



# Real-time Code Analysis: Proactive Protection Against New and Dynamic Malware Threats

## INTRODUCTION

Motivated by financial gain, cybercriminals launch attacks primarily via the Web. They understand that signature- and database-reliant solutions are not designed to protect against obfuscated malicious code served on compromised legitimate sites, Web 2.0 -based attacks, and other dynamic Web-based threats. These sophisticated attacks elude traditional security systems that rely on signatures or databases such as anti-virus, URL filtering and reputation-based security.

Organizations depend on the Web for online business applications, access to information, and communication with the public. This opens up opportunities for cybercriminals to invisibly inject and propagate malicious code. Organizations need to adopt security strategies that protect their network systems and data from malicious content.

This white paper examines the Crimeware industry and the Web-based methods currently used to sustain cybercrime. It also focuses on the business impact of these attacks and outlines the benefits of active Real-time Code Analysis technology for securing organizations from the growing malware threat.

## THE BUSINESS IMPACT OF CYBERCRIME

Attacks typically target internal user systems within a corporate network, using invisible Web-borne techniques to take control. With the necessary tools readily available on the Internet, gaining remote access to an internal workstation only requires determination from the cybercriminal. In just a few hours, a cybercriminal can stealthily gain access and take control of a company's critical internal business systems and data—and use them for profit.

Organized crime networks focus on infiltrating businesses and personal computers using the services of highly-skilled professional Crimeware writers. These crime pros need little time to access the victim's personal information. This significantly increases security risks and places a huge burden on security experts.

Using a \$100-\$200 “do-it-yourself” toolkit, cybercriminals can achieve the following for significant profit:

- Gain access to the balance sheets of companies and manipulate stock behavior
- Locate payroll information
- Access businesses' bank statements and transfer money
- Gain access to company budgets and private financial statements
- Steal a company's product roadmap and R&D work-plan for industrial espionage
- Capture credit card numbers for fraud purposes
- Steal intellectual property

### **According to research from M86 Security Labs:**

- *At least 6 in 10 malicious URLs pass through undetected in the absence of real-time code analysis technology.*
- *More than 90% of all malware is delivered through the Web.*
- *Up to 85% of all Web-based infections occur through legitimate Web sites.*
- *Zero-day vulnerabilities left users exposed to potential attacks 40% of the time in the second half of 2009 -- even with adequate antivirus protection deployed.*
- *The U.S tops the list of malware hosting locations, accounting for 43% of known malicious code worldwide — a 7.7% increase from the first half of 2010. China ranked second at 14.11%, and Russia was third at 4.10%.*

*The estimated total amount of annual losses due to computer-related crimes exceeds more than \$100 billion U.S.*

The damage to an organization from any of the above-mentioned illegal activities could be devastating. An organization's confidential information and intellectual property have substantial business value. With such an easy and profitable return on investment for cybercriminals, it is clear why governmental agencies, corporations, enterprises and small businesses have become prime targets.

## EMERGING CRIMEWARE TRENDS

Crimeware has become a business and its evolution is being driven by commercial and financial interests. A market exists for malicious code, governed by supply and demand. Vulnerabilities are being traded in online auctions, and commercialized malicious products, such as toolkits, are being developed and packaged to serve this market. Criminals are willing to pay large sums of money for bank account details, credit card numbers and confidential business data collected by trojans, keyloggers and other types of malicious code. As a result, profit-motivated and highly skilled crimeware writers are continuously finding new ways to mask, disguise and obfuscate their crimeware attacks. The rationale is simple – the longer their malicious code remains undetected, the more they can infect— and the higher their revenues grow.

