ANALYSIS 101

FOR HACKERS AND INCIDENT RESPONDERS

Kristy Westphal

DEFCON 27

A Four Hour Tour….

- Introduction
- Ignorance and importance to analysis
- On to hands on!
- Log analysis
- Network forensics
- Endpoint forensics
- Malware analysis
- A quick side journey to Cloud incident response
- Putting it all together

What did you just say?

- This class is about how to approach analysis techniques
- Not about how to use tools or hack stuff
- It’s all about understanding what you’ve found

Why am I here?

- Information security leader specializing in security assessments, operational risk and program development
- Security is painful all around; hopefully I can help
- Let’s share knowledge and make it less painful for all of us!





A LITTLE IGNORANCE

Why is this important?

“Ignorance is the absence of fact, understanding, insight, or clarity about something.” – Firestein

It is very difficult to find a black cat in a dark room—especially when there is no cat.

“In complex systems, decision-making calls for judgments under uncertainty, ambiguity and time pressure. In those settings, options that appear to work are better than perfect options that never get computed.”

-Sidney Dekker

Analysis is Like Solving a Mystery…

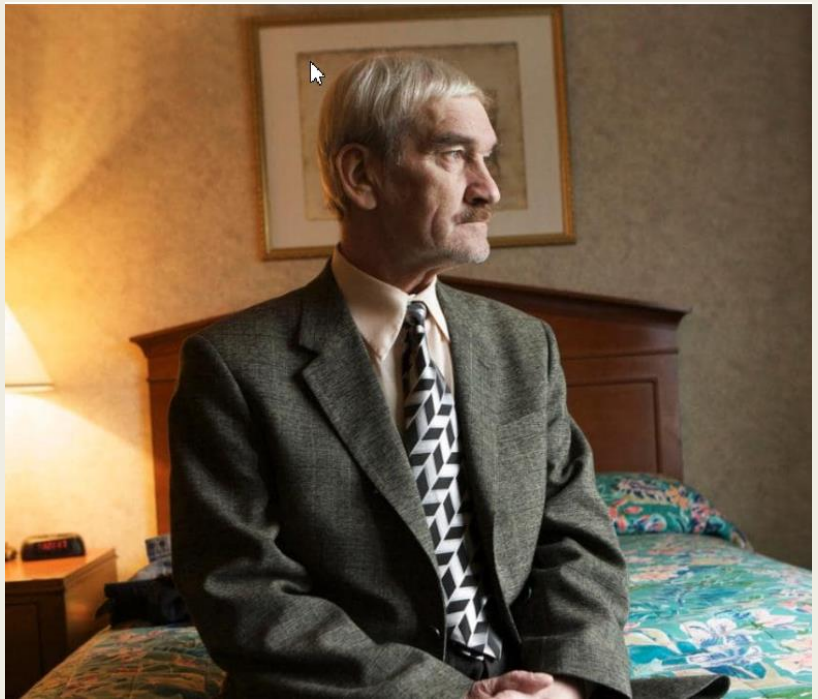
- "I was trained as a physicist, and in physics we're always trying to figure out how the world works," he explained. "But you have to ask the right questions. You have to investigate things. You always have to be willing to question your assumptions. DDoS defense is very similar. You can't just look at the attacks you're getting. You have to be more proactive and try to attract more attacks and take some risks.“

  –*Damian Menscher*

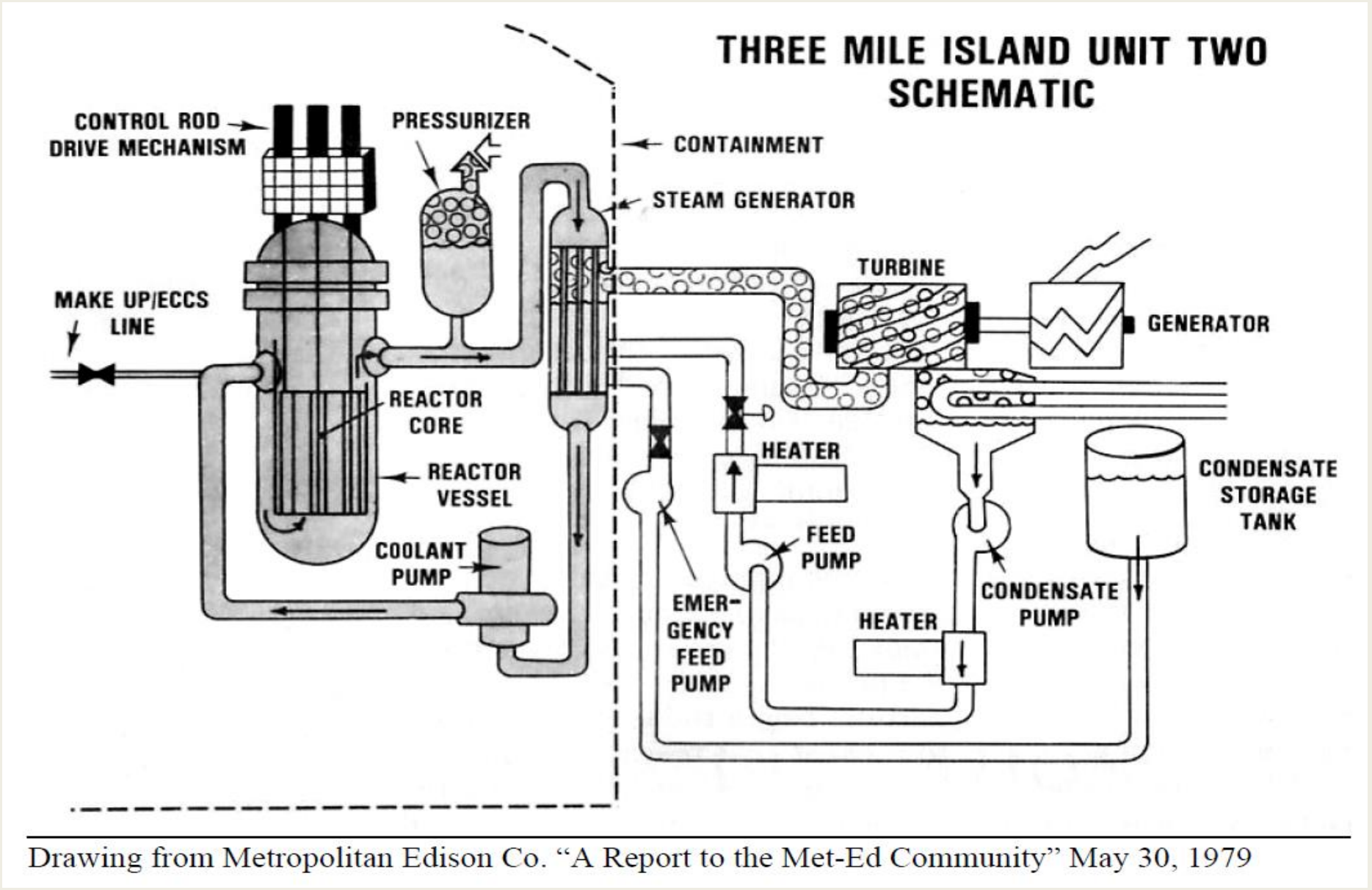
LET’S LOOK AT SOME HISTORICAL EXAMPLES

How to save the world

- Stanislav Petrov literally saved the world, in the face of wildly incomplete information

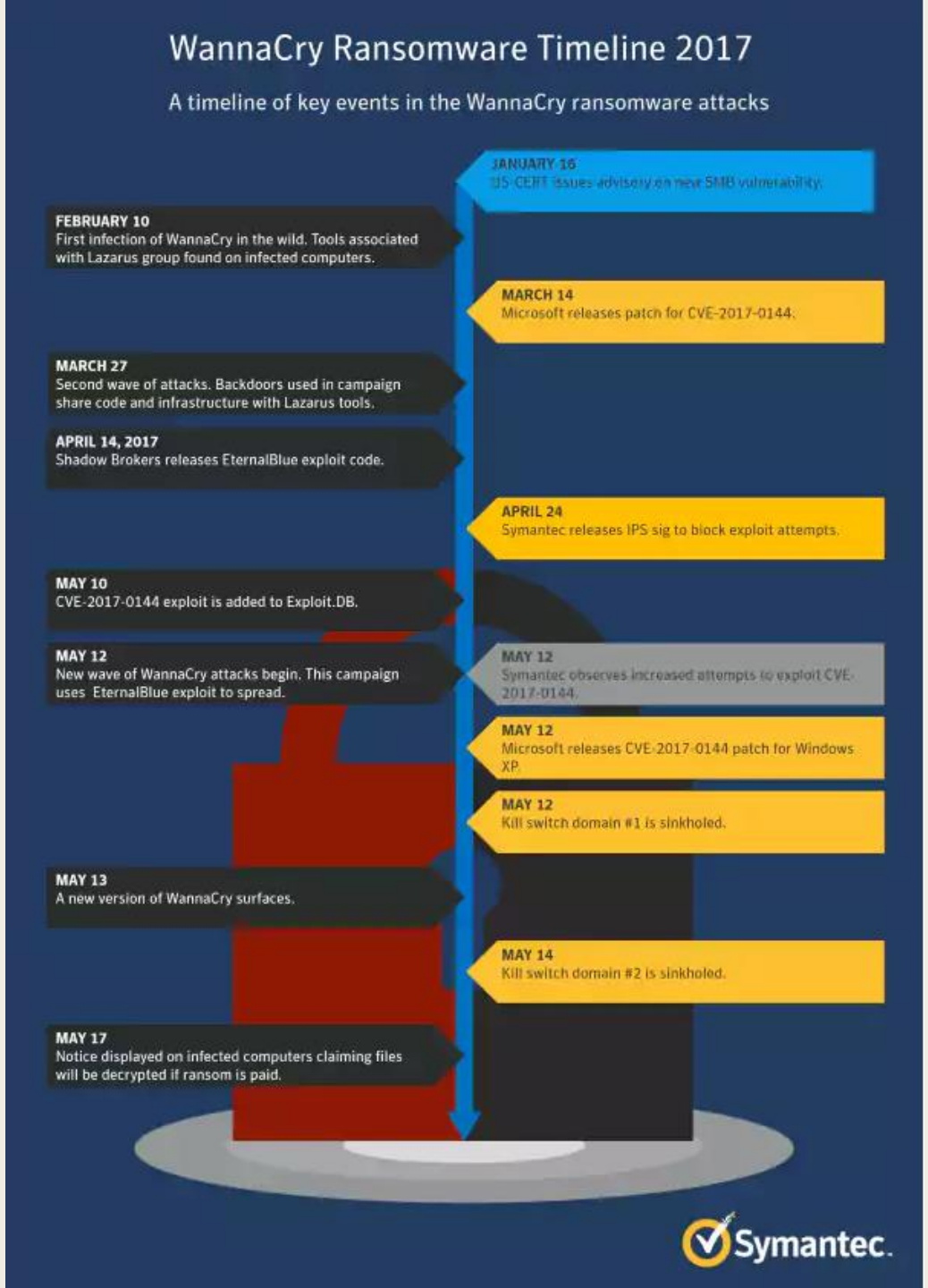


Or how about this mess?



Drawing from Metropolitan Edison Co. "A Report to the Met-Ed Community" May 30, 1979

Wanna Cry?



But you know what the most interesting thing is?

"We might even go a step further and recognize that there are unknowable unknowns—things that we cannot know due to some inherent and implacable limitation."
-Firestein



ANALYSIS PARALYSIS

(this also is Totter)

What justifies good analysis?

- Context
- Accepting that you don’t know everything
- Understanding there is more than one way to analyze something
- A little humility…

Traditional analysis techniques

- Qualitative v Quantitative
- We are generally trying to solve problems
  - *Mind Maps*
  - *Ishiwaka diagram (cause and effect diagrams)*
  - *Five forces (could be twisted to security analysis)*
  - *TOC (Theory of Constraints)*
  - *CPM (Critical Path Method)*
- These are great, but maybe not how to approach technical analysis
  - *So we turn to data analysis (yes, Big Data too)*

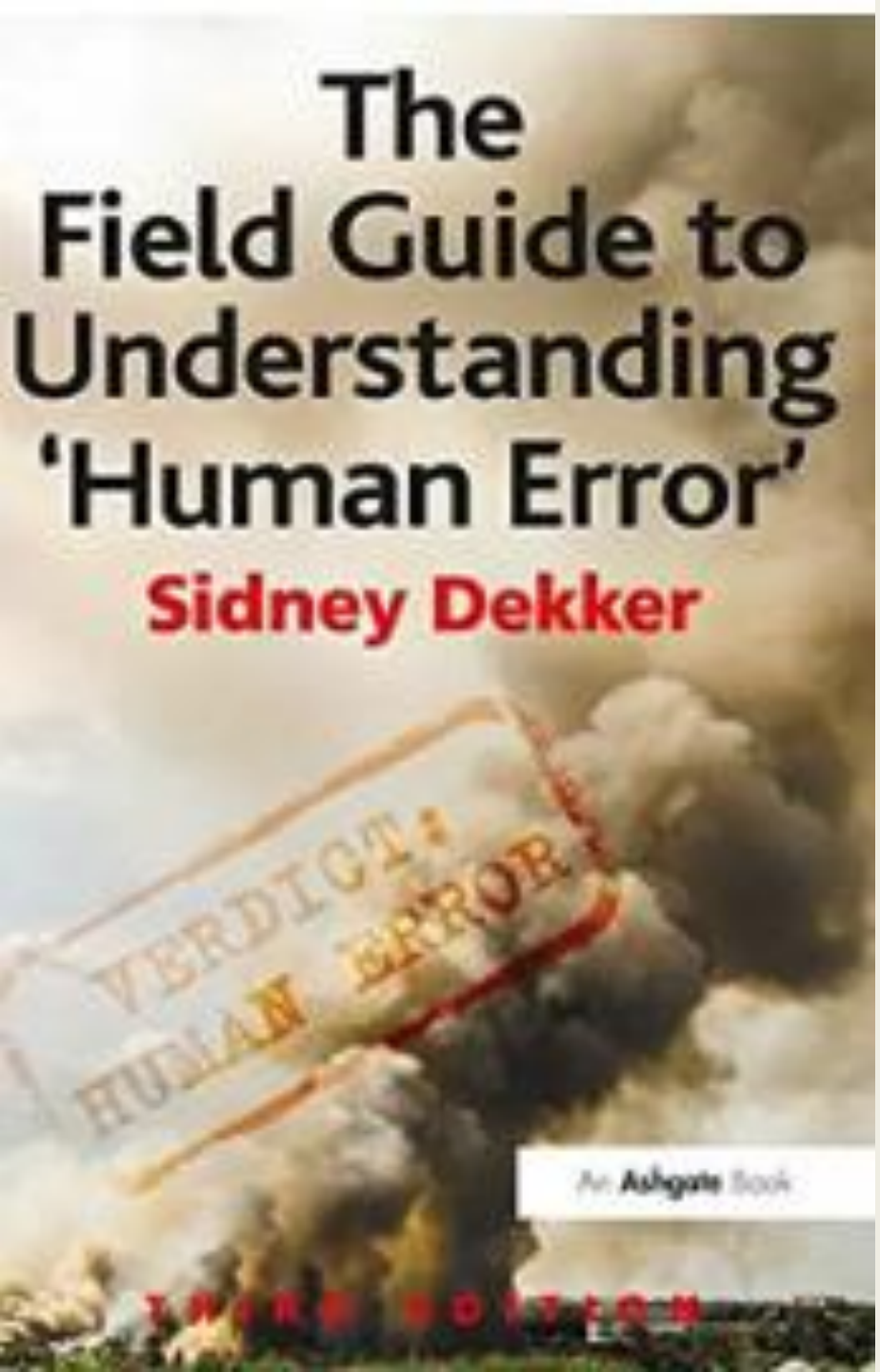
How do you like to do analysis?

- Spreadsheets?
- Text searches?
- Trend graphs?
- Data lakes?
- Did you say ‘reading log files?’

Think about a task you are given- how do you analyze it?

- You put together a timeline/project plan
- You work diligently to achieve it
- Yet the steps you originally map out never end up completed like you originally planned
  - *Oftentimes, the end-result isn't what was originally asked for either*

BUT MAYBE A LITTLE PROCESS



Keep this in mind…

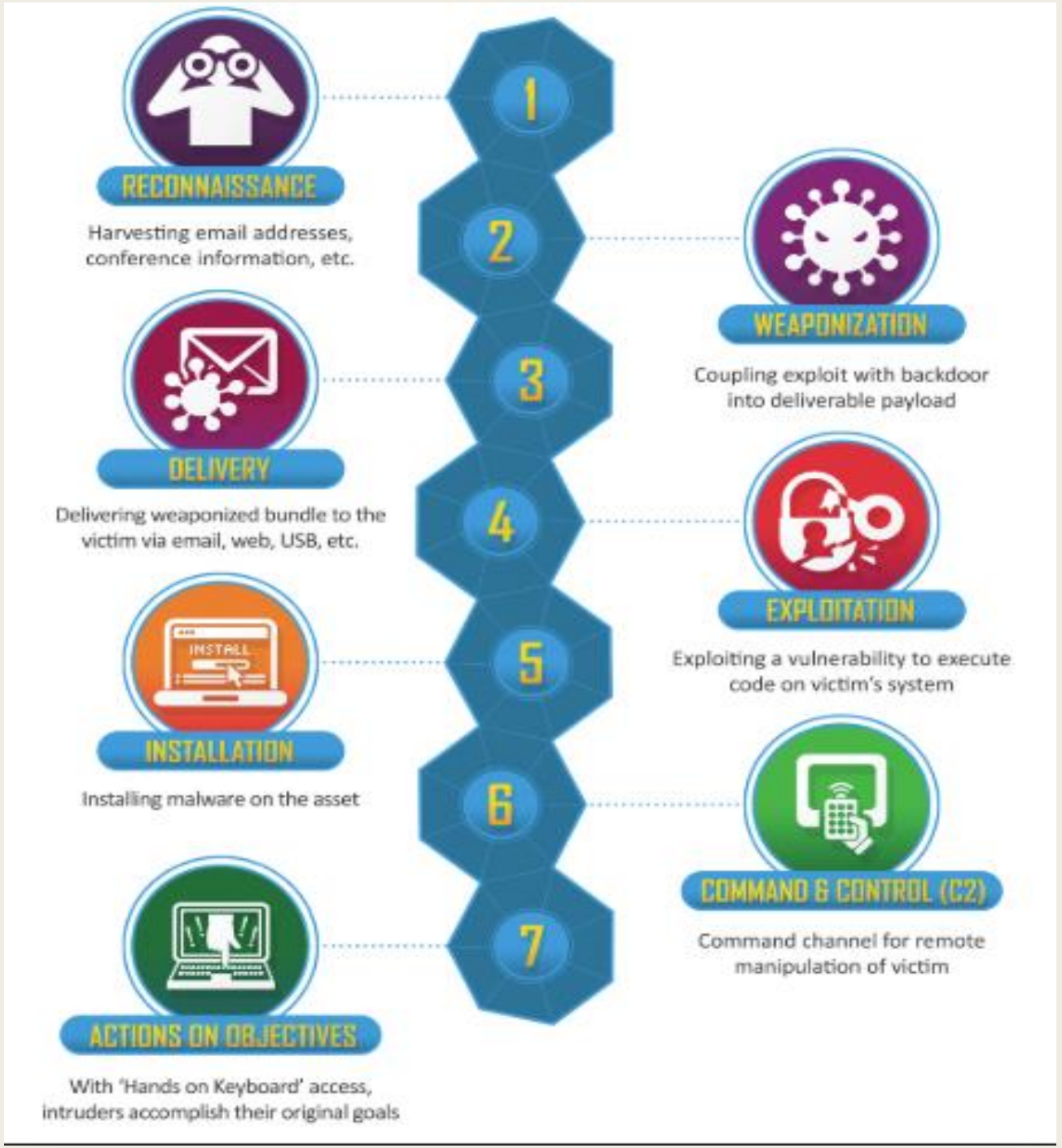
- Getting human factors data
- Building a timeline
- Putting data in context
- Leaving a trace
- Constructing causes
- Making recommendations

