eicar

position paper +++ position paper +++ position paper +++ position paper


Rainer Fahs, chairman

"THE FUTURE OF AV-TESTING"

BACKGROUND

Though the principles of self replicating code have been discovered long before, it is now nearly 30 years since the term "Computer Virus" was coined and its negative connotation has not only changed the way of automatic data processing and later network communications but also instigated a never ending challenge to societies and their ethic and moral concepts. When viruses started spreading uncontrolled and begun to impede on business processes governments and industry where in urgent need for defence against a hitherto unknown threat and in consequence the first AV engines and products appeared. Compared to Kondratief's development cycles the evolution of viruses (file, boot sector, stealth, polymorphic, metamorphic, encryption, macro, script) progressed in a remarkable pace and not only the character and types of viruses itself went through continuously evolution following the advancements in computing and network technology, also the proliferation of viral code changed with the evolution in communications technology starting from file sharing on removable media over e-mail and attachments to hidden active code in web-pages and targeted distribution using Trojan Horse principles where human engineering aspects are used as basis for technical approaches in equal proportions leaving the human related defence with laws and regulations trailing the problems.

SITUATION

While virus proliferation reached exponential growth rates and new variants appeared in parallel with new computing technologies only a hand full of AV engines where ever developed, all based on similar technical approach which was – and still is – reactive scanning for known viruses based on signature files. Around these core AV engines a new industry developed trying to keep abreast with the ever increasing amount of viruses and later Trojan Horses and other malicious code. New appearing malicious codes and their distribution techniques required more subtle technologies (cyclic redundancy checking, behaviour checking, and heuristics) in the AV products (AV is used as a synonym for all "anti" products), creating diversity in industry and the products but unfortunately no

eicar

position paper +++ position paper +++ position paper +++ position paper

SITUATION

standardised technology. The dramatic increase of viruses created and the ever increasing speed of infections all across the world in a reactive scanning environment created a problem with sharing of validated samples of viral code. Unfortunately, first discovery and analysis of a new virus created also a business advantage for the vendor of an AV product and thus no centralised sample verification and distribution across national and business boundaries has ever been created. This situation was fostering a business driven approach controlled by the core people in the AV industry who not only controlled the technical approach to the problem but also controlled and limited the intellectual approach to it. Access to samples of viral code (viruses in the wild) was, and still is, limited to a few "bona fide" researchers within the AV industry who closely control and monitor who is part of the club and who is outside, creating a competitive situation to scientific research.
In the early days, when viruses started to cause business disadvantages to industry an attempt to unite efforts against this new nuisance resulted in the founding of the European Institute for Computer anti Virus Research (EICAR) where most of the AV vendors participated in joint efforts against the ever increasing spreading of viral code. However, the active participation and willingness to share information was reciprocal to the business success of vendors. New developments or advancements in AV technology where not any more commonly shared research products but rather industrial research results, limiting the sharing of them between birds of a feather.

EICAR´S VIEW

The biggest common achievement – and hitherto the only one – was the creation of the EICAR Test file, a string of code that AV products recognise and confirms the correct installation of a product, the only standardised method of limited testing of an AV product. The ever increasing demand of better AV products also created a requirement to test these products. Starting with the Virus Test Centre (VTC) at Hamburg University the testing of AV products became a business itself and the common way of testing was – and still is – testing against real virus (Wildlist) samples. This created a situation – which is also still valid today – where a non standardised product was tested by diverse non standardised methodologies developed by each tester, with subsets (Zoo testing) of virus samples, leaving the results of the testing interpretable but suitable for marketing purposes. Testing methodologies have been adapted to the changing environment by the individual testers but no common approach to testing of AV products has been developed. Of course, AV product testing evolved from sheer AV testing to Malware testing, but still based on samples of malicious code. In consequence the ever increasing size of signature files extends scanning time for a PC and occupies critical resources thus limiting increasingly the computing power of the environment.

eicar

position paper +++ position paper +++ position paper +++ position paper

CURRENT CHALLENGES WHAT WE SEE:

- *"Bona fide researchers" from industry*
- *Position of these "bona fide researchers" is that writing of viruses (or creation of malware) is "prohibited", even for scientific researchers*
- *The EICAR code of conduct prohibits the distribution of viral code (malware), but allows the sharing of such information between researchers. "...exchange of such information with institutions, companies and persons is accepted, which are responsibly researching or are active in combating in this sector."*
- *This approach has lead to a situation where the defence side is dependent on the creativity of the bad guys who write new malware first before anti-measures or mechanisms are developed. This in principle has created a scientific deadlock, laming real scientific research in a pro-active way.*
- *Pro-active scientific approaches are required otherwise we will continue to be dependent on malicious intended new developments, a continuously race between "bad" and "good" resulting in reactive methods.*

The resulting complexity of AV products and the ever increasing emerging new threats and vulnerabilities of computing environments require a new approach to testing.

IT IS EICAR´S VIEW THAT TESTING SHOULD BE:

- based on agreed standard methodologies, within standardised test environments against clear established criteria making test results less interpretable,
- transparent and repeatable.
- should be developed by an independent organisation with involvement of all stakeholders based on scientific research.

eicar

position paper +++ position paper +++ position paper +++ position paper

SOLUTION: A TWO TIER APPROACH

1.

To foster a pro-active scientific approach the EICAR conference for the first time will host as part of a research project in close collaboration with ESIEA a challenge where students and any security researcher who wants to participate will demonstrate how to circumvent or disable AV products in different computing environments (mainly Win 7 in user mode). The objective of the research project is to learn from the challenges and to pro-actively advise the AV industry on hardening options for their products – if so required. The challenge will be in a strictly controlled environment and results will be available directly to conference attendees and of course the AV industry.

2.

Secondly EICAR will present at the next EICAR conference a new EICAR Test method, a routine allowing testing of the functionality of AV products without the requirement to use samples of viral code with respect to the current most widely encountered threats. EICAR has initiated research to issue new evaluation tools on a regular basis.

The new EICAR Test method will be publicly available as download product from the EICAR web site after the EICAR conference.

CONCLUSION:

EICARs position to unite efforts against malicious attempts on behalf of the user require this new independent scientific approach which results in the challenge and the new test method in support of the EICAR overall objectives and even more important, are in support of a united effort (inclusive the AV industry) and not in competition to the AV industry.

The demonstration of a new test method is beneficial for the AV industry and the user since a user is able to test by himself a product and thus having an objective analysis on the quality of the tested product.