้งไว้

3.3 เครื่องมือที่ใช้

3.3.1 ด้านฮาร์ดแวร์

- Laptop Dell Vostro 15 3000
- Laptop Asus ZenBook
- Computer Asus Vivo Book s14

3.3.2 ด้านซอฟต์แวร์

1) ระบบปฏิบัติการ Windows 10 เป็นระบบปฏิบัติการที่ใช้รองรับการทำงาน และตรวจจับมัลแวร์เรียกค่าไถ่

2) โปรแกรม Microsoft visual studio ใช้ในการเขียนและสร้างระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach

3.4 สรุปขั้นตอนการดำเนินงาน

การพัฒนาระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach เป็นการตรวจจับไฟล์ที่มีมัลแวร์เรียกค่าไถ่ฝังตัวอยู่ภายในซึ่งตรวจสอบจากโฟล์เดอร์ ด้วยการใช้เทคนิค signature-based detection ในการตรวจจับ ซึ่งสามารถสรุปขั้นตอนการพัฒนาได้ดังหัวข้อต่อไปนี้

3.4.1 ศึกษาความเป็นไปได้ของโครงงาน ขอคำแนะนำจากอาจารย์ที่ปรึกษา เพื่อศึกษาข้อมูลและค้นหาข้อมูลที่เกี่ยวเนื่องกับ Ransomware เพื่อนำมาทำการสร้างระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach หลังจากรวบรวมความต้องการของระบบแล้ว จากนั้นนำข้อมูลที่ได้รวบรวมมาทำการศึกษาความเป็นไปได้ของการพัฒนาระบบ

3.4.2 วิเคราะห์และออกแบบ GUI และฟังก์ชันการทำงานของระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach ตามความต้องการของระบบที่ได้ทำการศึกษาและรวบรวมมา

3.4.3 เขียนโปรแกรมและพัฒนาระบบ โดยในขั้นตอนการเขียนโปรแกรมหลังจากได้ทำการออกแบบ และรวบรวมข้อมูล ก็เริ่มดำเนินการพัฒนาระบบตามแผนที่วางไว้ โดยเริ่มจากการเตรียมข้อมูล Ransomware Signature พัฒนาระบบการตรวจจับ และ สร้าง GUI ให้ได้ผลลัพธ์ของระบบตามที่ได้ออกแบบและรวบรวมความต้องการไว้

3.4.4 ทดสอบระบบ ทำการทดสอบโดยการหาไฟล์ตัวอย่างและติดตั้งไฟล์ที่มี Ransomware แฝงอยู่ จากนั้นเริ่มทำการทดสอบระบบตรวจจับทั้งไฟล์ทั่วไปไม่อันตรายและไฟล์อันตราย เพื่อให้ผลลัพธ์เป็นไปตามที่ต้องการ และแก้ไขปรับปรุงการทำงานของระบบระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breachที่เกิดข้อผิดพลาดหรือไม่เป็นตามแผนที่วางไว้

3.4.6 สรุปผลลัพธ์การทำงานของระบบ ปัญหาที่พบ ข้อเสนอแนะ จัดทำเอกสาร และนำเสนอผลโครงงาน

บทที่ 4

ผลการดำเนินงานวิจัย

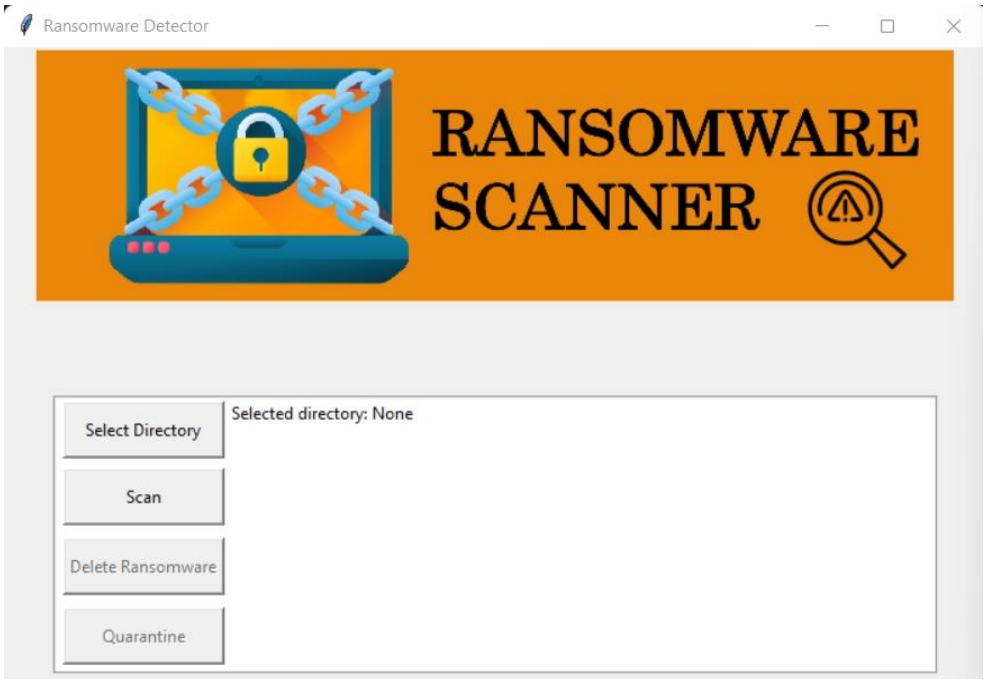
จากการจัดทำระบบการจัดการมัลแวร์เรียกค่าไถ่ พบว่าระบบสามารถทำการตรวจจับไฟล์ที่มีไวรัสเรียกค่าไถ่ รวมถึงกำจัดไฟล์ที่มีการแฝงตัวของไวรัสเรียกค่าไถ่ได้ โดยการเลือกสแกนไฟล์ที่ต้องการตรวจสอบ ระบบจะปฏิบัติการตรวจสอบ และหากไฟล์นั้นมีการแจ้งเตือนการแฝงตัวของไวรัสเรียกค่าไถ่ ผู้ใช้สามารถเลือกกักกันไฟล์เพื่อตรวจสอบความสำคัญของไฟล์ก่อนกำจัดได้ ซึ่งสามารถใช้งานได้ตามวัตถุประสงค์และขอบเขตที่คณะผู้จัดทำได้ตั้งเป้าหมายไว้

4.1 ผลการดำเนินงาน

การจัดทำระบบการจัดการมัลแวร์เรียกค่าไถ่ ได้มีการดำเนินตามที่ระบุขั้นตอนในบทที่ 3 โดยใช้โปรแกรม Visual Studio Code และภาษา Python ในการพัฒนาระบบ ซึ่งทำให้ได้ผลการดำเนินงานดังนี้

4.1. หน้าจอการทำงานของระบบ

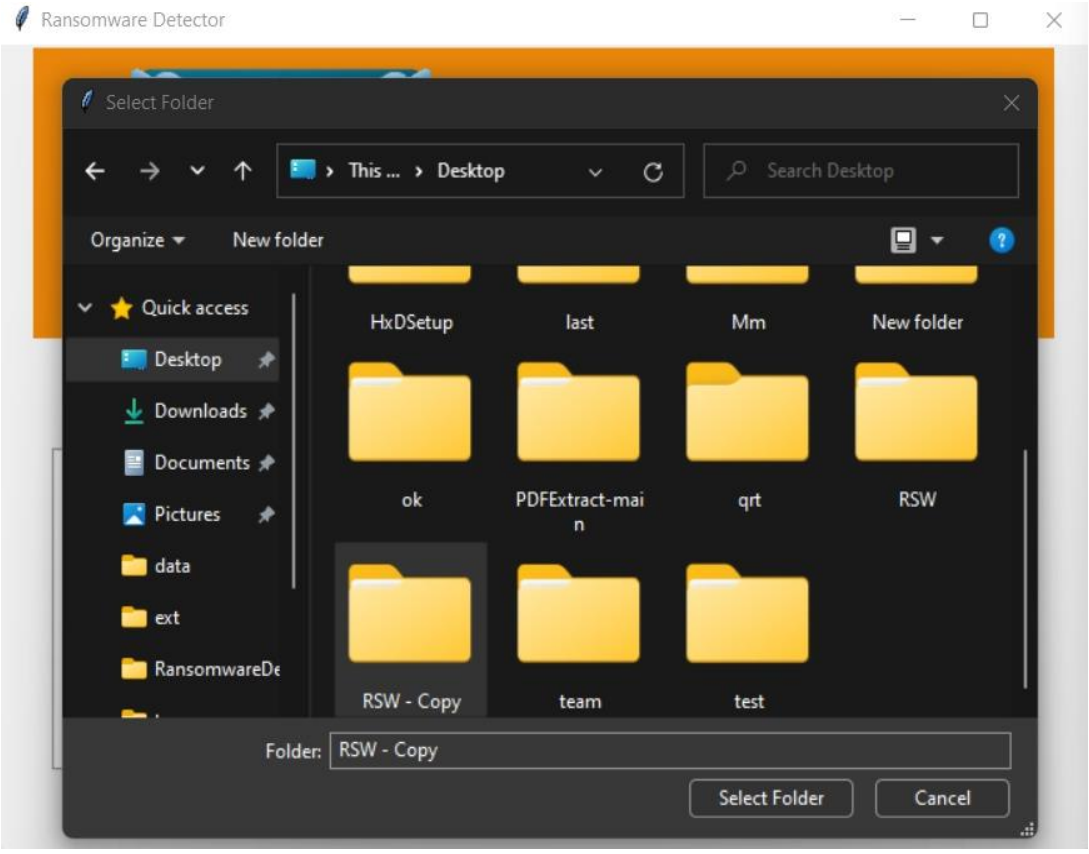
หน้าจอหลักของโปรแกรมจะแสดงปุ่มทั้งหมด 4 ปุ่ม ได้แก่ ‘Select Directory’ Button, ‘Scan’ Button, ‘Delete Ransomware’ Button และ ‘Quarantine’ Button



รูปที่ 7 หน้าจอหลักของโปรแกรม

- Select Directory เป็นปุ่มสำหรับเลือกโฟลเดอร์ที่ต้องการสแกน
- Scan เป็นปุ่มสำหรับการสแกนไฟล์ที่ได้ทำการเลือกมา
- Delete Ransomware เป็นปุ่มสำหรับการเลือกลบไฟล์ที่สแกนเจอไวรัสเรียกค่าไถ่แฝงตัวอยู่
- Quarantine เป็นปุ่มสำหรับกักกันไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่

4.2 เมื่อคลิกที่ปุ่ม Select Directory จะขึ้นหน้าต่างสำหรับเลือกไฟล์ภายในเครื่องของผู้ใช้



รูปที่ 8 แสดงหน้าต่างให้เลือกโฟลเดอร์ภายในเครื่องคอมพิวเตอร์ของผู้ใช้

4.3 เมื่อกดเลือกโฟลเดอร์แล้ว ที่อยู่ของโฟลเดอร์ที่เลือกจะแสดงที่ด้านขวาของปุ่ม

รูปที่ 9 แสดงผลลัพธ์การเลือกโฟลเดอร์

- Souece Code Select Directory

```
self.select_dir_button = tk.Button(frame, text="Select Directory", command=self.select_directory)
self.select_dir_button.place(x=5, y=2)
self.select_dir_button.config(height=2, width=15)

self.select_dir_label = tk.Label(frame, text="Selected directory: None", bg="white", wraplength=500, justify="left")
self.select_dir_label.place(x=122, y=0)
```

```
def select_directory(self):
    self.selected_dir = filedialog.askdirectory()
    self.select_dir_label.config(text="Selected directory: {}".format(self.selected_dir))
```

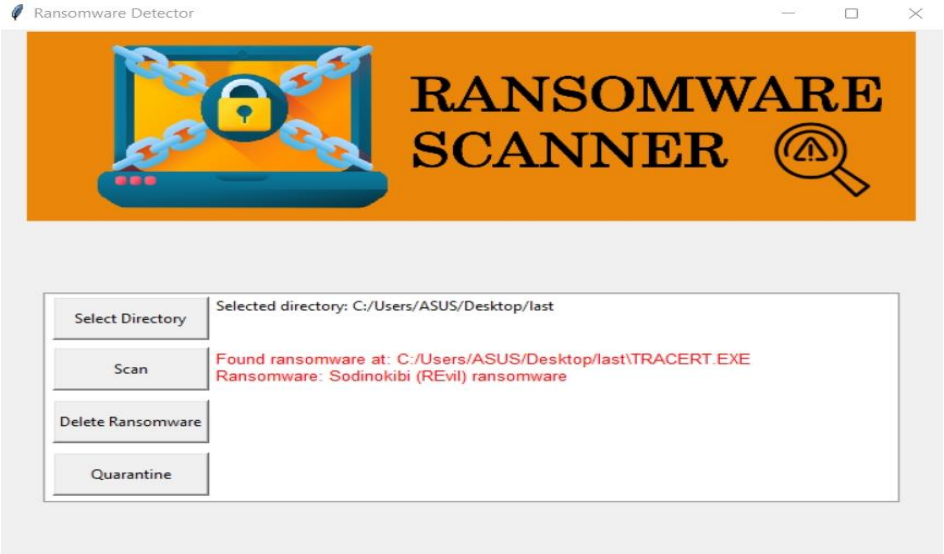
รูปที่ 10 Source Code Select Directory (2)

4.4 เมื่อเลือกโฟลเดอร์ที่ต้องการสแกนเรียบร้อยแล้ว ให้ทำการสแกนโดยคลิกที่ปุ่ม Scan เพื่อเริ่มการสแกน ซึ่งหากผู้ใช้กดปุ่ม Scan โดยที่ยังไม่ได้มีการเลือกโฟลเดอร์ โปรแกรมจะแสดงแจ้งเตือนให้เลือกโฟลเดอร์ที่ต้องการสแกนก่อน และหากโฟลเดอร์ที่สแกนไม่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ จะแสดงข้อความเป็น “Ransomware not found”

รูปที่ 11 โปรแกรมาแจ้งเตือนให้เลือกโฟลเดอร์ที่ต้องการสแกนก่อน

รูปที่ 12 ผลลัพธ์แสดงการสแกนโฟลเดอร์ที่ไม่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่

ในกรณีที่สแกนโฟลเดอร์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ จะแสดงข้อความเป็น “Found ransomware” ตามด้วยที่อยู่ของไฟล์นั้น และชื่อของไวรัสเรียกค่าไถ่ที่อยู่ในไฟล์นั้น



รูปที่ 13 ผลลัพธ์ของการสแกนโฟลเดอร์ที่มีไวรัสเรียกค่าไถ่

- Source Code Scan

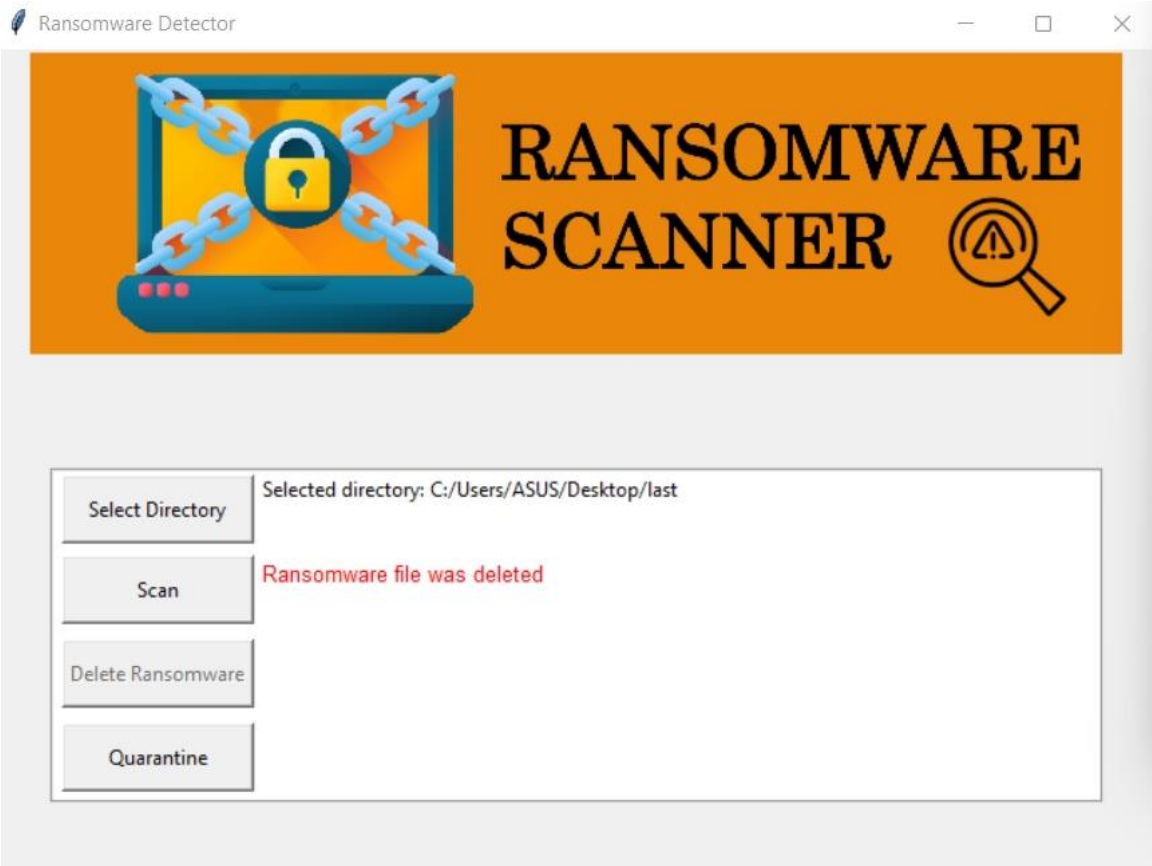
```
self.scan_button = tk.Button(frame, text="Scan", command=self.scan_directory)
self.scan_button.place(x=5, y=50)
self.scan_button.config(height=2, width=15)
```

รูปที่ 14 Source Code Scan (1)

```
def scan_directory(self):
    # Check if a directory has been selected
    if self.selected_dir is None:
        messagebox.showerror("Error", "Please select a directory to scan")
        return

    self.ransomware_found = False

    # Traverse the selected directory and its subdirectories and check each file for ransomware signatures
    for root, dirs, files in os.walk(self.selected_dir):
        for file in files:
            file = os.path.join(root, file)
            with open(file, 'rb') as f:
                contents = f.read()

                for signature ,ransomware_name in RANSOMWARE_SIGNATURES.items():
                    if signature in contents:
                        self.ransomware_found = True
                        self.result_label.config(text="Found ransomware at: {}\nRansomware: {}".format(file, ransomware_name), font=("Helvica", 10), fg = "red")
                        self.delete_button.config(state="normal")
                        self.quarantine_button.config(state="normal")
                        return

                    if not self.ransomware_found:
                        self.result_label.config(text="Ransomware not found", font=("Helvica", 10), fg = "blue")
                        self.delete_button.config(state="disabled")
                        self.quarantine_button.config(state="disabled")
```

รูปที่ 15 Source Code Scan(2)

4.5 จากนั้น หากผู้ใช้ต้องการเลือกลบไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ สามารถเลือกคลิกที่ปุ่มลบได้ทันที ซึ่งปุ่ม Delete Ransomware จะสามารถใช้งานได้ก็ต่อเมื่อเจอไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่เท่านั้น ซึ่งเมื่อผู้ใช้คลิกที่ปุ่ม Delete Ransomware แล้วสามารถทำการกำจัดไฟล์ไวรัสเรียกค่าไถ่ได้เสร็จสิ้น จะแสดงข้อความที่ด้านขวาของปุ่มเป็น “ Ransomware file was deleted”



รูปที่ 16 แสดงผลลัพธ์การกำจัดไฟล์ได้สำเร็จ

- Source code Delete Ransomware

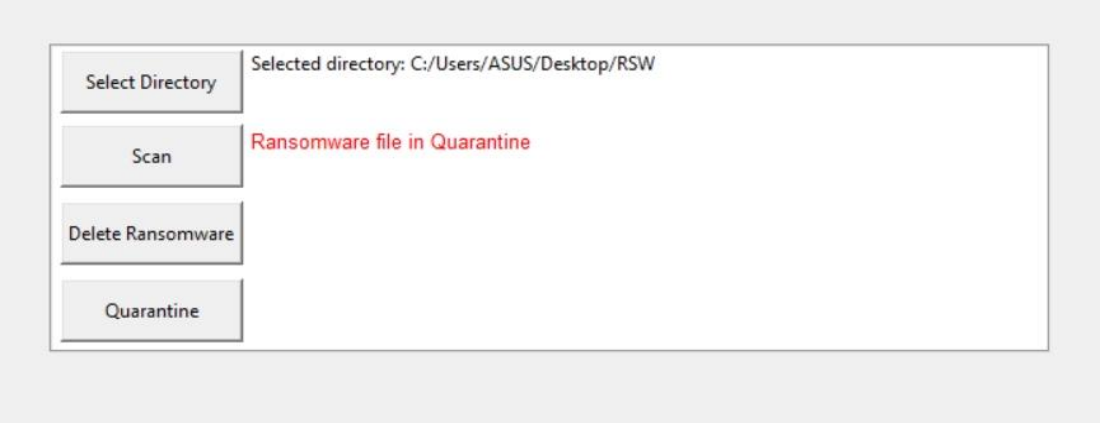
```
self.delete_button = tk.Button(frame, text="Delete Ransomware", command=self.delete_ransomware, state="disabled")
self.delete_button.place(x=5, y=100)
self.delete_button.config(height=2, width=15)
```

รูปที่ 17 Source Code Delete Ransomware (1)

```python
def delete_ransomware(self):
    if not self.ransomware_found:
        messagebox.showerror("Error", "No ransomware found, cannot delete")
        return

    # Get the file path that was identified as containing ransomware
    ransomware_file = self.result_label.cget("text").split("\n")[0].split(": ")[1]

    # Delete the ransomware file
    try:
        os.remove(ransomware_file)
        self.result_label.config(text="Ransomware file was deleted")
        self.delete_button.config(state="disabled")
        return
    except PermissionError:
        self.result_label.config(text="Access denied, cannot delete ransomware file")
    except FileNotFoundError:
        self.result_label.config(text="Ransomware file not found")
        self.delete_button.config(state="disabled")
```

รูปที่ 18 Source Code Delete Ransomware (2)

4.6 ในกรณีที่ผู้ใช้งานยังไม่ต้องการกำจัดไฟล์ที่มีการแฝงตัวของไวรัสเรียกค่าไถ่ที่สแกนเจอ เพื่อการตรวจสอบความสำคัญของไฟล์ที่สแกนเจอไวรัสเรียกค่าไถ่ สามารถเลือกกดปุ่ม Quarantine เพื่อกักกันไฟล์ไว้ก่อนทำการลบในภายหลังได้ โดยที่ปุ่มจะสามารถใช้งานได้ก็ต่อเมื่อสแกนเจอไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ ซึ่งเมื่อผู้ใช้คลิกที่ปุ่ม Delete Ransomware แล้วสามารถทำการกำจัดไฟล์ไวรัสเรียกค่าไถ่ได้เสร็จสิ้น จะแสดงข้อความที่ด้านขวาของปุ่มเป็น “ Ransomware file in Quarantine”



รูปที่ 19 ผลลัพธ์ของการกักกันไฟล์ไวรัสเรียกค่าไถ่ได้สำเร็จ

- Source Code Quarantine

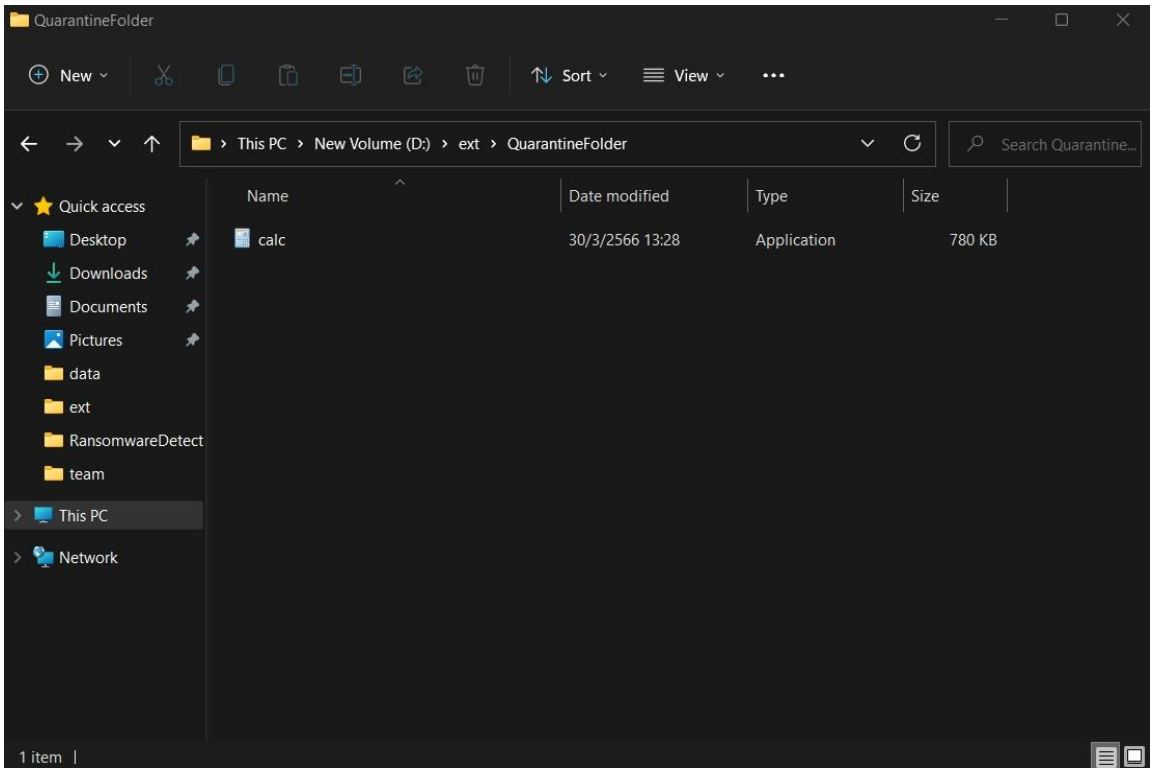
```
self.quarantine_button = tk.Button(frame, text="Quarantine", command=self.quarantine_ransomware, state="disabled")
self.quarantine_button.place(x=5, y=150)
self.quarantine_button.config(height=2, width=15)
```