### As of June 2010:

- *Gootkit website infections download FTP credentials and insert malicious IFRAME code snippets into any suitable Web pages.*
- *The Asprox bot returned, using SQL injection techniques to infect vulnerable ASP sites on a large scale.*

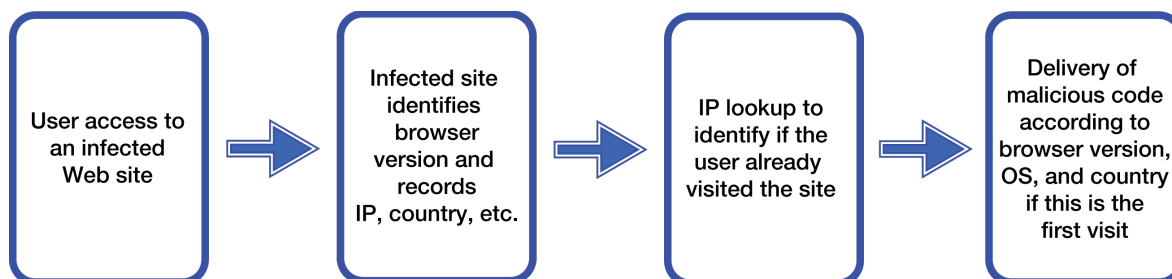
Trends such as evasive attacks and dynamic code obfuscation have become de facto standards for current Crimeware attacks. These attacks often combine multiple propagation methods and anti-forensic techniques to significantly improve the chances of going undetected by traditional security systems. A few of these key trends are described below.

### Evasive attacks

Research by M86 Security Labs uncovered a new genre of highly sophisticated attacks designed to evade signature-based and database-reliant security methods. These attacks represent a quantum leap in terms of their technological sophistication, going far beyond drive-by downloads and code obfuscation.

Using advanced techniques, these evasive attacks significantly reduce the malicious code's exposure, thus lowering the likelihood of detection while maximizing opportunities for infection. By keeping track of the actual IP addresses of visitors to a particular website or Web page, these attacks expose malicious code to innocent website visitors only once. The next time any of these visitors accesses that same Web page, benign content is displayed while all traces of the malicious code have completely vanished. This minimizes the exposure of the malicious code to forensic analysis or security research, as there is only a onetime opportunity for the visitor to be exposed to the malicious code.

Moreover, evasive attacks can not only identify the IP addresses of crawlers used by URL filtering, reputation services and search engines, but they can also reply to these engines with legitimate content. This way, these toolkits increase the probability of mistakenly being classified as a legitimate category. The combination of evasive attacks with code obfuscation techniques significantly enhances the capability of malicious code to go undetected for a longer period of time.



## Customers of a Global Financial Institution Targeted

*An attack initiated in July 2010 compromised more than 3,000 accounts and illegally transferred US\$889,000 from these accounts via money mules.*

*The cybercriminals who coordinated this man-in-the-browser attack used the Eleonore and Phoenix exploit kits to infect systems with the latest version of the Zeus Trojan.*

*M86 Security Labs uncovered this attack after the Trojan was detected by a potential victim's M86 SWG with Real-time Code Analysis technology.*

## Exploit Kits/Attack Toolkits

Cybercriminals create these professional-looking toolkits and sell them to other cyber-thieves who use them to install malware on victims' systems. Once installed, they steal critical information or hijack the unsuspecting victim's PC. The method is highly successful, easy to use and lucrative for cybercriminals.

The operators of exploit kits are part of an extensive underground economy where specialized participants offer tailored products and services to other cybercriminals through shady forums, Web sites that look legitimate, and personal contacts.

Exploit kits are typically used to:

- Steal critical information
- Send spam from a victim's computer
- Install other malware like fake anti-virus scareware, where revenues can be earned from successful "registrations" or Pay-Per-Install (PPI) programs

## Man in the Middle Malware

Since late 2009, new Man-in-the-Middle attacks, created to steal money from users' bank accounts, have increased in popularity and complexity. Despite this, most Web users are unaware of the problem.

What is a Man-in-the-Middle attack? Cybercriminals run malware on a victim's computer, changing the information sent between the user and the bank without detection. All the while, the victim believes he is conducting safe, legitimate transactions.

## Dynamic Code Obfuscation

Dynamic code obfuscation is a technique that basically scrambles any malicious code into what seems to be incomprehensible gibberish. It has become one of the favorite weapons for propagating malicious code due to its effectiveness in bypassing signature-based and database-reliant solutions.

