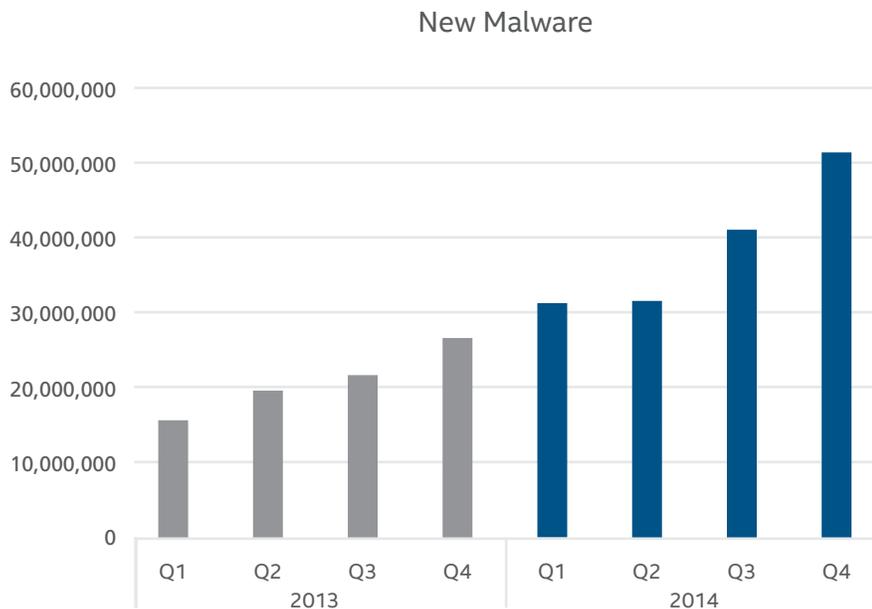


When Evolution Turns Dark

Polymorphic malware

Evolution serves a purpose in the animal kingdom—ensuring that traits which bolster survival are passed down through generations. Unfortunately, the same applies to the creation and development of malware. In Q4 2014, McAfee Labs counted more than 387 new malware samples per minute, or more than six every second.

That is six chances every second for the next Flame, Stuxnet, or any other infamous malware to be created. So it is especially worrisome when malware has evolved to become polymorphic. Polymorphic malware is a very difficult threat to combat due to the malware's changing its form with every new infection, meaning no two samples are the same.



Source: McAfee Labs, 2015.

Figure 1. Malware continues to grow quickly. McAfee Labs detects more than 387 new samples every minute.

Polymorphic Worm: W/32 Worm-AAEH

We discuss in depth the polymorphic worm W/32Worm-AAEH and the control infrastructure behind it in **Catch Me If You Can: Antics of a Polymorphic Botnet**. W/32Worm-AAEH is a polymorphic downloader with more than 2.25 million unique samples known to McAfee® Labs, and it has infected more than 23,000 systems. Once aboard its newly infected host, the worm can download a multitude of malware—including password stealers, ransomware, rootkits, spam bots, and other downloaders. In addition to downloading malicious tools, this threat morphs every few hours and rapidly propagates across the network. Since McAfee Labs has tracked this worm beginning in March 2014, the control server has replaced samples with new variants one to six times per day and the server-side polymorphic engine has serviced client-specific samples, guaranteeing a unique sample with each new download request.

The first known sample of W32/Worm-AAEH was found in June 2009 and, despite its age, the authors have ensured that the worm has stayed relevant through several obfuscation and antianalysis tricks that hinder detection. Encryption techniques are updated often, and code from open-source software projects has been added to make analysis more difficult. W32/Worm-AAEH can take the following actions:

- Execute at system startup and hide in the User Profile directory.
- Copy itself in all removable drives and use a hidden autorun.inf file to launch automatically.
- Use the string “Open folder to view files” as the action text in the local language, supporting 16 European languages.
- Disable Microsoft Windows Task Manager’s ability to terminate applications to prevent itself from being manually terminated by the user.
- Detect virtual machines and antivirus software.
- Terminate Internet connections to IP addresses at security companies.
- Use a domain generation algorithm to find its control servers.
- Inject malware into existing processes.
- Use encryption.
- Disable tools from terminating it.
- Spread itself via removable CD/DVD drives.
- Exploit a LNK file vulnerability (CVE-2010-2568).
- Insert itself in ZIP or RAR archives to aid its persistence and propagation.

