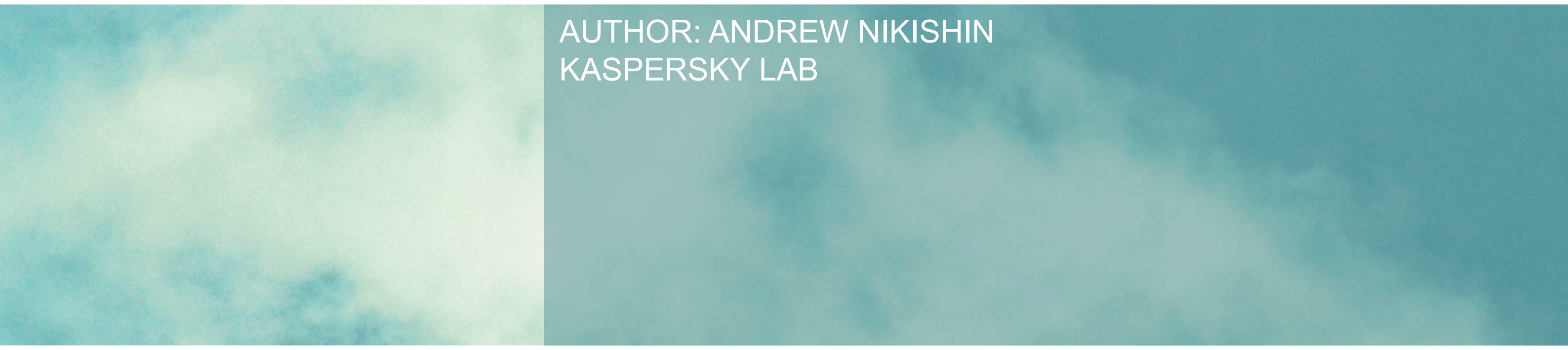
PROACTIVE PROTECTION MADE EASY



AUTHOR: ANDREW NIKISHIN
KASPERSKY LAB

Heuristic Analyzer

Policy-Based Security

Intrusion Prevention System (IPS)

Protection against Buffer Overruns

Behaviour Blockers

Different Approaches to Proactive Protection

Pros and Cons of Different Proactive Detection Methods

CONTENTS

1. INTRODUCTION

Surging numbers of virus outbreaks, hacker attacks making news, network scams, the threat posed by spyware – all of this has contributed to growth in demand for anti-virus systems. There are a multitude of anti-virus solutions on the market. How does one select the best product? Which anti-virus solution can guarantee 100% virus detection rates with the lowest possible false-positive levels? Which anti-virus solution offers the broadest range of technologies to ensure adequate protection of the computer and the network against all kinds of malicious program?

An essential part of any anti-virus product is the so-called anti-virus engine, the module responsible for scanning objects and detecting malicious programs. It is the anti-virus engine that determines the quality of malicious program detection, and therefore the protection level offered by an anti-virus solution. However, due to explosive growth in the number of malicious programs, the importance of pre-emptive – or proactive – methods of detecting malicious software has lately been increasing. These methods help detect malicious software before anti-virus databases are updated – in other words, detect a threat before it appears. Importantly, in this case false-positive rates should also be as low as possible (ideally, there should be no false positives at all).

This document describes and evaluates the main approaches to proactive protection implemented by different vendors. It is intended primarily for computer security experts familiar with the basic operating principles of anti-virus software.

2. PROACTIVE PROTECTION

In the past several years the “death” of classical anti-virus solutions, which use one kind of signature or another to detect malicious software, has been the subject of extensive discussion in the information security market. The principal reason for this is believed to be the speed with which malicious software is spreading, which is faster than the rate at which anti-virus databases are distributed. In addition, some time is always needed to analyze a new virus. Therefore, users remain unprotected from the time a malicious program is discovered until the time an anti-virus database update becomes available. Different companies envisage several different approaches to addressing this situation.

2.1 Heuristic analyzer

When the number of existing viruses exceeded several hundreds, anti-virus experts began to explore the idea of detecting malicious programs the existence of which is as yet unknown to the anti-virus program because the relevant signatures do not exist yet. As a result, the so-called heuristic analyzers were developed.

A heuristic analyzer is a set of subroutines analyzing the code of executable files, macros, scripts, memory or boot sectors to detect all sorts of malicious program that cannot be identified using the usual (signature-based) methods. In other words, heuristic analyzers are intended to search for unknown malicious software .

