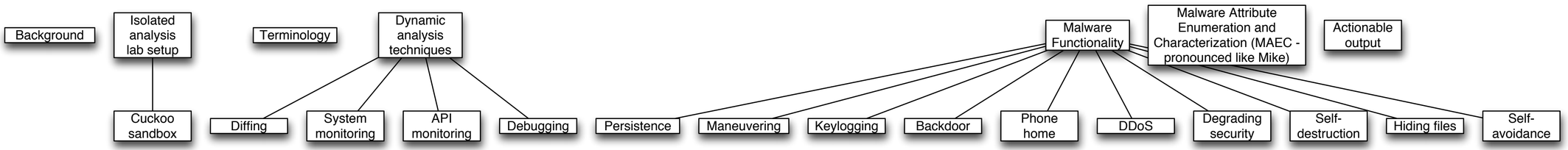
Malware Dynamic Analysis
Medium-granularity class topics covered
Veronica Kovah
CC BY AT licensed
hosted at OpenSecurityTraining.info



Malware Dynamic Analysis
Fine-grained/by class topics covered
Version 1 Kandel
CC BY Attributed
hosted at OpenSecurityTraining.info

- Backtrack1
  - Identifying file types
    - Portable Executables (PE) overview
      - Packed executables
  - Processes (dynamic linking)
    - Viewing running processes (lab)
    - Viewing DLL dependencies (lab)
  - Threads
  - Windows registry
    - Viewing registry entries (lab)
  - Windows services
    - svchost.exe
      - Viewing svchost services (lab)
    - Viewing running windows services (lab)
    - Viewing all windows services (lab)
  - Networking review
    - Inspecting packet capture (pcap) with Wireshark (lab)
    - Monitoring process network activity (lab)
- Isolated malware analysis lab
  - Virtualization hypervisor configuration
  - Linux host OS setting
    - Capturing packets between VMs (lab)
    - Using iptables to simulate network services to fool malware (lab)
- Malware Terminology
  - Bot
  - RAT
  - Downloader
  - Dropper
  - Spyware
  - Adware
  - Ransomware
  - Vendor malware naming conventions (and why they suck)
- Example RAT analysis
  - IR server creation (lab)
  - IR client creation (lab)
    - IR client (lab)
- Dynamic analysis fundamentals
  - Offline
    - Negative exe
    - Autoruns.exe
  - System Monitoring (dedicated programs for file, registry, process/thread, process/exe, net)
    - ProcessMonitor.exe (procmon)
    - Wireshark.exe
  - API tracing
    - WinAPIOverride32.64.exe
    - RohitLab API Monitor
  - Automating
    - IDA Pro
    - OllyDbg
    - Immunity Debugger
    - WinDbg
- Detecting persistence mechanisms
  - Autoruns.exe (lab)
    - How does Autoruns persist? (malware lab)
  - Common registry keys
    - How does Hydrabag persist? (malware lab)
  - Persistence through filesystem locations (lab)
    - Example use of "Image File Options" registry key (lab)
  - Observing IMAGINT with Regshot (malware lab)
  - Observing Hydrabag with Regshot (malware lab)
  - OLLVcode injection
    - Applnit_DlLs registry key
      - How does IMAGINT persist? (malware lab)
    - Observing Parkers malware using Regshot (malware lab)
    - Observing Ontmalgamer's rootkit using Regshot (malware lab)
    - Observing Ontmalgamer's rootkit using Regshot (malware lab)
    - DLL search path hijacking
    - Asynchronous Procedure Call hijacking
    - Checking Knowing.dll (lab)
    - Observing Nitol's malware using with ProcMon (malware lab)
    - CreateRemoteThread() - Win32 API
      - Codecave (injecting asm directly and then redirecting control with SetThreadContext() Win32 API)
    - SetWindowsHookEx() - Win32 API
    - IAT/EAT hooking
      - Inline hooking
- Obfuscating
  - Many other techniques not covered in this class due to time. E.g. screen capture, password dumping, keylogging, packet capture, stealing information, encrypting files, etc.
  - Keylogger malware using SetWindowsHookEx() Win32 API (malware lab)
    - Replacing dictionary (sethc.exe) with cmd.exe (lab)
      - Darkshell command & control (C2) monitoring (malware lab)
        - Darkshell C2 decryption (lab)
    - Send fake DDoS instruction to Darkshell (malware lab)
  - Malware Techniques
    - Anonymizers
    - Backdoor
    - Phone home
    - Distributed Denial of Service (DDoS)
    - Degrading Security
      - Disable security applications
      - Degrade security configurations
      - Disable updates
      - How is SpyEye degrading security? (malware lab)
      - How to corrupt degrading security? (malware lab)
        - How to run standalone DLLs (see above, not in class, but very important artifacts)
    - Self-instruction
      - How do Hydrabag & DarkShell delete themselves? (malware lab)
      - Capturing deleted files with CaptureBat.exe (malware lab)
      - How does AMXcom hide its files? (malware lab)
      - Viewing file attributes in ProcMon (lab)
    - Hiding files
      - How does Poison try avoid double infection? (malware lab)
    - Self-persistance
      - Anti-VM functionality
        - Use RemoteExec.exe for injection into processes
        - How to run standalone DLLs
          - Use rundll32.exe to call an exported function name to call, use C++ Explorer.exe to view exports
- Using an automated malware sandbox
  - Cuckoo Sandbox
    - Yara signatures
      - Agobot embedded strings signature
    - Short signatures
      - Dyndnsbot beaconing signature (lab)
    - Configuration data
    - Poison try analysis (malware lab)
      - Analyzing results (lab)
    - Perlite analysis (malware lab)
    - Nitol analysis (malware lab)
    - AMXcom analysis (malware lab)
- Malware Attribute Enumeration and Characterization (MAEC) announced via Mitre
- Actionable malware analysis