Week in the Life of a DFIR

Elizabeth Schweinsberg
@bethlogic

Motivation

What my friends think I do

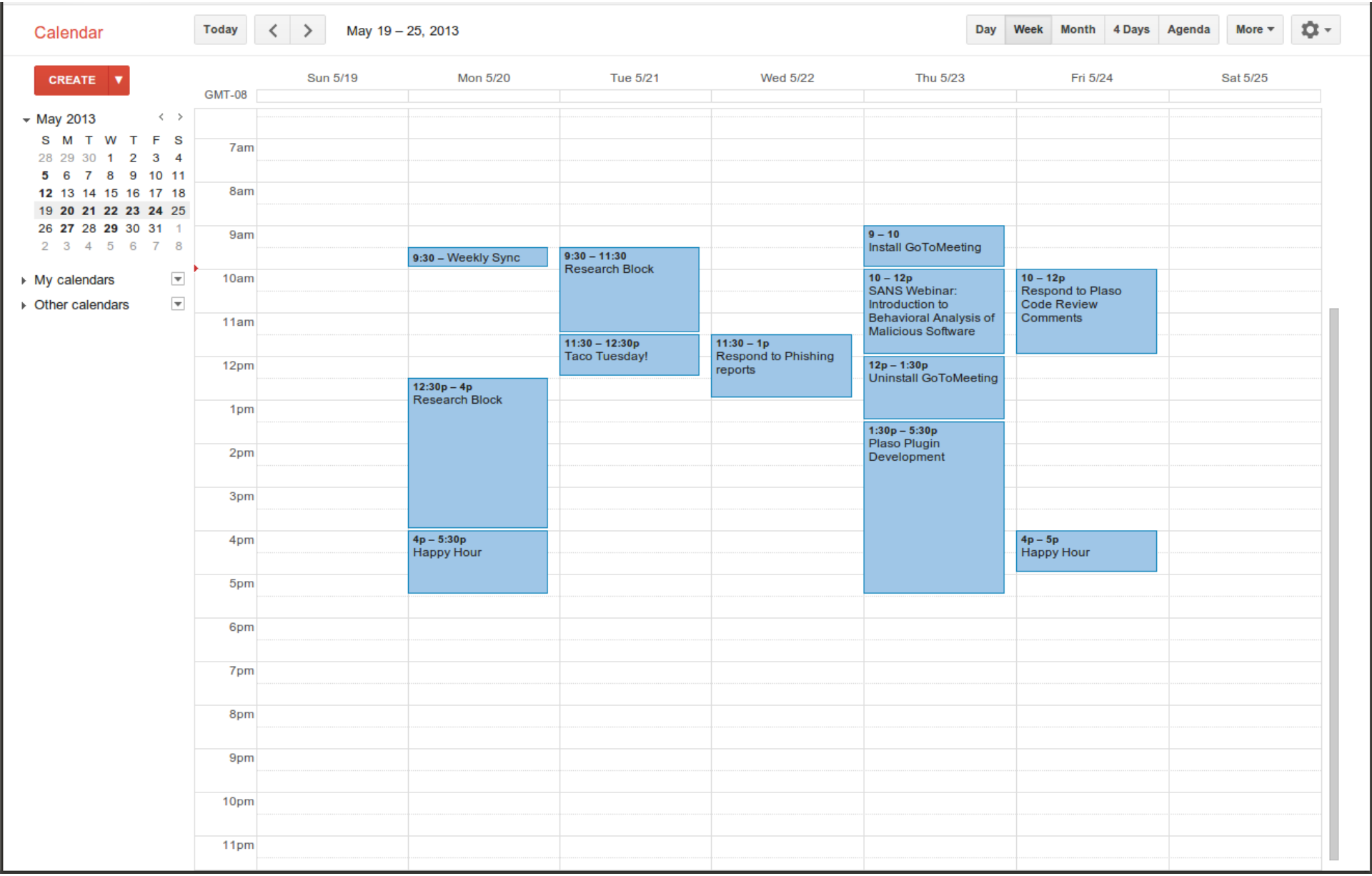
What my mom thinks I do

What IT thinks I do

What my cat thinks I do

What I think I do

What I really do


Calendar
Today
May 19 – 25, 2013
Day
Week
Month
4 Days
Agenda
More
CREATE
May 2013
S M T W T F S
28 29 30 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31 1
2 3 4 5 6 7 8
My calendars
Other calendars
GMT-08
Sun 5/19
Mon 5/20
Tue 5/21
Wed 5/22
Thu 5/23
Fri 5/24
Sat 5/25
7am
8am
9am
10am
11am
12pm
1pm
2pm
3pm
4pm
5pm
6pm
7pm
8pm
9pm
10pm
11pm
9:30 – Weekly Sync
9:30 – 11:30
Research Block
11:30 – 12:30p
Taco Tuesday!
11:30 – 1p
Respond to Phishing reports
12:30p – 4p
Research Block
4p – 5:30p
Happy Hour
9 – 10
Install GoToMeeting
10 – 12p
SANS Webinar: Introduction to Behavioral Analysis of Malicious Software
12p – 1:30p
Uninstall GoToMeeting
1:30p – 5:30p
Plaso Plugin Development
10 – 12p
Respond to Plaso Code Review Comments
4p – 5p
Happy Hour

Monday 9:30

Weekly Sync meeting with partner teams

It was a quiet weekend... too quiet...

Monday 10:23

Snort alert for a Java Exploit on a MacBook...

in Prague

- Have a local Tech remove drive from laptop and connect to your server for imaging
  - Calculate hashes
  - Copy drive to filer
  - Check hashes
- Research IDXs for today's case
  - A great blog tells you all you need to do!
  - http://computer-forensics.sans.org/blog/2013/02/16/idx-sample-file-malware
- Start log2timeline massive processing on the image and have a beer with co-workers before heading home

Tuesday

- Start investigation
  - Get an IDX parser from your research -- Perl or Python?
  - Use the timeline, grep, and icat to extract the IDX files
  - Run the IDX parser -- use the output to frame the data reduction
- Head to lunch for Taco Tuesday
- Read twitter and catch up on blogs
- Data reduction -- my timeline is 2GB! Where to begin?
  - Web history for that day
  - Process execution
  - Packet capture from the Snort alert
- Add IDX parser to the Plaso to-do list

