恶意代码分析与防治技术

第4章 虚拟机技术

王志
zwang@nankai.edu.cn

updated on 2022-10-16

南开大学 网络空间安全学院

2022-2023学年

Outline

- The Structure of a Virtual Machine
- Create a Virtual Machine
- Use a Virtual Machine
- The Risks

The Structure of a Virtual Machine

- Fresh malware can be full of surprises.

Dynamic Analysis

- Running malware deliberately, while monitoring the results
- Requires a **safe environment**
  - Quickly spread to other machines on the network
  - Air gap – no connection to Internet or other PC
  - Very difficult to remove

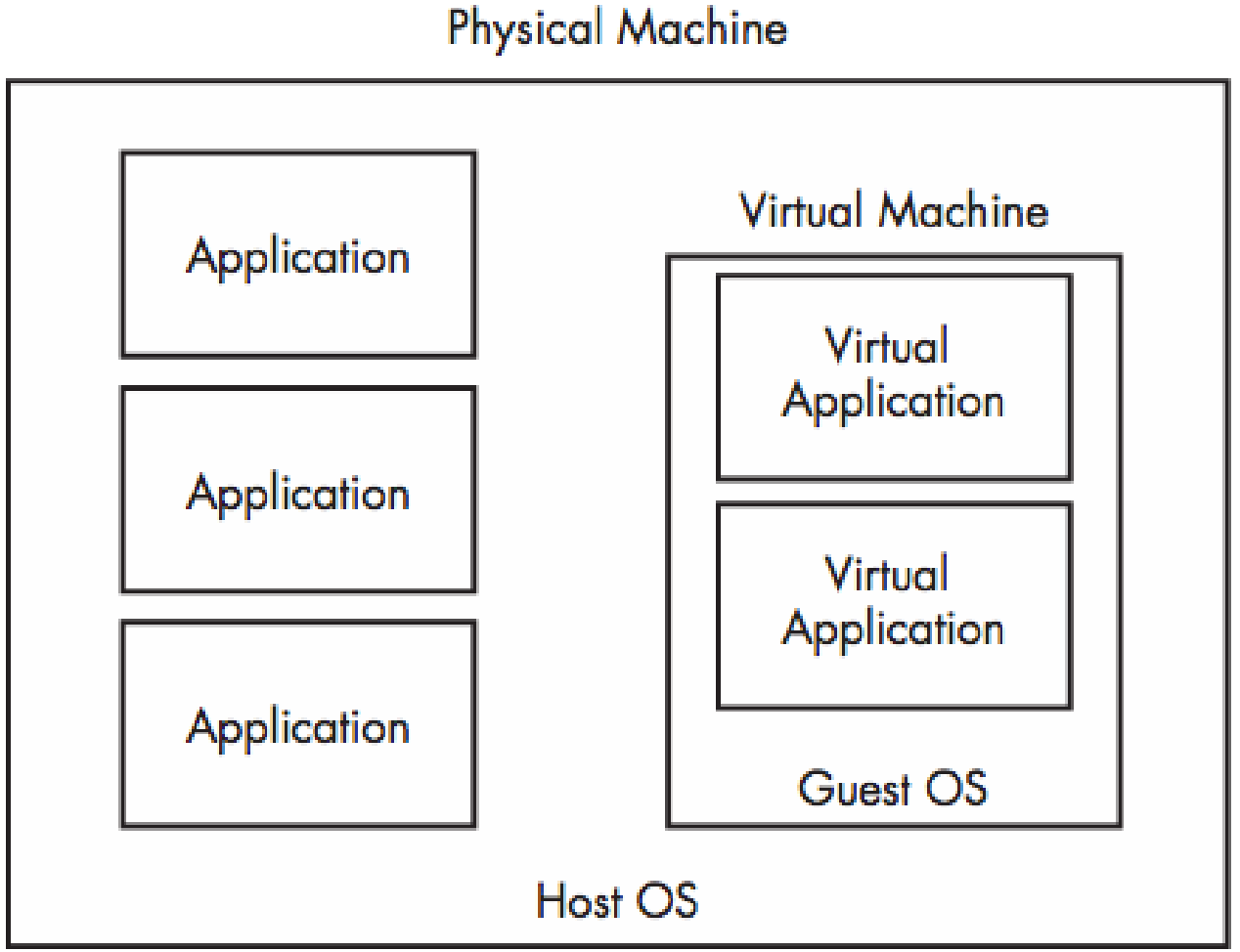
Physical Machines

- Disadvantages
  - No Internet connection, so parts of the malware may not work
  - Can be difficult to remove malware, so re-imaging the machine will be necessary

