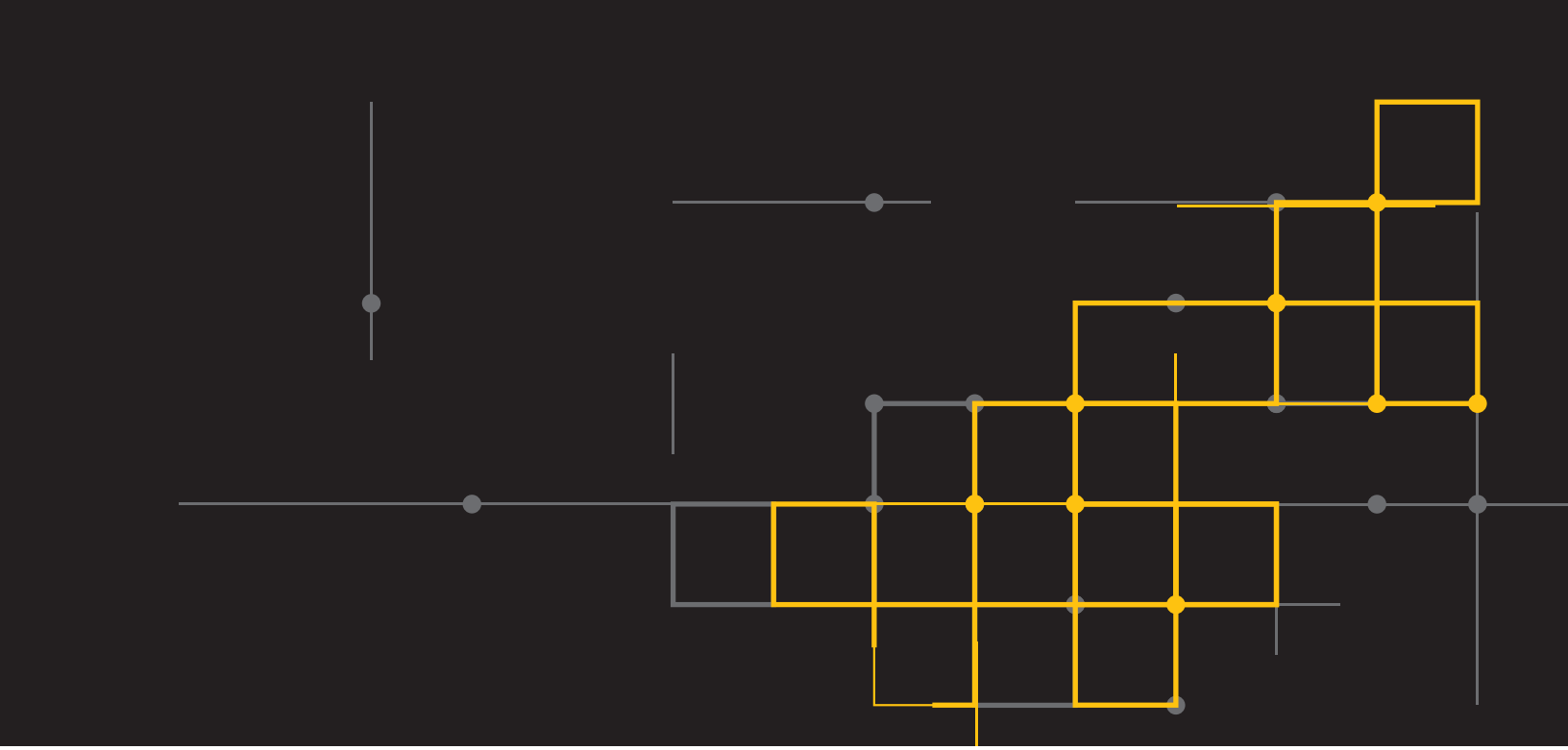

Symantec™ Cloud Generation Malware Analysis

White Paper | February 2017

Symantec™

Defeat Advanced Threats With Symantec Cloud Generation Malware Analysis

The success of recent malware attacks has made headlines by crippling corporations, robbing shareholders, and damaging the credit of thousands of consumers. These attacks make it abundantly clear that cybercriminals continue to evolve, creating adaptive threats and malware that can that can bypass the security defenses of many organizations. Some advanced malware can actually sense a sandbox environments and mutate like a biological virus.

At the same time, hackers continue to show endless ingenuity in penetrating corporate networks. As reported in the media, they gain entry through a variety of devices and third-party suppliers, including health insurance providers, printers, thermostats, and vending machines. Open public networks, cloud applications, and an expanding ecosystem of connected devices, all of which offer routes into your devices and networks, make the lives of cybercriminals easier.

