An Introduction to Incident Detection and Response

Memory Forensic Analysis

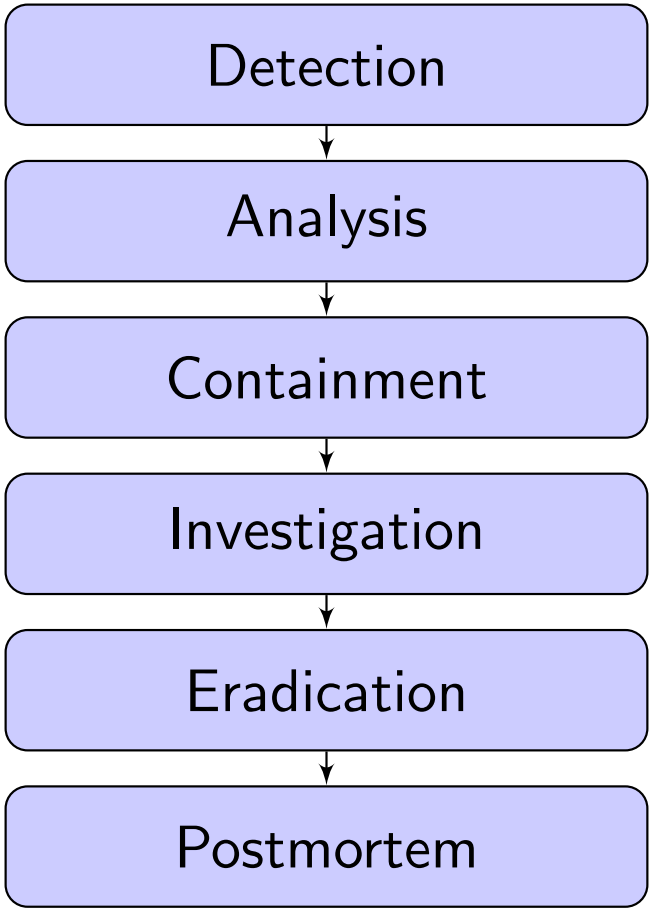
CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy -
TLP:WHITE

a@foo.be

February 6, 2015

An overview to incident response



Detection (the most common)

- External indicators (e.g. IOCs[1] shared with third-parties.
- Anomalies detected by internal or external people to the organization.
- Performance or stability anomalies detected internally.
- FP[2] incidents usually cross-checked via various sources.
- (careful) Analysis of logs produced by network or security devices/software.

[1] CIRCL MISP

[2] False positives

Detection means gathering, checking and data mining

- Minimal internal team is required to ensure the adequate detecting within your organization.
- Ticketing software (e.g. RTIR) is required to track down incidents/indicators.
- The internal team can rely on "Public Resource Teams", "Internal Teams" and "Commercial Teams" to operate.

Detection - how to deal with false positives?

If you receive an indicator detecting a potential incident, we have no guarantee to be accurate.

- Collecting the incident reports in a ticketing system helps to reduce the time to process FP events.
- Sometime the event itself is accurate (e.g. a server is no more responding) but does not lead to a security incidents.
- It's not uncommon to have an event (initially classified as FP) to become a real incident after some times.

Increase detection rate (and reduce analysis time)

Profiling networks and systems is a way to measure expected profile of running systems.

- File integrity check (e.g. default binaries checksum of internal software) is critical to detect unknown binaries and improve analysis time.
- Network profiling (e.g. bytes over time) of internal systems.
- Understand and define normal behaviors of networks, systems or applications (e.g. Which TCP ports are used by your internal software?).
- Keep logs[3] is critical especially that incidents may not discovered before months.

[3] log retention policy

Analysis - The Order of Volatility (OOV)

The expected life-time of data :

Type of Data	Life Span
Registers or cache	Nanoseconds
Main Memory	Ten Nanoseconds
Network State	Milliseconds
Running Processes	Seconds
Disk	Minutes
Backup Medias	Years
CD-ROMS or printouts	Tens of years

Sometimes a small process trace can explain more than 50 gigabytes of a single backup...

