Software Security API Meeting 2 Agenda

SolidCore:

1. How does Tempus use SolidCore?
2. Will our solution be replacing SolidCore at Tempus?
3. What makes SolidCore non-scalable? (What aspects of Solid Core do not allow it to be deployed on small retailer systems, other than cost?)

Malware Hash Registry:

1. We understand how malware hash registry works. What did you have in mind for this?

Madshi:

1. Why would we need Madshi?
2. Can we hook the windows API without it from Delphi? Looks like it would be useful for abstracting API calls across versions of Windows.
3. Madshi only hooks user mode APIs (what's that?) Do we need to worry about kernel mode APIs?
4. What about hooking reads instead of executions?

Delphi:

1. Delphi MFR?
2. What version of Delphi to use?
3. Why use Embarcadero?

Stakeholders/user interaction

1. Should a user be warned if a non-trusted executable tries to run, or should it just be denied?
2. Can user allow/deny execution?
3. How should the user be able to run a system scan in lockdown mode (what if we don't do the user interface)?
4. What exactly should the console do/have/support?

Hashing/Accessing Database:

1. When performing a system scan, which files should we hash/store?
2. Are we only hashing executables? Batch files? Command scripts?
3. What should we do about new files introduced after the last system scan? (Should we hook on file writes?)
4. When should we perform a check on the database? Should we interrupt when the file is read, or when it tries to execute? Should we only interrupt certain files? How do you filter? By extension?

Speed constraints:

1. Exactly how fast do you need the database to be? (COS)
   Are we talking seconds, or milliseconds?