


SPLITTING GEMINI

Adam Cecchetti





Who am I?

- Adam Cecchetti
 - Senior Security Consultant @
Leviathan Security Group
 - Security researcher by night
- 


Splitting Gemini

- Goals
- Utilize MultiCore CPUs in Rootkits
 - Remove Core from system for offensive usage
 - Vector for staying inside of system
 - Hiding code from main system
 - Effect remaining cores and kernel structures
 - “out of band”
- Alter Scheduler
 - Keep RQ and task list of SBP intact
 - Keep system exploited and stable
 - Maintain reasonable speed




Splitting Gemini

End Project Goals : Dark Knight

- Research offensive techniques for maintaining rootkit access
 - Create rootkit preservation software
 - Create Anti-AV/HIDS/Agent signature based filtering system
 - Be Batman for rootkits
- 

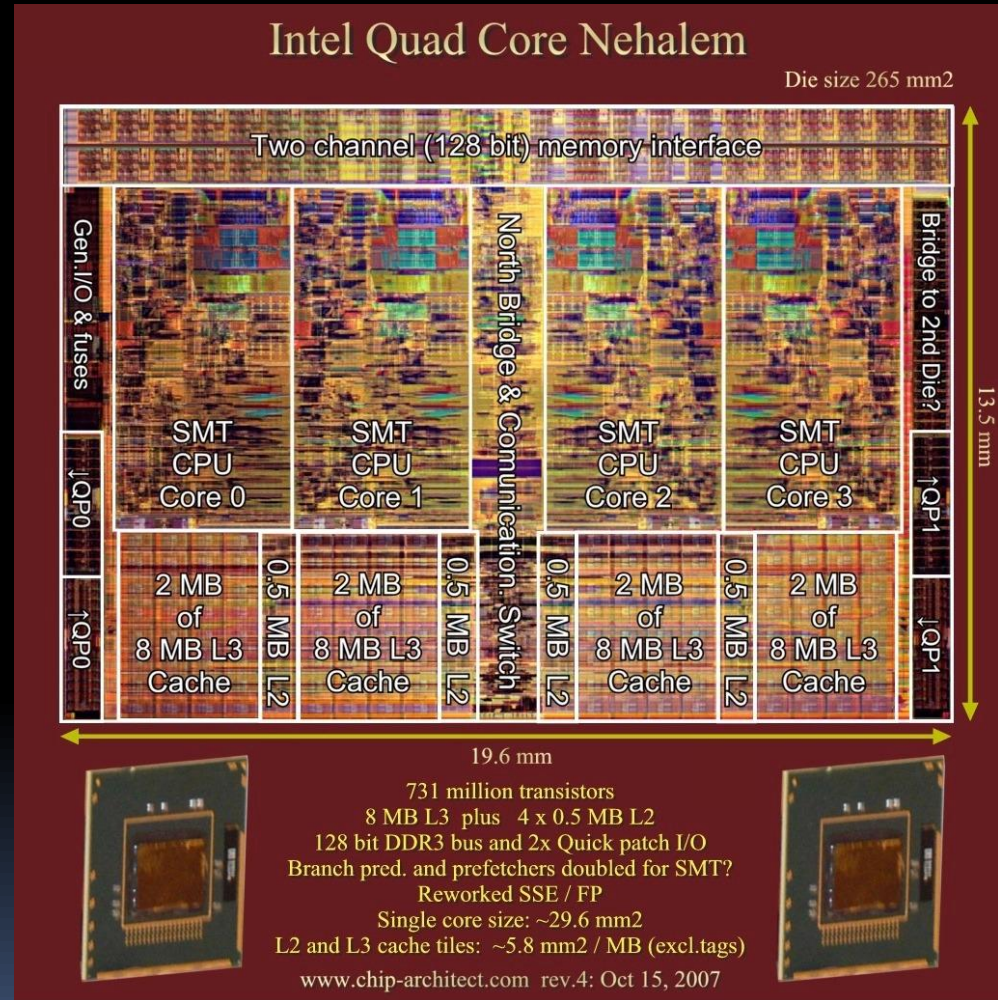


Motivation

- “You have root so what”
 - Rootkits vs Monitors/Tools/Admins
 - Scheduler seldom changes
 - Scheduler must be present in all systems
 - Number of cores continuously growing
- 

4 More Cores

- Cray, IBM, etc
- SMP
- Xeon
 - Hyper-Threading
- Core2Duo
 - 2 Cores
- Intel Nehalem
 - 4-8 Cores
- Future
 - $(n+1)^2$



Splitting Gemini

- Split core
- Remove AP CPU from MultiCore system
 - Migrate/Shutdown processes
 - Block interrupts
 - Clean up APIC
 - Remove CPU from masks / kernel data structures
 - Allocate data structures
 - Load tasks



