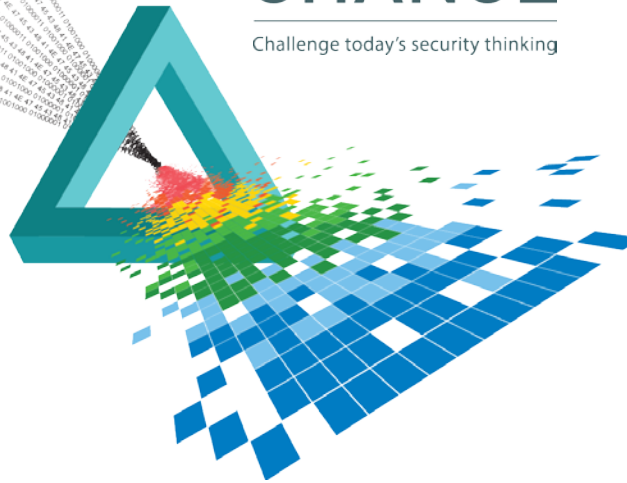
RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking



SESSION ID: CDS-R09

Debunking Myths About Attribution and New Strategies to Protect Your Data

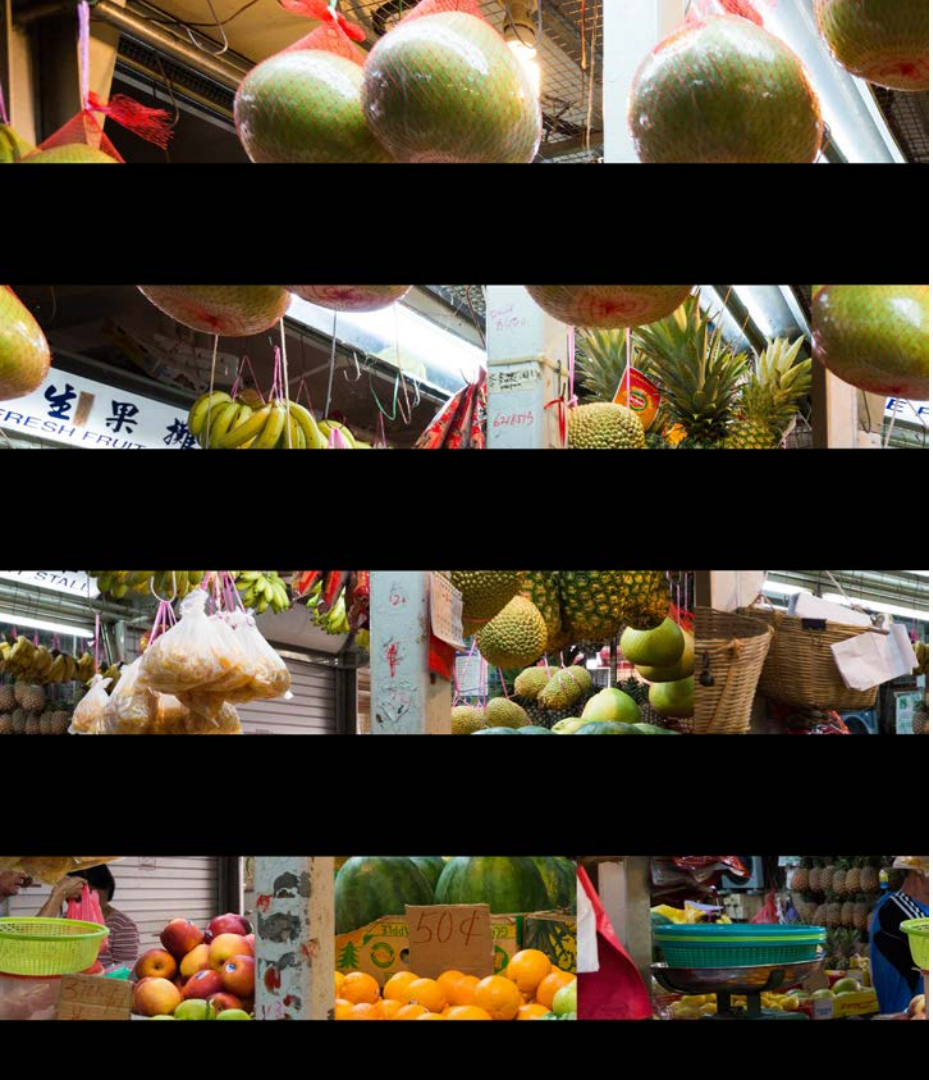
Mike Kendzierski

Technologist/Hacker/Reseacher/Inventor
Shoshn
@ShoshnLLC

```
100014B4        push    dword ptr [edi+4]
100014B7        pop     ecx
100014B8        push    edx             ; ucb
100014B9        push    74030000h       ; lp
100014BE        mov     [esp+20h+var_8], eax
100014C2        mov     [esp+20h+var_4], ecx
100014C6        call    ds:IsBadReadPtr
100014CC        mov     dword_10015650, eax
100014D1        rdtsc
100014D3        push    101h            ; dwMilliseconds
100014D8        push    eax
100014D9        pop     esi
100014DA        mov     ebx, edx
100014DC        call    ds:Sleep
100014E2        fld     ds:dbl_10001C60
100014E8        fldln2
100014EA        fxch    st(1)
100014EC        fyl2x
100014EE        fstp    dbl_10015000
100014F4        rdtsc
100014F6        sub     eax, esi
100014F8        mov     [esp+18h+var_8], eax
100014FC        sbb     edx, ebx
100014FE        sub     eax, eax
10001500        push    edx
10001501        pop     ebp
10001502        mov     ax, word_10014664
10001508        push    eax
10001509        push    6BEh
1000150E        call    ds:ChrCmpIW
10001514        push    Source          ; Source
1000151A        push    Dest            ; Dest
10001520        mov     dword_100154C0, eax
10001525        call    ds:wcscpy
1000152B        mov     dword_100155BC, eax
```

```
13086
13088                                   ; dwFreeTy