รูปที่ 20 Source Code Quarantine (1)

```
def quarantine_ransomware(self):
    if self.ransomware_found:
        for root, dirs, files in os.walk(self.selected_dir):
            for file in files:
                file_path = os.path.join(root, file)
                with open(file_path, 'rb') as f:
                    contents = f.read()
                for signature in RANSOMWARE_SIGNATURES:
                    if signature in contents:
                        dst_dir = r"D:\ext\QuarantineFolder"
                        os.makedirs(dst_dir, exist_ok=True)
                        dst_file_path = os.path.join(dst_dir, file)
                        try:
                            shutil.move(file_path, dst_file_path)
                            self.result_label.config(text="Ransomware file in Quarantine")
                        except PermissionError:
                            self.result_label.config(text="Access denied, cannot Quarantine ransomware file")
                            self.delete_button.config(state="disabled")
                            self.quarantine_button.config(state="disabled")
                        return
        self.result_label.config(text="Ransomware file not found")
        self.delete_button.config(state="disabled")
        self.quarantine_button.config(state="disabled")
    else:
        messagebox.showerror("Error", "No ransomware found, cannot Quarantine")
        return
```

รูปที่ 21 Source Code Quarantine (2)

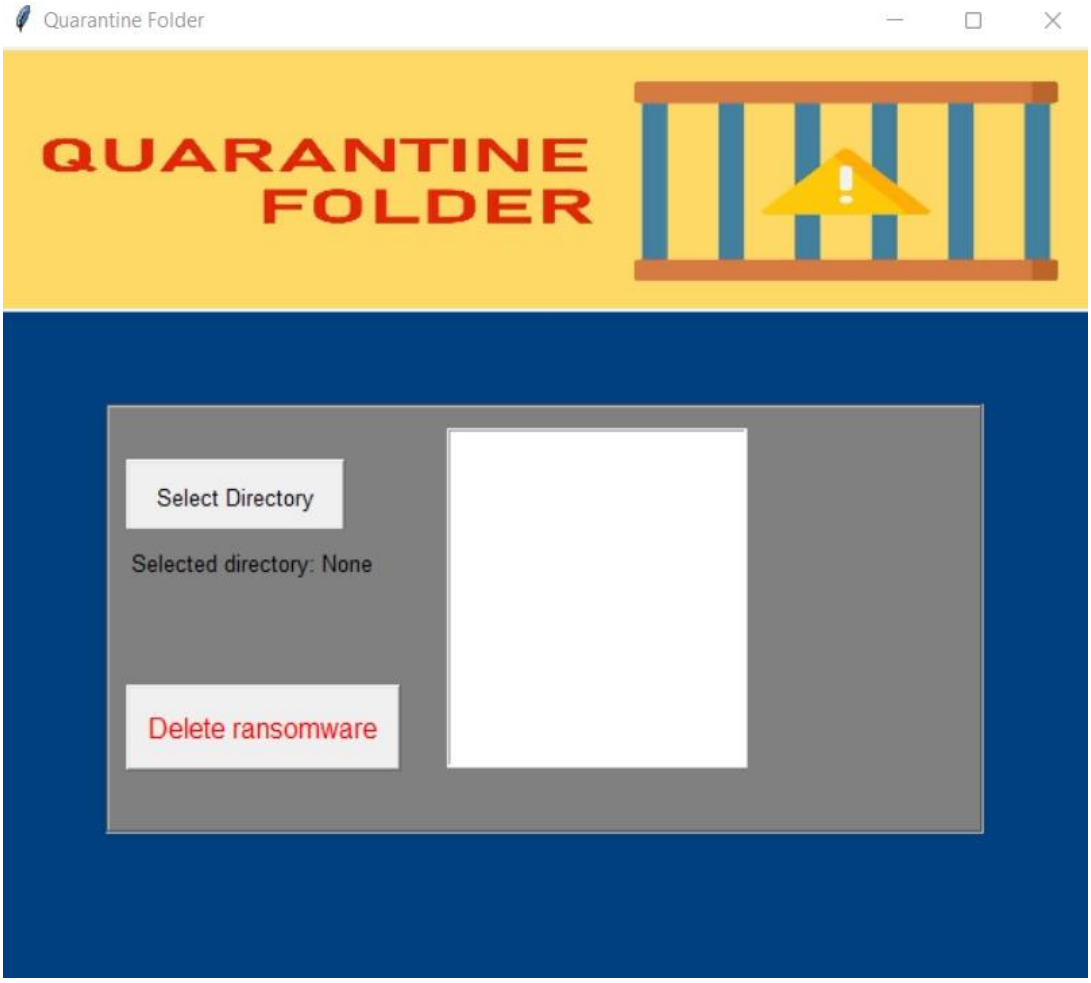
และเมื่อทำการกักกักไฟล์เรียบร้อยแล้ว ไฟล์นั้นจะย้ายไปอยู่ที่โฟลเดอร์ QuarantineFolder



*รูปที่ 22 แสดงผลลัพธ์การกักกันไฟล์ไปไว้ที่โฟลเดอร์ **QuarantineFolder***

4.7 เมื่อผู้ใช้กักกันไฟล์เสร็จสิ้นแล้ว หากต้องการตรวจสอบและทำการกำจัดสามารถทำได้โดยเข้าไปที่ระบบโฟลเดอร์ QuarantineFolder ซึ่งหน้าจอหลักของโปรแกรมจะมีปุ่มทั้งหมด 2 ปุ่มคือ “Select Directory” Buttton และ “Delete ransomware” Button

- หน้าจอหลักของระบบกักกันไฟล์ไวรัสเรียกค่าไถ่

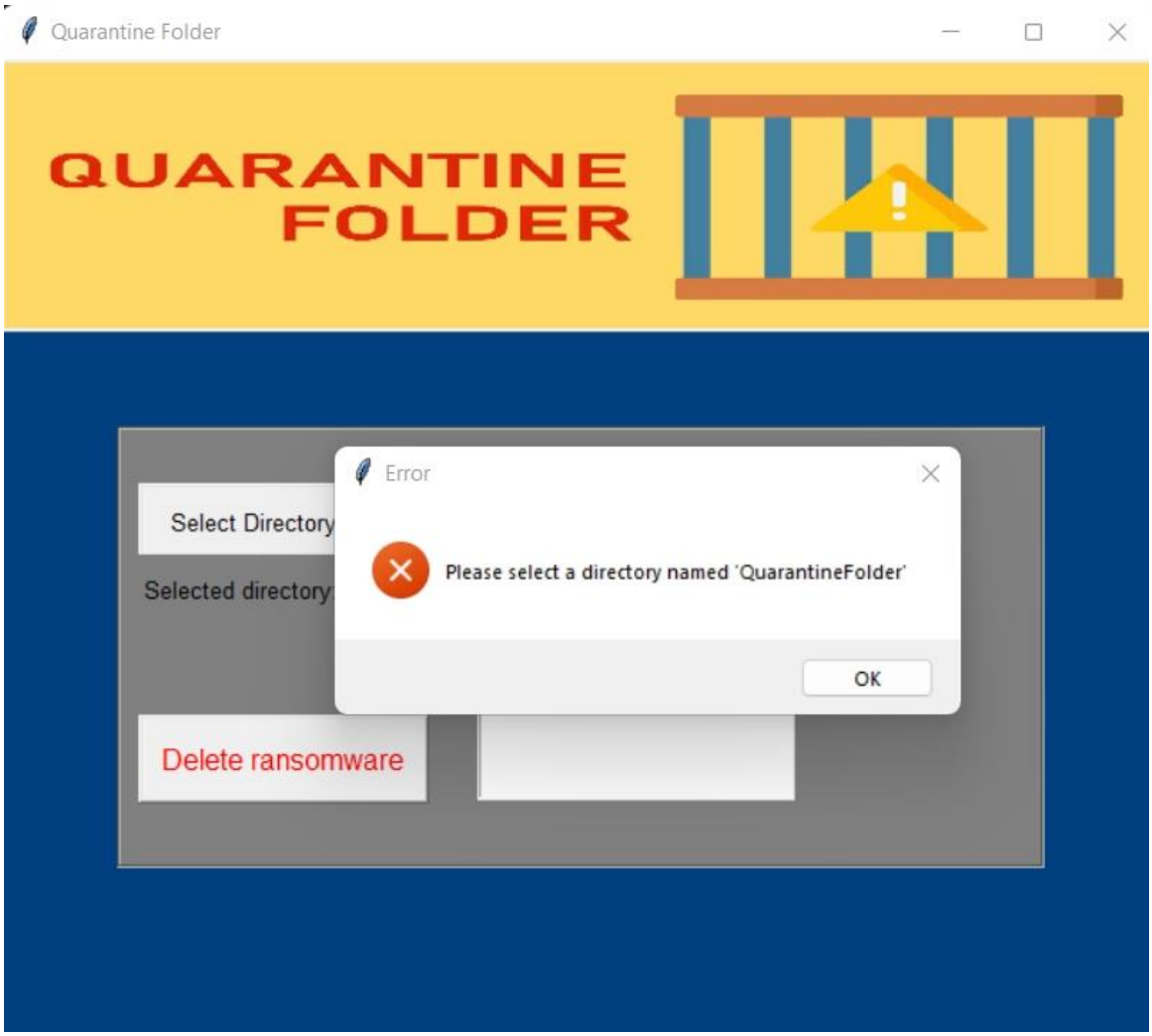


รูปที่ 23 หน้าจอหลักของระบบกักกันไฟล์ไวรัสเรียกค่าไถ่

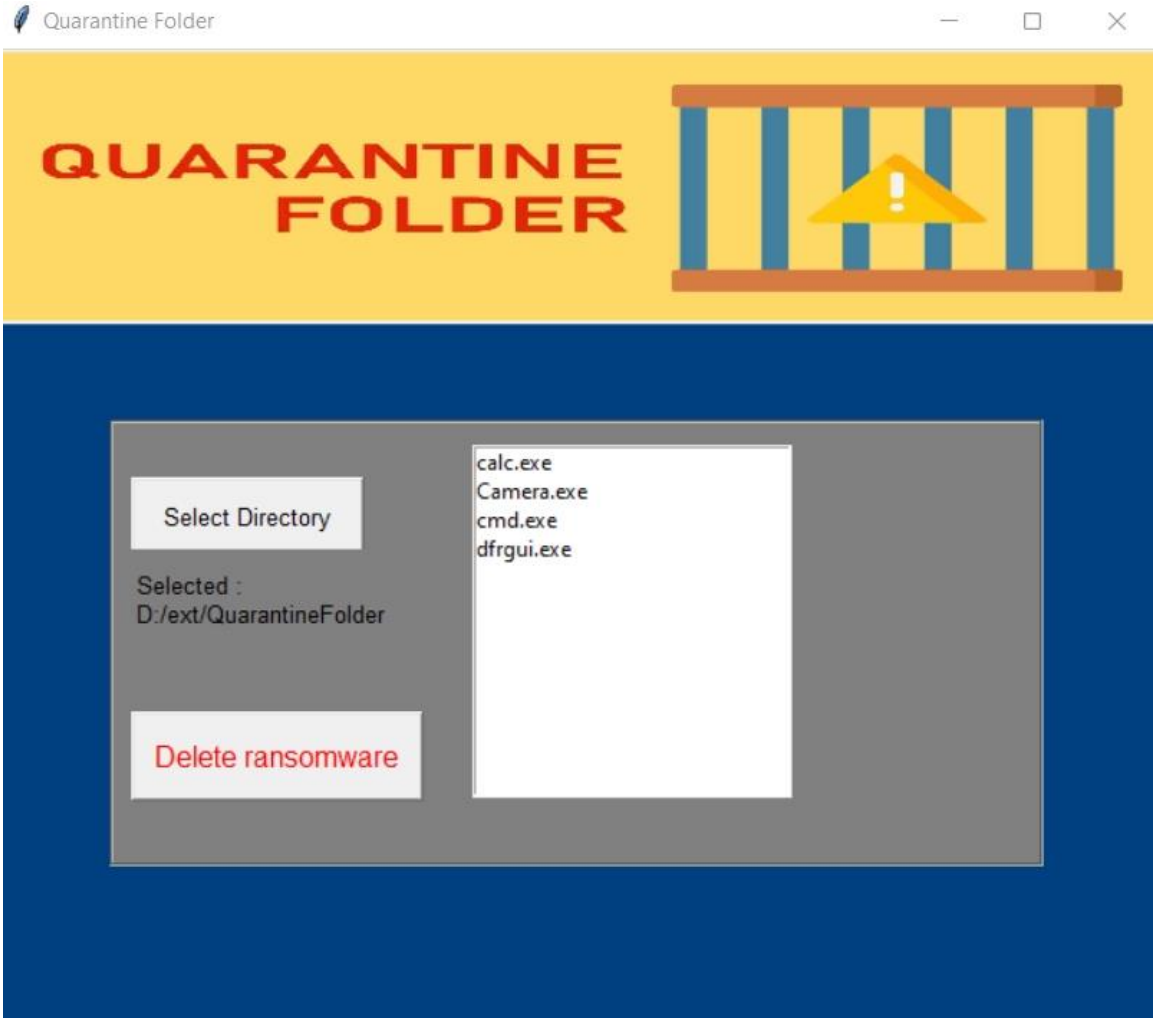
หลักการใช้งานของปุ่มมีดังนี้

- Select Directory เลือกโฟลเดอร์เพื่อเปิดดูรายการไฟล์ทั้งหมดภายในโฟลเดอร์
- Delete ransomware กำจัดไฟล์ที่เลือกภายในโฟลเดอร์

4.8 เมื่อผู้ใช้ทำการคลิกไปที่ปุ่ม Selec Directory จะแสดงหน้าต่างให้ผู้ใช้งานเลือโฟลเดอร์ที่ต้องการดูรายการไฟล์ ซึ่งจะสามารถเลือกได้เฉพาะโฟลเดอร์ “QuarantineFolder” เท่านั้น หากเลือกโฟลเดอร์อื่น จะแสดงกล่องข้อความแจ้งเตือนเป็น “Please select a directory named 'QuarantineFolder' " แต่หากเลือกเป็น QuarantineFolder โปรแกรมจะแสดงรายการไฟล์ในโฟลเดอร์ทันที



รูปที่ 24โปรแกรม แสดงผลลัพธ์การเลือกโฟลเดอร์อื่น



*รูปที่ 25 โปรแกรมแสดงผลลัพธ์ในการเลือกโฟลเดอร์ **QuarantineFolder***

โดยรายการไฟล์ที่แสดงภายในโฟลเดอร์ QuarantineFolder นั้นเป็นไฟล์ทั้งหมดที่ผู้ใช้ได้ทำการกักกันเอาไว้ ในกรณีที่ผู้ใช้งานต้องการตรวจสอบความสำคัญของไฟล์ก่อนทำการกำจัด

- Source Code Select Directory

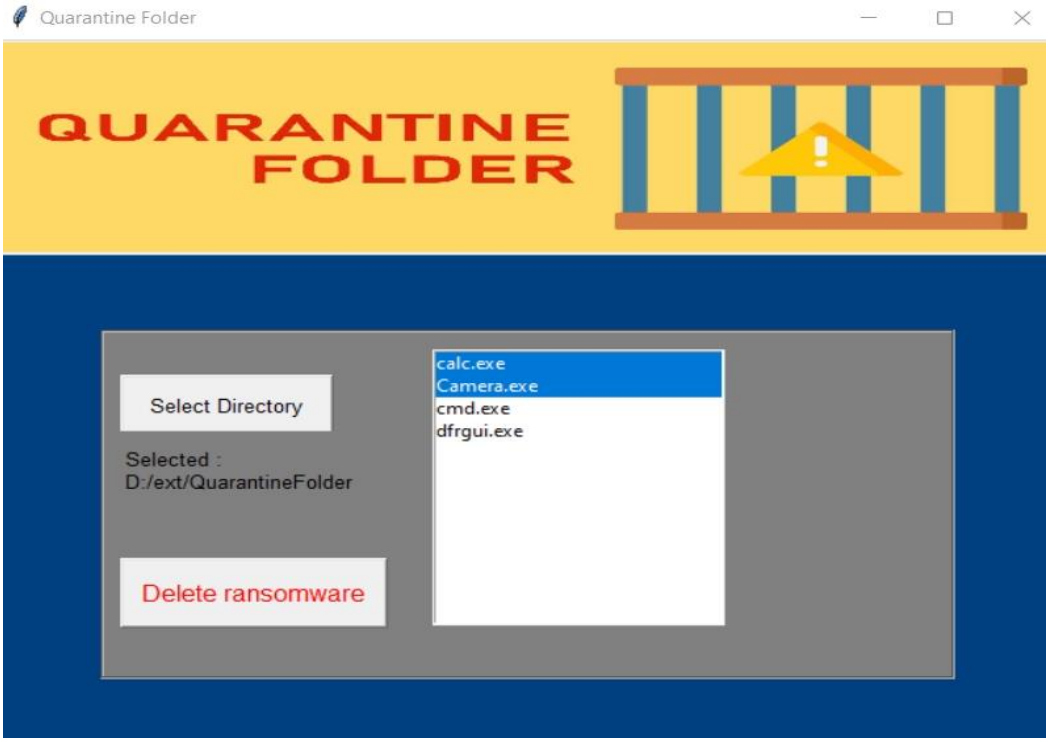
```
self.select_dir_button = tk.Button(frame, text="Select Directory", command=self.select_directory, font=("Helvica", 10))
self.select_dir_button.place(x=10, y=30)
self.select_dir_button.config(height=2, width=15)

self.select_dir_label = tk.Label(frame, text="Selected directory: None", pady=10, font=("Helvica", 10),bg = "grey", wraplength=150, justify="left")
self.select_dir_label.place(x=10, y=70)
```

รูปที่ 26 Source Code Select Directory (1)

```
def select_directory(self):
# Open a file dialog to select a directory
    folder_path = filedialog.askdirectory()

    # Check if the selected directory matches the desired name
    if os.path.basename(folder_path) != 'QuarantineFolder':
        messagebox.showerror("Error", "Please select a directory named 'QuarantineFolder'")
        return

    # Update the label with the selected directory
    self.select_dir_label.config(text="Selected : {}".format(folder_path))

    # Clear the file list
    self.file_list.clear()
    self.listbox.delete(0, tk.END)

    # Get a list of all the files in the directory
    files = os.listdir(folder_path)

    # Add each file to the listbox
    for file in files:
        file_path = os.path.join(folder_path, file)
        self.file_list.append(file_path)
        self.listbox.insert(tk.END, file)
```

รูปที่ 27 Source Code Directory (2)

4.9 เมื่อหน้าโปรแกรมแสดงรายการไฟล์แล้ว ผู้ใช้สามารถเลือกไฟล์ที่ต้องการกำจัด ซึ่งสามารถเลือกลบได้มากกว่าหนึ่งไฟล์ตามความต้องการ



รูปที่ 18 แสดงการเลือกไฟล์ที่สามารถเลือกได้มากกว่าหนึ่งไฟล์

- Source Code listbox

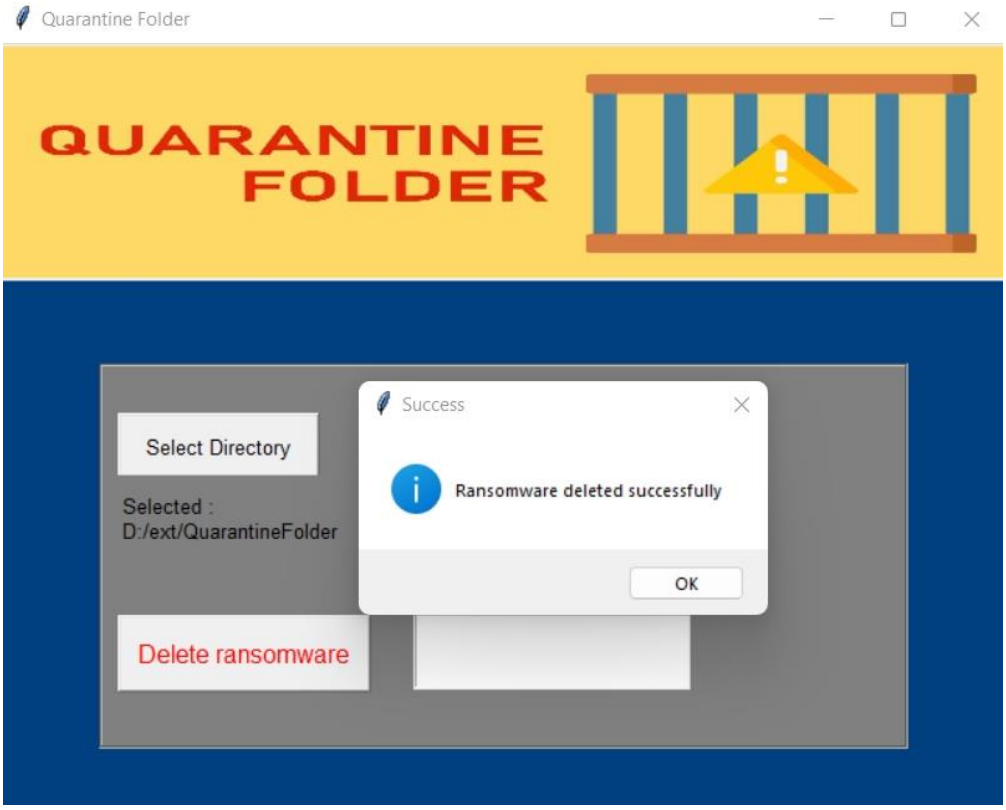
```
self.listbox = tk.Listbox(frame, selectmode=tk.MULTIPLE, width=29, height=12)
self.listbox.place(x=200, y=12)
```

รูปที่ 29 Source Code listbox (1)

```python
def update_files_list(self):
    self.listbox.delete(0, tk.END)  # clear the listbox
    self.file_list.clear()  # clear the file list
    self.folder_path = self.select_dir_label.cget("text")[11:]  # get the folder path from the label
    files = os.listdir(self.folder_path)
    for file in files:
        file_path = os.path.join(self.folder_path, file)
        self.file_list.append(file_path)
        self.listbox.insert(tk.END, file)
    self.delete_button.config(state="normal")
```

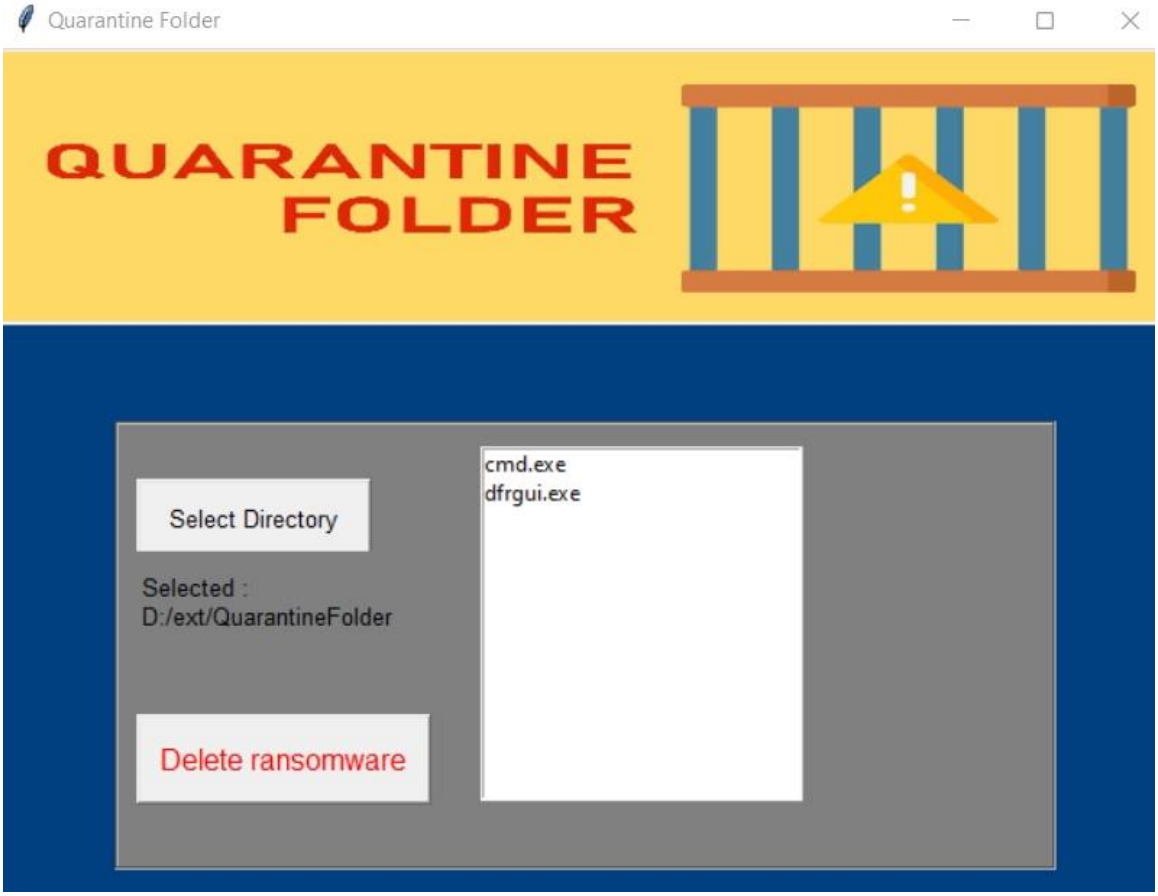
รูปที่ 30 Source Code listbox (2)

4.10 เมื่อเลือกไฟล์ที่ต้องการลบเรียบร้อยแล้ว สามารถคลิกที่ปุ่ม “Delete ransomware” เพื่อกำจัดไฟล์ที่เลือกได้ทันที และเมื่อสามารถกำจัดไฟล์ไวรัสเรียกค่าไถ่ได้สำเร็จจะแสดงกล่องข้อความเพื่อแจ้งเตือนการกำจัดไฟล์ที่สำเร็จ



