eScan Antivirus Technology

White Paper

Document Version (esnav 14.0.0.1)
Creation Date: 19th Feb, 2013

Antivirus Technology

The complexity of anti-virus software has grown enormously over the last few years. The methods used to detect viruses have become complicated. This paper discusses engines used by eScan to detect new threats in detail.

Introduction

This is an executive summary of the architecture, design and general structure of the eScan Antivirus engine (hereafter referred to as AV engine).

The modularized architecture used to build eScan has contributed to its ability to be used in a variety of environments ranging from embedded systems to workstations and high-end servers, in desktop, dedicated or generic server solutions. eScan Antivirus is portable and platform independent (such as: Windows, Linux).

The scanning engines are comprised of modules which are continually being developed to offer full protection against all types of malware including, but not limited to: executable viruses, script viruses, macro viruses, backdoors, trojans, spyware, dialers, etc. eScan technique makes it easier to detect a wide range of malicious code, including spyware and Trojan horse programs, in addition to viruses and other malware threats.

What options eScan Antivirus Engine has?

eScan employs multilayered approach to protect systems, discussing all the layers is out of the scope of this documentation. Here we are focusing on eScan AV engine, along with eScan AV engine, it also has strong Proactive Behavior Monitoring and eScan Cloud Technology. To know more about these technologies please refer to the white papers related to these technologies our website.

Check files for any type of malware – over Billions of virus records:

New version of eScan engine is built upon highly optimized data processing algorithms. It significantly reduce system load during scan operations by using advanced caching technology. The engine has a high detection rate of all common types of malware: file infectors (Viruses), malicious scripts, Trojan horses, Backdoors, Rootkits, Spyware, and Adware, network Worms etc.

Scanning of archives and other various formats

eScan engine unpacks these types of containers:

* Numerous popular archivers: ZIP, RAR, 7Zip, ACE, ARJ, MS CAB, IS CAB, GZ, BZ2, RPM, DEB, LZH, TAR, CPIO, ISO and some others;

* Other types of containers: CHM (Windows Help files), OLE2-containers (Office compound files) and others.

* All common installers: MSI, Nullsoft Installer, various types of self-extracting archives;

Remediation of files that were infected by virus file

Remediation technologies built into the engine allows removing malicious code from the infected application which retains application and operating system functionality and stops local epidemic. Today’s malware trends execute and copy droppers and make multiple system registry changes so that normal AV engine could detect the parent executable but unable to remediate changes done on the system. eScan advance engine keeps tracking of all the changes being done on the system and revert back those changes to normal.

Unique Heuristic Algorithms

Heuristic analysis uses typical malware behavior patterns to detect new and unknown malware that has not been processed by our virus lab and wasn’t yet added to virus signature. eScan Antivirus Engine has built-in heuristic scanner that helps to deal with the modern variants of malware.

Engine Updates

Our lab releases new malware database updates after every 2 hours. In case of some urgency (new emerging virus epidemic) we are able to deliver hourly urgent update. Planned releases of scanning engine up gradation are also delivered along with database updates. These might include scanning speed or memory footprint optimizations, and addition of new features.

Technology

It relates to methods for detecting viruses and malwares, and in particular anti-virus detection methods of scanning for malicious software such as viruses, worms and Trojans include content-matching methods and behavior/Heuristic based methods. In content matching method, the content of the suspected file is compared to database of known malware signatures. If a known virus signature is found in the suspected file, the file is marked as a virus. Content matching methods are more effective but may not be able to identify new malwares.

The other way of finding out if the information being scanned is dangerous, without knowing if it actually contains a virus or not, is the method known as 'heuristic scanning'. This method involves analyzing how the information acts and comparing it with a list of dangerous activity patterns.

