
CRYPSIS™
Malware Incident Response
Forensics 101 —
Stories from the Field
Jake Babbin | Director – Threat Intelligence | The Crypsis Group

Agenda

- Introductions
- State of Incident Response
- Incident Response 101
- Rapid Incident Response
- Conclusions
- Questions/Comments

Speaker Background

Currently

- Director of Threat Intelligence, The Crypsis Group

Prior

- Practice Director – Incident Response and Forensics McAfee/Intel Security (Americas)
- Incident Response Auditor for DoD CIO CND-SP/CCRI team
- Lead Analyst The White House Security Operation Center (EOP)
- Founded The White House Cyber Threat Cell
- Published Author
- Holder of a National Security Trademark
- Over 15 year career spanning a variety of customers in US Military, Intelligence Community, and Federal Law Enforcement

State of Incident Response

- It's not just for nation-states anymore
- It's a booming business — crimeware-as-a-service
  - → big businesses and specific industry vertical's are being targeted.
  - → Ransomeware is a revenue generating business
- It is estimated that the global cost of cyber crime is in the hundreds of millions to billions of dollars in losses each year.

Nation-states Still Very Relevant

- Some specific crimes are being brought to courts targeting awareness as well as damages for
  - → Intellectual property
  - → Research and Development
  - → Legal documents and trade agreements
- OPM Hack –
  - → China
  - → 21.5 million former, current, and prospective federal employees and contractors whose Social Security numbers, personal information, and background investigation

Federal case against 5 Chinese PLA (Peoples Liberation Army) cyber officers - https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

ODNI and FBI press release on Election concerns - https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement

Article on State Election Board hacks - http://abcnews.go.com/US/attempts-hack-state-election-systems-detected-fbi-director/story?id=42418303

Nation-states Still Very Relevant

- DNC Hack –
  - → Russia
  - → Theft of emails and documents from Democratic National Committee servers
- Two State Election Boards
  - → Russia
  - → Attempting to gain access to Voter Registration Databases
  - → Illinois and Arizona,
  - → Other states have concerns as well
- Today is it estimated that dozens of countries have stood up or are in the process of standing up cyber warfare capabilities and units.

Federal case against 5 Chinese PLA (Peoples Liberation Army) cyber officers - https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

ODNI and FBI press release on Election concerns - https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement

Article on State Election Board hacks - http://abcnews.go.com/US/attempts-hack-state-election-systems-detected-fbi-director/story?id=42418303

What Can We Do?
Incident Response 101

The Need Is More Than Here for Incident Response

Can your organization answer these questions

- Is your organization adequately prepared for an incident?
- When an incident occurs, is there a process and workflow to actively engage with management? Can leadership respond and engage back?
- After an incident, will management know how the incident occurred and to prevent the breach from happening again?
- Will management know what Intellectual property (IP) or data was compromised? What risks/losses does this reflect?

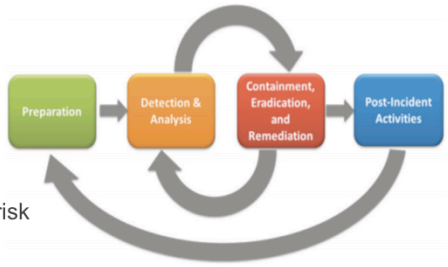
Incident Response 101

- Incident Response Life Cycle
- Basic information to Collect
- Typical issues
- First Steps
- Triage Techniques
- Tools

IR 101 — Incident Life Cycle (NIST)

Consists of 5 steps

- Prepare
  - → Prepare the Incident Response Plan
- Detection
  - → Detect the Incident
- Analysis
  - → Analyze the Incident data, impact, and risk
- Recovery
  - → Recover from the Incident
- After-Action
  - → Create an After Action Report and develop Lessons Learned



Incident Response Life Cycle

IR 101 — Basic Information to Collect

- Volatile data — This is data that can change quickly such as RAM, open files and processes and even some log files
  - → Capture RAM and process memory
    - Can provide unencrypted copies of running malware, recently used files, typed commands, and even passwords
  - → Capture Running processes, Open network ports, system services and devices and last 50 files modified/accessed
  - → Local Event logs (Windows System, Security and Application logs)
    - Capture any additional host logs (HIPS, DLP, firewall, etc)
- Physical Data
  - → Perform a full disk collection
  - → Log, photograph and seal if pursing legal recourse
- Collect 3rd party and Network/Enterprise data
  - → Network IDS/IPS logs
  - → Network Firewall and web proxy logs
  - → Other relevant data