Ways to do Security Operations/Security Analysis

- Know the tools/controls
  - *How they work*
  - *How they are implemented*
- Know your enemy
- Follow the bread crumbs
  - *Pivot through the tools*
- But know how to read the logs
  - *How? Open source or vendor resources*

Maybe some regular starting points

- So this thing happened (an alert, or you find something in a log)
- What steps to analyze?
  - *Logs*
  - *OSINT*
  - *Threat Intel data*
  - *Google*
  - *IOCs*
  - *Kill Chain*

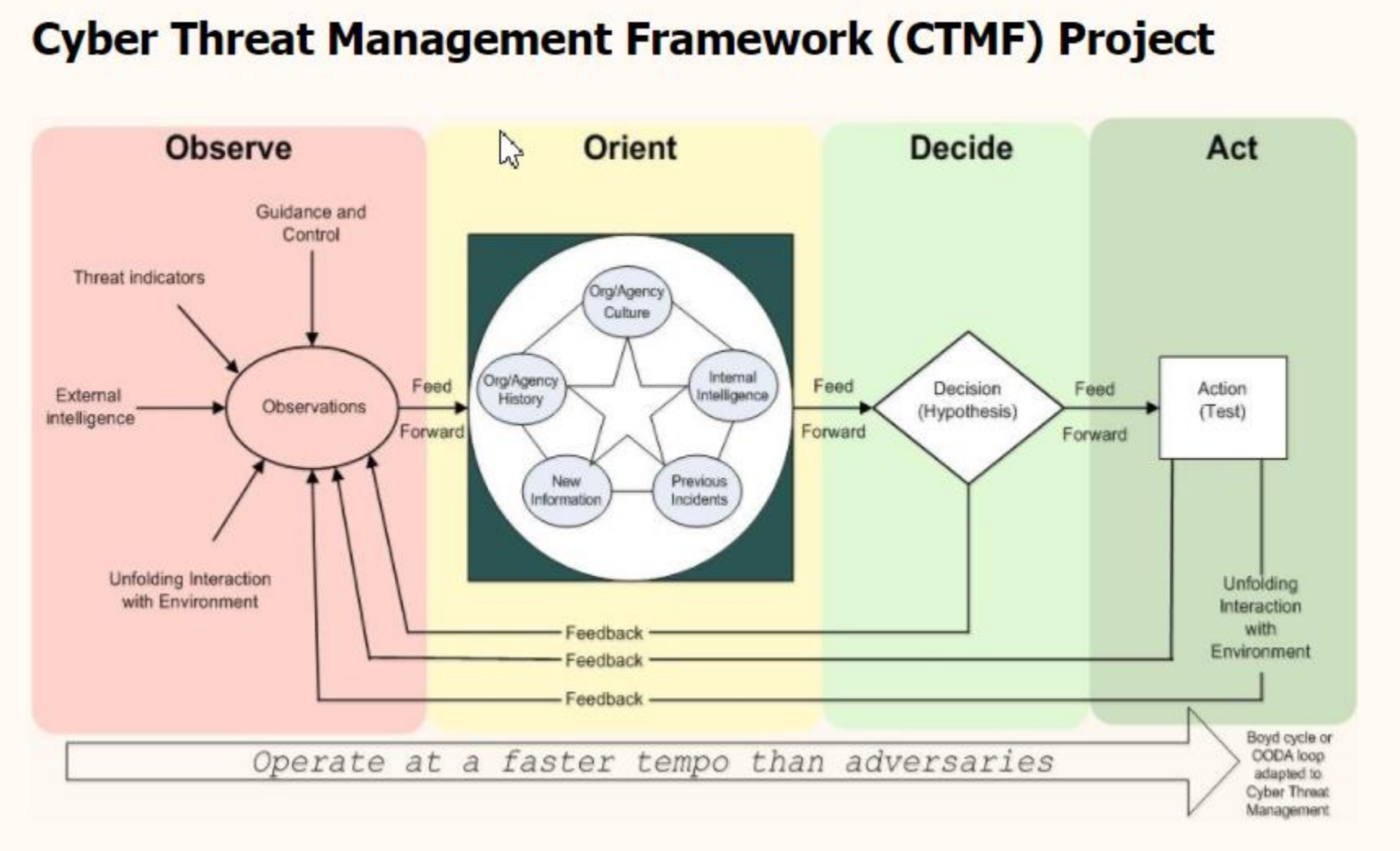

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Then maybe apply a little DREAD (longer term)



- I just felt that eyeroll. Yes, from you.
- But think about it; we need to think a little differently
- Having a framework for your questions can be helpful
- So use as you see fit
  - *For Damage: How big would the damage be if the attack succeeded?*
  - *For Reproducibility: How easy is it to reproduce an attack to work?*
  - *For Exploitability: How much time, effort, and expertise is needed to exploit the threat?*
  - *For Affected Users: If a threat were exploited, what percentage of users would be affected?*
  - *For Discoverability: How easy is it for an attacker to discover this threat?*

Another way to go



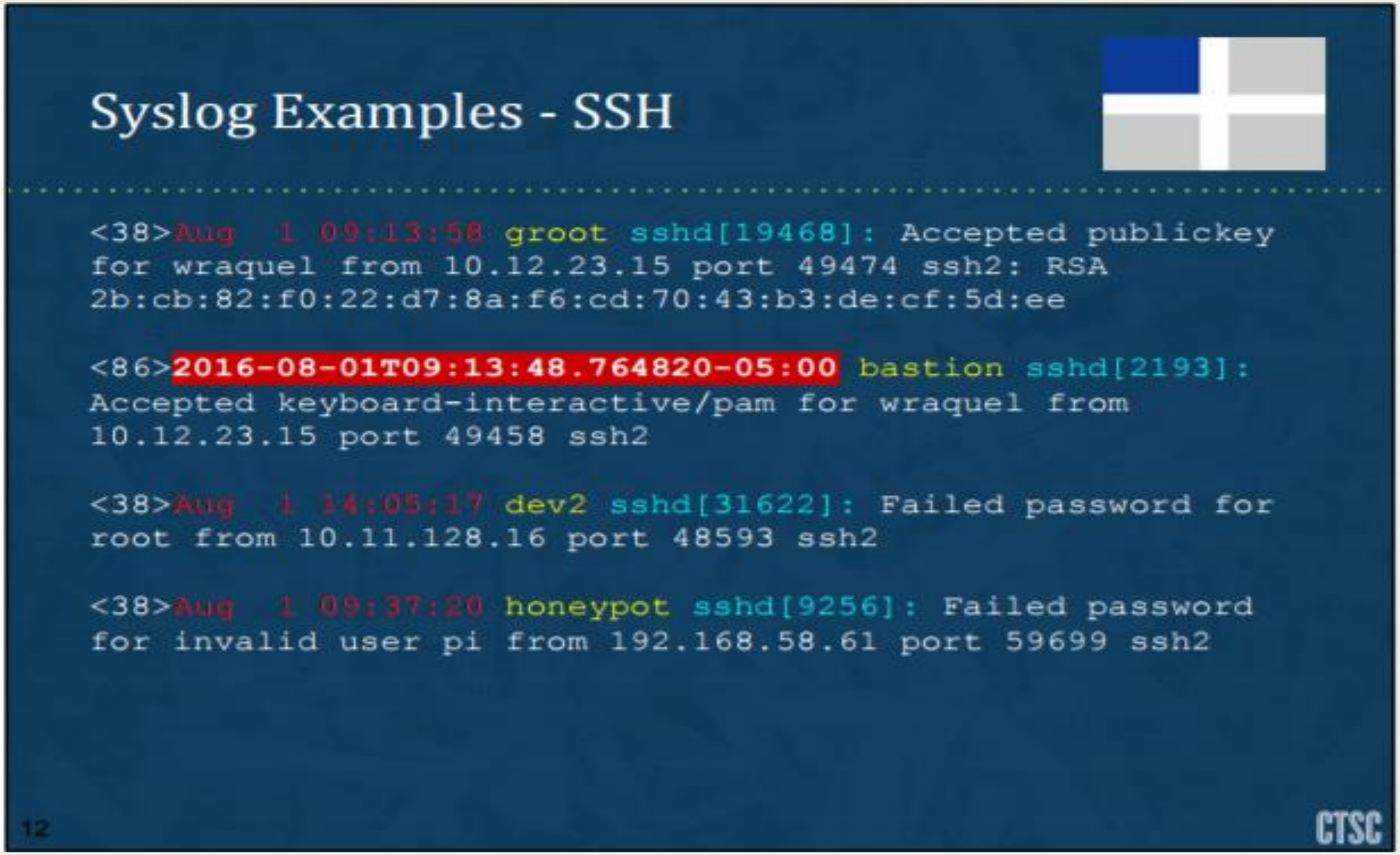
SPEED ROUND OF SAMPLES

What does this mean?

```
0C1AFAD4 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFAE4 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFAF4 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB04 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB14 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB24 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB34 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB44 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB54 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB64 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB74 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 90 90 ..............ÉÉ
0C1AFB84 EB 19 5B 4B 90 33 C9 90 80 7B 01 E9 75 01 C3 66 δ↓[KÉ3╔ÉÇ{☺θu☺├f
0C1AFB94 B9 7B 04 80 34 0B D8 E2 FA EB 05 E8 E2 FF FF FF ╣{♦Ç4♂╪Γ·§♣§Γ
0C1AFBA4 E9 E1 03 00 00 5F 64 A1 30 00 00 00 8B 40 0C 8B θß♥..._di0...ï@.ï
0C1AFBB4 70 1C AD 8B 68 08 8B F7 6A 0F 59 E8 81 03 00 00 pL↓ïh◘ï≈j☼Y§ü♥..
0C1AFBC4 90 E2 F8 68 33 32 00 00 68 55 73 65 72 54 8B 46 ÉΓ°h32..hUserTïF
0C1AFBD4 0C E8 EF 02 00 00 8B E8 6A 01 59 E8 61 03 00 00 .§∩☻..ï§j☺Y§a♥..
0C1AFBE4 E2 F9 68 6F 6E 00 00 68 75 72 6C 6D 54 8B 46 0C Γ·hon..hurlmTïF.
0C1AFBF4 E8 D0 02 00 00 8B E8 6A 01 59 E8 42 03 00 00 E2 §╨☻..ï§j☺Y§B♥..Γ
0C1AFC04 F9 68 6C 33 32 00 68 73 68 65 6C 54 8B 46 0C E8 ·hl32.hshelTïF.§
0C1AFC14 B1 02 00 00 8B E8 6A 01 59 E8 23 03 00 00 E2 F9 ▒☻..ï§j☺Y§#♥..Γ·
0C1AFC24 81 EC 00 01 00 00 8B DC 81 C3 80 00 00 00 6A 00 ü∞.☺..ï▄ü├Ç...j.
0C1AFC34 6A 1A 53 6A 00 FF 56 44 33 C0 40 80 3C 03 00 75 j→Sj. VD3└@Ç<♥.u
0C1AFC44 F9 89 86 90 00 00 00 C7 04 03 5C 61 2E 65 C7 44 ·ëåÉ...╟♦♥\a.e╟D
0C1AFC54 03 04 78 65 00 00 33 C9 51 51 53 57 51 33 C0 8B ♥♦xe..3╔QQSWQ3└ï
0C1AFC64 46 40 E8 5E 02 00 00 83 F8 00 0F 85 7F 01 00 00 F@§^☻..ã°.☼à⌂☺..
0C1AFC74 6A 00 6A 00 6A 03 6A 00 6A 02 68 00 00 00 C0 53 j.j.j♥j.j☻h...└S
0C1AFC84 8B 46 24 E8 3D 02 00 00 83 F8 FF 0F 84 5E 01 00 ïF$§=☻..ã° ☼ä^☺.
0C1AFC94 00 89 46 60 6A 00 50 FF 56 28 89 46 64 8B 86 90 .ëF`j.PˇV(ëFd
0C1AFCA4 00 00 00 C7 04 03 5C 62 2E 65 C7 44 03 04 78 65 ...╟♦♥\b.e╟D♥♦xe
```



Or how about this?



What does this mean?

Jul 16 10:54:39 SourceFire SFIMS: [1:469:1] ICMP PING NMAP [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 210.22.215.77 -> 67.126.151.137

- *“The known is never safe; it is never quite sufficient.” -Firestein*

Let’s talk about the three Cs

- Critical Thinking
- Communication
- Control of the Message



STOP. THINK CRITICALLY

Critical Security Thinking

- Critical security thinking is a term for the practice of using logic and facts to form an idea about security
- That idea may be an answer, a conclusion, or a characterization of something or someone so that verification tests can be well defined
- As an answer or a conclusion- which one makes the most sense?
- As a characterization - you'll know what you need to verify. It will also help you respect different opinions or viewpoints beyond security itself
- Critical thinking help you address contradictory conclusions and explore alternate consequences
- Even if the critical security thinking model can't provide an answer it should tell you what facts are still missing and from where you need to get them

Critical Thinking Process

- Process is “Dependent on the Analyst being able to discern true statements or at least recognize the degree of possible falsity or dynamic properties in a statement.” -OSSTM
- “The Analyst will need to have a good understanding of what is being analyzed and of logical fallacies used to make qualifiers, statements based on fallacious concepts usually in the form of axioms or best practices.” -OSSTM

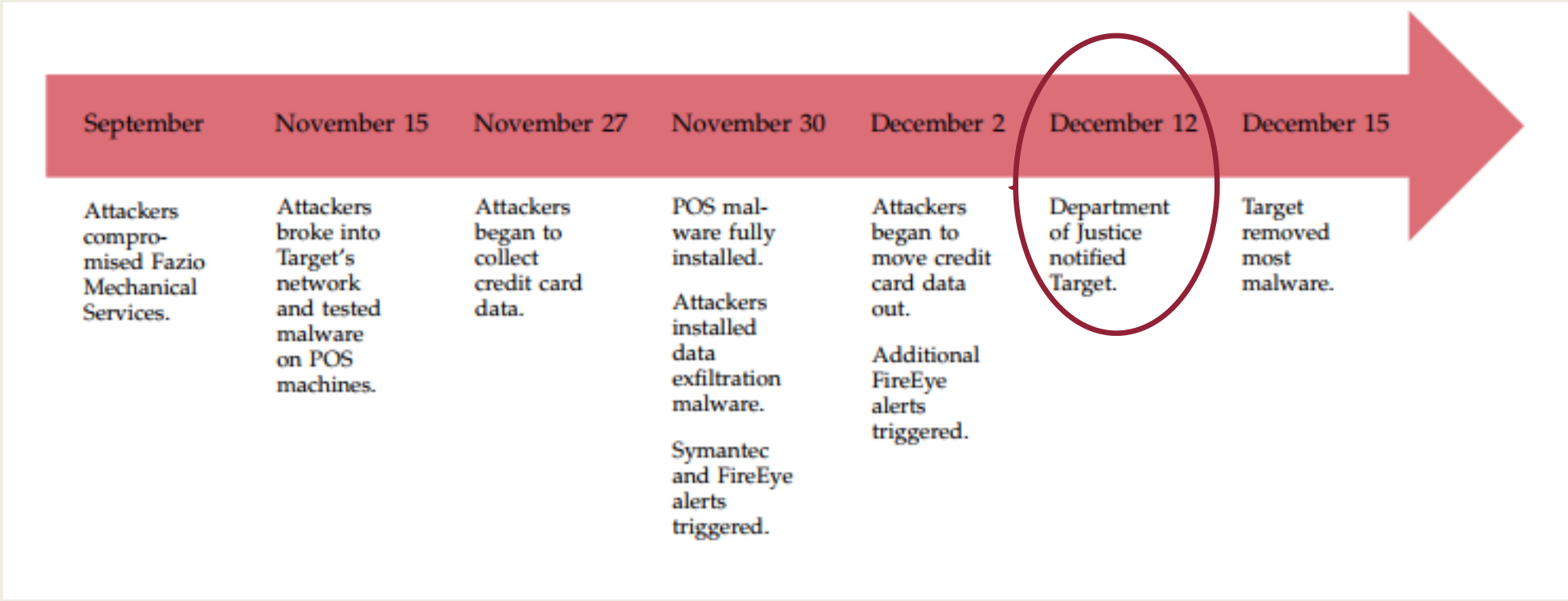
The Six Step Analysis Technique

1. Build your knowledge of the target
2. Determine the global level of experience
3. Determine any bias or ulterior motives
4. Translate jargon
5. Be sure the test platform analysis has been properly calibrated
6. Assure that the you get the most direct answer

Let's talk about Target (yes, again)

"Predicting or targeting some specific advance is less useful than aiming for deeper understanding." –Firestein

Ouch!



Hypothesis or no?