Both of these methods have their pros and cons. If only the content matching method is used, it is important to update it at least once a day. When you bear in mind that 15 new viruses are discovered every day, an antivirus that is left for two or three days without being updated is a serious danger. The heuristic method has the drawback that it can warn you about items that you know are not viruses. If you have to work with a lot of items that may be considered dangerous, you could soon tire of the notifications generated by this method.

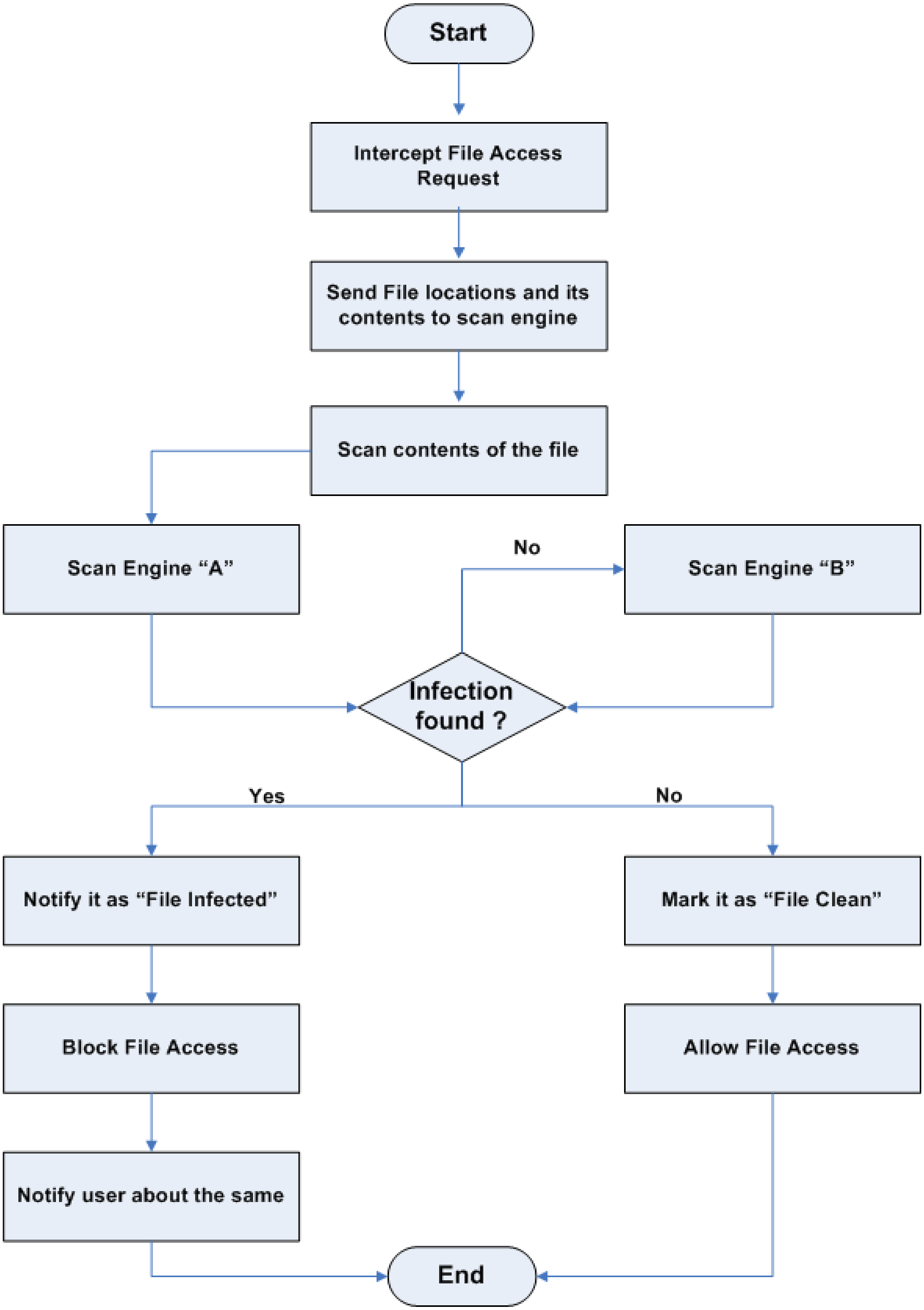
To match the content, eScan uses multiple engines to detect virus and other threats, why? Reason being, if one AV engine fails to detect the threat other should catch it and vice versa. When we say AV engine, it really means a

