Malware Response Test

Infragard Meeting

Thursday 15 Nov 2012

Disclosure

- This is not an FBI constructed / sanctioned presentation.
- This is simply a “working practitioner” session between members of the Infragard program with the hope that others will benefit from this type of “knowledge sharing”
- One member came up with this and the BOD thought the collective would benefit
- We’re also really hard up for topics / speakers at the quarterly meetings

Malware CIRP Test

- Objective
  - Right people & processes?
  - Make decisions?
  - Perform various tasks in short timeframe?
  - Ad Hoc organization to deal with low probability – high impact risk?
- 30 Min per day
- 4 Days
- Scenario based

Malware CIRP Test

- Look & feel of real CIRP event
- Can we leverage other corporate best practices / organizations?
- Limitations
  - Can’t predict next Zero Day
  - Can’t predict next “attack”
    - But I have a scenario that I think is realistic (not shared by everyone)
  - Can’t take too much time / effort

Malware CIRP Test Schedule

- “Foreplay”
- Day 1- Warnings on the horizon
- Day 2 – It’s in the neighborhood
- Day 3 – We’re infected
- Day 4 – wrap up / Lessons Learned

Foreplay

- Malware CIRP Test Reminder e-mail
- Just wanted to remind everyone that next week is the Malware CIRP test. I will be sending out “notices” / e-mails throughout the weekend and next week to hopefully stimulate some thought and discussion around the existing plan/team/effort.
- I also wanted to make the collective aware of some recent news items that may play a role in next weeks ‘test’:

Recent Front Page WSJ

- The 10/13 Weekend edition of the Wall Street Journal – front page – reports that Iran has been linked to a series of recent Distributed Denial of Service (DDOS) attacks against the major US banks. The article states that Iran is providing financial and technical support to hacker groups responsible for the DDOS attacks.

Recent Front Page WSJ

- The article also mentioned that this same hacker group was responsible for releasing a virus called “Shamoon” that “destroyed” data on 30,000 computers belonging to the Saudi Arabian Oil company in July. Below is the Wikipedia entry for Shamoon:

Shamoon

- **Shamoon**,[a] also known as Disttrack, is a modular computer virus discovered in 2012 that attacks computers running the Microsoft Windows "NT" line of operating systems (it is not known to function correctly on Windows 9x/ME). The virus is being used for cyber espionage in the energy sector.[1][2][3] Its discovery was announced on 16 August 2012 by Symantec,[2] Kaspersky Lab,[4] and Seculert.[5] Similarities have been highlighted by Kaspersky Lab and Seculert between Shamoon and the flame malware.[4][5]

Shamoon

- The virus has been noted as unique for having differing behaviour from other malware cyber espionage attacks.[6] Shamoon is capable of spreading to other computers on the network, through exploitation of shared hard drives. Once a system is infected, the virus continues to compile a list of files from specific locations on the system, erase and then send information about these files back to the attacker. Finally, the virus will overwrite the master boot record of the system to prevent it from booting.[2]

Shamoon

- The virus has hit companies within the oil and energy sectors.[1][3] A group named "Cutting Sword of Justice" claimed responsibility for an attack on 30,000 Saudi Aramco workstations, causing the company to spend a week restoring their services.[7] The group later indicated that the Shamoon virus had been used in the attack.[8] Computer systems at RasGas were also knocked offline by an unidentified computer virus, with some security experts crediting Shamoon for the damage.[9]
- (http://en.wikipedia.org/wiki/Shamoon)

Foreplay

- On page A7 of the October 20 Contra Costa Times, an AP article “White House readies order to share cyberthreat information” states: “The Obama administration expresses growing concern that Iran could be the first country to use cyberterrorism against the United States.”
- The exercise will be “fake” but the items listed above are real.
- I look forward to speaking with all of you on Monday.

Monday

1st day of Malware CIRP Test

First E-mail notification

- EXERCISE - COMPUTER INCIDENT NOTIFICATION - EXERCISE
- The parties listed below are investigating a POSSIBLE malware outbreak.
- A Malware Outbreak is not currently in progress. This is an effort to anticipate and prevent an outbreak.
- Date/time: 10/29/12 @ 0800 PT
- Incident coordinator POC: Neal McCarthy cell: 925.123.4567
- Approving manager POC: Elwin Jones

First E-mail notification

- Source of detection/notification: CNN/FBI: Based on the recent US/Israeli military strikes on Iranian nuclear facilities, CNN is reporting of warnings from senior levels within the US government of an eminent ‘cyber attack’ on the US. FBI sources through the Infragard program are also confirming that companies should start taking protective measures and developing response plans for a cyber attack.