1308D                                   ; dwSize
1308F                           15FFC, edx
13095                           15FF8, eax
1309A
1309C                           1423C
130A2
130A3                   pop     eax
130A9                   push    ds:VirtualAlloc
130AA                   pop     edi
130AB                   push    eax
130B0                   push    87Fh
130B2                   push    0
130B4                                                   es
130B5
130BB                                                   ab
130BD                                                   is
130C2
130C8
130CE
130D0
130D6
130D8
130DE
130DF
130E5
130E7
130E9
130EA
130EB
130EC                   jmp     loc_10001E34
130EC _DllMain@12       endp
```

Remember, what **insight** will we be giving the audience



Fruit is harder to steal when it is not sold *directly* on the street

Why We Are Here

- Train like the hackers do
- Learn their techniques
- Get the same education
- Application Whitelisting, file-based encryption
- Be rigorous with your patching

Time for Honesty

- There is no quick fix
- Hackers are better prepared, trained and more organized
- We need to monitor everything
- Attribution is a Team Sport!


Big Data
Vendor Management
Binary Metadata
Maltego
Open Source Research
Static Analysis
Dynamic Analysis
Passive DNS
Development Signatures
Malware Categorization

We Need to Be Comfortable with Ambiguity

- Attribution is too large & complex for a single person
- “Quality” attribution requires a team of experts and outside thinking
- Attribution is a case study of “Hurry up and Wait”