Tuesday - IDX Parsing

```
eschwein-macbookair:SANS eschwein$ python idx_parser.py java_602.idx
Java IDX Parser -- version 1.4 -- by @bbaskin

IDX file: java_602.idx (IDX File Version 6.02)

[*] Section 1 (Metadata) found:
Content length: 14180
Last modified date: Wed, 05 May 2010 01:34:19 GMT (epoch: 1273023259)

[*] Section 2 (Download History) found:
URL: http://www.gxxxxx.com/a/java/xxz.jar
<null>: HTTP/1.1 200 OK
content-length: 14180
last-modified: Wed, 05 May 2010 01:34:19 GMT
content-type: text/plain
date: Wed, 05 May 2010 03:52:31 GMT
server: Apache/2
deploy-request-content-type: application/x-java-archive
deploy_resource_codebase_ip: 10.18.250.10

[*] Section 3 (Additional Data) found:
[*] Serialized data found of type: Data Block
[*] Compressed data found
Manifest-Version: 1.0
Created-By: 1.6.0_18 (Sun Microsystems Inc.)


eschwein-macbookair:SANS eschwein$
```

Tuesday - IDX Parsing

```
eschwein-macbookair:SANS eschwein$ python idx_parser.py java.idx
Java IDX Parser -- version 1.4 -- by @bbaskin

IDX file: java.idx (IDX File Version 6.05)

[*] Section 1 (Metadata) found:
Content length: 7162
Last modified date: Thu, 26 Jul 2001 05:00:00 GMT (epoch: 996123600)
Section 2 length: 365
Section 3 length: 167
Section 4 length: 15

[*] Section 2 (Download History) found:
URL: http://xxxxc146d3.gxhjxxwsf.xx:82/forum/dare.php?hsh=6&key=b30xxxx1c597
xxxx15d593d3f0xxx1ab
IP: 10.7.119.10
<null>: HTTP/1.1 200 OK
content-length: 7162
last-modified: Mon, 26 Jul 2001 05:00:00 GMT
content-type: application/x-java-archive
date: Sun, 13 Jan 2013 16:22:01 GMT
server: nginx/1.0.15
deploy-request-content-type: application/x-java-archive

[*] Section 3 (Jar Manifest) found:
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.8.3
X-COMMENT: Main-Class will be added automatically by build
Class-Path:
Created-By: 1.7.0_07-b11 (Oracle Corporation)

[*] Section 4 (Code Signer) found:
[*] Found: Data block.  Length: 4
Data:           Hex: 00000000
[*] Found: Data block.  Length: 3
Data: 0                 Hex: 300d0a
```