This paper describes how malware is evolving, how it functions, and how it can be identified, neutralized, and blocked by what we refer to as cloud generation malware analysis, which is available as a robust enterprise cloud service. Let's start with how the blizzard of advanced malware alarms is affecting IT security teams.

The Car Alarm Syndrome

To a busy security team, dealing with up to hundreds of alarms every day can be numbing. This is similar to the car alarm phenomenon, in which a 1997 a study of insurance claims covering 73 million cars indicated no overall reduction in theft loss due to car alarms. And a law enforcement study of car alarm noise in New York City found that up to 99 percent of alarms are false. We can reasonably say that almost nobody pays much attention to them anymore. Unfortunately, there is a parallel in network security today.

Take the case of a large U.S. retailer. Using an opening unwittingly provided by an HVAC vendor, hackers introduced malware into the store's system just prior to the 2013 holiday shopping season. When the malware became active, it siphoned off customers' credit card data from point-of-sale checkout operations. The company's offshore security analysts detected the activity and sent an alarm to corporate headquarters. The company did not act. Days later, the security team sent another alarm, and again IT failed to take action. Weeks later, the U.S. Department of Homeland Security informed the retailer that approximately 40 million credit card numbers had been plundered from the company's system and were being offered for sale on the black market. Customers began staying away; sales plummeted; and the store's stock declined.

So the need is clear: a new defense to deal with a new generation of advanced threats—one that sends fewer but more meaningful alarms. To achieve this, companies need both the tools and the architecture to combat evolving threats.

Advanced Malware Can Learn to Avoid Detection

As network security advances, malware in turn grows more aware and adaptive, mutating like a biological virus to evade behavior detection. This can happen in various ways.

Virtual Machine Awareness

One powerful way to discover new malware attacks is sandboxing—isolating suspected or unknown files in a virtual machine (VM) environment that mimics a company's desktop systems. While isolated in the sandbox, suspect files are examined. If the file exhibits suspicious behavior in the sandbox, it is recognized as malicious, and information about the file is used to prevent further attacks from the newly discovered malware. In this instance, the malware's activity actually exposes its identity. An increasing number of attackers, however, are creating malware that can detect a virtual environment. If the VM-aware code senses a sandbox, it will disguise itself by going dormant or performing non-malicious acts, reducing the effectiveness of the sandbox.

How does malware detect virtual environments? One way is by determining if a live person is interacting with it. If the malware contains a dialog box, it will expect a human response. If nothing happens, the malware will presume it's in a sandbox and go dormant. Another way is by checking for virtual device drivers, telltale registry entries, and other giveaways. An example of this is unexpected system timing elements. In an actual Windows environment, events happen quickly, with known predictability. When hackers run performance calculations to check elapsed time for specific operations, a noticeable lag exposes the virtual environment.

Polymorphic Files and URLs

Malware files can mutate like an infectious virus to escape signature-based detection. Using automated systems, hackers can change a letter, insert a few extra bits, pack (compress) the code, reverse some nonessential instruction, or add some junk data, and then recompile to generate thousands of variants. Every time the file presents itself, it looks different. There is no vaccine for this. Signature-based security systems can't cope with the flood of viruses; some of them are bound to penetrate and begin to operate.

Attackers apply similar tactics to URLs, using domain-generating algorithms (DGAs) to mathematically compute new domains. The malware has access to these algorithms, allowing hackers to communicate with a URL for a set length of time (hours or days) and then move on to another URL; blacklisting just can't keep up.

Multistage, Multivector Attacks

Cyber criminals can tailor their activities to a specific target by selecting among web-based, email, or file-based intrusions, coordinating them, and staging the timing of events to achieve a focused result.

Encrypted Communication

Because most network security systems are unable to scan encrypted data to detect malware, hackers find it effective to use secure sockets layer (SSL) technology to build communication tunnels between embedded malware and remote command and control (C&C) servers.

Misleading File Types

Malware may masquerade as harmless files. Executable files may pretend to be JPEGs. There may be executable files inside a media file, an Excel file, or a PowerPoint file. A malware file can initially have a .jpg extension and then be renamed with an .exe extension and run by a second malware file. So, if your defenses are set to block all executables, the JPEG file may make it through and lie in wait until another file arrives that can change it to an executable and turn it on.

Sleeping Malware

Malware may be programmed to lie inactive until a specified date, exemplified by New Year's Day and April Fool's viruses. The virus may be analyzed but not considered malicious because it is dormant.

User Interaction Triggers

Malware requires a response in order to be activated. Because it often pretends to be legitimate, it may display a dialog box asking users to install some software. It will probably be accompanied by certification and a Windows "look" that seems familiar and friendly. The user clicks, "Yes – install," and the malware begins operating. Without user interaction, the malware remains passive. Legitimate software may be packaged inside malicious software; download a free version of something popular, and you may get more than you bargained for.

