Questions, Issues,

Concerns, Suggestions

Welcome at any time

Even Now

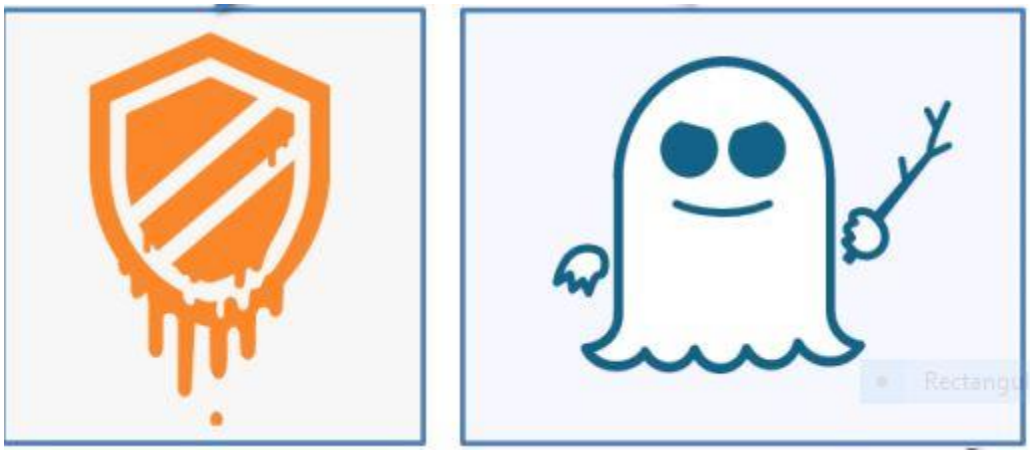
Sun City Computer Club

Windows SIG

January 23, 2018

Vocabulary

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless



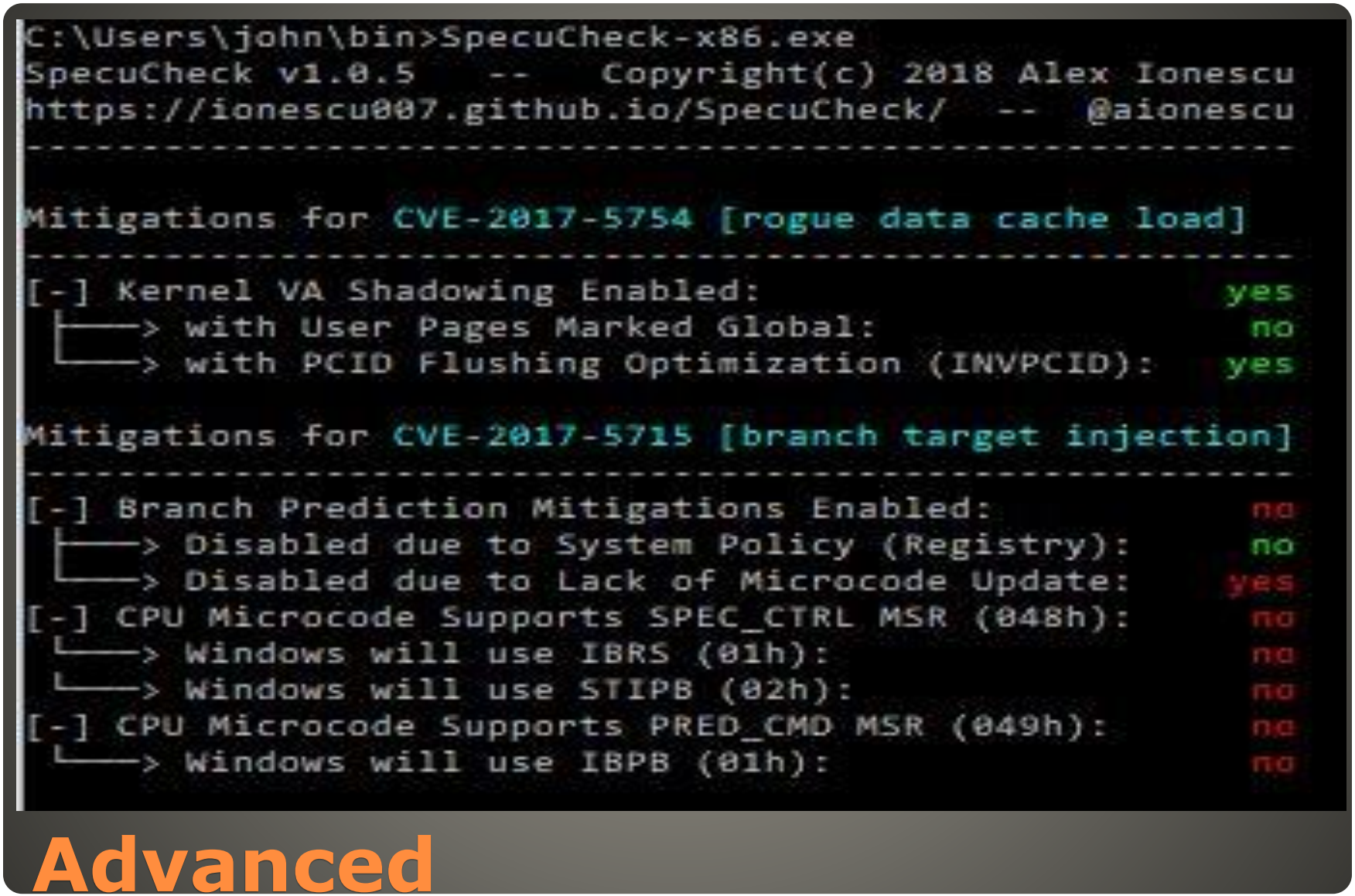
Current Topics

- Spectre and Meltdown
- speculative execution, branch prediction
- IoT
- Any/everything
- Kernel level code impacts
- Conspiracy??

