

THM_S3BOTS2 [300 series questions]

Question 1

Mallory's critical PowerPoint presentation on her MacBook gets encrypted by ransomware on August 18. What is the name of this file after it was encrypted?

Frothly_marketing_campaign_Q317.pptx.crypt

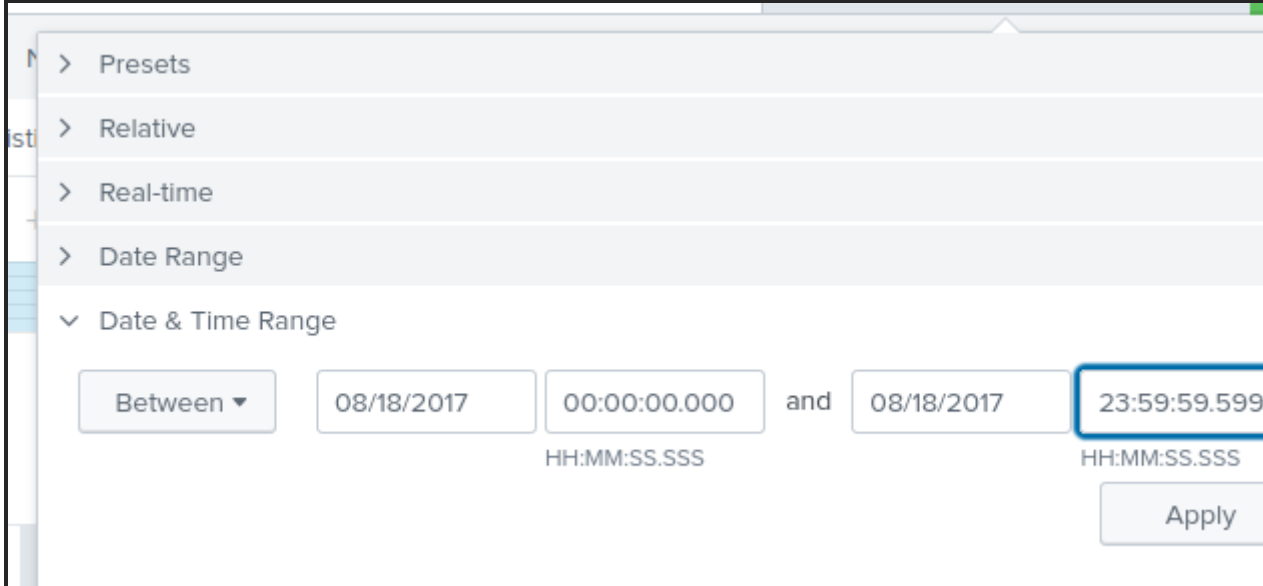
clues: Mallory | PowerPoint | MacBook | August 18

index="botstv2" ".ppt"
results: 4 events; two on Aug 29 and two on Aug 24; what gives?

Let's start over

index="botstv2" Mallory
Account_Name: mallory.krausen
Account_Domain: FROTHLY
ComputerName: venus.frothly.local; mercury.frothly.local
Host: MACLORY-AIR13--a MacBook Air 13?

index="botstv2" MACLORY-AIR13
Looks like I can narrow this to Aug 18, 2017



Complete 1,412,821 events (8/18/17 12:00:00.000 AM to 8/18/17 11:59:59.599 PM)
What!? She uses her computer too much! Maybe getting it locked up will do her some good!!!!

