Defending your network from unknown email threats

Paranoid adds the extra level of scanning capabilities required to detect suspicious email content from entering your network. The nature of the threat is constantly changing, which is why Paranoid adapts and learns with every email it scans.

Protecting against viruses is an arms race. To win the race, or at the very least remain one step ahead, it is vital that your opponent, the malware writer, knows as little as possible about the defences that protect one of the most vulnerable entry points into your network – email.

Traditional anti-virus protection works up to a point, but with most of the world connected to the Internet with high-speed connections, threats become global within hours, a change in the way virus writers distribute malware and the emerging threat of bespoke Trojans, organisations need to consider adding another layer of defence to their email security.

Worm outbreak

A few years ago, when a new email worm was discovered it was several weeks before it would amount to anything serious. Today, no sooner is a threat announced and before antivirus vendors can issue an update, malware writers have already moved to the next attack. Since email is the easiest method to find potential victims, these threats are then frequently distributed, disguised as genuine messages.

Although anti-virus vendors issue updates to counteract any vulnerability as quickly as they can, given the constraints that an update signature has to be developed and tested, there is a window of exposure where organisations are vulnerable.

Changing malware writing tactics

Some virus writers constantly revise their creation in order to bombard the anti-virus vendors with too much work in the hope that one variant will get through; others deliberately only send out a small amount of samples of new viruses in the hope of remaining under the anti-virus radar for as long as possible.

A few malware writers even wait until a major virus outbreak has occurred before releasing their latest work, on the off chance that not just the anti-virus companies but users as well, will be so vigilant about one virus that they miss another.

SC MAGAZINE AWARDS 2006 EUROPE WINNER

Best Anti-spam

SC MAGAZINE AWARDS 2006 EUROPE WINNER

Best Email Content Filtering

WEST COAST LABS CHECK MARK SEE YOUR SAFEGUARDS AT www.check-mark.com Anti-Spam

Protecting against constantly shifting tactics requires an extra layer of defence that is just as devious as the malware it blocks.

Blended threats and bespoke malware

The convergence of spam and viruses has never been stronger. Many of today's viruses spread using spamming techniques and many spam messages containing web links purporting to be to legitimate web sites are actually links to download malware such as keylogging or password stealing Trojan programs.

2005 saw incidents of highly targeted, company specific attacks designed to withdraw confidential information from the organisation. Although industrial espionage is not a new crime, the ubiquitous use of email throughout business has made it an easy entry point for a sophisticated social engineering attack.

Paranoid protects organisations against these threats

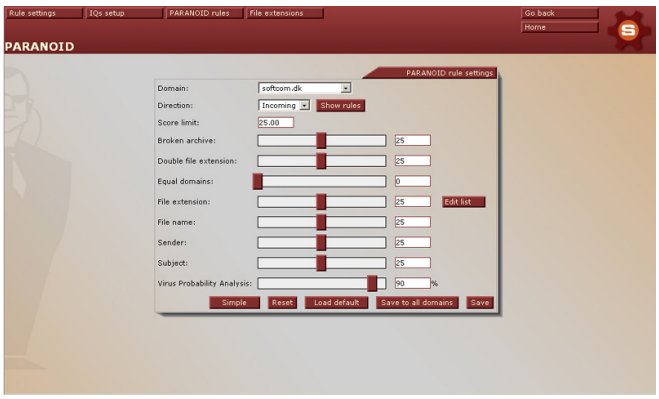
SoftScan developed Paranoid in response to these changing threats and its scanning capabilities provide several benefits when used in addition to traditional anti-virus products:

Undisclosed heuristics

Unlike anti-virus vendor's scanners, which also have some capabilities to detect unknown viruses, SoftScan's hosted solution makes it difficult for malware writers to reverse engineer (and test) the technology used in order to escape detection. This is because criminals can't simply download the Paranoid scanner.

Email focused

Email is the number one method of propagation for malware. By focusing singularly on email, Paranoid is able to concentrate its analysis in more depth as its efforts are not diluted by trying to detect malware from other sources.



Volume of data analysed

The large volume of data that SoftScan collects from a variety of sources enables Paranoid to analyse, compare and detect, with great accuracy, malware characteristics within email.

