



# From Zero-day to Real-time

How McAfee Artemis Technology combats real-time cybercrime with community threat intelligence

**There's no economic downturn in the business of cybercrime. McAfee® Avert® Labs detected more malware in the first five months of 2008 than were found in *all* of 2006 and 2007. More frightening: today's subtle, real-time malware acts before traditional signature-based protection can detect and respond. Cybercrime's new techniques demand a new weapon. McAfee Artemis Technology combines innovative ideas with web communities for**

## The Changing Threatscape

In cybercrime, the longer an exploit goes undetected and unknown, the more data it steals and damage it does. Expensive damage.

While consumers see an average loss of \$1200 (Source: IC3 – FBI & NW3C), the 2007 CSI/FBI enterprise survey revealed "the average annual loss reported in this year's survey shot up to \$350,424 from \$168,000 the previous year. Not since the 2004 report have average losses been this high."

## A Free Market

Cybercrime has adopted progressive business practices and advanced programming techniques to match the growing prizes, maturing technologies, and rich demographics of the Internet. No longer rogue developers in search of public acclaim, well-educated hackers now work as teams to identify opportunities and harvest rich rewards.

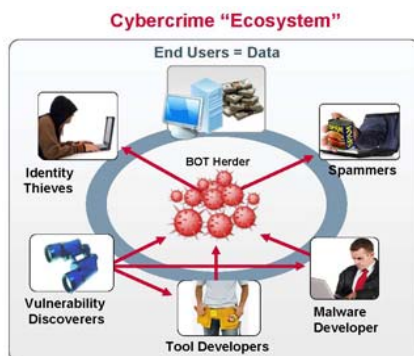


Figure 1. Cybercrime's distributed, optimized ecosystem.

Commercial tactics for niche marketing and build-or-buy investments help them target the ripest prospects with the most advanced tools.

Consider bots and social engineering. Bots now routinely take advantage of encryption and peer-to-peer networks to avoid detection and achieve resilience. When one zombie shuts down, its peers fill in. No obvious botnet controller exists to track down, offering little hope of convicting a malefactor.

Similarly, social engineering now uses clever programming and web business models to win its standard game. Small tricks with SQL injections, poisoned banner ads, misspellings, keywords, targeted spam, and click fraud capture big profits when they touch a large number of sites and systems.

Less sophisticated cybercriminals still use attacks that anti-virus vendors can catch, but signature-based anti-virus tools are becoming ineffective as fine targeting and one-time packing techniques now dominate commercial malware activities. Traditional tools will be even less relevant as the threatscape shifts to real-time behavioral exploits. Let's look at some examples.

## Targeted attacks increase ROI

Traditional malware defenses act on repeated patterns and volumes of activity. Criminals are fighting back with one-time-use and targeting

technologies that don't trigger these tools. These techniques pursue specific victims: high-visibility executives and high-value consumers. The time it takes to craft the attack pays off with a higher hit rate for a better return on investment.

Already, 80 percent of malware is packed, compressed, or encrypted to foil inspection (Source: Avert.) Packing programs generate multiple versions of the same malware, making each instance appear unique. This packed code challenges traditional .DAT-based technologies, which must add specific detection to recognize and unpack this malware, including compute-intensive decompression and decryption. With the majority of code now packed, generic detection authoring can be significantly more time consuming, slowing the overall response.

Take the spam experience. Security vendors are getting better at blacklisting known spammers and detecting suspicious code in more forms. Spammers have countered with targeting that generates only tens or hundreds of emails rather than thousands, avoiding volumes that trigger the blacklist threshold.

Targeted messages go to carefully chosen user email accounts and include details to make them seem credible. Two examples are phishing attacks, as in an eBay complaint email, and whaling attacks, which approach high-profile targets individually, as in email to a CEO from the Better Business Bureau.

### Web threats

Web 2.0 thrives on dynamic content. Server-side polymorphism conforms to the trend with single-use malware content. As users visit social sites like Facebook and LinkedIn, they receive malformed code in user-selected content or invisible drive-by downloads using JavaScript, Visual Basic Script, Adobe Flash, and ActiveX controls. After each download, polymorphic technologies alter the file, so that no two visitors receive the same code.

Social networking sites present a treasure trove of information on people and their business and personal activities. Mining this data makes targeted attacks more effective. In some cases, rich custom programming languages and widgets enable platform-specific threats. The social engineering fabric allows these threats to move from user to user inside the Web 2.0 server database itself. Since the

malware stays within a single system, it can produce great damage while intersecting with few defenses, generating a long payoff.