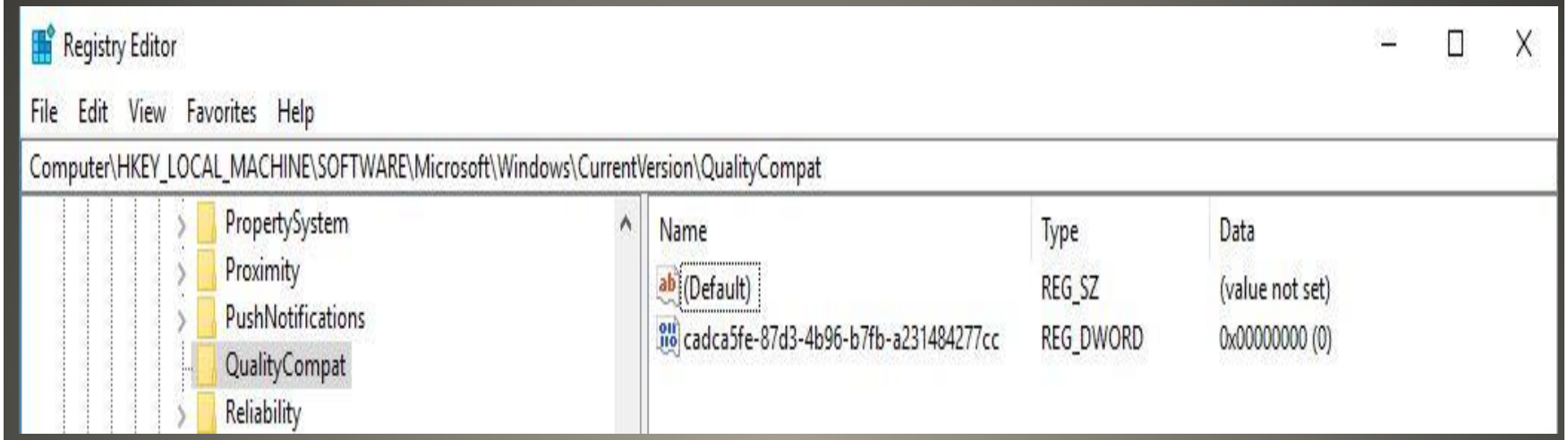

nsa
inside

Meltdown and Spectre

- ALL (USA?) CPUs for last decade
- BIOS, Firmware, microcode
- Work on remediation ongoing for months
- Linux kernel
- Speculative execution pipelining
- Cache lines filled at exception
- Code on your system
- “Gathered” memory may be of value
- Remediation may affect performance
- Internet of Things Thing Things
- WEB and Virtual machines
- Games


