Blocking internet threats: the avast! script engine

INTRODUCTION

Scripts are programs generally developed to control and operate various applications, such as web browsers, but are also increasingly used by malware creators.

In the past, email was the typical entry point for a computer infection. That has changed and the majority of all new infections are now delivered to computers via script-based malware. Consequently, all modern antivirus programs must be able to deal with such malware.

The avast! script detection engine has been designed with an emphasis on stopping malware at the point of entry. This white paper provides a technical overview of the advanced script detection engine used in avast! 5.0.

WHAT IS A SCRIPT?

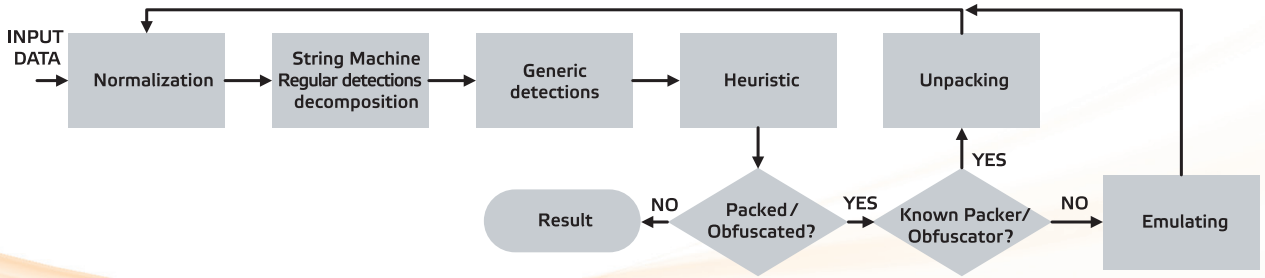
Scripts are often distributed, executed and interpreted from source code or byte code. Unlike compiled applications, which are generally platform-specific, scripts are usually platform independent and used to control or operate some other application – a web browser, for example. Because scripts to do not need to be compiled, they are relatively easy to create and modify which makes them ideal tools for malware creators – especially as they can be used to exploit vulnerabilities in a wide range of commonly used applications.

The most commonly used scripting languages are those which can interact with web applications and native operating system scripting (Java Script, Visual Basic Script, HTML, etc.). Script-based malware is often used to create the conditions and behavior necessary for exploiting a vulnerability in a specific target application (Microsoft Internet Explorer or Adobe Flash Player, for example).

As the volume of script-based malware has increased exponentially during recent years, it has become increasingly important for antivirus solutions to be able to detect and mitigate such threats.

TECHNICAL OVERVIEW OF THE AVAST! SCRIPT ENGINE

The script engine in avast! comprises a number of components or modules, which interact as shown in the diagram below:



The script engine in avast! has a number of features including:

- **Input data normalization** – Scripting languages are often case insensitive meaning that code written in uppercase can perform the same functions as code written in lower case. Simply adjusting the case of a portion of a script's code can make it invisible to the pattern matching engines in many antivirus solutions. Similarly, adding white spaces to the code can also confuse the pattern matching engine. The normalization module in avast!'s scripting engine standardizes the case and removes white spaces to produce a standard, unified form that is then processed by the engine's other components.
- **Fast scanning mechanism** – The normalized input data is scanned for signatures. At the end of the process, intelligent signature processing determines if the input data contains any signs of malware.
- **Decomposition** – This module is included inside the pattern matching algorithm and splits the script into small chunks that can be processed separately by the other components of the script engine. The goal of producing smaller pieces of

code is to speed up slower detection algorithms, especially when complex documents are being analyzed. Decomposition is very successful in enabling the detection of web-based infections where only small parts of a web page are infected.

- **Fast and easy signature addition** –To provide maximum security, it is important that new signatures can be added to the engine and tested in a speedy manner in order that updates can be pushed to end users in the shortest possible time. The script engine in avast! has been designed to enable this to happen.
- **Powerful generic and algorithmic detections** – Standard signature-based detection cannot be relied on to detect all strains of malware and malware families. The script engine in avast! has been designed to enable the speedy addition of algorithmic detection signatures. These generic signatures are very successful at detecting entire families of script-based malware (exploits, downloaders, packers, etc.).
- **Sensitive heuristic detections** – Algorithmic approaches to detect new and previously unseen malware are included in the core of avast!'s script engine. These detections are designed to be extremely sensitive and enable the setting of user-specified triggers.
- **Packed and obfuscated script detection** – Script-based malware is often created using third-party tools that transform simple scripts to more complex scripts with an identical functionality. Such transformations are used to bypass antivirus engines that would recognize the source script, but cannot recognize the transformed code. The avast! script engine contains algorithms to detect transformed scripts, along with algorithms for reverse transformation (a process known as "unpacking") for the most commonly used public script packers.
- **Detections directly connected to the URL blocker database** – This is a similar approach to signature-based detection, but detection is based on the host URL. This method can be used to discover the various redirection routines that direct users to malware distribution networks.