"…you may often miss data that would lead to a better answer, or a better question, because it doesn't fit your idea." –Firestein

- Virus outbreak on an IaaS platform

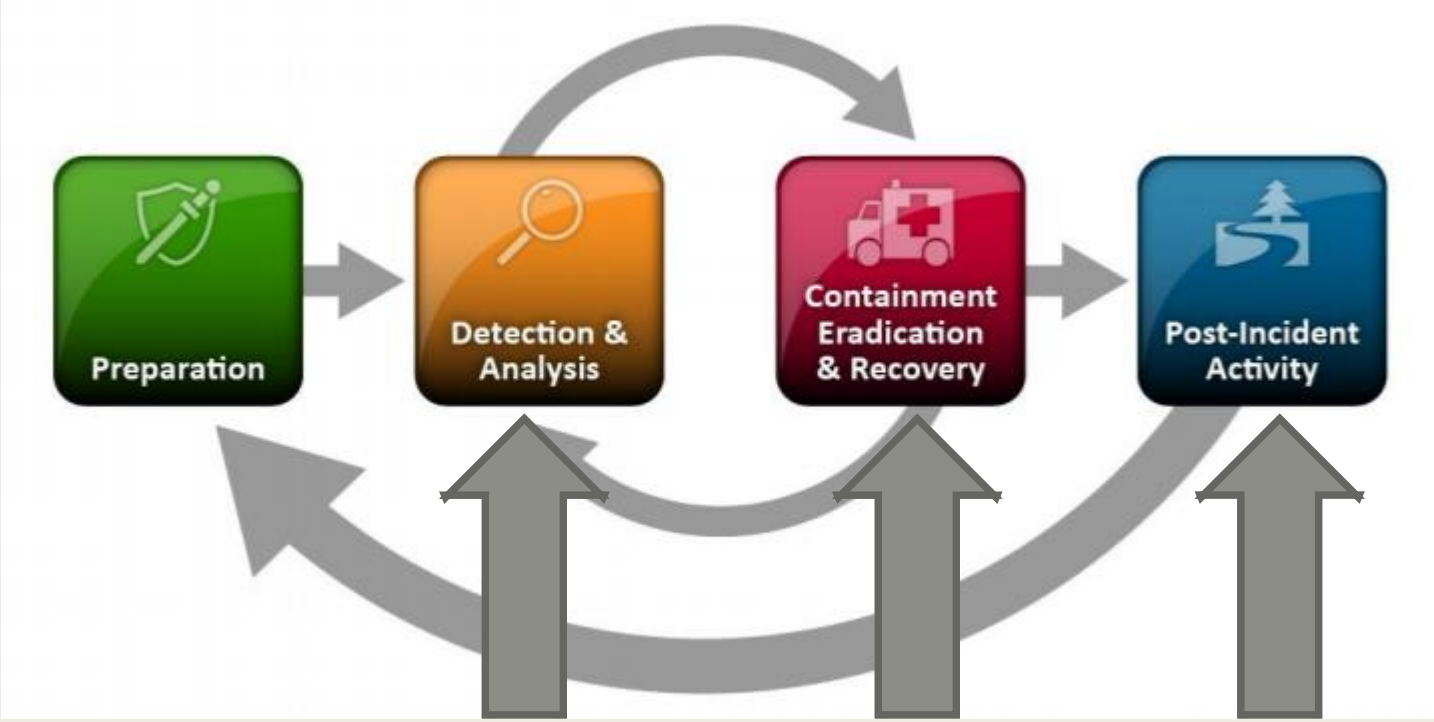
Let’s dissect a site for a second…

- /m/deals/christmas-gifts/sports-and-outdoors
- /m/deals/christmas-gifts/sports-and-outdoors/camping?_be_shelf_id=4138&cat_id=4125_546956_4128
- /account/login?tid=0&returnUrl=%2Fbrowse%2Fmovies%2F4096_530598
- /account/signup?tid=0&returnUrl=%2Fbrowse%2Fmovies%2F4096_530598
- /account/trackorder
- /account/login?tid=0&returnUrl=/easyreorder
- /account/signup
- /cart?source=pac
- /checkout/#/sign-in
- /checkout/#/fulfillment

COMMUNICATION: LET'S GET VISUAL



At what point does Visual Incident Response help?

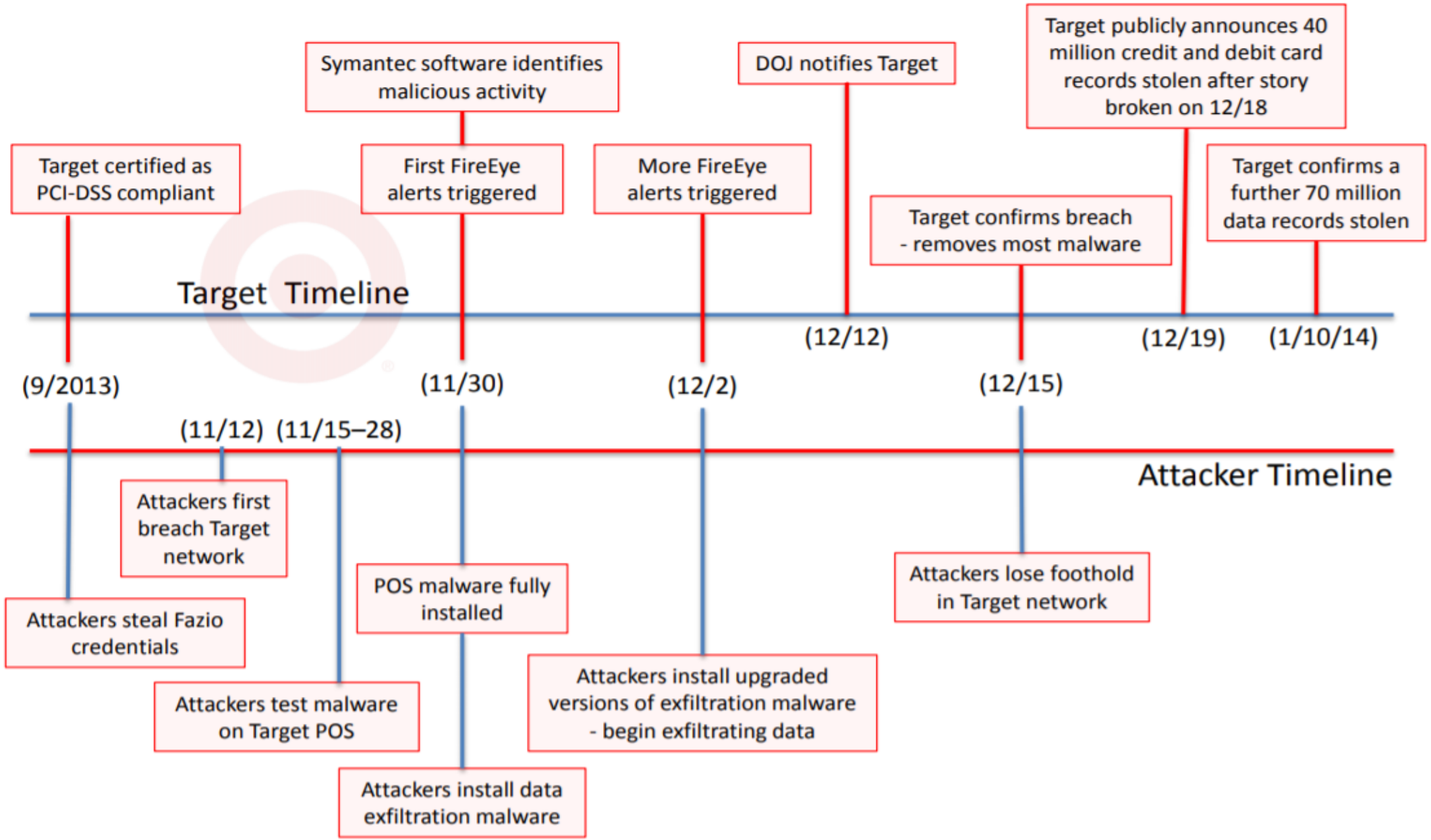


Here for sure

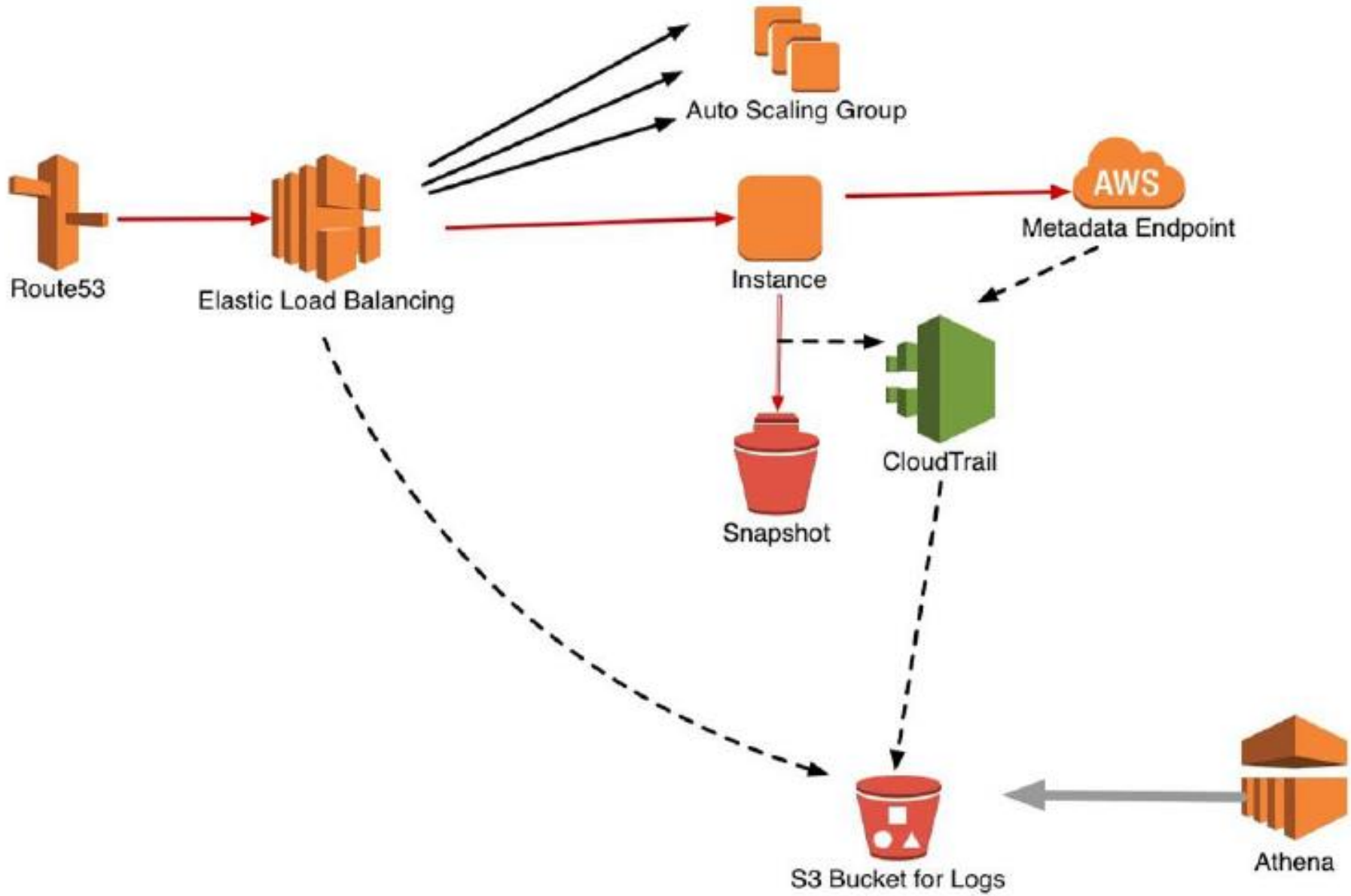
Sometimes here too

For sure here

A Timeline of the Target Data Breach



CLOUD TRAIL


Auto Scaling Group
Route53
Elastic Load Balancing
Instance
AWS
Metadata Endpoint
Snapshot
CloudTrail
S3 Bucket for Logs
Athena

Presentation

- From Avinash Kaushik:
- #1. Don't be sloppy. Your data presentation is your brand.
- #2. Bring insane focus, and simplify.
- #3. Calibrate data altitude optimally.
- #4. Eliminate distractions, make data the hero!
- #5. Lines, bars, pies… stress… choose the best-fit.
- #6. Consolidate data, be as honest as you can be.
- #7. Ditch the text, visualize the story.

“It’s not the ink, it’s the think”

Need help with visualization?

- Check out the Information is beautiful Facebook page
  - *You know pretty quickly what this is saying….*



Also pretty easy to understand



Controlling the message

- What’s going on
- Impacts of the event
- Actions
- Communication considerations

But how do I start?

- By asking questions
- Always assume (yes, you have permission) that you don't know everything
  - What are the facts?
  - How are some various ways that the facts came about?
  - Where did the incident start (or where do you think it started?)
  - How was the incident even detected?
  - What is normal behavior in the environment?
  - What are some ways around the normal stuff?
  - Are there related events?
  - Has anyone outside the company seen your indicators? (Google to the rescue!)
  - What other data do you need?
  - What is the flow of the incident?



LET’S DO THIS!!

Log analysis

- What is interesting?
- What is not interesting
- How to verify how interesting it really is

So what is this??

Fri Dec 15 18:00:24 2000

Acct-Session-Id = "2193976896017"
User-Name = "e2"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Framed-User
Framed-Protocol = PPP
Framed-IP-Address = 11.10.10.125
Calling-Station-Id = "+15678023561"
NAS-IP-Address = 11.10.10.11
NAS-Port-Id = 8
Acct-Delay-Time = 0
Timestamp = 976896024
Request-Authenticator = Unverified

Fri Dec 15 18:32:09 2000

Acct-Session-Id = "2193976896017"
User-Name = "e2"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Acct-Output-Octets = 5382
Acct-Input-Octets = 7761
Service-Type = Framed-User
Framed-Protocol = PPP
Framed-IP-Address = 11.10.10.125
Acct-Session-Time = 1905
NAS-IP-Address = 11.10.10.11
NAS-Port-Id = 8
Acct-Delay-Time = 0
Timestamp = 976897929
Request-Authenticator = Unverified

YOUR TURN!

For those who are brave….Looking for volunteers to:

- Tell us what you think you found
- Tell us about your approach
- Tell us how you supported your theory

NETWORKS

Network Analysis

- I see this thing, now what?
- What tools do you have available?
- What might you need to understand the full picture?
  - *The infamous network drawing*

What exactly is this?

- Everything that happens in between devices
  - *Trying to follow an endpoint or attacker's path*
- Firewalls, IDS/IPS, WAF, Packet Capture, Netflow
- Yes, more logs!
- And understanding what controls are in place and what their 'view' is

- 1.0 2017-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP FRA6 192.168.1.1 -
- 1.0 2017-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP IAD12 192.168.3.1 192.168.222.0/24
- 1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP FRA6 2001:db8::1234 2001:db8:abcd::/48
- 1.0 2017-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP IAD12 192.168.3.1 192.168.111.0/24
- 1.0 2017-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP JFK5 192.168.1.2 -

7/11/2017 6:14:44 AM 0598 PACKET 0000007029866CF0 UDP Snd (external forwarder IP) 6973 Q [0001 D NOERROR] A (8)services(9)example(3)com(0)

7/11/2017 6:14:44 AM 0598 PACKET 000000702141E170 UDP Snd (Internal Machine 1) 428c R Q [8281 DR SERVFAIL] A (8)services(9)example(3)com(0)

7/11/2017 6:14:44 AM 0598 PACKET 000000702141E170 UDP Snd (internal Machine 2) 86f3 R Q [8281 DR SERVFAIL] A (8)services(9)example(3)com(0)

7/11/2017 6:14:44 AM 0598 PACKET 000000702141E170 UDP Snd (Internal Machine 3) 3250 R Q [8281 DR SERVFAIL] A (8)services(9)example(3)com(0)

Aggregated flows 850332
Top 10 flows ordered by bytes:
Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Flags Tos Packets Bytes pps bps Bpp Flows
2005-08-30 06:50:11.218 700.352 TCP 126.52.54.27:47303 -> 42.90.25.218:435 ..... 0 1.4 M 2.0 G 2023 5.6 M 1498 1
2005-08-30 06:47:06.504 904.128 TCP 198.100.18.123:54945 -> 126.52.57.13:119 ..... 0 567732 795.1 M 627 2.5 M 1468 1
2005-08-30 06:47:06.310 904.384 TCP 126.52.57.13:45633 -> 91.127.227.206:119 ..... 0 321148 456.5 M 355 4.0 M 1490 1
2005-08-30 06:47:14.315 904.448 TCP 126.52.57.13:45598 -> 91.127.227.206:119 ..... 0 320710 455.9 M 354 4.0 M 1490 1
2005-08-30 06:47:14.316 904.448 TCP 126.52.57.13:45629 -> 91.127.227.206:119 ..... 0 317764 451.5 M 351 4.0 M 1489 1
2005-08-30 06:47:14.315 904.448 TCP 126.52.57.13:45634 -> 91.127.227.206:119 ..... 0 317611 451.2 M 351 4.0 M 1489 1
2005-08-30 06:47:06.313 904.384 TCP 126.52.57.13:45675 -> 91.127.227.206:119 ..... 0 317319 451.0 M 350 4.0 M 1490 1
2005-08-30 06:47:06.313 904.384 TCP 126.52.57.13:45619 -> 91.127.227.206:119 ..... 0 314199 446.5 M 347 3.9 M 1490 1
2005-08-30 06:47:06.321 790.976 TCP 126.52.54.35:59898 -> 132.94.115.59:2466 ..... 0 254717 362.4 M 322 3.7 M 1491 1
2005-08-30 06:47:14.316 904.384 TCP 126.52.54.35:59773 -> 55.107.224.187:11709 ..... 0 272710 348.5 M 301 3.1 M 1340 1

1070236831,0,3175466240,198.32.11.5,1,1500,3175436989,3175436989,0,0,130.74.208.0,169.232.72.0,198.32.11.4,33,35,1373,4753,6,0,16,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,3,1884,3175408565,3175433201,0,0,130.74.208.0,169.232.72.0,198.32.11.4,33,35,1373,4753,6,0,24,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,1,628,3175448463,3175448463,0,0,130.74.208.0,169.232.112.0,198.32.11.4,33,35,1373,3855,6,0,24,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,1,1500,3175442525,3175442525,0,0,130.74.208.0,169.232.112.0,198.32.11.4,33,35,1373,3864,6,0,16,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,1,1500,3175451974,3175451974,0,0,130.74.208.0,169.232.112.0,198.32.11.4,33,35,1373,3831,6,0,16,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,6,3768,3175398562,3175449061,0,0,130.74.208.0,169.232.112.0,198.32.11.4,33,35,1373,3831,6,0,24,16,16,25656,52
1070236836,0,3175471250,198.32.11.5,1,92,3175454577,3175454577,0,0,130.18.248.0,202.28.48.0,198.32.11.4,18,35,0,0,1,0,0,16,24,10546,4621
1070236836,0,3175471250,198.32.11.5,1,92,3175414202,3175414202,0,0,130.18.248.0,165.132.224.0,198.32.11.4,18,35,0,0,1,0,0,

Sep 7 06:25:17 PIXName %PIX-7-710005: UDP request discarded from 0.0.0.0/68 to outside:255.255.255.255/67
Sep 7 06:25:23 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:23 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:23 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:24 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:24 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:24 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:25 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:25 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:25 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:28 PIXName %PIX-7-609001: Built local-host db:10.0.0.1
Sep 7 06:25:28 PIXName %PIX-6-302013: Built inbound TCP connection 141968 for db:10.0.0.1/60749 (10.0.0.1/60749) to NP Identity Ifc: 10.0.0.2/22 (10.0.0.2/22)
Sep 7 06:25:28 PIXName %PIX-7-710002: TCP access permitted from 10.0.0.1/60749 to db:10.0.0.2/ssh
Sep 7 06:26:20 PIXName %PIX-5-304001: 203.87.123.139 Accessed URL 10.0.0.10:/Home/index.cfm
Sep 7 06:26:20 PIXName %PIX-5-304001: 203.87.123.139 Accessed URL 10.0.0.10:/aboutus/volunteers.cfm
Sep 7 06:26:49 PIXName %PIX-4-106023: Deny udp src outside:204.16.208.49/58939 dst dmz:10.0.0.158/1026 by access-group "acl_outside" [0x0, 0x0]
Sep 7 06:26:49 PIXName %PIX-4-106023: Deny udp src outside: 204.16.208.49/58940 dst dmz:10.0.0.158/1027 by access-group "acl_outside" [0x0, 0x0]
Sep 7 06:31:26 PIXName %PIX-7-711002: Task ran for 330 msec, Process= ssh_init, PC = fddd93, Traceback = 0x00FF1E6B 0x00FE1890 0x00FE0D3C 0x00FD326A 0x00FC0BFC 0x00FDBB8E 0x00FDBA4D 0x00FCD846 0x00FBF09C 0x001C76AE 0x00A01512 0x009CF6B5 0x00BDB9CE 0x00BDA502
Sep 7 06:31:32 PIXName %PIX-6-315011: SSH session from 10.0.0.254 on interface db for user "" disconnected by SSH server, reason: "TCP connection closed" (0x03)