### A case study

Social engineering, targeting, one-time-use code, and a social networking site can all be used together to steal sensitive data and trigger a compliance disclosure. Here's an example:

1. Criminals select a company in the news for customer service issues, with press coverage that includes an interview from the CEO and an angry customer
2. They mine LinkedIn for names, titles, and email addresses of senior staff from the company
3. The criminals create an email message directly to a staff member containing the customer name and a reference to the service issue. The message looks like it comes from the CEO and directs the staff member to open an attached message, supposedly from the customer.
4. The attached message seems like a legitimate email, but also installs a one-time-use malware payload that searches the employee's computer for sensitive customer information, then emails that information to the criminals
5. The employee sends the customer a message, fulfilling the CEO's request. The employee is unaware of the system breach, so the data loss goes undetected, allowing the criminals to make lucrative use of the customer data and creating a significant regulatory compliance breach.



Figure 2. Avert predicts malware volumes will grow 300 percent from 2007 to 2008 as cybercrime expands.

### More volume, more platforms, more trouble

Through targeting and packers, cybercriminals have flooded the Internet with malware. As Figure 2 demonstrates, McAfee researchers project 300 percent malware growth between 2007 and 2008. There is no reason for this trend to weaken as global access, Web 2.0, virtual and mobile platforms, and new communication techniques propel Internet growth. Increasing state-sponsored terrorism, aimed at disruption rather than profit, presents further incentive to target and conceal.

### The Protection Gap

Welcome to threat research today. McAfee Avert Labs researchers labor 24/7 in 16 countries around the world to craft over 3500 new detection signatures *each day*. But that still isn't good enough. As the targeting and packing trends indicate, signature-based techniques are losing their effectiveness.

A risky "protection gap" exists: 24-72 hours between the time malware is placed in the wild and the time protection is active on a given host. This gap comes from slow *detection* and outdated *response* models (Figure 3).



Figure 3. The scale and complexity of detection followed by a serial response model create a dangerous protection gap today.

### Several factors complicate malware detection

**Massive volume**—there are more suspicious samples to sift through to find malicious code.

Avert receives 50,000 samples of code daily, up from 15,000 per day in 2006.

**Frequency-based .DAT models**—packing, server-side polymorphism, and targeted attacks allow each exploit to appear small-volume or even one-time use to stay undetected

**Vector-based defenses**—most vector-based protections look at scripts, email, and documents, not at a secondary payload. If they don't recognize a pattern or signature at the first level, the malware passes through successfully.

### Today's response model is unwieldy

**Scheduled updates**—the current delivery model pushes batch .DAT updates on a regular schedule. Although the industry-standard interval has narrowed from monthly to daily to hourly (McAfee publishes early release .DATs hourly), even an hour is enough for drive-by downloads and other instant attacks to succeed.

**High-overhead administration**—consumers are the lucky ones, since most use automatic updates to maintain .DAT files. In the enterprise, however, administrators may be obligated to test and carefully monitor distribution of updates as part of configuration and patch management processes. These steps consume resources and create exposure as they delay distribution.

**Resource constraints**—.DAT file sizes are expanding with rising malware volumes, although a typical system uses only 0.1 percent of the .DATs it receives. Avert researchers estimate that at current rates, average AV signatures will exceed 100 Mb by 2010. The notion of pushing the entire blacklist of .DAT files to the end-point needs to change to reduce the impact on performance, storage, memory, and network bandwidth.

**False positives from blacklists**—erroneous blocking of legitimate traffic disrupts operations and productivity. Fixing false positives depends on the same laborious process as adding signatures in the first place.

As malware volumes spiral upward, the protection

gap will remain, unless the industry adopts more creative, time-sensitive techniques for both detection and response.

## Community Threat Intelligence in McAfee Artemis Technology

McAfee researchers have always used both automated and manual techniques to detect threats. Now they are finding safety in numbers: the numbers of systems and sensors connected over the web. This new real-time detection and response system, available now, is *McAfee Artemis Technology*.

With McAfee Artemis Technology, McAfee has re-architected its threat capture and analysis infrastructure to enhance and compress the research lifecycle. By harnessing the scale, diversity, redundancy, and reach of the Internet, McAfee closes both the *detection* and the *response* portions of the protection gap.