Heuristic analyzers have relatively low detection rates, as virus writers have dozens of ways in which they can “cheat” them. In addition, heuristic analyzers with high detection rates also have high false-positive levels, making them unacceptable for most purposes. Detection rates of even the best anti-virus products do not exceed 25-30% when it comes to new malicious programs. In spite of low detection rates, heuristic methods are still often used in contemporary anti-virus solutions. There is a simple reason for this: detection quality can be improved by combining various pre-emptive methods of virus detection.

2.2 Policy-based security

A security policy is an essential part of any well-designed strategy of protection against IT threats. A well-designed policy reduces several-fold the risk of infection by a malicious program, hacker attacks or leaks of confidential information. A simple example: if the user is not allowed to open e-mail attachments, the risk of a mail worm infecting the computer is practically eliminated. Blocking the use of removable media also reduces the risk of malicious code penetration. A security policy should always be designed very carefully to take into account the needs and business processes for all divisions and employees of the company.
Besides the approach described above, various vendors mention policy-based security in their information materials. There are currently several approaches to this method of ensuring security.

The Trend Micro approach

Trend Micro Outbreak Prevention Services. This service is based on distributing policies that help prevent an outbreak, i.e. a policy is distributed before anti-virus database updates or patches are released. At first glance, this looks like a reasonable solution. However, Trend Micro is slow to add procedures for detecting new malware, and the purpose of this solution is to “plug a hole” in the slow work of the TrendLab virus lab. In addition, creating a policy takes time (sometimes as long as it takes to analyze a virus and add detection procedures to the AV database), which means that there is still a time period during which a user is unprotected against the new threat. Another shortcoming of this approach is the rate at which security policies are changed. All the advantages of policy-based security are based on infrequent changes of the policies themselves. This helps the staff to get used to which things and actions are allowed and which are forbidden. However, if policies are replaced several times a day, this will only lead to confusion, resulting in no security policy at all. It would be more accurate to see the Trend Micro method as accelerated releasing of a certain kind of signature update rather than a policy-based security approach. Therefore, in most cases this approach is not really proactive. An exception is policies making it impossible to take advantage of certain software vulnerabilities.

The Cisco-Microsoft approach

Limiting access to the corporate network for computers that do not comply with the company's security policy (e.g. not having required operating system updates, the latest anti-virus database updates etc.). To bring a computer in line with the security policy, it is allowed access only to a special updates server. After installing all the necessary updates and performing other actions required by the security policy, the computer is granted access to the corporate network.

2.3 Intrusion prevention systems (ips)

Intrusion Prevention Systems (IPS) are able to close a computer's vulnerabilities that are most often used by malicious programs in order to block new threats before the anti-virus databases are updated. This involves blocking ports to eliminate the possibility of infection penetrating into the computer and further reproducing, creating policies to limit access to directories or individual files, detecting a source of infection on the network and blocking further communication with it. This technology offers good protection against hacker attacks and bodiless worms and viruses, but it is not effective against mail worms, classical viruses and Trojan programs.

2.4 Protection against buffer overruns

The idea behind this technology is preventing buffer overruns for the most common programs and Windows services, including Word, Excel, Internet Explorer, Outlook and SQL Server. Most attacks nowadays exploit various vulnerabilities involving buffer overruns. Preventing buffer overruns can also be regarded as proactive protection, as this technology simply prevents exploitation of such vulnerabilities by any malicious code or attack.

2.5 Behaviour blockers

The history of behaviour blockers goes back more than 13 years. This type of anti-virus software was not popular 8-10 years ago, but as new IT threats appeared, behaviour blockers were remembered again. The main idea behind a blocker is analysis of program behaviour and blocking of any hazardous actions. In theory, a blocker can prevent the distribution of any virus, both known and unknown (i.e. written after the blocker was released). This is the direction in which most anti-virus software developers are moving. There are numerous implementations of this technology. Most mail worm protection systems have lately been developed based on behaviour blocker mechanisms.

2.5.1 «Prehistoric» behaviour blockers

The first generation of behaviour blockers appeared as far back as the mid-nineties (at the height of the DOS virus era). Their operating principle was simple: when a potentially hazardous action was detected, the user was prompted to allow or block the action. In many cases this approach worked, but "suspicious" actions were also performed by legitimate programs (including the operating system), and if the user was not sufficiently competent, the anti-virus program's prompts caused confusion. As personal computers became more widespread, the average user's competence level decreased and the demand for the first generation of behaviour blockers waned.