IR 101 — Malware Forensics Examination

- Profile the system
- Examine the Volatile Data
- Examine any on disk Identified files
- Conduct scans for known malicious files/code
- Examine programs executed on the system
  - → Window Prefetch files
- Examine autorun locations
- Examine host Windows Event Logs
- Create a file system timeline
- Examine User web browsing activity
- Perform a Keyword search on the disk image
- Examine and suspected malicious files

IR 101 — Typical Issues

- Collection
  - → Memory collection
    - Can be defeated by malware through process hooking
    - Time consuming (takes time to image and parse memory)
    - Typically scanned with IOC's (Indicators of Compromise) of some kind.
    - Typically unable to be performed due to technical and political reasons
  - → Parse Program execution, autoruns, and the file system
    - Voluminous amounts of data to search
- Analysis
  - → Difficult to scale for multiple victims
  - → Storage and analysis takes time and space

IR 101 — First Steps

What to search for?

- Malware has a 2 goals
  - → Remain hidden on system
  - → Require access to run/function
- Something changed on the system to allow the malware inside
  - → Drive-by targeting a client-side application
  - → User opening malicious email attachment
  - → User running trojanized file such as a key generator
- Search for:
  - → Programs executing from temporary or cached folders
  - → Programs executing from user profiles
  - → Programs executing from All Users profile
  - → Programs executing from the Recycle Bin
  - → Programs stored as Alternate Data Streams
  - → Programs with random and unusual file names
  - → Windows programs in wrong folders

IR 101 — Triage Techniques

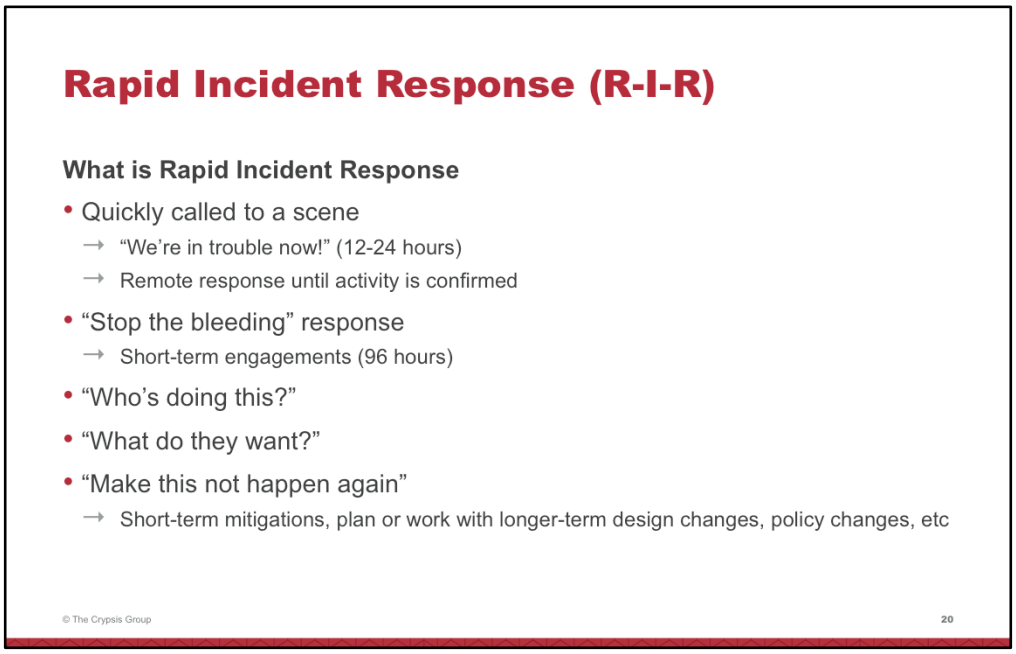
- Gain access to data quickly
  - → Remotely over the network to the live system
  - → Create and use collection scripts to 'collect' data off live system
- Examine key areas to identify
  - → Parse Program execution and Auto-start artifacts
  - → Review Program execution
    - Timeline activity searching for unusual activity
    - Pretech files
    - AppCompatCache registry key for related activity
    - MUICache registry key for unusual process paths
    - Auto-start locations and run keys
  - → Parse file system artifacts for Master File Table timelines that match up with activity
  - → Confirm any suspected files are malicious
    - One Option is to use Virustotal to search by hash (NOT UPLOAD FILES)
  - → Use public information to get more context about any hostile files (Google for example

