Understanding Stealth Malware

Joanna Rutkowska & Alexander Tereshkin

Version 1.4

Part 1: Subverting The System **Day 1: 9.00 – 12.30**

Lectures: 9.00 – 10.30

1. Introduction – why do we need all those rootkits?
2. Different types of system subversion (Type I, II and III)
3. Vista kernel protection and how it can be bypassed

Labs: 10.45 – 12.30

- Introduction to x64 kernel drivers
- Loading unsigned code into Vista x64
- Driver bugs: finding & exploiting

Part 2: Malware Hiding Strategies **Day 1: 14.00 – 17.30**

Lectures: 14.00-15.30

1. Process Hiding
2. Memory Hiding
3. Stealth by Design Malware
4. A few words about persistence

Labs: 15.30 – 16.00 & 16.15 - 17.15

- Playing with several process hiders (FU, FUTo, PHIDE2)
- Discovering hidden processes using KD
- Playing with Shadow Walker
- Uncovering Shadow Walker
- Playing with fully functional SbD rootkit

Part 3: Network Subsystem Subversions **Day 1: 17.30 – 19.00**

Lectures: 17.45 – 19.00

1. Overview of the Windows Networking
2. Focus on NDIS
   - NDIS6 anatomy
   - Hooking NDIS at various levels
3. Applications of NDIS hooking
   - Implementing SbD network backdoors
   - Implementing covert channels
   - Bypassing PFWs
4. Endless arm-race?

Part 3: Network Subsystem Subversions (Labs) **Day 2: 9.00 – 11.15**

Labs: 9.00 – 10.30 & 10.45 – 11.15

- Hooking NDIS at various levels
    - Level 1: NDIS_OPEN_BLOCK,
    - Level 2: X_FILTER/X_BINDING_INFO
    - Level 3: Hooking at Miniport level
- Playing with SbD Network Backdoor
- Bypassing commercial Personal Firewalls (*)

Part 4: Virtualization-based malware **Day 2: 11.15 – 17.00**

Lectures: 11.15 – 12.30

1. Hardware Virtualization Technology
2. Introducing Blue Pill
3. Detecting the presence of a VMM
    - Direct timing analysis with trusted time source
    - Defeating timing analysis with trusted time source
    - Detecting hypervisor via CPU bugs
    - Detecting CPU resource discrepancies: TLB profiling
    - Defeating other attacks
4. Detecting the BP explicitly
    - Memory scanning
    - Memory hiding strategies
5. Supporting nested hypervisors
6. The future of virtualization-based malware?
    - In the future everything runs inside a Virtual Machine…
    - VMM hijacking?
    - Trusted boot process and ”late launch” – how they change the battlefield?

Labs: 14.00 – 16.00 & 16.15 – 17.00

- Playing with the New Blue Pill
- Detection using external time source
- Surviving timing analysis that uses trusted time source
- Advanced TLB profiling-based detection
- Searching for Blue Pill in memory
- Running Blue Pills inside each other
- Running Virtual PC 2007 inside Blue Pill(*)

Part 5: Cheating Forensic Analysis **Day 2: 17.00 – 18.30**

Lectures: 17.00 – 18.00

1. Cheating software based forensic tools
2. Cheating hardware based forensic tools

Labs: 18.00 – 18.30

- Memory acquisition via FireWire
- Defeating h/w based memory acquisition (*)

Game Over? **Day 2: 18.30 – 19.00**

1. A philosophical summary of the training and final Q&A