Apr 1st 2020 – Status Report

Group #1 - Alistair Godwin, Francesco Losi, Michael Sciortino

Program Short Desc:

Free Root Beer App (Malicious SignUp).

Program exploits user wanting a free root beer and asks them to willingly signup with an email + personal information.

Good: Uses automated web-scraping to legitimately sign the users up for coupons – because everybody deserves savings.

Evil: Will unwillingly steal data as a keylogger in background that is sent back to daemon. Try to steal information like: email, password, firstname, lastname, postalcode, domain (pull from email), IP, location (interpret via IP if possible) using regex. Format this into CSV files that can be sold for stacks of cash. *<insert evil laughter >*

Progress Made:

- M1 Submitted on time. Github was setup and tasks assigned for sprint #1 due Apr 4th 2020
- Tasks have been split up as noted below with progress made on all 3.
- Daemon Mechanize library switched with BeautifulSoup4 -> Successfully requested and grabbed the coupon site using beautiful soup and requests
- CSV work on daemon started
- Client prompts for data and stores it for later work

Also found an email validation exploit on A&W's website - can print unlimited coupons without valid emails. lol

Work Underway:

As defined by tasks on next page. Each member has been assigned tasks on Github with progress meeting this Saturday.

Work Next Week:

- Link task components into 2 working files for daemon and client.
- Client must complete double forking
- Test and debug components.
- Test cross-computer connections.
- Potentially determine solution for anti-bot CSRF tokens
- Assign follow-up tasks as determined from Saturday's meeting.

Collaboration:

Github(Branches setup for each member) / **Discord**(Next Meeting Saturday) and **WhatsApp**(informal)

---PROJECT TASK List FOR SPRINT #1 + #2---

---*DAEMON*--- Francesco

- 1A) Make Current Daemon a double forked daemon
- 1B) Make a handle function that accepts data from our clients
- 2A) Function can receive some commands like: "Send"(the stolen data)
- 2B) Send will receive Comma seperated data(not all data may come, expect nulls):
- email,firstname, lastname, postalcode, domain(pull from email),
- IP, location(call an api lookup if possible on the IP and/or postalcode)
- 3A) Store all this data into an array and then store in a named csv file
- 3B) Call SignUp() with the array of data
- 4)(Potentially if time available) allow for on-demand requests to be sent to client like force-send and take-screenshot.

---*DAEMON MECHANIZE/BS4*--- Alistair

- Create a SignUp() function – use BS4 instead of Mechanize library
- 1B) Parse the array data and validate it
- ~~2A) Potentially use os.fork() here to avoid blocking~~
- 2B) Use Beautiful soup and requests to check website existance
- 3A) This function will use the ~~mechanize API~~ BS4 to fill in forms on the A&W Website and submit
- 3C) Fill in form and submit
- 3B) Find and capture CSRF token and session ID
- 4) POST request with form and csrf data as JSON object

---*CLIENT*--- Michael

- Make the host politely ask the user if they want to signup for free root beer + coupons. At minimum we need their email.
- 1A) We also want to prompt for: FirstName, LastName, PostalCode(for local offers). Store this data in an array
- 1C) Ask the user if they want to signup more people - loop back to 1A
- 2A) Make the host os.fork()
- 2B) Have host contact daemon and send back that array, then close connection()
    - 2C) SFTP may be required here
- 3)The fork should quietly double fork and detach from the terminal - like how the daemon does it.
- 3B)This fork will first determine the user's IP address and then starts keylistening.
- 4)The key listener will listen for all strokes and try to regex for things like emails and postalcodes which it will store in an array.
- 5) (If we have time and its possible, see if you can take and send back screenshots of active window too)Contact the daemon and send back that data every randInt() hours + randomMinutes()