รูปที่ 31 แสดงการแจ้งเตือนการกำจัดไฟล์สำเร็จ

และหากผู้ใช้งานคลิกปุ่ม OK หน้าโปรแกรมจะทำการ Refresh ที่กล่องข้อความที่แสดงไฟล์ภายในโฟลเดอร์ทันที เพื่อให้ทราบได้ว่าไฟล์ที่เลือกนั้น สามารถกำจัดได้เสร็จสิ้นแล้ว



รูปที่ 32 โปรแกรมแสดงผลลัพธ์ให้ทราบว่าไฟล์ที่เลือกถูกกำจัดเสร็จสิ้นแล้ว

บทที่ 5

สรุปผลโครงงานและข้อเสนอแนะ

ในบทนี้จะกล่าวถึงบทสรุปและข้อเสนอแนะของระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach เพื่อเป็นพื้นฐานที่จะนำไปสู่การพัฒนาต่อไป

5.1 สรุปผลการดำเนินการ

5.2 ปัญหาที่พบในการศึกษา

5.3 ข้อเสนอแนะ

5.1 สรุปผลการดำเนินการ

ระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach มีวัตถุประสงค์เพื่อพัฒนาระบบที่สามารถจัดการระบบความปลอดภัยทางด้านไวรัสเรียกค่าไถ่
และ เพื่อสร้างเครื่องมืออีกทางเลือกในการจัดการกับความปลอดภัยทางด้านไวรัสเรียกค่าไถ่ โดยทำการพัฒนาระบบด้วยภาษา Python บนโปแกรม Microsoft visual studio เพื่อตรวจจับและกำจัดมัลแวร์เรียกค่าไถ่ที่แฝงเข้ามาภายในไฟล์โดยใช้เทคนิค Signature-based คือการตรวจหาไฟล์อันตรายโดยการจับจากรหัส md5hash กลุ่มตัวอย่างที่ผู้จัดทำได้ทำการรวบรวมมาและแปลงให้เป็นค่า binary สำหรับการตรวจจับภายในไฟล์ที่ต้องการทดสอบ และได้ทำการทดสอบการทำงานและประสิทธิภาพของระบบจากไฟล์ตัวอย่างทั้งไฟล์ที่เป็นอันตรายและไฟล์ที่ปลอดภัย

สรุปผลการทดสอบระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach บนระบบปฏิบัติการ Windows ได้ว่าระบบสามารถทำการตรวจจับไฟล์ที่เป็นมัลแวร์เรียกค่าไถ่ได้ โดยการสแกนทีละไฟล์ภายในโฟลเดอร์ที่เลือกเพื่อทำการสแกน หากภายในโฟลเดอร์นั้นมีมากกว่าหนึ่งไฟล์ ระบบก็จะทำการสแกนทีละไฟล์ตามลำดับ หากพบมัลแวร์เรียกค่าไถ่ระบบจะหยุดการสแกนและแสดงที่อยู่ ชื่อ ของไฟล์ดังกล่าว หมายเลข binary และชนิดของมัลแวร์เรียกค่าไถ่ที่พบตามที่ได้กำกับไว้ที่หมายเลข binary ของข้อมูล Signature ตัวอย่าง หลังจากมีการตรวจพบแล้วผู้ใช้สามารถเลือกกักกันไฟล์ไว้ก่อนหรือต้องการลบ หากต้องการลบไฟล์ดังกล่าวก็จะถูกลบออกไปจากระบบ แต่ถ้าหากผู้ใช้ต้องการที่จะกักกันไฟล์ไว้ก่อน ไฟล์ดังกล่าวจะถูกย้ายไปยังโฟล์เดอร์ “Quarantine” หลังจากนั้นก็สามารถทำการลบไฟล์ดังกล่าวได้เช่นกัน โดยการเลือกลบไฟล์จาก List box จากการเลือกเข้าไปยังโฟล์เดอร์

“Quarantine” ก็จะสามารถเลือกไฟล์อันตรายที่ต้องการและเลือกดำเนินการลบออกจากเครื่องคอมพิวเตอร์ได้ทันที ตามความต้องการของผู้ใช้งานบนระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach ที่สามารถใช้งานได้ง่ายและสะดวก

5.2 ปัญหาที่พบในการศึกษา

5.2.1 จากการพัฒนาระบบตรวจจับภัยคุกคามทางความมั่นคงปลอดภัยทางไซเบอร์ รูปแบบ Data breach ระบบยังไม่สามารถตรวจจับมัลแวร์เรียกค่าไถ่ได้ทุกชนิด

5.2.2 หลังจากเลือกลบไฟล์ในList Box ของหน้าQuarantine สำเร็จแล้ว รายการชื่อไฟล์ในList Box จะยังไม่ทำการอัพเดตเป็นปัจจุบัน ต้องเลือกDirectoryใหม่ รายการชื่อไฟล์ใน List Box จึงจะอัพเดต

5.2.3 หากโฟลเดอร์ที่เลือกเพื่อทำการสแกน มีโฟลเดอร์อยู่ภายใน การทำงานก็จะช้าตามปริมาณของโฟล์เดอร์ภายในโฟลเดอร์นั้นเว้นแต่ว่าไฟล์อันตรายที่มีมัลแวร์เรียกค่าไถ่จะเป็นไฟล์แรกๆที่ตรวจเจอ

5.3 ข้อเสนอแนะ

5.3.1 พัฒนาระบบให้การตรวจสอบbinary ทำได้จากการดึงข้อมูลได้จาก csv ไฟล์เพื่อง่ายต่อการอัพเดตข้อมูล Ransomware Signature ต่อไป

5.3.2 ใช้ Model Machine Learning ในการพัฒนาระบบการตรวจจับ เพื่อให้สามารถวิเคราะห์มัลแวร์เรียกค่าไถ่ที่ไม่มีในฐานข้อมูลได้จากการ train และ test ของModel Machine Learning

5.3.3 ปรับปรุงและออกแบบการใช้งานและหน้าGUIของระบบให้มีความทันสมัยมากขึ้น

บรรณานุกรม

[1] คริชณะ ฉิมมณี และ มณีสุข โชติรุ่งรัตน์“แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ในเขตพื้นที่พุทธสถาน กรณีศึกษาเมสแก๊งA Guideline for Ransomware Detection and Prevention at the Buddhist Places : A case study of Maze Gang,” [ออนไลน์]. เข้าถึงได้จาก: https://so04.tci-thaijo.org/index.php/JMA/article/view/250039/173621 [สืบค้นเมื่อ 5 มีนาคม 2566]

[2] ญาณพล ยั่งยืน และ อัศว์ณุต แสงทองดี “แนวทางการรับมือและการรับแจ้งเหตุของตำรวจต่อกรณีมัลแวร์เรียกค่าไถ่,” [ออนไลน์]. เข้าถึงได้จาก: https://so02.tci-thaijo.org/index.php/sahasart/article/view/245102 [สืบค้นเมื่อ 5 มีนาคม 2566]

[3] Akashdeep Bhardwaj , Vinay Avasthi, Hanumat Sastry and G. V. B. Subrahmanyam“Ransomware Digital Extortion: A Rising New Age Threat,”. [ออนไลน์]. เข้าถึงได้จาก: https://d1wqtxts1xzle7.cloudfront.net/55107670/01_Published_Paper__1_Ransomware_Digital_Extortion_A_Rising_New_Age_Threat_INDJST-libre.pdf?1511615379=&response-content-disposition=inline%3B+filename%3DRansomware_Digital_Extortion_A_Rising_Ne.pdf&Expires=1680179509&Signature=H7VbuYNrQ6gCnY7THELX0kNKtAo-o1kSL9kAa3sex5DzbMFcSMIQyaznB852iR9UY5Htox3Nsi0JwiGuKRJyKmKZlFkz0AE6rGup-4JTiCA1l630vFWqODmdvd8e~Y-c9XeehwTHrc9bQThx5Ryv7DdI6pJHHj75zQzPFfPCOTgn36dlWFBKZANEKyqt7Rs7cwlcpD6kE2Bnwx3Tp9EJAynjezEi3jS3izm-j6KzhrGdARa-8UBCQe8t8~M5R9cBdhfpU79G1oHvO22DXNYP2tGwDVd6L0e4i-CvTK5kGT8mw7PqGg833AhFWMSCYMRjMV9Fcm6A4SPLUn2CN9~log__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA [สืบค้นเมื่อ 3 มีนาคม 2566]

[4] Amazon Web Services. “ Python คืออะไร,” [ออนไลน์]. เข้าถึงได้จาก: https://aws.amazon.com/th/what-is/python/ [สืบค้นเมื่อ 20 มีนาคม 2566]

[5] Mohammad Bagher Bahador, Mahdi Abadi and Asghar Tajoddin. “HLMD: a signature-based approach to hardware-level behavioral malware detection and

classification," [ออนไลน์]. เข้าถึงได้จาก: https://link.springer.com/article/10.1007/s11227-019-02810-z [สืบค้นเมื่อ 11 มีนาคม 2566]

[6] Trend Micro. " Ransomware Definition," [ออนไลน์] เข้าถึงได้จาก: trendmicro.com/vinfo/ph/security/definition/ransomware/ [สืบค้นเมื่อ 20 มีนาคม 2566]

[7] Visual Studio. "Visual Studio,". [ออนไลน์]. เข้าถึงได้จาก: http://blog.bru.ac.th/wp-content/uploads/bp-attachments/10774/Chapter-1.pdf [สืบค้นเมื่อ 20 มีนาคม 2566]

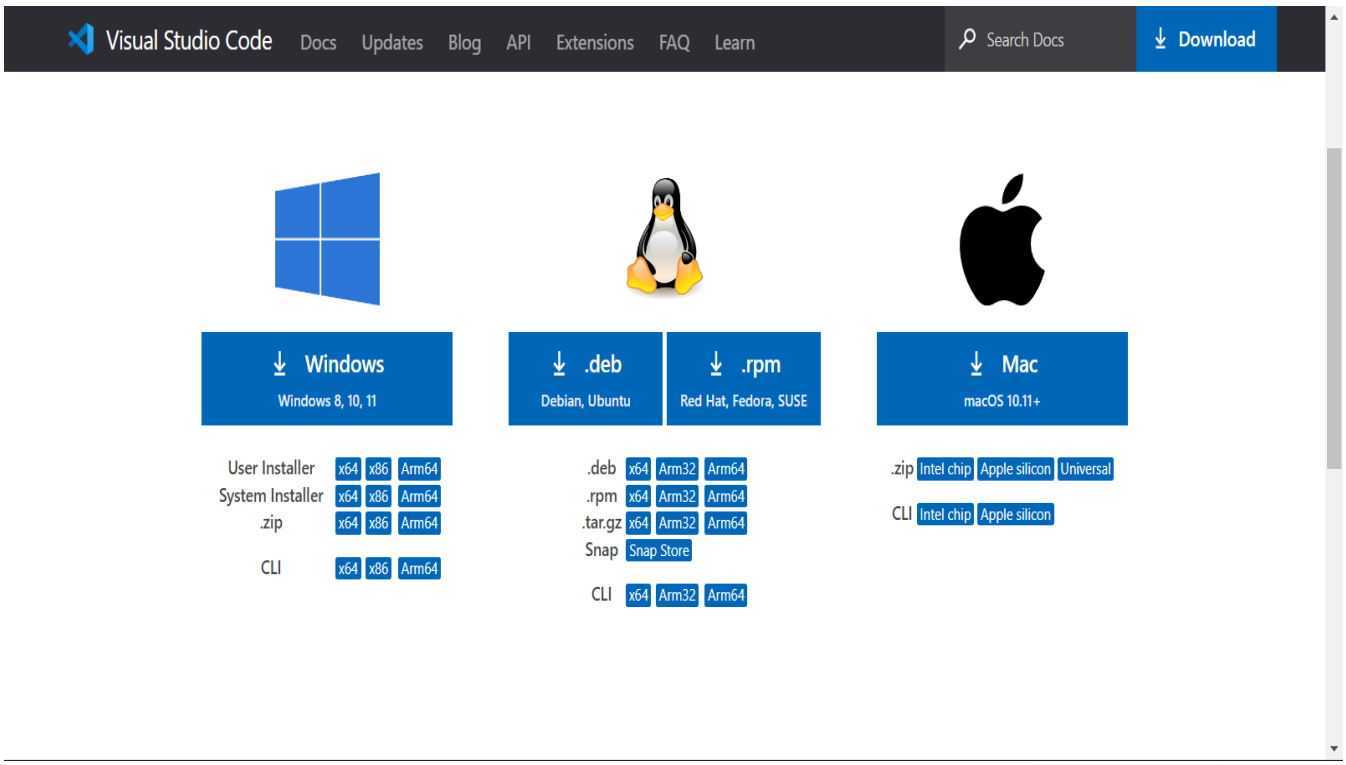
ภาคผนวก

ภาคผนวก ก

ขั้นตอนการติดตั้งโปรแกรม Visual Studio Code

เข้าไปที่เว็บไซต์ของ Visual Studio Code แล้วเลือก Downloads จะแสดงหน้าให้เลือกการติดตั้ง

ให้เลือกตามระบบปฏิบัติการของผู้ใช้ และรอให้การติดตั้งเสร็จสิ้น

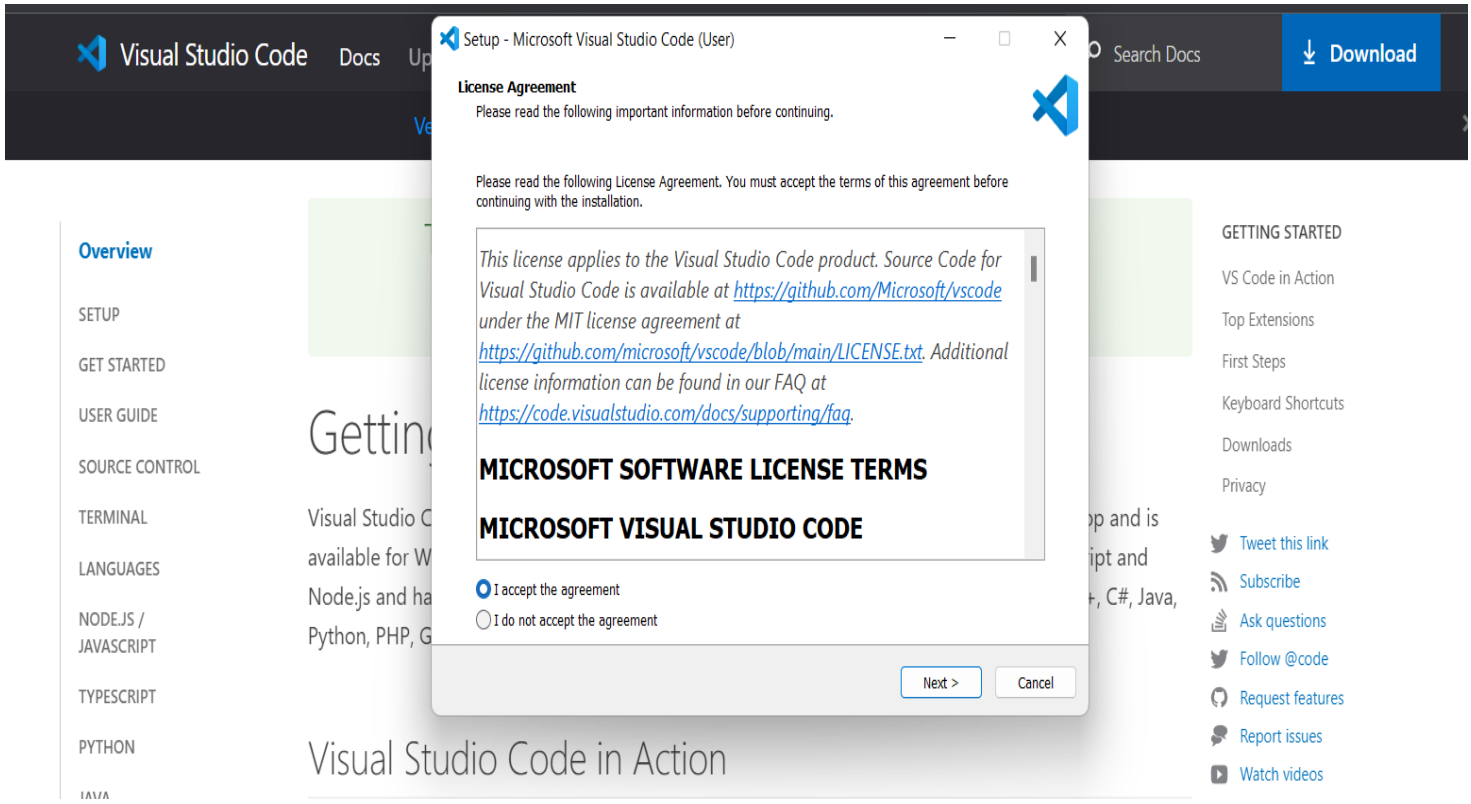


รูปที่ 33 หน้าเว็บไซต์แสดงให้เลือกการติดตั้ง

เมื่อติดตั้งเสร็จสิ้น จะแสดงหน้าสอบถามการยอมรับเงื่อนไข

ให้เลือก ‘accept the agreement’

แล้วคลิก Next

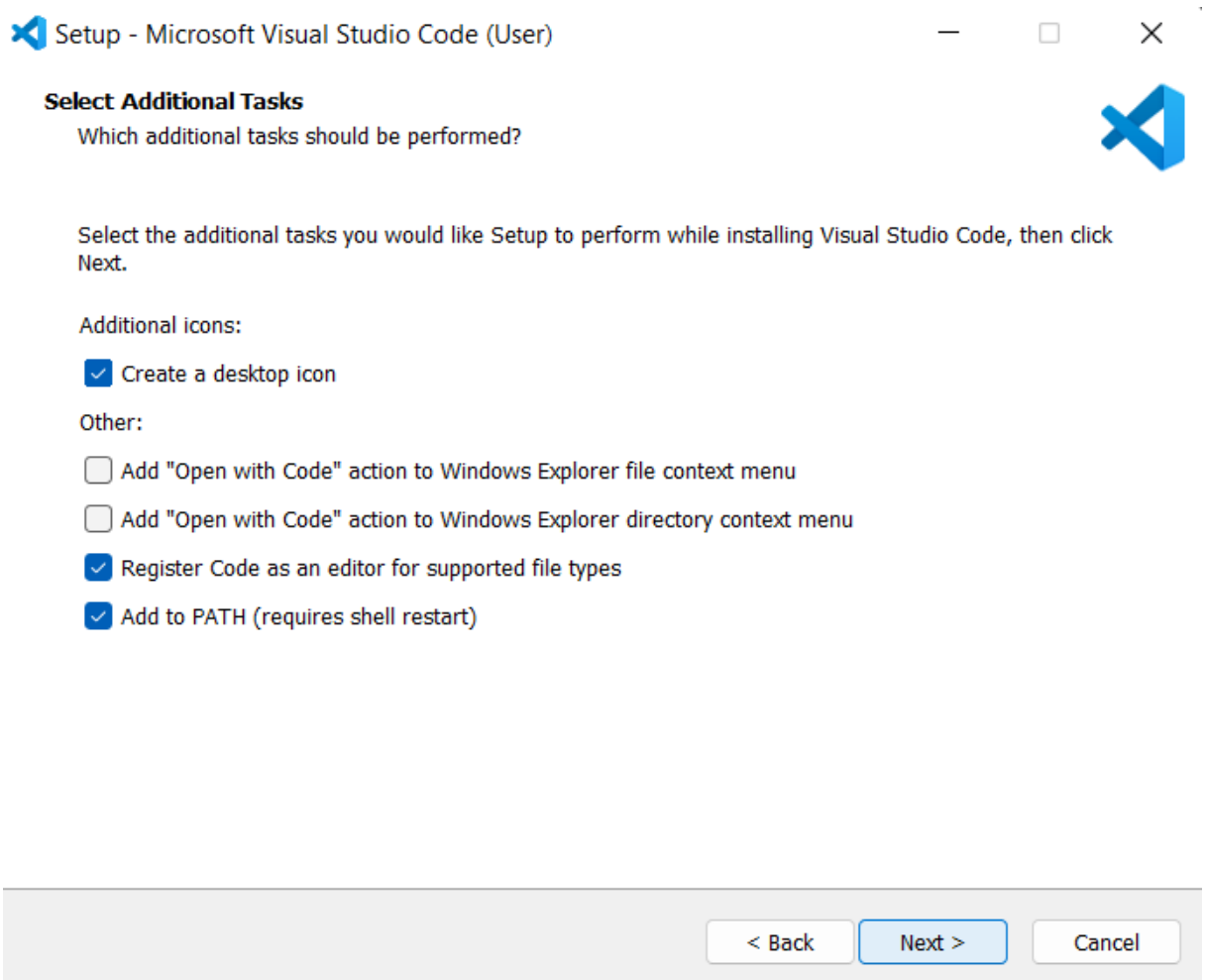


รูปที่ 34 สอบถามการยอมรับเงื่อนไข

จะขึ้นหน้าต่าง Setup

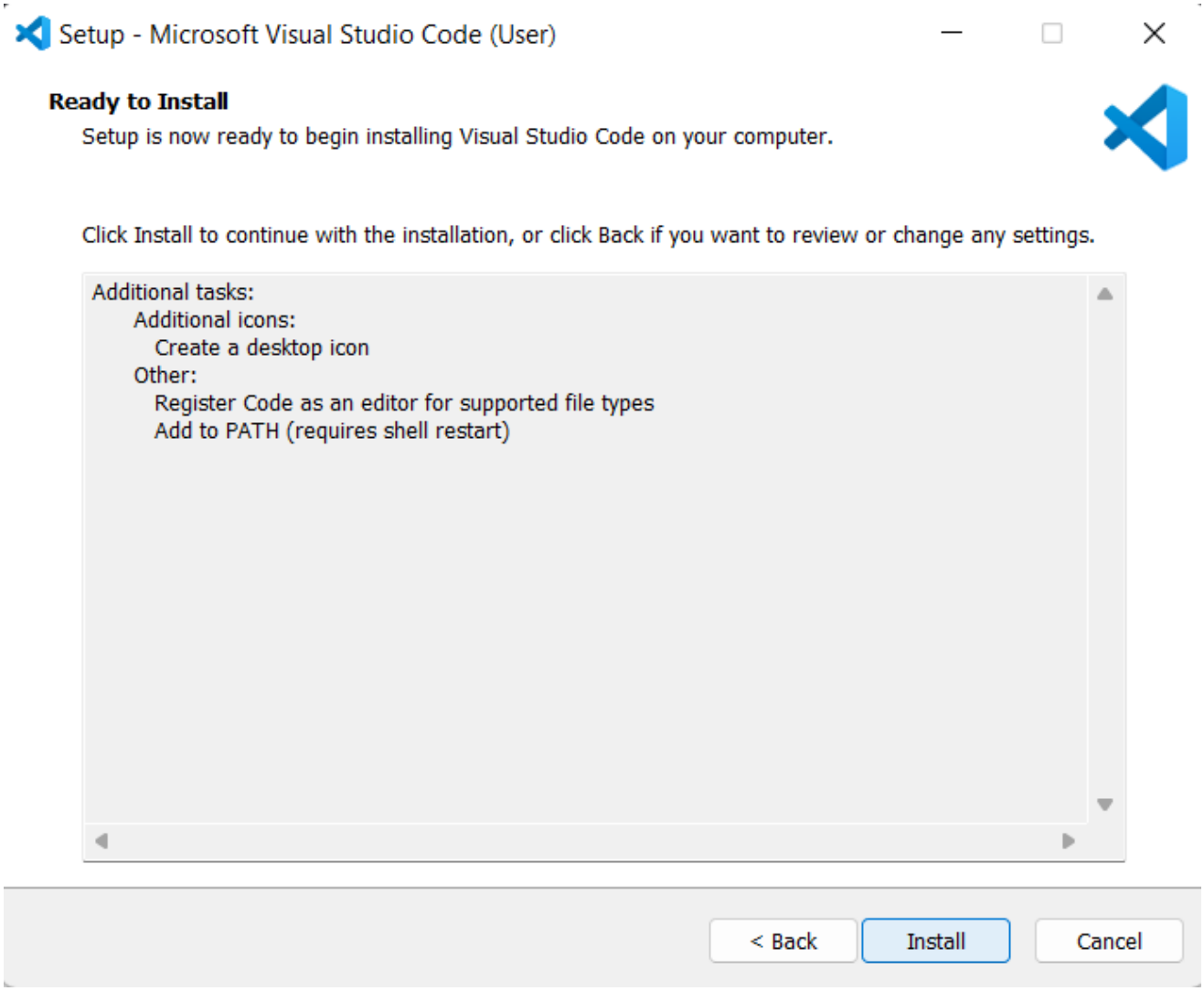
เลือก ‘Create a desktop icon’ เพื่อสร้างทางลัดสำหรับเข้าโปรแกรม และตรวจสอบให้แน่ใจว่า "Add to PATH" ได้ถูกเลือก

หลังจากนั้นคลิก "Next"