In order to provide maximum protection, the script engine interacts and integrates with other components and modules in avast! including:

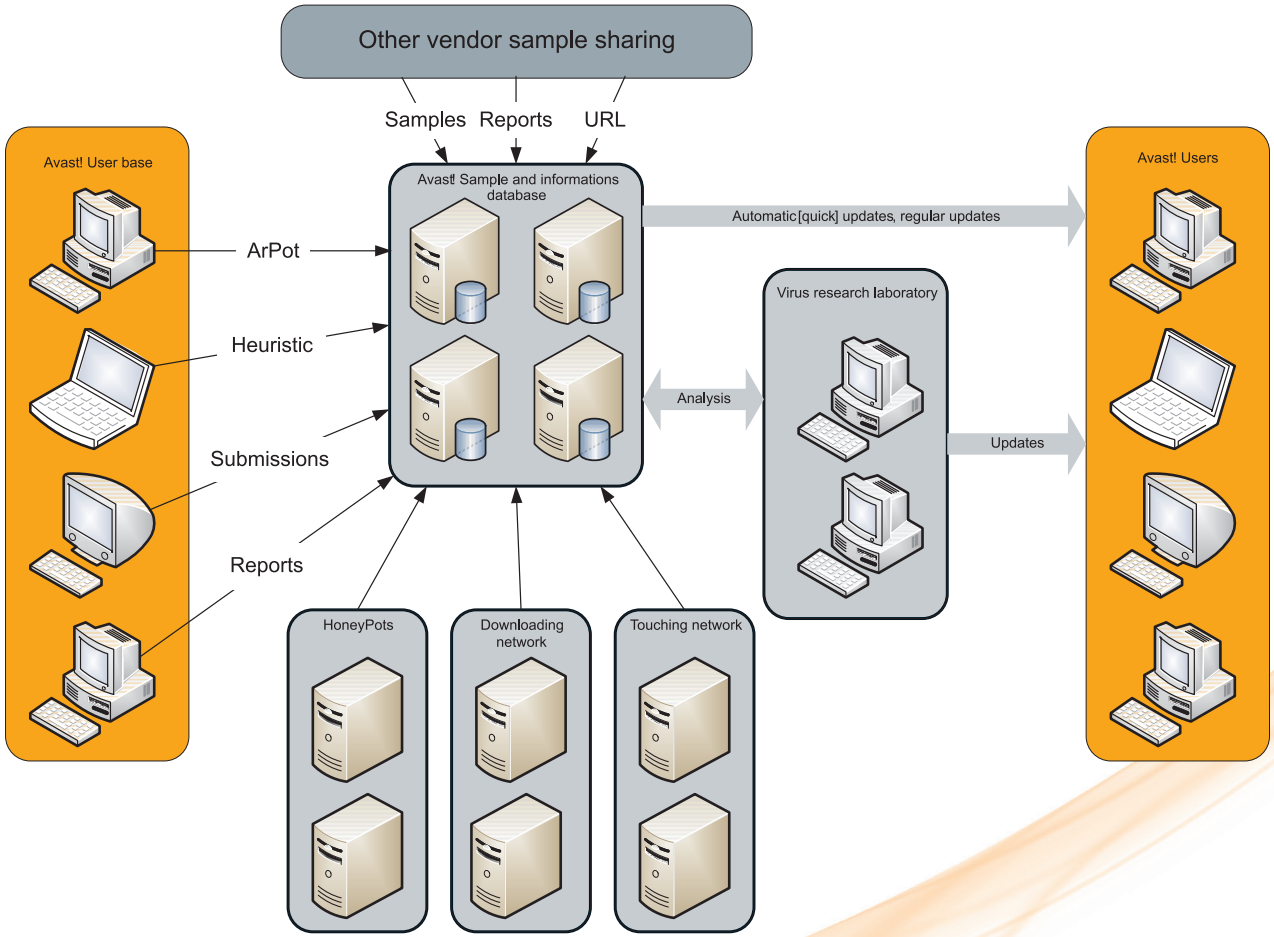
- **Web Shield** – The Web Shield is a feature of avast! that monitors and filters all HTTP traffic. As an increasing number of viruses (and other malware such as adware, spyware and dialers) are being distributed via the web, the need for effective countermeasures has increased. The Web Shield acts as a transparent HTTP proxy and is compatible with all major web browsers, including Microsoft Internet Explorer, Mozilla Firefox and Opera. Unlike many competing solutions, the Web Shield's impact on browsing speed is negligible. This is because of a unique feature called "Intelligent Stream Scan" that enables the Web Shield to scan objects on-the-fly, without the need for excessive caching of data. Stream scanning is performed in memory – without the necessity to flush the contents to disk – providing the maximum possible throughput.
- **Script Shield** – The Pro and Internet Security editions of avast! include an additional module, not contained in the Free Antivirus edition, called the Script Shield. This module watches all Windows Scripting Host (WSH) scripts being executed in the operating system and scans all the scripts (both remote and local) run as part of a web page within the Windows Scripting Host or Internet Explorer.
- **File System Shield** – File system protection ensures that no virus will be started on the computer. It offers a wide range of settings, such as the option to specify that files will be scanned during copying, or that scanning should include only files with a specified set of extensions.

