# BEHAVIOR-BASED DETECTION FOR FILE INFECTORS

AVAR 2010

*by Rajesh Nikam*

Quick Heal

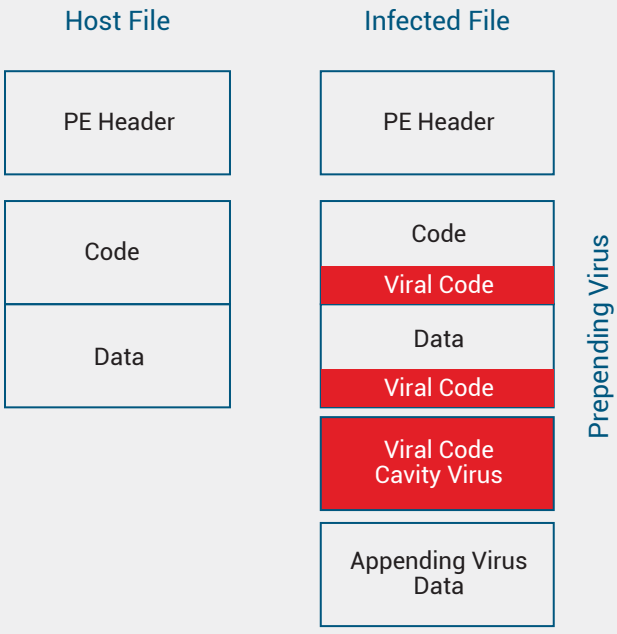
*Security Simplified*

# MOTIVATION

- The exponential rise of malware samples is an industry-changing development.
- Security Products are now augmenting traditional detection technologies with a Behavior-based approach.
- Behavior-based detection works for:
  - Bots, Mass mailing worms, Drive-by downloads, Spyware, Backdoors, Dialers, Keyloggers etc.

# FILE INFECTORS aka VIRUSES

- **Different types of viruses**
  - Appending Viruses
    - Append code at the end of the host file
    - Add new section or modify the last section
  - Pre-pending Viruses
    - Add code at the beginning of the host file
  - Cavity Viruses
- **Entry Point Obfuscation**
  - Modify code near the Entry Point.
  - By modifying control transfer instructions with jmp/call/push-ret.



# BEHAVIOR-BASED DETECTION

- **How it works?**
  - Monitors dynamic behavior of applications.
  - It does so by intercepting system calls.
  - It blocks applications when suspicious behavior is detected.
- **Types**
  - Anomaly based.
  - Policy based.

# CHALLENGES

- **Key Challenge**
  - To identify **characteristics** which are **consistently found in known and unknown** virus samples.
- **Not to detect these legitimate processes as a virus:**
  - Software Updates
  - Compilers/Linkers
  - Executable File Packers
  - Repair by an Anti-Virus Product
- **Process Code Injection**

# COMMON VIRUS TRAIT - REPLICATION

- Infiltrates local and network drives to hunt for target executables.
- Checks for specific file properties.
- **Inserts virus code.**
- Adjusts **AddressOfEntryPoint** or **patch code** to transfer control to virus code.
- They either:
  - use in-place file infection or
  - modify temporary copy of a file and overwrite original file

# SOFTWARE UPDATES

## WINDOWS UPDATE AND OTHER SOFTWARE UPDATES

| File Name | Publisher | Version | |
|---|---|---|---|
| | | Before Update | After Update |
| mspaint.exe | Microsoft Corporation | 5.1.2600.5512 | 5.1.2600.5918 |
| wintrust.dll | Microsoft Corporation | 5.131.2600.5512 | 5.131.2600.5922 |
| ie4uinit.exe | Microsoft Corporation | 6.00.2900.5512 | 8.00.6001.18968 |
| cabview.dll | Microsoft Corporation | 6.00.2900.5512 | 6.00.2900.5927 |
| ieakeng.dll | Microsoft Corporation | 6.00.2900.5512 | 8.00.6001.18702 |
| iedkcs32.dll | Microsoft Corporation | 6.00.2900.5512 | 18.00.6001.18968 |
| mshta.exe | Microsoft Corporation | 6.00.2900.5512 | 8.00.6001.18702 |

# COMPILERS/LINKERS

- Use Memory-mapped files (MMF) mechanism to build the target PE file.
- They then update CheckSum and TimeDateStamp.
- Only a few viruses like **W32.Kriz** are known to update Checksum after infection.
- Special case: **W32.Induc.A** is a virus which targets Delphi Compiler.

