

Carbon Black.

Women in Tech @ Tufts Conference 2019

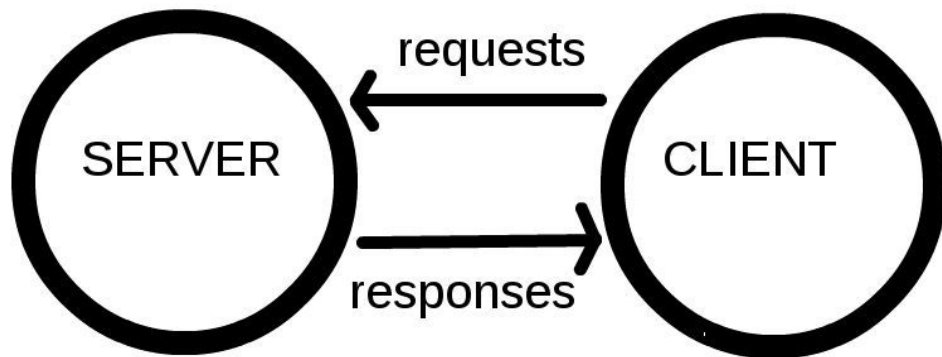


- What is Carbon Black?
- What are we building?
- What is a web server?
- What is Flask?
- Let's Code!
- Next Steps

Carbon Black.

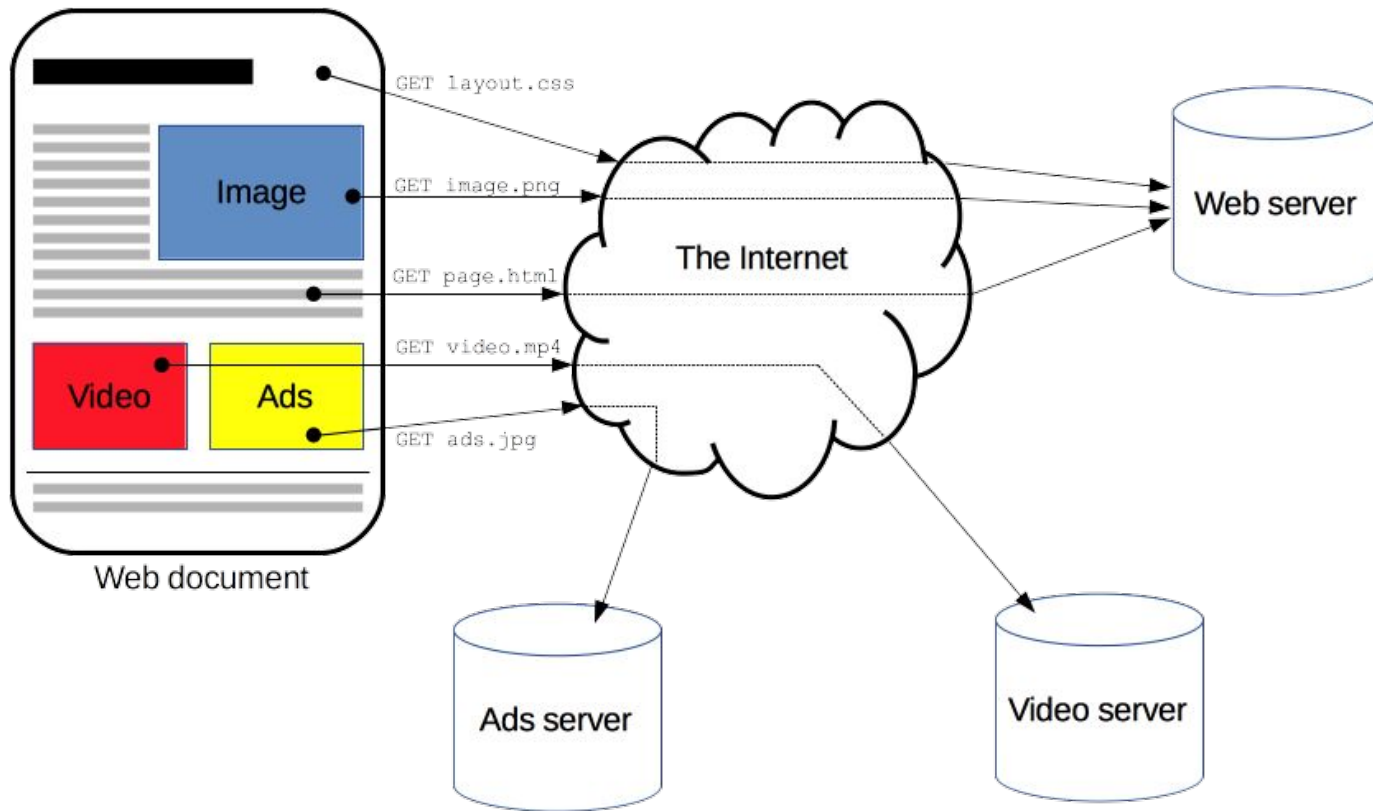


What is a web server?



- Static web server
 - Serves content “as is”
- dynamic web server
 - Static web server + additional software

HTTP/HTTPS



What is Flask?



- Micro web framework written in Python
- Minimalistic - easy to get started, flexible, powerful
- Documentation: <https://flask.palletsprojects.com/en/1.1.x/>

What can you do with Flask?

- Used by many technology companies as a key component of their product
 - Pinterest, Uber, Reddit
- Part of testing framework at Carbon Black


What is Virustotal?

- <https://www.virustotal.com>
- Engine that combines many antivirus products and online scan engines to check for reputation of files, URLs, domains, IP addresses and hashes
- CB SOC team uses to check for reputation of possibly malicious files and websites



Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community

FILE URL SEARCH



0A9F10925AF42DF94925D07112F303D57392C908

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more.](#)



88c90c2b123a357423ab3241624cba49d57122ee3b8ff4130504090c174bb09d



51 engines detected this file



88c90c2b123a357423ab3241624cba49d57122ee3b8ff4130504090c174bb09d

BPA.Transport.dll

64bits

assembly

pedll

238 KB

Size

2019-05-31 20:52:38 UTC

2 months ago



DETECTION

DETAILS

RELATIONS

COMMUNITY 1

Ad-Aware

Trojan.GenericKD.41174900

AhnLab-V3

Trojan/Win32.Agent.C2985661

Alibaba

Trojan.Win32/Turla.94aab752

ALYac

Backdoor.Turla.A

Antiy-AVL

Trojan/Win32.LightNeuron

Arcabit

Trojan.Generic.D2744774

Avast

Win32:Turla-AR [Trj]

AVG

Win32:Turla-AR [Trj]

Avira (no cloud)

TR/RedCap.igtrt

BitDefender

Trojan.GenericKD.41174900

CAT-QuickHeal

Trojan.Lightneuron

Comodo

Malware@#626z1jidism

CrowdStrike Falcon

Win/malicious_confidence_100% (W)

Cylance

Unsafe

Cyren

W64/Trojan.RSGX-2906

DrWeb

Trojan.Neuron.2

Emsisoft

Trojan.GenericKD.41174900 (B)

eScan

Trojan.GenericKD.41174900

Let's Code!

Where can you take this project next?

Extending the Dashboard:

- Integrate additional APIs
- Add a database
- Add graphs to visualize data

Other Flask App Uses:

- Create a personal website
- Create any kind of website!

Tutorial Source Code (On Github):

<https://github.com/deannabaris/wit-security-app-tutorial>



Carbon Black.

Questions?