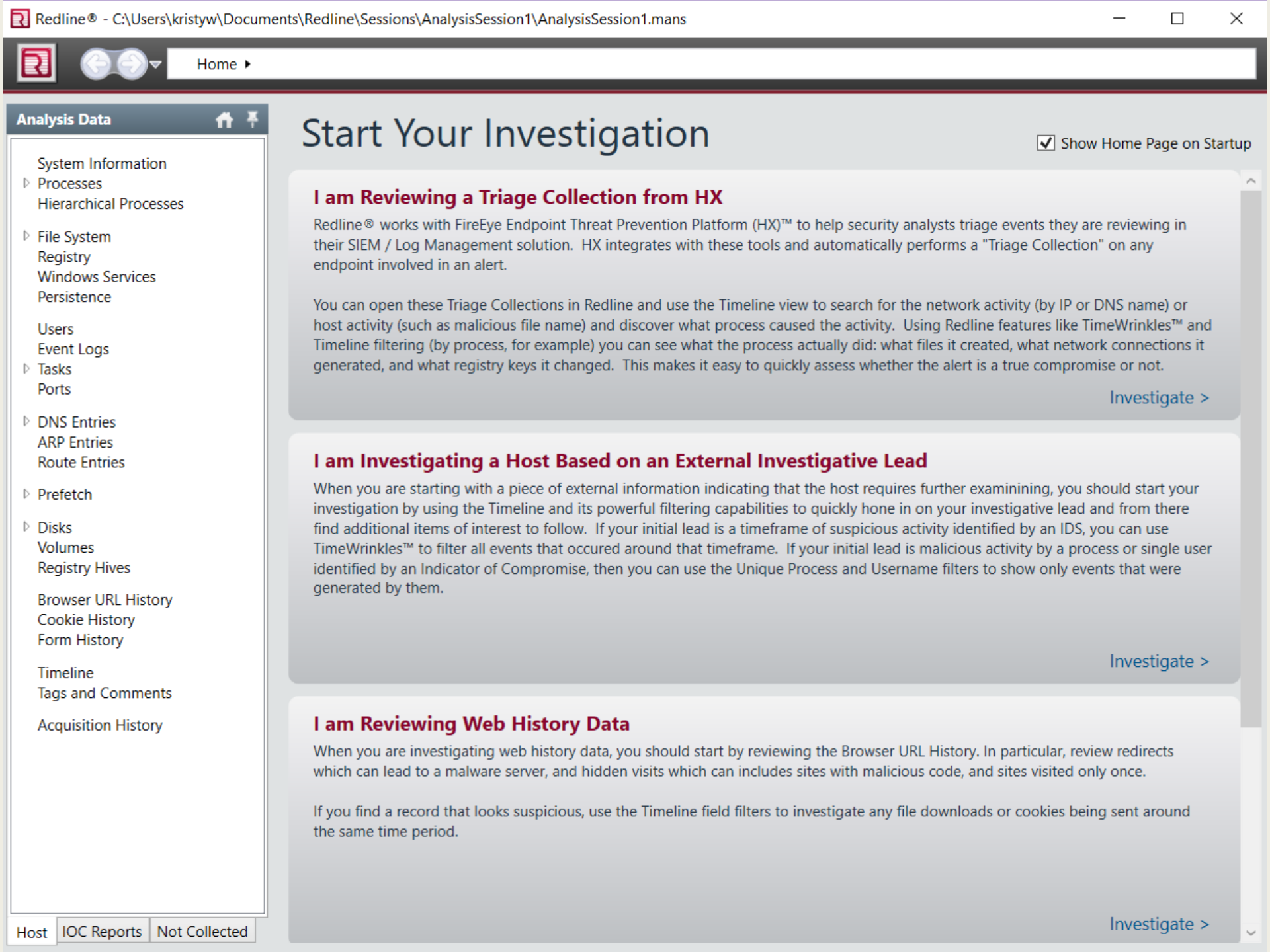
YOUR TURN!

ENDPOINTS

Endpoint Forensics

- I don’t have time for full forensics, what can I do in a brief time period?
- What does the information gathered mean?
- Set your scope first
- What behavior are you seeing?
  - *Indicators?*
- If you have a little time:
  - *Sysmon*
  - *Redline*
- If not grab these:
  - *Rift*


Redline®
Redline®
Collect Data
Create a Standard Collector >
Create a Comprehensive Collector >
Create an IOC Search Collector >
Analyze Data
From a Saved Memory File >
Open Previous Analysis >


Redline® - C:\Users\kristyw\Documents\Redline\Sessions\AnalysisSession1\AnalysisSession1.mans
Home
Analysis Data
System Information
Processes
Hierarchical Processes
File System
Registry
Windows Services
Persistence
Users
Event Logs
Tasks
Ports
DNS Entries
ARP Entries
Route Entries
Prefetch
Disks
Volumes
Registry Hives
Browser URL History
Cookie History
Form History
Timeline
Tags and Comments
Acquisition History
Host
IOC Reports
Not Collected
Start Your Investigation
Show Home Page on Startup
I am Reviewing a Triage Collection from HX
Redline® works with FireEye Endpoint Threat Prevention Platform (HX)™ to help security analysts triage events they are reviewing in their SIEM / Log Management solution. HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.
You can open these Triage Collections in Redline and use the Timeline view to search for the network activity (by IP or DNS name) or host activity (such as malicious file name) and discover what process caused the activity. Using Redline features like TimeWrinkles™ and Timeline filtering (by process, for example) you can see what the process actually did: what files it created, what network connections it generated, and what registry keys it changed. This makes it easy to quickly assess whether the alert is a true compromise or not.
Investigate >
I am Investigating a Host Based on an External Investigative Lead
When you are starting with a piece of external information indicating that the host requires further examinining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWrinkles™ to filter all events that occured around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.
Investigate >
I am Reviewing Web History Data
When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can includes sites with malicious code, and sites visited only once.
If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.
Investigate >

Timeline Configuration

Show Only Events Associated with Selected User:

- (unknown)
- BUILTIN\Administrators
- DESKTOP-QPHCRMF\Administrator
- DESKTOP-QPHCRMF\DefaultAccount
- DESKTOP-QPHCRMF\defaultuser0
- DESKTOP-QPHCRMF\Guest
- DESKTOP-QPHCRMF\kristyw
- DESKTOP-QPHCRMF\WDAGUtilityAccount
- Everyone
- Font Driver Host\UMFD-0
- Font Driver Host\UMFD-1
- Font Driver Host\UMFD-2
- Font Driver Host\UMFD-3
- kristyw
- NT AUTHORITY\LOCAL SERVICE
- NT AUTHORITY\NETWORK SERVICE
- NT AUTHORITY\SYSTEM
- NT SERVICE\AppReadiness
- NT SERVICE\Audiosrv
- NT SERVICE\BthAvctpSvc
- NT SERVICE\bthserv
- NT SERVICE\DiagTrack
- NT SERVICE\MapsBroker
- NT SERVICE\TrustedInstaller
- NULL SID
- S-1-5-96-0-4
- Window Manager\DWM-3
- WORKGROUP\DESKTOP-QPHCRMF$

TimeCrunches™ 0 | Users | Processes

Fields | TimeWrinkles™ 0

Enter string to find here... | Reg Ex | In All Fields | Clear Column Filters | Prev | Next

Timestamp	Field	Summary
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** Adobe Acrobat Update... **Status:** SCHED_S_TASK... **MD5:** **Creator:** Adobe Systems Incorpor...
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** GoogleUpdateTaskMach... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** GoogleUpdateTaskMach... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** McAfee Remediation (Pr... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** AppleSoftwareUpdate **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** McAfee Auto Maintenan... **Status:** SCHED_S_TASK... **MD5:** **Creator:** McAfee
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** OfficeBackgroundTaskH... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** OfficeBackgroundTaskH... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** PolicyConverter **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** SmartScreenSpecific **Status:** SCHED_S_TASK... **MD5:** **Creator:** $(@%systemroot%\syst...
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** VerifiedPublisherCertSto... **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** Microsoft Compatibility... **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** ProgramDataUpdater **Status:** SCHED_S_TASK... **MD5:** **Creator:** $(@%SystemRoot%\syst...
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** StartupAppTask **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** appuriverifierdaily **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** appuriverifierinstall **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** CleanupTemporaryState **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** DsSvcCleanup **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** Pre-staged app cleanup **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** Proxy **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** BitLocker MDM policy R... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** UninstallDeviceTask **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** BgTaskRegistrationMaint... **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** AikCertEnrollTask **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation

3,507,129 Items

This is frac/rift for Windows info gathering

```
#Get the system hive
system32\/config\/SYSTEM$
#Get the default hive
system32\/config\/DEFAULT$
#Get the sam hive
system32\/config\/SAM$
#Get the security hive
system32\/config\/SECURITY$
#Get the software hive
system32\/config\/SOFTWARE$
#Get the contents of the Tasks directory for Windows 2000, XP, @003
\/Windows\/Tasks\/
#Get the Contents of the Tasks directory for Windows 7+
\/Windows\/System32\/Tasks\/
#Get a copy of the task scheduler logs
Microsoft-Windows-TaskScheduler*\.evtx$
#Gathers all users ntuser.dat files
ntuser.dat$
#Win7 shellbag data
#\Users\[user]\AppData\Local\Microsoft\Windows\UsrClass.dat
usrclass.dat$
#Win8 Application Experience and Compatibility  C:\Windows\AppCompat\Programs\Amcache.hve
amcache.hve$
#journeyintoir.blogspot.com/2014/04/triaging-with-recentfilecachebcf-file.html
RecentFilecache.bcf$
#Get the contents of the Prefetch directory
\/Windows\/prefetch\/
```

Second half.....

```
#Event Logs for Vista+
system32\/winevt\/logs\/
#Event Logs for WinXP
\/appevent.evt$
\/sysevent.evt$
\/secevent.evt$
#WinXP Recycle Bin
\/info2$
#Vista+ Reycle Bin; Gets Index files
\/\$Recycle.bin\/S-.*\/\$I.*
#Gets everything in the Recycle.bin folder
#\/\$Recycle.bin\/
#Page file
#\/pagefile.sys$
#Hibernation file
#\/hiberfil.sys$
#Microsoft Malicious Software Removal (MSRT)
\/Windows\/Debug\/mrt.log$
\/Windows\/Debug\/mrteng.log$
#Windows Defender Logs
\/ProgramData\/Microsoft\/Windows Defender\/Support\/.*log$
#Powershell Info
\/Windows\/System32\/wbem\/Repository\/OBJECTS.DATA$
\/Windows\/System32\/wbem\/Repository\/FS\/OBJECTS.DATA$
#Syscache.hve  https://github.com/libyal/winreg-kb/blob/master/documentation/SysCache.asciidoc
\/System Volume Information\/Syscache.hve
```

This is frac/rift for *nix info gathering

```
#Shell Info
\.bash_history
\.bashrc
\/\.csh
\/\.zsh
\/\.sh_history
\/\.profile
#SSH
\.ssh
#etc dir
^\/etc\/
#Cron
^\/var\/spool\/at
^\/var\/spool\/cron
^\/var\/spool\/anacron
#logs
^\/var\/log\/
^\/var\/adm\/
```

Sample Windows event log

- System
 - Provider
  [Name] Microsoft-Windows-Sysmon
  [Guid] {5770385F-C22A-43E0-BF4C-06F5698FFBD9}

  EventID 1
  Version 5
  Level 4
  Task 1

  Opcode 0

  Keywords 0x8000000000000000

 - TimeCreated

  [SystemTime] 2019-06-21T17:49:33.036975300Z

  EventRecordID 2380270

  Correlation

 - Execution
  [ProcessID] 4212
  [ThreadID] 7464
  Channel Microsoft-Windows-Sysmon/Operational
  Computer DESKTOP-QPHCRMF
  - Security
  [UserID] S-1-5-18

Second part of the event log

- EventData

  RuleName
  UtcTime 2019-06-21 17:49:33.034
  ProcessGuid {404F8C83-18AD-5D0D-0000-0010951EC630}
  ProcessId 30664
  Image C:\Program Files\Splunk\bin\splunk-optimize.exe
  FileVersion 7.3.0
  Description splunk-optimize
  Product splunk Application
  Company Splunk Inc.
  CommandLine splunk-optimize -d "C:\Program Files\Splunk\var\lib\splunk_internaldb\db\hot_v1_4" -x 40290210304 --log-to--splunkd-log --write-level 1
  CurrentDirectory C:\WINDOWS\system32\
  User NT AUTHORITY\SYSTEM
  LogonGuid {404F8C83-5448-5D05-0000-0020E7030000}
  LogonId 0x3e7
  TerminalSessionId 0
  IntegrityLevel System
  Hashes SHA1=9EACAE222E8B87066B98061A57E3E9986D8C7317
  ParentProcessGuid {404F8C83-5459-5D05-0000-0010FD270400}
  ParentProcessId 4596
  ParentImage C:\Program Files\Splunk\bin\splunkd.exe
  ParentCommandLine "C:\Program Files\Splunk\bin\splunkd.exe" service

GUESS WHAT?

Yep, it’s your turn

MALWARES

Malware Analysis

- Why malware analysis for the incident responder?
  - *What is it doing?*
  - *Has data left my network?*
- What kind of environment
- Triage and Analysis
  - *Quick and dirty ways to peek under the hood*
- Tools
- DO NOT OPEN MALWARE WITHOUT PROPER ENVIRONMENT!!!

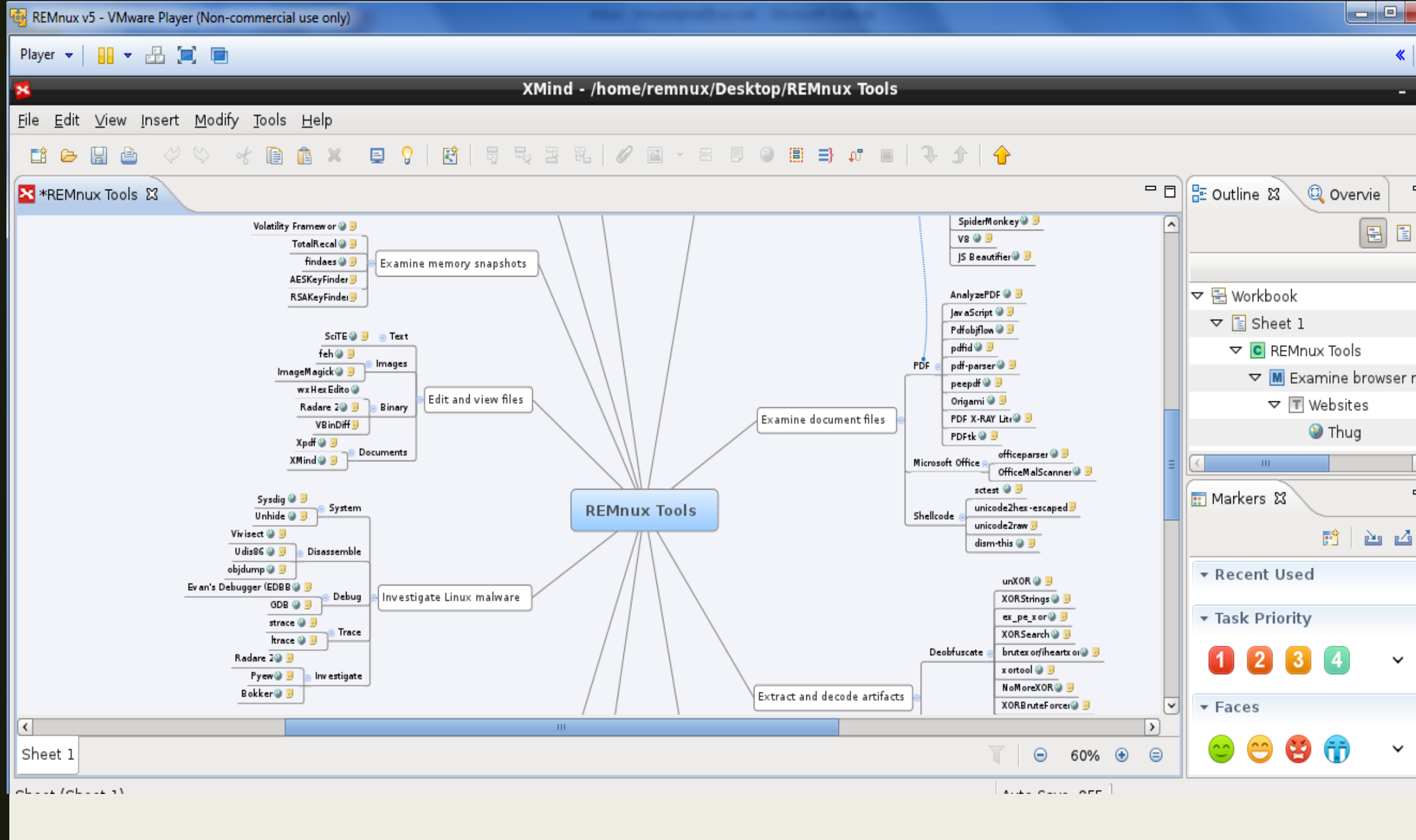


Why do you want to know this?

- You want to know what the heck you are dealing with
- And make a quick determination if data was breached

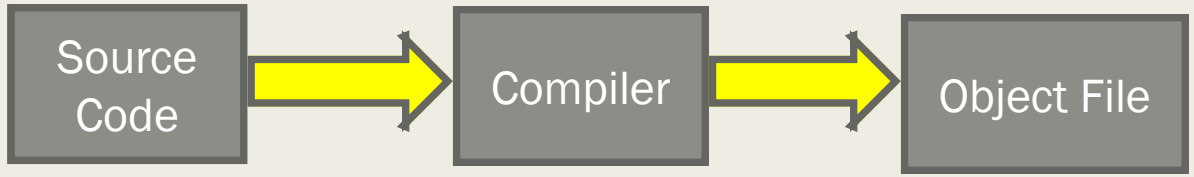
What Kind of Environment?