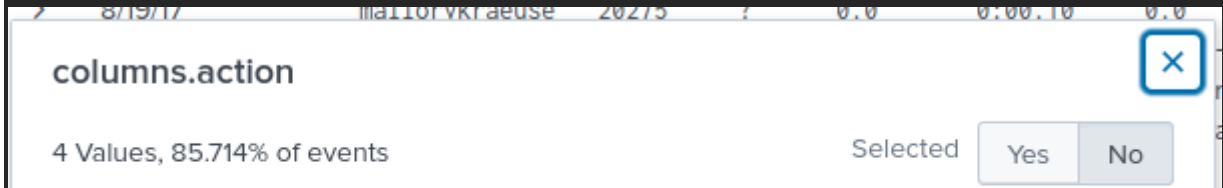
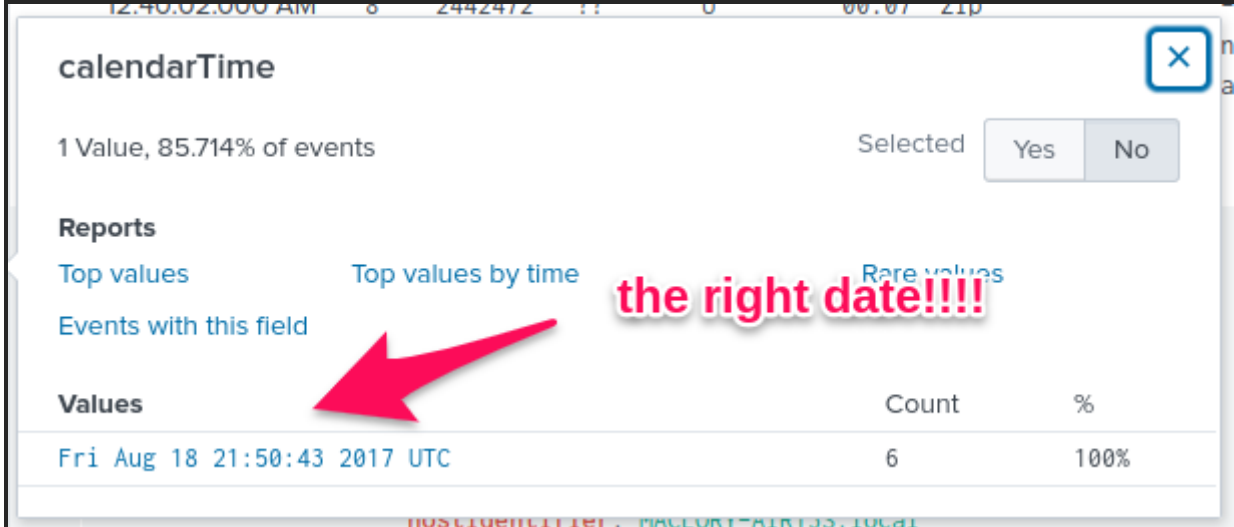
index="botstv2" MACLORY-AIR13 PowerPoint
Results: 0
No Good

FROM THE GUIDE

index="botstv2" host="MACLORY-AIR13" (*.ppt OR *.pptx)

Maybe my time is should be "all time" since she didnt make the presentation on the 18th.

index="botstv2" host="MACLORY-AIR13" (*.ppt OR *.pptx)



Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
ATTRIBUTES_MODIFIED	2	33.333%
DELETED	2	33.333%
CREATED	1	16.667%
MOVED_TO	1	16.667%

could be the encryption?



name

1 Value, 85.714% of events

Selected Yes No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
file_events	6	100%

this caught my eye

But if I had just looked at the main field I would have seen this right in front my face

1 index="botsv2" host="MACLORY-AIR13" (*.ppt OR *.pptx)

All time

7 events (before 2/2/22 10:31:10.000 AM) No Event Sampling

Job

Smart Mode

Events (7)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

1 hour per column

Hide Fields

All Fields

20 Per Page

Time

Event

8/19/17 12:40:02.000 AM

mallorykrause 20275 ? 0.0 0:00:10 0.0 2128 2442472 ?? U 00:07 zip n/Frothly_marketing_campaign_Q317.pptx.crypt_/Volumes//FROTHLY/Home/mallory.krausen/Frothly_marketing_campaign_Q317.pptx host = MACLORY-AIR13 source = ps sourcetype = ps -0_-P_UH9PUnePPK0vYybBKRDmukR_/Volumes//FROTHLY/Home/mallory.krause

Question 2

There is a Games of Thrones movie file that was encrypted as well. What season and episode is it?
Season 07; Episode 02

Let me try this:
index="botsv2" host="MACLORY-AIR13" ("GoT" OR "Game of Thrones")

Question Hint

The season and episode is in the filename.

