28 – Anti-Virtual-Machine Techniques

Why Rage Against the (Virtual) Machine
VMware Artifacts
Bypassing VMware Artifact Searching
Vulnerable Instructions
Red Pill
No Pill Technique
Phatbot
str Instruction Method
Recap
VM Escape
Why Rage Against the (Virtual) Machine?

- Honeypots, online virus scanners, and malware researchers often use VMs.
- Purveyors of malware may want to make sure their code is not able to be caught doing what it does best.
- Popularity of anti-VM is waning because many targets now deploy VMs. (If all it took to be malware free would be to run a VM, everyone should run a VM—or at least pretend to do so.)
- Anti-VM techniques usually target VMware.
VMware Artifacts

• Several notable processes can be detected: `VmwareService.exe`, `VmwareTray.exe`, `VmwareUser.exe`
• See what this does if you are running in a VM:
  
  ```
  net start | findstr VMware
  ```
• MAC address of VMware hosts starts with 00:0C:29 by default.
• Countermeasures:
  - Patch strings starting containing substring `VM`
  - Change MAC address
  - Patch code checks
  - Uninstall or net stop “VMware Tools Service”
Bypassing VMware Artifact
Searching

• Process list searching will usually involve calls to
  – CreateToolhelp32Snapshot
  – Process32First
  – Process32Next

• Can patch the searched string or the control flow

• Process may also search memory for occurrences of the (sub)string VMware.
Vulnerable Instructions

- VMware interprets some privileged instructions in kernel mode, but runs user mode instructions directly on the processor but traps instructions that interact with hardware. A few instructions access hardware information but don't cause interrupts.

- These will behave slightly differently in a VM: sidt, sgdt, sldt, cpuid because the VM will store different information in the registers they consult and no interrupt is generated to allow the VM to know it needs to patch the returned information.
Red Pill

- Executes `sidt` instruction to get value of the IDTR register.
- Key code:
  ```
  sidt  fword ptr [eax]
  mov   al, [eax+5]
  cmp   al, 0FFh
  jmp   short loc_401E19
  ```
- 0xFF is start of the base memory address which VMware always sets fo 0xFF.
- Doesn't function correctly on multi-core machines because each processor has unique IDT.
- Countermeasures
  - Use multicore machine
  - Modify instructions
No Pill Technique

- **Uses** `sgdt`, `sldt`, and `smsw` for greater reliability.

- LDT structure location on host machine will be zero but is nonzero on virtual machine unless Acceleration is disabled in the VM Processor settings.

- If `sgdt` and `sldt` fail to show presence of a VM, the high order bits returned by `smsw` are inspected.
Phatbot method

- VMware uses virtual I/O ports to communicate to host OS for copy/paste, etc. Phatbot uses this as follows:

```
    mov  eax, 'VMXh'
    mov  ebx, [ebp+var_1C]
    mov  ecx, 0xA
    mov  dx, 'VX'
    in    eax, dx
    ...
    mov  eax, [ebp+var1C]
    cmp  eax, 'VMXh'
```

- 'VMXh' = 0x564D5868 is a magic number used by VMware to insure communication is intended.
- 0xA is a parameter to request the VMware version type
- 'VX' = 0x5658 is the port used by VMware to communicate with host OS
- If request succeeds, value of eax on call is echoed to ebx on return.
str Instruction Method

- str retrieves the segment selector from the task register which points at the *task state segment* (TSS) of the currently executing task.
- If the first two values contained in the TSS are 0x40 and 0x14 respectively, then VMware is being used.
- Countermeasures:
  - Use multiprocessor machine
  - Patch code
Recap

• If you see any of these instructions:
  - sidt
  - sgdt
  - sldt
  - smsw
  - str
  - in
  - cpuid

  you should suspect that VM detection is being used and inspect the surrounding code carefully.

• ScoopyNG implements all checks we've discussed.
VM Escape

- VMware is software running on your machine and hence, it may be vulnerable to exploit.
- Features that enhance Host/Virtual machine communication are one source of vulnerability, so it's generally best to disable shared folders.
- Cloudburst exploited a vulnerability in the 3D code of VMware's virtualized video device.
- Always use the most recent version of VM software available to you.
Next Time

• Exercises! Exercises! Exercises!