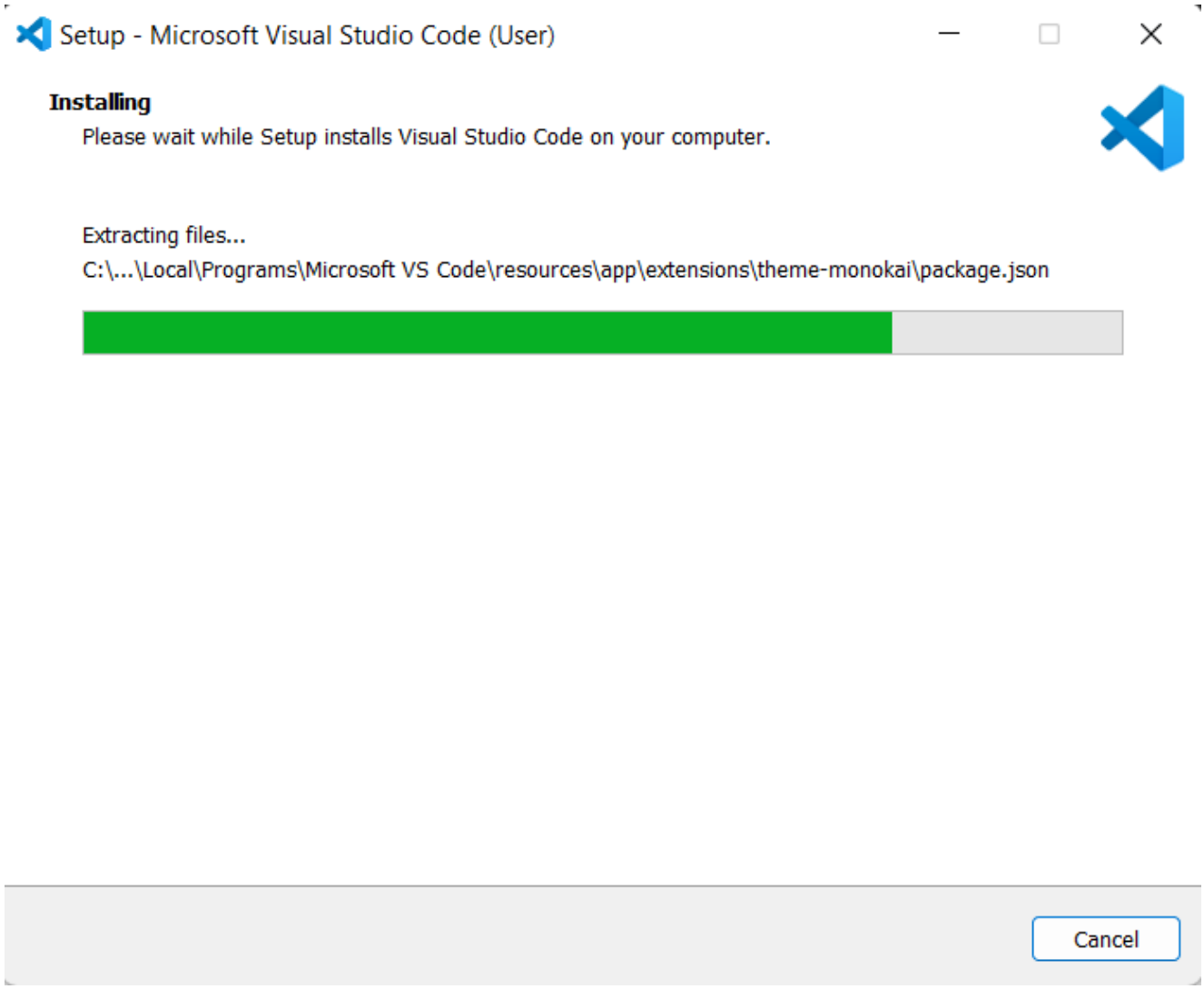
รูปที่ 35 แสดงหน้าต่าง Setup

คลิก ‘Install’



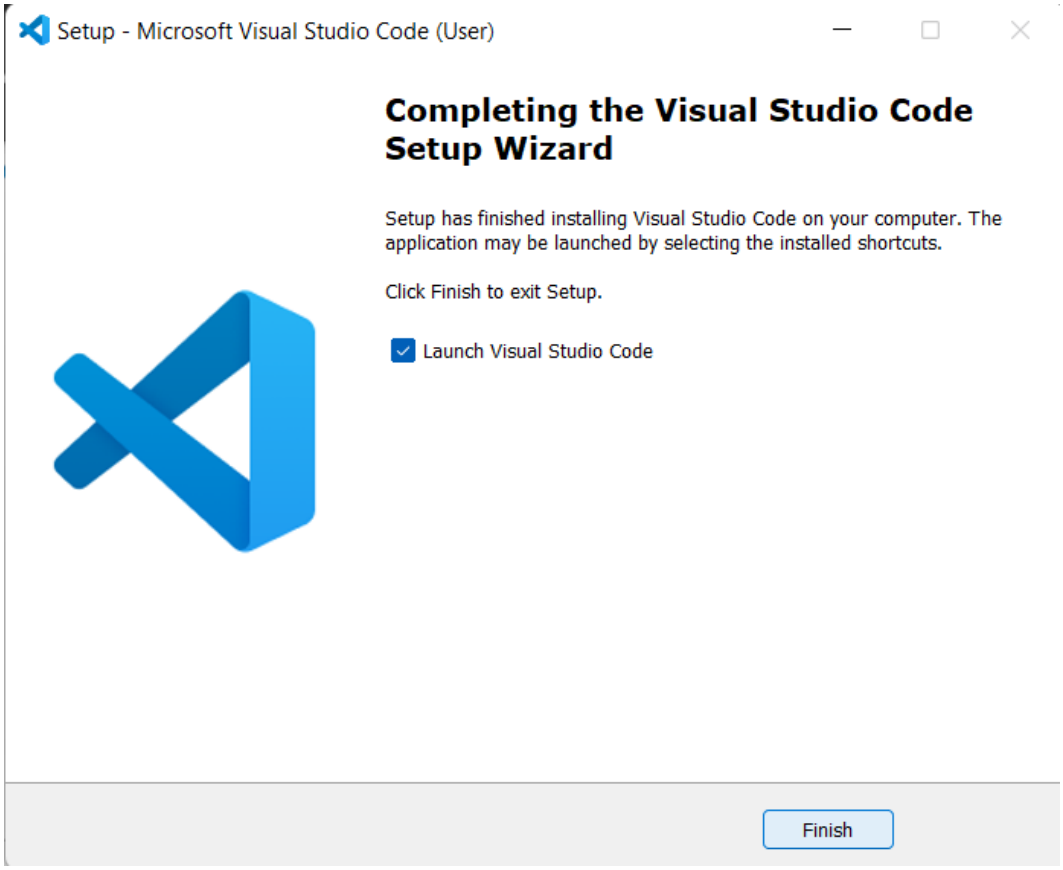
รูปที่ 36 หน้าต่างแสดงความพร้อมในการติดตั้ง

รอให้การติดตั้งเสร็จสิ้น



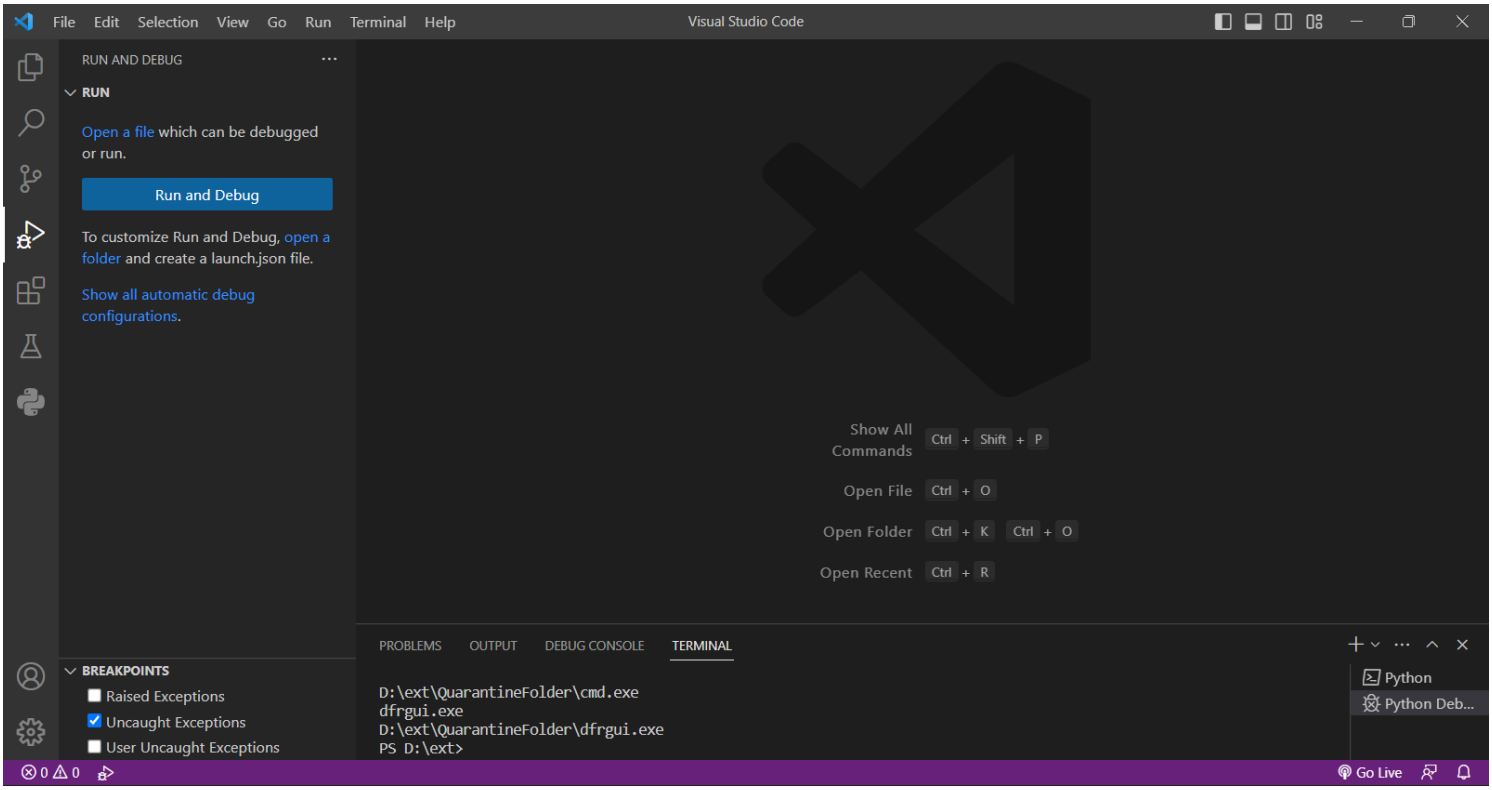
รูปที่ 37 หน้าต่างแสดงการติดตั้ง

คลิก ‘Finish’



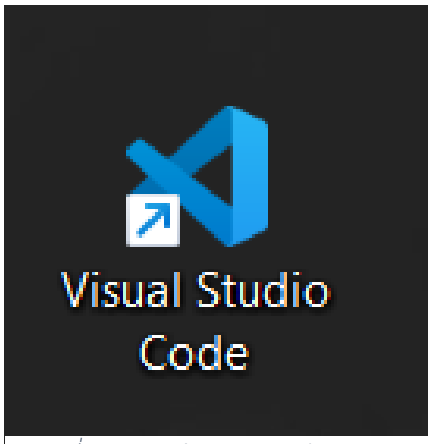
รูปที่ 38 หน้าต่างแจ้งเตือนการติดตั้งสำเร็จ

เสร็จสิ้นการติดตั้งสามารถใช้งานโปรแกรมได้ทันที



รูปที่ 39 หน้าโปรแกรมหลังติดตั้งเสร็จเรียบร้อย

หน้า Desktop จะแสดงทางลัดสำหรับการเปิดใช้



รูปที่ 40 ทางลัดสำหรับการเปิดใช้โปรแกรม

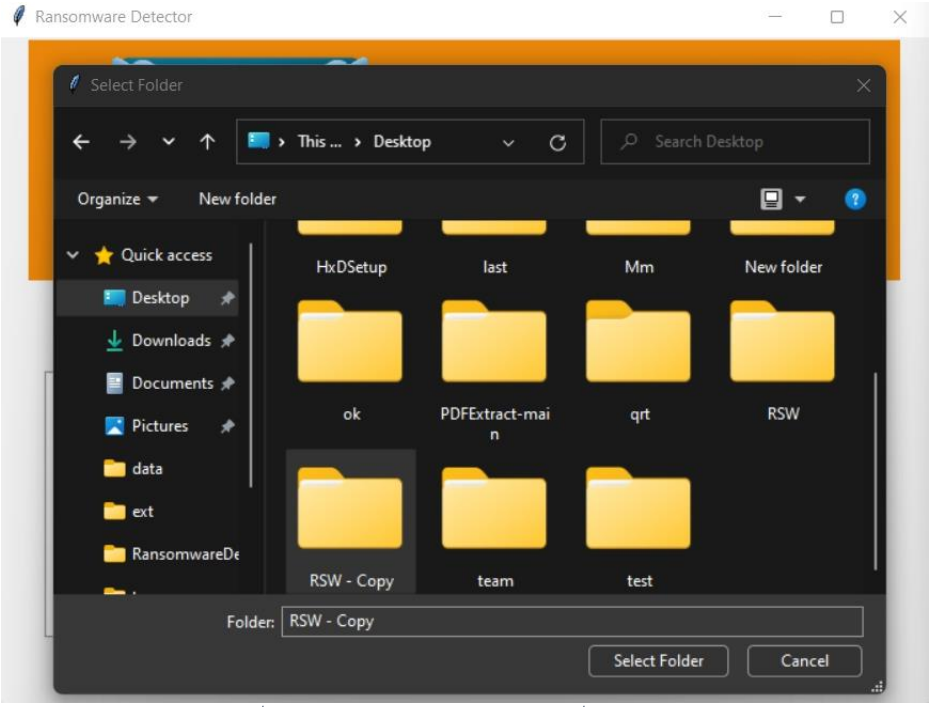
ภาคผนวก ข

คู่มือการใช้งาน

ขั้นตอนการเลือกโฟลเดอร์ที่ต้องการสแกน

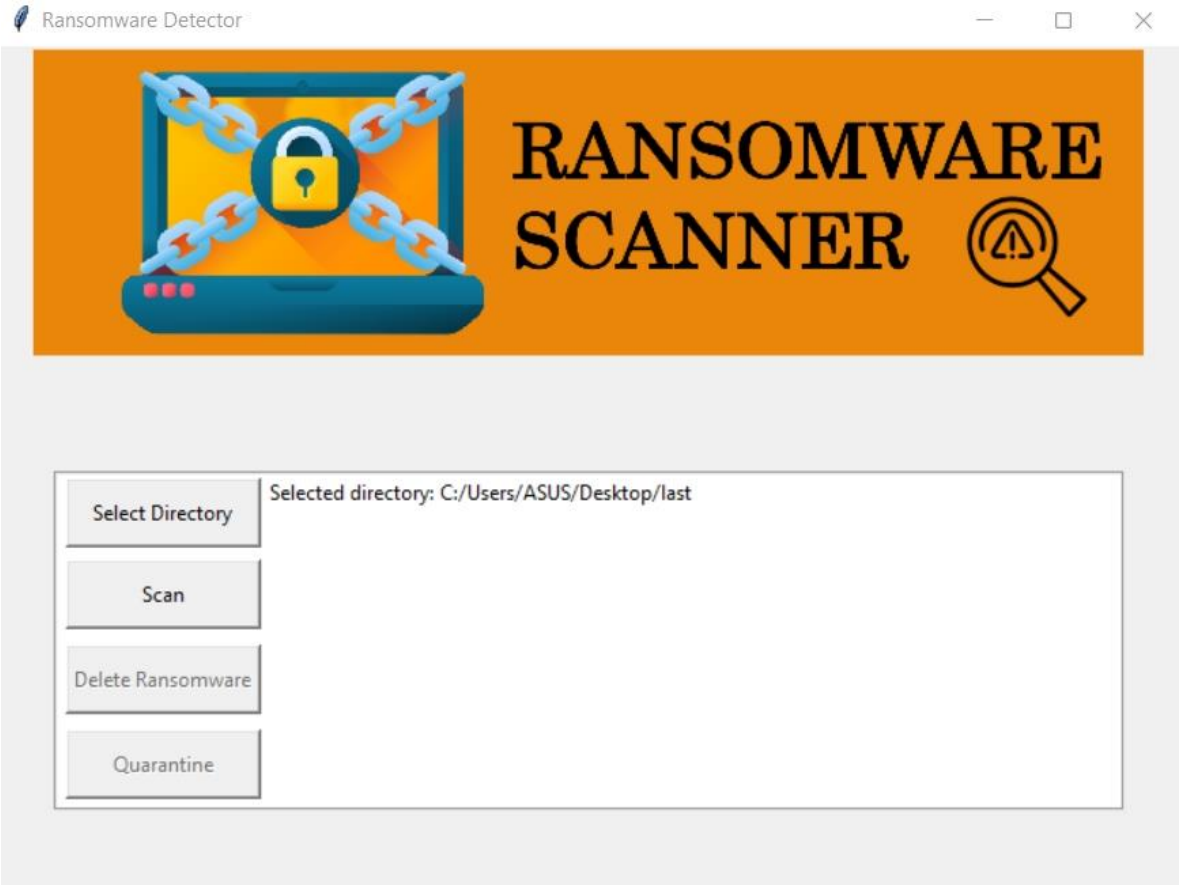
รูปที่ 41 หน้าจอหลักของโปรแกรม

- คลิกที่ปุ่ม Select Directory เพื่อเลือกโฟลเดอร์ที่ต้องการสแกน แล้วเลือกโฟลเดอร์ที่ต้องการ และคลิก Select Folder



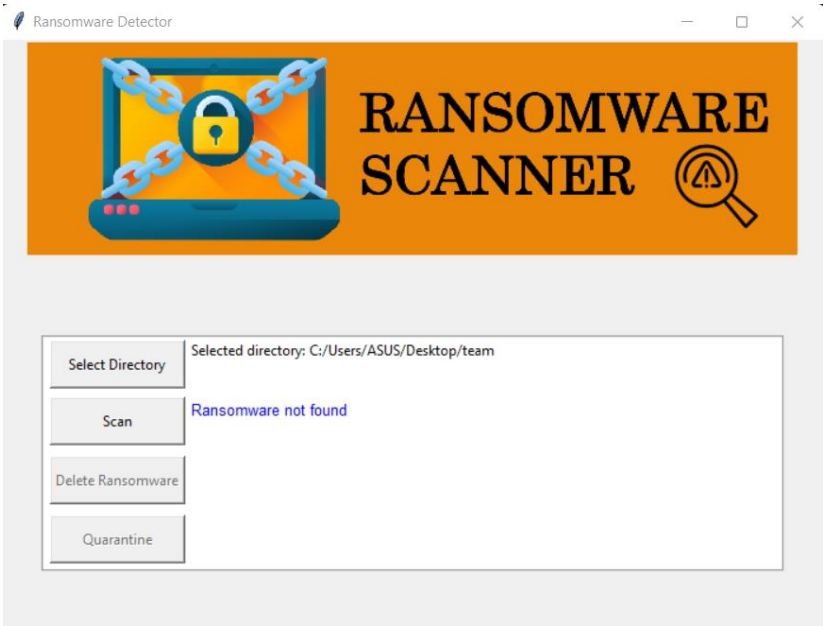
รูปที่ 42 หน้าต่างให้เลือกโฟลเดอร์ภายในเครื่องคอมพิวเตอร์

เมื่อกดเลือกโฟลเดอร์แล้ว ที่อยู่ของโฟลเดอร์ที่เลือกจะแสดงที่ด้านขวาของปุ่ม



รูปที่ 43 แสดงผลลัพธ์การเลือกโฟลเดอร์

เมื่อเลือกโฟลเดอร์ที่ต้องการสแกนเรียบร้อยแล้ว ให้ทำการสแกนโดยคลิกที่ปุ่ม Scan เพื่อเริ่มการสแกน หากโฟลเดอร์ที่สแกนไม่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ จะแสดงข้อความเป็น “Ransomware not found”

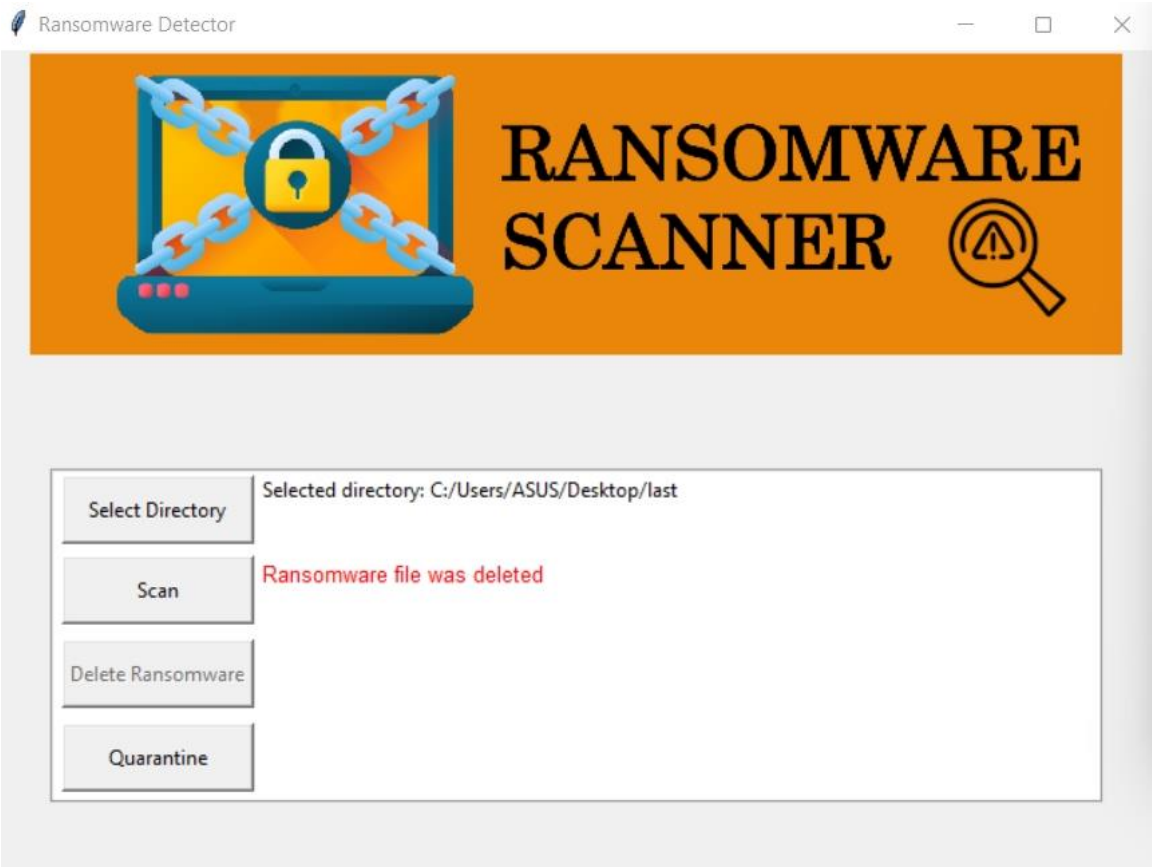


รูปที่ 44 โปรแกรมแจ้งเตือนให้เลือกโฟลเดอร์ก่อนการสแกน

ในกรณีที่สแกนโฟลเดอร์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ จะแสดงข้อความเป็น “Found ransomware” ตามด้วยที่อยู่ของไฟล์นั้น และชื่อของไวรัสเรียกค่าไถ่ที่อยู่ในไฟล์นั้น

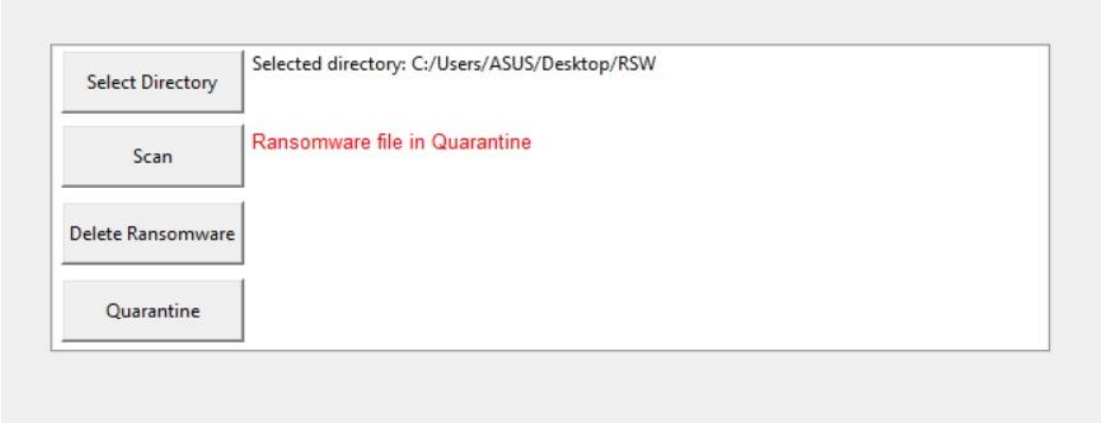
รูปที่ 45 แสดงผลลัพธ์การสแกนโฟลเดอร์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่

จากนั้น หากผู้ใช้ต้องการเลือกลบไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ สามารถเลือกคลิกที่ปุ่มลบได้ทันที ซึ่งปุ่ม Delete Ransomware จะสามารถใช้งานได้ก็ต่อเมื่อเจอไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่เท่านั้น ซึ่งเมื่อผู้ใช้คลิกที่ปุ่ม Delete Ransomware แล้วสามารถทำการกำจัดไฟล์ไวรัสเรียกค่าไถ่ได้เสร็จสิ้น จะแสดงข้อความที่ด้านขวาของปุ่มเป็น “ Ransomware file was deleted”



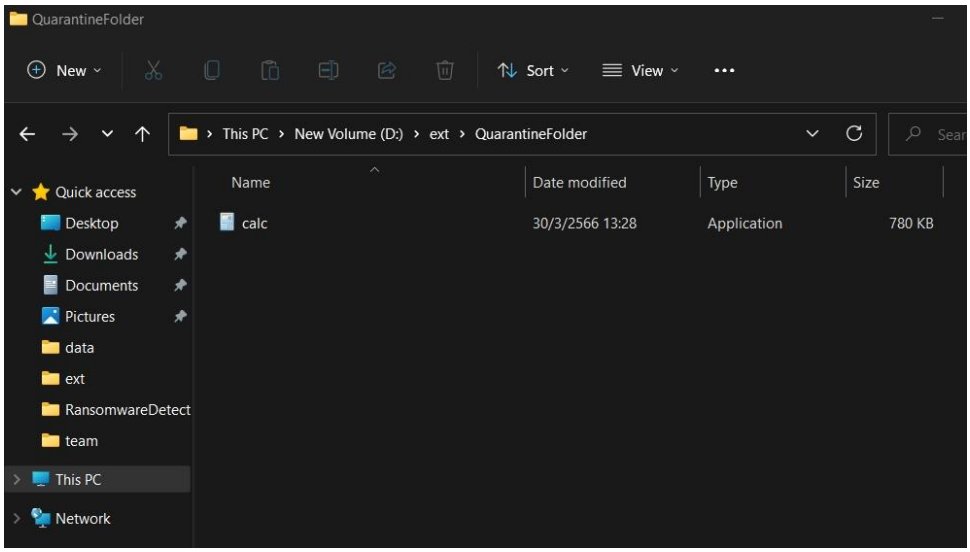
รูปที่ 46 แสดงผลลัพธ์การลบไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่