1 index="botsv2" host="MACLORY-AIR13" ("GoT" OR "Game of Thrones") action=removed

1 event (before 2/2/22 10:44:43.000 AM) No Event Sampling

Events (1)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

20 Per Page

Hide Fields

All Fields

Time

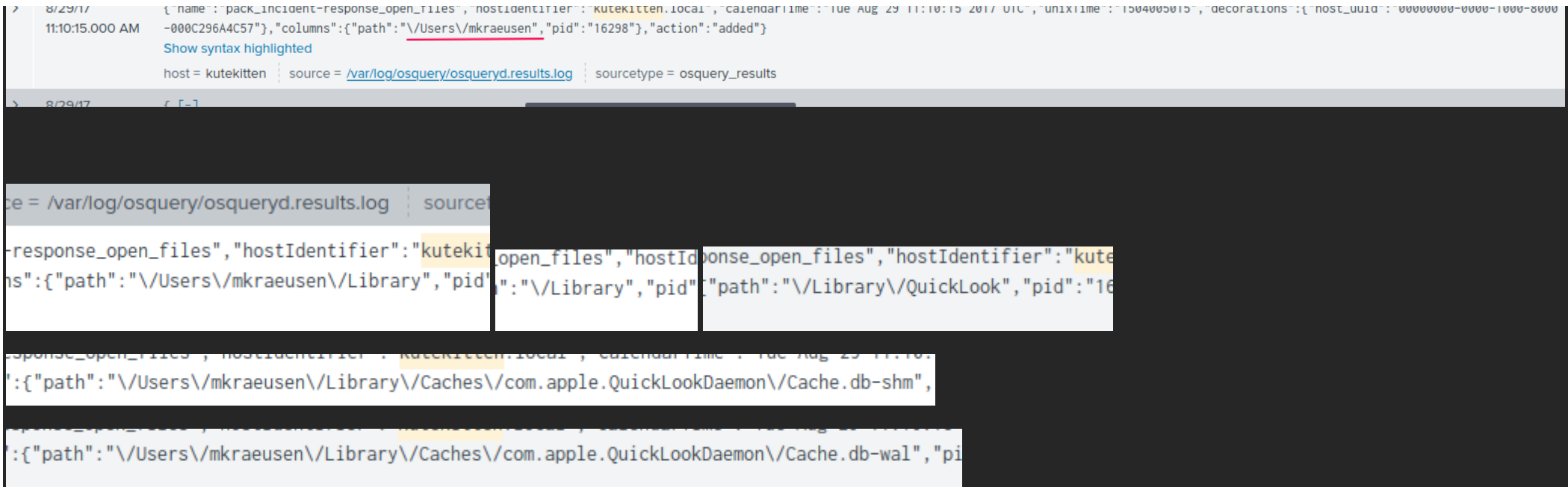
Event

8/18/17 10:53:08.000 PM

{ [-] action: removed

under "actions" I saw a few added and one removed. It's the right answer but I don't see how it is the encrypted one.





Looks like MANUAL ENUMERATION

index="botsv2" "kutekitten" "\\Users"