Tuesday - Plaso Filtering

```
eschwein-macbookair:plaso eschwein$ psort.py -o L2tcsv ../test_data/mac_demo.dump "SELECT foo WHERE
source is 'WEBHIST' AND date > '2013-07-01' and date < '2013-08-01' LIMIT 5"
date,time,timezone,MACB,source,sourcetype,type,user,host,short,desc,version,filename,inode,notes,for
mat,extra
07/08/2013,16:24:09,UTC,.A..,WEBHIST,Chrome History,Page Visited,-,-,http://www.apple.com/startpage/
 (Apple - Start),http://www.apple.com/startpage/ (Apple - Start) [count: 0] Host: www.apple.com (URL
 not typed directly - no typed count),2,/dev/sde2:/Users/demouser/Library/Application Support/Google
/Chrome/Default/History,338223,-,ChromeHistoryParser,
07/08/2013,16:24:13,UTC,.A..,WEBHIST,Chrome History,Page Visited,-,-,https://www.google.com/search?c
lient=safari&rls=en&q=google+chrome&ie=UTF-8&o...,https://www.google.com/search?client=safari&rls=en
&q=google+chrome&ie=UTF-8&oe=UTF-8 (google chrome - Google Search) [count: 0] Host: www.google.com (
URL not typed directly - no typed count),2,/dev/sde2:/Users/demouser/Library/Application Support/Goo
gle/Chrome/Default/History,338223,-,ChromeHistoryParser,
07/08/2013,16:24:16,UTC,.A..,WEBHIST,Chrome History,Page Visited,-,-,http://www.google.com/url?sa=t&
rct=j&q=&esrc=s&source=web&cd=1&ved=0CEQQFjAA&...,http://www.google.com/url?sa=t&rct=j&q=&esrc=s&sou
rce=web&cd=1&ved=0CEQQFjAA&url=http%3A%2F%2Fwww.google.com%2Fchrome%2F&ei=refaUdrFC-HniALbnIDoDg&usg
=AFQjCNFw-0GuxyuZwraQHrJ5tqsxgerAFQ&bvm=bv.48705608 d.cGE (http://www.google.com/url?sa=t&rct=j&q=&e
src=s&source=web&cd=1&ved=0CEQQFjAA&url=http%3A%2F%2Fwww.google.com%2Fchrome%2F&ei=refaUdrFC-HniALbn
IDoDg&usg=AFQjCNFw-0GuxyuZwraQHrJ5tqsxgerAFQ&bvm=bv.48705608 d.cGE) [count: 0] Host: www.google.com
(URL not typed directly - no typed count),2,/dev/sde2:/Users/demouser/Library/Application Support/Go
ogle/Chrome/Default/History,338223,-,ChromeHistoryParser,
07/08/2013,16:24:20,UTC,.A..,WEBHIST,Chrome History,Page Visited,-,-,https://www.google.com/intl/en/
chrome/browser/thankyou.html (Chrome Browser),https://www.google.com/intl/en/chrome/browser/thankyou
.html (Chrome Browser) [count: 0] Host: www.google.com (URL not typed directly - no typed count),2,/
dev/sde2:/Users/demouser/Library/Application Support/Google/Chrome/Default/History,338223,-,ChromeHi
storyParser,
07/08/2013,16:25:39,UTC,.A..,WEBHIST,Chrome History,Page Visited,-,-,https://accounts.google.com/Ser
viceLogin?service=chromiumsync&sarp=1&rm=hide&...,https://accounts.google.com/ServiceLogin?service=c
hromiumsync&sarp=1&rm=hide&continue=https%3A%2F%2Fwww.google.com%2Fintl%2Fen-US%2Fchrome%2Fblank.htm
l%3Fsource%3D0 (Google Accounts) [count: 0] Host: accounts.google.com (URL not typed directly - no t
yped count),2,/dev/sde2:/Users/demouser/Library/Application Support/Google/Chrome/Default/History,33
8223,-,ChromeHistoryParser,
[INFO]
********************************** Counter ***********************************
[INFO]              Stored Events : 1352209
[INFO]       Events Filtered Out : 3225
[INFO]           Events Included : 5
[INFO]                Limited By : 5
eschwein-macbookair:plaso eschwein$
```