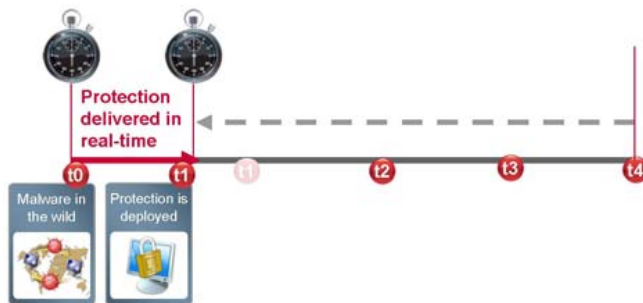


Figure 4. McAfee Artemis Technology captures community threat intelligence to quickly diagnose and respond to malware, compressing the protection gap.

The concept is simple. From millions of active users, a much larger number of systems than ever before possible, McAfee Artemis Technology captures and correlates fingerprints of new and potentially malicious code. In milliseconds, sophisticated McAfee Avert threat analysis tools crosscheck characteristics and intelligently assess each sample's likely threat level. Then McAfee Artemis Technology tells the host system how to respond to minimize risk.

### Automated capture

More than 125 million computers run McAfee security products every day around the world, with more connected to the McAfee Total Protection

Service for hosted security. In the past, these detection systems only *received* update files and threat information on a schedule. Now, this community *contributes* proactively.

Through McAfee Artemis Technology, these systems transmit compact fingerprints to an automated evaluation system for immediate assessment.

### Innovative heuristics

Not only does this pool provide a staggering number of new fingerprints—each computer contributes a handful of fingerprints daily—it offers the freshest possible insight into potentially malicious files. With multiple, diverse data points, sophisticated heuristics can build up profiles of “bad” code based on reputation, activity, signature, source, frequency, and geography.

More than just looking at the threat vector—the distribution channel and format of the threat—McAfee examines the payload itself, in detail, to help isolate and identify new threats.

For speedy review, automated pre-analysis tools combine with a weighted scale based on Avert's experience with similar types of code. They generate a grade and a probable risk estimate to support a very accurate recommendation about how defenses should respond.

Whitelists and blacklists work together to improve detection without sacrificing quality. Blacklists cause immediate blocking of known bad code when there is a low-risk of false positives. Whitelists ensure innocent material goes through by clearing known good code.

This whitelist/blacklist model has been proven in the fight against spam, especially the rapid evolution of spam and phishing campaigns. Lightweight whitelists and blacklists help McAfee anti-spam keep up with targeting, resulting in a 98 percent accuracy rate with no false positives (Source: West Coast Labs, October 2007).

As new data comes in, the analysis activity adapts. If a sample suddenly comes up repeatedly, its analysis takes priority: this may be a potent new threat. This dynamic response helps McAfee Artemis Technology

identify patterns and trends more quickly.

### Collaboration across research communities

Since cybercriminals use so many different tactics today, research must cross-traditional boundaries to be effective. After twenty years, McAfee has built an extensive, multi-disciplinary, global team of threat researchers.

Where some companies focus exclusively on malware or spam, McAfee researchers *also* examine vulnerabilities, spyware, web security, governance and compliance, and intrusion prevention. Collaboration across this range of threat vectors yields rapid diagnosis (Figure 5).

For example, SiteAdvisor uses automated tools and community rating systems to detect and monitor newly registered domains and the files on them, as well as existing websites. It adjusts its assessment of each site's trustworthiness as the site evolves.

This insight can feed across to provide context and details to host and network intrusion prevention, anti-spam, and other analysis teams.

### Instant Response

A global network of active threat intelligence systems enables a new class of real-time response. Not a replacement for existing systems, McAfee Artemis Technology reinforces and extends today's

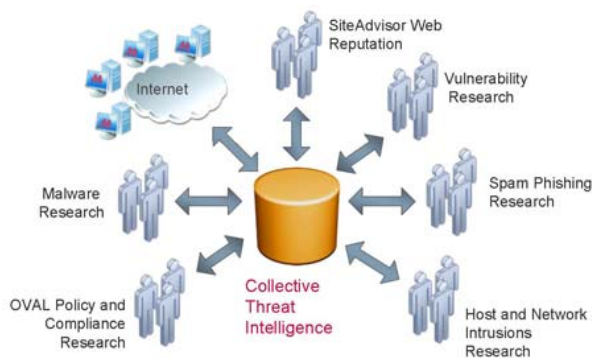


Figure 5. Active Protection synthesizes the research of multiple disciplines to assess the probable risk of each code sample.

defenses, such as agent-based anti-virus and host intrusion prevention.