columns.path

18 Values, 42.69% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
/Users/mkraeusen/Library	36	24.658%
/Users	18	12.329%
/Users/mkraeusen	18	12.329%
/Users/mkraeusen/Library/Caches	18	12.329%
/com.apple.QuickLookDaemon/Cache.db	18	12.329%
/Users/mkraeusen/Library/Caches	18	12.329%
/com.apple.QuickLookDaemon/Cache.db-shm	18	12.329%
/Users/mkraeusen/Library/Caches	18	12.329%
/com.apple.QuickLookDaemon/Cache.db-wal	18	12.329%
/bin/bash	3	2.055%
/Applications/Mail.app/Contents/PlugIns	2	1.37%
/MailCacheDelete.appex/Contents/MacOS	2	1.37%
/MailCacheDelete	2	1.37%
/Applications/Safari.app/Contents/PlugIns	2	1.37%
/CacheDeleteExtension.appex/Contents/MacOS	2	1.37%
/CacheDeleteExtension	2	1.37%
/Applications/iBooks.app/Contents/PlugIns	2	1.37%
/iBooksCacheDelete.appex/Contents/MacOS	2	1.37%
/iBooksCacheDelete	2	1.37%

let's check this out!!!!

looks a-okay to me

After Looking at the guide to point me to downloads (don't know how they figured that out) ; I jumped to action, created

1 index=botsv2 host="kutekitten" "\\Users\\mkraeusen\\Downloads" "columns.action"=CREATED

1 event (before 2/2/22 11:31:43.000 AM) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 20 Per Page

Time	Event
8/3/17 6:19:07.000 PM	{ [-] action: added calendarTime: Thu Aug 03 18:19:07 2017 UTC }

SELECTED FIELDS host 1


```
z source 1
z sourcetype 1

INTERESTING FIELDS
z action 1
z calendarTime 1
z columns.action 1
# columns.ctime 1
z columns.category 1
# columns.ctime 1
# columns.gid 1
# columns.hash 1
# columns.inode 1
z columns.md5 1
# columns.mode 1
# columns.mtime 1
z columns.sha1 1
z columns.sha256 1
# columns.size 1
```

```
columns: { [-]
  action: CREATED
  atime: 1501784329
  category: Downloads
  ctime: 1501784329
  gid: 20
  hashed: 1
  inode: 1214407
  md5: 72d4d364ed91dd9418d144a2db837a6d
  mode: 0777
  mtime: 1501221650
  sha1: 794bcba867307b5f947f6c939eb4df1d2c9b8
  sha256: befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271
  size: 13494
  target_path: /Users/mkraeusen/Downloads/Important_HR_INFO_for_mkraeusen
  time: 1501784335
  transaction_id: 60632
  uid: 502
```

Post | Feed | Li... Spotify – Even...

AttackBox IP:10.10.190.195

Firefox

h/search?q=search in ...

erChef GitHub - swisskyrepo/... Reverse Shell Cheat S...

0 Per Page ▾

ent

```
[-]
action: added
calendarTime: Thu Aug 03 18:19:07 2017 UTC
columns: { [-]
  action: CREATED
  atime: 1501784329
  category: Downloads
  ctime: 1501784329
  gid: 20
  hashed: 1
  inode: 1214407
  md5: 72d4d364ed91dd9418d144a2db837a6d
  mode: 0777
  mtime: 1501221650
  sha1: 794bcba867307b5f947f6c939eb4df1d2c9b8
  sha256: befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271
  size: 13494
  target_path: /Users/mkraeusen/Downloads
  important_HR_INFO_for_mkraeusen
  time: 1501784335
  transaction_id: 60632
  uid: 502
}
decorations: { [-]
  host_uuid: 00000000-0000-1000-8000-000C296A4C57
  username: mkraeusen
}
hostIdentifier: kutekitten.local
name: file_events
unixTime: 1501784347

Show as raw text
t = kutekitten | source = /var/log/osquery/osqueryd.results.log
rcetype = osquery_results
```