- Something isolated off of your network
- You can do a quick inspection (if you have to) with a Notepad
  - *But anything further should be isolated!*
- Try REMnux
- Or SIFT
- Cygwin helps in a pinch as well

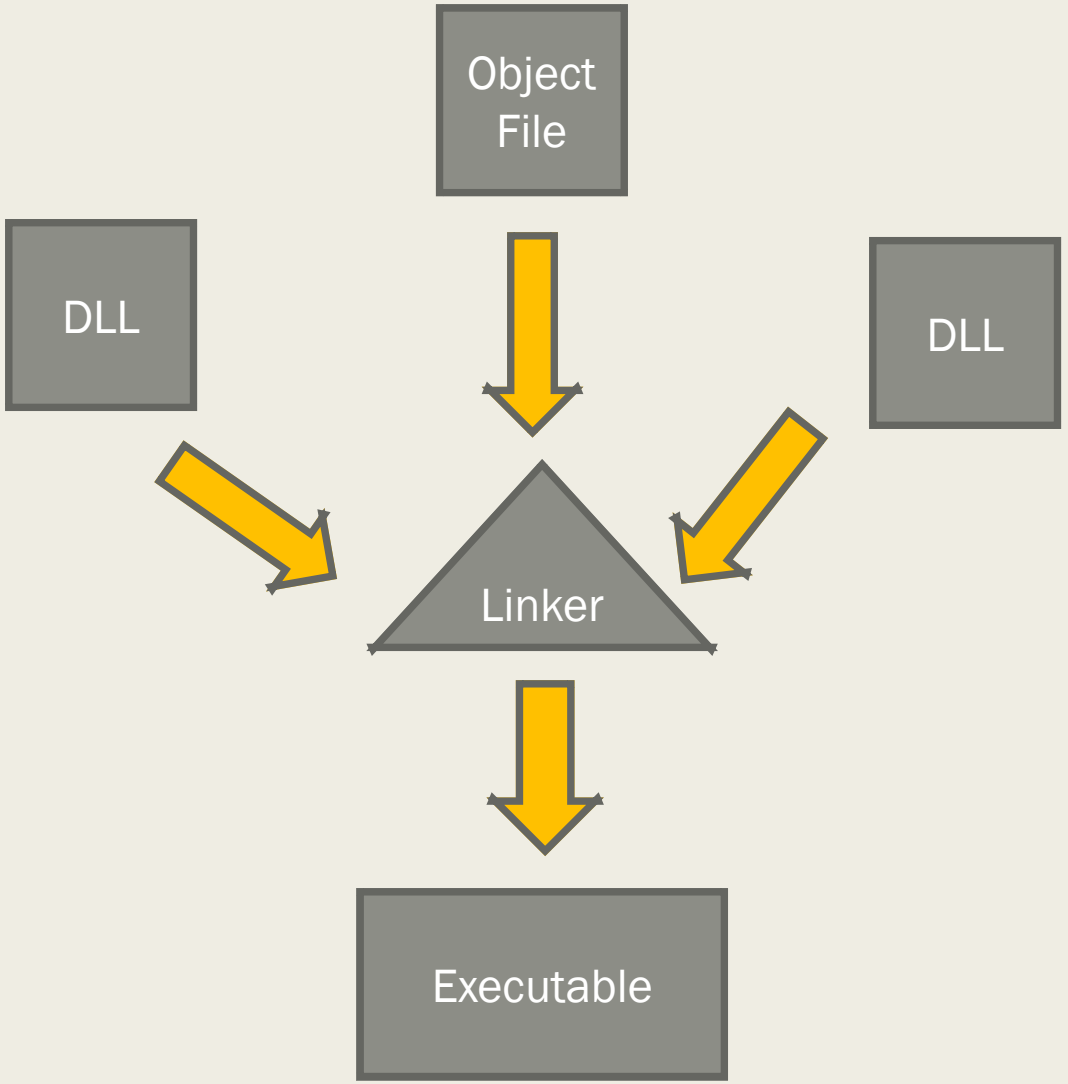

REMnux v5 - VMware Player (Non-commercial use only)
Player
XMind - /home/remnux/Desktop/REMnux Tools
File Edit View Insert Modify Tools Help
*REMnux Tools
REMnux Tools
Examine memory snapshots
Volatility Framework
TotalRecal
findaes
AESKeyFinder
RSAKeyFinder
Edit and view files
Text
SciTE
Images
feh
ImageMagick
wxHexEditor
Binary
Radare 2
VBinDiff
Documents
Xpdf
XMind
Investigate Linux malware
System
Sysdig
Unhide
Disassemble
Vivisect
Udis86
objdump
Debug
Evan's Debugger (EDBB)
GDB
Trace
strace
ltrace
Investigate
Radare 2
Pyew
Bokker
Examine document files
PDF
SpiderMonkey
V8
JS Beautifier
AnalyzePDF
JavaScript
Pdfobjflow
pdfid
pdf-parser
peepdf
Origami
PDF X-RAY Lite
PDFtk
Microsoft Office
officeparser
OfficeMalScanner
Shellcode
sctest
unicode2hex-escaped
unicode2raw
dism-this
Extract and decode artifacts
Deobfuscate
unXOR
XORStrings
ex_pe_xor
XORSearch
brutexor/iheartxor
xortool
NoMoreXOR
XORBruteForcer
Outline
Overvie
Workbook
Sheet 1
REMnux Tools
Examine browser
Websites
Thug
Markers
Recent Used
Task Priority
Faces
Sheet 1
60%

Reverse Engineering

- Working our way backwards
  - *Huh?*
  - *OK, let's start from the beginning*
- These tools make programs:
  - *Compilers- A program that translates the programming statements written in a high level language into another form.*
  - *Assemblers- a program that takes basic computer instructions and converts them into a pattern of bits that the computer's processor can use to perform its basic operations.*
  - *Linkers- Creates an executable file by linking the required libraries and code to an object file*
  - *Object file = Machine code*



Linker

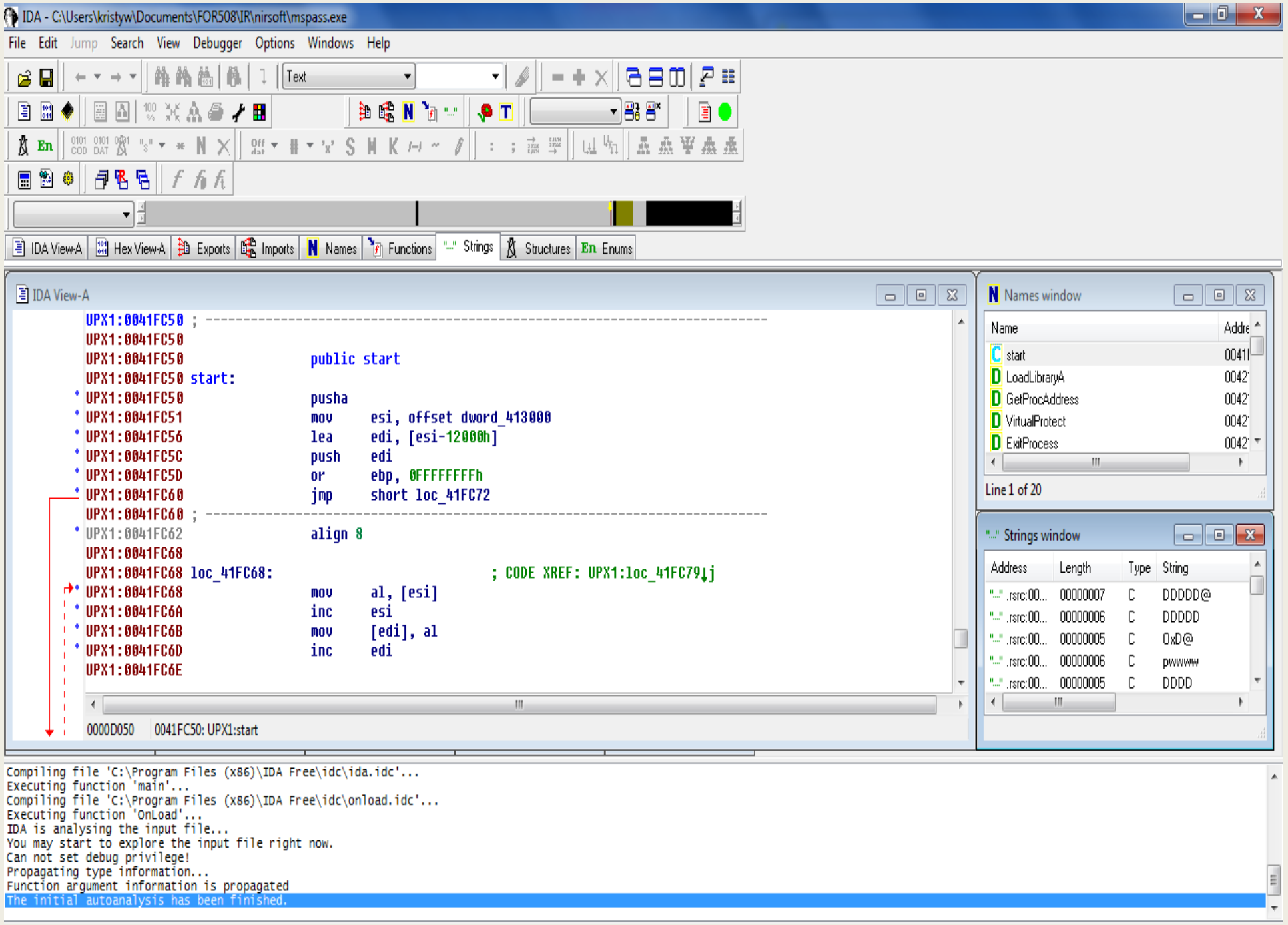


Binary Analysis

- Typically two ways to analyze:
  - *Static: Reading through program code*
  - *Dynamic: Allowing the malware to execute in a controlled environment while recording every observable aspect of its behavior using any number of system utilities.*
- Static executables is compiled with all of the necessary libraries and code it needs to execute
- Dynamic depend upon shared libraries to run

Debugger

- Typically used for one of two tasks:
  - *Examining memory images (e.g. core dumps) associated with crashed processes*
  - *Executing processes in a controlled manner*
- How do I execute a process in a controlled manner?
  - *Attach to a running process*
  - *Try opening the running process in IDA before attempting to attach to the running process*
  - *Can also launch the process under debugger control*
    - This is almost the best because you can watch every action it takes, including startup
- Useful for obfuscated code analysis


IDA - C:\Users\kristyw\Documents\FOR508\IR\nirsoft\mspass.exe
File Edit Jump Search View Debugger Options Windows Help
IDA View-A Hex View-A Exports Imports Names Functions Strings Structures Enums
IDA View-A
UPX1:0041FC50 ; ---------- public start
UPX1:0041FC50 start:
UPX1:0041FC50 pusha
UPX1:0041FC51 mov esi, offset dword_413000
UPX1:0041FC56 lea edi, [esi-12000h]
UPX1:0041FC5C push edi
UPX1:0041FC5D or ebp, 0FFFFFFFFh
UPX1:0041FC60 jmp short loc_41FC72
UPX1:0041FC60 ; ----------
UPX1:0041FC62 align 8
UPX1:0041FC68 loc_41FC68: ; CODE XREF: UPX1:loc_41FC79↓j
UPX1:0041FC68 mov al, [esi]
UPX1:0041FC6A inc esi
UPX1:0041FC6B mov [edi], al
UPX1:0041FC6D inc edi
UPX1:0041FC6E
0000D050 0041FC50: UPX1:start
Names window
Name Addre
start 0041
LoadLibraryA 0042
GetProcAddress 0042
VirtualProtect 0042
ExitProcess 0042
Line 1 of 20
Strings window
Address Length Type String
.rsrc:00... 00000007 C DDDDD@
.rsrc:00... 00000006 C DDDDD
.rsrc:00... 00000005 C 0xD@
.rsrc:00... 00000006 C pwwww
.rsrc:00... 00000005 C DDDD
Compiling file 'C:\Program Files (x86)\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Can not set debug privilege!
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.

Disassembler

- Undoes the assembly process
  - *Bingo!*
  - *Versus a decompiler that produces output in a high level language*
  - *So this is easy, right?*

Why decompiling isn’t easy

- Compilation process is lossy
  - *No variable or function names at the machine language level*
- Compilation is a many-to-many operation
  - *Translation can happen in many different ways*
- Decompilers are very language and library dependent
  - *If you use one type of compiler to compile and another to decompile, results may vary*
- A nearly perfect disassembly capability is needed in order to accurately decompile a binary
  - *Errors or omissions in the disassembly phase will propagate to decompiled code*

Finding your Target: Windows

- What is a suspicious file?
  - *Of unknown origin*
  - *Unfamiliar*
  - *Seems familiar, but why is it in this location?*
  - *Similarly named to a known or familiar file, maybe misspelled or otherwise slightly varied*
  - *Determined to conduct anomalous activity*
  - *In other words: not just one way to find these things*

Things you'll want to define

- What type of file is it?
- What is it's intended purpose?
- What is it's functionality and capability?
- What does the file suggest about the sophistication level of the attacker?
- What affect does this file have on the system?
- What is the extent of the infection or compromise (both system and network)?
- What remediation steps are necessary because the file exists on the system?

The process in order

- Obtain suspicious file
- Document the details pertaining to the system
- Hash the file
- Compare the file against known samples
- Classify the type of file
- Scan with tools that can identify known signatures
- Examine the file with analysis tools to look for malicious properties

Continuing the process

- Extract and Analyze any ASCII or Unicode strings, then metadata, then symbolic information
- Reveal any code obfuscation or armoring techniques like packers, wrappers, or encryption
- Correlate. Is the file dynamically or statically linked? Are there any dependencies?
- Research. Time to go online and see if anyone else has run into this code.

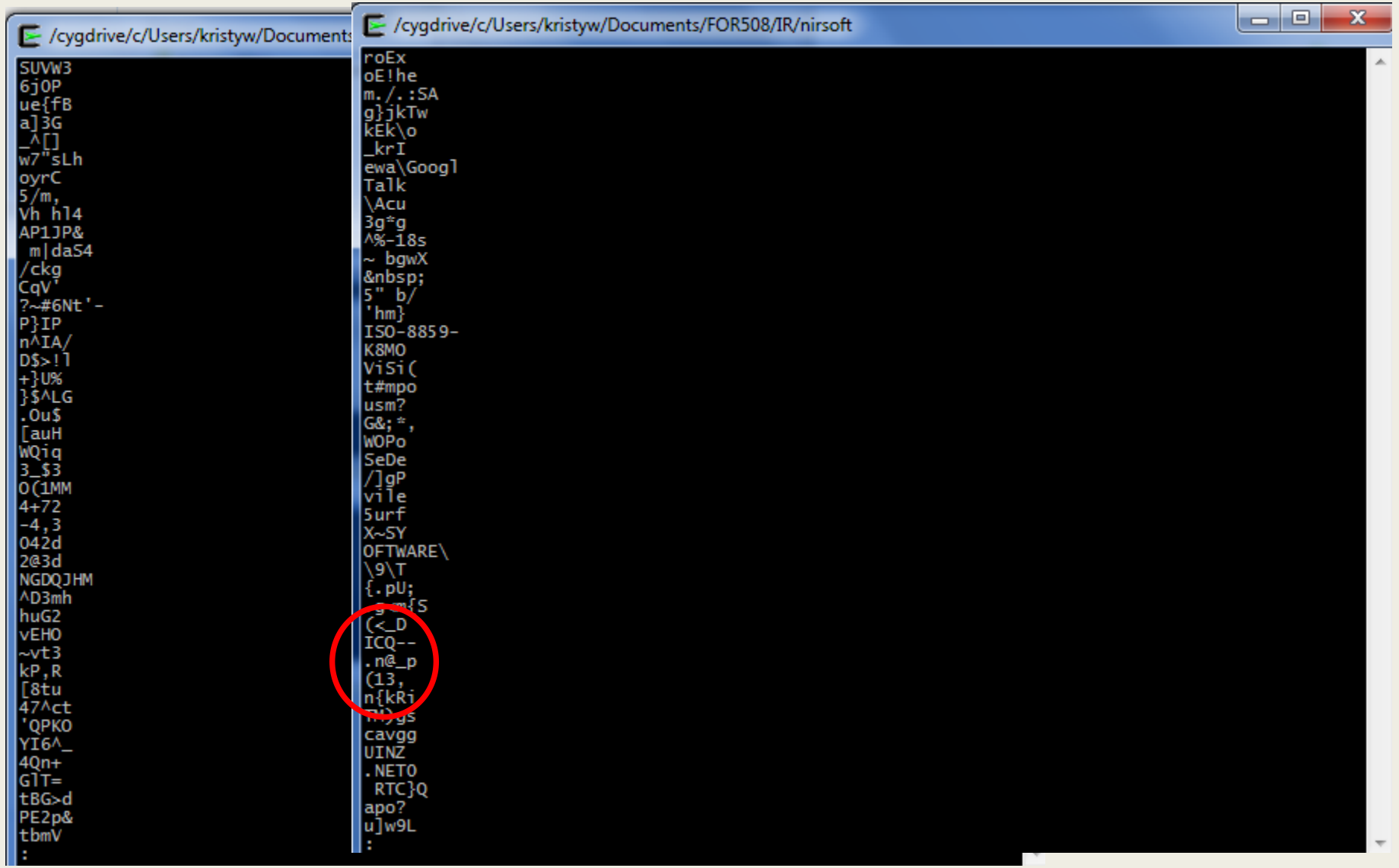
File signature ID and Classification

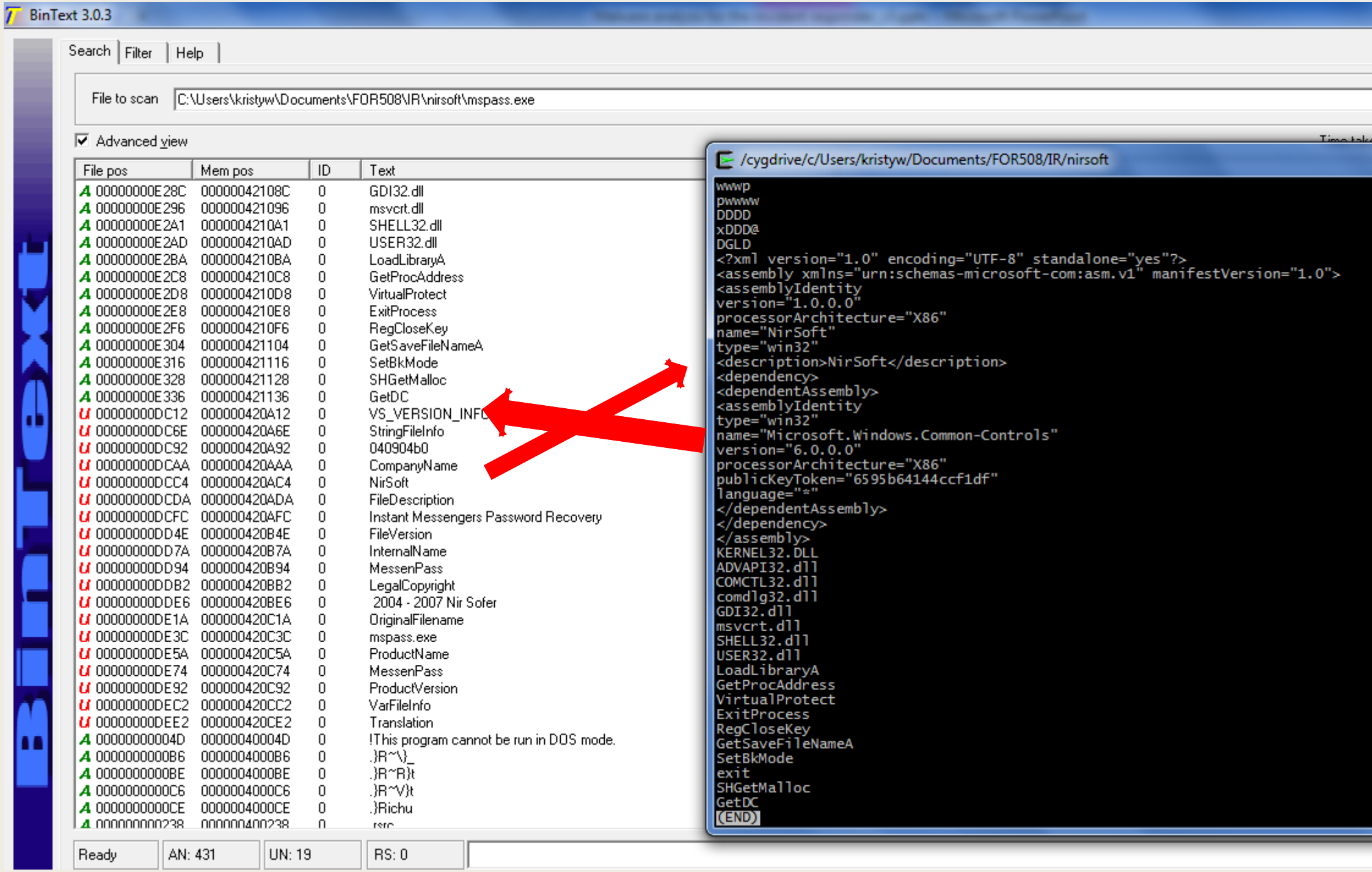
- We now want to look in the file to see the true signature
  - *A signature is a unique number of bytes written to a file's header*
  - *A hex viewer is your friend*
  - *Try MiniDumper (http://www.softpedia.com/progDownload/Windows-Portable-Applications-Portable-MiniDumper-Download-105882.html)*
- Then, identify the native operating system and architecture the code runs on (or classifying)