HOW MALWARE SAMPLES ARE GATHERED

In order to protect users from newly released script-based malware, the script engine needs to be updated with new signatures, new generic signatures and new heuristic signatures. The majority of this background information comes directly from the avast! Virus Lab, where malware samples are collected from various sources as indicated in the diagram:

By collecting samples from multiple sources, AVAST is able to ensure that it is able to release updates that mitigate new and emerging threats in the shortest possible time:

- **avast! user base** – avast! users can elect to provide data to the company in order to help fight malware. This data can be split into four categories:
  - **Behavior Shield** – Intelligent behavioral sensors included in avast! 5.0 monitor computers for signs of suspicious activity. Any incident is reported to AVAST's database servers together with any additional context information that may be needed for further analysis.
  - **Heuristic** – Samples determined by avast! as potential malware are sent to AVAST's servers for detailed analysis.



- **Manual submission** – Manual submission of suspicious samples through email or directly through the avast! interface
- **Reports** – Any incident can be reported to AVAST's servers to build statistics about spreading malware.

– **Honeypots** – Dedicated servers with the ability to monitor and catch any suspicious behavior or attack. These servers automatically collect samples and data from bots and worm infections all over the web.

– **Downloading network** – Any reported URL is checked for its content. If it really contains malware samples or web infections, it is added to the Touching network list.

– **Touching network** – Monitors websites that were either previously infected or distributing malware.

– **avast! sample and information database** – Used to store information about every sample AVAST receives. Every incoming file is processed through various operations in order to identify suspicious samples:

- **Data mining** – Important data is stored directly in AVAST's databases.
- **Offline heuristic analysis** – Extremely sensitive heuristic detection methods are used to distinguish actual malware samples from clean samples.
- **Offline clustering** – Algorithms are designed to separate incoming samples into similar groups.
- **Automatic signature generation** – ready to be used in pulse and regular updates, to ensure that users are protected against threats in the shortest possible time.
- **Automatic update creation**.

– **Virus Lab** – Deeper analysis and development of complex detection methods. Creation of manual updates.

CONCLUSION

Scripts are being used more and more frequently in web-based attacks and are also becoming increasingly sophisticated and harder to detect. The script engine in avast! has been designed from the ground up to provide users with industry-leading protection against scripts, and to ensure that users are protected against new and emerging threats in the shortest possible time.

ABOUT AVAST SOFTWARE

Based in the Czech Republic, AVAST Software (formerly ALWIL Software) has been producing industry-leading security solutions since 1991 and is the developer of the award-winning avast! product line. As a global company, AVAST has partners all around the world who contribute to the continuous development and improvement of their products and provide technical support to clients in their native language.

AVAST's mission is to provide both home users and businesses with solutions that are easy-to-use, affordable and exceptionally effective.

To find out more about AVAST Software and the avast! product line, please visit **www.avast.com**.