First E-mail notification

- Outbreak characteristics: Destructive in nature, self propagating, targeting US/Israeli (Western?) based computers, exploiting recent or even “zero day” vulnerability(ies) for the purpose of causing ‘significant harm’.
- Technical impact: Once infected, assume systems will no longer be operational and require extensive resources to be repaired/replaced.

First E-mail notification

- Business impact: Loss of IT capability may have a devastating impact on business operations
- Next Steps:
- -review of possible proactive & reactive options
- - Confirmation of appropriate parties involved with Malware CIRP (especially decision making.)
- Next update and Means: Mon 10/29/12 @ 1330 PT – 1-866-123-4567 pc 123456
- End of Message

Day 1 Malware CIRP Test Meeting

Monday 10/29/12 @ 1330

- EXERCISE -

Latest Update

- CNN/FBI: Based on the recent US/Israeli military strikes on Iranian nuclear facilities, CNN is reporting of warnings from senior levels within the US government of an eminent ‘cyber attack’ on the US. FBI sources through the Infragard program are also confirming that companies should start taking protective measures and developing response plans for a cyber attack.

Latest Update

- Outbreak characteristics: Destructive in nature, self propagating, targeting US/Israeli (Western?) based computers, exploiting recent or even “zero day” vulnerability(ies) for the purpose of causing ‘significant harm’.

Latest Update

- Technical impact: Once infected, assume systems will no longer be operational and require extensive resources to be repaired/replaced.
- Business impact: Loss of IT capability may have a devastating impact on business operations

Today's Objectives

- Consequence Management (High Level)
- Confirm adequacy of Malware CIRP
  - Decision Making capability
  - Sufficient participation
  - Adequacy of the CIRP
- Anticipate
  - Proactive measures
  - Reactive measures

Consequence Management

- What is the worst thing this “attack” could do (technical)?
- How do we prevent/detect/correct it?
- What is the worst thing that could happen to the company (Consequence)?
- How do we prevent/detect/correct it?

Confirm Adequacy of Malware CIRP

- Decision Making capability
- Sufficient participation/staffing
- Adequacy of the CIRP

Proactive Measures

- Back up data
- Ensure virus signatures are up to date
- Turn off systems when not in use
- Validate DR & BC plans
- Mobilize CIRP
- Heightened awareness of media and other “intel”
- Prepare for Reactive measures

Reactive Measures

- Containment Plans
  - Contain external sources
    - Internet
      - Most critical vs. least critical services
    - Remote access
    - Third party connections
  - Internal containment
    - Isolate by regions
    - Isolate retail from corporate HQ
    - Isolation within corporate

Reactive Measures

- Communications without e-mail
  - Corporate
  - District offices
  - “Overseas”
- Implementation of DR & BC
  - ID critical bus functions
  - ID most vulnerable functions (based on knowledge of attack)

Report of the 9/11 Commission

- **Imagination**
  The most important failure was one of imagination. We do not believe leaders understood the gravity of the threat. The terrorist danger from Bin Ladin and al Qaeda was not a major topic for policy debate among the public, the media, or in the Congress. Indeed, it barely came up during the 2000 presidential campaign.
- Al Qaeda's new brand of terrorism presented challenges to U.S. governmental institutions that they were not well-designed to meet. Though top officials all told us that they understood the danger, we believe there was uncertainty among them as to whether this was just a new and especially venomous version of the ordinary terrorist threat the United States had lived with for decades, or it was indeed radically new, posing a threat beyond any yet experienced.
- As late as September 4, 2001, Richard Clarke, the White House staffer long responsible for counterterrorism policy coordination, asserted that the government had not yet made up its mind how to answer the question: "Is al Qaeda a big deal?"
- A week later came the answer.

Day 2 Malware CIRP Test

Day 2 E-mail Notification

- EXERCISE - COMPUTER INCIDENT NOTIFICATION - EXERCISE
- The parties listed below are investigating a POSSIBLE malware outbreak.
- A Malware Outbreak is not currently in progress within the company. This is an effort to anticipate and prevent an outbreak.
- Date/time: 10/30/12 @ 1100 PT
- Incident coordinator POC: Neal McCarthy cell: 925.123.4567
- Approving manager POC: Elwin Jones

Day 2 E-mail Notification

- Source of detection/notification: CNN is currently reporting that a “Stuxnet” type of virus has been detected in the East Coast of the US. Although details are incomplete, the virus attacks windows based systems using previously undisclosed vulnerabilities via an e-mail based worm. The virus attacks the hard-drive of the system so that the computer is no longer able to access the information stored on the drive, rendering the system inoperable. US DHS is holding a press conference at 14:00 (PT). NO COMPANY OFFICES HAVE BEEN IMPACTED BY THIS VIRUS.