Tuesday - Plaso Filtering

```
eschwein-macbookair:plaso eschwein$ psort.py -q ../test_data/mac_demo.dump "SELECT datetime, message, f
ilename WHERE filename contains 'LaunchAgent' LIMIT 5"
datetime,message,filename
2012-06-20T20:25:08+00:00,/dev/sde2:/System/Library/LaunchAgents/com.apple.TrustEvaluationAgent.plist,/
System/Library/LaunchAgents/com.apple.TrustEvaluationAgent.plist
2012-06-20T20:39:15+00:00,/dev/sde2:/System/Library/LaunchAgents/com.apple.imklaunchagent.plist,/System
/Library/LaunchAgents/com.apple.imklaunchagent.plist
2012-06-20T20:39:23+00:00,/dev/sde2:/System/Library/Frameworks/InputMethodKit.framework/Versions/A/Reso
urces/imklaunchagent,/System/Library/Frameworks/InputMethodKit.framework/Versions/A/Resources/imklaunch
agent
2012-06-20T20:39:23+00:00,/dev/sde2:/System/Library/Frameworks/InputMethodKit.framework/Versions/A/Reso
urces/imklaunchagent,/System/Library/Frameworks/InputMethodKit.framework/Versions/A/Resources/imklaunch
agent
2012-06-20T20:42:29+00:00,/dev/sde2:/System/Library/LaunchAgents/com.apple.midiserver.plist,/System/Lib
rary/LaunchAgents/com.apple.midiserver.plist
```

Tuesday, during NCIS:LA...

DNS Hijack Alert for your .fn cc tld

Receive an alert from our 3rd party monitoring system that the DNS resolution our cc tld for Florin (.fn) has been redirected to a non-corporate site.

- Confirm that webfu.fn is not pointing to our page anymore
  - Grab a screenshot, check whois, and check dig to collect intel
- Get someone to redirect
- Work with your Domain Management company to contact the registry
- Give PR a heads up

Wednesday

- Bug the Domain Monitoring company to get a postmortem from the .fn registrar
- Respond to emails about reports of phishing
  - Get headers and look into the origins of the email
  - Search Google for reports
  - Reassure your coworkers that it’s standard spam and nothing targeted

Wednesday 13:43

Lost Laptop with Confidential Data

A financial analyst reports that her car was broken into while she was at dinner the night before and her work bag containing her work laptop, RSA token, and tablet with corporate data access were stolen.

- Get her to change her password, and revoke any other access like OAuth tokens
- Look at her account access for the last day -- no unusual locations
- Talk to her about confidential data and if she had any on her laptop
- Talk to the lawyers about what she reports

Thursday

- Install the Citrix GoToMeeting on MacBook Air
- Watch a SANS webcast -- Introduction to Behavioral Analysis of Malicious Software
- Pick the next plaso plugin from the priority list and start coding!