Here's how it works:

1. The agent on a host system scans an executable received in email or presented by a website
2. The code is compared to its local .DAT database
3. If the code is not recognized, but still looks suspicious—if a file is packed, for instance—the agent uses a live connection to send a tiny, definitive fingerprint of that code to the McAfee Artemis Technology network
4. Based on its likely risk, McAfee Artemis Technology tells the VirusScan agent to block, quarantine, or clean if it can (based on policies set by the enterprise administrator or consumer). In enterprises, the agent also notifies ePO of the detection.
5. If not recognized, the sample is permitted to execute on the client, while on the backend the sample is queued for analysis. This background analysis continues as each additional appearance of the code brings new information.

Through McAfee Artemis Technology analysis, a previously unknown code sample may eventually be determined to be malicious. This assessment will be reflected in the McAfee Artemis Technology response from that point on, and a traditional .DAT file may be published for download in the traditional fashion.

### Zero-touch, Zero-cost Enablement

McAfee Artemis Technology takes effect painlessly. In the enterprise, there's zero effort by the end-user or the administrator, since McAfee Artemis Technology operates on existing agents, scanning, and management infrastructure. There's nothing new to test or pilot, no tedious rollout or

deployment disruption.

The enterprise administrator just checks a box in the ePO management console to activate, then begins to see the additional detections appear in ePO reports. The new detections are identical to traditional VirusScan .DAT detections.

Consumers enable McAfee Artemis Technology through a standard .DAT update that becomes active by default.

### Ends the Protection Gap

Because of McAfee's enormous installed base of active users, the sample size is much greater than what other security vendors see. Real-time analysis from so many different sources minimizes the window in which a threat can proliferate. Where complex threats with payloads and multiple systems are involved, like the storm worm or botnet, McAfee Artemis Technology offers a markedly higher chance of detection before any payload can be placed.

### Guides community research

The entire community learns with each new sample and evaluation. "Telemetry data" captured throughout the Internet provides information on prevalence, variety, thresholds, and the propagation speed of new threats. As researchers share their insights within product teams and across communities, everyone can better invest scant research resources to benefit customers and the Internet as a whole.

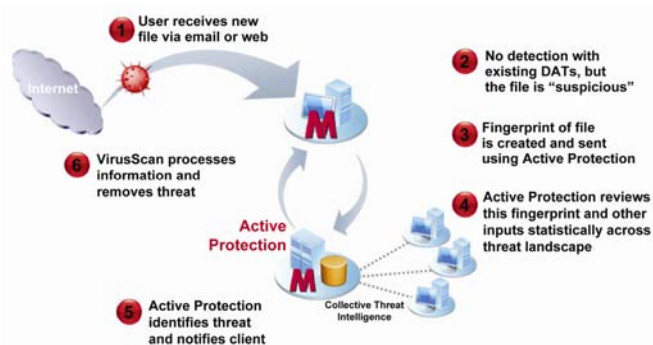


Figure 6. Agents use Active Protection for an immediate, relevant threat assessment based on the latest Internet activities and threat analysis

### Resilient

McAfee Artemis Technology servers are distributed and optimized around the world to ensure immediate response in every region. This localized model allows the system to scale and adapt with the Internet.

### Relevant

As threats diversify and blend, the McAfee Artemis Technology approach delivers relevant protection. The agent asks for analysis of the threats it's really facing, rather than having to be content with generic .DATs. Relevance increases the odds that threats will be pre-empted before they damage systems or steal precious data.

### Protecting Today

McAfee Artemis Technology is available now, at no additional cost, to consumers and enterprise customers using McAfee VirusScan products or the McAfee Total Protection Service.

### A Model for the Future

McAfee Artemis Technology reveals a real-time delivery model for specialized tools. In this first release, by adding a tiny function as a .DAT update, McAfee Artemis Technology enables a supplemental scan that leverages the existing robust McAfee anti-virus scan engine and update systems. Each .DAT file update can easily add or remove this and other new functions. Looking ahead, this flexible delivery scheme will support targeted release of critical new tools, as systems need them, at lightning speed.

The continuous flow of McAfee Artemis Technology data will help McAfee detect malware more quickly, build more accurate blacklists and whitelists, and adjust its risk predictions and thresholds more precisely.