Dynamic code obfuscation serves each visitor to a malicious site with a different instance of the obfuscated malicious code (based on random functions, parameter name changes, and the actual content). In order to detect the existence of such a particular piece of malicious code and block it, a signature-based security solution would need millions of signatures to be effective. Dynamic code obfuscation enables the reuse of multitude of older attacks as it can bypass anti-virus systems and still be effective on unpatched PCs.

Dynamic code obfuscation, automated code obfuscation utilities and other encoding methods enable attackers to plant "invisible" malicious code that infects a user's machine as soon as that user visits the malicious site.

In April/May 2009, a widespread, high-profile attack, "Gumblar", grew rapidly, affecting as many as 60,000 legitimate websites. Another attack named "Belade" affected 40,000 legitimate websites.

## Web 2.0 Exploits

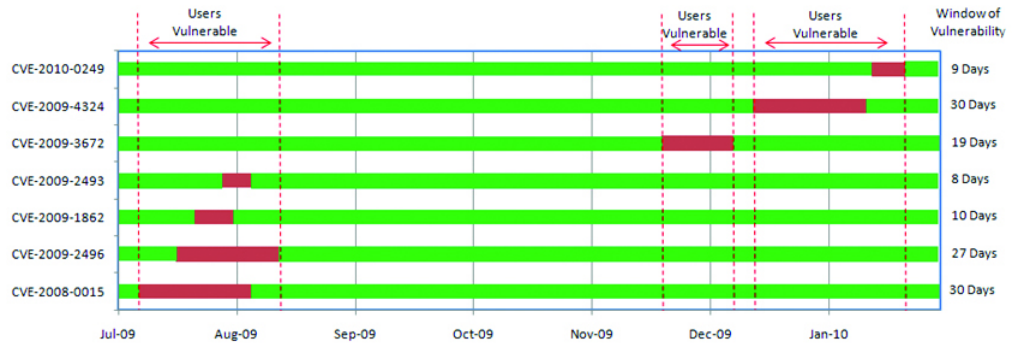
Web 2.0 applications offer significant business advantages for users, from information gathering to collaboration and customer outreach. But it also opens the door to new propagation methods for malicious code. Because Web 2.0 platforms (such as Facebook, Twitter, MySpace, Wikipedia and blogs) enable anyone to upload content, these sites are easily susceptible to cybercriminals who intend to upload malicious content. One example is the online banner advertisement that ran on MySpace.com and other sites in 2006. It used a known Windows security flaw to infect more than a million users with Crimeware. The majority of these popular websites are still "trusted" by URL Filtering/Categorization products, so will not be blocked—even if they contain malicious code.

This technique is especially effective, because the code is never revealed on the site and can be encrypted in transit using SSL. It is unlikely that URL filtering solutions will detect a malicious site, because they don't know which parameters will activate the malicious AJAX request.

*In some cases, a set of PDF exploits is the only method a cybercriminal needs to attack via a Web page.*

### Zero-day Attacks

Zero-day exploits have significant infection success rate. Below is a timeline showing seven zero-day attacks from the second half of 2009 and how the Window of Vulnerability is a significant problem. In this example, users were left vulnerable to these attacks nearly 40% of the time—even when assuming updates were performed immediately. Zero-day vulnerability exploits give attackers the ability to increase their chances for successful infection or exploitation significantly.



### Infection of Rich Content Types

Cybercriminals increasingly use rich content types, such as Adobe Flash and PDF files, to distribute malware on Web 2.0 and high-profile, compromised Web sites. They package malicious code into one of these files because most desktop antivirus scanners ignore file attachments. Once the blank file is opened, the malicious code executes and compromises the user's system. In some cases, a set of PDF exploits is the only method a cybercriminal needs to attack via a Web page.