Thursday 15:07

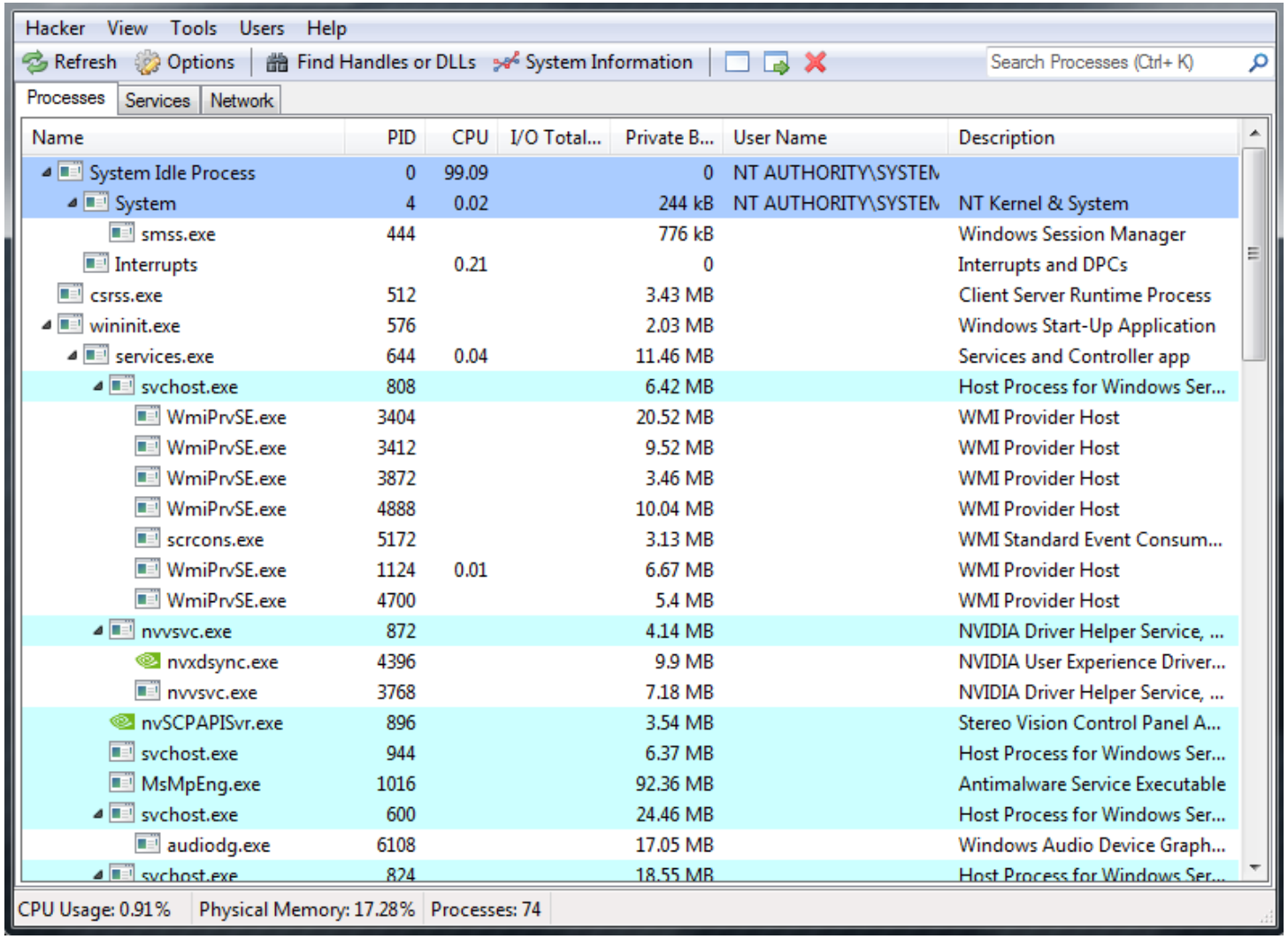
Fireeye alert for a malicious file download

- Connect to GRR to investigate
- Run the Chrome History flow
- Find out there was more than one Chrome profile, so go back and run that flow on all the profiles
- Pull down Registry files and Windows Evtx files
- Run plaso on them for a timeline
- Catch the original website that redirected to the malicious one, see the file downloaded, and execution stopped by Bit9
- Feed the URLs to the Safe Browsing team, upload to VirusTotal

