The FireEye Difference

The Competitive Advantages of FireEye Technology

OraTech Consulting Limited

Topics

- What Gets Analysed?
- What's in the Box?
- The Hypervisor
- Monitoring Virtual Execution
- Where to Put the Sandbox
- Management Overhead

What Gets Analysed?

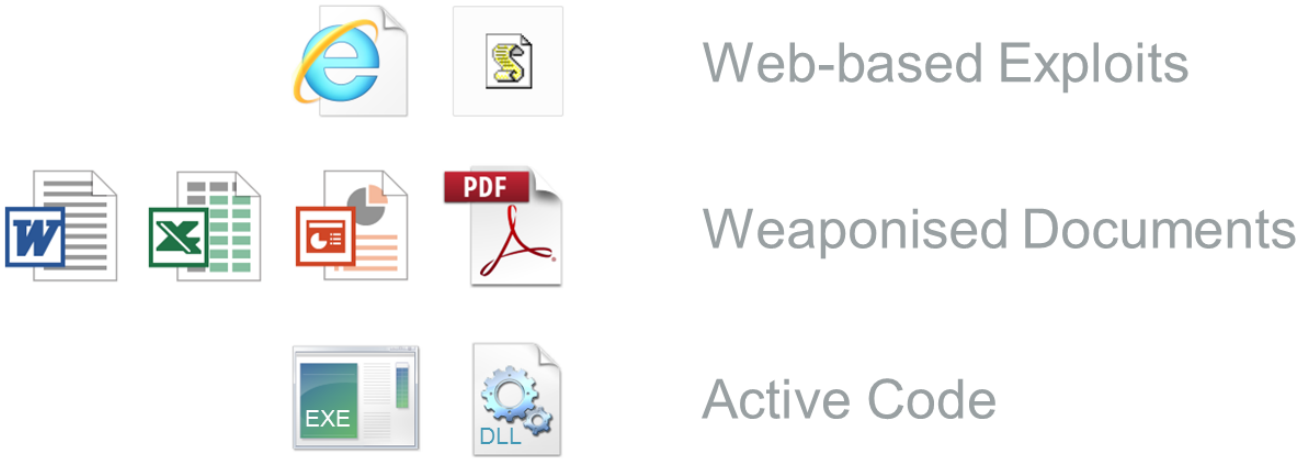
The Issue

With high volumes of organisational web and email traffic, it would be impossible for any advanced threat detection solution to submit all content for virtual analysis (sandboxing). Therefore a decision must be made as to which types of content get submitted and which don't.

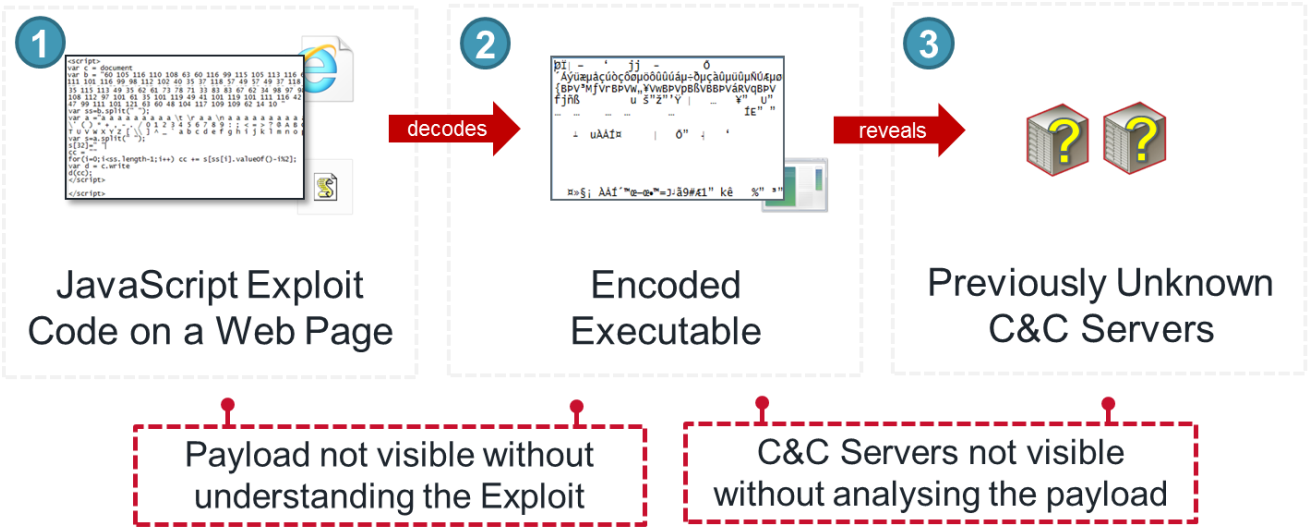
Getting these 'Input Criteria' right is key to detection efficacy and scalability.