Virus Probability Analysis (VPA)

This is the core of Paranoid. VPA is an extremely intensive process that enables SoftScan to detect malware before traditional anti-virus scanners have adjusted to the threat.

How Paranoid adds an extra layer of defence

Paranoid adds an extra level of scanning capabilities to detect suspicious content or simply block emails that violate company policies by using a series of rules. When a rule applies to the scanned message it assigns the email a number of points. If a message receives enough points equal to or more than the score limit, Paranoid blacklists the message.

The default action is to quarantine inbound messages blacklisted by Paranoid. This action can be configured depending on an organisation's operational need. In addition, users can configure incoming and/or outgoing Paranoid options by simple enabling or disabling the scanning rules.

How Paranoid determines if an email message is suspicious can be broken down into three broad categories. The first two constant threat analysis and malware instance monitoring are very similar to the heuristics used by anti-virus products to detect viruses.

Constant threat analysis

Paranoid scans more than 10 million emails every day and learns and improves with every message it stops. By constantly analysing large volumes of data, Paranoid has a vast database from which it can compare emails with previous samples. In addition, SoftScan receives further data from honeypots deliberately set up to attract malicious software.

Malware instance monitoring

Paranoid monitors and analyses each email message it scans to ascertain the number of instances of certain malware characteristics that occur over a period of time. This includes subject lines, the rate of transmission, payloads and how it is delivered. Paranoid then uses this information to establish patterns in the data that help to detect when a new piece of malware is distributed via email.

The trouble with depending solely on these methods is that it relies on the quantity and quality of suspicious data previously acquired to light up the radar. With virus writers changing tactics to stealth mode, constant threat analysis and malware, instance monitoring alone is no longer enough.

> *"SoftScan makes email security simple. We don't have to worry about maintenance or updates, and any emails the system isn't sure about – something which is almost inevitable with some of the email addresses of our clients – are easily released.*
>
> *We haven't seen a virus since we started using SoftScan three years ago, Paranoid stops anything that might have otherwise slipped through and that includes malware as yet unknown to the anti-virus scanners."*

David Sorkin, Information Technology Manager, The Appointment Group

Virus Probability Analysis

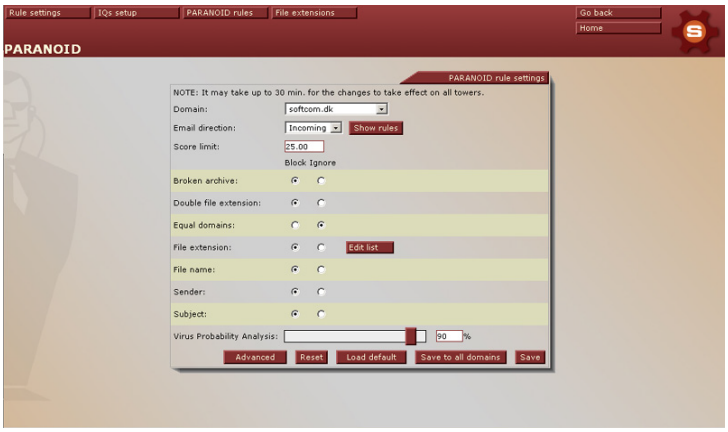
Paranoid's Virus Probability Analysis (VPA) developed exclusively for SoftScan by anti-virus experts, calculates the probability of harmful content within an email.

Once the email has passed through the normal anti-virus filters, VPA carries out a series of steps that includes analysing both the email message and any attachments in great depth. It looks at a variety of different characteristics that may identify the message as suspicious including the binary code of any attachment, the binary type used and what's inside the binary. VPA also investigates the email message itself looking at specific characteristics, where it came from and a series of other distinguishable features.

If the malware writer has deliberately forged the email or binary in an attempt to avoid detection, then VPA switches tactics too and reanalyses the message using a different set of rules.

Paranoid does all this and still delivers your mail with only a five second delay.

This type of analysis uses large amounts of CPU resources, which is why Paranoid leaves the detection of known viruses to traditional anti-virus scanners that are very effective at scanning large databases of malware already listed. Paranoid only receives email that has been through this stage, enabling it to focus its intensive processes on catching zero-day threats and new malware before it enters the network.



SoftScan (UK)
No 1 Liverpool St.
London
EC2M 7QD

020 7956 2029
sales@softscan.co.uk
www.softscan.co.uk