Virtual Machines

- The most common method
  - completely isolated
- This protects the host machine from the malware
  - Except for a few very rare cases of malware that escape the virtual machine and infect the host

VM Structure



VMware Player

- Free but limited
- Cannot take snapshots
- Cannot clone or copy VM
- VMware Workstation or Fusion is a better choice, but they cost money
- VirtualBox, Hyper-V, Parallels, or Xen.

Create a Virtual Machine

Configurations

- Disk
  - enough to store the guest OS and tools for malware analysis
  - 20 GB hard drive
  - Resizable

Configuration

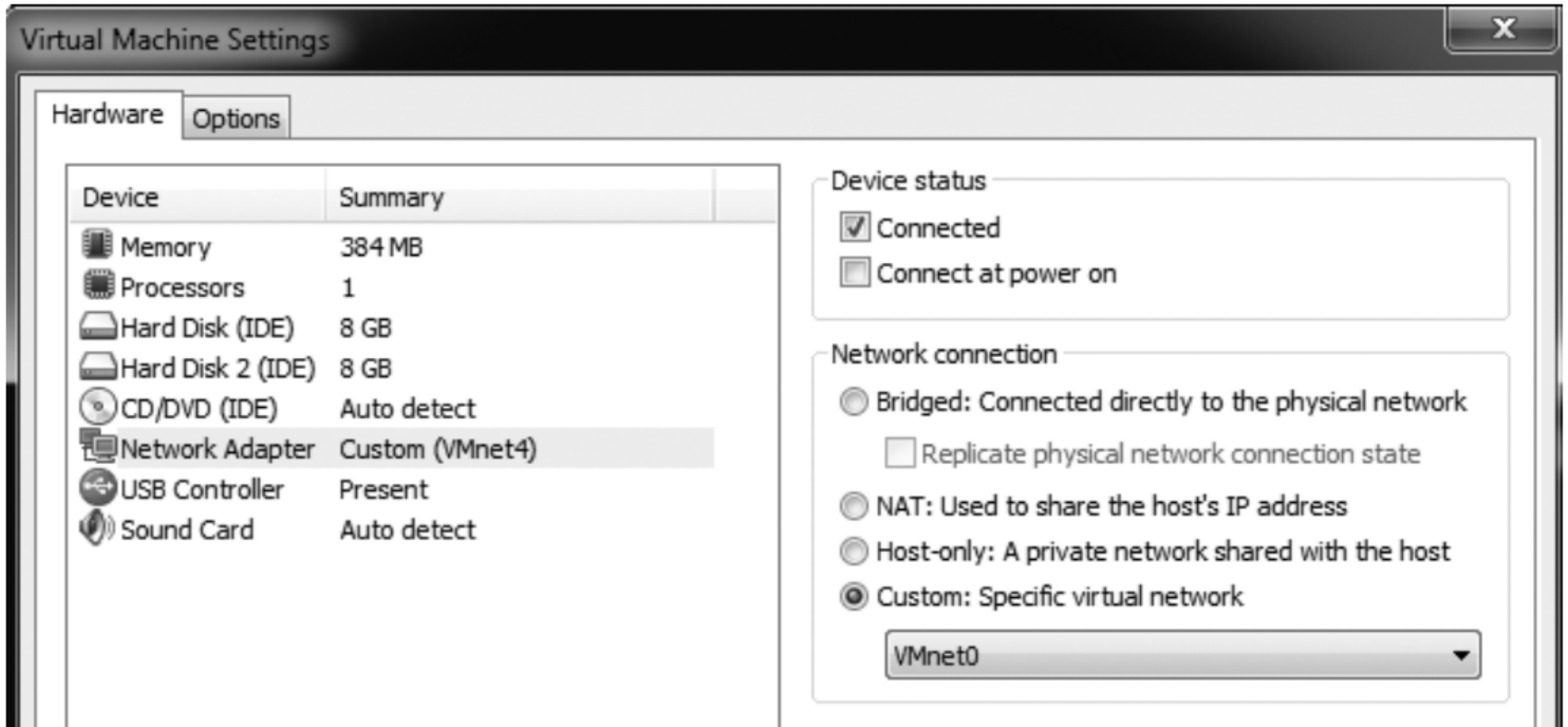
- OS
  - Windows XP is still the most popular OS (Surprisingly)
  - The malware we are analyzing targets Windows XP, as most malware does
  - New programs are compatible to older system
  - We focus our explorations on Windows XP