C:\Users\john\bin>SpecuCheck-x86.exe
SpecuCheck v1.0.5 -- Copyright(c) 2018 Alex Ionescu
https://ionescu007.github.io/SpecuCheck/ -- @aionescu
Mitigations for CVE-2017-5754 [rogue data cache load]
[-] Kernel VA Shadowing Enabled: yes
> with User Pages Marked Global: no
> with PCID Flushing Optimization (INVPCID): yes
Mitigations for CVE-2017-5715 [branch target injection]
[-] Branch Prediction Mitigations Enabled: no
> Disabled due to System Policy (Registry): no
> Disabled due to Lack of Microcode Update: yes
[-] CPU Microcode Supports SPEC_CTRL MSR (048h): no
> Windows will use IBRS (01h): no
> Windows will use STIPB (02h): no
[-] CPU Microcode Supports PRED_CMD MSR (049h): no
> Windows will use IBPB (01h): no

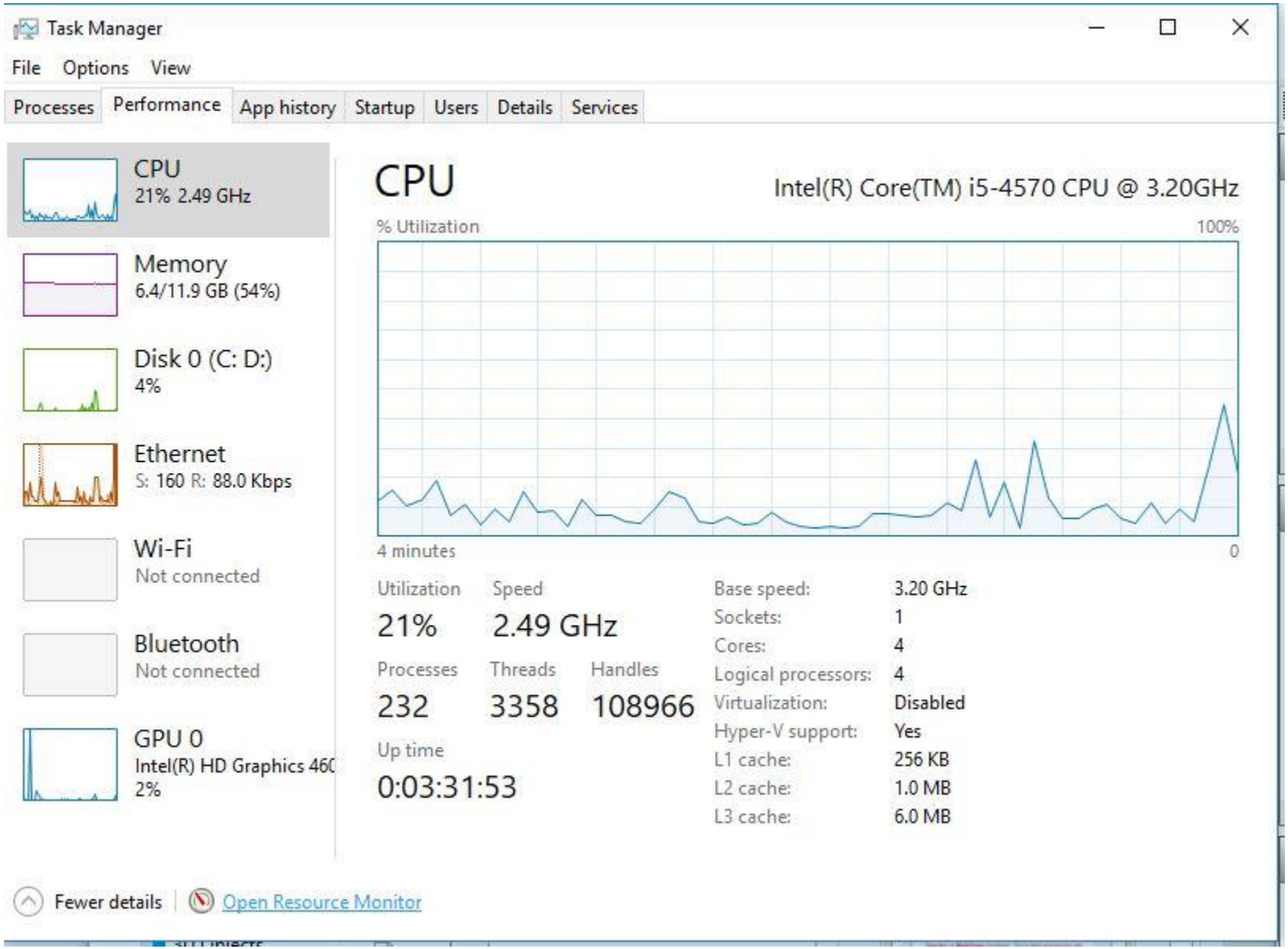
Advanced


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat
PropertySystem
Proximity
PushNotifications
QualityCompat
Reliability
Name
Type
Data
(Default)
REG_SZ
(value not set)
cadca5fe-87d3-4b96-b7fb-a231484277cc
REG_DWORD
0x00000000 (0)

