(U) TCB Jamboree 2010 Abstracts

TOP SECRET//SI//NOFORN/ORCON
From WikiInfo-NF
Jump to: navigation, search

Contents

[hide]

- 1 TCB Jamboree 2010
  - 1.1 Passing Clearances
  - 1.2 Location
- 2 Presentation Abstracts
  - 2.1 (U) Times
  - 2.2 Tuesday, 16 March
    - [redacted]
  - 2.3 Presentation Abstracts – Wednesday, 17 March
    - [redacted]
  - 2.4 Demonstration Abstracts
    - 2.4.1 (S//NF) Covert Execution via Bypassing Disk Access
    - [redacted]

[edit] TCB Jamboree 2010

(C) CIA will host a US-only conference on trusted computing technologies 16–17 March. Registration is now open by sending an e-mail message to [redacted] with your full name, SSN, and contact number. **Note that you will be required to pass your clearances in a VR even if you think you are perm certed for this facility.**

[redacted]

[edit] Demonstration_Abstracts

(U) The demonstration promenade will open on the first day of the Jamboree from lunch until 5pm. Conference attendees are welcome to stop by at any time, view the tools, and discuss the techniques with the representatives.

[edit] (S//NF) Covert Execution via Bypassing Disk Access

Presenter: [redacted]

(S//NF) Personal Security Products (PSPs) pose an increasing risk to implants by both pattern matching binary files to detect harmful code and using heuristics to dynamically detect harmful code. This detection is done by analyzing the executables on disk, including detecting when new files are written to disk. When starting a user-mode process, Windows verifies the image of the executable on-disk. Even modern rootkits that start user-mode processes from the kernel must first write the executable to disk, potentially alerting PSPs. To counteract this type of detection, Northrop Grumman Xetron created Orca, a Windows kernel mode driver that is capable of starting Windows executables covertly without alerting PSPs. One of the key features research and developed for Orca is the capability to start user-mode implant executables from kernel mode without writing the file to disk first, thus preventing the PSP from seeing disk activity and then scanning the implant.</p>

(S//NF) Orca circumvents PSP detection by launching processes disklessly. Essentially, Orca creates a clone of an in-memory process. After performing some cleanup on the clone, new executable code is mapped from Orca's memory into the memory of the cloned process. This capability has been tested and found to support most executables without requiring any modification to the executable.

[edit] [redacted]

[redacted]