Unique and Targeted Malware

Some malware can be incorporated in a targeted "spearfishing" attack. It will trick you into opening a file by using information specific to you. The hackers may be very familiar with your environment and the assets they're looking for. They may look for a specific system state, such as the presence of a custom application, which indicates a desired target. Malicious malware may look for the directory path that leads to its target. It leaves no signature and is rarely exposed.

The Solution: Cloud Generation, Targeted Malware Analysis Services

New technology from Symantec—Malware Analysis Services—ensures strong capabilities to address evolving attack techniques. Specifically, advanced analysis techniques that identify and neutralize malware designed to evade detection. These techniques block known threats, analyze anything new and not known, and stifle evolved attacks. By grading the risk of each threat, the car alarm syndrome disappears.

Dual Detection Methodologies

The Symantec Malware Analysis Service uses a powerful combination of emulation and virtualization to identify both types of malicious code—VM-aware and nonVM-aware. Virtualization takes place in a virtual machine—a fully licensed version of Windows in which the user can install any application (Office, Adobe, Quicken, or custom applications) that are built in-house. We call it Intelligent VM, or iVM.

The emulative sandbox environment is not Windows software. Instead, it is a fully re-created computing environment based on a Windows-like API. In this completely controlled artificial space, users can exercise the malware to make it think it's interacting with a real computer. For example, if the malware is set to sleep until a specific date, the malware analysis service can make it believe that day is here.

It's extremely difficult for any malware author to evade both the virtual and emulative environments. This unique combination is resulting in extremely high success rates in identifying malware.

Kernel-Level Detection

Symantec malware analysis detects behaviors deep in the kernel—not in the user space. This makes detection evasion difficult because evasion techniques are programmed in the user space. The intention to perform malicious action remains discoverable in the kernel, and the malware analysis service reports on these low-level events. So, even if malware authors are able to display harmless characteristics, Symantec analysis sees the truth deep in the kernel.

AntiVM Environment Settings

Malware authors know how to look for indicators of a virtual environment, such as virtual devices or telltale registry settings and keys. To combat this, Symantec has spent years and taken great pains to make its virtual machine environment undetectable to malware. The Symantec Malware Analysis Service applies multiple settings that include changing virtual device names, removing registry entries and disabling guest additions. If the malware tests the waters by offering up a dialog box or asking questions, the malware analysis service responds like the real system.

AntiVM Pattern Matching and Risk Rating

The Malware Analysis Service replaces signature-based detection with behavior detection patterns. Symantec developed hundreds of behavior patterns, and a subset of them is specifically designed to catch malware as it looks for the presence of a virtual environment. The malware analysis service analyzes behaviors deep in the kernel, looking for specific actions.

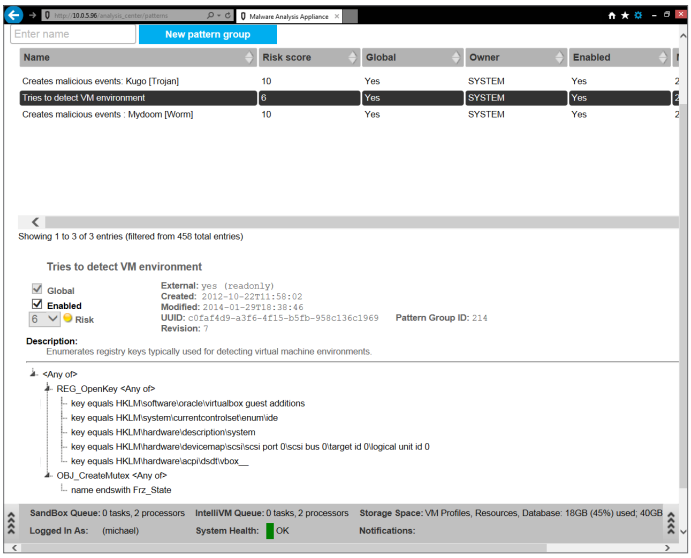

Figure 1. Malware Analysis Service "Grades" Each Risk
The highlighted malware is trying to detect a VM environment by checking registry keys. The keys can be hidden or removed to make them undetectable. Instead of giving malware a binary "good" or "bad" label, the custom pattern matching of the Symantec Malware Analysis Service applies a grade to the seriousness of each risk as it's identified. Scoring the threats helps to eliminate false alarms.

Using Symantec™ Advanced Threat Prevention

Multiple Lines of Defense

Done right, malware analysis provides enhanced protection against the evolved techniques of malware authors. But if not deployed effectively, there may be an ocean of responses to trivial malware, leading to car alarm syndrome: too many alarms, followed by overreaction, followed by the dangers of benumbed under reaction.