Why it Matters

Advanced threat actors use many types of content to mount their attacks. Binary executable types like EXE and DLL are obviously worthy of inspection, but targeted spear phishing attacks more commonly use weaponised PDF or MS Office documents. Drive-by and watering hole attacks, on the other hand hide their exploits in web page content .

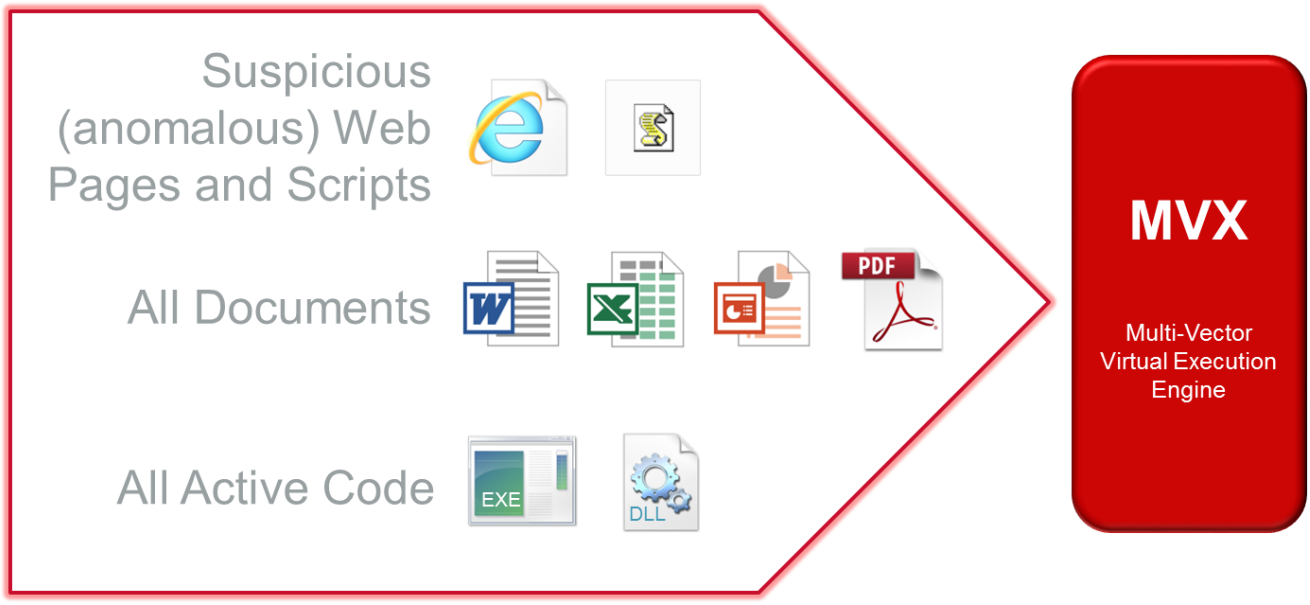


In more sophisticated web-based attacks (including Operation Aurora from as far back as 2010) the exploit is the key to the entire attack, by decrypting all further components as they are written to disk. Miss the exploit and you miss the attack.



The FireEye Difference

FireEye is not just a sandbox for running executables. It is the result of a five year research project to isolate and analyse all types of threatening content. Set against the current threat landscape, this 'threatening content' includes executables, Java applets, PDF files, Office documents and importantly, the suspicious web page content where exploits are found.



FireEye's decision of what to analyse is entirely led by the current state of the threat, and will continue to track this as it evolves. It is not led by the technical limitations of a hastily assembled sandbox.

Questions to Ask About Advanced Threat Detection Solutions

- What types of content get sent for virtual/sandbox analysis?
- Can it isolate and send suspicious web page content (like obfuscated JavaScript) for analysis