- On access scanner engine which works as TSR (Terminate and Stay in residence)
- Scanner engine needs update module to update virus signatures and detect known threats.
- Notification module connected to scan engine
- It also includes heuristic analyzer
- Multi - threading architecture in order to increase system performance

Generally these 5 things make the Anti-virus engine, which helps in preventing known viruses and other malwares from system. Anti-virus engines are provided on end-user client systems running an operating system such as windows, mac, and Linux as an endpoint suite or it can be provided on mail gateways where it will scan for viruses and threats in an email.

One important aspect of eScan AV engine that it takes a backup of important system files. In case, if any false positive is detected, it restores them with backup files without any downtime.

Following flow chart shows the basic functionality of eScan AV engine


Start
Intercept File Access Request
Send File locations and its contents to scan engine
Scan contents of the file
Scan Engine "A"
No
Scan Engine "B"
Infection found ?
Yes
No
Notify it as "File Infected"
Mark it as "File Clean"
Block File Access
Allow File Access
Notify user about the same
End

The interpretation mechanism must be specific to each operating system or component in which the antivirus is going to be implemented. Every time the information on a disk or floppy disk or flash drive is accessed, the antivirus will intercept the read and write calls to the disk, and scan the information to be read or saved. This operation is performed through a driver in kernel mode in Windows operating system.
When it intercepts a file request call, the file information and path is send to the AV engine, then AV engine "A" scan the file using content matching method against its virus signatures. If infection is found in that file the file is marked as virus and then AV engine takes action on that file based on the default configuration like quarantine/disinfect/delete. If found clean it will be send to the AV engine "B", again the same process will be followed. If Second engine also found the file is clean, then the access to that file will be allowed else default action will be taken.

Detection Rates

When talking about AV engine, detection of viruses and malware threats are the important criteria. Different antivirus programs have different detection rates, which both virus definitions and heuristics are involved in. Some organizations do regular tests of antivirus programs in comparison to each other, comparing their detection rates in real-world use. AV-Comparatives, AV-Test.org, VB100 and ICSA regularly release studies that compare the current state of antivirus detection rates. The detection rates tend to fluctuate over time – there's no one best product that's consistently on top. If you're really looking to see just how effective an antivirus program is and which are the best out there, detection rate reviews and studies are the place to look.

eScan is participating in all the tests and continuously doing well in all the tests. eScan AV engine earn very good points in current AV-Test testing cycle where it is placed in TOP 3 AV vendor list.

Speed

This is very important factor when it comes to an Anti-virus, The scanning speed should be faster and detection rate should be higher. Scanning contains real time scanner, on access scanner and on demand scanner/schedule scanner. For an AV engine, speed is deciding factor when customers use it in the real time environment, scanning speed should not affect system performance degradation. eScan AV engine is designed is such a way that it scores higher point among all the existing AV vendors.

How to test?

A simple way to check if eScan AV engine is loaded and it is working correctly. Once eScan AV engine installed visit www.eicar.org and download a test virus called eicar.com, eScan AV engine should detect this file as virus and should notify user accordingly. This indicates that eScan AV engine is loaded and working.

CONCLUSION

Clever engine design, careful programming of an AV database, and the combination of generic and heuristic detection methods can achieve stunning results in detecting and cleaning the majority (up to 80–90%) of new field viruses.

Today eScan has multilayer approach when it comes to detect any unknown threats; eScan has developed Proactive Technology and Cloud Scanning to evade zero-day threats.