Friday

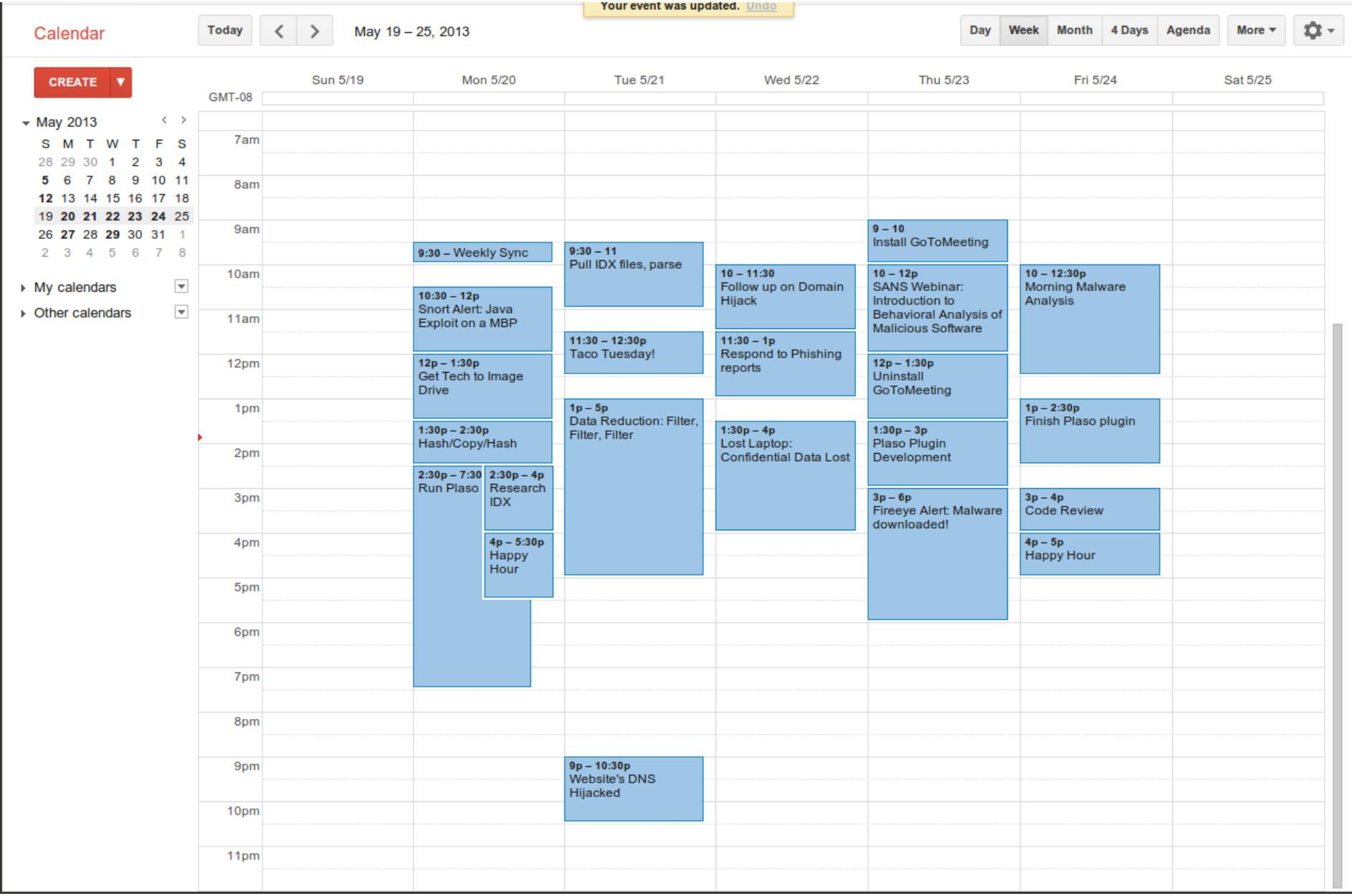
- Quick analysis of the binary -- it was just the dropper
  - Run this file in a sandbox, capture the web requests it makes
  - Fetch the next file -- wget from an EC2 instance?
  - Do some analysis on the 2nd Stage - What's the C2?
    - Strings + Grep on the EXE: What do you see? Or don't see?
    - Fire up the sandbox again to run the 2nd stage
    - Decide to try out Process Hacker that Lenny Zeltser mentioned in the Webcast yesterday
    - Check out the binary in IDAPro
  - Write a Snort signature to detect the dropper and main file

Friday - Analysis



Friday - After Lunch

- Finish the plaso plugin you started on Thursday…
- Wait for Code Review comments...
- Have a beer with coworkers, and head out for a hopefully quiet weekend


Your event was updated. Undo
Calendar
Today
May 19 – 25, 2013
Day
Week
Month
4 Days
Agenda
More
CREATE
May 2013
S M T W T F S
28 29 30 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31 1
2 3 4 5 6 7 8
My calendars
Other calendars
GMT-08
Sun 5/19
Mon 5/20
Tue 5/21
Wed 5/22
Thu 5/23
Fri 5/24
Sat 5/25
7am
8am
9am
10am
11am
12pm
1pm
2pm
3pm
4pm
5pm
6pm
7pm
8pm
9pm
10pm
11pm
9:30 – Weekly Sync
10:30 – 12p
Snort Alert: Java Exploit on a MBP
12p – 1:30p
Get Tech to Image Drive
1:30p – 2:30p
Hash/Copy/Hash
2:30p – 7:30
Run Plaso
2:30p – 4p
Research IDX
4p – 5:30p
Happy Hour
9:30 – 11
Pull IDX files, parse
11:30 – 12:30p
Taco Tuesday!
1p – 5p
Data Reduction: Filter, Filter, Filter
9p – 10:30p
Website's DNS Hijacked
10 – 11:30
Follow up on Domain Hijack
11:30 – 1p
Respond to Phishing reports
1:30p – 4p
Lost Laptop: Confidential Data Lost
9 – 10
Install GoToMeeting
10 – 12p
SANS Webinar: Introduction to Behavioral Analysis of Malicious Software
12p – 1:30p
Uninstall GoToMeeting
1:30p – 3p
Plaso Plugin Development
3p – 6p
Fireeye Alert: Malware downloaded!
10 – 12:30p
Morning Malware Analysis
1p – 2:30p
Finish Plaso plugin
3p – 4p
Code Review
4p – 5p
Happy Hour