For example, McAfee Host Intrusion Prevention customers use application controls today to restrict application use on systems. Administrators can explicitly define applications that may run (the whitelist) or must never run (the blacklist).

With McAfee Artemis Technology, very small, very explicit application control rules might be provided to the agent to guide its response to file-based threats. If it detects a suspicious pattern of API calls, application control could be used to block execution of that unique executable.

The whitelist plus blacklist approach increases accuracy and prevents false positives. When Host Intrusion Prevention triggers on that suspicious API call, the whitelist might be queried in real-time to determine if that call is a just-released application that should be allowed rather than an attack that should be blocked.

For web threats, today's reputation lists are only as accurate as their timestamps, since malicious code can invisibly change repeatedly using polymorphism. To defend more rigorously in real-time, the McAfee Artemis Technology model could use whitelists and blacklists for URLs within sites, and could maintain dynamic screening against malicious downloads, controlling them as miniature applications. Although individual pages and downloads would be blocked, the bulk of a networking or shopping site would remain accessible.

### **Behavioral tools defy one-time-use tactics**

Much of security has centered on protections at the file level. These defenses have raised the barriers to entry for file-based exploits. Naturally, criminals have moved to exploit systems and operating environment resources. For instance, virtualization vulnerabilities grew over 400 percent from 2006 to 2007 (Source: National Vulnerability Database).

Malware authors move fast here, too: 32 percent of exploits are released within three days of a vulnerability being discovered (Source: Avert).

To recognize and shut down these complex attacks, Host and Network Intrusion Prevention Systems (Host IPS and Network IPS) use behavioral inspection that monitors a variety of system operations looking for suspicious or unusual activities.

Behavioral protection is a logical extension of the McAfee Artemis Technology real-time model. From acting based on file attributes—fingerprints, the way a file is packed, or its prevalence and frequency—protections can act based on multiple

behavioral dimensions, such as the processes created, the files modified, or the action a process takes. The McAfee Artemis Technology detection system will notice the new behaviors immediately, assess their risk, and respond with the appropriate content or reaction.

Behavioral protection like this will defend against one-time-use exploits disguised by packing and polymorphism. It will create barriers to entry that make whole classes of threats obsolete, forcing cybercriminals to make expensive investments in new techniques that will lower their ROI.

### **Conclusion**

Cybercriminals are watching the clock. They are counting the elapsed time from the planting of their malware, through its detection, to the moment effective protections go live on targeted systems. This precious time—the protection gap—enables their profits.

The McAfee Artemis Technology model virtually eliminates this protection gap. Community threat intelligence and innovative threat research techniques compress the detection and response lifecycle. They capture unprecedented numbers of malware data points and return instant, accurate assessments of risk. Although a complex technology, McAfee Artemis Technology appears all but invisible to end-users.

This new, low-overhead layer of online security takes away the delays of traditional signature-based defenses. It is like having a personal threat researcher to protect each system on the road, at home, and at work.

Beyond today's threats, McAfee Artemis Technology offers a window into how adaptive and behavioral protections will face off against real-time, one-time-use threats. Effectively and efficiently.

Learn more at <http://www.mcafee.com>

### **Brought to you by McAfee Avert Labs**

McAfee Avert Labs is the global research team of McAfee Inc. With research teams devoted to malware, potentially unwanted programs, host

intrusions, network intrusions, mobile malware, and ethical vulnerability disclosure, Avert Labs enjoys a broad view of security. This expansive vision allows McAfee's researchers to continually improve security technologies and better protect the public.

### **About McAfee, Inc.**

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. It delivers proactive and proven solutions and services that secure systems and networks around the world, allowing users to browse and shop the web securely. With its unmatched security expertise and commitment to innovation, McAfee empowers home users, businesses, the public sector, and service providers by enabling them to comply with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

*<http://www.mcafee.com>*

---

McAfee, Inc.  
3965 Freedom Circle  
Santa Clara, CA 95054,  
888.847.8766  
[www.mcafee.com](http://www.mcafee.com)

© 2008 McAfee, Inc. No part of this document may be reproduced without the expressed written permission of McAfee, Inc. The information in this document is provided only for educational purposes and for the convenience of McAfee's customers. The information contained herein is subject to change without notice, and is provided "as is" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance. McAfee, Avert, and Avert Labs are trademarks or registered trademarks of McAfee, Inc. in the United States and other countries. All other names and brands may be the property of others.