Technology Spotlight

Next-Generation Endpoint Security Beats Malware Variants Through Behavior-Based Analysis

Sponsored by: Stormshield

Duncan Brown
January 2016

INTRODUCTION

Enterprises are increasingly being attacked by threat actors that are using ever more ingenious and innovative methods to breach defenses. Actors know that traditional endpoint protection solutions, such as antivirus, are based on signatures that identify known threats, and so they alter the appearance of malware by creating variants. These variants look different, thus avoiding detection, but act in the same way as the original malware. This IDC Technology Spotlight addresses how new antimalware approaches are required to combat malware variants, and discusses a behavior-based approach to malware detection offered by Stormshield.

WHY TRADITIONAL ANTIVIRUS APPROACHES ARE INEFFECTIVE

We are seeing an unprecedented and seemingly limitless explosion in the number and types of attack being launched on a daily basis. For example, ENISA (the European Network and Information Security Agency) cites a 14-fold increase in the number of PC malware infections since 2012 (source: ENISA Threat Landscape 2014).

The traditional, and still prevalent, method of detecting malware is to create a signature, which acts like a fingerprint used to identify a specific piece of malicious code. All widespread antivirus software applications and many network-based malware detection solutions (such as firewalls) work on the premise of signatures.

Signatures work well, as long as the malware has been seen before and a signature created. But signature-based technologies have two fundamental weaknesses. Firstly, they only work on malware that has been seen previously. If a completely new malicious program is released then no antivirus solution will detect it. The second weakness of signature-based methods is that it is relatively easy to recompile the malware source code with a few extra lines of redundant code, creating a variant of the original malware. This compiled object would appear different to an antivirus program, but still retain its malware properties. Subsequent iterative enhancements in the malware would also result in new variants. It is easy to see how simple it is to generate numerous variants of a single piece of malware, and in fact this process of creating variants is widely automated now.

Other types of variants include malware programs with essentially the same operation and function as the original, but created by a different originator. These copycat variants are just as potent as the originals, but often have added features to circumvent protection mechanisms introduced to detect and remediate the original malware.

For example, Dridex, a notorious Trojan malware aimed at the banking sector, was apparently disabled in October 2015 when the network of botnet servers was seized by law enforcement officers. However, within one month, Dridex had resurfaced, and had spawned 10 new variants.

Similarly, the success of CryptoLocker has spawned a number of similarly named but otherwise unrelated Trojans that operate in much the same method as the original, yet are entirely different from a signature-based detection standpoint.

Estimates vary, but sources put the number of new variants at between 350,000 and 1,000,000 each day. At this rate, a traditional signature-based approach to detect malware seems pointless: no antivirus program is updated on anything like the frequency required to cope with this proliferation of malware. The cycle of malware detection, fingerprinting, updating of the malware database, and distribution of new fingerprints to endpoints is too long and cumbersome to cope with the number of variants now appearing.

Clearly, then, we need a different approach to detecting malware. While signature-based antimalware programs still have their uses, they are now insufficient to cope with the rapid growth of malware variants.

The problem remains, though, that we are still searching for malware that, by its nature, evades traditional methods of detection. How then can we detect and to protect ourselves from that which we do not know exists?

DETECTING UNKNOWN UNKNOWNS

Much has been said and written about the concept of the inevitable breach. The idea is premised on the proliferation of malware and the prediction that, using signature-based approaches, an enterprise cannot conceivably keep out all variants of malware all of the time. The implication of this assessment is that enterprises need to look for evidence of malware across their estate, and assume that malware already exists within their organization. A corresponding shift away from traditional *prevent and protect* strategies and toward an emphasis on *detect and respond* approaches follows. But organizations then face challenges in resourcing the new skills required to analyze breaches and react with remediation techniques.

Or enterprises can maintain a list of known good applications. This is the converse of maintaining a large database of malware signatures. Rather than looking for bad applications (malware) and blocking it, the enterprise looks for good applications and allows only these "white-listed" apps to run.

This is a reasonable approach, but it suffers from a similar problem to that of malware variants: the proliferation of applications. Enterprises often have hundreds or even thousands of applications which are perfectly legitimate, but which change on a highly frequent basis (for example, as they are upgraded with new functionality). The rate at which applications are updated betrays the use of agile software development practices that can generate a new version of a program on a near-daily basis. Thus the known-good approach is similarly hamstrung by the substantial effort of maintaining and updating the list of known-good applications and their variants.

But what if we searched for malware not based on how the physical object file appeared, but how it acted? Two completely different types of ransomware, coming from different origins, would appear completely different to any signature-based antivirus solution. However, they would act in very similar ways, accessing a computer's registry, contacting a command and control server, encrypting files, and so on. A protective system based on examining the actions of the malware would detect this similar activity, and would assume it was malicious.

This approach addresses not only the issue of looking for known knowns and the management overhead of maintaining white-listed applications. It also solves the issue of scale, and renders the proliferation of malware variants irrelevant. This is because, although there is a high and increasing number of malware variants, they operate in very similar ways. The number of malware behaviors is considerably smaller, and is thus much more manageable as an approach.

The question then is how to implement such an approach. Clearly, the primary modus operandi will be based on an analysis of how malware operates. Some systems use a heuristic techniques – these are approaches based on best guesses and other imperfect but practical problem solving methods. The value of these approaches, that they can work on partial information, is also their weakness. They are often based on incomplete information that can lead to variable results including a high number of false positives.