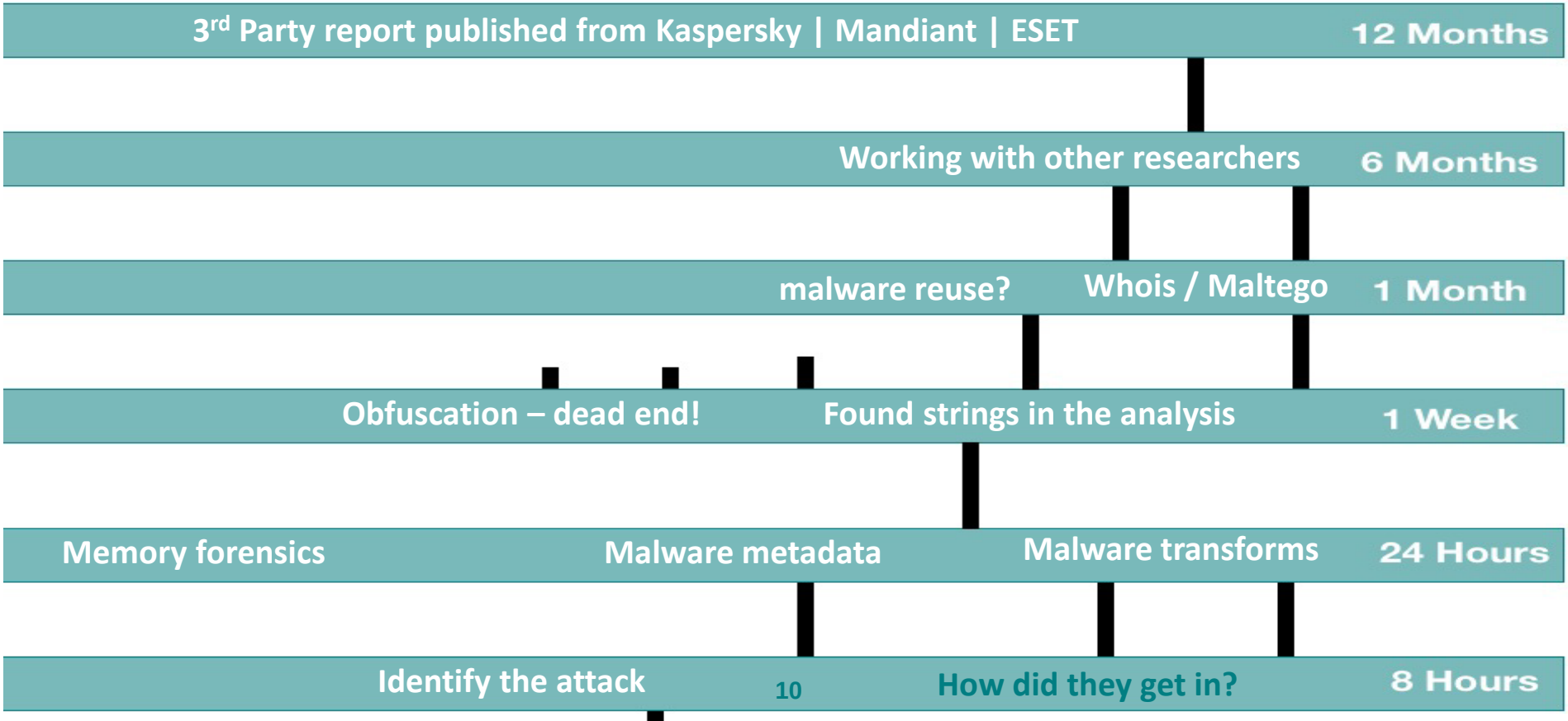
Malware Kill Chain

- Hackers don’t have super powers
- The bad guys still have to acquire the ability to execute code on a compromised system
- And there are only so many ways to do this
  - Email is your #1 danger (by a long shot)

We Need to Be Comfortable with Ambiguity

- We’re never going to be at “100%” confidence
- Are you comfortable with 75%?
- How about 80% but it will take another six months?

~Typical Attribution Progress



If we could have attribution right now, what would we do with it?

Attribution is Both an Art & Science

- We’re never going to be at “100%” confidence
- Attribution is about asking the “right” questions
- Understanding that the evidence may be placed there to trick you
- Obfuscation tools are there for a reason
- Story – VB script to add junk instructions to further obfuscate assembly code

What We Want

- We want the breadcrumbs (technical artifacts) that they leave behind in the form of software (malware binaries)
- The malware binaries contain metadata that we can use to data mine (either now or in the future when our tools work)
- Get the same education
- Application Whitelisting, file-based encryption
- Be rigorous with your patching

Attribution Unwinds Incrementally

Everything leaves a trail


Your data

Our Goals

- How do we get to a high enough confidence interval?
- How long will it take?
- What do we do with the data?