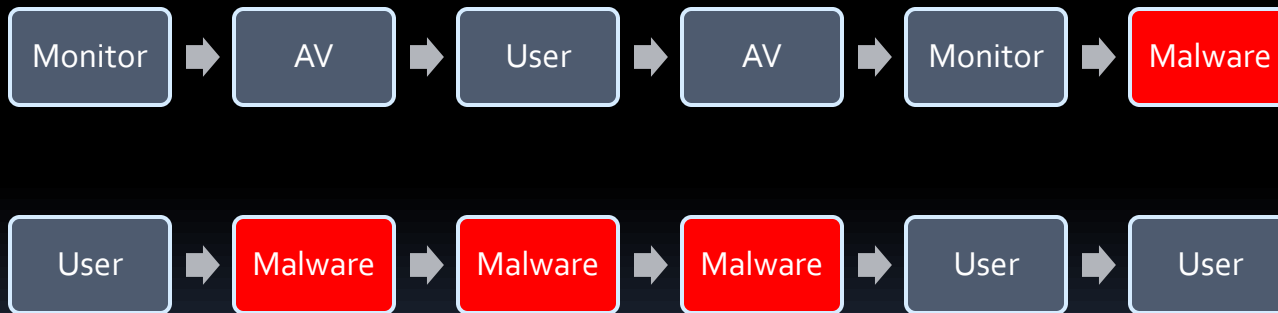
Scheduler

- Scheduler
 - Common entry points
 - PlugSched makes testing easy



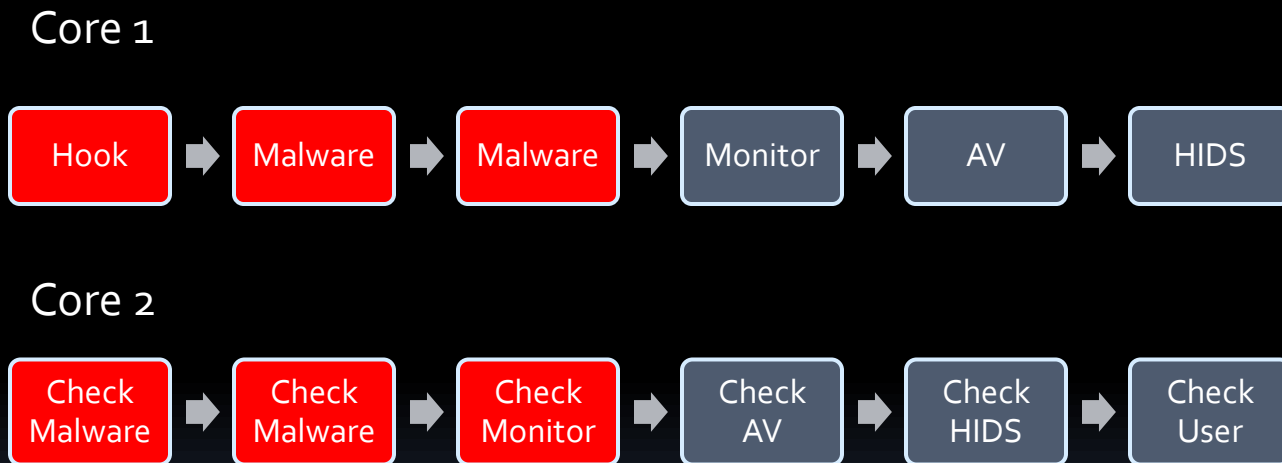
Process Starvation

- Selective process execution
 - 1 for you 10 for me
 - Dining philosophers be damned...



Process Filtering

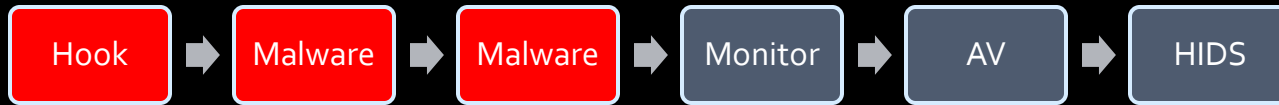
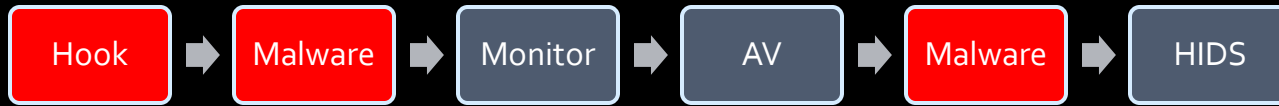
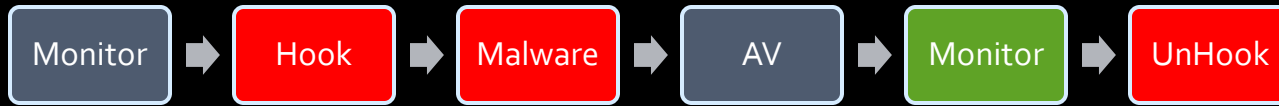
- Keep rootkit hostile processes from running



Process Drift


- Selective Temporary Starvation
- Create a window where the system can be treated as if there is no monitoring software
- Remove Monitor/AV hooks
- Run Malware
- Allow malware to cleanup after itself
- Resume execution of monitoring processes

Process Drift





False Reporting

- Return of Time Sharing
 - Runtime utilization
 - Amazon SDS
 - Shared hosting/Virtual Clusters
 - GPUs/Grids/Clusters
- 

A vertical bar on the left side of the slide, consisting of several colored segments: a small pink square at the top, a grey square, a yellow square, and a long pink rectangle at the bottom.

Tech Demo

I must be insane...

Future Work

- Continue work for reliable runtime splitting
- Investigate additional schedulers and kernel processes
- Anyone in the house a Windows scheduler expert?
 - I'd love to talk to you 😊
- NonCPU Rootkits
 - GPU/NPU rootkits
 - CUDA/Killer API Frameworks

Future Work

- Give some cores back!
 - Fairly Easy to detect a CPU is missing
 - Replace CPU with a GPU
 - Step 1: Allocate Kernel structures for GPU
 - Step 2: ??? (CUDA+GPU<- "magic" ->VCPU code)
 - Step 3: Profit!



Questions?