IR 101 — Example Tools

- Windows Prefetch files
  - → WinPrefetchView http://www.nirsoft.net/utils/win_prefetch_view.html
- Windows Registry Hives
  - → RegRipper http://code.google.com/p/regripper/downloads/list
  - → Auto_rup http://code.google.com/p/regripper/downloads/list
- NTFS File system Artifacts
  - → AnalyzeMFT https://github.com/dkovar/analyzeMFT
  - → Windows Journal Parser http://tzworks.net/prototype_page.php?proto_id=5
- Windows Event Log
  - → Windows Event Log Explorer http://www.eventlogxp.com

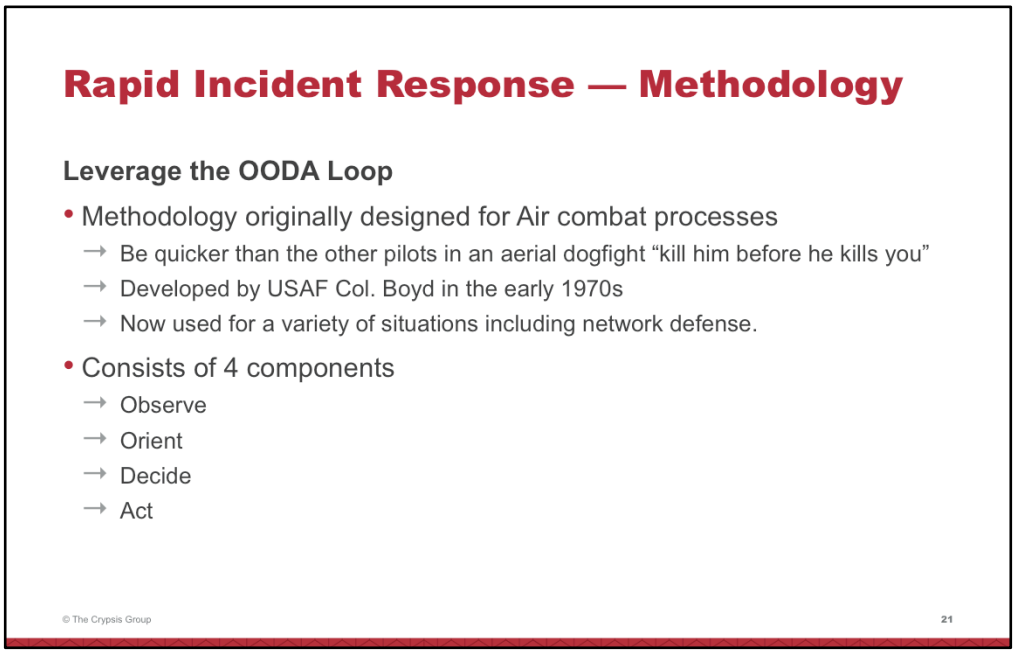
Putting it All Together

- Introducing Rapid Incident Response
- Otherwise known as “Tactical Incident Response”
  - → Used when an organization needs to ‘stop the bleeding’ from an attack
  - → Time is critical
  - → Not likely to purse legal recourses
- Can leverage multiple organization/agency collaboration to discover and attribute attack



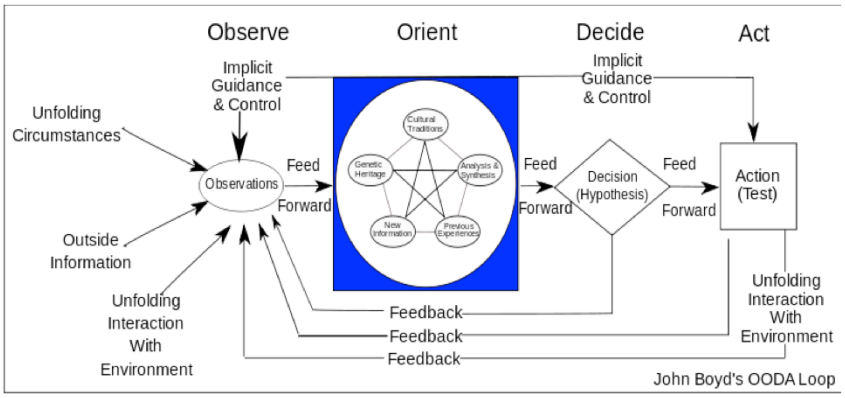
Quickly called to a scene – my old example 6 hours anywhere in the world