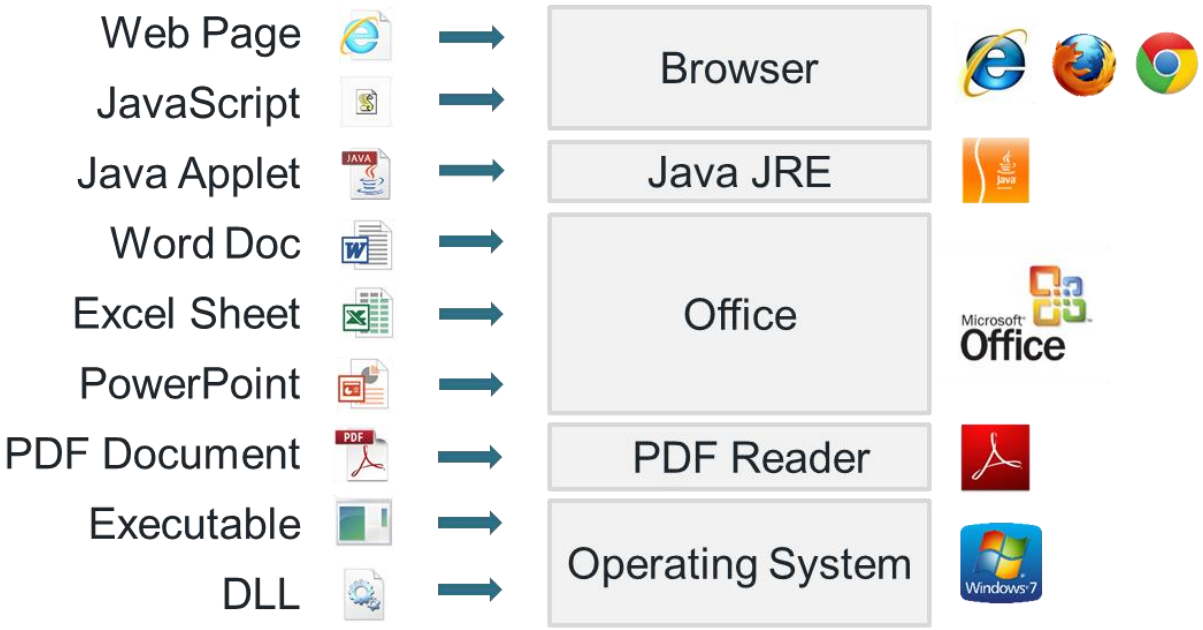
What's in the Box?

The issue

Having established that a wide variety of content needs to be selected for analysis, it is important to consider how that content will react when placed into the virtual analysis or sandbox environment.

Why it Matters

It's all very well selecting a wide range of content types for submission to your sandbox, but what's the point of submitting a suspicious Word document if the sandbox does not have a copy of MS Office to react with it?



Once again, dealing with executables is easy - they only need a basic Windows environment in which to run. Exploits and document-based content however, need a reactant – a matching client-side application that can open them.

To complicate things further, attacks may be constructed to react only with specific versions of these applications and plug-ins. So not only is the range of applications and plug-ins in your sandbox important, but also the range of versions of each. There are no simple solutions here.

The FireEye Difference

For analysis, FireEye runs Windows guest images fully populated with all the usual desktop applications and plug-ins. In fact FireEye currently offers five different varieties of guest image, accommodating different versions of Windows with different application and plug-in versions.

FireEye Guest images include various versions of client side applications and plug-ins, including:-

- Adobe Reader
- Adobe Flash Player
- Java Runtime Environment (JRE)
- Internet Explorer
- Firefox
- Microsoft Office
- Many others

By selecting the most appropriate guest image (or if in doubt, running the same content in several guest images) FireEye can provide the closest execution environment to your own workstations – a critical success factor for detecting advanced attacks.

Questions to Ask About Advanced Threat Detection Solutions

- How many different OS and service pack combinations are available for virtual analysis?
- What applications and plug-ins (and what range of versions) are available in the sandbox to react with my content?

The Hypervisor

The Issue

All Advanced Threat Detection solutions use some form of virtualisation technology to provide the many disposable sandbox instances that are required to analyse enterprise content. The underlying operating system used to arbitrate resources between many virtual operating systems is known as a hypervisor. Common hypervisor technologies include VMware, Microsoft Hyper-V, Oracle VirtualBox and Zen.

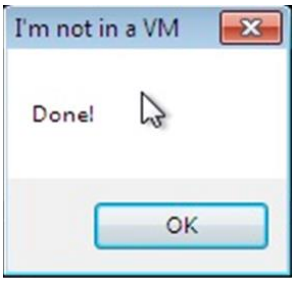
None of these commercial hypervisor products were designed with security analysis in mind, and most will disclose their identity freely by means of running processes (like VMware Tools) or device identities (like VMware Virtual SCSI Disk).

Why it Matters

Advanced malware is often 'VM aware' and will actively seek out markers of common hypervisors when deciding whether or how to execute.

The FireEye Difference

FireEye uses a custom hypervisor, built from the ground up for the purpose of security analysis. It shares none of the common markers of the commercial hypervisors, and is therefore much more resistant to detection.