ในกรณีที่ผู้ใช้งานยังไม่ต้องการกำจัดไฟล์ที่มีการแฝงตัวของไวรัสเรียกค่าไถ่ที่สแกนเจอ เพื่อการตรวจสอบความสำคัญของไฟล์ที่สแกนเจอไวรัสเรียกค่าไถ่ สามารถเลือกกดปุ่ม Quarantine เพื่อกักกันไฟล์ไว้ก่อนทำการลบในภายหลังได้ โดยที่ปุ่มจะสามารถใช้งานได้ก็ต่อเมื่อสแกนเจอไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่ ซึ่งเมื่อผู้ใช้คลิกที่ปุ่ม Quarantine แล้วจะแสดงข้อความที่ด้านขวาของปุ่มเป็น “ Ransomware file in Quarantine”



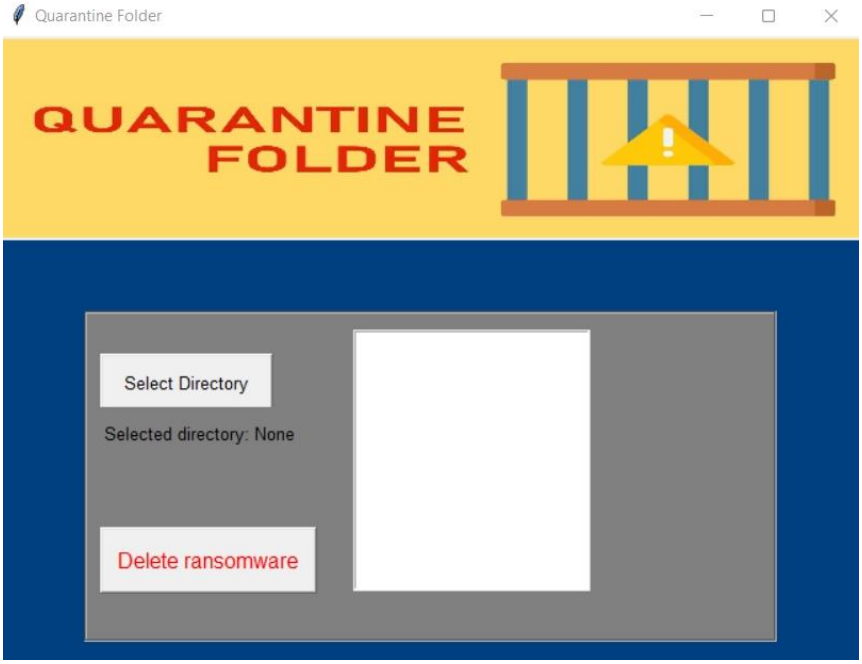
รูปที่ 47 แสดงผลลัพธ์การกักกันไฟล์ที่มีไวรัสเรียกค่าไถ่แฝงตัวอยู่

และเมื่อทำการกักกันไฟล์เรียบร้อยแล้ว ไฟล์นั้นจะย้ายไปอยู่ที่โฟลเดอร์ QuarantineFolder



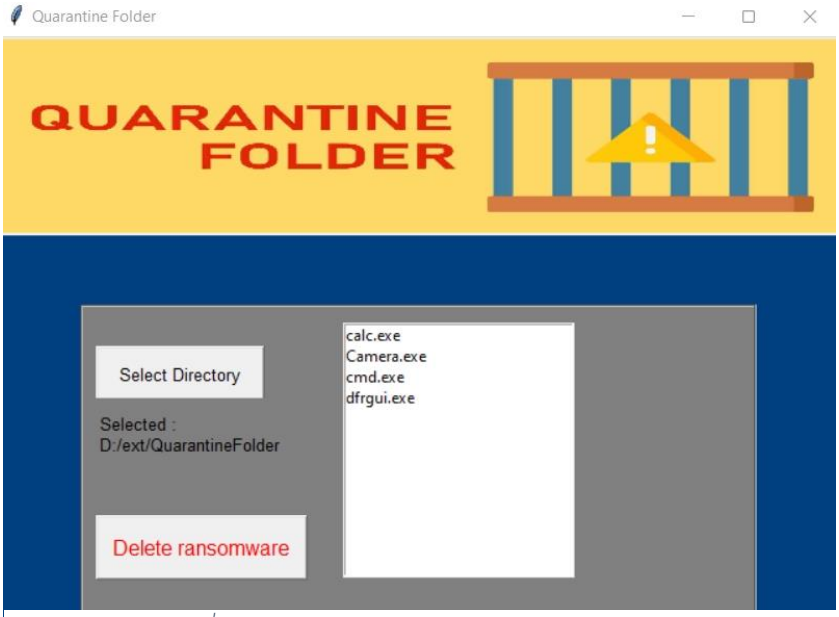
รูปที่ 48 การตรวจสอบการกักกันไฟล์

เมื่อผู้ใช้กักกันไฟล์เสร็จสิ้นแล้ว หากต้องการตรวจสอบและทำการกำจัดสามารถทำได้โดยเข้าไปที่ระบบโฟลเดอร์ QuarantineFolder



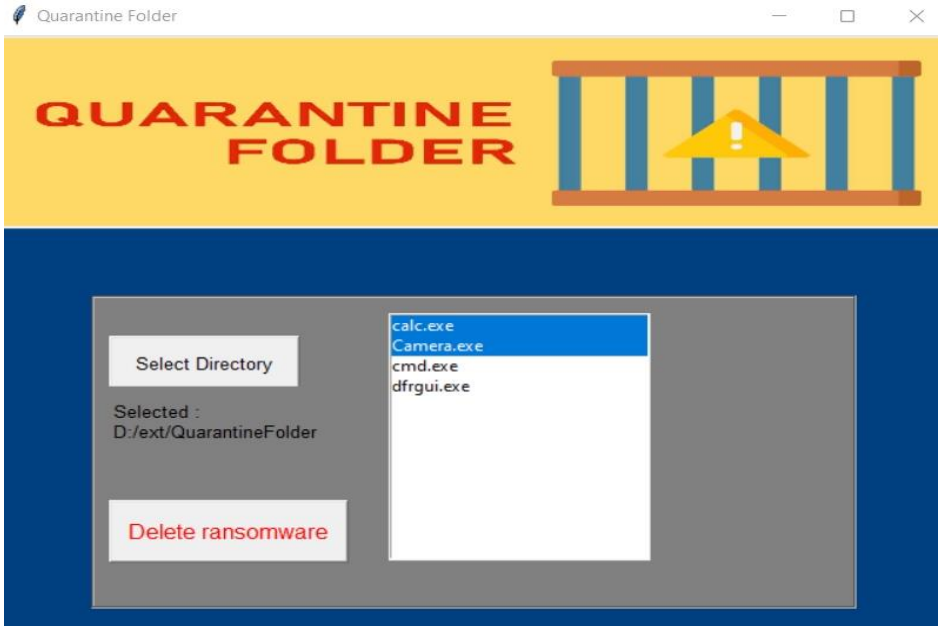
รูปที่ 49 หน้าจอหลักของระบบกักกันและกำจัดไฟล์

เมื่อผู้ใช้ทำการคลิกไปที่ปุ่ม Selec Directory จะแสดงหน้าต่างให้ผู้ใช้งานเลือโฟลเดอร์ที่ต้องการดูรายการไฟล์ ซึ่งจะสามารถเลือกได้เฉพาะโฟลเดอร์ “QuarantineFolder” เท่านั้น เมื่อเลือกแล้วโปรแกรมจะแสดงรายการไฟล์ในโฟลเดอร์ทันที



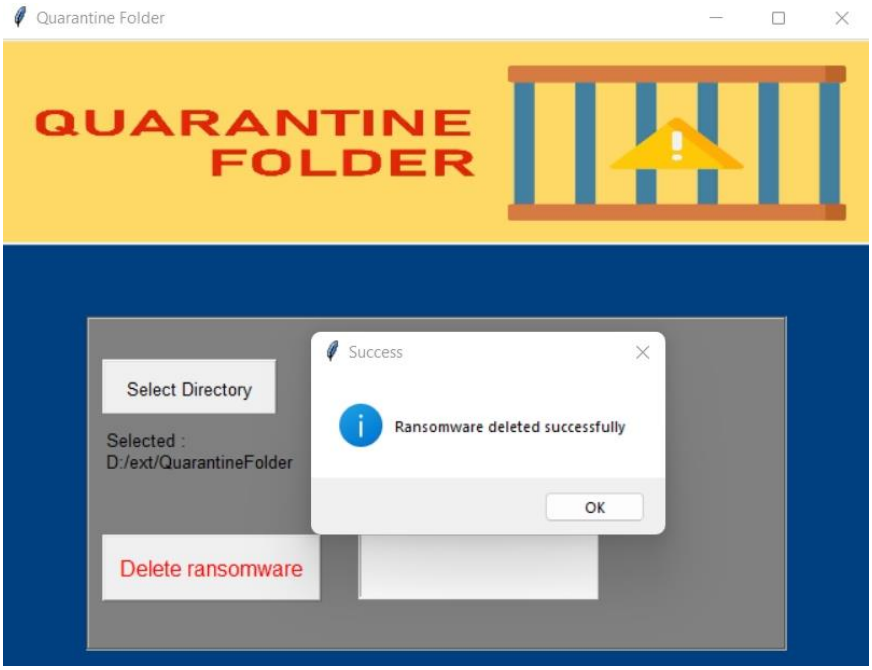
*รูปที่ 50 แสดงรายการไฟล์ในโฟลเดอร์ **QuarantineFolder***

เมื่อหน้าโปรแกรมแสดงรายการไฟล์แล้ว ผู้ใช้สามารถเลือกไฟล์ที่ต้องการกำจัด ซึ่งสามารถเลือกลบได้มากกว่าหนึ่งไฟล์ตามความต้องการ



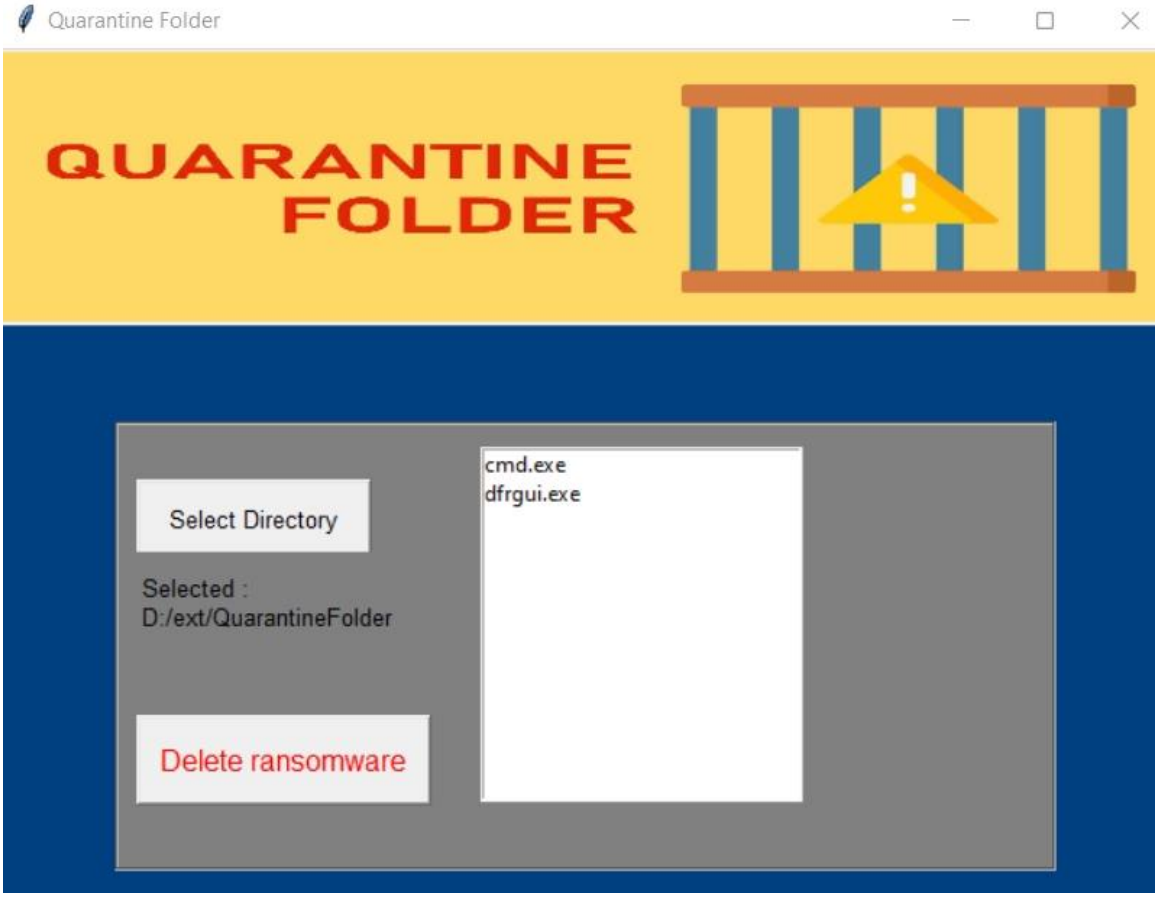
รูปที่ 51 แสดงการเลือกไฟล์ที่สามารถเลือกได้มากกว่าหนึ่งไฟล์

เมื่อเลือกไฟล์ที่ต้องการลบเรียบร้อยแล้ว สามารถคลิกที่ปุ่ม “Delete ransomware” เพื่อกำจัดไฟล์ที่เลือกได้ทันที และเมื่อสามารถกำจัดไฟล์ไวรัสเรียกค่าไถ่ได้สำเร็จจะแสดงกล่องข้อความเพื่อแจ้งเตือนการกำจัดไฟล์ที่สำเร็จ



รูปที่ 52 แสดงการแจ้งเตือนการกำจัดไฟล์สำเร็จ

และหากผู้ใช้งานคลิกปุ่ม OK หน้าโปรแกรมจะทำการ Refresh ที่กล่องข้อความที่แสดงไฟล์ภายในโฟลเดอร์ทันที เพื่อให้ทราบได้ว่าไฟล์ที่เลือกนั้น สามารถกำจัดได้เสร็จสิ้นแล้ว



รูปที่ 53 โปรแกรมแสดงผลลัพธ์ให้ทราบว่าไฟล์ที่เลือกถูกกำจัดเสร็จสิ้นแล้ว

ภาคผนวก ค

Source code

- **Source Code Convert md5hash to byte**

```
import csv
import codecs
with open('input.csv', 'r') as csv_file:
    csv_reader = csv.reader(csv_file)
    next(csv_reader)  # skip header row if present
    with open('output.csv', 'w', newline='') as output_file:
        csv_writer = csv.writer(output_file)
        csv_writer.writerow(['Signature', 'Filename'])
        for row in csv_reader:
            filename = row[0]
            md5hash = row[1]
            byte_hash = codecs.decode(md5hash, 'hex')
            csv_writer.writerow([byte_hash, filename])
```

- **Source Code Ransomware Detection**

```
import os
import tkinter as tk
from tkinter import filedialog, messagebox
```

```
import csv

import shutil

import tkinter.messagebox as messagebox

# Define and initialize RANSOMWARE_SIGNATURES

RANSOMWARE_SIGNATURES = {



    b'MZ\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff': 'Ryuk
ransomware',

    b'MZ\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff': 'Sodinokibi
(REvil) ransomware',

    b'\x6d\x6f\x72\x6a\x61\x76\x61\x00\x4d\x53\x57\x53\x6f\x66': 'Maze
ransomware',

    b'\x55\x55\xaa\xaa\x11\x11\x33\x33\x00\x00\x8e\xe5': 'Dharma
ransomware',

    b'\x21\x3c\x61\x72\x63\x68\x3e': 'Locky ransomware',


b'\x00\x4d\x5a\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff\x00\x00':
'WannaCry ransomware',

    b'\x2e\x74\x6f\x72\x00\x00':'GandCrab ransomware',
```

b'\x30\x82\x01\xff\x02\x01\x01\x04\x04\x00\x02\x00\x00\x00\x81\x88':'CryptoLocker ransomware',

b'\x4d\x5a\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff\x00\x00':'Petya ransomware',

b'\x67\x33\x33\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00':'Locky ransomware',

b'\n\t\xa2\x1c/(\xc8\xc5\xb5\xd1h\xfe\xb6h\xa8\x0b' :' VirusShare_0a09a21c2f28c8c5b5d168feb668a80b ',

b'\xbcL\xe1\xd0FoBI4\x18\xd6[\x9a\x1e\x88\x0f' :' VirusShare_bc4ce1d0466f42493418d65b9a1e880f ',

b'0\x86\xd1h*\x10\xbc\xa6\x19E\xcc\xca\x93\xcc\x80\x98' :' VirusShare_3086d1682a10bca61945ccca93cc8098 ',

b'\x06\x83\xb5\x86\xf3\xb9\xeaz\x06\xd4\xd3\x15U\xf3\x1f\x80' :' VirusShare_0683b586f3b9ea7a06d4d31555f31f80 ',

b'\xd7M\xae\xe5\x15\xbdZw\xf2\x99\x15\x1aV\x8c\xb5z' :' VirusShare_d74daee515bd5a77f299151a568cb57a ',

b'~\xf3Q*\xf9Z\xe7\xb3=B\x99\x0fE\x05W\xaf' :' VirusShare_7ef3512af95ae7b33d42990f450557af ',

b'\x8f\x9dm\xa5\xb0\xc7\xb8\xbc\x8e}\x90\x80#\xae\xb7\xf1' :'
VirusShare_8f9d6da5b0c7b8bc8e7d908023aeb7f1 ',

b'1\xcd"\xb7\xcd\x84#T\x83B\xfeH1\xbek<' :'
VirusShare_31cd22b7cd8423548342fe4831be6b3c ',

b'\xa0%\x9c\x15\xb0\xcb\x1b\xc6\x93@Gn\x03\xacp\xb0' :'
VirusShare_a0259c15b0cb1bc69340476e03ac70b0 ',

b'\t?bf\x1b\xd4\xc2\xf4\xc9\xe8\xe5\t `] ' :'
VirusShare_093f62661bd4c2f4c9e8e50920605d20 ',

b'Y7\xc4\xef\xa8\x8b\x85\xe7\xcc\x16\xecl\xd1@G\x96' :'
VirusShare_5937c4efa88b85e7cc16ec6cd1404796 ',

b'\xd6\xd5\xff\x08N\xef7K\xe4\x83:\x17\xb7.\xf1 ' :'
VirusShare_d6d5ff084eef374be4833a17b72ef120 ',

b'\xd7\xc3\x1fO\xc9\x1a%)\xab\x08\xf4\x89\xe9\xad\xf1\x9a' :'
VirusShare_d7c31f4fc91a2529ab08f489e9adf19a ',

b'-o\xd9w\x07\xdd$\xb6\x0c\xa9\xf0\xc7M\xd1d\x90':'
VirusShare_2d6fd97707dd24b60ca9f0c74dd16490 ',

b'=\x13\x128\xb8\xd6)Sa\xc6f\xde\x0e\xacE\xd4' :'
VirusShare_3d131238b8d6295361c666de0eac45d4 ',

b'\xcc^\xc9\xfd\x1b\x89YE\xa4\xc1\x9aE`\xfb\xf1\xd1' :'
VirusShare_cc5ec9fd1b895945a4c19a4560fbf1d1 ',

b'8&D\xb7KV\xf8\x81{d\xa1T\x0c\\\xaas':'
VirusShare_382644b74b56f8817b64a1540c5caa73 ',

b'\xb1\xbe\x1cN8\x9a\xb6\xad\xd4\xa2\x05\xb0$.\n\xe8' :'
VirusShare_b1be1c4e389ab6add4a205b0242e0ae8 ',

b'\xac\xb0^\x95\xd7\x13\xb1w/\xb9j^`}S\x9f' :'
VirusShare_acb05e95d713b1772fb96a5e607d539f ',

b' \xcd\xd5r\xe0\x7fP\x86\xc1\x81\\OJj\xde\x10' :'
VirusShare_20cdd572e07f5086c1815c4f4a6ade10 ',

b'\xe0\xdf\xfe\xdb\xfc"J\xc4\xd17eNE\xd2d\xdb' :'
VirusShare_e0dffedbfc224ac4d137654e45d264db ',

b'\xee^\xd0\xe3^\xe9e\xca\xf97Q\x92`\xccJ\xc3' :'
VirusShare_ee5ed0e35ee965caf937519260cc4ac3 ',

b'\xcc\x94\x07\xa0Q\xe9\xd8\xef\r\xbe;\x05\x93\x17\x83\xe5' :'
VirusShare_cc9407a051e9d8ef0dbe3b05931783e5 ',

b'\xeeI\xad\xaf\x8d\xca\xc4\xdd\x7f6D\x90\x8d\x85\x1a\xda' :'
VirusShare_ee49adaf8dcac4dd7f3644908d851ada ',

b'R\xde\x90\x9ah\x08\x91]\xf92`6\xb3C\x10a' :'
VirusShare_52de909a6808915df9326036b3431061 ',

b't\xb7\x08K\xe0sH\x8f\\\x14L\x12\xda\xb0\xf4\xbe' :'
VirusShare_74b7084be073488f5c144c12dab0f4be ',

b'e\x8d\xcb9\x9e\xfa\xa7B\xd7\x0c\x89:rFlN' :'
VirusShare_658dcb399efaa742d70c893a72466c4e ',

b'\x0e%@\x82\xe8\x87d#\xfbu\xc5i\x8f\x98/\xa4' :'
VirusShare_0e254082e8876423fb75c5698f982fa4 ',

b'\xf3\xb6 \xbd\xf9:\x05K\x8b`\xc3\x07@\x99\x95w' :'
VirusShare_f3b620bdf93a054b8b60c30740999577 ',

b'\xe1Nh\x84\xfc\xb0u\xc6\xc2k\x188y\x9fY-' :'
VirusShare_e14e6884fcb075c6c26b1838799f592d ',

b'\xbc\x99\x87\\76\x1a\x81\xce\x97\x89t\xa9c\xca"' :'
VirusShare_bc99875c37361a81ce978974a963ca22 ',

b' \xc7\xceg\x9d\xdem\x81a\xc0\xb2\xdc\x80\x82\x19\x95' :'
VirusShare_20c7ce679dde6d8161c0b2dc80821995 ',

b'\x93\x81h{\xbaP>&=Wq\xef\x0fs\x0e\xb0' :'
VirusShare_9381687bba503e263d5771ef0f730eb0 ',

b'\xba\xa0\x98F\xb0SA\x83\xef\x89,n\xbe\xb4\xc0{' :'
VirusShare_baa09846b0534183ef892c6ebeb4c07b ',

b'-I\xc4\xdb\xb9\x90r_\x15\x0b\x85p\xe8J\xbfT' :'
VirusShare_2d49c4dbb990725f150b8570e84abf54 ',

b'X\x189=\x84\x14d\x89Y^4*g\x87c^' :'
VirusShare_5818393d84146489595e342a6787635e ',

b'\xc8\xdca\x8b,\xd7\xde\x1c\x90$\xa4\x06\xa8~\xcd\xa4' :'
VirusShare_c8dc618b2cd7de1c9024a406a87ecda4 ',

b'\x9e\xc2\xd1\xcfK\xc7E0\nq\t\x00k\xa0af' :'
VirusShare_9ec2d1cf4bc745300a7109006ba06166 ',

b'\x02\xed\xe61\xa3\xa1(\xa7[\xf0\xa2p\x8bj7;':'
VirusShare_02ede631a3a128a75bf0a2708b6a373b ',

b'\x96W\x8f\x08\xaeu\xe5\xd8~\xac\x00,\x11ei\xe2' :'
VirusShare_96578f08ae75e5d87eac002c116569e2 ',

b'X\x7f\xee\\\x8d)\x03\xcd\x82*\xfbv\xcc\x1b&T' :'
VirusShare_587fee5c8d2903cd822afb76cc1b2654 ',

b'\xef\xeb]\xe8c\xd5*\x9d\x93z\x0eR\x91;#0' :'
VirusShare_efeb5de863d52a9d937a0e52913b2330 ',

b'\xa4\xd21_\x05\xdb8]\x88\xd7\x07\xaf\x03\x0c1@' :'
VirusShare_a4d2315f05db385d88d707af030c3140 ',

b'\xbd\xc4t\xdf\xc452\xb5/\xf4\x8b\xe2\xc9\xaa\x97u' :'
VirusShare_bdc474dfc43532b52ff48be2c9aa9775 ',

b'\xb19\x1cK\xbeCL\xe6\xe8\xf8/\xf6\x0bL\xcb\xdf' :'
VirusShare_b1391c4bbe434ce6e8f82ff60b4ccbdf ',

b'\x9a\\\xb2\xe8bb\x8d\xd5\x0c\xa8\xd4\x13\r\x8bu\xfc' :'
VirusShare_9a5cb2e862628dd50ca8d4130d8b75fc ',

b'\xd7\xda\xf6\xe89\xaf\x15\x9d\xb9_&ST\xdfq\xd1' :'
VirusShare_d7daf6e839af159db95f265354df71d1 ',

b'\xb3\xcd\xd9^7\xd6\xf3a\xe1\x9f?\xe5\x80\xe4A5' :'
VirusShare_b3cdd95e37d6f361e19f3fe580e44135 ',

b'\x1c\xd7\x0f\xbf\x1cP\xe4\x1e\x06U\x93\x11\xa7~\x9b\xe6' :'
VirusShare_1cd70fbf1c50e41e06559311a77e9be6 ',