File Classification tools

- File (Linux or Cygwin)
- TrID (http://mark0.net/soft-trid-e.html)
- TrIDNet (gui version of TrID)
- DROID (not the phone) (http://digital-preservation.github.io/droid/)
- Exeinfo (http://www.nirsoft.net/utils/exeinfo.html)
- I encourage you to try more than one, then compare results

```
kristyw@WilburJunior /cygdrive/c/Users/kristyw/Documents/FOR508/IR/nirsoft
$ file mspass.exe
mspass.exe: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
```




BinText 3.0.3
Search
Filter
Help
File to scan
C:\Users\kristyw\Documents\FOR508\IR\nirsoft\mspass.exe
Advanced view
File pos
Mem pos
ID
Text
A 00000000E28C 000000042108C 0 GDI32.dll
A 00000000E296 000000421096 0 msvcrt.dll
A 00000000E2A1 0000004210A1 0 SHELL32.dll
A 00000000E2AD 0000004210AD 0 USER32.dll
A 00000000E2BA 0000004210BA 0 LoadLibraryA
A 00000000E2C8 0000004210C8 0 GetProcAddress
A 00000000E2D8 0000004210D8 0 VirtualProtect
A 00000000E2E8 0000004210E8 0 ExitProcess
A 00000000E2F6 0000004210F6 0 RegCloseKey
A 00000000E304 000000421104 0 GetSaveFileNameA
A 00000000E316 000000421116 0 SetBkMode
A 00000000E328 000000421128 0 SHGetMalloc
A 00000000E336 000000421136 0 GetDC
U 00000000DC12 000000420A12 0 VS_VERSION_INFO
U 00000000DC6E 000000420A6E 0 StringFileInfo
U 00000000DC92 000000420A92 0 040904b0
U 00000000DCAA 000000420AAA 0 CompanyName
U 00000000DCC4 000000420AC4 0 NirSoft
U 00000000DCDA 000000420ADA 0 FileDescription
U 00000000DCFC 000000420AFC 0 Instant Messengers Password Recovery
U 00000000DD4E 000000420B4E 0 FileVersion
U 00000000DD7A 000000420B7A 0 InternalName
U 00000000DD94 000000420B94 0 MessenPass
U 00000000DDB2 000000420BB2 0 LegalCopyright
U 00000000DDE6 000000420BE6 0 2004 - 2007 Nir Sofer
U 00000000DE1A 000000420C1A 0 OriginalFilename
U 00000000DE3C 000000420C3C 0 mspass.exe
U 00000000DE5A 000000420C5A 0 ProductName
U 00000000DE74 000000420C74 0 MessenPass
U 00000000DE92 000000420C92 0 ProductVersion
U 00000000DEC2 000000420CC2 0 VarFileInfo
U 00000000DEE2 000000420CE2 0 Translation
A 00000000004D 00000040004D 0 !This program cannot be run in DOS mode.
A 0000000000B6 0000004000B6 0 .}R~\}_
A 0000000000BE 0000004000BE 0 .}R~R}t
A 0000000000C6 0000004000C6 0 .}R~V}t
A 0000000000CE 0000004000CE 0 .}Richu
Ready
AN: 431
UN: 19
RS: 0
/cygdrive/c/Users/kristyw/Documents/FOR508/IR/nirsoft
wwwp
pwwww
DDDD
xDDD@
DGLD
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
version="1.0.0.0"
processorArchitecture="X86"
name="NirSoft"
type="win32"
<description>NirSoft</description>
<dependency>
<dependentAssembly>
<assemblyIdentity
type="win32"
name="Microsoft.Windows.Common-Controls"
version="6.0.0.0"
processorArchitecture="X86"
publicKeyToken="6595b64144ccf1df"
language="*"
</dependentAssembly>
</dependency>
</assembly>
KERNEL32.DLL
ADVAPI32.dll
COMCTL32.dll
comdlg32.dll
GDI32.dll
msvcrt.dll
SHELL32.dll
USER32.dll
LoadLibraryA
GetProcAddress
VirtualProtect
ExitProcess
RegCloseKey
GetSaveFileNameA
SetBkMode
exit
SHGetMalloc
GetDC
(END)

Anti-virus scanning

- Freeware AV is a good start
  - *ClamWin*
  - *AVG*
  - *Malwarebytes*
- VirusTotal is a great online tool
- VirScan.org (??)
- Hybrid Analysis (https://www.hybrid-analysis.com/)
- https://zeltser.com/automated-malware-analysis/

Late Rent Notice c58.doc.vbs

This report is generated from a file or URL submitted to this webservice on June 21st 2019 00:29:25 (CEST)
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.30 © Hybrid Analysis - learn more

Incident Response

Risk Assessment

Persistence	Modifies auto-execute functionality by setting/creating a value in the registry
	Schedules a task to be executed at a specific time and date
	Spawns a lot of processes
Fingerprint	Queries process information
	Reads the cryptographic machine GUID
Evasive	Checks a device property (often used to detect VM artifacts)
	Found a reference to a WMI query string known to be used for VM detection
Network Behavior	Contacts 1 domain and 1 host. View all details

Additional Context

Related Sandbox Artifacts

Associated SHA256s	0b34551d355a734409a405cdcbfc9c463b45c85d52cfaaab52b6278460514645

Malicious Indicators 11

General

The analysis extracted a file that was identified as malicious

details 14/71 Antivirus vendors marked dropped file "ishpc.exe" as malicious (classified as "Trojan.Kryptik" with 19% detection rate)
source Extracted File
relevance 10/10

The analysis spawned a process that was identified as malicious

Installation/Persistance

Allocates virtual memory in a remote process

Writes data to a remote process

Unusual Characteristics

Contains native function calls

Spawns a lot of processes

Suspicious Indicators 21

Anti-Reverse Engineering

- Checks a device property (often used to detect VM artifacts)

Environment Awareness

- Contains ability to query CPU information
- Found a reference to a WMI query string known to be used for VM detection
- Reads the active computer name
- Reads the cryptographic machine GUID

General

- Contains ability to find and load resources of a specific module

Installation/Persistance

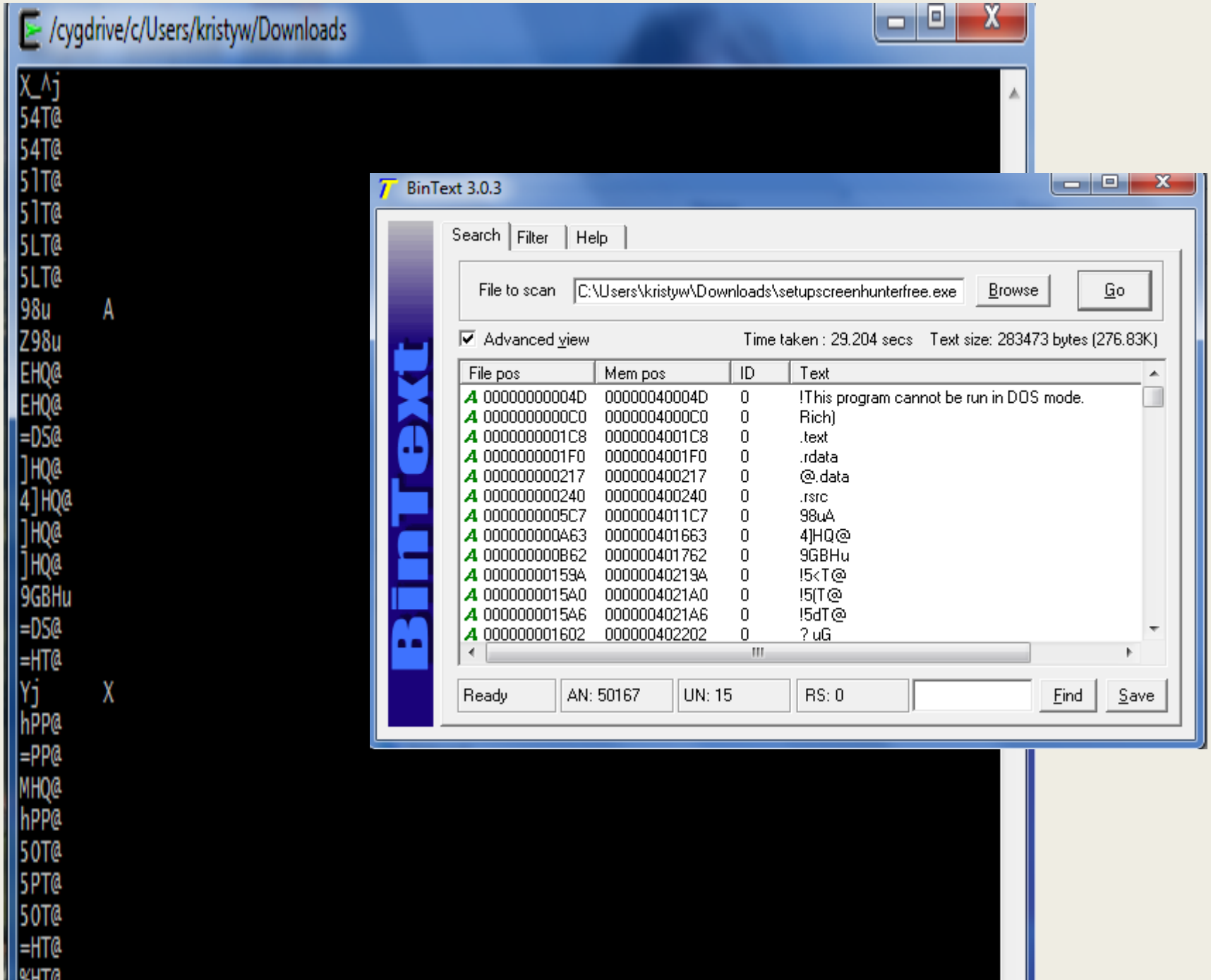
- Drops executable files
- Modifies auto-execute functionality by setting/creating a value in the registry

Network Related

- Sends traffic on typical HTTP outbound port, but without HTTP header

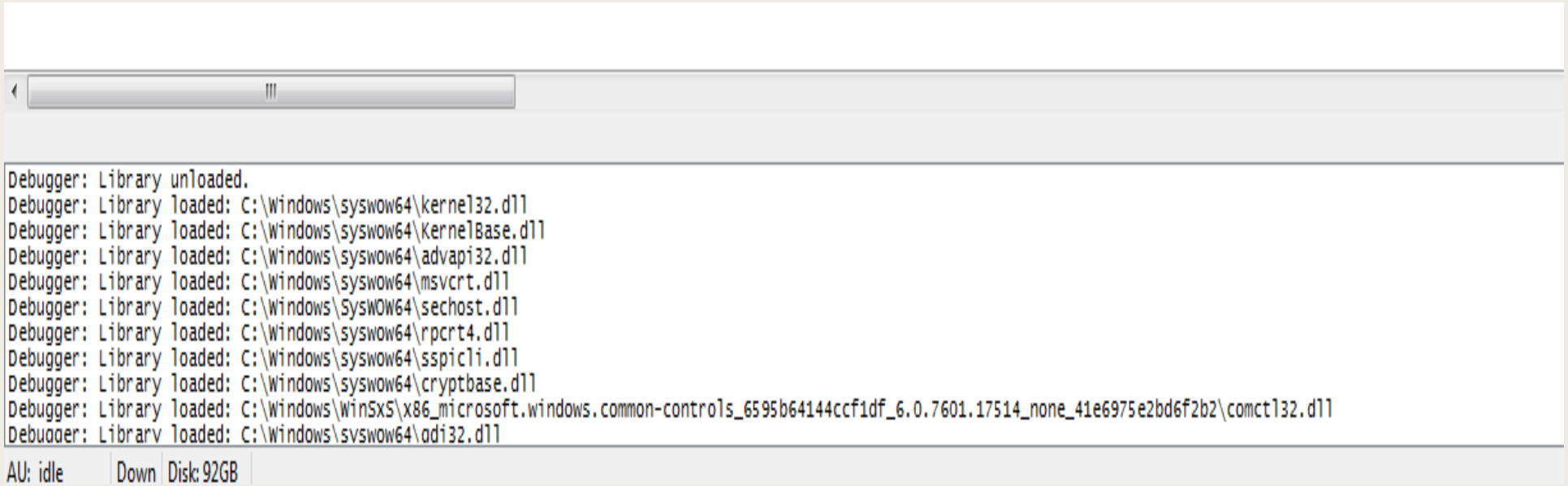
Looking for the good stuff

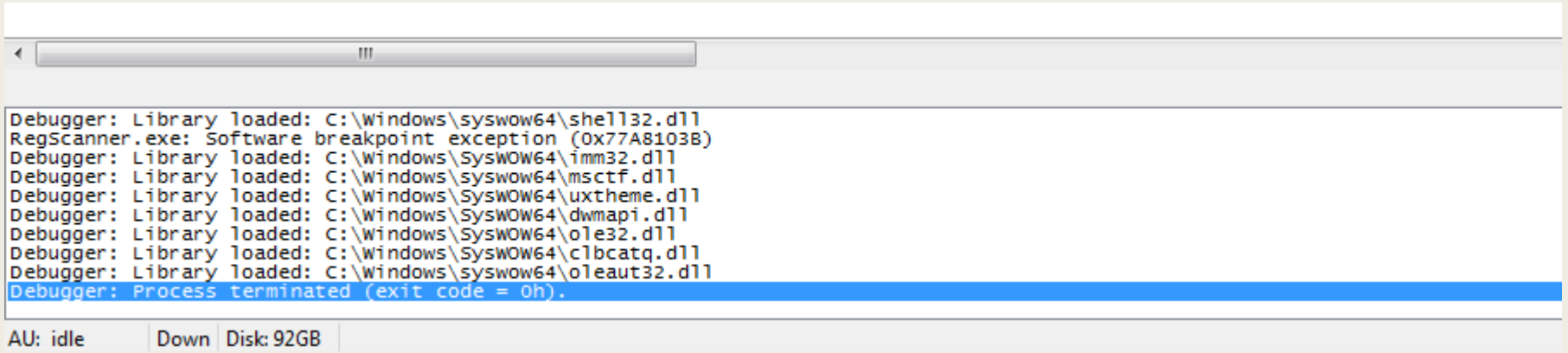
- To help hunt for the ASCII and Unicode
- Looking for embedded strings and other metadata
  - *Strings*
  - *Bintext (http://b2b-download.mcafee.com/products/tools/foundstone/bintext303.zip)*
  - *Google!*
  - *TextExtract (http://download.cnet.com/Text-Extract-Utility/3000-2351_4-75939982.html)*


/cygdrive/c/Users/kristyw/Downloads
BinText 3.0.3
Search
Filter
Help
File to scan
C:\Users\kristyw\Downloads\setupscreenhunterfree.exe
Browse
Go
Advanced view
Time taken : 29.204 secs
Text size: 283473 bytes (276.83K)
File pos
Mem pos
ID
Text
00000000004D 00000040004D 0 !This program cannot be run in DOS mode.
0000000000C0 0000004000C0 0 Rich)
0000000001C8 0000004001C8 0 .text
0000000001F0 0000004001F0 0 .rdata
000000000217 000000400217 0 @.data
000000000240 000000400240 0 .rsrc
0000000005C7 0000004011C7 0 98uA
000000000A63 000000401663 0 4]HQ@
000000000B62 000000401762 0 9GBHu
00000000159A 00000040219A 0 !5<T@
0000000015A0 0000004021A0 0 !5(T@
0000000015A6 0000004021A6 0 !5dT@
000000001602 000000402202 0 ? uG
Ready
AN: 50167
UN: 15
RS: 0
Find
Save

Symbolic and Debug info

- If the executable isn’t stripped of it’s function names (symbols) then we may be able to understand what it does
- Nm is our tool (https://sourceware.org/binutils/docs/binutils/nm.html)
- Or maybe dumpbin with /symbols (native tool to Visual Studio)
- x64dbg and x36dbg (https://x64dbg.com/#start)


Debugger: Library unloaded.
Debugger: Library loaded: C:\Windows\syswow64\kernel32.dll
Debugger: Library loaded: C:\Windows\syswow64\KernelBase.dll
Debugger: Library loaded: C:\Windows\syswow64\advapi32.dll
Debugger: Library loaded: C:\Windows\syswow64\msvcrt.dll
Debugger: Library loaded: C:\Windows\SysWOW64\sechost.dll
Debugger: Library loaded: C:\Windows\syswow64\rpcrt4.dll
Debugger: Library loaded: C:\Windows\syswow64\sspicli.dll
Debugger: Library loaded: C:\Windows\syswow64\cryptbase.dll
Debugger: Library loaded: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Debugger: Library loaded: C:\Windows\syswow64\gdi32.dll
AU: idle
Down
Disk: 92GB


Debugger: Library loaded: C:\Windows\syswow64\shell32.dll
RegScanner.exe: Software breakpoint exception (0x77A8103B)
Debugger: Library loaded: C:\Windows\SysWOW64\imm32.dll
Debugger: Library loaded: C:\Windows\syswow64\msctf.dll
Debugger: Library loaded: C:\Windows\SysWOW64\uxtheme.dll
Debugger: Library loaded: C:\Windows\SysWOW64\dwmapi.dll
Debugger: Library loaded: C:\Windows\SysWOW64\ole32.dll
Debugger: Library loaded: C:\Windows\SysWOW64\clbcatq.dll
Debugger: Library loaded: C:\Windows\syswow64\oleaut32.dll
Debugger: Process terminated (exit code = 0h).
AU: idle
Down
Disk: 92GB

Metadata

- Any links to libraries or object code
- But you may also find stuff like:
  - *Program author*
  - *Program version*
  - *Publisher*
  - *License*
  - *Disclaimers*
  - *Warnings*
  - *Comments*

File obfuscation

- Many reasons why this is employed, but let's focus on how to find this technique
- Packer/compressor/packing is essentially just compressing a file
  - *Typically writes a stub at the end of the file to be able to decompress the file*
  - *Important to do homework here to use the right unpacker or you could corrupt the file*
- Don't forget to make a copy please!

