WHITE PAPER:
SYMANTEC CYNIC™

Symantec Advanced Threat Protection

Symantec Cynic™

Who should read this paper

This white paper is intended for CIOs, CISOs, and security professionals tasked with protecting their organization from targetted attacks and advanced threats.

This paper gives an overview of the new Symantec Cynic™ technology introduced with and used by Symantec Advanced Threat Protection.

Symantec™

Content

Overview

Threat actors have easy access to malware development tools that make it cheap and easy to develop customized targeted malware that is undetectable by traditional security systems. These same tools also include features which enable malware to become undetectable by the most popular sandbox products, such that with the check of a box, your investment in advanced threat detection becomes worthless, and the bad guys breach your network. Symantec was built on the ability to identify malicious files at scale, and we plan to deliver the analytical power of Symantec directly to your organization through Symantec Advanced Threat Protection.

Cynic is a cloud-based dynamic malware analysis service that provides the ability to detect advanced threats. Unlike most sandbox analysis products, which focus on offering a variety of virtual machines or customer-specific images to detonate and detect malware, Cynic uses a suite of analysis technologies, coupled with our global intelligence and analytics data, to accurately detect malicious code.

By performing analysis in the cloud, Symantec can offer more in-depth processing at a scale and speed that cannot be achieved with an on-premises deployment.

Proven Technology

One of technologies included within Cynic is Symantec Skeptic™. Skeptic has been in use for more than a decade within the Symantec™ Email Security.cloud platform, protecting against threats that are not detected by signature-based antivirus scanners. The static code analysis offered by Skeptic is undetectable by malware authors and cannot be circumvented by VM-evasive behaviors. In fact, due to the years of machine learning accumulated within the technology, the more evasive a program behaves, the easier it is to identify it as a malicious file.

A second proven technology employed by Cynic is SONAR™. SONAR is a behavioral analysis system that monitors files as they run, comparing the behaviors of the program to the behaviors of the billions of malicious samples Symantec has analyzed over the years. As opposed to signatures, SONAR employs behavioral profiles and file reputation data to accurately identify files as benign or malicious. The level of accuracy provided by SONAR enables easy comparison between network and endpoint security events, allowing related security events to be correlated and, if appropriate, marked as automatically resolved.

Virtual Execution and Detonation

The newest technology included within Cynic is a proprietary virtual execution system, also known as a sandbox environment. Like other sandboxes, this system employs multiple virtual machines utilizing different operating systems. On these virtual machines, Symantec uses components of Symantec Workspace Virtualization™, powered by Altiris Technology, to switch various applications into the virtual machines to check for application exploits and unique targeted attacks. For each operating system, Symantec is able to rapidly change out the versions of frequently targeted applications, such as Java™, Adobe Acrobat Reader™, and Microsoft Office™, to quickly evaluate files across different platforms. The analysis component included in this system benefits from the Symantec Global Intelligence Network, which enables telemetry-driven execution and conviction of advanced threats. Additionally, Symantec can provide unique insight into the threat actors themselves, using the trillions of rows of analytics and telemetry to associate new threats with those previously linked to known adversaries.

As with all other sandbox based detection methods available in this space, the Symantec virtual execution system will be subject to detection by malware code. Between August 2014 and April 2015, Symantec noted a rise in "Hypervisor Aware" malware from 18% to 28%[1], showing that malware authors are attempting to evade sandbox detection. For this reason, Cynic includes an additional layer of analysis on physical hardware. This layer is employed for malware samples that attempt to check if it is being analyzed in a hypervisor. When malware detects

[1] Symantec Internet Security Threat Report, volume 20

that it is running in a virtual machine, sometimes it will do nothing, hoping to remain undetected. Or worse, it will behave differently than it would on a physical machine, thus misleading incident responders who may be looking for evidence of compromise.

Cynic compares the results from the virtual analysis with the results of the physical analysis to make sure that the indicators discovered are the most useful for the detection of the threat.

Summary

Symantec's multi-dimensional analysis is a true next-generation execution environment. Cynic takes the results from all of these technologies and provides the verdict and analysis results to you, along with valuable threat intelligence that Symantec has on the sample, to give you the information you need to take action.

Cynic is currently able to process all Windows executable file types, as well as Java, PDF, Microsoft Office documents, and container files such as ZIP. Detonation and analysis occurs on Windows XP and Windows 7, on 32 and 64 bit platforms. Additional file types and operating system coverage will be added over time.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com