0wning Antivirus

Why AV?

Attractive Attack Surface

- Gateways, Servers, Clients, ISP's, Third Party Vendor Products
- Heterogeneous and Layered Environments
- Un-trusted Data Processing
- Designed for a variety of Platforms

How Does AV work?

- Signature vs. Behavior
- Enterprise vs. Consumer Architecture
- Common Components
- Standard Features
- Common Configurations

Code Coverage - Signatures

- Byte Comparison
- Strings
- Calculations
- Field Sizes
- Ida Examples

Code Coverage – Core Utilities

- Reads
- Allocations
- Buffered Writes
- Conversions (e.g. StringToNumber)
- Format Specific (e.g. EXE & OLE)
- Ida examples

Code Coverage –Constructs

- Checksum, CRC, etc.
- Inherited File Structures
- Commonly Grouped Processors
- Ida Examples

Audit Points - Inefficiencies

- Engine vs. Product differences
- Default Scan Levels
- File Size Limitations
- Order Of Operations
- Format Collisions
- Ida Examples (McAfee)

Audit Points – Memory Corruption

- Inconsistent Checks
  - Length
  - Position
  - Signature
- Ida Examples (Symantec)

Audit Points – Memory Corruption

- Wrappers that:
  - Truncate
  - Misuse Sign
  - Wrap, Overflow, Underflow
- Ida Examples (TrendMicro)

Audit Points – Memory Corruption

- Error-Prone Formats:
  - 32 bit fields
    - PECOFF
    - Packed PECOFF
    - SFX
  - String Based Formats
    - TNEF
    - MIME
    - PDF
  - Archive Formats
    - Uncommon
- Ida Examples (Symantec, McAfee, Trend Micro, F-Secure)

Audit Methodology

- Identify Utility Functions
  - Wrappers, FileIO, Allocations
- Survey Utility Function Contexts
  - Reads
  - Allocations based on file data
  - Copies based on file data
- Reverse File Format Processors
  - Resolve Indirection for FileIO
  - Follow unchecked integers being stored in classes
  - Track class member offsets and sizes

Future Points of Interest

- Large Files
  - Signed Checks
  - Type Truncation
  - Integer Overflows/Wraps/Underflows
  - Ida Examples
- New Formats
  - Formats implemented due to bugs
  - Formats implemented due to wide use
- Product Administration

Questions?