Advanced


InSpectre: Check Spectre and Meltdown Prevention
InSpectre
Release #1
Check Windows operating system
and processor hardware safety.
Freeware by Steve Gibson / @Sggrc
Spectre & Meltdown Vulnerability
and Performance Status
Vulnerable to Meltdown: YES!
Vulnerable to Spectre: YES!
Performance: GOOD
(full details below)
See GRC's InSpectre webpage at: https://grc.com/inspectre.htm
for a full explanation of the use and operation of this freeware utility.
Enable Meltdown Protection
Enable Spectre Protection
Exit


InSpectre: Check Spectre and Meltdown Prevention
InSpectre
Release #1
Check Windows operating system
and processor hardware safety.
Freeware by Steve Gibson / @Sggrc
update the system's hardware and software for maximum security and performance.
This system's present situation:
This 64-bit version of Windows is not aware of either the Spectre or Meltdown problems. Since Intel processors are vulnerable to both of these attacks, this system will be vulnerable to these attacks until its operating system has been updated to handle and prevent these attacks.
See GRC's InSpectre webpage at: https://grc.com/inspectre.htm
for a full explanation of the use and operation of this freeware utility.
Enable Meltdown Protection
Enable Spectre Protection
Exit


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
21% 2.49 GHz
Memory
6.4/11.9 GB (54%)
Disk 0 (C: D:)
4%
Ethernet
S: 160 R: 88.0 Kbps
Wi-Fi
Not connected
Bluetooth
Not connected
GPU 0
Intel(R) HD Graphics 460
2%
CPU
Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz
% Utilization
100%
4 minutes
0
Utilization
21%
Speed
2.49 GHz
Processes
232
Threads
3358
Handles
108966
Up time
0:03:31:53
Base speed: 3.20 GHz
Sockets: 1
Cores: 4
Logical processors: 4
Virtualization: Disabled
Hyper-V support: Yes
L1 cache: 256 KB
L2 cache: 1.0 MB
L3 cache: 6.0 MB
Fewer details
Open Resource Monitor

Current Topics

- Microsoft patch office docs ALL versions
- Office macros
- AOL and Verizon emails from Gmail domain
- Facebook Help “Foreign interference”


Find Friends
93
Back
foreign interference
What is our action plan against foreign interference?
We've taken down fake accounts and Pages created by foreign actors attempting to interfere in the 2016 US Elections. Check to see if you liked or followed a Facebook Page or Instagram account created by the Internet Research Agency - the organization associated with these accounts and Pages.

Suggestions

- Patch Windows
  - backup, MCT, restore point
  - Check the patches
- Patch any/everything
  - backup, save settings & configurations
- Monitor news, accounts, environment
- Use multiple browser instances
- For sensitive sites
  - Use more secure browser
  - Use browser add-ons & extensions
  - Check those browser settings, add-ons, etc.

Suggestions

- BEFORE EACH sensitive session
  - Check add-ons and extensions for updates
  - Check browser for updates
  - Open ONE tab only
  - Use multi-factor authentication
  - Enable minimal settings
  - Check for online alerts
  - Monitor accounts
  - Close & exit browser