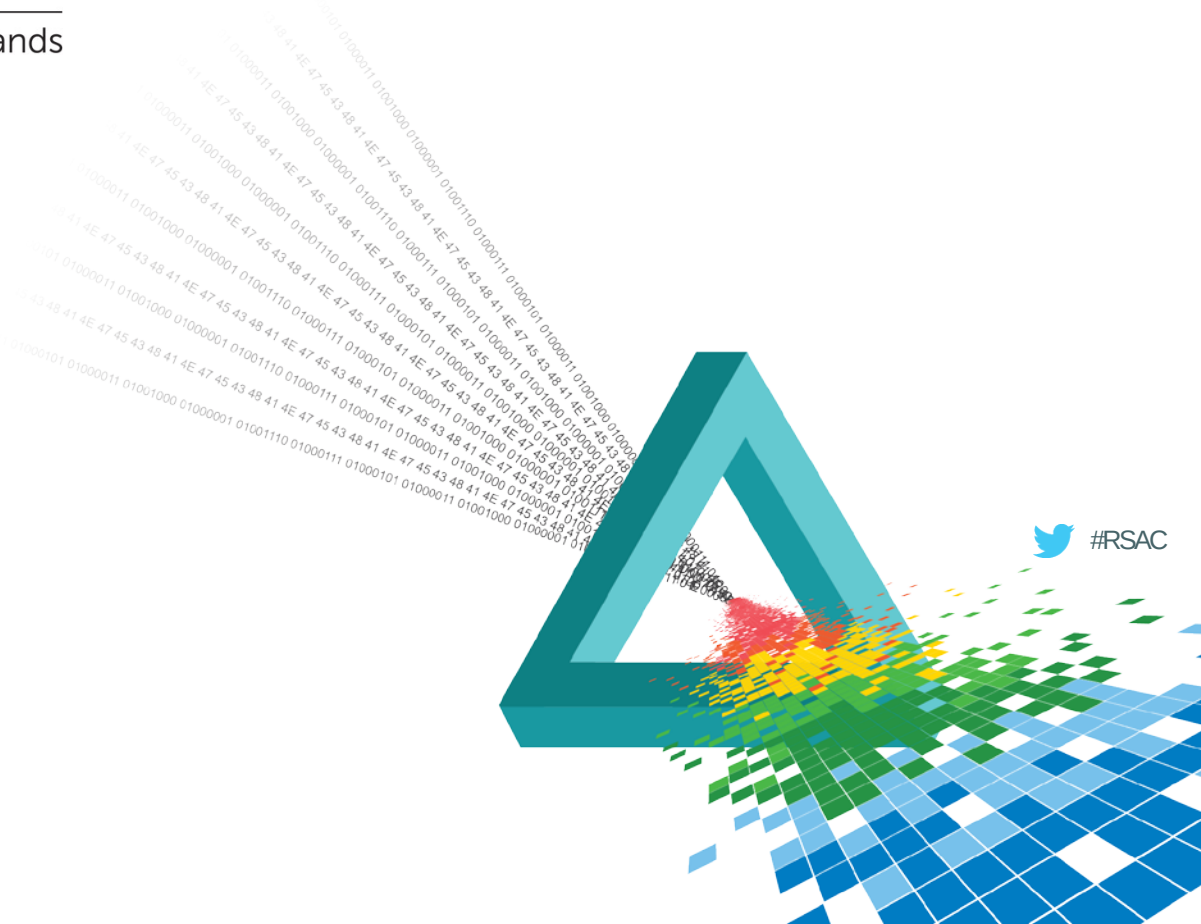
How do you prepare for an APT-like attack?

Insight

- Attribution is both an Art and Science
- There is a lot you can do today to protect your data
- Tools to make you less vulnerable”
- Need the “hacker mindset”
- Become bigger than your problem & take action
- No more fear, let’s review the truth
- How do you know what you are up against?

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

Attribution Myths

Myth #1 – Attribution is Hard

- Easy to Learn, Lifetime to Master
- All of the tools are available
- If you can read ASCII, you can do attribution
- Remove the fear
- The learning curve is not as bad as you think

Attribution is Easy?

