Malware Analysis Gateway Development

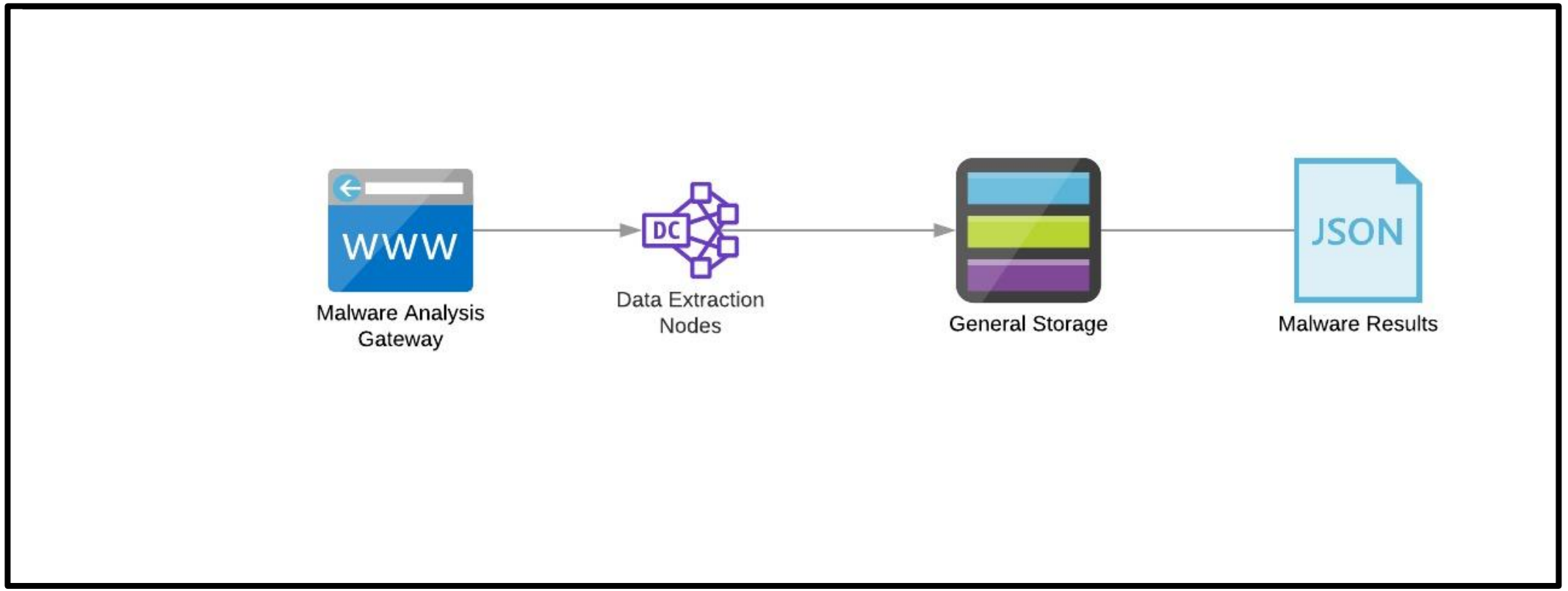
BY: PHOTO BOMBERS

SHANIQWA BARBER, TOREY BELL, KELLY CONLON, LA'ANDREA GATES, KYANIE WATERS

MENTOR:

CHRISTOPHER LANCLOS

We developed a malware analysis gateway that provides extracted data from submitted executable samples.


WWW
Malware Analysis Gateway
DC
Data Extraction Nodes
General Storage
JSON
Malware Results

Cloudy Clustering

*Access to web platforms

*Shared file system

*Group Sharing


Desktop
kellyconlon — photobo...
Safari
kellyconlon — photobo...
kellyconlon — kac5224@login4.stampede2:~ — -bash — 80×24
| Name Avail SUs Expires | Name Avail SUs Expires |
| Venmo-Project 2090 2020-09-30 | A-ccvis 15342 2019-12-31 |
Disk quotas for user kac5224
| Disk Usage (GB) Limit %Used File Usage Limit %Used |
| /home1 1.7 10.0 16.91 13685 200000 6.84 |
| /work 0.0 1024.0 0.00 11 3000000 0.00 |
| /scratch 0.0 0.0 0.00 8 0 0.00 |
Tip 30 (See "module help tacc_tips" for features or how to disable)
If you want to see all the currently loadable modules that contain the string "abc" execute:
$ module avail abc
This works for spider and list as well.
login4(1000)$ packet_write_wait: Connection to 129.114.63.44 port 22: Broken pipe
Kellys-MacBook-Pro:~ kellyconlon$
[Restored Nov 20, 2019 at 10:41:33 AM]
Last login: Wed Nov 20 09:41:23 on console
Kellys-MacBook-Pro:~ kellyconlon$
Terminal
SOLIDS
Lecture 19 notes
Lecture 20 video
Read 5.5, 5.8, 5.10, 5.11
HW:
5.8-6,10,11,12,14, 5.10-1,8
5.10- 10,12, 5.11-2
Stickies

Photo Bombers' Git Hub

https://github.com/laandreagates/Photobomb-Malware-Analysis-Gateway-

Photo Bombers

Shaniqwa Barber
Shaniqwa.Barber@mvsu.edu

Kelly Conlon
kconlon@utexas.edu

Torey Bell
Torey.Bell@mvsu.edu

Kyanie Waters
Kyanie.Waters@mvsu.edu

La'Andrea Gates
LaAndrea.Gates@mvsu.edu

THANK YOU!


SGCI
Science Gateways
Community Institute


Cloudy
Cluster
by Omnibond™


powered
by
aws


Google Cloud