Main Goals
– not trying to be onsite forever 96 hours on scene total
- Identify the attackers and their goals in attacking victim
- Eject them from the victim network



OODA Loop Definition - http://en.wikipedia.org/wiki/OODA_loop

RIR — OODA Loop



RIR — OODA Loop (cont'd)

Observe

- Assess the victim and their damages
  - → Logs and victim information (verbal reporting from people)
  - → Sometimes 3rd party reporting

Orient

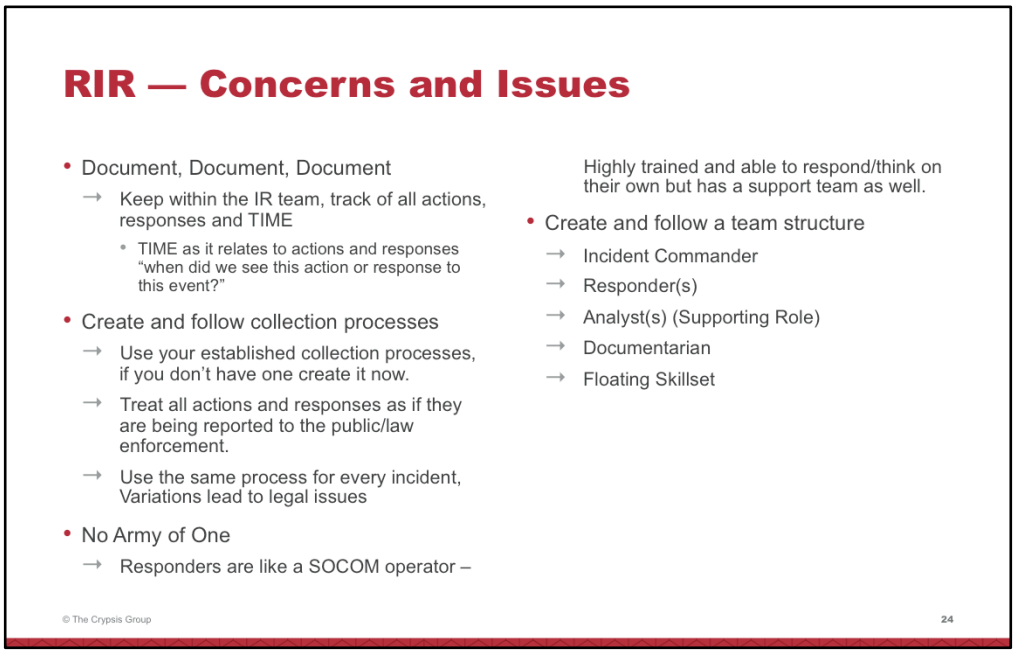
- Prepare to take actions based on damage and attribution
  - → Newly placed sensors or logs
  - → Malware reverse engineering
  - → Discovered files
  - → Compromised systems

Decide

- Choose how to best mitigate the situation
  - → Blocking activity
  - → Monitor/Observe if Law Enforcement involvement

Act

- Take action
  - → Cut systems off/burn and rebuild
  - → Disable user accounts
  - → Issue new blocks



I can't stress enough how important it is to document all parts of an incident, roles and keeping track of time for all of these.

There are several tools that allow you to track all actions during an incident you need to decide what works best for you, BEFORE an incident.
Notecase –
Dradis –
Veris (Verizon Online system)
Group Silc/Jabber Channel
Sharepoint (blog site)
Mind Mapping

Email is quite horrible middle of an incident not only keeping track of all the threads but the time to get information to needed people is often wasted.

Create and use every time for every incident the same collection processes. Variations off of this can hurt a case they can also quickly lead a team down the wrong 'rabbit hole'.