### Hiding Malicious Links via Shortened URLs

Sparked largely by Twitter, which restricts the number of characters allowed in a posted URL, shortened URLs are increasingly popular. This process masks the original source URL, replacing it with a shorter address. Though convenient for social networking posts, shortened URLs make it easy for cybercriminals to obscure malicious links and harder for users to determine what content they'll actually receive. Not surprisingly, the majority of malicious links our M86 Security Labs experts detected on social networking sites in 2009 were shortened URLs.

### Search Engine Optimization (SEO) Poisoning

Many cybercriminals use sophisticated, highly automated systems to move their illegitimate landing pages up in the results rankings. They create and post Web pages with keywords and phrases related to hot trends and popular topics, driving users to their malicious Web pages unknowingly. And because most users trust search engine results, they visit these infected Web pages freely.

### Google SSL (Encrypted) Search

Google recently launched a beta release of its new search over SSL feature. This enables users to hide their search terms and search results pages from an organization's Web filter, making Acceptable Use Policies (AUPs) and compliance enforcement more difficult. This is problematic for customers who need to allow access to essential Web tools such as Google Mail and Google Apps while blocking SSL proxies.

The M86 SWG solves the Google search-over-SSL problem. Instead of blocking all SSL traffic, which also means blocking useful tools such as Google Mail and Google Apps, the M86 SWG allows IT managers to filter Google SSL search and provides granular control of all SSL traffic. This enables users to access Web tools (like Google Mail and Apps) but prevents employees from accessing Google SSL search, ensuring compliance with AUPs without limiting productivity.

## REAL-TIME CODE ANALYSIS TECHNOLOGY

To safeguard information assets from malicious Web threats, security technologies need to analyze each piece of incoming and outgoing Web content regardless of its origin, context, and appearance in real time. Proactive Real-time Code Analysis identifies malicious code the first time it appears. It analyzes incoming and outgoing Web content in real-time, understands its intent, and blocks Crimeware when detected.

Signature- and database-reliant technologies alone do not protect against obfuscated malicious code, dynamic threats or Web 2.0-based attacks. M86's patented active Real-time Code Analysis technology scans each and every piece of incoming and outgoing Web content in HTTP/HTTPS and analyzes it in real time regardless of its originating URL and without signature matching. Therefore, it detects and blocks Crimeware, targeted attacks and other malicious web content, even when hiding in SSL traffic, from entering corporate networks. M86's active real-time code analysis technology is highly effective in handling unknown, dynamic and rich Web content that cannot be detected by reactive signature- and database-reliant security technologies, as well as traditional threats.

In the event a legitimate Web site is compromised, M86's Dynamic Web Repair™ removes the malicious code seamlessly—without blocking the Web site. After eliminating the offending code, this technology delivers the safe Web content to the user, ensuring continued productivity.