Terminal

VIRUSTOTAL

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 14

Ad-Aware	Backdoor.Perl.Quimitchin.B
AhnLab-V3	Perl/Agent
ALYac	Backdoor.OSX.Fruitfly
Arcabit	Backdoor.Perl.Quimitchin.B
Avast	BV:FruitFly-A [Trj]
AVG	BV:FruitFly-A [Trj]
Avira (no cloud)	OSX/Fruitfly.EL.1
BitDefender	Backdoor.Perl.Quimitchin.B
ClamAV	Osx.Trojan.Fruitfly-6210055-0
Comodo	Malware@#3a7bizoalhe2m
Cynet	Malicious (score: 99)
DrWeb	Mac.BackDoor.Rifer.10
Emsisoft	Backdoor.Perl.Quimitchin.B (B)
eScan	Backdoor.Perl.Quimitchin.B
ESET-NOD32	OSX/FruitFly.F
F-Secure	Malware.OSX/Fruitfly.EL.1
Fortinet	OSX/Quimitchin.Altr.bdr
GData	Backdoor.Perl.Quimitchin.B
Ikarus	Trojan.OSX.Fruitfly
Kaspersky	HEUR:Backdoor.Perl.Agent.ao
Lionic	Trojan.Perl.Agent.mlc
MAX	Malware (ai Score=100)
McAfee	Perl/Dropper.a
McAfee-GW-Edition	Perl/Dropper.a
Microsoft	Backdoor.Perl/Shellbot.A!MTB
NANO-Antivirus	Trojan.Script.Backdoor.fmqmlr
Sangfor Engine Zero	Malware.Generic-Script.Save.ba130
Sophos	Troj/Bckdr-RUC
Symantec	OSX.Quimitchin
Tencent	Perl.Backdoor.Agent.Aiie
Trellix (FireEye)	Backdoor.Perl.Quimitchin.B
TrendMicro	PERL_QUIMITCHIN.A
TrendMicro-HouseCall	PERL_QUIMITCHIN.A
Antiy-AVL	Undetected
Baidu	Undetected

hmmmm,
ya think?

index=botsv2 host="kutekitten" USB

```
> 8/3/17 6:18:10.000 PM {"name":"pack_hardware-monitoring_usb_devices","hostIdentifier":"kutekitten.local","calendarTime":"Thu Aug 03 18:18:10 2017 UTC","unixTime":"1501784290","decorations":{"host_uuid":"00000000-0000-1000-8000-000C296A4C57","username":"mkraeusen"},"columns":{"model":"Mass Storage","model_id":"6387","removable":"1","serial":"849083BA","usb_address":"1","usb_port":"1","vendor":"Generic","vendor_id":"0583"},"action":"added"}
Show syntax highlighted
host = kutekitten | source = /var/log/osquery/osqueryd.results.log | sourcetype = osquery_results

> 8/3/17 6:18:10.000 PM {"name":"pack_hardware-monitoring_usb_devices","hostIdentifier":"kutekitten.local","calendarTime":"Thu Aug 03 18:18:10 2017 UTC","unixTime":"1501784290","decorations":{"host_uuid":"00000000-0000-1000-8000-000C296A4C57","username":"mkraeusen"},"columns":{"model":"Mass Storage","model_id":"4100","removable":"1","serial":"0701348CAE3C4831","usb_address":"1","usb_port":"1","vendor":"Generic","vendor_id":"13fe"},"action":"removed"}
Show syntax highlighted
```

host = kutekitten | source = /var/log/osquery/osqueryd.results.log | sourcetype = osquery_results

My Question

Why is there two different USB devices at the same time? Both were inserted(?) at the same time, just before the malware was installed? One belongs to Kingston, the other Alcor.

Question 4

What programming language is at least part of the malware from the question above written in?
Perl

index="botsv2" "kutekitten""\\Users\\mkraeusen\\Downloads"
Brings us to:

columns.target_path

1 Value, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
/Users/mkraeusen/Downloads	5	100%
/Important_HR_INFO_for_mkraeusen		

index="botsv2" "kutekitten""\\Users\\mkraeusen\\Downloads"
"columns.target_path"="/Users/mkraeusen/Downloads/Important_HR_INFO_for_mkraeusen"

This brings up 5 entries but all I know is to look at the raw text for something, but I see nothing that points me to the answer.