Most people forget that an incident keeps going even while we are sleeping, away, doing other actions, etc. A supporting group possibly at a home site can pay dividends during a case. For example in one case I had several gigs of log data to process that had been collected through the day. I was busy on scene reversing some captured malware and still imaging/processing hard drives; I needed to look through the log data for signs of our known compromised user accounts and their actions on the network. The support team of analysts back at HQ were 24/7 and they were able during the overnight hours and while I was working on the malware and imaging to process the logs and bring back a list of other hosts we would need to collect.

There is no one-man/woman shows; this is a team effort to not only maintain knowledge but also with the amount of data we are tasked with examining/cataloging growing exponential.

Team Structure
Incident Commander – this person is charged with running the show. They not only coordinate actions and tasks they are also charged with knowing at any given time the status of the incident. This person also is the single point that all team members keep informed of updates. They also are the voice/contact for the victim and anyone outside of the team to communicate with; this prevents mis-information, tasks errors and generally helps the team stay cohesive.

Responder(s) – This person or people if the incident is quite large, should be Senior in their experiences responding to incidents. They should be a jack of all trades so they can respond and think on scene as needed. (network detection analyst, a forensics analyst, malware (intro), Security engineering, application/services awareness, and be able to create scripts/solutions on the fly) This is your SOCOM operator and is your on-scene view of the entire incident response team to a victim.

Analyst(s) – These can be a supporting group within a Security Operations Center who may have a variety of skills and knowledge but are there to assist with tasks.

Floating Skillset – This position is one that is useful to bring in and out people with different skills. For example if the responder is on a scene where the victim has a custom web-app that has been broken into a developer of the app or a specialist may be needed to support the incident.

Documentarian – this person should be attached at the hip to the Incident Commander making sure everything is collected, cataloged and timestamped as it relates to the incident. Once the incident is over this person will be invaluable with the documentation when creating After-Action Reports (AAR), team and process reviewing (What did the team do right? Wrong? Changes needed to our processes?)

Rapid Incident Response
Examples of use

RIR — Examples

Example 1

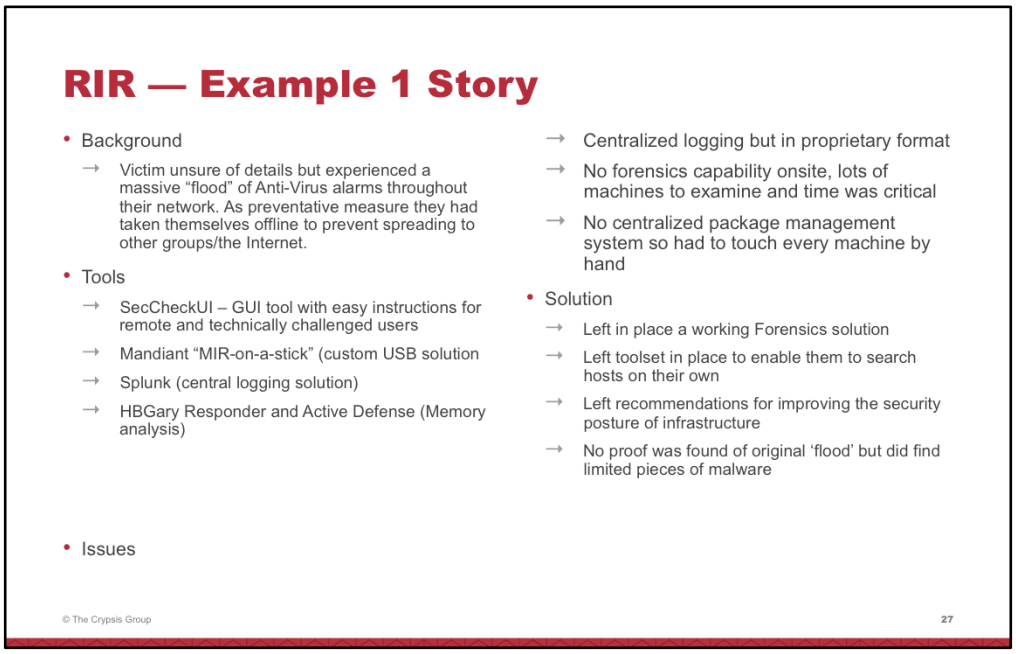
- Victim reports massive compromise and has taken themselves offline