Day 2 E-mail Notification

- Outbreak characteristics: Windows based, Zero Day, Attacks hard-drive making system inoperable. Self-propagating via e-mail.
- Technical impact: Once infected, assume systems will no longer be operational and require extensive resources to be repaired/replaced.
- Business impact: Loss of IT capability may have a devastating impact on business operations
- Next Steps:
- Start formal Incident Response actions
- - Formalize assignments/roles

Day 2 E-mail Notification

- - decide on next steps
- - start tracking assumptions and tasks assigned
- - Notify senior management?
- - Initiate containment actions?
- - Develop “triggers” for future actions
- Next update and Means: Tues10/30/12 @ 1330 PT – 1-866-123-4567 pc 123456
- End of Message

Day 2 Malware CIRP Test Meeting

Tuesday 10/30/12 @ 1330

- EXERCISE -

Latest Update

- Source of detection/notification: CNN is currently reporting that a “Stuxnet” type of virus has been detected in the East Coast of the US. Although details are incomplete, the virus attacks windows based systems using previously undisclosed vulnerabilities. The virus attacks the hard-drive of the system so that the computer is no longer able to access the information stored on the drive, rendering the system inoperable. US DHS is holding a press conference at 14:00 (PT). NO CORPORATE OFFICES HAVE BEEN IMPACTED BY THIS VIRUS.

Latest Update

- Outbreak characteristics: Windows based, Zero Day, Attacks hard-drive making system inoperable. Self- propagating via e-mail.
- Technical impact: Once infected, assume systems will no longer be operational and require extensive resources to be repaired/replaced.
- Business impact: Loss of IT capability may have a devastating impact on business operations

Proactive Measures

- Back up data
- Ensure virus signatures are up to date
- Turn off systems when not in use
- Validate DR & BC plans
- Mobilize CIRP
- Heightened awareness of media and other “intel”
- Prepare for Reactive measures

Reactive Measures

- Containment Plans
  - Contain external sources
    - Internet
      - Most critical vs. least critical services
    - Remote access
    - Third party connections
  - Internal containment
    - Isolate by regions
    - Isolate retail from corporate
    - Isolation within coporate

Reactive Measures

- Communications without e-mail
  - Corporate HQ
  - District offices
  - “Overseas”
- Implementation of DR & BC
  - ID critical bus functions
  - ID most vulnerable functions (based on knowledge of attack)

What else?

- What aren’t we thinking about?
- Are we doing enough to protect our ability to make sales / generate revenue / service customers?

Day 3 Malware CIRP Test

Day 3 E-mail Notification

- EXERCISE - COMPUTER INCIDENT DECLARATION – MALWARE OUTBREAK – EXERCISE
- You are being notified that a MALWARE OUTBREAK IS OCCURRING and corporate resources will be required to support this incident.
- Incident summary: The Eastern division office has been affected by some sort of malware that has caused 15 of the systems to crash – creating the “Blue Screen of Death”. Local Field Services (IT) resources are unable to bring the systems back online without completely rebuilding the systems from scratch. None of the data on the drives has been recoverable. This is believed to be due to the “stuxnet” type virus currently being reported in the media.

Day 3 E-mail Notification

- Technical impact: Windows systems are being rendered inoperable.
- Business impact: The Eastern Division office has shut down all computer systems within the office. No impact is reported at any of the stores.
- Coordination conference call to be held at:
- Date 10/31/12
- Time 1330 PT
- Call in number 866-123-4567
- Passcode 123456

Day 3 E-mail Notification

- Incident coordinator POC: Neal McCarthy cell: 925.123.4567
- Approving manager POC: Elwin Jones
- Refer to the following items for additional information:
- The initial Incident Notification is attached to provide more details regarding the incident and efforts prior to making this declaration
- In order to access the corporate Computer Incident Response Plan (CIRP) for Malware Outbreaks, refer to the internal corporate site: http://collab.yourcompany.com/it/cirp/Malware%20CIRP/Forms/AllItems.aspx
- End of Message

