Virus Stealer

สาขาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์
มหาวิทยาลัยขอนแก่น

หลักการและเหตุผล

ปัจจุบันผู้คนส่วนใหญ่ชอบความสะดวกสบาย ไม่ว่าจะเป็นการใช้ชีวิต การใช้สื่อ Social ซึ่งความสะดวกสบายเหล่านี้ทำให้เราเคยชินและมองข้าม ความอันตรายของการใช้คอมพิวเตอร์ จึงมักละเลยในการใช้ Anti-Virus เนื่องจากต้องมีการซื้อผลิตภัณฑ์ของแท้และค่าใช้จ่ายที่สูง จึงมีน้อยคนที่จะตัดสินใจซื้อผลิตภัณฑ์ของแท้เพื่อที่จะป้องกันข้อมูลส่วนตัวภายในคอมพิวเตอร์ จึงทำให้มีช่องโหว่ในการโจรกรรมข้อมูลจากคอมพิวเตอร์ได้ ในช่องทางต่างๆ เพื่อจะชี้ให้เห็นถึงช่องโหว่ดังกล่าว พวกเราจึงต้องการศึกษาและสร้าง Virus Stealer เพื่อสาธิตหนึ่งในวิธีการโจรกรรมข้อมูล โดยที่ผู้คนเหล่านั้นไม่รู้ตัวเลยด้วยซ้ำ

วัตถุประสงค์

1. เพื่อศึกษาหลักการทำงานของ Virus
2. เพื่อศึกษาวิธีการโจรกรรมข้อมูล
3. เพื่อศึกษาโปรแกรมเพิ่มเติมที่สามารถประยุกต์ใช้ในการโจรกรรมข้อมูลได้

คณะผู้จัดทำ GROUP 5

นายวิชยุตม์ ศรีละ	603021056-2
นายธนพนธ์ แสนขวา	603020348-4
นายสืบสกุล เทียมรินทร์	603020371-9
นายดลธรรม ไกรอนุพงษา	603020343-4
นายไชยพศ อเสกจันทร์สกุล	603020339-5
นายชนาธิป เกิดเกรียงไกร	603021042-3

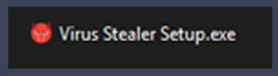
อาจารย์ที่ปรึกษา

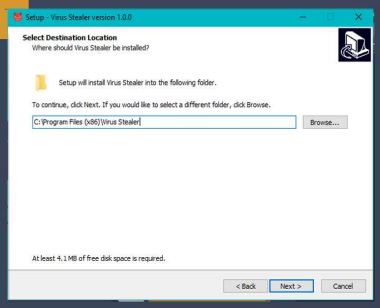
อ. ดร.จักรชัย โสอินทร์

342376
INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

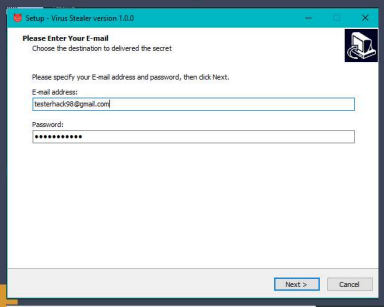
หลักการทำงาน

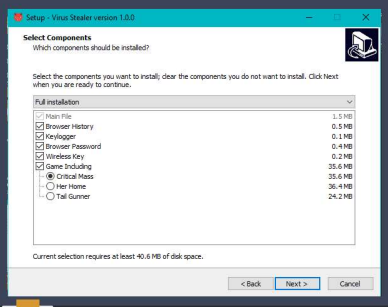
- โปรแกรมจะมีตัว Setup เพื่อตั้งค่าต่างๆ ตามที่ผู้ใช้ต้องการ



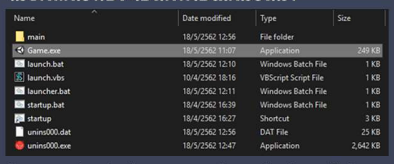


- ในการ Setup จะให้ผู้ใช้หรอกที่อยู่อีเมลล์และรหัสผ่านที่ผู้ใช้ต้องการให้ส่งข้อมูลของเหยื่อไป รวมทั้งมี function ให้ผู้ใช้เลือกได้ตามต้องการ



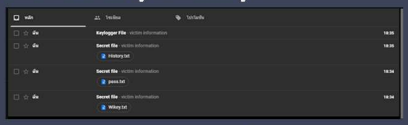


- เมื่อทำการ Setup เสร็จสิ้น โปรแกรมจะมีหน้าตาเป็นไอคอนเข้าเกม เมื่อคลิกเข้าไปจะเป็นการเปิดเกมขึ้นมา



Name	Date modified	Type	Size
main	18/5/2562 12:56	File folder	
Game.exe	18/5/2562 11:07	Application	249 KB
launch.bat	18/5/2562 12:10	Windows Batch File	1 KB
launch.vbs	10/4/2562 18:16	VBScript Script File	1 KB
launcher.bat	18/5/2562 12:11	Windows Batch File	1 KB
startup.bat	18/4/2562 16:39	Windows Batch File	1 KB
startup	18/4/2562 16:27	Shortcut	3 KB
unins000.dat	18/5/2562 12:56	DAT File	25 KB
unins000.exe	18/5/2562 12:47	Application	2,642 KB

- ในขณะเดียวกันโปรแกรมจะทำการฝังตัวลงไปใน Path %AppData% ของเหยื่อ จากนั้นโปรแกรมจะทำการขโมยข้อมูลและส่งข้อมูลที่ได้ไปที่ e-mail ของผู้โจรกรรมข้อมูล



- โปรแกรมจะทำการส่งข้อมูลทุกครั้งที่เหยื่อเปิดเครื่องขึ้นหรือคลิกเข้าเล่นเกม หน้าตาของไฟล์ที่ถูกส่งไปจะอยู่ในรูปแบบไฟล์ .txt และ .log

สรุปผลการดำเนินงาน

โปรแกรมนี้สามารถทำงานได้ตามวัตถุประสงค์และขอบเขตที่ตั้งไว้และสามารถนำไปพัฒนาต่อยอดเพื่อเพิ่มประสิทธิภาพและการทำงานที่มากกว่านี้ได้ ทั้งนี้โปรแกรมยังมีข้อจำกัดในการทำงานอยู่คือไม่สามารถหลีกเลี่ยงการตรวจจับจากโปรแกรม Anti-Virus ได้ ทางคณะผู้จัดทำหวังเป็นอย่างยิ่งว่าข้อจำกัดนี้จะหมดไปและสามารถทำงานได้อย่างเต็มประสิทธิภาพในอนาคต

ซอฟต์แวร์ที่ใช้พัฒนา

PowerShell
vbscript
NirSoft Tools and Utilities
innoSETUP

Reference
https://www.nirsoft.net
https://github.com/MinhasKamal/StupidKeylogger
https://vm360degree.com/tag/powershell
https://mindphp.com
https://www.aripfan.com/file-bat/
http://www.jrsoftware.org