20 - Malware Behaviors 2

Persistence
Privilege Escalation
Rootkits
Persistence – Windows Registry

- **Popular registry key to update:**
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- Many other persistence registry locations.

- Monitor registry changes during dynamic analysis. Regshot, ProcMon, CaptureBAT, etc.

- Other registry entries: AppInit_DLLs, Winlogon, SvcHost_DLLs.
Persistence - AppInit_DLLs

- Key appears in
  
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

- Value is a list of DLLs.

- These will be loaded into any process that loads User32.dll.

- Malicious dlls can be inserted into the list

- DLLMain will check to see if loading process is suitable for executing malware behavior.
Persistence – SvcHost DLLs

- **Svchost.exe**: generic executable for running services that run from dlls.
- Groups of services defined in
  
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

- Services defined in
  
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ServiceName

- Malware will often reuse an existing service group or overwrite a noncritical service.
Persistence – Trojanized Binaries

• Malware may patch a system binary to force extra (malicious) code to run.

• Often code at the beginning of a function will be overwritten by a call/jump to extra code followed by a return/jump to the next instruction.

• Code may include a pusha to store registers.
Persistence – DLL Order Hijacking

• Windows has default search order of directories containing DLLs unless process uses KnownDLLs protection method.

• This order puts the current directory of the application at the head of the list.

• Examples: iexplore.exe loads ntshrui.dll from ...\Windows\System32 but if a different ntshrui.dll is placed in ...\Windows, it will be loaded instead.

• Many executables are susceptible.
Privilege Escalation

- Most users run with Administrator privileges. Malware writers appreciate their service!
- The book states the majority of privilege escalation methods are “zero-day attacks … many of which can be found in the Metasploit framework.” This is incorrect as anything in Metasploit is no longer zero-day!
- SeDebugPrivilege allows admin users to do system level debugging, giving LocalSystem account access. You'll see calls to OpenProcessToken, LookupPrivilegeValueA, and AdjustTokenPrivileges.
Rootkits

- A rootkit will modify system functionality to obscure its presence.

- Import Address Table (IAT) hooking
  - Import address table provides addresses of system functions (book example `TerminateProcess`)
  - IAT hook will identify current address, replace with its own code that provides special behavior in some cases (don't allow malware to be terminated) and pass control to the normal system code for other cases.
  - Easily detectable (if you make the effort)

- Inline hooking
  - Instead of changing function address, change function code
Next Time

- Read PMA Chapter 12 (Covert Malware Launching)
- Do the Chapter 11 exercises!