Example 2

- Victim was notified by Law Enforcement that they have a ‘problem’

Example 3

- Victim unsure of what they observed and now is requesting assistance in ‘finding the bad guys’



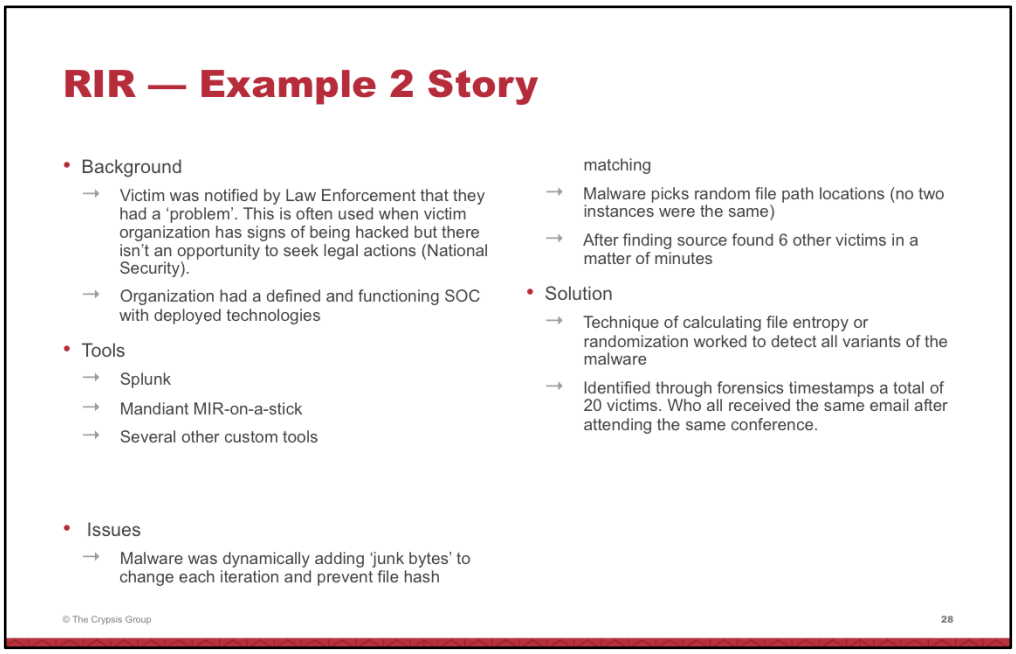
Started by examining a suspect machine
found several pieces of malware
analyzed to confirm that no real-time activity was occuring (no reverse shells)

Issue 1 –
Central logs from devices but in proprietary tool so they can't be searched

Issue 2 –
No forensics capability, lots of drives to image and time was a factor
- using local instance of a live CD to create stand alone analysis machines

Issue 3 –
No central SCCM so have to go touch every machine (luckily everything was on one campus in several buildings and local staff really wanted to help!)

Solution –
Left them in place the working forensics capability moving forward
Left in place several of the tools including secCheckUI to help "gut check" systems that they thought could have common malware
Left them recommendations and some improvements to their existing security infrastructure



Arrived and the remote support group from the SOC was able to show some suspicious domains and connections but nothing solid.

Examined one machine and through analysis process was able to identify a suspicious file