Questions to Ask About Advanced Threat Detection Solutions

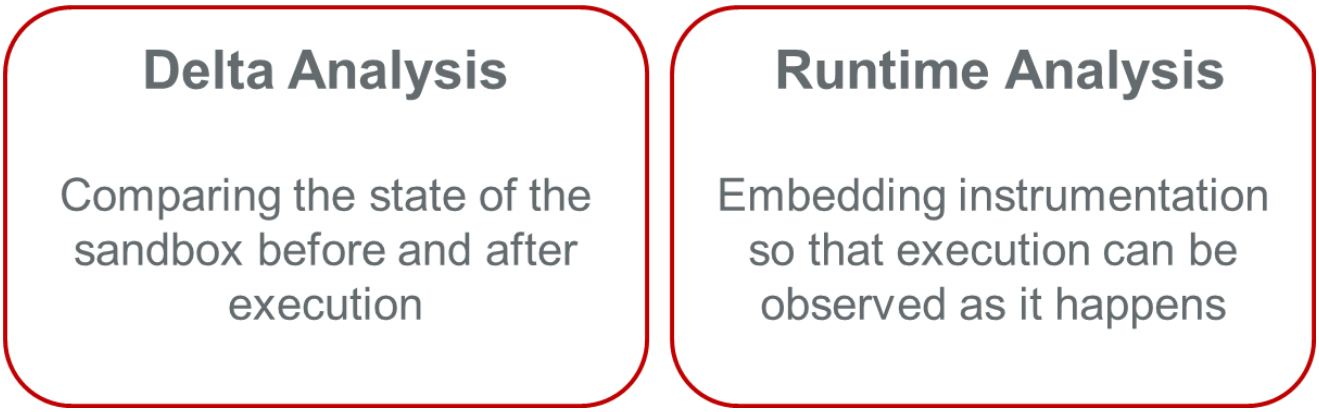
- What type of hypervisor is used? How would it resist VM aware malware?

Monitoring Virtual Execution

The Issue

Pacing the right content into a sandbox with the right reactant applications is only part of the story. How you monitor and react to the execution of that content is critical to detection efficacy.

There are two main technological approaches to this:-



Technically speaking, delta analysis is relatively trivial to implement. Runtime analysis is much more challenging, as it involves placing instrumentation inside the VM, or hypervisor, or both.

Why it Matters

Delta analysis will only record changes that are persistent after execution has completed. It cannot 'see inside the box' during runtime, so it is unable to:-

- See any operations that run in memory
- See files that are written and subsequently deleted
- React to evasive operations that the malware might perform (like going to sleep for 30 minutes).

The FireEye Difference

FireEye performs analysis with full runtime awareness, using deeply embedded instrumentation. It can observe every step of malware execution and act upon a wide range of conditions like:-

- Malware going to sleep
- Malware requiring mouse movement or keystrokes before executing
- Malware making DNS or other network requests

FireEye is able to provide a detailed chronological log of everything that occurred during analysis, including operations running in memory and files that were written but subsequently deleted.

Questions to Ask About Advanced Threat Detection Solutions

- How is execution monitored? Is it simply by comparing a snapshot of the VM before and after execution?

Where to Put the Sandbox

The Issue

Virtual execution is a CPU-intensive activity. Providing this capability on premise requires expensive CPU-dense hardware.

A quicker route to market is to locate the capability in the cloud where CPU capacity is easy to provision and less expensive.

Why it Matters

The cloud model requires that content be sent out of the organisation for analysis. This is not much of an issue for executables, but a huge issue when it comes to documents.

Cloud services are always multi-tenanted and potentially hackable.

Some advanced malware is location-aware, and will only execute inside the target network.

The FireEye Difference

All virtual execution takes place on-premise, with no files submitted to the cloud. Results are available in minutes, not hours or days.

Questions to Ask About Advanced Threat Detection Solutions

- Do you have any issue with your documents being submitted to a cloud service?

Management Overhead

The Issue

Advanced threat detection is a complex space. IDS/IPS and network anomaly based solutions are renowned for 'noise', false positives and administrative overhead.

Often customers must set their own balance between detection and false positives by tuning policies and maintaining whitelists.

Why it Matters

Not every customer has the time, skills or inclination to maintain this policy balance.

Policy de-tuning and 'whitelist creep' lead to heavily degraded security over time, and interesting events do not stand out from the background noise.

The FireEye Difference

FireEye has no policy, no rules, no tuning, and near zero false positives.

It can be installed and adding actionable intelligence (without noise) within hours.

Questions to Ask About Advanced Threat Detection Solutions

- How much time do you expect to spend monitoring, tuning and administering the solution?