Ah, it was back on the virustotal entry under details

www.virustotal.com/gui/file/befa9bfe488244c64db096522b4fad73fc0

Sourcing and... Spotify – Even... Spotify – Don't... Python

SUMMARY

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Basic Properties

MD5

72d4d364ed91dd9418d144a2db837a6d

SHA-1

794bcba867307bdbd5f947f6c939eb4df1d2c9b8

SHA-256

befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271

SSDEEP

384:xEWXD5fBirq/W2YyY8TbftcZWhtm1lTBcXtWloQXJ:xPBirq/WfAbqitukKXt+RJ

TLSH

T142529E95D2149F61C7F9213ED80B42E71B28DFF32B864B3647526C401879BDBA47EBA0

File type

Perl

Magic

a /usr/bin/perl script text executable

TrID

Unix-like shebang (var.1) (gen) (63.6%)

TrID

Perl script (36.3%)

File size

13.18 KB (13494 bytes)

Question 5

When was this malware first seen in the wild? Answer Guidance: YYYY-MM-DD
2017-01-17

www.virustotal.com/gui/file/befa9bfe488244c64db096522b4fad73fc0

Sourcing and... Spotify – Even... Spotify – Don't... Python

SUMMARY

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

VIRUSTOTAL

SUMMARYDETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY14

Basic Properties

MD5

72d4d364ed91dd9418d144a2db837a6d

SHA-1

794bcba867307bdbd5f947f6c939eb4df1d2c9b8

SHA-256

befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271

SSDEEP

384:xEWXD5fBirq/W2YyY8TbftcZWhtm1lTBcXtWloQXJ:xPBirq/WfAbqitukKXt+RJ

TLSH

T142529E95D2149F61C7F9213ED80B42E71B28DFF32B864B3647526C401879BDBA47EBA0

File type

Perl

Magic

a /usr/bin/perl script text executable

TrID

Unix-like shebang (var.1) (gen) (63.6%)

TrID

Perl script (36.3%)

File size

13.18 KB (13494 bytes)

History

First Seen In The Wild

2017-01-17 19:09:06 UTC

First Submission

2017-01-31 16:54:15 UTC

Last Submission

2022-01-20 11:12:40 UTC

Last Analysis

2022-01-20 11:12:40 UTC

Names

fpsaud

fpsaud.txt

Question 6

The malware infecting kutekitten uses dynamic DNS destinations to communicate with two C&C servers shortly after installation. What is the fully-qualified domain name (FQDN) of the first (alphabetically) of these destinations?

eidk.duckdns.org

VIRUSTOTAL

SUMMARYDETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY14

Contacted Domains

Domain

Detections

Created

Registrar

eidk.duckdns.org

0 / 90

2013-04-12

GANDI SAS

eidk.hopto.org

2 / 90

2000-02-17

TLDS L.L.C. d/b/a SRSPPlus

radarsubmissions.apple.com

0 / 90

1987-02-19

CSC CORPORATE DOMAINS, INC.

radarsubmissions.apple.com.akadns.net

0 / 90

1999-05-12

Akamai Technologies, Inc.

valid-apple.g.aaplimg.com

0 / 90

2013-05-21

CSC CORPORATE DOMAINS, INC.

world-gen.g.aaplimg.com

0 / 90

2013-05-21

CSC CORPORATE DOMAINS, INC.

Question 7

From the question above, what is the fully-qualified domain name (FQDN) of the second (alphabetically) contacted C&C server?

eidk.hopto.org

Contacted Domains

Domain

Detections

eidk.duckdns.org

0 / 90

eiak.duckans.org	0 / 90
eidk.hopto.org	2 / 90
radarsubmissions.apple.com	0 / 90
radarsubmissions.apple.com.akadns.net	0 / 90
valid-apple.g.aapling.com	0 / 90
world-gen.g.aapling.com	0 / 90

I guess these last 4 questions were to make up for the pain of question 3