Crypters (Cryptor?)

- Using encryption to hide the innards of the file
- Like packers, a stub is left so that when the file is executed, it can be decrypted
- To find, use these tools:
  - *Peid (http://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml)*
  - *PE Detective (http://www.softpedia.com/progDownload/PE-Detective-Download-93097.html)*
  - *RDG Packer Detector http://www.rdgsoft.net/*

Binders, Joiners and Wrappers

- These are pretty much the same thing
- They take Windows PE files and make them a single executable
- When executed, the order in which the files execute is determined by the author
- Can open/execute or copy
- Find a bunch here: http://exe-binder.sharewarejunction.com/

Now what? Triage and Analysis

- Timelines are helpful
  - *But remember: on Windows systems the timestamp isn't always what it seem*
- There is no one way to address all malware encounters
  - *But a process does help!*
- Review installed programs
  - *Registry is a good starting place*
- Examine pre-fetch files
  - *These are files created when a program is executed that enables speedier subsequent access to the program*
  - *Found with a '.pf' extension*

More!

- Inspect executables
  - *Make sure that you do a file signature match*
  - *The extension may have been changed*
  - *May also be encoded to hide detection*
- Now check Services, Drivers, Auto-start locations and Scheduled jobs
- Analyze log files
  - *May have clues as to anomalous activity*

And there’s more

- Review user accounts
- Examine the file systems
  - *Looking for hidden files after bringing back a system*
  - *Look in %systemroot%\system32*
  - *Look around in close location to where you might have already found malware*
- Registry
- Restore points
  - *Found in the hidden volume “System Volume Information”*
- Keyword searching

Searching the database

- When you disassemble a file, you create a database
- What techniques do you use to search for things?
  - *Text (uses the disassembly window)*
  - *Binary (uses the Hex View window)*
  - *In these analyses, Case sensitivity may make a difference (why?)*

What. Is. It. doing?

- Establish an environment baseline
  - *There are many ways to do this*
  - *But virtualization is a great option*
  - *First key: take a snapshot of the system before you do anything*
    - Host Integrity Monitors- like Winalysis (http://winalysis.soft112.com/) or RegShot (http://sourceforge.net/projects/regshot/)
    - Installation Monitors- InstallWatch (http://installwatch-pro.en.lo4d.com/), InstallRite (http://www.softpedia.com/progDownload/InstallRite-Download-78545.html) or InstallSpy (http://www.softpedia.com/get/Internet/Popup-Ad-Spyware-Blockers/InstallSpy.shtml)

Pre-execution Preparation

- We want to monitor:
  - *Processes*
  - *File system*
  - *Registry*
  - *Network activity*
  - *API calls*
- Through both passive and active monitoring activities

Executing the code

- Simple execution- just run it!
- Installation monitor- load the program into a monitoring tool
- API monitor- launch it through an API monitoring utility

System and Network Monitoring

- First note here: if you need to adjust anything, take note of what happens directly after you do
- Then just observe the basic areas to see what happens
- Netcat may be a valuable tool here to help intercept requests
- Online sandboxes available as well

Has data left my network?

- The big question (often, without an answer!)
- However, if you understand what the malware is doing
  - *You may be able to give an answer with reasonable certainty*

Process Spying

- Using various tools to watch the API calls of a process can be pretty interesting
- Also will guide you to files that it may access on the system
- As well as to registry calls
- Think of how you want to record all this activity for your reporting that you will create later!

Interacting with and Manipulating

- API hooking may be a technique we use here
  - *SpyStudio is a tool for this (http://www.nektra.com/products/spystudio-api-monitor/download/)*
  - *Allows us to intercept function calls*

Exploring and Verifying Functionality and Purpose

- While we really want to let the program runs its intended purpose through on the Internet, that's not what we should do
- Tools that help emulate the interaction help our more complete understanding
  - *Like HTTrack for web activity (http://www.httrack.com/page/2/)*
  - *What others might be useful here?*

Event Reconstruction and Artifact Review

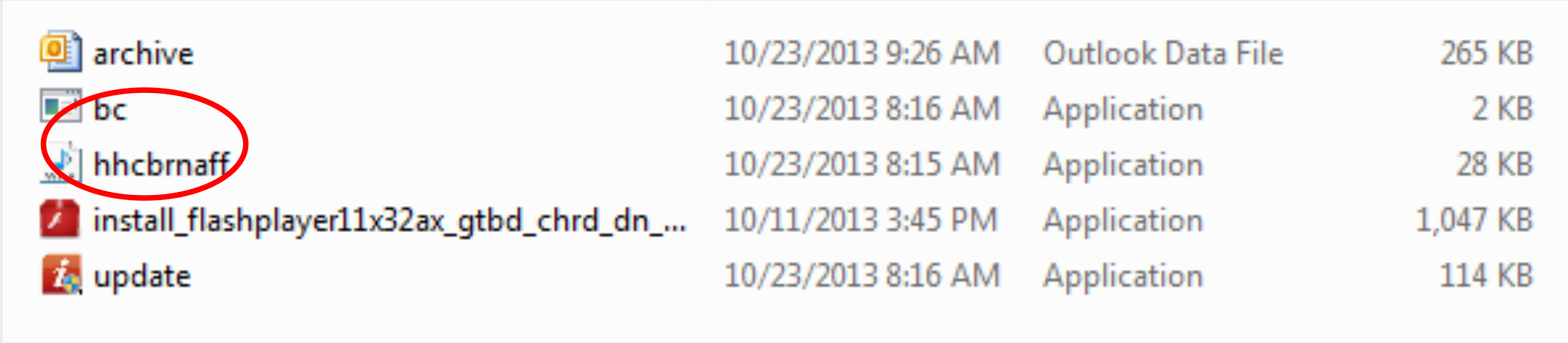
- Now take all of the previous steps and put it all together
  - *Remember that I mentioned the problem of recording all these steps?*
  - *Now is the time to bring it all together and answer all of the questions mentioned in part 1*
  - *What's the best way to do this?*

A side trip…but worth it

- A closer look at…Cryptolocker
  - *Let's take a look at a real troublemaker*
  - *And why it's so darn hard to know what they do*



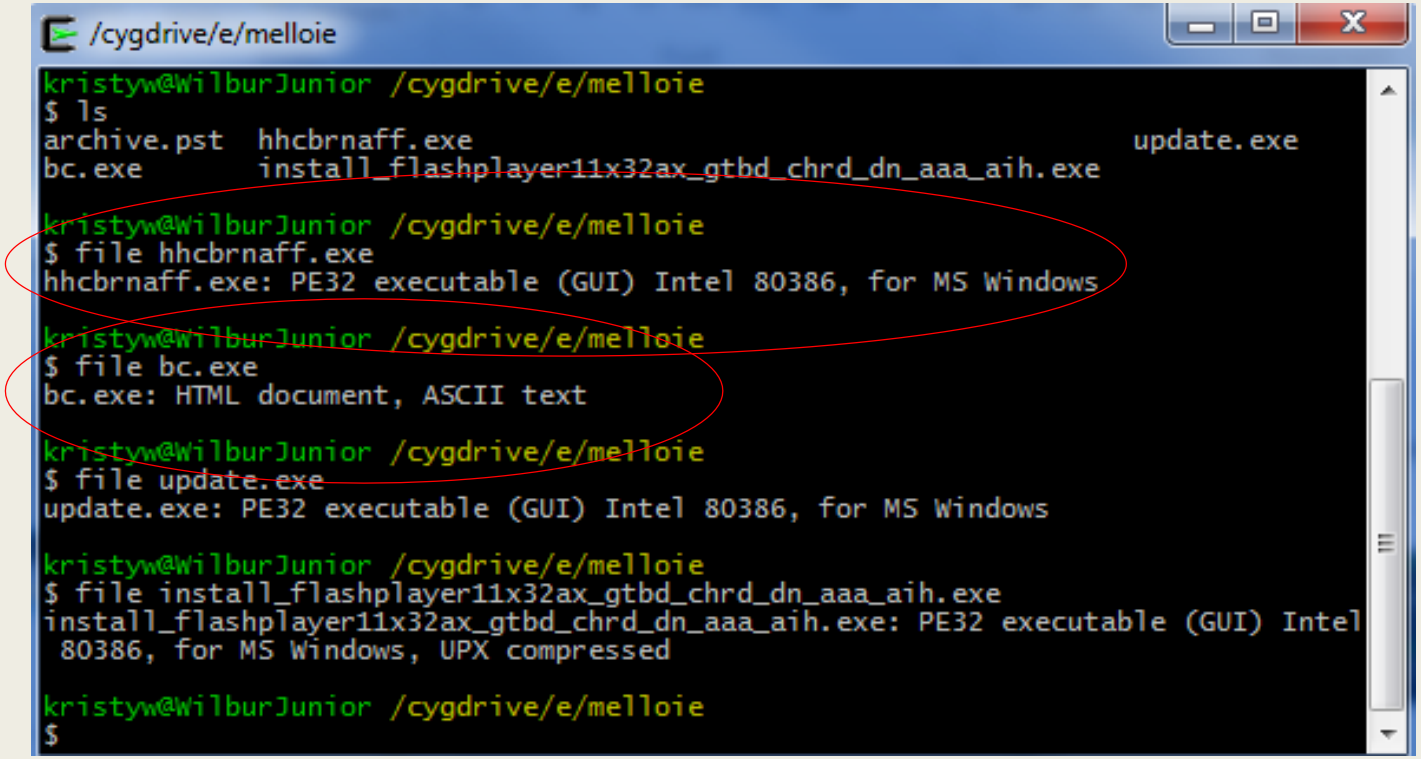
Some interesting suspects

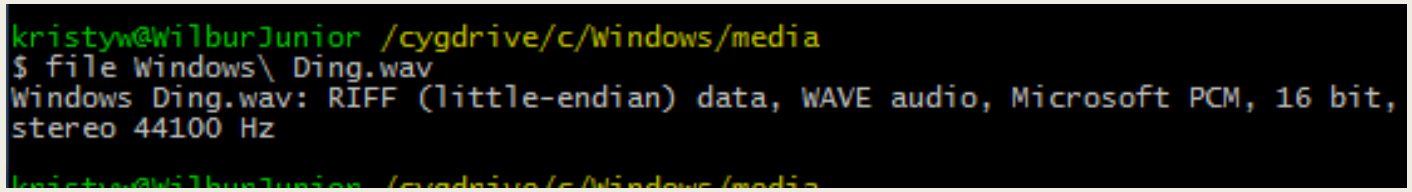


archive	10/23/2013 9:26 AM	Outlook Data File	265 KB
bc	10/23/2013 8:16 AM	Application	2 KB
hhcbrnaff	10/23/2013 8:15 AM	Application	28 KB
install_flashplayer11x32ax_gtbd_chrd_dn_...	10/11/2013 3:45 PM	Application	1,047 KB
update	10/23/2013 8:16 AM	Application	114 KB

What the heck are these two?

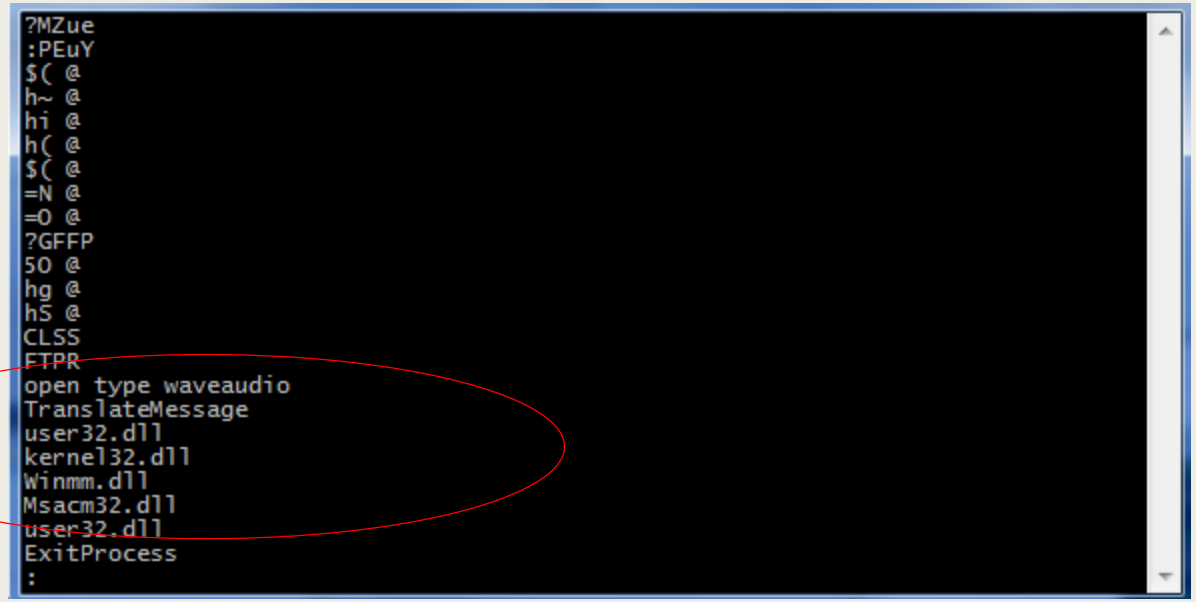
This doesn't help





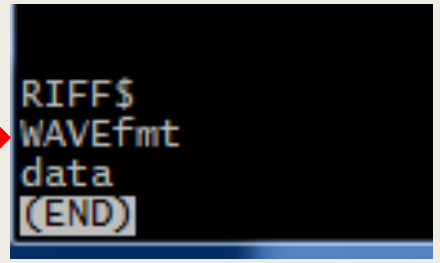
This is what a normal .wav file looks like

Compare strings

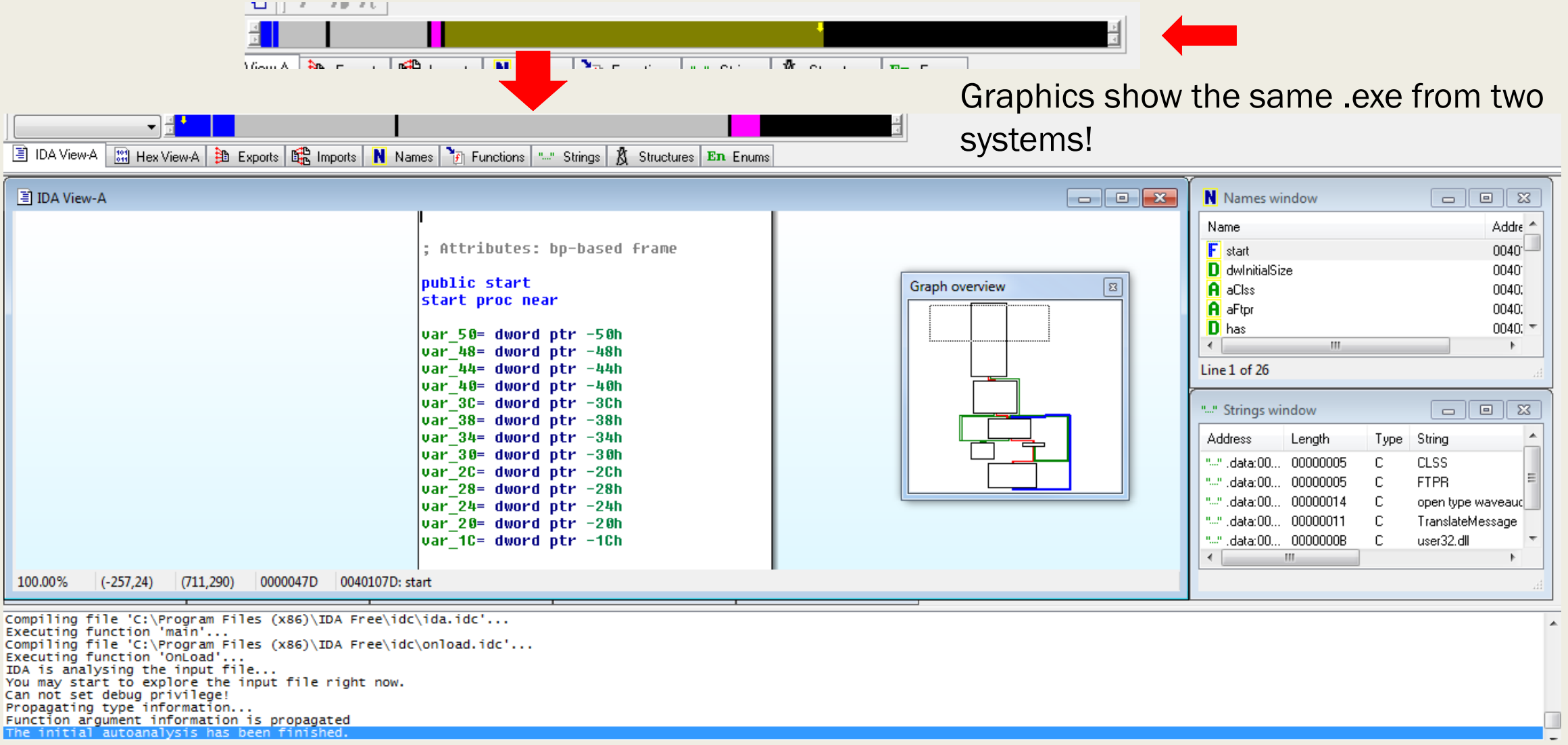


Bad file

Good file



IDA Pro will show us?



Graphics show the same .exe from two systems!

Shows a little more complexity, but also shows a whole lot of obfuscated code. Decision point: do you go further or seek other options?