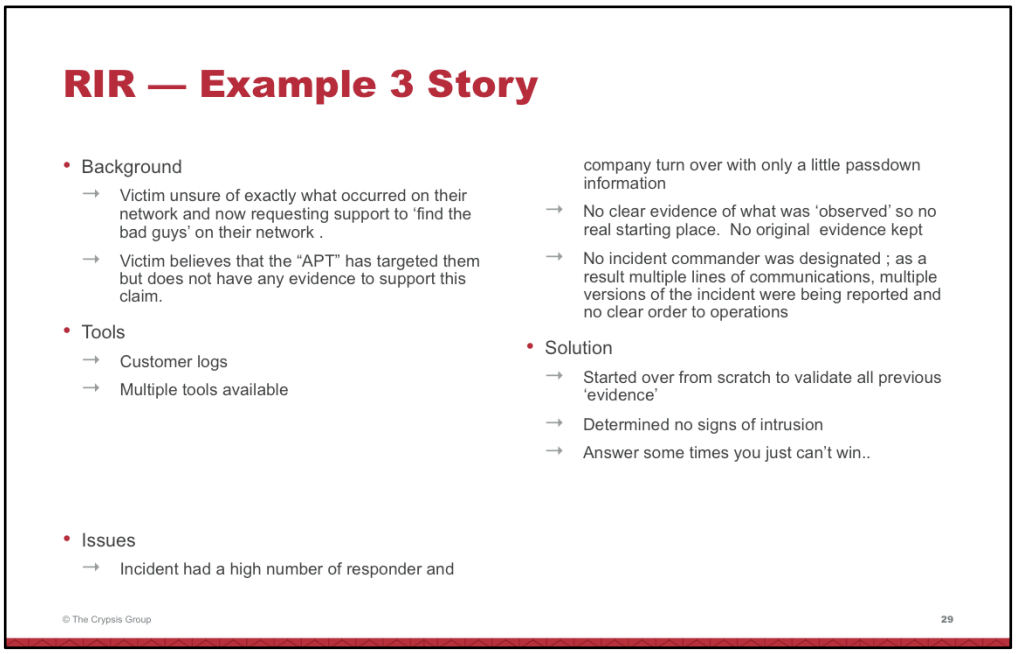
Issue 1 – Malware dynamically adds "junk bytes" to it's end for each mutation
no MD5 hashing or file size identification

Issue 2 – Malware picks a series of random path locations to hide in
no common path to find

Issue 3 – after finding the first victim identified 6 other machines in a matter of minutes

Solution – tried a new tool tracking file entropy (amount of randomization in a file) and ran it across all 7 machines…. Malware lit up like a x-mas tree same entropy value down to the thousanths place!

Solution – Identified timestamps of installs and was able to track back to a total of 20 victims all who received the same email over a month ago after all team members to a specific task attended a conference.



A number of issues

Issue 1 - High number of responder turnover and little passdown information.

Issue 2 - No clear information on what was actually 'seen'
As a result no original evidence was collected.

Issue 3 – no incident commander was designated so multiple people at the victim site were running around with different versions of status, what was 'taken', what was 'hacked' and no clear oder to operations

Solution –
Capture and organized/document 'facts' starting from scratch
Work through and prove correct or incorrect 'comments' about the 'incident'
Re-collect or collect 'evidence' to support 'facts'

A longer term team is currently handling the 'incident' and trying to work through the issues above still.

Answer some you can't win….

RIR — Last Thoughts

- No solution is perfect
- Feedback into your processes and documentation will improve your response capabilities
- Lifecycle tools and processes as your needs change and the attacks change.
- Every case will be different

Conclusions

- Cyber crime and attacks will increase
- Creating and implementing an incident response plan is critical
- There are multiple methods to identify and mitigate malware
- Document and Collaborate
- **This is an arms race** — test and discover new tools and techniques

Tool List — Take-a-way

- Network Collection
- Malware Sandbox
- Host Collection
- Disk Forensics support
- Memory Forensics support
- Communications/Incident Management

FREE TOOLS AND LINKS

Network Forensics Tools
Solera Free VM - http://www.soleranetworks.com/solera-networks-vmware-support-statement/
Netwitness (free) – http://netwitness.com/products-services/investigator-freeware
Bro (application layer IDS) – http://www.bro-ids.org
Argus (flow tool) – http://qosient.com/argus

Live CD's
Helix – http://www.e-fense.com/products.php
DEFT linux – http://www.deftlinux.net/
CAINE – http://www.caine-live.net/
REMUX – http://zeltser.com/remnux/
Security Onion - http://securityonion.blogspot.com/

Quick Collection tools
SecCheckUI – http://sc.mynetwatchman.com/downloads/SecCheckUI.exe
Moonsols – http://www.moonsols.com/
BartsPE (for a clean windows environment) – http://www.nu2.nu/pebuilder/
Windows Forensics toolchest – http://www.foolmoon.net/security/wft/index.html
MIR-on-a-stick – MIR support
Mandiant Free tools – http://www.mandiant.com/resources/downloads