Incident Analysis - Theory

- Broad definition of (computer) forensic analysis : *"Forensic analysis involves the preservation, identification, extraction, documentation and interpretation of computer data"*
- *To reach those goals, the forensic specialists follow clear and well-defined methodologies. Flexibility is highly required when encountering the unusual.*

Incident Analysis - Methodology

- Acquire the evidence without altering or modifying the original source.
- Authenticate that you gathered the evidence in a proper way.
- Analyze the non-original collected data without modifying it.

Gathering evidence: memory acquisition

- If the system is **not** running, recovering hibernation file/crash dumps/pagefiles from disk.
- If the system is running and accessible, acquire memory with win32dd/win64dd (or DumpIt or KnTDD).
  - win32dd.exe -I[0—1] memory.dump
  - dumpit.exe
- If the system is running but not accessible, hardware techniques using Firewire/DMA access limited to the first 4GB of memory.

Gathering evidence: memory acquisition - remote acquisition

- Systems are not always physically accessible.
- Some of the tools can save to a share the memory dump or use an encrypted network tunnel (e.g. over SSH).
- Remote acquisition over the network is not always recommended.
- Remote access and storing the raw dump file locally is an acceptable solution.

```
1 psexec.exe \\remotesys -e -w c:\ c:\\win32dd.exe c:\\
      winlocal.raw
```

Memory acquisition of virtualized systems

- VMware ESX (and related products)
  - .vmem, .vmss and .vmsn files need to be collected for memory analysis.
- VirtualBox
  - via the debugvm command (vboxmanage debugvm dumpguestcore –filename dump.elf)
  - strip elf part to get raw data

```
1 head -c $(($size+$off)) dump.elf | tail -c +$(($off+1)) >
      dump.raw
```

Gathering evidence: memory acquisition - risks

- Memory acquisition is performed with administration privileges.
  - If the system is suspicious (and infected), the credentials used might be abused/gathered by the attacker.
- Still better than user-space tools like Process Explorer (e.g. malware rootkits).
- Don't do acquisition when huge processes are running in memory (e.g. AntiVirus full scan, disk indexing,...).
- Don't forget that some malware know about memory acquisition tool.
- Disk acquisition should be done just after memory acquisition (comparing disk/memory is useful).

Analysis of the evidence: memory analysis

- Unstructured analysis (e.g. grep, strings) $\rightarrow$ easy for analysis checking but out-of-context.
- File carving $\rightarrow$ quick extraction of contiguous data for files or executables.
- Structured analysis $\rightarrow$ interpretation of operating system data structure, kernel-user space separation.
  - Volatility[4], Mandiant Redline.

[4] https://code.google.com/p/volatility/

Installing volatility

- https://github.com/volatilityfoundation/volatility
- git clone https://github.com/volatilityfoundation/volatility.git
- cd volatility
- python vol.py (pip install the missing packages)

Image profile

- python vol.py –info
- python vol.py imageinfo -f your.dump
- python vol.py –profile=WinXPSP3x86 shellbags -f your.dump
- python vol.py –profile=WinXPSP3x86 pslist -f your.dump
- python vol.py –profile=WinXPSP3x86 userassist -f your.dump

Malware analysis - complexity

- What's the exact definition of a malware? (from remote access tool to custom payload used in targeted attacks)
- Malware are not only payload on Windows machine (but also active malicious javascript, repurposed software, bundle software, ...)
- It's context dependent.

Malware - analysis

During the memory or disk forensic, various suspicious files were found and could be malware. Two different approaches can be used:

- Static analysis
  - File characteristics (Known operating system file? meta-information?)
  - Result from multiple A/V detection
  - Results from dissasembly
- Dynamic analysis[5]
  - Executing malware in a controlled environment to understand the behavior during runtime
  - Logging API calls
  - Intercepting and logging network access
- Usually a combination is used to overcome limitation of dynamic and static analysis (e.g. Anti-VM/debug, Turing's Halting problem, target specific requirements...)

[5] CIRCL DMA access