### Key Features of Real-time Code Analysis

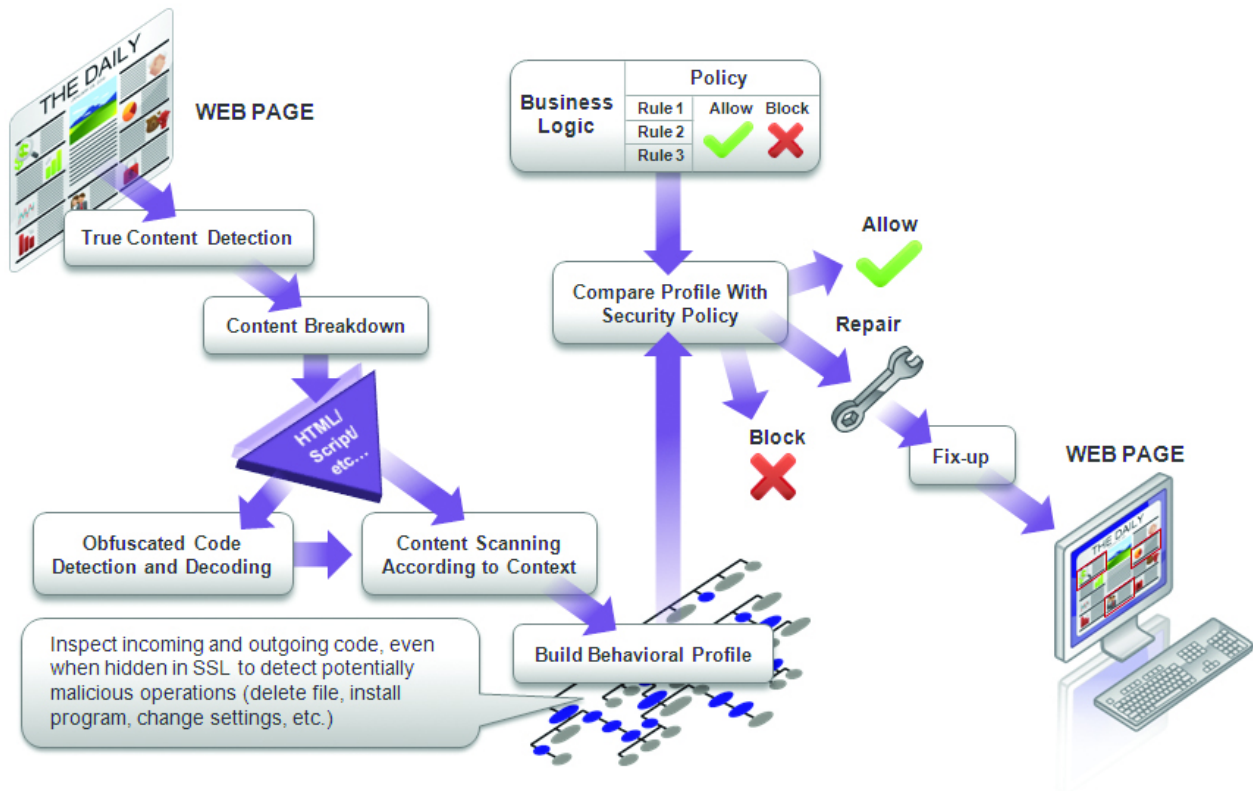
When Web content is processed by M86's active real-time scanning engine, its analysis consists of several steps, including:

- Identifying different file type variations, spoofed file types, archived executables and encoded script files using true content type detection algorithms
- Inspecting all inbound and outbound content, including HTTP/HTTPS
- Detecting/decoding obfuscated code that tries to “bypass” security scanners
- Dissecting HTML code into individual components (HTML commands, text sections, style sheets, URI, scripts, external object activation, etc.)
- Scanning each active content component using a sub-engine that analyzes Java, ActiveX, JS/VB Scripts, HTML, XML, CSS, and HTTP/HTTPS/SSL in context
- Constructing a behavior profile that encompasses the combined operational behavior of the active content components
- Comparing the behavior profile against a comprehensive list of security profiles and immediately blocking any behavior profile violation
- Performing a fix-up attempt for instances of a “blocked” decision, sanitizing the malicious portions, and serving the Web page with as much functionality as possible

The real-time behavior-based security engine understands the programmatic connections among the various bits and pieces of code. Each individual piece of code can be benign and easily avoid network-level scanning devices and signature-based scanning technologies. Deep scanning of the combined operations (resembling a compiler working with a runtime interpreter) can detect the true intended action that the code will perform when it reaches the user's desktop.

M86's scanning engine is not affected by programmatic variances, such as changing names of objects and variables in the scripts, cross-calls between scripts, and alternating calling sequences.

## How the M86 Secure Web Gateway Analyzes a Web Page



## BENEFITS TO ORGANIZATIONS

### M86 Real-Time Security:

- Detects and prevents Crimeware and Web 2.0 attacks despite the advanced propagation techniques and anti-forensic methods (code obfuscation, evasive attacks, random file names and URLs) being used
- Analyzes every piece of Web content in real time, regardless of its originating URL and without signature-matching
- Increases knowledge and awareness of the incoming and outgoing content and its associated behavior when it enters/exits the organization (results in more educated security policy definitions and risk analyses)
- Reveals malicious combinations of individually innocent functions using deep code analysis
- Exposes Crimeware that tries to extract private information and publish it to the Internet or to access private and unauthorized information
- Reduces transmission costs and downloading time through transparent handling of Web traffic
- Provides a flexible and scalable data analysis platform for internal use, audits, and compliance requirements using an external reporting and logging system
- Assists in complying with regulations such as SOX, HIPAA, FISMA, GLBA and PCI DSS
- Increases Web 2.0 and productivity control with URL filtering engines, available with the Vital Web Security Suite