- Yes and No.
- There are several steps
- It all starts with logging and understand the vulnerabilities
- Everyone makes mistakes (over the long haul)
- Big Data your friend
- Focus on the process, not the end result

Myth #2 – You know who is stealing your data

- Malware tools use some sort of obfuscation techniques
- 90% of the attribution claims are circumstantial
- How do they know?
- What tools are they using?
- Obfuscation, obfuscation, obfuscation
- You know it when you see it

Myth #3 – You Can Rely on Your Vendors

- Start pushing back on your vendors
- How can you test in an intergrated environment?
- At a macro level, it's not a bad place to start
- Throwing money at the problem only creates more problems
- You are better off working with your partners or competitors
- Share, Share, Share!

Myth #4 –Attribution Doesn't Matter

- To better defend the perimeter, we need to know what their tools are
- Improves our ability to disrupt the attack and know what they are after
- It does matter, regardless if you can't do anything about it

So how do you know that?

- Longitudinal studies
- Everyone makes mistakes
- Big Data
- Malware repositories
- Share Threat Information among the security community
- Volume, volume, volume!

Myth #5 – Attribution is Science

- Attribution is both Art & Science
- And experience and intuition
- Correlation does not imply causation
- Today's Stuxnet is tomorrow's Shamoon…
- While there are methodologies, each one is unique
- Stay flexible, work with the smartest people you can find

We need a framework

- For attribution, there are many frameworks to analyze the malware killchain
- You will need a large team and it won't happen overnight
- Big Data can help make the process easier (in the future)

Myth #6 – IP Theft Primarily Exists in Asia

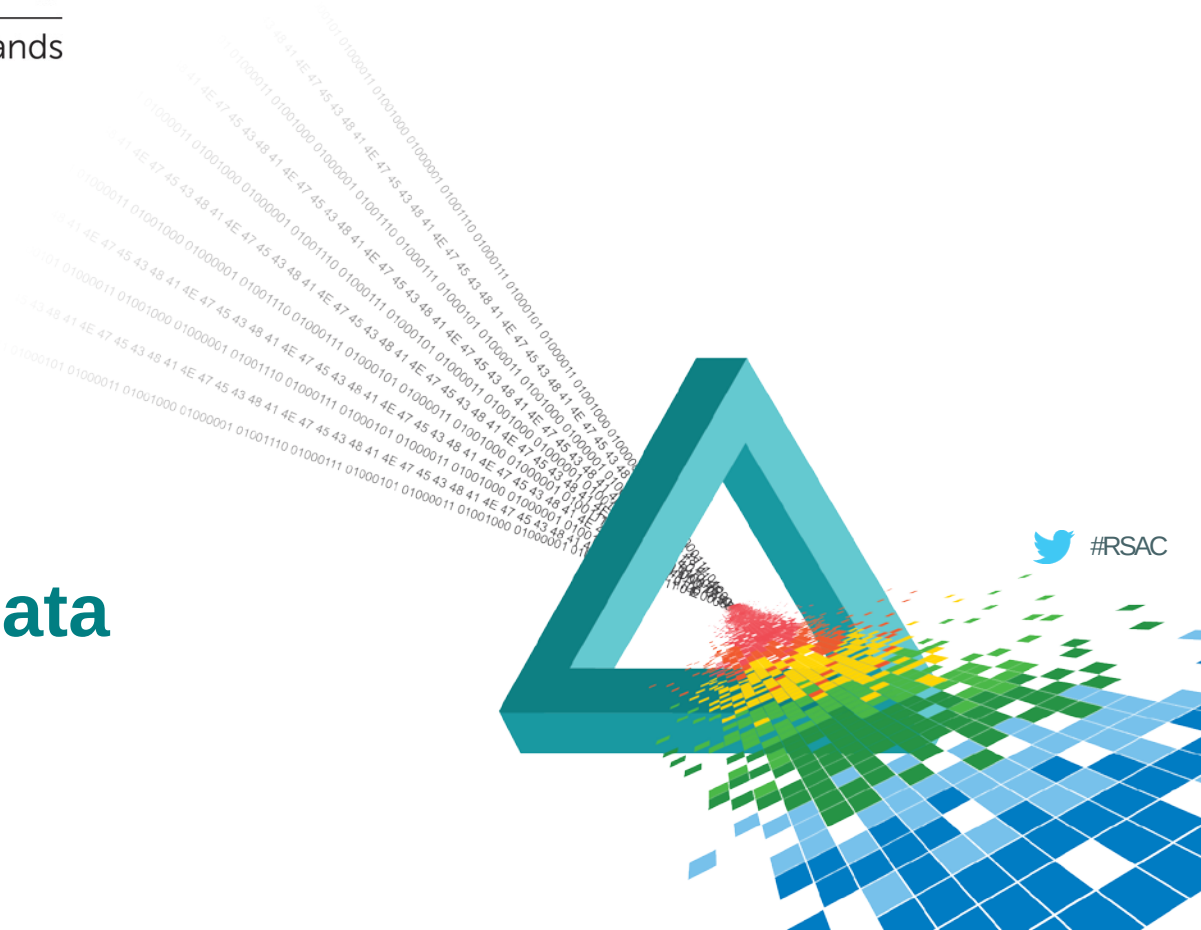
- Completely wrong!
- IP theft has been around as long as people could steal
- The United States stole most of the technology from the British to launch the industrial revolution
- When an innovation economy has IP worth protecting, expect more IP right enforcement
- The opportunity cost to stop the theft is just not there