b'\xf3+\xda@\xb9\xd7\x8c\xf2\xe9z\xf3\xe5\x81\xca\xa4\xd0' :'
VirusShare_f32bda40b9d78cf2e97af3e581caa4d0 ',

b"Mla04\t0\x1a\x99\xa4R\x84\x9a'\x10\xd0" :'
VirusShare_4d6c61303409301a99a452849a2710d0 ',

b'D\xd3\x9c\xee&8\x1a\xf9\xbf\xd9fe\x9e\xf4\xe3t' :'
VirusShare_44d39cee26381af9bfd966659ef4e374 ',

b'Ll\xed\x05\x1b\xab\x8e\xa5\x14\xbb7G\x15\xe6\xacZ' :'
VirusShare_4c6ced051bab8ea514bb374715e6ac5a ',

b'\x87\xfct\xc2]\x1fd\x9d\x8f\x80?\xe5|v`l' :'
VirusShare_87fc74c25d1f649d8f803fe57c766049 ',

b'\xaa\xbe\x82\xeeyJM\xd2{GU})F\xfc{' :'
VirusShare_aabe82ee794a4dd27b47557d2946fc7b ',

b'\xefX,:t}\xbf8\xce!\xd0\xe3|\xb5\xf1\x10' :'
VirusShare_ef582c3a747dbf38ce21d0e37cb5f110 ',

b'=Tn}g\x89$\t\xbe\x1f\x12\xea\x95P\t^' :'
VirusShare_3d546e7d67892409be1f12ea9550095e ',

b'>\x9e\xd3\x13P\x89\x84#\x93\x1a\xfd\xa6Y\xa8C@':'
VirusShare_3e9ed31350898423931afda659a84340 ',

b'F\x84\xa8G9V\xbf|\x12\r\x01w\xc9\x1a5\x17' :'
VirusShare_4684a8473956bf7c120d0177c91a3517 ',

b"\x9c\xe5\xf6\t\xdf'\xd6\x97\xf6\x0c\xc5\xf2X3\xf6\x92" :'
VirusShare_9ce5f609df27d697f60cc5f25833f692 ',

b'\xa1Z\xa2\xc1W\x08\xc7\x87;\xb6V\x18\x0f\xc1\xbf\xd5' :'
VirusShare_a15aa2c15708c7873bb656180fc1bfd5 ',

b'\x16\xdb\x99\xb5d\x1bk\xc5\xec\x00-\x93\xe4.\x1c&' :'
VirusShare_16db99b5641b6bc5ec002d93e42e1c26 ',

b'\xda\xe8\x10\xed\x8c\xf1\x80\xa9\x9a\x0c\x05r\xb4\xf8\xf9\xb5' :'
VirusShare_dae810ed8cf180a99a0c0572b4f8f9b5 ',

b'\xd8m\xf33\xf5\x9f\xa5\xc6\xda\xbc\xcax\x05pz\x90' :'
VirusShare_d86df333f59fa5c6dabcca7805707a90 ',

b'\xaf\x92\xa20k\xa7\xb9\xfe^.,\xb9\x93\x8f\x88\xa2' :'
VirusShare_af92a2306ba7b9fe5e2e2cb9938f88a2 ',

b'\xc9\xc7\x90*|OL\xad\x90\x85\xd7\xa8{\x8e\xc6\xd0' :'
VirusShare_c9c7902a7c4f4cad9085d7a87b8ec6d0 ',

b'\xb8\xc1\x93x\xbfk\xb6\xb8 LKeC\x94\xc2\x10' :'
VirusShare_b8c19378bf6bb6b8204c4b654394c210 ',

b'4\x0f\xb7\x89\xff\xb1,\xb5kc\xdfv\xc7\x87\xb5\xce' :'
VirusShare_340fb789ffb12cb56b63df76c787b5ce ',

b'/\xe67\xd2(y=I\xaa\xc2\xf7\xbeM?0R' :'
VirusShare_2fe637d228793d49aac2f7be4d3f3052 ',

b'zn\x8b\x1b\x19\xdd)aT\x01^\x0b\xd5\x9c\xe1<' :'
VirusShare_7a6e8b1b19dd296154015e0bd59ce13c ',

b"+\xd96\xa1s\x1biT\xba'J\xa7\x1b5G\xa1" :'
VirusShare_2bd936a1731b6954ba274aa71b3547a1 ',

b'o\xc0:g\xd8\xc9\xde\xeb\x14\xec\xe5\xdb\xcd\x9f(n' :'
VirusShare_6fc03a67d8c9deeb14ece5dbcd9f286e ',

b' P9\x9b\x95\xd8l\xdaL\xf2;\x00\x0em"t' :'
VirusShare_2050399b95d849da4cf23b000e6d2274 ',

b'Y\xd8)\xe3\xf3\xf0\xfb,\xc1\x91\x7f\xec\xd8\x1b\x82\x98' :'
VirusShare_59d829e3f3f0fb2cc1917fecd81b8298 ',

b'\xb8.V\xc5\xabA\xf9\x00\x1b\x86(&tH\x90\x8f' :'
VirusShare_b82e56c5ab41f9001b8628267448908f ',

b"]\t\xa1\xfd\x08/\x84'\xaa\xea\xad\x19\x93\x86\xcb\xc5" :'
VirusShare_5d09a1fd082f8427aaeaad199386cbc5 ',

b'\xe1Qi\xcf\x03\xe7\xf6\x11K@\xc21\xbej\x14N' :'
VirusShare_e15169cf03e7f6114b40c231be6a144e ',

b'\x08\x9f\xaeKk2\xa7\xc8\xeb\xb5\xcd\xfa\x04\x1d\xf3\xbc' :'
VirusShare_089fae4b6b32a7c8ebb5cdfa041df3bc ',

b'\x16\x0bj\x96\x10=\xd8\xca{i\t[\xf0\xc7q\x89' :'
VirusShare_160b6a96103dd8ca7b69095bf0c77189 ',

b'\x14\xdf\xa4\x99\xe7\xb8\xc2\xac\x1f}\x0c!V,-\xdd' :'
VirusShare_14dfa499e7b8c2ac1f7d0c21562c2ddd ',

b'\xb5\x90\xb4\x15\x88\xa0\x95]\xa2\xd4\x91\xb3\x057\xe5\xbc' :'
VirusShare_b590b41588a0955da2d491b30537e5bc ',

b'\xd9\xcd\xfbt#AG\xac\\\xf5I6\xb7Z\xadT' :'
VirusShare_d9cdfb74234147ac5cf54936b75aad54 ',

b'7\xa1\xd3}\xfe\xd8\xb7:\xa0\xfa0N\xf5\xb8\x1a\x10' :'
VirusShare_37a1d37dfed8b73aa0fa304ef5b81a10 ',

b'\x0b\x8c\xad\x9f\x8dY\x17\xf4\x93\x0e\xb0/\x0b$S\xf6' :'
VirusShare_0b8cad9f8d5917f4930eb02f0b2453f6 ',

b'\x88\xa5\x15\xfdy\x9a\xcd\x89\x014\x1fS\x01\x0b\x12\x16' :'
VirusShare_88a515fd799acd8901341f53010b1216 ',

b'\r\x0e\x1d{jx\x82\xa3\x18\x92c_%aT\xd0' :'
VirusShare_0d0e1d7b6a7882a31892635f256154d0 ',

b'\xe4\xad\x0c!OU\x87>\xbbZJ\x8eT\xe5\x84J' :'
VirusShare_e4ad0c214f55873ebb5a4a8e54e5844a ',

b'\x82\xf54RVhp\x83\xa5\x92^\xfbcB<\x16' :'
VirusShare_82f5345256687083a5925efb63423c16 ',

b'\xec,qPg\xec\xb2&9\xaf\xb2h\x82\xdb0w' :'
VirusShare_ec2c715067ecb22639afb26882db3077 ',

b'\x0c}^\xe4\x92?\x9a^\x91\x13\xa4#@w\xc3\xe0' :'
VirusShare_0c7d5ee4923f9a5e9113a4234077c3e0 ',

b'\r\x02\r\t\xac\xd47\xb8\xe1\xc2\r\xcaY\xc0\xf3\xa6':'
VirusShare_0d020d09acd437b8e1c20dca59c0f3a6 ',

b'\\3\x01\x01^\x9e\x05\xce\xc1$!\xc1L#\x92 ' :'
VirusShare_5c3301015e9e05cec12421c14c239220 ',

b'A\xbc\xc8i\xf3\x8a\x15m\x1b=-\xc6\x0e \xd0.' :'
VirusShare_41bcc869f38a156d1b3d2dc60e20d02e ',

b'\xe9\xf1\x08\xbf\xe4\xf2G\xdb\x95\x97\xaa\x1dm@\x8c\xb9' :'
VirusShare_e9f108bfe4f247db9597aa1d6d408cb9 ',

b"\xda\xbcp`$\xff\x9d97\xa4\xda\x86~\x02'$" :'
VirusShare_dabc706024ff9d3937a4da867e022724 ',

b'\xe1\x9d\x17\x80\xf1.\x0bg\xea\xd3\xe7E\xbcBT\xcd' :'
VirusShare_e19d1780f12e0b67ead3e745bc4254cd ',

b'\xdf<u\xd1 w?\x88\xed\xb0b\xb5\xe2\xb6\xd57' :'
VirusShare_df3c75d120773f88edb062b5e2b6d537 ',

b'\xb7\xe1\x16v\xc0,\xb0v\xcc\x1d\xad\x87m=D?' :'
VirusShare_b7e11676c02cb076cc1dad876d3d443f ',

b'\x85\x0c\x99\xc5\x85\xfd\xbe\x93?#\xc7\nc~\xa3\xe8' :'
VirusShare_850c99c585fdbe933f23c70a637ea3e8 ',

b'AO\\\x83k\\\xc3\x12\xa5\xef\xfd?k\xb8\xb1f' :'
VirusShare_414f5c836b5cc312a5effd3f6bb8b166 ',

b'=\xcd^\xa0UE\xda>\x84\x98OyR\x11}\xc9' :'
VirusShare_3dcd5ea05545da3e84984f7952117dc9 ',

b'O\xc4F\x96\xdb\x9f!\xee\x9f\xf9\x1f]#\x82\xdf\x81' :'
VirusShare_4fc44696db9f21ee9ff91f5d2382df81 ',

b'6\xe5\xa8@\xcd\x8ce\x17}\x9a>\xa9/\xf6\xd5L' :'
VirusShare_36e5a840cd8c65177d9a3ea92ff6d54c ',

b'\x9f!\x1f\xb3\xbe\xd9\xcb\x12\x92Q+=\x9e\xd3\xed\xfb' :'
VirusShare_9f211fb3bed9cb1292512b3d9ed3edfb ',

b'\xe2\x1a}\xba\x1f\x1bB\xeaS\xb3\xbb\x7f\xab\xa3aX' :'
VirusShare_e21a7dba1f1b42ea53b3bb7faba36158 ',

b'\x01\xbd\x02\xb4"\xcd\xc7\xb9\xb4\xdcP6\xd3\xed5P' :'
VirusShare_01bd02b422cdc7b9b4dc5036d3ed3550 ',

b'\xe6\xe3K\x0ee#\x18\x1c\x8d\xd6k\xc2qQ3\xd0' :'
VirusShare_e6e34b0e6523181c8dd66bc2715133d0 ',

b'\x84\x1a\xcaVl\xc1\xd4jx\xdc\x0f\x0eM/"\x05' :'
VirusShare_841aca566cc1d46a78dc0f0e4d2f2205 ',

b'\x8fM\x85N\x13u\xa9\xb2DY\x1a\\\xe7\x87m]' :'
VirusShare_8f4d854e1375a9b244591a5ce7876d5d ',

b'\xc8\x83\x16\xfb-\x06\xd1N\xc9\xbeco\xf3kP\xb8' :'
VirusShare_c88316fb2d06d14ec9be636ff36b50b8 ',

b'S\xcc\x90AAv\xf6^m\x8d\x00\xd1x\x04\x1f\xb5' :'
VirusShare_53cc90414176f65e6d8d00d178041fb5 ',

b'\xb9hw\x91\x81\xa7!+i\xc5A\xae\xb4x8\x87' :'
VirusShare_b968779181a7212b69c541aeb4783887 ',

b'\xf6K\xd8\x90\xf3\x18\xff\x1a\xd2.\x00\xfa\xa0Y\xec\x8b' :'
VirusShare_f64bd890f318ff1ad22e00faa059ec8b ',

b"\xfb\xa7'm[\x17\x88G\x87\xb1\x9b\xf1\x83\xa3A\xec" :'
VirusShare_fba7276d5b17884787b19bf183a341ec ',

b'H\x92\x8a|\xe8Q$4\xd0_M\xad\xf5\t\x0ej' :'
VirusShare_48928a7ce8512434d05f4dadf5090e6a ',

b'\xe1\xe9v\x95\x08\xd3\xd8\x1e\x9a\xb0\x85\x86\xd6\xce\xba\x00'
:' VirusShare_e1e9769508d3d81e9ab08586d6ceba00 ',

b'P\xb7\x12\x88\xcbFv\xfcGE\xa7>\x8fN\xb4\xe9' :'
VirusShare_50b71288cb4676fc4745a73e8f4eb4e9 ',

b'\xaf^\x88\xdfyy(c]\xcd\xdd\xd2\x18\xf2z\x10' :'
VirusShare_af5e88df797928635dcdddd218f27a10 ',

b'5\xb4\xd7\xd6\t.\xa7-\xc8;\x8f\x01?>.\xe2' :'
VirusShare_35b4d7d6092ea72dc83b8f013f3e2ee2 ',

b"Up\x8bd\x82Q\xaexf\x87\xa1'\xdc\xf4\xbeK" :'
VirusShare_55708b648251ae786687a127dcf4be4b ',

b'\x93\x92\xd9\xa0\xb7/D\x08\x81\xa6C2\xfbt\xef\xc0' :'
VirusShare_9392d9a0b72f440881a64332fb74efc0 ',

b'\xa2\xd8\xabvc\xd3\xb0\x15\x80\xe7[\x116\xbb^\x98' :'
VirusShare_a2d8ab7663d3b01580e75b1136bb5e98 ',

b'\xa0*\xffu=\xff\xb1:\xd04\xcag\xae\xd9\x85\xd8' :'
VirusShare_a02aff753dffb13ad034ca67aed985d8 ',

b"\xd0\xda'\x06\xd3S~\xd3\xcc7\rd\x882*\xb0" :'
VirusShare_d0da2706d3537ed3cc370d6488322ab0 ',

b'\xc2\xdb\r\x85\x16]:"\x9c\xd9\xce\xe2F\xb1\xa7\xad' :'
VirusShare_c2db0d85165d3a229cd9cee246b1a7ad ',

b'\xb9{\x05v$\xd4\x9f\x84B\x96oL\x16\xf5\x10\x90' :'
VirusShare_b97b057624d49f8442966f4c16f51090 ',

b'9\x88k\xa0#\xe0\x88N\xf9\x8b\xcb\xce\xbb\xb1\x93p' :'
VirusShare_39886ba023e0884ef98bcbcebbb19370 ',

b'z\xb6\xd6}\xa6\xb5\xb4\x1e\xbe\xb6\x93]\x8f=y\xd1' :'
VirusShare_7ab6d67da6b5b41ebeb6935d8f3d79d1 ',

b'\xe2@\xdc\x8d\xdbj\xc6\x9a\x8f\xb5\xce~\x16\xba\xccR' :'
VirusShare_e240dc8ddb6ac69a8fb5ce7e16bacc52 ',

b'V\xf1b\xc1\x1a\xff\xb0&&F8\x1b\t\x81^\xf0' :'
VirusShare_56f162c11affb0262646381b09815ef0 ',

b'q\xdd\xb5\t~a\x920\xd3\xfaEoX\x7fsG' :'
VirusShare_71ddb5097e619230d3fa456f587f7347 ',

b'nnr\xe5\xcf\xb9\x15\xf23\xebuo\n\x04\x81\xcc' :'
VirusShare_6e6e72e5cfb915f233eb756f0a0481cc ',

b']V\xcd6$\xff\x8c\x9b\xd6\x04.$\xec\x1d\xbf\x90' :'
VirusShare_5d56cd3624ff8c9bd6042e24ec1dbf90 ',

b'\x8b4\x80\xf2\xf3~btVyx\xb5<\x94\xa1\x80' :'
VirusShare_8b3480f2f37e6274567978b53c94a180 ',

b',`~t\x8c&\xa0\xd3\xaf\x9e>\xd7A\xfeJ\xc1' :'
VirusShare_2c607e748c26a0d3af9e3ed741fe4ac1 ',

b'\xc2A\x83\xbb\x15\x96r\xef\xffX\xc9\x08\xb8\xad\xe1\x03' :'
VirusShare_c24183bb159672efff58c908b8ade103 ',

b'\x13\xff~$\x89\x98\x19\xd7\xad\xa4\xb1\xf9u\xdbP^' :'
VirusShare_13ff7e24899819d7ada4b1f975db505e ',

b'\xde\xe3\xbe\x14f\x0c\x10@\x1a\x18\x0c-\rc\xbd\xc9' :'
VirusShare_dee3be14660c10401a180c2d0d63bdc9 ',

b'\xfa\xa6\xefO\\Y2\x818\xc6O\xc1P\xcd\xdb\xc0' :'
VirusShare_faa6ef4f5c59328138c64fc150cddbc0 ',

b'*\x05\xc01\x95\xb8\xed\xa8\xde\x9c\t\x1c\xfec\x98\xcc' :'
VirusShare_2a05c03195b8eda8de9c091cfe6398cc ',

b'\x82\x0c\xe0<\xa9\xe6\xbd\xcfd\xdd\xdc+4x- ' :'
VirusShare_820ce03ca9e6bdcf64dddc2b34782d20 ',

b'\x87;\xb0\xdaV4L\xc4\x9ba\xe8\xe49\xdb\xc8\x92' :'
VirusShare_873bb0da56344cc49b61e8e439dbc892 ',

b'\xacxl\x07\xf15{\xe0\xf1\xc1k\xea\xe8\xd0\xb2\x80':'
VirusShare_ac786c07f1357be0f1c16beae8d0b280 ',

b'\xbd4Twp\x89\\\xd3\x7f\xdaxM\xb4,L\xd0' :'
VirusShare_bd34547770895cd37fda784db42c4cd0 ',

b'\xe3\x93\xb6\tU\x0e\xcf\xf2\x9c\xd1HT8\xeb\xa5\x14' :'
VirusShare_e393b609550ecff29cd1485438eba514 ',

b'\xf3\x88T\xb8\xfd\x89\xa9\xe5\x7f\xfb\xcb\xfbV\x97\xb8S':'
VirusShare_f38854b8fd89a9e57ffbcbfb5697b853 ',

b'\xb50\xc6{\x8e1\xc9\xf5B\xdc\x17\xb0j\xcaǧ\x90' :'
VirusShare_b530c67b8e31c9f542dc17b06aca6790 ',

b'\xb3(\x18f\xc6\xde{\xa3\xc0\x1e\xfd \n4G ' :'
VirusShare_b3281866c6de7ba3c01efd200a344720 ',

b'\xc2\xd6\r\xd2V\xef\x05\xd1\xba;;|+`\xc0\x94' :'
VirusShare_c2d60dd256ef05d1ba3b3b7c2b60c094 ',

b"\x14X\x83\xe8Gs\xad\xeb\xe5\xb7'\xc8\x0eq\xefx" :'
VirusShare_145883e84773adebe5b727c80e71ef78 ',

b'OE\xeaY\xe2\xe2O\x17\x17M\x7f)k\xb0v\x80':'
VirusShare_4f45ea59e2e24f17174d7f296bb07680 ',

b'w\xe2\xfen\xe3\x18\x88\x8b\xd8\xadh\xf17\xe2,\x8c' :'
VirusShare_77e2fe6ee318888bd8ad68f137e22c8c ',

b'\xcdXl\x08\xa2\xc9\xb0\xc0\xaf\xc9\xea\xac]\xdbq\\' :'
VirusShare_cd586c08a2c9b0c0afc9eaac5ddb715c ',

b"zi'\x0f\x01\xe1\x0b\x9fm\x00Q6\x12\x0cn\xb0" :'
VirusShare_7a69270f01e10b9f6d005136120c6eb0 ',

b'\xb3\x95\xbd\x98b\x83\xbb%\xe6u\xb3\xc8\x89|\xc3\x03':'
VirusShare_b395bd986283bb25e675b3c8897cc303 ',

b'\x1a\xc0\xc9,\xdd\xbe\x16\xb5Xk\xeb5\xe7\x9d\xb9\xd2' :'
VirusShare_1ac0c92cddbe16b5586beb35e79db9d2 ',

b'\xf3\x1dUo\xf3\x82\xdb\x99#\x81C\xc6\x8e\xda\x15\xb6' :'
VirusShare_f31d556ff382db99238143c68eda15b6 ',

b'?}\xa6\x13\x97\x83\xcf\x9b\xda\xb1$\x8e\xa2\xde\x10\xe1' :'
VirusShare_3f7da6139783cf9bdab1248ea2de10e1 ',

b'\xab\xd9\x7f[\xebK\xe3\xfe\x1a5\xdc\xde\x90Lq{' :'
VirusShare_abd97f5beb4be3fe1a35dcde904c717b ',

b'=\xe3~+\xc5Y\xe8\xe48\x88\xae\xafS\xc3\xed\x02' :'
VirusShare_3de37e2bc559e8e43888aeaf53c3ed02 ',

b'\x07\xab,\x9f)\x08\x8cR\xf0\x91I\x81\xfa\xcfG\x10' :'
VirusShare_07ab2c9f29088c52f0914981facf4710 ',

b'\x16\xdc\x93\x85c\xae\x15\xda\x17>~"\x1b\x15DE' :'
VirusShare_16dc938563ae15da173e7e221b154445 ',

b'\x07r\xbe\xbc\x96P&\x14.\xee\xd6\xc0\xcc\x0c\xd9\x99' :'
VirusShare_0772bebc965026142eeed6c0cc0cd999 ',

b'\xf34\xaf\xae\xd7\x9a\xf1\xb0\x18\t\x15\xa6\xf0&\xa0(' :'
VirusShare_f334afaed79af1b0180915a6f026a028 ',

b':\x86\xd16\xfc\xe2\x9c\xc93\xb9\xbbF\x9d[\xbfa' :'
VirusShare_3a86d136fce29cc933b9bb469d5bbf61 ',

b'\xd6\x84\x96\xc2\xea\xef\x13\xc8n\xb68\xd0Tn}\xa3' :'
VirusShare_d68496c2eaef13c86eb638d0546e7da3 ',

b'\x0f\xec\\4w\xa1H\x88A\xb7#\x8a\xc0l\x97\xe0' :'
VirusShare_0fec5c3477a1488841b7238ac06c97e0 ',

b'\xbd\xa5\x87\xc4Hf\xa1\x176[o!a\xbb\xdf{' :'
VirusShare_bda587c44866a117365b6f2161bbdf7b ',

b'\x17<P\xfd\x11\xf6\x8f\xe8H\x12}\\\xe5\xd4Y\xbd' :'
VirusShare_173c50fd11f68fe848127d5ce5d459bd ',

b')/\xf6\xbb62\x88g\xea\xb5\xe8\xe4i \xa5\xe0' :'
VirusShare_292ff6bb36328867eab5e8e46920a5e0 ',

b'/,\xc2\x9av\x1a&\xdf\x13\x88u\x14\xbe\xb7\x86\xe4' :'
VirusShare_2f2cc29a761a26df13887514beb786e4 ',

b'\xd1\xbf\xe6\x8c\xac\n\xeaLZV\x908\x9bp\xea\xd5' :'
VirusShare_d1bfe68cac0aea4c5a5690389b70ead5 ',

b'n\xc5W\xa1\xaa\xcaY\xe7X\xcf\x87e\xfb\xbc\xd3\x03' :'
VirusShare_6ec557a1aaca59e758cf8765fbbcd303 ',

b'o\x93\x07JT^O\x8b\x18%\xa0l\xbcJ_\xcc' :'
VirusShare_6f93074a545e4f8b1825a06cbc4a5fcc ',

b'O\xa7D\xc5\xa2\xd0\xb4\x0b\xf27h\xa6[\x0cO\x06' :'
VirusShare_4fa744c5a2d0b40bf23768a65b0c4f06 ',

b'czE\xa2\x12\x94O\xecy\x7f\xbbL\xda\xc5\x8af' :'
VirusShare_637a45a212944fec797fbb4cdac58a66 ',

b'v\x05\xaa^1E3\xbb\x11\x12}\xc9B2\xb0\xb0' :'
VirusShare_7605aa5e314533bb11127dc94232b0b0 ',

b'\xc1\xd0\xd5\xe8&\xa7\xfc\xc8N\xcd\x7fN\x9a\xa8\x81E' :'
VirusShare_c1d0d5e826a7fcc84ecd7f4e9aa88145 ',

b'X\xe9\n\x1c\xdc\xf2\xb4H\xbb\xfb\x8a)\xbcz*{' :'
VirusShare_58e90a1cdcf2b448bbfb8a29bc7a2a7b ',

b">r\xba9L,gS\xc5\x9b\xe7\xcfF\x04\x14'" :'
VirusShare_3e72ba394c2c6753c59be7cf46041427 ',

b'6\xe1"\x96\x16\x07\xc5\xca\x15d\t5lG\xef\x10' :'
VirusShare_36e122961607c5ca156409356c47ef10 ',

b'\xcb\x00\x96\x03N\nz\xb311\x16A\x87Q\xb9\xe7' :'
VirusShare_cb0096034e0a7ab3313116418751b9e7 ',

b'\x17\xa2A1\x17-c\x17<.\\\xb1\xc3\x9c\xa5\xb0' :'
VirusShare_17a24131172d63173c2e5cb1c39ca5b0 ',

b'\xf0\xaf\xb4z\xf6Ez\xdaa\xccao@\xfc\xb2T' :'
VirusShare_f0afb47af6457ada61cc616f40fcb254 ',

b'?\x81\xb1\xd7+s\x9f\x8dO\xdb\x82R\xf3\xe4y ' :'
VirusShare_3f81b1d72b739f8d4fdb8252f3e47920 ',