2.5.2 Behaviour blocker for vba programs. KAV Office Guard

As mentioned above, the principal shortcoming of early behaviour blockers was the frequency with which a user was prompted for action. This was because a behaviour blocker was unable to decide whether a particular action was malicious or not. However, with programs written in VBA it is easy to distinguish malicious actions from useful with a very high degree of accuracy. This is why KAV Office Guard is not as "obtrusive" as its file brethren. However, despite asking the user fewer questions this blocker has not become less reliable: a user utilizing it is protected against practically all macro viruses, both existing and those not yet written. In other words, by using advantages offered by an operating environment it became possible to achieve a reasonable balance between reliability and the number of prompts a user gets. However, in terms of its operating principles KAV Office Guard is still a "prehistoric" behaviour blocker.

2.5.3 Second-generation behaviour blockers

The second generation of behaviour blockers is different in that they analyze sequences of actions rather than individual actions, using this analysis to decide whether a particular piece of software is malicious. This greatly reduces the frequency with which a user has to be prompted, improving detection reliability at the same time. An example of a second-generation behaviour blocker is the Proactive Defense Module implemented in Kaspersky Lab products.

2.6 Different Approaches to Proactive Protection

StormFront, the first product in the new generation of commercial proactive protection systems based on behaviour blockers, was released by Okena, a company specializing in development of intrusion detection and protection systems. In January 2003 Okena was acquired by Cisco Systems, and StormFront was released as Cisco Security Agent. This product is a classical behaviour blocker designed for corporate customers. The product needs to be set up by a qualified administrator before it can be used.

McAfee is actively developing proactive protection technologies incorporated into products in the McAfee Entercept family. These products are able to close a computer's vulnerabilities to a new threat before anti-virus database updates are released (IPS/IDS). This involves blocking ports, i.e. the possibility of infection penetrating into the computer and further reproducing, creating policies to limit access to directories or individual files, detecting a source of infection on the network and blocking further communication with it. In addition, these products are able to prevent buffer overruns for approximately 20 most common programs and Windows services, including Word, Excel, Internet Explorer, Outlook and SQL Server, which can also be regarded as proactive protection. Personal products use only WormStopper, an improved heuristic technology detecting Internet worms distributed via e-mail and blocking suspicious activity on a computer, such as sending a large number of unauthorized e-mails to people in the address book.

Panda TruPrevent is comprised of three components: a process behaviour analyzer, which analyzes the behaviour of processes running on the system and detects suspicious actions, a heuristic analyzer and a set of IDS functions detecting malicious packets and protecting against buffer overrun. The product is positioned by Panda Software as the second line of defence against any unknown malicious software (a classical anti-virus solution is should be used as the first line of defence) and is designed to detect unknown malware launched on the computer. The product is intended for end-users (not an administrator).

In Symantec products, pro-active protection incorporates a built-in heuristic analyzer capable of detecting unknown virus modifications based on their characteristic actions on the system, as well as Norton Internet Worm Protection, a set of IPS/IDS (Intrusion Prevention/Detection System) components blocking the most common paths used by malware to penetrate into the system (Prevention) and detecting suspicious actions (Detection). Also, the company offers Outbreak Alert, a feature providing alerts on particularly hazardous internet threats (supplied as part of Norton Internet Security 2005). In addition, at the service level Symantec offers Early Warning Services (EWS), a service providing early alerts when vulnerabilities are identified. The service is now being integrated into a new system, Global Intelligence Services.

Microsoft is also developing proactive methods of protection against malicious software. The details and time frame are unknown.

Trend Micro's PC-cillin Internet Security 2005 incorporates a heuristic analyzer and an Outbreak Alert System providing proactive notification of new impending threats. Its corporate product, Trend Micro OfficeScan Corporate Edition 6.5, uses signatures with the Outbreak Prevention Service, which automatically configures protection rules to prevent infection from penetrating into the system even before anti-virus databases are updated. This functionality is not available in the personal product.

In BitDefender products proactive protection means a behaviour analyzer blocking malicious programs based on analyzing their characteristic actions on the system (the application monitors system files, the system register and internet activity).

New Kaspersky Lab products use the company's proven heuristic analyzer in combination with a number of cutting-edge proactive protection technologies. Kaspersky Lab products use an intrusion detection and prevention system (IPS/IDS) designed to fight hacker attacks and bodiless viruses. The notification system notifies users of outbreaks and other security events. But the most important innovation from the viewpoint of fighting new threats is the second-generation behaviour blocker. The blocker has an important feature: "rollback" of actions performed by malicious code. This helps dramatically reduce the number of questions the system asks the user and reduce the risk of damage to the system before new malicious software is detected.