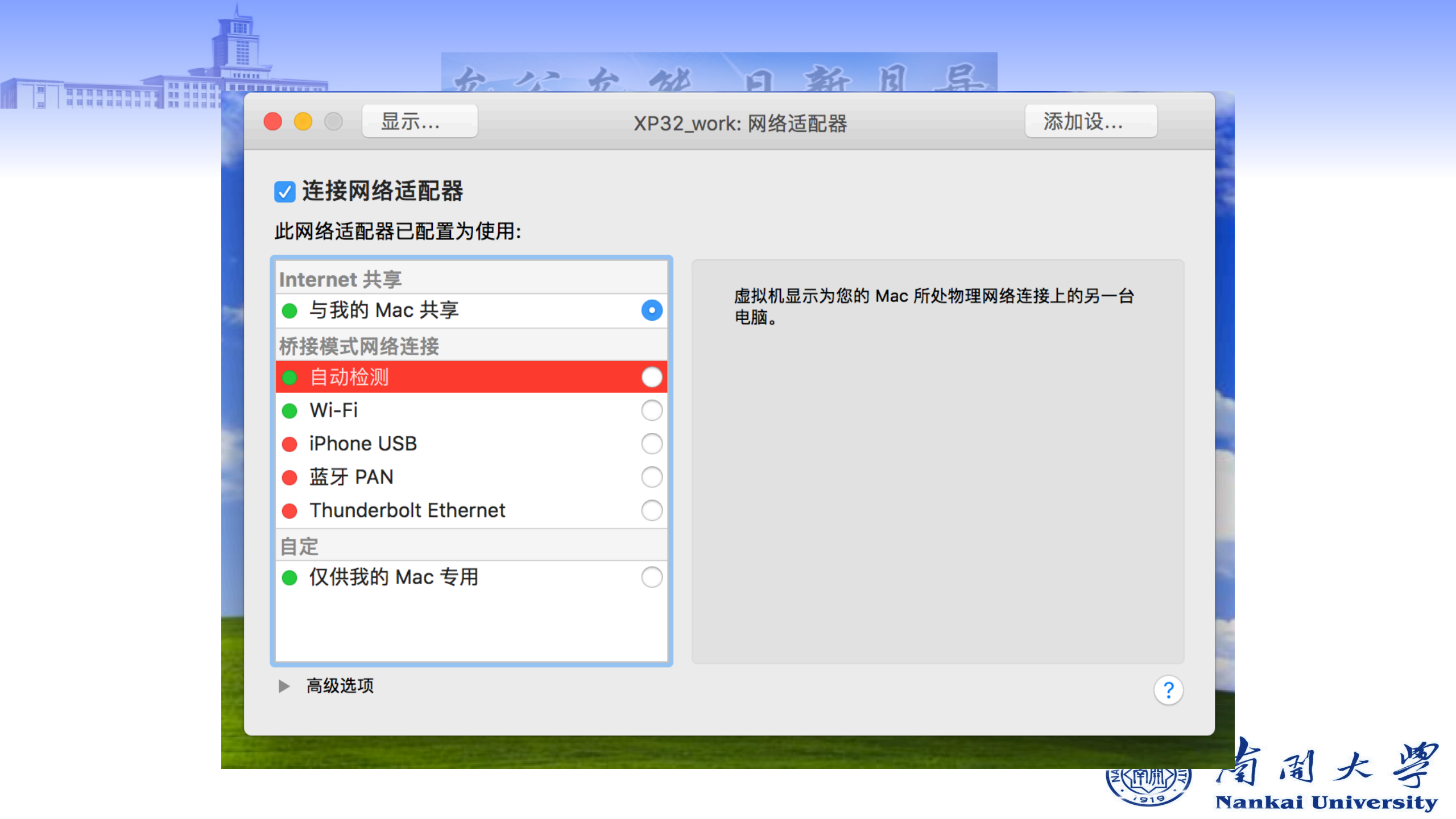
Configuration

- Application
  - VMware tools
  - tools for malware analysis
    - IDA Pro
    - Ollydbg
    - ...
    - Appendix B
    - tools.pediy.com