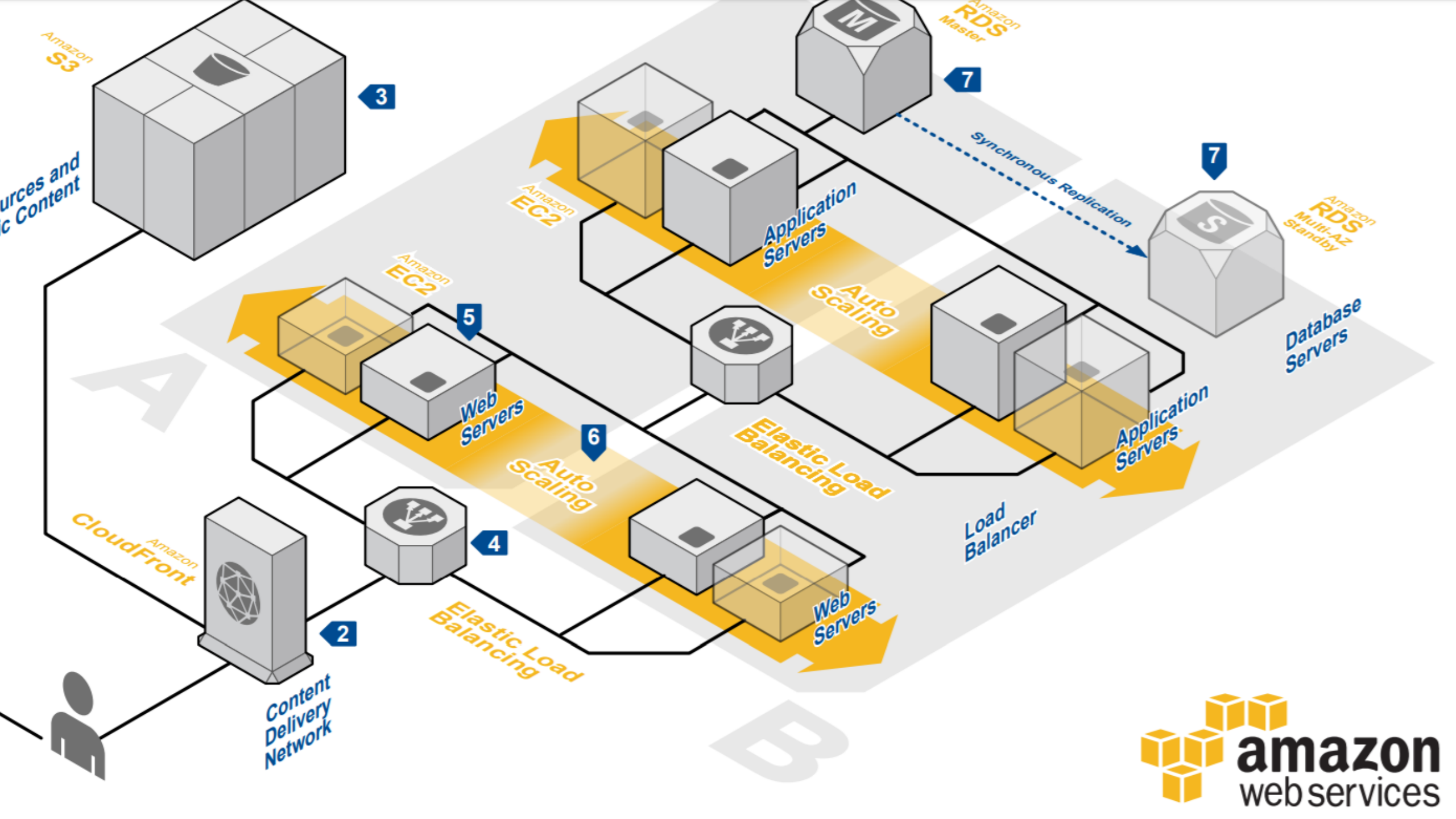
YOUR TURN!

TO THE CLOUDS!

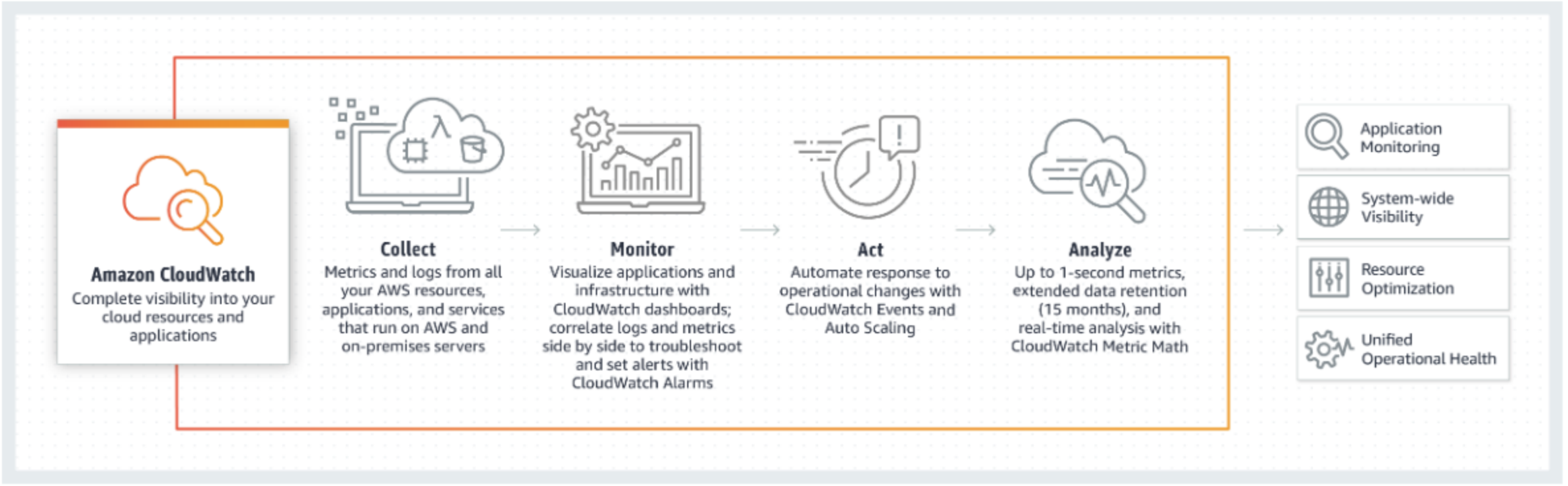


Cloud analysis

- How is cloud response/analysis different?
- How might it not be different?
- Couple of AWS examples
- And one Azure (just for fun)


Amazon S3
urces and
ic Content
3
Amazon RDS
Master
7
Synchronous Replication
7
Amazon RDS
Multi-AZ
Standby
Amazon EC2
Application Servers
Auto Scaling
Database Servers
Amazon EC2
5
Web Servers
6
Auto Scaling
Elastic Load Balancing
Application Servers
Load Balancer
Amazon CloudFront
4
Elastic Load Balancing
Web Servers
2
Content Delivery Network
A
B
amazon
web services

How it works


Amazon CloudWatch
Complete visibility into your cloud resources and applications
Collect
Metrics and logs from all your AWS resources, applications, and services that run on AWS and on-premises servers
Monitor
Visualize applications and infrastructure with CloudWatch dashboards; correlate logs and metrics side by side to troubleshoot and set alerts with CloudWatch Alarms
Act
Automate response to operational changes with CloudWatch Events and Auto Scaling
Analyze
Up to 1-second metrics, extended data retention (15 months), and real-time analysis with CloudWatch Metric Math
Application Monitoring
System-wide Visibility
Resource Optimization
Unified Operational Health

Components of interest

- Shared Responsibility Model- tells you what you can access and what you can’t
- IAM
- Host
- Data
- Applications
- (Sound familiar?)





AWS Logging Services

Overview

A configuration package to enable AWS security logging and activity monitoring services: **AWS CloudTrail**, **AWS Config**, and **Amazon GuardDuty**. The package also includes an S3 bucket to store CloudTrail and Config history logs, as well as an optional CloudWatch log group to receive CloudTrail logs.

Configure & Deploy

Configuration Presets

Environment

production

- Enables AWS CloudTrail, AWS Config, and Amazon GuardDuty
- CloudTrail Trail applid to all regions and Log File Integrity Validation is enabled
- S3 Bucket for CloudTrail logs and Config Logs: Server Side Encryption, Server Access Logging, and Block Public Access
- CloudTrail configured to forward events to a CloudWatch Log Group, with 90 days retention period

Configuration Template

S3 Bucket EDIT

AWS CloudTrail EDIT

Items 9 Size 4.4 KB Launch in AWS Account YAML/JSON

```
AWSTemplateFormatVersion: '2010-09-09'
Description: ''
Resources:
  S3SharedBucket:
```

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "accountId": "123456789012",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:22:54Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]}},
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 0,
            "name": "pending"
        },
        "previousState": {
            "code": 80,
            "name": "stopped"
        }
    }]}}
}]}
```

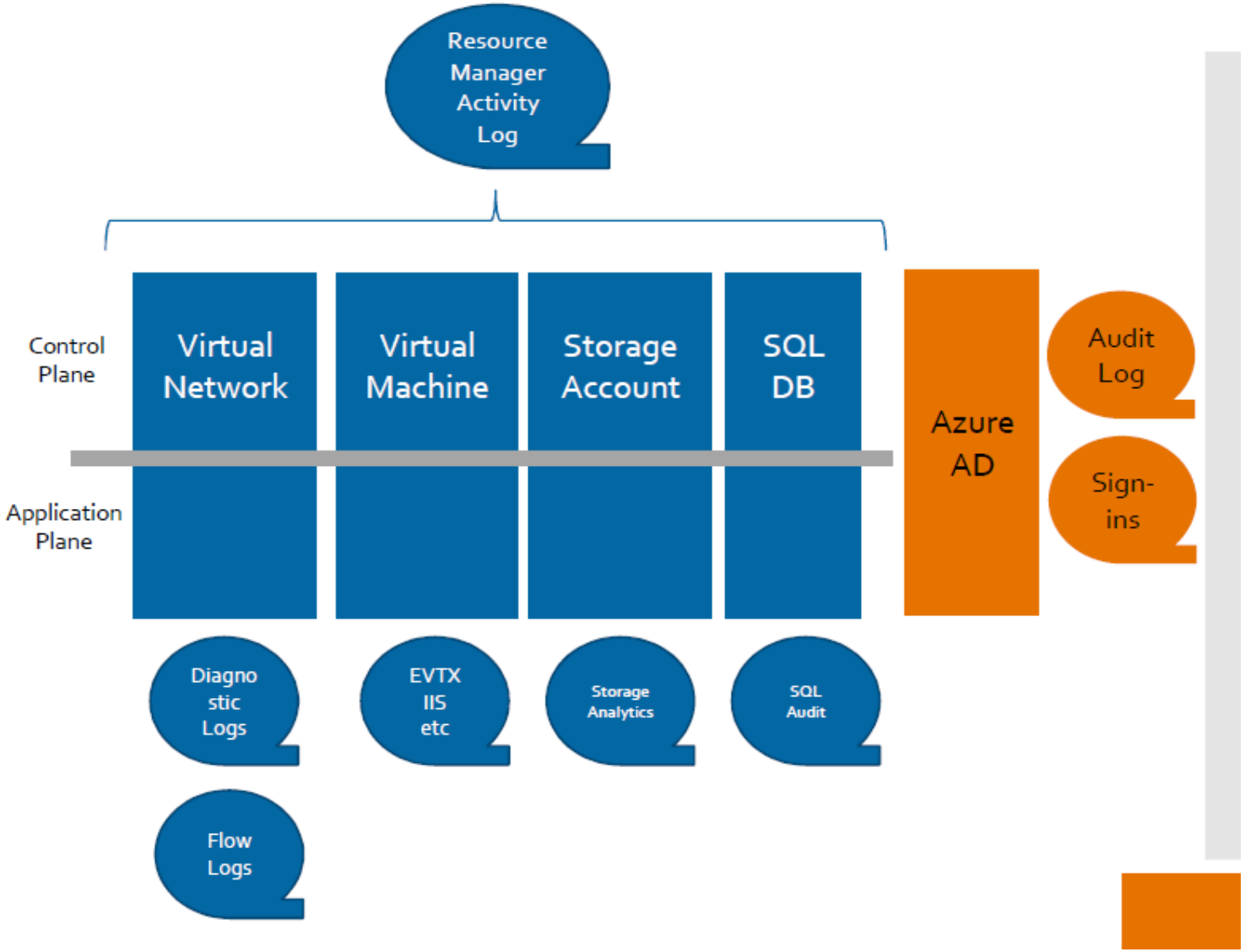
Don’t forget about Azure

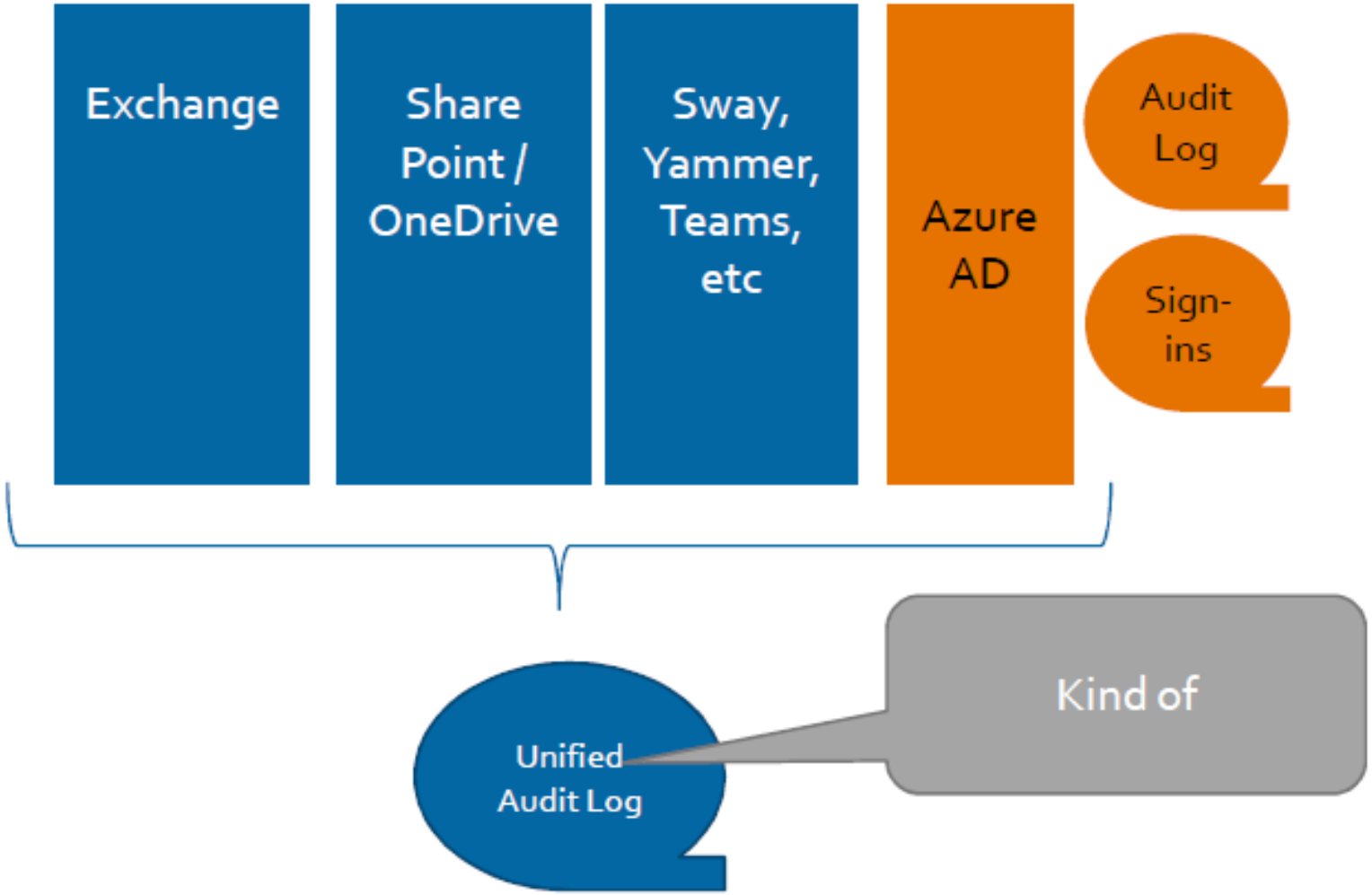
- https://docs.microsoft.com/en-us/azure/security/azure-log-audit
- Very similar in JSON format
- Otherwise tells you different things
- Use Security Center to help
- https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-schema
- https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-overview

Types of Azure logs

- Activity logs
- Diagnostic logs
- AD reporting
- Virtual machines and cloud services (event and syslog)
- Storage analytics
- Network security group flow logs
- Application
- Process data/security alerts

Azure Logging





https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema

```
{
    "records": [
        {
            "time": "2015-01-21T22:14:26.9792776Z",
            "resourceId": "/subscriptions/s1/resourceGroups/MSSupportGroup/providers/microsoft.support/supporttickets/115012112305841",
            "operationName": "microsoft.support/supporttickets/write",
            "category": "Write",
            "resultType": "Success",
            "resultSignature": "Succeeded.Created",
            "durationMs": 2826,
            "callerIpAddress": "111.111.111.11",
            "correlationId": "c776f9f4-36e5-4e0e-809b-c9b3c3fb62a8",
            "identity": {
                "authorization": {
                    "scope": "/subscriptions/s1/resourceGroups/MSSupportGroup/providers/microsoft.support/supporttickets/115012112305841",
                    "action": "microsoft.support/supporttickets/write",
                    "evidence": {
                        "role": "Subscription Admin"
                    }
                },
                "claims": {
                    "aud": "https://management.core.windows.net/",
                    "iss": "https://sts.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/",
                    "iat": "1421876371",
                    "nbf": "1421876371",
                    "exp": "1421880271",
                    "ver": "1.0",
                    "http://schemas.microsoft.com/identity/claims/tenantid": "1e8d8218-c5e7-4578-9acc-9abbd5d23315 ",
                    "http://schemas.microsoft.com/claims/authnmethodsreferences": "pwd",
                    "http://schemas.microsoft.com/identity/claims/objectidentifier": "2468adf0-8211-44e3-95xq-85137af64708",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn": "admin@contoso.com",
                    "puid": "20030000801A118C",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier": "9vckmEGF7zDKk1YzIY8k0t1_EAPaXoeHyPRn6f413zM",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname": "John",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname": "Smith",
                    "name": "John Smith",
                    "groups": "cacfe77c-e058-4712-83qw-f9b08849fd60,7f71d11d-4c41-4b23-99d2-d32ce7aa621c,31522864-0578-4ea0-9gdc-e66cc564d18c",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": " admin@contoso.com",
                    "appid": "c44b4083-3bq0-49c1-b47d-974e53cbdf3c",
                    "appidacr": "2",
                    "http://schemas.microsoft.com/identity/claims/scope": "user_impersonation",
                    "http://schemas.microsoft.com/claims/authnclassreference": "1"
                }
```

LAST ROUND!

Wrapping up (you made it!!)

- Definitely use tools to help you with the tonnage of data you have to deal with
- But understand what feeds the tool
  - *And how the tool may present it*
- Why didn't I cover application logs?
- Don't go it alone….



Resources

- https://github.com/chaoticmachinery/frac_rift Endpoint Collection Tools
- https://d1.awsstatic.com/whitepapers/aws-security-best-practices.pdf AWS Security
- http://www.onstrat.com/osint/
- https://www.hybrid-analysis.com/
- https://inteltechniques.com/
- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- https://www.fireeye.com/services/freeware/redline.html

Resources, part deux

- Malware Forensics: Investigating and Analyzing Malicious Code Cameron H. Malin, Eoghan Casey, James M. Aquilina
- Eagle, Chris The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler. No Starch Press.
- Eilam, Eldad Reversing: Secrets of Reverse Engineering. Wiley.
- http://www.reddit.com/r/ReverseEngineering/
- http://www.virusign.com/
- https://zeltser.com/malware-sample-sources/
- https://zeltser.com/malicious-software/
- Yurichev, Dennis. An Introduction to Reverse Engineering for Beginners. http://beginners.re/RE_for_beginners-en.pdf



THANK YOU!!

Keep the conversation going!

kmwestphal@cox.net