b'\x90\xb9PX\xf1\xfa\x1d\x1fPV\x84\x87S\xbbk\xdf' :'
VirusShare_90b95058f1fa1d1f5056848753bb6bdf ',

b'`\xe1\xf0^\x13C\x08\x83\xa2\x14\x11\xc9\x13\xf2o`' :'
VirusShare_60e1f05e13430883a21411c913f26f60 ',

b'\xcbW\xf1\xa4\x94*{\x98q\x9eJ.\x81\x84\xa80' :'
VirusShare_cb57f1a4942a7b98719e4a2e8184a830 ',

b'Mj}\x8c\xd4wl\xc3\xf5J<\xa3\xf3O5\xc4' :'
VirusShare_4d6a7d8cd4776cc3f54a3ca3f34f35c4 ',

b'\xd7\x0f[j\xa8\xa7\x82\x08Yl\xfc\x9c\x01\xc4\xe1\xf3' :'
VirusShare_d70f5b6aa8a782085949fc9c01c4e1f3 ',

b'd\x99EJ\xd3\xb6eu\x1e\xab\x83Y\xe7\xdfmz' :'
VirusShare_6499454ad3b665751eab8359e7df6d7a ',

b'\xcd\xf56s\xcfa\x1a\x86.\x98\xda\xccGP\x96\xd9' :'
VirusShare_cdf53673cf611a862e98dacc475096d9 ',

b'\x0f\x01n\xd4X\xef\xe2"L\x9aV\xb4\xb1\x11\r8' :'
VirusShare_0f016ed458efe2224c9a56b4b1110d38 ',

b'\x0e6\xc6\x8d\xef\x80\xc0U\xbe\xd6\x9f?\x06<T\xd0' :'
VirusShare_0e36c68def80c055bed69f3f063c54d0 ',

b'\x06\xcb\xe7\xa1tH\xc0xVX\x1c\xf6Mv\t\x10' :'
VirusShare_06cbe7a17448c07856581cf64d760910 ',

b'\xa39{8;JS#\xc7\xf2\x86\x0e\x16\x17\\!' :'
VirusShare_a3397b383b4a5323c7f2860e16175c21 ',

b'\x12\xa8F\x01\x9c\x15!\x1d\xe8\x92\xb5\x82\x84\xcc\x03D' :'
VirusShare_12a846019c15211de892b58284cc0344 ',

b'\xa6u]StL\x1c\x9c\xbd\x9elL\xac\x7fw\xfe' :'
VirusShare_a6755d53744c1c9cbd9e6c4cac7f77fe ',

b'Ga&\x9f\x13\x92\x85\xe7Y\xb7\x04\x00\xf9&d\x90' :'
VirusShare_4761269f139285e759b70400f9266490 ',

b'\x10\x88\xf8\xd0\x91\x9eCy\xceh\xf9\x9f\x90T\x03r' :'
VirusShare_1088f8d0919e4379ce68f99f90540372 ',

b'D\xe3\xd1\x7f\x8c\x18\xcc|/\xa20\xcf\x13^\x13\xb2' :'
VirusShare_44e3d17f8c18cc7c2fa230cf135e13b2 ',

b'\r@\xe5+\x0c\xd3\xff\x00J\x94\xed1\xeb\x1cO\x13' :'
VirusShare_0d40e52b0cd3ff004a94ed31eb1c4f13 ',

b'\x0f\xbf\x8c\x91\xaf\xd0\x999\xc5\xad~\xdc^\xbb<b' :'
VirusShare_0fbf8c91afd09939c5ad7edc5ebb3c62 ',

b'L\xd5S\xe2T\xe2\xe8\xee\x92&x>u\x90\x90\xd2' :'
VirusShare_4cd553e254e2e8ee9226783e759090d2 ',

b'9{\xdfP\x0bW\xe7\x1fl\xa8\xdb\x92\x0f\xa6.\xaf' :'
VirusShare_397bdf500b57e71f6ca8db920fa62eaf ',

b"\xde'f\xa2~#+\xc4\xfdD\xd8\x9c\xfaG\x8f>" :'
VirusShare_de2766a27e232bc4fd44d89cfa478f3e ',

b'\xd7\\\x90\x87v\xa9&\xf4\xf2\x16\xdd^\x07\xa5Xe' :'
VirusShare_d75c908776a926f4f216dd5e07a55865 ',

b'\x97\xec\xa4?\x0b]\x7fd\xf1%|d\x18X\x18D' :'
VirusShare_97eca43f0b5d7f64f1257c6418581844 ',

b'\xa8"\xf4 \xbb\x9c\x99\x17(\xf4\xfd}\xcd\xd7"'' :'
VirusShare_a822f420bb9c991728f4fd7dcdd72222 ',

b'\x91\xc1\x10n\xf5q\x89k\x81\xf6\xc9L\xfa\x9d\t\xbc' :'
VirusShare_91c1106ef571896b81f6c94cfa9d09bc ',

b'+E\xd8y\xff(-\x05@+\xf3$\xacl\xe1\x80' :'
VirusShare_2b45d879ff282d05402bf324ac6ce180 ',

b'\xaa6}\x94\xa8#F\x0e\x14\xec_D\x9cf\x94j' :'
VirusShare_aa367d94a823460e14ec5f449c66946a ',

b'\xccy\t\xaa\xfcY\xe2/\xf7gU\xe5\x17Hf\x11' :'
VirusShare_cc7909aafc59e22ff76755e517486611 ',

b',rU\xb4%\xa9y\xa0\xd0\xfdAw\x94=\x8az' :'
VirusShare_2c7255b425a979a0d0fd4177943d8a7a ',

b'/\xce\x1e\xd1\x91,\xfc\x90\xb5}\x84\xae\xea\x8a\x02\x93':'
VirusShare_2fce1ed1912cfc90b57d84aeea8a0293 ',

b'\x0fb-\x0f\x08j\xed\xe7^.\x87\x93"\xf9\xd99' :'
VirusShare_0f622d0f086aede75e2e879322f9d939 ',

b':-hW\x8c\xd6b\x1e\xfd?)#\xc5\xf9\xff@' :'
VirusShare_3a2d68578cd6621efd3f2923c5f9ff40 ',

b'\x9bQ\x8a\xdf@\x1e\x10\xe2\xa9&T\xbbk\xde\x1d\xc5' :'
VirusShare_9b518adf401e10e2a92654bb6bde1dc5 ',

b'\x93=\x9a\xc5\xb3\xcb\xce\xc3\xcb\xac\x0b\x8e\x14\xd8\xbd\xc1'
:' VirusShare_933d9ac5b3cbcec3cbac0b8e14d8bdc1 ',

b'\x99\xb2\x8d\x82\xf4\x0f\xaa\xdf\xe5\xcf9]\xde\xa8e(' :'
VirusShare_99b28d82f40faadfe5cf395ddea86528 ',

b'd~\xb7\xab\x9e\xe7,\xdf\x833C\xcc\xcad\xcd~' :'
VirusShare_647eb7ab9ee72cdf833343ccca64cd7e ',

b'\x1at\xae\'\xb8\xf3\x96\x8b\x9f",\xe9\xf9O\x90\xd0':'
VirusShare_1a74ae27b8f3968b9f222ce9f94f90d0 ',

b'k\x90\x98\xc3\x8f_\xe4\x83\xdb\x92k\xc5\xc6\xc7A\xe0' :'
VirusShare_6b9098c38f5fe483db926bc5c6c741e0 ',

b'K\xb0b\xcd\x17\x1dcK@\xf9:5@y\xe4P' :'
VirusShare_4bb062cd171d634b40f93a354079e450 ',

b'&\x0e\xac\xbd;A\x937\xf4i\xab\xa2h\x0b\x98`' :'
VirusShare_260eacbd3b419337f469aba2680b9860 ',

b'\xd3\x1e\xfe\x98\x08\x8eD$\xf0\xe8\xd3"L\x1d\xe5P' :'
VirusShare_d31efe98088e4424f0e8d3224c1de550 ',

b"\xf0\xa4)4\x8cS\xe56\x14\x0e'\xad$\x82\x80\x8e" :'
VirusShare_f0a429348c53e536140e27ad2482808e ',

b'\xf5\xf6\x155%\x8b\xa0\xa7\x12\n4\xea_\xda[p' :'
VirusShare_f5f61535258ba0a7120a34ea5fda5b70 ',

b'\xc1\x1d\xe2\x93\xfa\xbd\xd1\x10\xcd\xcf\xba\xe6\xe2@\xefp' :'
VirusShare_c11de293fabdd110cdcfbae6e240ef70 ',

b'\x1d\x86!O\xb2\xe5\xe9\xdf\x06\x04F\x14y\\\x17\x10' :'
VirusShare_1d86214fb2e5e9df06044614795c1710 ',

b'n\xbd\xe8A@\x03\xb8\xa0\xbd8\x06\x84\xa7\xc0Hc' :'
VirusShare_6ebde8414003b8a0bd380684a7c04863 ',

b'\xb5R\xc1\x03"L\xe7\x8b\xd1\xf5\xe5\x96$E\xdd\x80' :'
VirusShare_b552c103224ce78bd1f5e5962445dd80 ',

b'\xdbXi\xb5\x8e\xb4\x80><\x82p\xdb"\xc5\xa2q' :'
VirusShare_db5869b58eb4803e3c8270db22c5a271 ',

b'l*f\xe1d4\xe9\xe6\xde\xbb\xa2\xb3z\xe7\xbeP' :'
VirusShare_6c2a66e16434e9e6debba2b37ae7be50 ',

b'\xc3@l\xc6\xb6V\x07\xe8\x15\xd6Qf@\xa2\xf2\xcd' :'
VirusShare_c34049c6b65607e815d6516640a2f2cd ',

b'\x94\xa1\xdc\xda\xe6\xd1y#\x07\x9d\xba\xfeV7u\xf0' :'
VirusShare_94a1dcdae6d17923079dbafe563775f0 ',

b'p\x17\xbav\x18-c(\xf1(:2?]\x9ai' :'
VirusShare_7017ba76182d6328f1283a323f5d9a69 ',

b'\x15\xee\xf6\x041>\x0e>\x9dy\xb1M\x0ef+b':'
VirusShare_15eef604313e0e3e9d79b14d0e662b62 ',
b'\xe5UOA\t(\xa1\xf7R\xde\x98\x9f\xcf]\x99\xac' :'
VirusShare_e5554f410928a1f752de989fcf5d99ac ',
b'\xc1\xd1c\x1aH\xd3\xe9\xae\xb0\xeeu`\xc9\xe0EE' :'
VirusShare_c1d1631a48d3e9aeb0ee7560c9e04545 ',
b'\xb2\xc1\n\xb1\x18@n\x85\xaa\x89\x87\xf1.e\xfc0' :'
VirusShare_b2c10ab118406e85aa8987f12e65fc30 ',
b'\xdb\x0c\xa7\xbbsm\x11\xd8\xf3\x80\xb1|2\xc5\xbe\xdd' :'
VirusShare_db0ca7bb736d11d8f380b17c32c5bedd ',
b'\xf3\x912\x17\xafK\xa03X\x12\xfe\xb5\xd04\x90F' :'
VirusShare_f3913217af4ba0335812feb5d0349046 ',
b'M\xdd\xb9\x8d|\xd0f\xb3[a\xa4\x95F3\x9d\xd7' :'
VirusShare_4dddb98d7cd066b35b61a49546339dd7 ',
b'\xb4\x98=\xd8\xe4 l/lw\x0fV\xd50\xec\xa3' :'
VirusShare_b4983dd8e4206c2f6c770f56d530eca3 ',
b'\x96\xd26\x95\xd2\x9bg\xcd\xe9Z\x97\x80dY\xb3@' :'
VirusShare_96d23695d29b67cde95a97806459b340 ',
b'\x97y\x96\x82\x1e\xaejd\xc6\xb8L2-C\xb8\xbf' :'
VirusShare_977996821eae6a64c6b84c322d43b8bf ',
b'\xdd:\x8ee\x08w\x8be\x8aa\x16\x0b\xba\xfe\xa6\xc0' :'
VirusShare_dd3a8e6508778b658a61160bbafea6c0 ',

b'\xed\x89\xeaS\x0c\xc7&1\xc2\xcbc(\x7f[\xdc\xdb' :'
VirusShare_ed89ea530cc72631c2cb63287f5bdcdb ',

b'\xe8\xf8 \xbc#ar\xc1\xde;\x14w\xf3,.y' :'
VirusShare_e8f820bc236172c1de3b1477f32c2e79 ',

b'\xdf\xa1P1\x85\xaa\r:\x8ap3\xa9f\x14Y\x10' :'
VirusShare_dfa1503185aa0d3a8a7033a966145910 ',

b'\x19\\)\x87s\x97\xc9\xc9,\x8a\x04!\xd7\x16\xb8@' :'
VirusShare_195c29877397c9c92c8a0421d716b840 ',

b'H\xf1\x17\xf6\x0c\xf3\x1c\x9a_\xad8\x90\x9eWiF' :'
VirusShare_48f117f60cf31c9a5fad38909e576946 ',

b'C\x1c\xe2"\xa5\xa8\xd8ZeH}\xed2;3\x8a' :'
VirusShare_431ce222a5a8d85a65487ded323b338a ',

b'@@\xb7\x7f\x02k\xac\xdd\x18\xd8<\x97Y\x86\x98\xb6' :'
VirusShare_4040b77f026bacdd18d83c97598698b6 ',

b'2S\r\x17\xadY\x92 1p\xf0\x8di\\\xb8B' :'
VirusShare_32530d17ad5992203170f08d695cb842 ',

b'\xa8\xe4\xbde\xeem\xf4C\xfa, \x96c\xf05\xeb' :'
VirusShare_a8e4bd65ee6df443fa2c209663f035eb ',

b'\xc5\x920\x07\x9esju[\xf1g\xea\x13d\xe1\xf7' :'
VirusShare_c59230079e736a755bf167ea1364e1f7 ',

b',\xf8A\xb5*\xb8\xd5:\x9e\x02\xe7\x99l0\xbdp' :'
VirusShare_2cf841b52ab8d53a9e02e7996c30bd70 ',

b'\x0b;[ZKj~\xf56\xbb\x9e\xe9\x98\xb2\x17\xd0' :'
VirusShare_0b3b5b5a4b6a7ef536bb9ee998b217d0 ',

b"'\xb6\x10\x06l\xaf\xf0\xb8F\xf7/\x1bIq\x88\x80" :'
VirusShare_27b610066caff0b846f72f1b49718880 ',

b'\xbaQheC\x8b`D\xe0`\xfaT6\x96M\x0e' :'
VirusShare_ba516865438b6044e060fa5436964d0e ',

b'd\xcc\xff\x14\x16\x14\xb0\x8fQ\x86\xe5s`\xb1=\xac' :'
VirusShare_64ccff141614b08f5186e57360b13dac ',

b'x\xb3\xc1\xff\xbbg\x1f\xbb\x0c\x03\xe1\xde\x15+\xc2\xb4' :'
VirusShare_78b3c1ffbb671fbb0c03e1de152bc2b4 ',

b'X\xddf\xe7\xbf\x07\xaa\x91\x8dDl\xf7\xfao\x00\x8a' :'
VirusShare_58dd66e7bf07aa918d446cf7fa6f008a ',

b'\xfc*\x11\xb0\xe4_&\xa5\x1a\x03\xec\xa1\xe4\xfe\xdc\x02' :'
VirusShare_fc2a11b0e45f26a51a03eca1e4fedc02 ',

b'U\xb3\x11\xcd\x9a\xdd\xfc\xbf\x94\xc7\x80\x0f \x9a[4' :'
VirusShare_55b311cd9addfcbf94c7800f209a5b34 ',

b'p"\x1d\xb3w\xe3\xb1\x9b\x1ay\x9a?\xcd\xd39h' :'
VirusShare_70221db377e3b19b1a799a3fcdd33968 ',

b'D\xa9\xb3\x87\x88\x84\x8a\xde\x96\xf0\xa0\xcf3\xfd3\x1f' :'
VirusShare_44a9b38788848ade96f0a0cf33fd331f ',

b"\xa3>\xe1\xe9W\xdeQ*\x97'm\xd3\xb9/\xed?" :'
VirusShare_a33ee1e957de512a97276dd3b92fed3f ',

b'\xeb\xf8L\xf4\x1b\xf5s\xeb7d\x1fg\xeap\x13\r' :'
VirusShare_ebf84cf41bf573eb37641f67ea70130d ',

b'\x84\xf5\xbbK\xa0\xd7\xa1-\x03R\xed_\x9cc\x0b\xc1' :'
VirusShare_84f5bb4ba0d7a12d0352ed5f9c630bc1 ',

b'2TyuF\x0eT\x99\x1f\xea#\xddh\x8a\xc0\xf0' :'
VirusShare_32547975460e54991fea23dd688ac0f0 ',

b')\xd8N\xa2\x91{\xcb\x89\x00\xcdl\xc6\xc4\xccL\x98' :'
VirusShare_29d84ea2917bcb8900cd49c6c4cc4c98 ',

b'K\xb48TRi\x96X\xf4WkM\xf4\xf4\x98\xec' :'
VirusShare_4bb4385452699658f4576b4df4f498ec ',

b'\x98\xee\\\x10o\xe9\xa4\x17\xfc^\xdc2!\x17\xc9\xbd' :'
VirusShare_98ee5c106fe9a417fc5edc322117c9bd ',

b'l*\x88\x8e\xfbXg\xbf\x83\xb5\xc98\x01\xe8f!' :'
VirusShare_492a888efb5867bf83b5c93801e86621 ',

b'\xb6\xa3&?O\xb1"\x99\xa9\xd7\x8a\x1a\xae\xb27\x84' :'
VirusShare_b6a3263f4fb12299a9d78a1aaeb23784 ',

b'\xe2\xf0\xa3)\xf3~\x8b\xd0\x99\x06_\xdc=d\x16\xb0' :'
VirusShare_e2f0a329f37e8bd099065fdc3d6416b0 ',

b"'-\x82\xd2v\xc7\xb6\xb5\x8c\xc8\xed\xcdvm:\x90" :'
VirusShare_272d82d276c7b6b58cc8edcd766d3a90 ',

b'O\x14\x88\xbd\x08?P\x83/\x06\xbd"~\xf7\xb1`' :'
VirusShare_4f1488bd083f50832f06bd227ef7b160 ',

b'\xe1E\xaa\xcf\xfdT7\xe3\x05Wj\x17yZ\xc3\\' :'
VirusShare_e145aacffd5437e305576a17795ac35c ',

b'\\\x1d"F\x1c\xe1\xb4\x85,G\xbe\x0fd\xb2\x0f/' :'
VirusShare_5c1d22461ce1b4852c47be0f64b20f2f ',

b'3v]\x0f\xee<\xbc\xd9\x96]|\xb1\xa3\xeb\xcb\x94' :'
VirusShare_33765d0fee3cbcd9965d7cb1a3ebcb94 ',

b'\xac\x19De\xff,\xf8UB\xdf\x1e\xb3]\x9c\n\xdc' :'
VirusShare_ac194465ff2cf85542df1eb35d9c0adc ',

b'\x80J\x86\x8d\x00\xedL\x04\x11qF\x0eLXy\x82' :'
VirusShare_804a868d00ed4c041171460e4c587982 ',

b'\xe2"o\xb2\x9c\xc4\x806>l\xddl.\xee\x7f\x8c' :'
VirusShare_e2226fb29cc480363e6cdd492eee7f8c ',

b']*\x8e\x9a\xd3\x8b\xddb\x81\xd0*\x8b\xe4N\xd5\xaf' :'
VirusShare_5d2a8e9ad38bdd6281d02a8be44ed5af ',

b'\x0bxa\xd8Z\x8620\xd8\xef.\xa8b(6D' :'
VirusShare_0b7861d85a863230d8ef2ea862283644 ',

b'\xa2A\xedl\x12\xc6\x94\xf1\x91\x96\xd0\xa1-\xbdL@' :'
VirusShare_a241ed6c12c694f19196d0a12dbd4c40 ',

b"3\xa3e\x84\xcaZ5\xdeu\x1eMxX\xaa'\x86" :'
VirusShare_33a36584ca5a35de751e4d7858aa2786 ',

b'\xcf}\x0bA^\xba\xcdL\xa3\xba\x90\xfc\xadmk\xa3' :'
VirusShare_cf7d0b415ebacd4ca3ba90fcad6d6ba3 ',

b't\xa9\x93\x0b\xc7\xf9\x06\\\x80:S\x9b\x8f\x809\xa5' :'
VirusShare_74a9930bc7f9065c803a539b8f8039a5 ',

b'\xa4M\x1d\x8a\r\xfa\x1f\xa8\x05\x915\xb0\xf8\xce\x9aU' :'
VirusShare_a44d1d8a0dfa1fa8059135b0f8ce9a55 ',

b'\x8e\x8e\x82\x04\xce\t\xaa[\xaa\x14[\xdd>\x94\x9e\xcb' :'
VirusShare_8e8e8204ce09aa5baa145bdd3e949ecb ',

b'lo\x9b\xfd\x8f"\xb1\x10\x17\x17\xef\x94\x8e\n\xeb\xbb' :'
VirusShare_6c6f9bfd8f22b1101717ef948e0aebbb ',

b'"\x94\x95\xddbST\x07`\x9e\x8e\xac>\xae\xfbd' :'
VirusShare_229495dd62535407609e8eac3eaefb64 ',

b'H\x87\xdd\xc5z\x84\x12\x97c\xdc\xad\x80<\xac%\xb4' :'
VirusShare_4887ddc57a84129763dcad803cac25b4 ',

b'HJ>\x99!za\xd8q\x96\xbe\x0fTL\xbb\x8a' :'
VirusShare_484a3e99217a61d87196be0f544cbb8a ',

b'8*\x00y\xeal\x87=\xc7\xa5\x19\xc3@\xc1\xd4\x80' :'
VirusShare_382a0079ea6c873dc7a519c340c1d480 ',

b'P\xf7zd\xe5\xecb\xc6\x1c\x06\xc3\xd4sR\xe0\xa6' :'
VirusShare_50f77a64e5ec62c61c06c3d47352e0a6 ',

b'\xa9\x15R\xb7f.\xc5LD1\xb0M\x91`2\x0c' :'
VirusShare_a91552b7662ec54c4431b04d9160320c ',

b'f\x16\x80\x04\xd9o\x0f\x05\xbf,\x12p\xc9eP\x81' :'
VirusShare_66168004d96f0f05bf2c1270c9655081 ',

b'\xb0.\xb5\xed\xf1B{\xd6\x00\xf2BI\xb1M\xa6p' :'
VirusShare_b02eb5edf1427bd600f24249b14da670 ',

b'/nY\x12\xedK/O\xce\x9f>\xe0!\x7f\x11b' :'
VirusShare_2f6e5912ed4b2f4fce9f3ee0217f1162 ',

b"\xfe\x95\x99)\x08'\xae\x8fTb\xb2\xc2\x90p6\xc5" :'
VirusShare_fe9599290827ae8f5462b2c2907036c5 ',

b'\x18\xfa\xef\x85DCA\xde\xed}gWS+g\xff' :'
VirusShare_18faef85444341deed7d6757532b67ff ',

b'C\x0fW\xa5\xcf\xfd\xf6\x98\xcd\x9c\x97\xd8`b%-' :'
VirusShare_430f57a5cffdf698cd9c97d86062252d ',

b'\xa3\x9b\x7f\xf0g\xe2\tu\xf7\x88\xb1\x1f\xec\x11\x92\x96' :'
VirusShare_a39b7ff067e20975f788b11fec119296 ',

b'J\x10^K1\x95W\x89\xd2\r\xe6\xe6\x9ebY6' :'
VirusShare_4a105e4b31955789d20de6e69e625936 ',

b'\x95b\x81\x05[\x82\xf1\xcb\xb9\x19|\x86)<x\x1f' :'
VirusShare_956281055b82f1cbb9197c86293c781f ',

b'\x98\x88-\x0f\x0f\xab\xe9\xdfK{\xed\xd3\x01\x089U' :'
VirusShare_98882d0f0fabe9df4b7bedd301083955 ',

b'e\x8e\x93\xe2\xd3\xa1\xb7B]\xec\xa5\x10\xc2/\x93R' :'
VirusShare_658e93e2d3a1b7425deca510c22f9352 ',

b'\x15\xcfIL\x9d\x1b\xe9;\x8e\x98\xff\xac_=\xf0\xe9' :'
VirusShare_15cf494c9d1be93b8e98ffac5f3df0e9 ',

b'\x15_6\x964.\xa7;\xa0\x99\xa7\xa2\xaaZ\t\xf5' :'
VirusShare_155f3696342ea73ba099a7a2aa5a09f5 ',

b'\xba\x84\x8a\x9d\xc1\xd5}\xd7\xb5\xb9\xa4\x0bHR\x17\r' :'
VirusShare_ba848a9dc1d57dd7b5b9a40b4852170d ',

b'C\xa6\x99o\xd6\x0c8\x84q\xb4\xc93\x8b\xd3\r\xa0' :'
VirusShare_43a6996fd60c388471b4c9338bd30da0 ',

b"\x8fs`ih\xa4F|\xad\x028DT\x8f'3" :'
VirusShare_8f73606968a4467cad023844548f2733 ',

b'\x8b\x9cJ\x10#s\xfbG|\x94[h\xbe\x11\x14\xd0' :'
VirusShare_8b9c4a102373fb477c945b68be1114d0 ',

b'h^(\x85c*\x84aX\x84\xd3\xa418S\xc6' :'
VirusShare_685e2885632a84615884d3a4313853c6 ',

b'\x03ZU\x97\x89\xf7?\xba\xc7&\x0e\xd2\xb9K8\xc7' :'
VirusShare_035a559789f73fbac7260ed2b94b38c7 ',

b'\xde\xddj-\x0cC\xdd9ipG\x02\xb7@\xc0\xc9' :'
VirusShare_dedd6a2d0c43dd3969704702b740c0c9 ',

b'\x9a\xa7\x85\xc4\x94\x19\xbd\x8f>\xf7\r\x82\xab\x83\xb3\x89' :'
VirusShare_9aa785c49419bd8f3ef70d82ab83b389 ',

