WHITE PAPER:
SYMANTEC™ ADVANCED THREAT PROTECTION

Detecting Advanced Threats and Evasive Malware with Symantec Cynic™

Who should read this paper

This whitepaper will explain the benefits of a cloud-based approach and detail the detection mechanisms within Symantec Cynic, which is included with Symantec Advanced Threat Protection.

Symantec

Content

Introduction

Threat actors have 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 has invested decades in building technology to accurately identify malicious files at scale, and with Symantec™ Advanced Threat Protection we deliver the full analytical power of Symantec directly to your organization through a next-generation analysis service called Symantec Cynic™.

Cynic is much more than a sandbox detection application. Rather, it is a cloud-based malware analysis platform consisting of many technologies, including sandboxing and detonation, static based detection, file reputation, context intelligence, and network traffic analysis. Unlike the majority of other sandbox analysis products, which require customers to provide dedicated virtual machines or organization-specific images to detonate and detect malware, Cynic uses this suite of analysis technologies across multiple operating systems and multiple application versions. Running as a cloud service makes it possible to do this analysis at a scale and speed that is almost impossible to achieve with simpler on-premises sandbox products. And as a cloud service can be rapidly updated without causing downtime, Symantec can update the detonation environment operating systems and applications at will so that it adapts as attacks and malware change.

Further to this, we can make use of physical hardware within the Cynic cloud platform to trigger virtual machine-aware malware that is specifically designed to evade today's sandboxing detection. This rapid analysis over multiple scenarios, platforms and application versions, coupled with intelligence from our massive global sensor network data, means Symantec Advanced Threat Protection is able accurately detect malicious code fast and minimize the risk of false positives.

Access to Symantec Cynic is included with all of the three Symantec Advanced Threat Protection control point products:

- Symantec™ Advanced Threat Protection: Endpoint
- Symantec™ Advanced Threat Protection: Network
- Symantec™ Advanced Threat Protection: Email

A Cloud-Powered Execution Environment

Symantec has a well-established track record of providing highly-available cloud services, with almost two decades of SLA-beating performance with Symantec Email Security.cloud and Symantec Web Security.cloud.

In true cloud fashion, Cynic is built as an elastic service that scales on-demand to process as many objects and requests as necessary. In turn, without being constrained to a particular size or constrained by an amount of processing power, Cynic can utilize a large number and variety of images and, by using Symantec Workspace Virtualization technology, it is able to rapidly cycle through multiple scenarios covering a matrix of different application versions to trigger advanced malware and trace its execution behavior effectively.

Finally, by running this as a cloud service, Symantec has the ability to upgrade the Cynic detection technologies, add new file type support, and add new scenarios without requiring upgrades or changes on our customers' part, meaning that the best possible protection is online at all times without enforcing upgrade cycles - reducing the cost to maintain and manage the on-premises side of security infrastructure.

Detecting and Tracing Advanced Threats

Cynic detects malicious code and suspicious behavior by using a proprietary conviction engine to inspect files using the vast array of prevention and detection technologies that Symantec has created over decades of research and development. This conviction engine arrives at either a clean or malicious verdict based on the results from all of these components analyzing the file, along with data from our massive cyber intelligence and sensor network.

To make sure it is able to detect malware behavior accurately, Cynic's execution environment leverages a variety of behavioral tracing technologies monitoring both user-mode and kernel-mode hooks. It observes not only the operating system and applications but also the network activity through external packet capture.

The behavioral tracing technology only adds value if malware is triggered. To have an effective execution environment, it has to have a large variety of images on which the malware will execute. These images and scenarios cover many permutations of operating system versions, operating system patch levels, application versions, and run-time environment versions.

When it comes to evasive malware, a growing trend is for malicious files to detect and identify the execution environments themselves, so they can either avoid detection or exhibit completely different behaviors in the hope of throwing security solutions off their scent. There are a number of ways that malware attempts to modify its behavior based on the environment:

1. It may look for specific security vendor processes, files, or registry keys that are created and used by agent-based behavioral tracing.
2. The current crop of sandbox technologies place a limit on the amount of time they spend executing and analyzing a file, so malware will often try to sleep over that time period.
3. It may look for evidence that it has landed on an actual endpoint and not a VM by checking for specific proof of human interaction prior to activating its payload, such as mouse scrolling or clicks, keyboard interaction, or even specific device drivers.
4. Malware also tries to communicate with external network locations to detect tracing, detect isolation or even to communicate with command-and-control servers as part of its infection actions. Because Cynic executes the malware in a secure environment, it allows malware to communicate externally and analyzes this traffic as a part of the data sent back to the conviction engine.
5. Some malware will not run when it detects specific hardware resources, for example, looking for physical CPU cores, and uses the access characteristics as a way to avoid detection. For example, the response time for an emulated or virtually abstracted CPU might be different to that of an actual CPU on physical hardware.