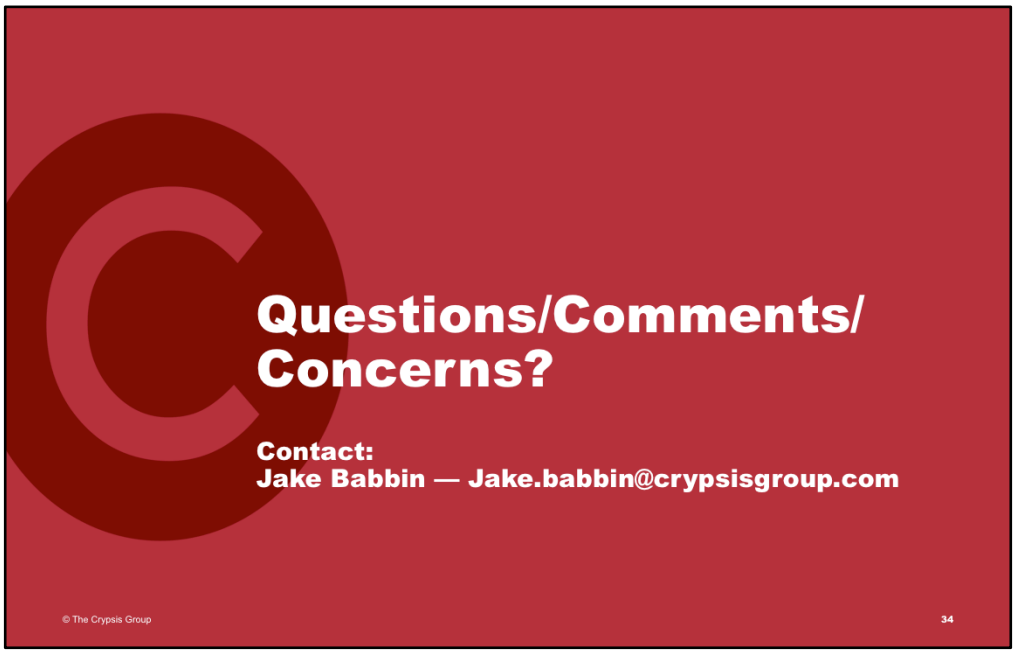
Volatile/RAM tools
Volatility – https://www.volatilesystems.com/default/volatility
mdd (Mantech DD) – http://sourceforge.net/projects/mdd/
Hbgary Fastdump (free) – http://www.hbgary.com/free-tools
FTK Imager - http://accessdata.com/support/adownloads#FTKImager
Encase commandline – need support license first

Drive Analysis tools
FTK Imager - http://accessdata.com/support/adownloads#FTKImager
Sleuthkit/Autopsy – http://www.sleuthkit.org/

Misc/Specific task tools
Dropbox forensics – http://computer-forensics.sans.org/blog/2011/06/17/digital-forensics-rain-drop-keeps-falling-on-my-box
Dropbox Reader - http://www.cybermarshal.com/index.php/cyber-marshal-utilities/dropbox-reader
Creepy (Geo-location tool for images) – https://github.com/ilektrojohn/creepy#readme
Watson (CEIC 2012 presentation – Identification of cloud services use on a machine) – http://www.cernam.com/watson

Documentation –
Notecase – http://notecase.sourceforge.net/ MAY BE NOTECASE PRO NOW http://www.notecasepro.com/features.php
Dradis – http://dradisframework.org/
AIRT – http://airt.leune.com/
CERTBE AbuseHelper - https://www.cert.be/pro/abusehelper
http://code.google.com/p/abusehelper/
WebJob: The Minimally Invasive Incident Response Framework! - http://webjob.sourceforge.net/WebJob/
Conceptboard - Realtime Teamwork & Collaboration Software - http://conceptboard.com/teamwork

others? -
Cisco Incident Response tool - http://cir.recurity.com/
grr - GRR Rapid Response is an Incident Response Framework - http://code.google.com/p/grr/
MIR-ROR: Motile Incident Response – Respond Objectively, Remediate - http://mirror.codeplex.com/
SILC – www.silcnet.org
Visual Understanding Environment - http://vue.tufts.edu/index.cfm
Xmind - http://www.xmind.net/index/


Questions/Comments/
Concerns?
Contact:
Jake Babbin — Jake.babbin@crypsisgroup.com
© The Crypsis Group
34