Similarly, some approaches use an analysis of statistical data. These approaches compare families of malware and extract data from multiple variants such as file size, code metrics, and so on. These approaches require a high number of samples from which to generate sufficient data in order to detect malware. And malware originators can tune their output to avoid meeting statistical thresholds, thus circumventing detection.

A more rounded approach to these problems is to focus less on the physical manifestation of malware – its appearance and structure, for example – or rules based on partial information, and to look instead at what the program actually does: what behaviors it exhibits that betray its purpose.

CONSIDERING STORMSHIELD ENDPOINT SECURITY

Stormshield Endpoint Security (SES) is a next-generation endpoint security solution that monitors and blocks suspicious behavior in applications and operating systems. It works not by looking for the physical attributes of an application that is suspected malware but by examining what that program does.

Malware programs exhibit certain types of behavior that no valid or authorized application would exhibit. For example, legitimate applications would never have a need to use keystroke logging capability, or make changes to protected operating system files, or access memory that has not been allocated to it. It follows that any application that is attempting to do such things is probably malware and should be quarantined or disabled. (In some instances such behaviors are in fact legitimate, in which case a SES administrator may authorize such actions.)

SES works in this way, and operates at a kernel level to detect not only application-level malware but that aimed at the operating system itself too. SES can detect a variety of malware behaviors such as illegal memory access and vulnerability exploitation. Importantly, it also detects suspicious behaviors by legitimate applications: one of the common methods of payload delivery is via embedding malware inside PDF, Flash, or Microsoft Office files. These approved applications are then hijacked to execute malicious code. SES detects this anomalous behavior and blocks it. SES has successfully blocked a series of variant-based malware including Dridex, CryptoLocker, Carbanak, and BackOff.

This approach has several advantages over traditional antivirus methods and other analytical techniques. Firstly, because SES is looking for behaviors it uses a generic set of rules and indicators to detect suspicious activity. This means that there is no need for regular updates containing the latest malware signatures. The delay between malware identification and signature creation and distribution can be lengthy – weeks or months in some cases – which exposes organizations to unnecessary risk. SES' approach removes this extended exposure to vulnerability. SES is therefore always up-to-date, and it protects against so-called zero-day attacks (those that have never been seen before).

Chief information security officers (CISOs) hate upgrading and patching their security estate as it adds management overhead and distraction to what is already their often overburdened responsibilities. Patching may also affect stability of applications, especially those built on dated architectures. SES is able to offer protection into the future, but it also adds security to legacy infrastructure, such as Windows XP, Windows 2003 Server, and other end-of-life and unsupported environments. Such platforms may never have been protected before, or only poorly protected: SES offers immediate retrospective protection of these legacy operating systems.

SES also works across not only the operating system environment but also peripherals such as USB keys, and detects data transfers to and from such devices. It also monitors activity across a variety of network protocols such as WiFi and 4G. It thus covers both online and offline environments.

CHALLENGES

Antivirus solutions by themselves are only 30%-40% effective against known threats (source: ENISA) and are 100% ineffectual against new threats and those that obfuscate themselves. Adopting a new approach appears to make sense, if not as a replacement for antivirus then at least as an additional approach. However, CISOs can be a conservative group, and shifting one's mindset from traditional methods can be difficult. In addition, CISOs need to accept that they cannot prevent malware from being installed in their infrastructure. The prevalence of phishing attacks means that at least some attempts at intrusion will succeed (applying the laws of averages and large numbers). Similarly, social engineering techniques will ensure that some malware crosses the firewall via USB keys or other peripherals. Accepting the fact that systems will be breached is tough, requiring a cultural and professional adjustment. But pride in prevention must give way to emphasis on early detection: a CISO's best hope is to detect the presence of malware as it tries to interact with the host system.

Some CISOs will be concerned that, in essence, waiting for malware to act – rather than preventing it from being installed in the first place – may allow data corruption on the endpoint. An example is CryptoLocker, which corrupts data as soon as it is executed. The question is, how quickly can a new malware be detected at the endpoint and stopped? The answer depends on the approach taken, and where the detection capability resides. Often, detection capability sits alongside the operating system, and either works as an extension of the OS, or subservient to it. IDC thinks that the OS itself also needs protection and that detection capability should reside at the kernel layer. This means that the OS itself benefits from protection, and becomes resistant to malware.

Protecting the endpoint is a constant battle, but sometimes the greatest weakness is finding all of those endpoints in the first place. Particularly – but not exclusively – in larger organizations, endpoints can be installed on the corporate network without awareness or authorization by systems administrators. These unknown endpoints then do not receive updates or patches as required, leaving them (and hence the rest of the organization) vulnerable to attack. IDC believes that endpoint discovery is one of the major challenges to organizations, and is a prerequisite to good corporate security.

CONCLUSIONS

As enterprises are under continued and relentless attack from threat actors, the need to improve protection and detection beyond traditional capability increases. IDC believes that, while antivirus solutions are still useful against known threats, the prevalence of zero-day vulnerabilities means that they are not sufficient to counter new malware variants that have not been seen before. Alternative approaches are required.

Much attention has been given to heuristic and statistical approaches, but these have weaknesses that diminish their effectiveness. Stormshield's approach using behavioral analytics does not depend on such methods, and is effective against both existing known and new unknown malware. It is therefore well positioned as a leader in the next generation of endpoint protection technologies.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com