Configuring VMware

- We can disable networking by disconnecting the virtual network adapter





Use a Virtual Machine

Connecting Malware to the Internet

- For a more realistic analysis
- Risks: propagation, DDoS, Spam,...
- Pre-analysis: what might do when connected

Connecting Malware to the Internet

- NAT mode lets VMs see each other and the Internet, but puts a virtual router between the VM and the LAN
- Bridged networking connects the VM directly to the LAN
- Can allow malware to do some harm or spread – controversial
- You would send spam or participate in a DDoS attack

Snapshots

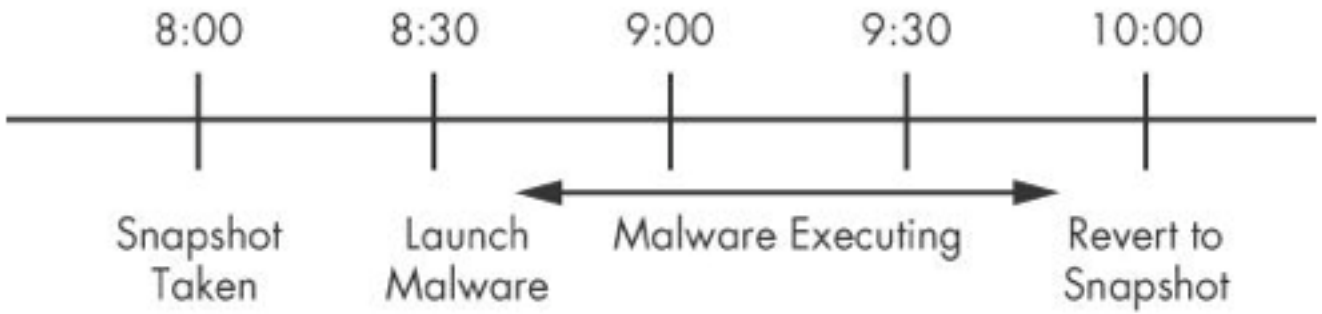


Figure 3-5. Snapshot timeline

Transfer File

- VMware drag-and-drop feature
  - from host OS to guest OS
  - from guest OS to host OS
- Shared folder
  - accessible from both the host and guest OS

The Risks

Risks of Using VMware for Malware Analysis

- Malware may detect that it is in a VM and run differently
  - Chapter 17: anti-VMware techniques
- VMware has bugs: malware may crash or exploit it
  - drag-and-drop vuln
  - fully patched
- Malware may spread or affect the host – don't use a sensitive host machine

Virtual Machine Escape

- Breaking out of VM
  - CVE-2007-1744 Directory traversal vulnerability in shared folders feature for VMware
  - CVE-2008-0923 Directory traversal vulnerability in shared folders feature for VMware
  - CVE-2009-1244 Cloudburst: VM display function in VMware
  - CVE-2012-0217 The x86-64 kernel system-call functionality in Xen 4.1.2 and earlier
  - CVE-2014-0983 Oracle VirtualBox 3D acceleration multiple memory corruption
  - CVE-2015-3456 VENOM: buffer-overflow in QEMU's virtual floppy disk controlle

Conclusion

Analyzing malware using VMware

1. Start with a clean snapshot with no malware running on it.
2. Transfer the malware to the virtual machine.
3. Conduct your analysis on the virtual machine.
4. Take your notes, screenshots, and data from the virtual machine and transfer it to the physical machine.
5. Revert the virtual machine to the clean snapshot.

Discussion

- Malware authors thought only analysts would be running the malware in a virtual machine.
  - VM is becoming more and more common
  - valuable victim ?
- Will anti-VM techniques probably become even less common?

恶意代码分析与防治技术

第4章 虚拟机技术

王志
zwang@nankai.edu.cn

updated on 2022-10-16

南开大学 网络空间安全学院

2022-2023学年