Day Three
Malware Outbreak
- EXERCISE -

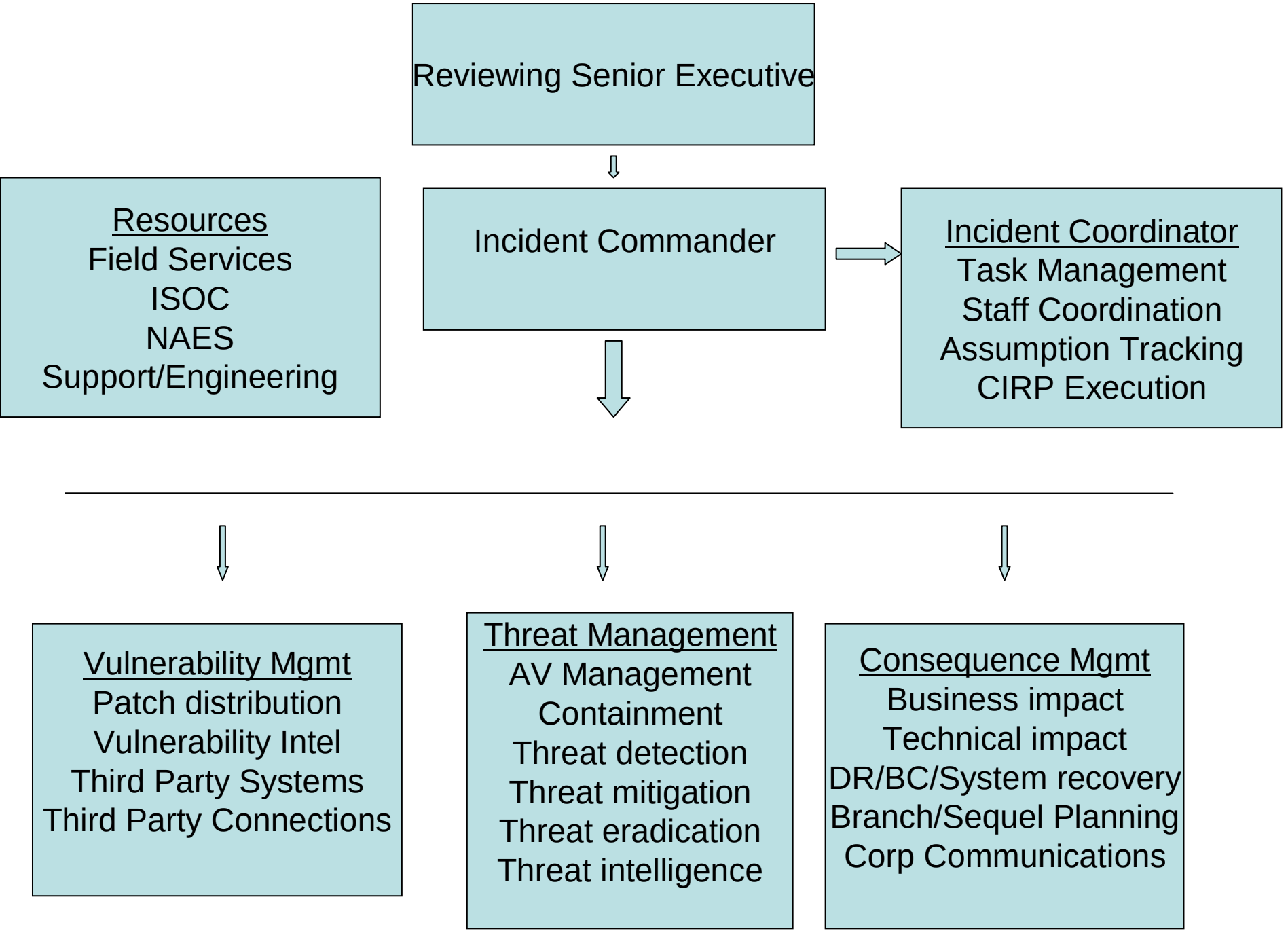
Status Brief
of
31 Oct 2012 / 1330 PT
- EXERCISE -

Status Brief Outline

- Updates:
  - Latest Media / Industry reports
  - Malware Response Assignments
  - Vulnerability-threat-consequence updates
  - Previously assigned tasks & assumptions
- Next Steps (Efforts)
- Incident Commanders input
- Next status brief
- Execute

Presentation Rules

- Presenters, Do not read your slides to the audience – if your audience cannot read – we're in big trouble. If you have to explain all your slides – you're in big trouble.
- The longer you take talking about what needs to be done, the less time you have to actually do it.
- New entries in red, repeat info in black
- Slides will be posted and available to everyone
- A brief where all that you hear is "next slide please" is a GOOD brief
- Get your slides in at least 15 min prior to the next brief