Software, not infrastructure

- Focus on what is in the pipe, not the pipe itself
- Because attacks are normally tied to the perimeter, most companies focus on the “infrastructure”
- The more “sophisticated attacks” are done at the software layer
- Hackers have a step up due to their “learning agility” and experience

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



Protecting Your Data

Blended Analysis

- Information from all sources
  - Passive DNS, malware families, vendor reviews, VirusTotal
  - Every data point has value
  - Tying the attacks to one another
- Changing the Mindset
  - This is not a quick fix
  - Longitudinal study on your enterprise

Identifying the Attack

- At the perimeter
  - Firewalls
  - H/IDS, N/IDS
- Internally
  - Data Loss Prevention agents

Big Data

- Collect everything – log analysis, wire analysis
- Malware binary repositories to query

ALL YOUR BASE ARE BELONG TO US

Analyzing the Malware

- Automated Analysis
  - Sandboxes, VirusTotal, What files it creates in the file system
  - Cuckoo
- Static Analysis
  - Strings, Project Executable Objects
- Manual Behavor
  - Sniffers
  - ProcMon, ProcExp,
- Manual Dissembly / Debugging
  - Deobfuscation

Let’s Talk Attribution

- Compiling information

Environmentally Aware Malware

- Anti-analysis techniques?
  - 88% of malware includes Anti-reverse Engineering mechanisms
    - Qual
    - Passing along to the RE teams
  - 81% include anti-virtualization techniques
  - 43% include anti-debugger techniques
  - Anti-Sandboxing
- Throwing money at the problem only creates more problems
- You are better off working with your partners or competitors

Anti-Debugging

- Tracking the program as it runs
- Is ICE running? (SoftIce)
- API-based – IsDebuggerPresent
- Flags based
- Timing based – Is the program slowing down?
- Exeception Based
- Breakpoint Detection

Reversing the issue

- Let’s pretend we actually know who is behind the attacks

You still need to…

- Have a data classification policy
- Physically segment your most sensitive data
  - “Air gapped”
- Have an auditing/logging/alert policy
- Know your partners upstream and downstream dependencies (weaknesses)
- Hire hackers

Applying Your New Knowledge

- Hire Hackers!
- Get the “Hacker Education”
- Learn Assembly!
- Share Threat Intelligence
- Collect Everything

Taking Action – Protecting Your Data

- Maltego
- Start your own data repository (Intro to Big Data)
- File-based Encryption
- Application Whitelisting
- Data Classification Policy
- Air Gap / Physically segment your most sensitive data
- Don’t rely on just your software / dashboards

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Thank you!