## Deploying Real-time Code Analysis within the M86 Secure Web Gateway

- Inspects all Inbound and outbound content including HTTP/HTTPS content
- Provides a comprehensive list that includes actions on the 'File Access' level, 'Processes' level, 'Registry' level, 'Network Access' level, 'Windows' level, etc. In each category, M86 offers a long list of actions.
- Includes a wizard-driven security policy decision-making system with a single-click rules refinement enhancement
- Includes an integrated dashboard that provides instant information on the system's performance and its risk level using an extensive set of graphs and views for quick and accurate insight
- Creates rules flexibly with connections between all types of filters
- Enables any rule to be attributed to any user or group of users through granular security policies
- Identifies multiple types of content regardless of variations and spoofed types, archived executables, or encoded script files using true content type detector

## ADVANTAGES OVER OTHER SECURITY SOLUTIONS

Signature- and database-reliant Internet security solutions are limited in preventing new types of dynamic Web-borne attacks. Due to the volatility of website content and the evasive nature of modern attacks, the task of tracking or categorizing malicious web content is virtually impossible. Obfuscated malicious code lurks behind innocent-looking websites, ready to infect corporate networks and systems long before a signature-based anti-virus solution can be updated or a software patch can be installed. The primary types of signature- and database-reliant Internet security solutions are discussed below.

### Anti-Virus Scanning

Reactive in nature, anti-virus solutions are mainly effective against known threats and are powerless against dynamically obfuscated and zero-day attacks, which often use multiple technologies, stages and angles of attack. Hackers are also clever enough to test their malicious code against anti-virus products before releasing them to ensure the code will not be detected.

Traditional anti-virus solutions block known viruses and worms by comparing content against signature databases which need to be updated each time a new virus is discovered. Since viruses spread at tremendous speed, anti-virus vendors receive new attack samples, create new patches (or signatures), and deliver them to their anti-virus products databases. While these updates take place, virus writers are already busy working on the next viruses for which signatures don't yet exist. The result of this endless loop is exposure to dangerous attacks.

Using anti-virus scanners alone will not provide the level of protection needed to prevent malware attacks. But when used alongside Real-time Code Analysis, users will be fully protected.

## Reputational databases

Similar to URL categorization, reputation services use Web crawlers to map the Web and assign a reputation score for each website. Parameters consist of the IP of the hosted site, the owner of the site (such as a Fortune 500 company), how long the domain is registered, and whether the URL appears in mass spam emails. Although the resulting database is substantial, it doesn't cover the entire Web and cannot be updated in real time.

New infected Web pages are often found on legitimate sites that carry a favorable reputation score. Usually, reputation services will not block malicious content on these sites, since they have good reputations, valid owners, and a long registration.

The M86 Secure Web Gateway (M86 SWG) takes a completely different approach, using Real-time Code Analysis on each Web page. It reads the program code in real time and determines what this code intends to do. Both known and unknown malicious code is detected using this technology without the need to rely on any database. By analyzing the program code in real time, the M86 SWG provides a level of security that is not covered by reputation services.

## Intrusion detection and intrusion prevention systems

Intrusion Detection System (IDS) products detect situations once the network has already been infected. They identify patterns of network traffic behavior (involving one computer or a group of computers) that may indicate the spread of a worm or other anomalies. When this happens, they perform damage control by cutting off the network traffic, isolating a group of computers and alerting the administrator. This results in a negative user experience and decreased productivity.

