

Scut AntiVirus Malware Notation Criteria

Modern malware is complex and is becoming increasingly hybrid and start to emulate real life bio-models. There are Trojan-Worm-Virus - depending on the infection state, infected trojans, infected backdoors, infected worm-virus parties etc. This are NOT mistakes of ciber-criminals, this are hybrid advanced systems which work next to each other for automatic and large scale infiltration and spreading purposes.

Notations are by their nature, reductionist. NovusOrdo lab. model for malware notation is `MasterClasses[1...11].SubClass[Type{1...4}].Name[Type{1...3}].Variant[Type{1...3}]`

Master Classes are from 1 to 11 and they are named as follows: Virus class, Trojan class, Exploit class, Backdoor class, Keylog class, Worm class, HackTool class, RootKit class, Adware class. The order of classes does not matter, you must see them as sets.

The last two of the master classes are Spyware class and Malware class, they are for unclassified malware and spyware that Scut AntiVirus encounters in the wild.

SubClass names are of four types: [FT] File Types SubClass, [AT] Action Types SubClass, [SP] Spreading Pathways SubClass, [OS] OS name SubClass. The SubClass type is chosen depending on which SubClass properties distinguishes from the rest. Scut Antivirus malware notation criteria is as follows:

Scut AntiVirus Malware Classes names:

- Virus generic class
- Trojan generic class
- Exploit generic class
- Backdoor generic class
- Keylog generic class
- Worm generic class
- HackTool generic class
- RootKit generic class
- Adware generic class
- Spyware generic class
- Malware generic class

Scut AntiVirus Malware SubClass names:

[FT] ➤ File Types SubClass:

- ▶ JS
- ▶ SWF
- ▶ ASP
- ▶ VBS
- ▶ BAT

- ▶ PHP
- ▶ VBA
- ▶ HTM
- ▶ MTH
- ▶ XML
- ▶ CSS
- ▶ INF
- ▶ REG
- ▶ Perl
- ▶ MSEXcel
- ▶ MSOffice
- ▶ MSWord
- ▶ Unclassified

[AT] ➤ Action Types SubClass:

- ▶ Boot
- ▶ Clicker
- ▶ Nuker
- ▶ Dialer
- ▶ DoS
- ▶ DDoS
- ▶ Downloader
- ▶ Dropper
- ▶ Flooder
- ▶ GameThief
- ▶ Notifier
- ▶ Proxy
- ▶ Sniffer
- ▶ Spam
- ▶ Spoofer
- ▶ Spy
- ▶ RCE
- ▶ VirTool
- ▶ Constructor
- ▶ Unclassified

[SP] ➤ Spreading Pathways SubClass:




- ▶ IM
- ▶ IRC
- ▶ Net
- ▶ P2P
- ▶ Email
- ▶ SMS
- ▶ AOL
- ▶ Unclassified

[OS] ➤ OS name SubClass - for non portable applications:




- ▶ DOS
- ▶ Win16
- ▶ Win32

- ▶ Win64
- ▶ Linux
- ▶ UNIX
- ▶ SymbOS
- ▶ Mac
- ▶ WinCE

Malware Name:

- [MKN]  Malware Known Name - if the malware has a stable file name, will have that name.
- [MEN]  Malware Effects Name - the effects they cause after execution of that type of malware.
- [MUS]  Malware Unic String - unique string found inside the malicious file, if it is readable and has a meaning.

Malware Variant Name:

- [MCN]  Metamorphic Core Name - one version with multiple forms of itself.
- [PCN]  Polymorphic Core Name - one version with multiple file types and multiple forms for each file type.
- [MVN]  Malware Variant Name - various changes, packagings and compilations of the same malware