  Client side ONLY

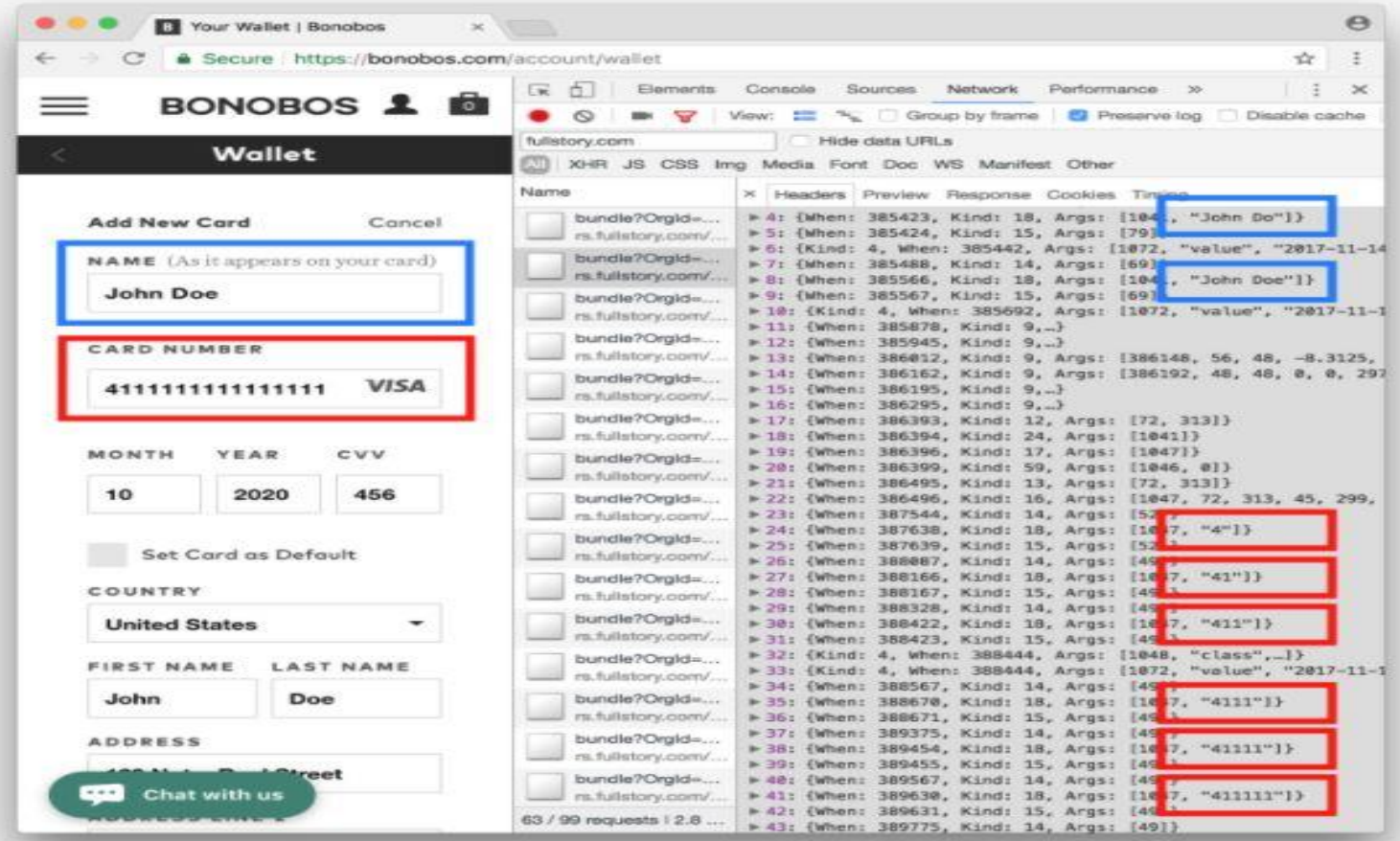
Suggestions

- Use Linux VM requires some effort
- Chromebook not to my liking
- Quad 9 DNS settings on devices
- Internet of Things
- Home infrastructure
- Use for old smart devices

The Adthink script contains very detailed categories for personal, financial, physical traits, as well as intents, interests and demographics. It is hard to comment on the exact use of these categories but it gives a glimpse of what our online profiles are made up of:

birth date, age, gender, nationality, height, weight, BMI (body mass index), hair_color (black, brown, blond, auburn, chestnut, red, gray, white), eye_color (amber, blue, brown, grey, green), education, occupation, net_income, raw_income, relationship states, seek_for_gender (m, f, transman, transwoman, couple), pets, location (postcode, town, state, country), loan (type, amount, duration, overindebted), insurance (car, motorbike, home, pet, health, life), card_risk (chargeback, fraud_attempt), has_car(make, model, type, registration, model year, fuel type), tobacco, alcohol, travel (from, to, departure, return), car_hire_driver_age, hotel_stars

Audienceinsights.net



Web Session Replay

- Questions, suggestions, comments?
  - Chicken Little
  - Tortoise and hare
  - Each of us safer, all of us safer