To avoid falling for these and other malware evasion techniques, Cynic has been engineered with a large number of built-in techniques, including a proprietary human behavior simulator that replicates realistic human interaction, along with a physical execution environment as an additional measure against virtual machine-aware code. Cynic makes dynamic decisions about which files to route to this physical execution environment based on observations in other analysis engines, including anomalies or suspicious results sent to the conviction engine, such as if it has detected evasion techniques and unusual static analysis results. Intelligence-led execution is also a key differentiator for Cynic. It has the unique advantage of leveraging Symantec's vast telemetry to make informed decisions based upon a file's reputation or different behavior in its execution environment, compared to the real world.

The computational power afforded by delivering Cynic as a cloud service allows the file execution, tracing, and conviction to be performed in minutes, as opposed to the hours or days it would take an on-premises solution. The conviction verdict and file behaviors are returned directly to Symantec Advanced Threat Protection, which is then able to uncover attacks that would otherwise evade detection and use the detailed intelligence to quickly search for any other related attack artifacts across the infrastructure.

Turning Execution Data into Actionable Intelligence

All three of the Symantec Advanced Threat Protection control points can send suspicious or unknown files to Cynic for analysis. After the file is processed, Cynic will return up to three sets of data back to the Advanced Threat Protection platform.

1. Verdict: A binary decision, it is either clean or malicious.
2. Execution report: The full trace of the files behaviors when executed.
3. Intelligence report: Any and all information Symantec knows about the threat.

Symantec Advanced Threat Protection provides a consolidated view of all three of these data sets as an Incident - a collection of one or more suspicious events or activities that are important enough to highlight to a security analyst. All of the incidents for an organization's infrastructure, across endpoint, network, and email, are displayed in the Incident Manager. This is a single view within Symantec Advanced Threat Protection's management console where a security analyst can coordinate the investigation and remediation of suspicious and malicious files. A demonstration of the investigation and remediation capabilities is available at http://atp.symantec.com

When Cynic returns results on a malicious file, there are two automatic actions that Symantec Advanced Threat Protection will perform.

1. A new incident will be created in in the Incident Manager.
2. Advanced Threat Protection: Email will block the email from delivery if a verdict is returned within the maximum hold time set by the email administrator.

The incident includes data returned as part of the execution report, which is a summary of the events and actions that a file takes when it is executed. The report output details disk reads and writes, any network communications initiated by the object, and any files, processes, and registry keys that are created or modified. It also includes data on the evasion techniques used by the object such as the amount of time it was in a sleep state, or any tasks or processes that were scheduled to take place. These data points can be used by a security analyst to discover other infections across the organization using the powerful search and sweep capabilities built in to Symantec Advanced Threat Protection.

Along with the data specific to this file, Cynic will supply detailed information that Symantec knows about the attack, including countries where the attack or file has been seen before, when it was first and last seen, all known and alternative paths and filenames, alternative files created and any related or similar files, and whether Symantec believes it is an attack targeted at the organization.

Symantec Advanced Threat Protection will also correlate any incidents that match or are related to this attack in one place, without requiring any manual searching. Security analysts can visualize and quickly remediate all related attack components. For example, all files used or created as part of the attack, all email addresses to which the attack was targeted, and all malicious IP addresses and domains. This significantly reduces the number of incidents that security analysts need to investigate and means that advanced attacks can not only be detected but also be contained in in minutes, not weeks or months.

Summary

Symantec's multi-dimensional analysis is a true next-generation execution environment. Cynic both utilizes many of Symantec's best of breed and patent pending technologies and is backed by the ingestion of 60GB of new aggregated security intelligence every day. This Intelligence is fed by tens of billions of events from millions of endpoints and gateways. All of this 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 able to process and return intelligence on all portable executable file types, as well as Java containers, PDF documents, Microsoft Office documents, and container files such as ZIP. Additional file types and operating system coverage will be added over time.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

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