# PROCESS CODE INJECTION

- Insert code to running process by
  - WriteProcessMemory , CreateRemoteThread
  - SetWindowsHookEx API, AppInit_DLL registry key, etc.
- Create legitimate process in suspended mode and overwrite the process memory with viral code.

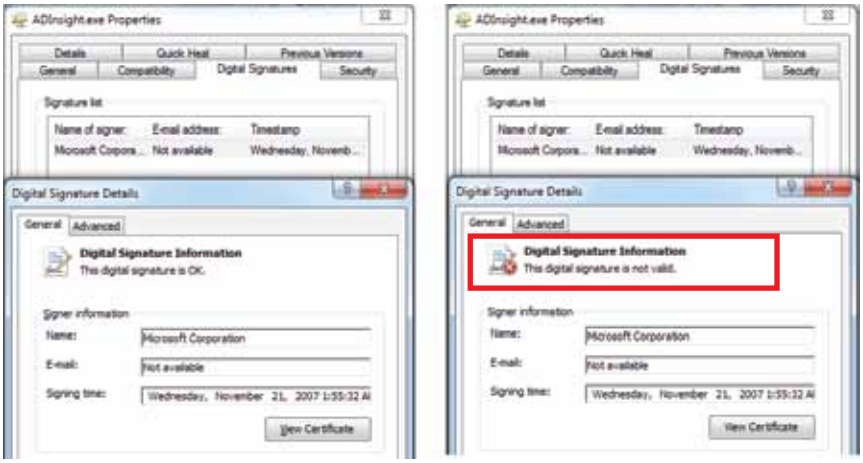
# PROCESS CODE INJECTION BLOCKER

- System Service Dispatch Table (SSDT) Hooking
  - ZwOpenProcess, ZwCreateProcess(Ex)
    - DesiredAccess - PROCESS_CREATE_THREAD, PROCESS_VM_WRITE
  - ZwAllocateVirtualMemory
  - ZwWriteVirtualMemory
  - ZwCreateThread
- SSDT Hooking officially not supported
  - Kernel Patch Protection
  - Kernel Data and Filtering support

# FILE SYSTEM MONITOR

- Based on "Minispy" from Windows Driver Kit.
- File CREATE handler
  - Already existing PE file opened in WRITE mode.
  - Entire file is read and deleted.
- Extract PE file properties
  - Entry Point, Checksum, TimeDateStamp, Section properties, Version Information, Digital Signature.
- File WRITE handler
  - Memory-mapped files (MMF) technique.
  - WriteFile API are treated differently.
- Update section information if the region falling in a particular section is modified.
- File CLOSE Handler
  - Is TimeStamp & CheckSum updated
  - Is Version Information present
    - Is Version Information updated
  - Is Digital Signature present
    - Is Vigital Signature valid
- Check for modification of section properties, Entry Point, EPO etc. to identify type of infection.

# INFECTION AND DIGITAL SIGNATURE




*Digital Signature of **ADIsight.exe** file before and after **W32.Pulkfer.A** infection*

# OBSERVATIONS

| Virus families | New section added | Last section modified | Prepending | OEP modified | EPO | LastSection Writeable | Process code injection | DLL Infector | DigiCert tampered |
|---|---|---|---|---|---|---|---|---|---|
| Fujack | | | Y | Y | | | | | Y |
| Jadtre.A | Y | | | Y | | Y | Y | | N/A |
| PatchLoad | Y | | | Y | | Y | | | N/A |
| Ramnit.A | Y | | | Y | | Y | | Y | N/A |
| Runouce.B | | Y | | Y | | Y | | | Y |
| Agent | | | Y | Y | | Y | | | Y |
| Genome | Y | | | | Y | Y | | | Y |
| Pulkfer.A | Y | | | Y | | Y | | | Y |
| Small | Y | | | Y | | | | | Y |
| Virut.D | | Y | | | Y | | | | Y |
| Virut.G | Y | Y | | | Y | | Y | | Y |
| Sality.U | | Y | | | Y | Y | Y | Y | Y |
| Sality.R | Y | Y | | | Y | Y | Y | Y | Y |

# LIMITATIONS

- Behavior-based detection requires applications to be running in order to scan them.
- It cannot give the actual name or nomenclature of the detected malware samples.

# CONCLUSION

- Behavior-based detection augments virus protection with **Process code injection blocker** and application **white-listing**.
- It helps to mitigate virus outbreaks.
- It collects and stores new/undetected viruses which are found on the user's machine.