Symantec™ Web Security Service	• Block all known web threats • Allow known good traffic with application white listing, and block known bad traffic with malware scanning
Symantec™ Malware Analysis Service	• Analyze unknown threats

Figure 2. Symantec Malware Analysis Service
This cloud generation service helps users overcome car alarm syndrome by incorporating advanced malware analysis in a complete security solution to perform the tasks shown here.

Building Trust by Scoring and Prefiltering

The filtering power of the intelligent, in-depth defense provided by the malware analysis service reduces the need for analysis and grade threats to eliminate false alarms. It also builds trust in the reliability of the system. The content analysis capabilities of the Symantec Web Security Service draw on a database of more than one million records to identify applications and files in real time. It allows prefiltering of threats by scoring them on a scale of 1 to 10 to determine if they are malware, goodware, or unknownware.

A file or application that has been coming into the system for years without a problem would rate a 10. Another that is unknown but comes without negative reports could be rated a 2 or a 3. A retail organization, like the one described earlier, would rate malware that targets cash registers and point-of-sale card swiping as a 1. A company running Linux® will register the entry of Windows®-targeted malware, but it will not be rated high enough to create an alarm that requires attention. Some industries, such as banks, may choose to restrict downloads to high-rated known good files.

With content analysis capabilities, fewer files will be sent to antimalware engines and sandboxing systems. Alarms will be fewer and more meaningful. To put this in perspective, the following facts represent a typical business day at a financial organization—a Symantec customer with 250,000 employees:

- Employees make 660 million attempts to contact websites.
- They make 2.2 million attempts to access known malicious sites that are blocked by the Symantec Global Intelligence Network, using input from threat information of 15,000 enterprises and 175 million consumer and enterprise endpoints.
- Network perimeter antimalware blocks 244 malicious files.

Keep in mind that the blocked sites referred to here are truly malicious, not simply undesirable. They could include popular and trusted sites that have been infiltrated and corrupted. The point is that the tremendous potential for generating alarms, and the time-consuming challenges this presents to IT security, are greatly reduced.

The Symantec Malware Analysis Service delivers actionable information about malware attacks. It provides detailed analysis of malicious behavior patterns, key indicators that malware has compromised something in the system, and a timeline for how malware works.

The Advanced Threat and Malware Prevention Architecture

Symantec's approach provides an elegant, high-efficiency architecture for advanced cloud generation analysis and associated incident resolution. It functions as follows:

1. A user downloads content from the web through the Web Security Service secure gateway, which has content analysis capabilities to check the file in real time against the known-good file whitelist database hosted in the Global Intelligence Network. If it's listed there, the file is delivered and the processing is finished.

2. If the file is not whitelisted, it's scanned by one or two antivirus (AV) engines in the Symantec Web Security Service. If the file is a known-bad (rated 0) it is blocked and its URL is added to the Global Intelligence Network.

3. If the file is neither known-good or known-bad (rated 1), it can be sent to a sandboxing service. When sandboxing is complete, the result goes to the content analysis portion of the Web Security Service. If the file is malicious, the system updates its file hash database and tells the proxy component of the service to block all subsequent requests to the same object. It also updates the Global Intelligence Network with the object's URL, file hash, timestamp, and filename.

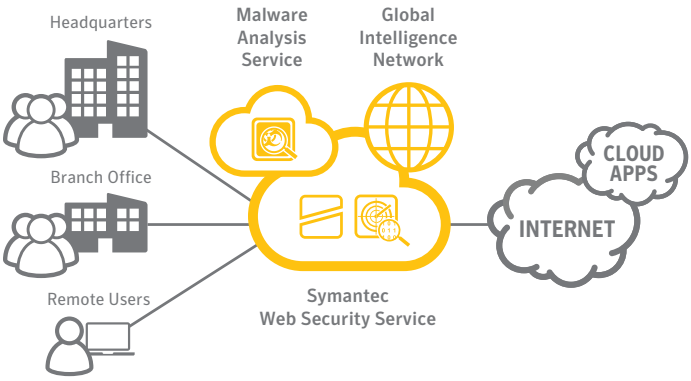

Figure 3. Symantec Cloud Security Services
Cloud-delivered services for access control, advanced threat protection, web security, and information protection.

Advanced Threats and Malware Require Cloud Generation Analysis and Protection

Corporate networks are challenged by the two connected problems described above: too many alarms, and evolved malware with ingenious abilities to avoid detection.

The solution is a cloud-based service architected to combine a secure web gateway, incident containment, advanced malware analysis, incident resolution, and a threat-scoring system that signals alarms on a rational basis. The Symantec Web Security Service, along with the integrated Symantec Malware Analysis Service, provides the advanced threat prevention needed in a cloud-based subscription service. These powerful tools can be used to accomplish a key corporate core objective: protecting company assets by passing the known-good, blocking the known-bad, and quickly and accurately analyzing the unknown.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec Corporation World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com