2.6.1 Other methods

Mail traffic can be protected using special methods based on analyzing messages passing through a mail server, helping to nip an outbreak in the bud. The following statistics can give grounds for suspecting the beginning of an outbreak:

- Mass mailing or reception of identical attachments;
- Mass mailing or reception of identical messages with different attachments;
- Attachments with double extensions
- Etc.

In addition, linguistic analysis can be performed on message bodies.

2.7 Summary

Summarizing the above, it can be said that the following proactive protection methods are currently available on the market:

1. A process behaviour analyzer analyzing processes running on the system and detecting suspicious actions, i.e. unknown malicious programs.
2. Elimination of possibilities for virus penetration into the computer, blocking

of ports which are used by known viruses and which might be used by their new modifications (the IPS/IDS component).
3. Prevention of buffer overruns for Windows programs and services that are mst commonly used by intruders in their attacks (the IPS/IDS component).
4. Minimization of damage done by an infection, preventing it from spreading further, limitation of access to files and directories, detection and blocking of the source of infection on the network (IPS/IDS component).
Hence, it can be said that proactive protection technologies are developing from a plaything of professionals or computer geeks into a tool for home and corporate users and are becoming a priority area for anti-virus software vendors.

2.8 Pros and Cons of Different Proactive Detection Methods

2.8.1 Heuristic analyzer

Pros:
- A well-known and proven technology.
- Does not require frequent updates.

Cons:
- Takes up large amounts of CPU time.
- Low detection rates (25-30%).
- High false-positive levels (increasing when detection rates go up).

This technology can be used in all anti-virus products both on workstations and on file or mail servers and internet gateways. The heuristic analyzer is currently the only proactive technology that can be used effectively in all anti-virus products.

2.8.2 Policy-based security

Pros:
- An essential part of any integrated approach to security.
- Does not depend on software type.

Cons
- Talking of detection rates makes no sense, as there is no way of calculating them.
- The Trend Micro approach is essentially not a proactive method. It is a variation on the signatures theme, with policy descriptions used in place of signatures. Therefore, in most cases this approach is not proactive.

Policy-based security can be used in some form by any company regardless of size, IT infrastructure or field. Moreover, a well-designed policy can help reduce the risks associated with IT threats several-fold at practically no cost.

2.8.3 IPS

Pros:
- A good technology for protecting against hacker attacks and bodiless worms and viruses.

Cons
- Not applicable to detecting other types of malicious software.
- Requires updating attack signatures.
- This technology has proved to be very effective in products for protection of workstations and internet gateways. IDS can not be used for mail traffic protection.

2.8.4 Protection against buffer overruns

Pros:
- A good technology for protecting against malicious software using vulnerabilities like "buffer overrun" – 100% detection rates.
- Does not require updates.
- False positives practically non-existent.

Cons:
- Can not be used to detect other types of malicious software.
- Most modern computers incorporate support for this technology at the hardware level (NX flag in AMD CPU's, Execution Disable Bit – Intel) – there will be no demand for the software implementation.

Taking into account that all modern processors support buffer overrun protection at the hardware level, the future of a software implementation is doubtful. Despite this, there is demand for buffer overrun protection of workstations, internet gateways and other servers with direct internet connections.

2.8.5 Behaviour blockers

Pros:
- Relatively high detection rates (up to 60-70%).
- A well-known and proven technology.
- Does not require frequent updates.
- Detection of any types of malicious software.
- Requires little CPU time and other resources compared to heuristic analyzers.

Cons
- False positives.
- Behaviour blockers ask users many questions requiring them to make decisions.
- A "rollback" function is required (restoring the system from changes made by the malicious code prior to its detection, at the stage of information gathering).

Behaviour blockers are applicable only in cases when execution of a suspicious program is possible, i.e. on workstations. On mail and file servers and gateways suspicious programs should not be launched at all, and will therefore not need a behaviour blocker.

3. CONCLUSIONS

Of all the proactive methods of detecting malicious software described above, behaviour blockers are the most promising. Intrusion detection and prevention systems and heuristic analyzers also have potential, providing that their shortcomings described above can be diminished. However, none of these technologies alone can cope with the task of ensuring maximum detection of malicious programs with minimum false-positive rates. Only an integrated approach uniting various technologies can achieve this objective.

3.1 Summary Table of Proactive Technologies Used by Vendors

	Cisco	McAfee	Panda	Symantec	Trend Micro	BitDefender	Kaspersky
Heuristic Analyzer		●	●	●	●	●	●
IPS		●	●	●			●
Buffer Overrun		●					
Policy based					●		
Alerting system				●	●		●
Behaviour Blocker	●		●			●	●