Reviewing Senior Executive
Resources
Field Services
ISOC
NAES
Support/Engineering
Incident Commander
Incident Coordinator
Task Management
Staff Coordination
Assumption Tracking
CIRP Execution
Vulnerability Mgmt
Patch distribution
Vulnerability Intel
Third Party Systems
Third Party Connections
Threat Management
AV Management
Containment
Threat detection
Threat mitigation
Threat eradication
Threat intelligence
Consequence Mgmt
Business impact
Technical impact
DR/BC/System recovery
Branch/Sequel Planning
Corp Communications

Assigned Roles

- Incident Commander: Steve Jones
- Reviewing Senior Executive: ?
- Incident Coordinator: Neal Jones
- Vulnerability Manager: Kevin Jones?
- Threat Manager: Nathan Jones
- Consequence Manager: Amy Jones

Media / Industry Updates

- As of 10/31/12 @ 1330 PT
- CNN: Virus is believed to be work of same folks responsible for extensive DDOS attacks on major US banks - Izz ad-Din al-Qassam Cyber Fighters,
- CNET: Virus initially propagates as e-mail worm with malicious attachment (Phishing)
- CNET: Once on machine spreads via shared drives

Media / Industry Updates (Cont.)

- CNN reports a vulnerability with “Windows Update” service that has not been released/patched by Microsoft
- Appears to only affect US windows PCs
- Calls to AV vendor have not been answered (everybody else is calling them too)
- Media / Industry reports have not been verified and may be speculative or incomplete

Vulnerability Update

- Exploited Vulnerability: Recent media reports “think” it is a new vulnerability with the Windows Update function.
- Patch/remediation info: Awaiting info from AV vendor / media
- Corrected systems:
- Vulnerable Systems: US Windows platforms
- Vulnerable third party systems:
- Third party network connections:

Threat Update

- Description of threat:
  - What does it do? Makes Hard drive Inoperable
  - How does it work/mature? Unknown
- SWY AV Status: Current w/ known vulns
- Threat signatures/indicators: BSOD
- Additional Info on the threat: Current media reports: Phishing e-mail w/ malicious attachment, once opened spreads within network leveraging shared drives
- Threat info is current as of: 10/31/12 @ 1330 PT

Consequence Update

- Current Business impact of threat: Eastern division office shut down
- Current technical impact of threat: Unknown
- Current Business impact of response: None
- Current technical impact of response: None
- Probable business impact with current approach: Unknown
- Any significant business concerns: Do not allow to impact retail operations

Previously assigned Tasks

- Task title – assigned to – due

Current Assumptions

- Summary – assigned to
- Existing spam/Phishing technology will block e-mail propagation – Nathan
- Retail sites protected via PCI measures and not at risk - Nathan

Planning Guidance

- From the textbook
  - Prioritize the handling of the incident based on its business impact (consequence).
  - Containment takes priority over eradication and recovery

Vulnerability Mgmt Efforts

- Tasks necessary to remediate vulnerability
  - Start rolling out patches once known
- Are current efforts sufficient
- Next steps
- Issues/roadblocks – Patches Unknown

Threat Mgmt Efforts

- Tasks necessary to remediate threat
  - Propagation – Block E-mail? Containment?
  - Mitigation Unknown
  - Detection Look for network spikes? Phishing e-mail “signature”
  - Eradication FS onsite rebuild
- Are the current efforts sufficient
- Next steps
- Issues/Roadblocks Need more info

Consequence Mgmt Efforts

- Current efforts to reduce/mitigate effects on the business
  - Containment Prevent from spreading to Corporate and especially stores
  - DR/BC/System Recovery
  - Manual/back-up processes
  - Tolerance/co-existence w/ malware NO
- If current efforts unsuccessful – what should we do Protect Retail/stores at all cost
- Do we need to notify anybody?

Incident Commanders Guidance

- Are we on the right track
- What information do we need to know and don’t currently have
- What additional tasks need to be assigned
- Expectations by the next status brief
- Contact the Incident Commander/Task Force ASAP if any of the following occur:

Next Status Brief

- When Thursday 11/1/12 @ 1330 PT
- Where 866-123-4567 pc 123456
- Send slide input at least 15 minutes prior to Neal.McCarthy@yourcompany.com
- These slides can be accessed online at:

So, how did it go?

- Identified major gaps in our ability to make “hard” decisions – especially with significant business impact(s)
- Need to “normalize” better with current ‘production outage’ process/team
- “Fight the enemy (virus), not the scenario”
- Are we too trusting/dependent of our technologies (that the bad guys have too)?
- Work in progress