



Globalization and advancements in Information and Communication Technologies have brought the world closer together and permits rapid access to mammoth services for large-scale collaboration. Apart from the benefits, security threat is also growing equally fast. Malicious software threat has become prominent in the recent times. According to 2008 and 2009 statistics, the number of malicious software has surpassed the published legitimate software worldwide. This is drastically affecting the accuracy of anti-virus solutions, as it becomes very difficult to quickly release the signatures.

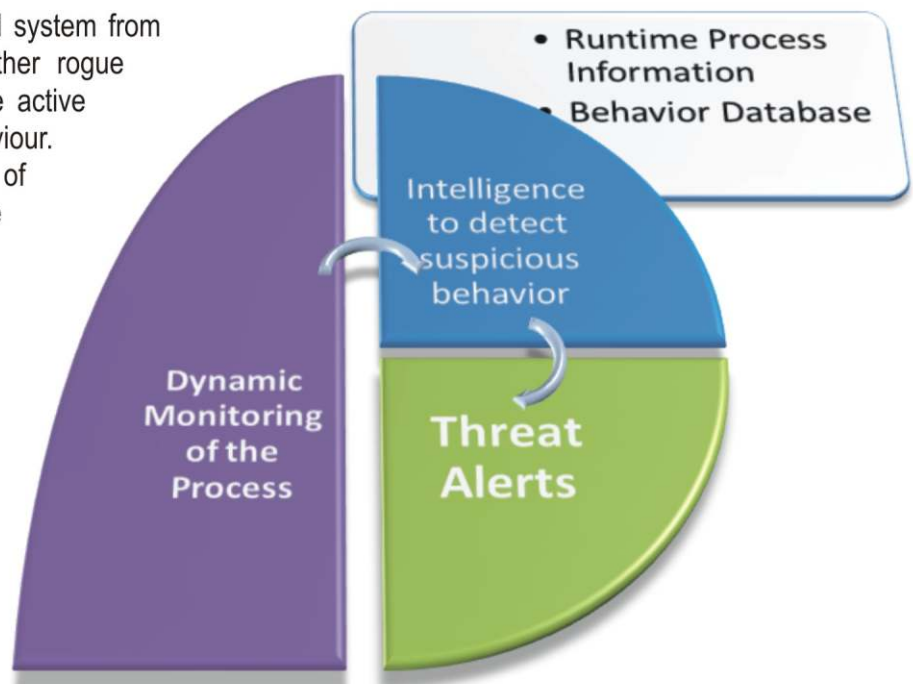
MALWARE RESIST addresses the malicious software issue using behaviour based detection technique. This solution eliminates the need for constantly generating and updating the new malicious software signatures. It helps to detect zero-day attacks, without compromising the system performance or daily updating.

Real-Time Scrutiny of Processes

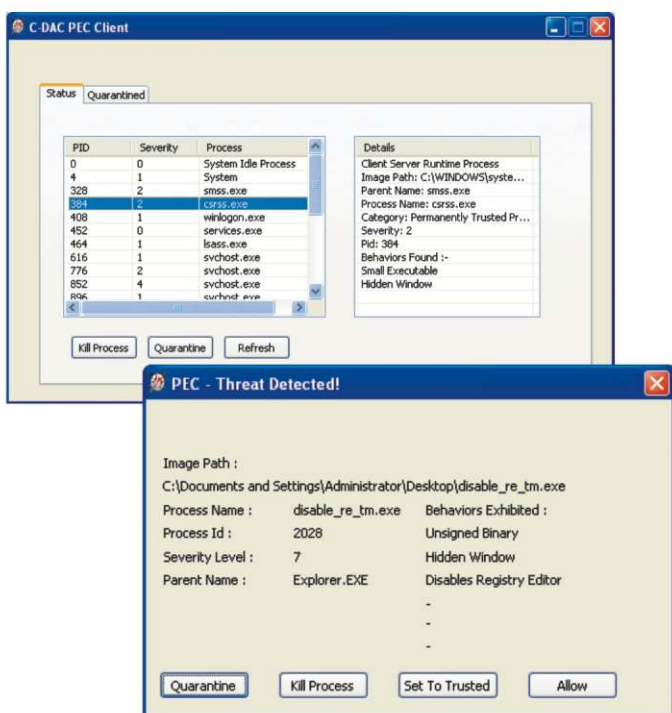
MALWARE RESIST protects an end system from damage caused by malware or any other rogue software by continuously scrutinizing the active programs or processes for malicious behaviour. The Processes are monitored for a set of critical behaviors that could affect the normal functioning of the system.

MALWARE RESIST notifies user through an alert in case of any critical and suspicious behaviors. This helps user to protect from the Malware by quarantining the processes. These quarantined processes are terminated and will not be allowed to create again. In spite of alert from **MALWARE RESIST**, in case if the user trusts the program, **MALWARE RESIST** provides facility to enable it as a trusted program.

Severity level is associated with every behaviour and these levels are fixed based on the severity of the damage caused by it. A threshold is fixed and in case if the severity level of behaviour crosses it, user will be explicitly notified.



- Small memory footprint and high detection rate
- Co-exists with Anti Virus Solutions
 - Low False Positive Rate
 - Easy to Deploy and Use



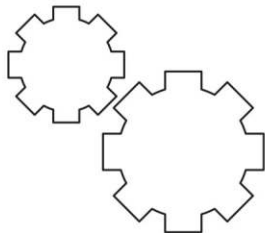
Detection Based on Runtime Behaviour

MALWARE RESIST uses Runtime Behaviour based technique for detecting malicious activity on the end system. **MALWARE RESIST** classifies malicious behaviour into various categories based on the severity of the behaviour and its detection context.

Few Behaviors are given below:

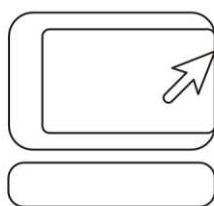
- Maliciously packed executables
- Changing security settings
- Hidden processes
- Code injection attempts
- Disabling system tools like registry editor

A process is tracked with these behaviors as well as their combinations to detect the suspicious activity.



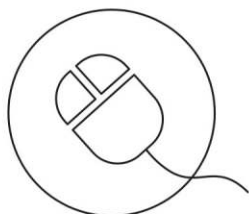
Categorize Processes

Categorizes the system processes as permanently trusted, user level processes can be set by the user as trusted and all other processes will be treated as untrusted. Alerts will be triggered during runtime, based on detection mechanism



Lightweight

Uses minimal system resources and still provides best detection



Detects unknown threats

Detects unknown threats as detection mechanism is based on behavior