Investigator of Interest –
Our Philosophy of Adaptive Incident Response
Pascal Arends, FoxCERT
• Pascal Arends

• pascal.arends@fox-it.com
• cert@fox-it.com
• +31 15 284 79 99
• +31 800 FOXCERT (24/7)
Topic:

- Why Adaptive Incident response
- What is Adaptive Incident Response
- Defining your investigation strategy
- Tips and Tricks
The spying program
They know everything

• Your mail server is being tapped!
• They have access to your chat server!
• They are listening on your system!
Nothing to see here move along

- A lot of communication before the investigation
- Attacker can easily monitor this with an automated system
- He knows the indicators you are looking for and use these as keywords for spying on you
Adaptive Incident Response
Adaptive Incident Response

- Cyber threat landscape
- Incident information
- Attacker profile
- Business impact
Running scared

• Keep the investigation noise down
• The attacker will not run at first sight of an investigation
• Advanced attackers are in your network for the long run
• He has to maintain a lot of systems to.
• The investigator and attacker have a information gap, speculation is needed.
Adaptive IR defining your investigation strategy
Scoping

- Fact finding
  - Investigation motivation
  - Investigation leads
Scoping

• Attacker profiling
  – Analyze all the facts/information
  – Make hypotheses

• Which is the more likely hypothesis
  – Bored kid or Espionage
  – Could it be an activist/hacktivist
Scoping

- Threat landscape
  - Who are your enemies
  - What can they get (Crown-Jewels)
  - External exposure
Investigation questions

- What happened
- Is it targeted
- What has been stolen
- Who did it
- How return to business-as-usual (fast)
Business-as-usual considerations

• Management Doesn’t want to hear anything about BAU not being top priority

• With BAU being highest priority they don’t see the full extent of the breach, what information the attacker has, in what stage the attacker is.

• At the end the business cannot give a complete picture to the stake-holders
Business-as-usual considerations

(Short term) Reasons not going back to BAU:
• (Better) Attacker profiling
• What is the attacker searching for
• What does the attacker know
• In what stage of the attack are they
• Targeted or not
Business-as-usual considerations

(Long term) Reasons not going back to BAU:

• Better remediation
• More lessons learned
• Better defenses for possible upcoming breaches
Determining the strategy

• Combine the gathered information
  – Investigation facts
  – Attacker profile
  – Hypotheses
  – Threat landscape
  – Business impact
Intrusive VS Non-Intrusive investigation

• Intrusive advantages:
  • Faster
  • Smaller group has to know details

• Intrusive disadvantages:
  • Attacker can easily detect the investigation
Intrusive VS Non-Intrusive investigation

• Non-intrusive advantages:
  • Monitor the attacker
  • Better remediation
  • More lessons learned/ better prepared next time.

• Non-intrusive disadvantages:
  • Slower
  • More employees need to know details
Noise level Non-intrusive investigation
Noise level (typical) breach
Turn the table
Out-Of-Band communication

• Don’t use production communication channels

• Use separate investigation machines

• Use a back-up internet line?

• Use a out of band document exchange portal
Hide the noise

- The idea is to make as little noise as possible during the investigation, hide in normal day-to-day routines.
  - Use out-of-band sources
  - Use admin tools
  - Use maintenance windows
  - Pull disks (RAID setup?)
  - Use passive network monitoring
Network investigation

High noise
• Software on the host

Medium noise
• TAP/HUB

Low noise
• Switch SPAN
Host acquisition

**High noise**
- Live acquisition
- Installing agents
- Running scripts

**Medium noise**
- Offline acquisition
- Using installed agent

**Low noise**
- Pulling disks (RAID1)
- Make VM snapshots
- Getting information out of backups
- Using maintenance window
Host investigation

High noise
• Live investigation

Medium noise
• Using installed agent
• Retire a system (for live investigation)

Low noise
• Offline investigation
Malware investigation

High noise
- Online research
- Dynamic analysis w. Internet

Low noise
- Static analysis
- Dynamic analysis no internet
Log investigation

High noise
• Live log investigation
• Collect logs through scripting/agents

Low noise
• Pre installed central log collector
Readiness

• Have a data acquisition plan
• Have a central log collector
• Have the backup schema
• Have a SPAN-port available on switches
• Know your Threat landscape
• Talk with the MT about investigation strategies
• Have out-of-band communication channels
If you want to stay off your attackers radar, hide!!

And make the attacker become the defender
Questions?

- pascal.arends@fox-it.com
- cert@fox-it.com
- +31 15 284 79 99
- +31 800 369 23 78 (24/7)