b'\xf1\xe3\x05\xa8\x90\x8a\xe8\n\xfc\xd5\xf66\x15\xe3*\x80' :'
VirusShare_f1e305a8908ae80afcd5f63615e32a80 ',

b'\xcc\xbb\xb1\x9ag\x81*\xbbV6x\xfaV.\xc3\xb6' :'
VirusShare_ccbbb19a67812abb563678fa562ec3b6 ',

b's1+\xed\xa3\x16\xf6R\x94\xe4ci\xbd\x94\xd6\x92' :'
VirusShare_73312beda316f65294e46369bd94d692 ',

b'\xd2\x05%\xe6\x98\x04\x81\x81\x9e-1\xd4Yh\xdd?':'
VirusShare_d20525e6980481819e2d31d45968dd3f ',

b'*Y\x1e\xed\x7fB\x971\xf3\xc8\xcd\xba\xbdd\x0f\xd6' :'
VirusShare_2a591eed7f429731f3c8cdbabd640fd6 ',

b'\\\xd5O}\x86\x97\x08\x8b\x05\xcbk\x8f-[o\xe3' :'
VirusShare_5cd54f7d8697088b05cb6b8f2d5b6fe3 ',

b'\t>\x17\x91\xa4\xce\xb3\x06#\x8a\xfd\xe6*Q\xd7\x02' :'
VirusShare_093e1791a4ceb306238afde62a51d702 ',

b',\xbb\xceb\xd8\xfd\xb1\xd2\x7f\xef\xc5\xe8\xc5\xc2\x8e\xb5' :'
VirusShare_2cbbce62d8fdb1d27fefc5e8c5c28eb5 ',

b'\xf6\xa0}\xc9S=\x19\xae\x04\x96\xb7\x9f\\\xa6\xb9:' :'
VirusShare_f6a07dc9533d19ae0496b79f5ca6b93a ',

b'e\x11\xe23\xd7\xb4\x11N\x8f\x93C\xd0\xdc\x18\xcbR' :'
VirusShare_6511e233d7b4114e8f9343d0dc18cb52 ',

b'\\,8\xb0\xfb\x950\xa2\xdb\x98\xce\xe9\xb5\x80\x85\x92' :'
VirusShare_5c2c38b0fb9530a2db98cee9b5808592 ',

b'Q\x89\xee\xce?\x91e\xe3\xe6\xb05\xb3z\xdb\x81\xf9' :'
VirusShare_5189eece3f9165e3e6b035b37adb81f9 ',

b'\x1b\xbc\xd3O\x19M\x1a_#>h\x9f\xd1\x11\x0f\x80':'
VirusShare_1bbcd34f194d1a5f233e689fd1110f80 ',

b'Q<mk]~N\xf2l\xf8\x19\xba\xd6HV\xf3' :'
VirusShare_513c6d6b5d7e4ef249f819bad64856f3 ',

b'\xc64;\x02]\xe6)k}f*\xd67\xf45\xf0' :'
VirusShare_c6343b025de6296b7d662ad637f435f0 ',

b'\xfb\x94\t\\\x90\x87 \x97\xafH\x9e\x0e\x97\xfe\n\xa3' :'
VirusShare_fb94095c90872097af489e0e97fe0aa3 ',

b'\xce\xd5\xde\x80C\xca\xc1\xb2\xccu\xc7:\x00\xc8N\x8c' :'
VirusShare_ced5de8043cac1b2cc75c73a00c84e8c ',

b'u\x9fM[\xe7\xb6\xa5\xcf1\xb0\xccet\x0f&@' :'
VirusShare_759f4d5be7b6a5cf31b0cc65740f2640 ',

b'\xc1\x1e@e\x1bC\xdbB\xf3}t\x9ai\xcdQ\x85' :'
VirusShare_c11e40651b43db42f37d749a69cd5185 ',

b'G\xddl\xa7$\x95Y\x7f\xd0%\x81\x11BS\xfa\xbf' :'
VirusShare_47dd6ca72495597fd02581114253fabf ',

b'GL:\xfa9\x933\x162\xcc\x0f\xfb\x01h=\xa0' :'
VirusShare_474c3afa3993331632cc0ffb01683da0 ',

b'\n\xd5\x88\x19\xb2\xd2\xd1 \xee\x01\xbdy\xf0/\x86-' :'
VirusShare_0ad58819b2d2d120ee01bd79f02f862d ',

b'\xd2c\x9e\xa9\xaf\x9a\x8a\xe12\xda\x1b\x94,\xc5V`' :'
VirusShare_d2639ea9af9a8ae132da1b942cc55660 ',

b'^\xe5e\xf400,\xb1\xac\xbc4\xa7\xf3\xa3\x1f\xf4' :'
VirusShare_5ee565f430302cb1acbc34a7f3a31ff4 ',

b'\xf6\x02\x13\x17R<\x16K\xa52>\xe7q\xd2K\x98' :'
VirusShare_f6021317523c164ba5323ee771d24b98 ',
b'rn\xe4\x11\xff\xdc\x94\xe5\x17,8=\xefPd1' :'
VirusShare_726ee411ffdc94e5172c383def506431 ',
b'\xfb\xb0%:*\xdfi\x96\x04/\xff\x9dH\xfb\xbb`' :'
VirusShare_fbb0253a2adf6996042fff9d48fbbb60 ',
b'\x1eu\x01\xc5@\x18\xcf\xc61\xad\xe1\xda\xe3\xa2\x83\xd0' :'
VirusShare_1e7501c54018cfc631ade1dae3a283d0 ',
b'B\x0c\xed\xb3\x8da\xf5\x81c\x04\x9cK\xa1\xcf*/' :'
VirusShare_420cedb38d61f58163049c4ba1cf2a2f ',
b"&\\\xa3\xce\xa6\x1e'\xa9\x1a\xe7=T\x8dKR\xe0" :'
VirusShare_265ca3cea61e27a91ae73d548d4b52e0 ',
b']$\x89Y\xefqPDL\x81\x15\xf4\xecz\xc8\xb0' :'
VirusShare_5d248959ef7150444c8115f4ec7ac8b0 ',
b'\x8c\x88\xb9B"\x92\xae@\x10\x9c\x9f]5\xf9\xb8\x0b' :'
VirusShare_8c88b9422292ae40109c9f5d35f9b80b ',
b'\x8e\x87\xac\x15\xe1\xf24B\x9a\xf4\x19\x9al\x03y\x98' :'
VirusShare_8e87ac15e1f234429af4199a6c037998 ',
b'\xbc\xf5hBN\xfe,/\x95GG\xa1\x0e\xb90z' :'
VirusShare_bcf568424efe2c2f954747a10eb9307a ',
b'\xa6C\xfcM\xf5v\x9c\xc5a\xb6]\xeai\xa1\xe5\x86' :'
VirusShare_a643fc4df5769cc561b65dea69a1e586 ',

b'\xd5\xf1^\x9c\x0b\xcb\xean\x14p\xe7J**n\xd2' :'
VirusShare_d5f15e9c0bcbea6e1470e74a2a2a6ed2 ',

b'W\x92&A"Q\x135\xe4\xa3\xb3o\xa7\xa5)\xf0' :'
VirusShare_5792264122511335e4a3b36fa7a529f0 ',

b'K\tGP\xef\x1b\xae\xf4\xeb\xee4A\xda\xf0\xa00' :'
VirusShare_4b094750ef1baef4ebee3441daf0a030 ',

b'\x8b\xaf\x8f\xcb\xbaZ\xd0\x03m\xaa\xbf\x1ag\xe9\xa3\xd0' :'
VirusShare_8baf8fcbba5ad0036daabf1a67e9a3d0 ',

b'\xe7\x9b\xa0\x9f\x83[\xd4\x17\xc7Wy8&\x10\x930' :'
VirusShare_e79ba09f835bd417c757793826109330 ',

b'\xd2\x14\xdf\xba\x82\xf9\x07Z\x9fD\x86[q\x90&\xf4' :'
VirusShare_d214dfba82f9075a9f44865b719026f4 ',

b'\xb5\x1f\xd8\xf9\xddu\xdb\xe0\xc6\xfb\x995\xfdj\x1eQ' :'
VirusShare_b51fd8f9dd75dbe0c6fb9935fd6a1e51 ',

b'v\x9f\xfaG~\x14M6E\x08\x9d^Q\x86\xb7\xb0' :'
VirusShare_769ffa477e144d3645089d5e5186b7b0 ',

b'\xe5Z\xd0O\xad\xaeW\xa1\xbf\xe5F\xd8\xc1\xbd\xe9\xff' :'
VirusShare_e55ad04fadae57a1bfe546d8c1bde9ff ',

b'\xe8\x08\x80\xc6\xa8\xedb\xa9\xa8\x12QPS\x03\xff\xdc' :'
VirusShare_e80880c6a8ed62a9a81251505303ffdc ',

b'3\x93\x14BXJ\x8b\x07\xdal\xee\x15K^\x98\xb9' :'
VirusShare_33931442584a8b07da49ee154b5e98b9 ',

b'\xcd>\xb4\xbe\xa3\x9e\x96H\xe8\x06:\x0e\x0f\x97s\xf0' :'
VirusShare_cd3eb4bea39e9648e8063a0e0f9773f0 ',

b'\xe5\xa4\x8c\x9c\x9e\x95\xefo\x81\xb8\xabw\xef\xd4g\xe0' :'
VirusShare_e5a48c9c9e95ef6f81b8ab77efd467e0 ',

b'\x10\x9d;H\x1b\xcc\xa2\xd8\xb2&r\x9bF\x98\x18^' :'
VirusShare_109d3b481bcca2d8b226729b4698185e ',

b'y~\xf0\x96\x89\x1aq\xdeX\xe3\x07\xaa\xcac\xda ' :'
VirusShare_797ef096891a71de58e307aaca63da20 ',

b'c\x92\xe2xN\xcf\xf8\xe7\xb1C\xd6\xf3\xad\xcd,\xec' :'
VirusShare_6392e2784ecff8e7b143d6f3adcd2cec ',

b'8/\x80\xbe\x13 2j%A0e/\x9c\xcf\x02' :'
VirusShare_382f80be1320326a254130652f9ccf02 ',

b'+\xfb\x0e\xf1\xb8\x11$\xcaa\xc9<4\x1a\x9e\xd1d' :'
VirusShare_2bfb0ef1b81124ca61c93c341a9ed164 ',

b'\xf44\xff\xb5\xc0\xeeA\x10s\x01\xcd\xd2\x87\x0b\x8c\xb3' :'
VirusShare_f434ffb5c0ee41107301cdd2870b8cb3 ',

b'\xfd2\x02\xa5w\xe2\x1b\xd5\xf2>@\x04y\rE\x9e' :'
VirusShare_fd3202a577e21bd5f23e4004790d459e ',

b'\xaf\xc1?\xde\x86)\x8ej\xed\x10zGl\rq\xc2' :'
VirusShare_afc13fde86298e6aed107a476c0d71c2 ',

b'\xabR\xf3\xa1>t\xc6X\xf5[\xc4\xdbUZ\x98\xc7' :'
VirusShare_ab52f3a13e74c658f55bc4db555a98c7 ',

b'Y\xfaV\x03\xcf\xe5\xb7\xfd$,N\xd7\n\x87\xdf\xa0' :'
VirusShare_59fa5603cfe5b7fd242c4ed70a87dfa0 ',

b'\x8f\xbb\xa3\t\x1c\x0b\x86\xfb\xf1\xc1\xc4P\xd8g\x0c\xd0' :'
VirusShare_8fbba3091c0b86fbf1c1c450d8670cd0 ',

b'\xd2\x98&\xb4\xe6\x17\xe3yo\x14\x12\x8f\x0bn\xc0G' :'
VirusShare_d29826b4e617e3796f14128f0b6ec047 ',

b'\xdf\x85\xa9\x89\x9bh\x01l{\xb0\xf7c)\x94\xdb\x10' :'
VirusShare_df85a9899b68016c7bb0f7632994db10 ',

b'\x01\xa8\xc4\xb8$>\xde\xad\x1f\xf6\xde\n\x9d\x9f\x01\xd0' :'
VirusShare_01a8c4b8243edead1ff6de0a9d9f01d0 ',

b'\xa4\xda\xb5\x83\xed|\xeb\xa1\xe8\x15)\x1e\x19\xcd\xb6\xb1' :'
VirusShare_a4dab583ed7ceba1e815291e19cdb6b1 ',

b'\xc1 \x9ey\x1eO\x8a\xff\x06\x13\xd9\x9b\xda\xca\xd4\x07' :'
VirusShare_c1209e791e4f8aff0613d99bdacad407 ',

b'\x9a\x06J\xc21\x96\x0b\x00v(T\x802\xa5\xec\xb7' :'
VirusShare_9a064ac231960b007628548032a5ecb7 ',

b'#\xc8\xc5[\xe3ySIp,\x14\x9e\xeb1\xc6\x84' :'
VirusShare_23c8c55be3795349702c149eeb31c684 ',

b'\xaa(\x01\xb8!\x82\xbc\xac0P\xe0\xa1!\x0c\x1a\xc4':'
VirusShare_aa2801b82182bcac3050e0a1210c1ac4 ',

b'\xe3\xcb\xe8\xaf=\x18\x8e_s\xca\xd3\xb2\xf0\xb4/\xf0' :'
VirusShare_e3cbe8af3d188e5f73cad3b2f0b42ff0 ',

```
    b'\xe4<\xbe\xe7\x8a\xdan\xbf\xa8~Z\xa2\x8c\xbeU4':'
     VirusShare_e43cbee78ada6ebfa87e5aa28cbe5534        ',

    b'\xc6\xa3ft\xb4O\xce\x0fiC\x8a\x03w\xcb\x19m'       :'
     VirusShare_c6a36674b44fce0f69438a0377cb196d         ',

    b'\xe0\xdd]\xa1\xbfEj\xa2N[\x00\xa8\xd0{\x02\x8b'     :'
     VirusShare_e0dd5da1bf456aa24e5b00a8d07b028b        ',

    b"\xb2\x13\xf7\x89\x190Lw'\x8c\xd9\xce\xe7\xab\x99\x8b"  :'
     VirusShare_b213f78919304c77278cd9cee7ab998b        ',

    b'l\x8c\xe8\xfa&\x86+"\x80\xc3(\xd7\xe9\xe5\x92\x06'          :'
     VirusShare_498ce8fa26862b2280c328d7e9e59206        ',

    b'`c\xad\x8c\x10\xa5-\xbb\xa9A\xd4nc\x04\xfd\x94'   :'
     VirusShare_6063ad8c10a52dbba941d46e6304fd94        ',

    b'\x18\xff\x94\x8aq\x8f\xe9\xd0\xe3\x9d#\xae\x82\x9d\xe4\xc0'    :'
     VirusShare_18ff948a718fe9d0e39d23ae829de4c0         ',

    b'\x8e\xe8\x95\xa2\xaf\xc6C\xcah \x06\x03$\xf2\x9e\xec'     :'
     VirusShare_8ee895a2afc643ca6820060324f29eec         ',


}


class RansomwareDetectorApp:

    def __init__(self, master):
```

```
        self.master = master
        self.master.title("Ransomware Detector")
        self.master.geometry("700x500")

        # Initialize variables
        self.selected_dir = None
        self.ransomware_found = False

        # UI elements
        bg_label = tk.Label(root, image=bg_image)
        bg_label.grid(row=0, column=0, columnspan=2)

        frame = tk.Frame(root, bg='white', borderwidth=2, relief="groove")
        frame.place(relx=0.5, rely=0.7, relwidth=0.9, relheight=0.4,
anchor='center')

        self.select_dir_button = tk.Button(frame, text="Select Directory",
command=self.select_directory)
        self.select_dir_button.place(x=5, y=2)
        self.select_dir_button.config(height=2, width=15)
```

```
        self.select_dir_label = tk.Label(frame, text="Selected directory: None",
bg="white", wraplength=500, justify="left")
        self.select_dir_label.place(x=122, y=0)



        self.scan_button = tk.Button(frame, text="Scan",
command=self.scan_directory)
        self.scan_button.place(x=5, y=50)
        self.scan_button.config(height=2, width=15)

        self.result_label = tk.Label(frame, text="", bg="white",
wraplength=800, justify="left")
        self.result_label.place(x=122, y=50)

        self.delete_button = tk.Button(frame, text="Delete Ransomware",
command=self.delete_ransomware, state="disabled")
        self.delete_button.place(x=5, y=100)
        self.delete_button.config(height=2, width=15)
```

```
        self.quarantine_button = tk.Button(frame, text="Quarantine",
command=self.quarantine_ransomware, state="disabled")
        self.quarantine_button.place(x=5, y=150)
        self.quarantine_button.config(height=2, width=15)

        # Prevent the master window from resizing based on the size of its
contents
        master.grid_columnconfigure(0, weight=1)
        master.grid_rowconfigure(1, weight=1)

    def select_directory(self):
        self.selected_dir = filedialog.askdirectory()
        self.select_dir_label.config(text="Selected directory:
{}".format(self.selected_dir))

    def scan_directory(self):
        # Check if a directory has been selected
        if self.selected_dir is None:
            messagebox.showerror("Error", "Please select a directory to scan")
            return
```

```
        self.ransomware_found = False


        # Traverse the selected directory and its subdirectories and check
each file for ransomware signatures
        for root, dirs, files in os.walk(self.selected_dir):
            for file in files:
                file = os.path.join(root, file)
                with open(file, 'rb') as f:
                    contents = f.read()


                    for signature ,ransomware_name in
RANSOMWARE_SIGNATURES.items():
                        if signature in contents:
                            self.ransomware_found = True
                            self.result_label.config(text="Found ransomware at:
{}\nRansomware: {}".format(file, ransomware_name), font=("Helvica", 10), fg
= "red")
                            self.delete_button.config(state="normal")
                            self.quarantine_button.config(state="normal")
```

```
                return


            if not self.ransomware_found:
                self.result_label.config(text="Ransomware not found",
font=("Helvica", 10), fg = "blue")
                self.delete_button.config(state="disabled")
                self.quarantine_button.config(state="disabled")
                #self.delete_button.config(state="disabled")



    def delete_ransomware(self):
        if not self.ransomware_found:
            messagebox.showerror("Error", "No ransomware found, cannot
delete")
            return


        # Get the file path that was identified as containing ransomware
        ransomware_file = self.result_label.cget("text").split("\n")[0].split(": ")[1


        # Delete the ransomware file
```

```
        try:
            os.remove(ransomware_file)
            self.result_label.config(text="Ransomware file was deleted")
            self.delete_button.config(state="disabled")
            return
        except PermissionError:
            self.result_label.config(text="Access denied, cannot delete
ransomware file")
        except FileNotFoundError:
            self.result_label.config(text="Ransomware file not found")
            self.delete_button.config(state="disabled")


    def quarantine_ransomware(self):
        if self.ransomware_found:
            for root, dirs, files in os.walk(self.selected_dir):
                for file in files:
                    file_path = os.path.join(root, file)
                    with open(file_path, 'rb') as f:
                        contents = f.read()
```

```
                for signature in RANSOMWARE_SIGNATURES:
                    if signature in contents:
                        dst_dir = r"D:\ext\QuarantineFolder"
                        os.makedirs(dst_dir, exist_ok=True)
                        dst_file_path = os.path.join(dst_dir, file)
                        try:
                            shutil.move(file_path, dst_file_path)
                            self.result_label.config(text="Ransomware file in
Quarantine")
                        except PermissionError:
                            self.result_label.config(text="Access denied, cannot
Quarantine ransomware file")
                            self.delete_button.config(state="disabled")
                            self.quarantine_button.config(state="disabled")
                        return
            self.result_label.config(text="Ransomware file not found")
            self.delete_button.config(state="disabled")
            self.quarantine_button.config(state="disabled")
        else:
```

```
        messagebox.showerror("Error", "No ransomware found, cannot
Quarantine")
        return


root = tk.Tk()
bg_image = tk.PhotoImage(file="banner.png")
bg_image = bg_image.subsample(2, 2)


app = RansomwareDetectorApp(root)
root.mainloop()
```

- **Source Code Quarantine**

```
i mport os
import tkinter as tk
from tkinter import filedialog, messagebox
from PIL import Image


# set the directory path
folder_path = r"D:\ext\QuarantineFolder"
# get a list of all the files in the directory
```

```
files = os.listdir(folder_path)

# loop through each file in the folder

for file in files:

    # print the file name

    print(file)


    # print the file address

    file_path = os.path.join(folder_path, file)

    print(file_path)


class RansomwareDetectorApp:

    def __init__(self, master):

        self.master = master

        # Set the title and size of the window

        self.master.title("Quarantine Folder")

        self.master.geometry("650x550")

        root.configure(bg='#004080')

        # Add a label at the top of the frame
```

```
        #self.header_label = tk.Label(root, text="Files in Quarantine Folder",
font=("Arial", 20))
        #self.header_label.pack(pady=15)
        bg_label = tk.Label(root, image=bg_image)
        bg_label.grid(row=0, column=0, columnspan=2)


        self.file_list = []
        frame = tk.Frame(root, bg="gray", borderwidth=2, relief="groove")
        frame.place(relx=0.5, rely=0.6, relwidth=0.8, relheight=0.45,
anchor='center')
        self.listbox = tk.Listbox(frame, selectmode=tk.MULTIPLE, width=29,
height=12)
        self.listbox.place(x=200, y=12)


        self.select_dir_button = tk.Button(frame, text="Select Directory",
command=self.select_directory, font=("Helvica", 10))
        self.select_dir_button.place(x=10, y=30)
        self.select_dir_button.config(height=2, width=15)
        self.select_dir_label = tk.Label(frame, text="Selected directory: None",
pady=10, font=("Helvica", 10),bg = "grey", wraplength=150, justify="left")
```

```
        self.select_dir_label.place(x=10, y=70)


        self.delete_button = tk.Button(frame, text="Delete ransomware",
command=self.delete_ransomware, state="normal", font=("Helvica", 12),
fg="red")
        self.delete_button.place(x=10, y=160)
        self.delete_button.config(height=2, width=17)


        master.pack_propagate(False)


    def select_directory(self):
    # Open a file dialog to select a directory
        folder_path = filedialog.askdirectory()


        # Check if the selected directory matches the desired name
        if os.path.basename(folder_path) != 'QuarantineFolder':
            messagebox.showerror("Error", "Please select a directory named
'QuarantineFolder'")
            return
        # Update the label with the selected directory
```

```
        self.select_dir_label.config(text="Selected : {}".format(folder_path))


        # Clear the file list
        self.file_list.clear()
        self.listbox.delete(0, tk.END)


        # Get a list of all the files in the directory
        files = os.listdir(folder_path)
        # Add each file to the listbox
        for file in files:
            file_path = os.path.join(folder_path, file)
            self.file_list.append(file_path)
            self.listbox.insert(tk.END, file)
    def update_files_list(self):
        self.listbox.delete(0, tk.END)  # clear the listbox
        self.file_list.clear()  # clear the file list
        self.folder_path = self.select_dir_label.cget("text")[11:]  # get the
folder path from the label
        files = os.listdir(self.folder_path)
```

```
        for file in files:
            file_path = os.path.join(self.folder_path, file)
            self.file_list.append(file_path)
            self.listbox.insert(tk.END, file)
        self.delete_button.config(state="normal")


    def delete_ransomware(self):
        selected_indices = self.listbox.curselection()
        if len(selected_indices) == 0:
            messagebox.showerror("Error", "No files selected, cannot delete")
            return
        for index in selected_indices:
            file_path = self.file_list[index]
            try:
                os.remove(file_path)
            except Exception as e:
                messagebox.showerror("Error", str(e))
        # Refresh the file list
        self.update_files_list()
```

```
        messagebox.showinfo("Success", "Ransomware deleted successfully")
        return
root = tk.Tk()
bg_image = tk.PhotoImage(file="QRTbanner.png")
bg_image = bg_image.subsample(2, 4)
app = RansomwareDetectorApp(root)
root.mainloop()
```

ภาคผนวก ง

ประวัติผู้จัดทำ

ประวัติผู้จัดทำโครงงานวิจัย

ชื่อ-นามสกุล :	นางสาวปณิธาน วสุวัต
รหัสนักศึกษา :	116210906008-4
สาขาวิชา/ภาควิชา :	สาขาวิชาเทคโนโลยีสารสนเทศ
วัน/เดือน/ปีเกิด :	18 กรกฎาคม 2542
ประวัติการศึกษา :	มัธยมศึกษาตอนต้น (ม.3)
	โรงเรียนสาธิต “พิบูลบำเพ็ญ” มหาวิทยาลัยบูรพา
	ปีที่สำเร็จการศึกษา พ.ศ.2558
	ประกาศนียบัตรวิชาชีพ(ปวช.)
	วิทยาลัยอาชีวศึกษาชลบุรี
	ปีที่สำเร็จการศึกษา พ.ศ.2562
ที่อยู่ :	บ้านเลขที่ 55/25 หมู่บ้านชลญาวิลล์ หมู่6 ถนนมิตรสัมพันธ์
	ตำบลบ้านปึก อำเภอเมือง จังหวัดชลบุรี 20130
อีเมล์ :	Teamahah@gmail.com

ประวัติผู้จัดทำโครงงานวิจัย

ชื่อ-นามสกุล :	นางสาวบุญฑริกกา นิซัน
รหัสนักศึกษา :	116210906015-9
สาขาวิชา/ภาควิชา :	สาขาวิชาเทคโนโลยีสารสนเทศ
วัน/เดือน/ปีเกิด :	24 กุมภาพันธ์ 2544
ประวัติการศึกษา :	มัธยมศึกษาตอนต้น (ม.3)
	โรงเรียนบ้านสวนอุดมวิทยา
	ปีที่สำเร็จการศึกษา พ.ศ.2559
	ประกาศนียบัตรวิชาชีพ(ปวช.)
	วิทยาลัยอาชีวศึกษาชลบุรี
	ปีที่สำเร็จการศึกษา พ.ศ.2562
ที่อยู่ :	บ้านเลขที่ 37/3 หมู่1 ตำบลประจันตคาม
	อำเภอประจันตคาม จังหวัดปราจีนบุรี 25130
อีเมล์ :	Freshbtrk@gmail.com