Intrusion Prevention Systems (IPS) and similar "smart packet filtering" solutions usually operate at Layers 2 through 4 of the OSI networking model, and attempt to identify communication patterns (such as rate of transmission) of packets coming into the network. However, powerful and sophisticated attacks cannot be identified at the single-packet level, because these attacks are constructed of high-level scripting and HTML operations within the context of whole web pages. A pattern identified in a single packet cannot determine if this packet is a part of a code that will try to exploit the target PC. In addition, IPS is not effective against social engineering techniques that simply trick users into clicking "OK" to install Crimeware and malware without their knowledge.

## Heuristic technologies are prone to false-positives

Heuristic-based technologies detect infections by scrutinizing a program's overall structure, its computer instructions and other data contained in the file. The heuristic scanner then makes an assessment of the likelihood that the program is malicious based on the logic's apparent intent. Anti-virus engines typically use heuristics to identify variations of known viruses. They often fail to detect new infections because there are too many ways to obfuscate malicious code. The only sure way to know if content is malicious is to watch it run in real time. This accounts for the high rates of false-positives that users of heuristic-based systems receive.

In contrast, M86's real-time behavior-based engine identifies "concrete" behavior, enabling it to minimize over-blocking. It detects and identifies the true behavior of obfuscated code that could be used for malicious purposes.

## Gateway-based URL filtering (including dynamic URL filtering)

Gateway-based URL filtering products check URLs in a database which clusters them in categories and requires constant updates. URL categorization vendors use Web crawlers to map the Web and assign a category to each URL, such as advertisement, finance, or gambling. It is almost impossible to map the entire Web this way because websites are highly dynamic. As a result, these databases can only be as accurate at their latest scan.

URL filtering blocks non-productive sites, enabling companies to control employees' browsing habits, ensuring productivity and network performance. However, it is limited in its ability to protect users from Web-based attacks.

Dynamic URL filtering tries to classify websites (which are not in the database) based on text and graphics. However, the presence of legitimate text and graphics is no guarantee that a site will be 100% Crimeware-free. Moreover, most infected Web pages are on hacked legitimate websites.

M86's Real-time Code Analysis technology determines the intended behavior of Web content based on the actual code, regardless of its URL. It detects Crimeware by analyzing code in real time, providing a level of security unmatched by any URL filtering technology. While URL filtering ensures productivity, it should be used in addition to Real-time Code Analysis to provide a complete, effective solution.

## CONCLUSION

Financial gain drives the proliferation of Crimeware, and cybercriminals use sophisticated techniques to evade signature- and database-reliant security tools. Attempts to pattern malicious code and create signatures, or to categorize known malicious sites do not sufficiently defend against the wave of dynamic Web threats. Clearly, an additional security layer is needed.

The answer is Real-time Code Analysis technology. The M86 Vital Web Security Suite™, which includes active Real-time Code Analysis technology, achieves the highest rate of malicious code prevention. Central to the M86 SWG, this suite of technologies analyzes all incoming and outgoing Web content in real time, regardless of its original source. And it determines the potential effects of the code before it executes. By understanding the true intent of Web content, M86's active Real-time Code Analysis technology detects and prevents Crimeware despite the propagation techniques and anti-forensics methods in use. This prevents any malicious Web content from entering or exiting the corporate network, protecting organizations from the costly damage that can result from malware attacks.

## ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

---

### TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit [www.m86security.com/downloads](http://www.m86security.com/downloads)



**Corporate Headquarters**  
828 West Taft Avenue  
Orange, CA 92865  
United States  
Phone: +1 (714) 282-6111  
Fax: +1 (714) 282-6116

**International Headquarters**  
Renaissance 2200  
Basing View, Basingstoke  
Hampshire RG21 4EQ  
United Kingdom  
Phone: +44 (0) 1256 848 080  
Fax: +44 (0) 1256 848 060

**Asia-Pacific**  
Suite 3, Level 7, 100 Walker St  
North Sydney NSW 2060  
Australia  
Phone: +61 (0)2 9466 5800  
Fax: +61 (0)2 9466 5899

Version 08/26/10