

Scut, the new AntiVirus engine on horizon

an article by Paul Gagniac

Scut antivirus engine is our new approach on software security. An AntiVirus engine built from scratch at Novus Ordo lab. and integrated in Scut Antivirus on-demand scanner for now and in future products which shall appear in a very short time.

Unlike its competitors, which have years of experience due to market age, the SCUT antiviral engine structure is based heavily on statistics and on new approaches to the security problems.

Being old and experienced in antivirus world is not always an advantage, affects the mentality of antivirus experts and, as expected, antiviral engine structure due to a known constant, is called inheritance !.

This legacy of old malware cause design misconception of antivirus engines and bad understanding of heuristics. Many antivirus products which are not working on old systems, have virus signatures that are 15-20 years old, and the rate of virus infection for viruses older than 1997-1999 is almost equal to zero on new operating systems in accordance with our experience. A good example are state of art variants of Win32/CIH, in good old times the lions of the jungle, now this variants are unable to infect new systems from several years now.

Scut antivirus engine detected most viruses after the manner of infection, other antivirus products classify them in many subcategories, work that is not bad, but definitely a waste of signatures.

For instance, Win32/Virut virus is classified in 50 variants by other antivirus companies, Scut antiviral engine finds all this variants and classify them in only six types of infection: Virus.Win32.Virut.a, Virus.Win32.Virut.b, Virus.Win32.Virut.c, Virus.Win32.Virut.d, Virus.Win32.Virut.e and Virus.Win32.Virut.f. That means 50 virus signatures optimized to 6 signatures.

The Win32/Sality virus is known to have 30 variants by other antivirus companies, which are optimize for detection in scut engine to only 8 signatures, and so on.

The cold reality is that heuristic emulation methods are still slower than holy signature scanning methods, even at seven million signatures in testing at Novus Ordo lab. Believe it or not, heuristic detection methods of today are still using signatures, dinamic signatures or functional signatures, fact for which a scanner can detect malware structures which has not yet met.

And as I realize, heuristic signatures are here to stay, even for malicious self-packed structures.

Other legacy of malware is what I call temporary trojanware. In most cases trojan programs, especially Trojan-Downloaders, are part of a elaborat and complex information theft, and the simplest system of this type is the model Exploit-Trojan-Server, now the server has a physical location and is easily detected, and once detected, the server is stopped, or as the case an account is closed on that server.

When the server is closed, the malware is no longer dangerous to the user, and the trojan signature now becomes legacy for the antivirus database, and in time this is a big problem. Scut Center checks

for signature lifetime through emulation of elements stored in the Scut Viral Bank. Such examples can be found in Trojan.Zbot series, Trojan-Downloader series, etc.

This accumulation of legacy signatures can trigger false alarms, phenomenon which already happend in many cases.

Scut Antivirus On-Demand is the latest technology for fighting Malware. This scanner incorporates the following modules: AntiVirus, AntiWorm, AntiTrojan, AntiRootkit, AntiSpyware, AntiKeylog, AntiRA, AntiCrimeware, AntiPhising.

Scut AntiVirus Scanner

Scanner menu

- Scan my computer
- Critical Scan
- Path Scan
- Scanner Settings
- Quarantine

Scanner status

Antivirus Quick Status:

- Last UpDate: 01.01.2009
- AV definitions: 364535 MS
- Engine version: V1.6.0.56
- Proactiv Detection: OFF

Scan for Malware

Proactiv protection report:

- Firewall scan request: 1
- Dependencies scan: 1
- Total malware found: 102475
- Total suspect files: 2592

Antivirus Engine:

- Coincidence Coefficient : 80
- Similarity Coefficient: : 6
- Metamorphic level: : 16
- Polimorphic level: : 65

Scan My Computer

Critical Scan

Real time disk access: R: [0 r/s] - W: [3 w/s]

Scut Total Security 2010 is a complex and complete protection system, universal for home users, small businesses and large networks, this solution includes 360 safe-guard security modules.

Stay sharp to the new release of Scut Total Security !
The new technology is coming soon !

Press [here](#) to visit Scut Security Center for more info ...

Hide this !

Requests for PC resources are very low, can operate on 300 MHz CPU and 128 RAM. Setup requires only 20 MB free hard drive space. As a scanner runs on all Windows operating systems.

It scan's the entire computer or, at user choice, only parts of the PC - for detection of viruses, trojan-parties, backdoors, rootkit programs, keylogs, exploit methods, etc.. The capture below is an example test scanning with already known malicious files:

Scut AntiVirus Scanner

Scanner menu

Scan my computer

Critical Scan

Path Scan

Scanner Settings

Quarantine

Scanner status

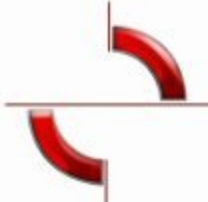
Antivirus Quick Status:

- Last UpDate: 01.01.2009
- AV definitions: 364535 MS
- Engine version: V1.6.0.56
- Proactiv Detection: OFF

Quarantine

Qarantined/Locked malware: 1175

Action	Malware	Path	No.
QUARANTINED	Virus.W32.Sality.l	C:\Documents and Sett...	01
QUARANTINED	Virus.W32.Sality.q	C:\Documents and Sett...	02
QUARANTINED	Virus.Win32.Delf.a	C:\Documents and Sett...	03
QUARANTINED	Virus.Win32.Delf.a	C:\Documents and Sett...	04
QUARANTINED	Virus.Win32.Delf.c	C:\Documents and Sett...	05
QUARANTINED	Virus.Win32.Delf.j	C:\Documents and Sett...	06
QUARANTINED	Virus.Win32.Delf.d	C:\Documents and Sett...	07
QUARANTINED	Virus.Win32.Delf.r	C:\Documents and Sett...	08
QUARANTINED	Virus.Win32.Delf.w	C:\Documents and Sett...	09
QUARANTINED	Virus.Win32.Delf.w	C:\Documents and Sett...	10
QUARANTINED	Virus.Win32.Neshta.b	C:\Documents and Sett...	11
QUARANTINED	W32/Netsky.p@MM	C:\Documents and Sett...	12
QUARANTINED	Virus.W32.Parite.d	C:\Documents and Sett...	13
QUARANTINED	Virus.Win32.Delf.n	C:\Documents and Sett...	14
QUARANTINED	Virus.W32.Parite.d	C:\Documents and Sett...	15
QUARANTINED	Virus.Win32.Plutor.b	C:\Documents and Sett...	16
QUARANTINED	Virus.Win32.Delf.n	C:\Documents and Sett...	17
QUARANTINED	Virus.Win32.Zori.a	C:\Documents and Sett...	18



Scut Total Security 2010 is a complex and complete protection system, universal for home users, small businesses and large networks, this solution includes 360 safe-guard security modules.

Stay sharp to the new release of Scut Total Security !
The new technology is coming soon !

[Press here to visit Scut Security Center for more info ...](#)

The users have 10 days of use, enough time to deal with their computer problems.

If possible, viruses should be deleted upon detection or if they are attached to an executable file it is possible to disinfect that file, although this disinfection process does not always work and could negatively affect your computer.

Your computer is acting strangely and you suspect you may be dealing with a virus or trojan horse ?!
 Scan your computer now!