

Behind The Scenes Security: eEye in Focus

Creating an Award Winning Product

The eEye / Norman partnership is a strong one. Norman was chosen as the only anti-virus¹ to be utilized within Blink Endpoint Security², regarded as one of the strongest host-based protection suites on the market³. Norman was selected for its unique ability to identify malware via generic sandbox methods while also supporting this tool with rapid malware signature development. In a world where the cat-and-mouse game of malware authors vs. anti-virus vendors constantly keeps the end-user behind the 8-ball, Norman decided to develop a powerful Windows emulator that can analyze the behavior of a potential piece of malware during runtime without causing any undesired effects to the host system. Blink has seen immediate success with this addition to the suite, and eEye is very proud of the incredible protection we've been able to offer our customers for even the most cutting edge malware and exploits.

Advancing Research Services

The eEye Research Team also utilizes the stand-alone Norman Sandbox Analyzer⁴ and Analyzer Pro⁵ tools to deliver timely intelligence and response to our eEye Preview⁶ customers. The eEye Preview customers encompass some of the most sensitive critical infrastructure industries, so timely and informative analysis is an absolute necessity. eEye Research has some of the best and brightest minds when it comes to exploit and malware analysis, but must also lean on a suite of home-grown and outside-developed automated tools in order to assist the researchers with the large amount of analysis requests from our customers.

Rapid Analysis

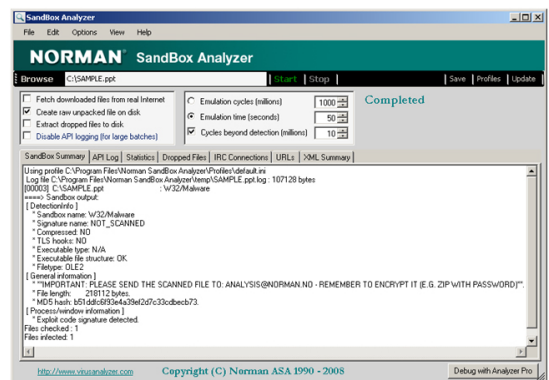
At the forefront of malware and exploit auto-analysis tools is the Norman Analyzer. This tool allows the eEye Research to get a very quick idea of what a sample might potentially be doing before analyzing it at a binary level.

The overall concept of the Analyzer is to unleash the Norman Sandbox against multiple samples in a very rapid fashion in order to quickly profile them for potential malicious intent. While this unique tool is incredibly effective at identifying

standard malicious trojans and binaries very quickly, the eEye Research Team utilizes the tool to perform analysis of potentially malicious files without any previous signature detection from another AV vendor in order to identify previously unknown malware or potentially zero-day exploit threats.

Expanding Instant Exploit Discovery

The Norman Analyzer also includes functionality to search files for exploit code. This is a very important ability, as it allows eEye Research to utilize the Analyzer against our very large database of potentially malicious files, typically Microsoft Word, PowerPoint, or Excel files. When eEye Research identifies a sample via the Norman Analyzer with a log entry of "Exploit code signature detected and will start executing there", the Research Team immediately knows that it is dealing with a very serious sample. The Analyzer will then extract the "dropped" executable (typically a trojan) from the file, and then run that through a separate analysis. The eEye Research Team is expected to analyze hundreds (if not thousands) of potentially malicious documents a week; performing this type of "tier-1" analysis allows the team to focus manual malware dissection resources to the most critical issues, while still ensuring that a very large percentage of exploit documents are being identified immediately in an automated fashion.



This tool effectively allows the Research Team to perform large amounts of analyses within minutes that would normally take weeks if not months if being performed manually by reverse engineering methods.

¹ <http://www.eeye.com/html/assets/pdf/VB100eEye-May08.pdf>

² <http://www.eeye.com/html/products/blink/reviews/index.html>

³ <http://www.eeye.com/html/assets/pdf/ISM.pdf>

⁴ <http://www.norman.com/microsites/malwareanalyzer/Products/analyzer>

⁵ <http://www.norman.com/microsites/malwareanalyzer/Products/analyzer-pro>

⁶ <http://www.eeye.com/html/services/preview/index.html>

Where No Tool has Gone Before

When more information about a specific sample is required, the Analyzer Pro tool is often used by eEye Research to perform deep-dive analyses on malicious binary samples. This allows the Researcher to perform a very technical analysis of a binary on his own workstation in rapid fashion without the need of setting up a test environment or worrying about VM detection.

One of the most useful tools is the ability to “jump backwards” while debugging a sample. This allows the researcher to more effectively analyze a sample and seemingly “go back in time” to differentiate memory-that-was to memory-that-will-be, saving very important time during the analysis process. This is not an option when debugging malware on a live system, and if the Researcher skips ahead even just one instruction, he or she is required to revert the system in order to review the memory map of the sample at that specific time. This issue is exacerbated by the need to perform this analysis outside of a VM (because of the numerous VM detection methods employed by malware) and wait for a hardware revert system to restore the image to a clean state.

Another important feature of Analyzer Pro are the many options available when it comes to networking, perhaps most importantly the ability to allow for full networking capabilities, thereby allowing the sample to communicate with the Internet directly.



This unique ability allows the researcher to effectively “sniff” network traffic of the sample while it is still in a sandbox, potentially allowing for botnet monitoring or malicious traffic signature development. When this type of work is being done on hardware without emulation, it becomes difficult to know for certain that the network host’s network sniffer is no longer tainted, and would require an inline traffic sniffer, thereby making a seemingly simple endeavor a very complicated one.

Combining Security Intelligence

Norman understands that they must constantly push the envelope when it comes to the analysis of future threats and how to deal with exploits and malware from a detection aspect. The eEye Research and Norman Research teams regularly consult one another on performing more effective detection and analysis, and both teams have been able to increase their independent knowledge of how exploits and malware work in a modern environment. The Norman teams constantly deliver timely and effective updates to all of their products, and have an incredibly quick turnaround when it comes to feature enhancements or the seldom requested bug fix.

Overall, the Analyzer and Analyzer Pro tools delivered by Norman have become some of the most often used tools by the eEye Research team when analyzing file-format exploits and malware samples. The eEye Research Team relies on these tools on an hourly basis to deliver timely intelligence to some of the most sensitive eEye Preview customers, and is able to attribute expansions within eEye Research’s malware analysis capabilities directly to utilizing the Norman Analyzer and Analyzer Pro tools.

About eEye



eEye Digital Security®

eEye Digital Security® is pioneering a new class of security products: integrated threat management. This next-generation of security detects vulnerabilities and threats, prevents intrusions, protects all of an enterprise’s

key computing resources, from endpoints to network assets to web sites and web applications, all while providing a centralized point of security management and network visibility.

eEye’s research team is consistently the first to identify new threats in the wild, and our products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself. Founded in 1998 and headquartered in Orange County, California, eEye Digital Security protects more than 9,000 corporate and government organizations worldwide, including half of the Fortune 100. For more information, please visit www.eeye.com



Norman Data Defense Systems is the US subsidiary of leading European security vendor Norman ASA. Based in Washington, DC and San Francisco, Norman DDS offers the complete Norman portfolio, which includes analysis tools and solutions for malware, spyware, spam, and phishing as well as a desktop firewall. Through its Norman SandBox technology, Norman leads the way in the world of proactive anti-virus solutions. The company is anticipating dynamic growth in 2007 and beyond with the addition of some exciting new products and the expansion of its current partner network. To find out more about the company, visit Norman Data Defense Systems on the Internet at www.Norman.com/US.

NORMAN®