What Can Be Done to Prevent Infection?

Although the threat is consistently polymorphic, the core behavior has remained virtually the same, allowing customers to easily prevent infections by taking these precautionary measures:

Category	Rule
Common maximum protection	Prevent programs registering to AutoRun
User defined	Prevent file execution in %USERPROFILE% directory
User defined	Block outbound connections to ports 7001–7008, 8000–8003, 9002–9004, and 20000–40000 (Legitimate applications may use these ports)

Table 2. Access Protection Rules to Stop W32/Worm-AAEH

How Can Intel Security Help Protect Against W32/Worm-AAEH?

McAfee, a part of Intel Security, brings together diverse security technologies to meet the expanding capabilities and increasing stealth of advanced malware such as W32/Worm-AAEH. Here are the key products that will enable your company to protect itself against polymorphic malware.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense is a multilayered malware detection solution that combines multiple inspection engines. The engines perform signature- and reputation-based inspection, real-time emulation, full static-code analysis, and dynamic sandboxing. McAfee Advanced Threat Defense protects against advanced worms like W32/Worm-AAEH.

- **Signature-based detection:** Detects viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks. Its comprehensive knowledgebase is created and maintained by McAfee Labs, and currently includes more than 150 million signatures, including W32/Worm-AAEH.
- **Reputation-based detection:** Looks up the reputation of files using the McAfee Global Threat Intelligence network to detect newly emerging threats.
- **Real-time static analysis and emulation:** Quickly finds malware and zero-day threats not identified with signature-based techniques or reputation.
- **Full static code analysis:** Reverse-engineers file code to assess all its attributes and instruction sets, and to fully analyze the source code without execution. Comprehensive unpacking capabilities open all types of packed and compressed files to enable complete analysis and malware classification, allowing your company to understand the threat posed by the specific malware.
- **Dynamic sandbox analysis:** Executes the file code in a virtual runtime environment and observes the resulting behavior. Virtual environments can be configured to match your company's host environments, and support custom OS images of Windows 7 (32- or 64-bit), XP, Server 2003, Server 2008 (64-bit), and Android.

McAfee Endpoint Intelligence Agent

McAfee Endpoint Intelligence Agent (EIA) resides on an endpoint and provides per-connection information, such as user identity and hash values of executables that initiate both internal and external network connections. McAfee EIA enables the detection of worms such as W32/Worm-AAEH as it attempts to phone home, and allows your company to interrupt and remediate.

- **Deny inbound or outbound connections to unknown and known bad processes:** McAfee EIA monitors endpoints for any outgoing connections and lets users create firewall and IPS rules based on file reputation.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) is a comprehensive, real-time, cloud-based threat intelligence service that allows Intel Security products to block cyberthreats across all vectors—file, web, message, and network. Proactively protect against polymorphic malware with these features:

- **Intelligence through vector correlation:** Collects and correlates data from and across all key threat vectors—file, web, email, and network—to detect blended threats.
- **Comprehensive threat intelligence platform:** Collects threat intelligence from millions of sensors on customer-deployed Intel Security products such as endpoint, web, mail, network intrusion prevention systems, and firewall devices.
- **Security Connected:** Integrates with other Intel Security products to provide the broadest threat data, deepest data correlation, and most complete product integration available today to ensure protection against worms like W32/Worm-AAEH.

McAfee Host Intrusion Prevention System

McAfee Host Intrusion Prevention System protects against advanced threats such as polymorphic malware through the combination of signature and behavioral intrusion prevention system protection with a truly dynamic, stateful firewall. McAfee Host Intrusion Prevention System enforces broad IPS and zero-day threat protection coverage across all levels—network, application, and system execution—to protect against evolving threats like W32/Worm-AAEH.

- **Powerful behavioral and signature analysis:** Secure your endpoints against polymorphic malware such as W32/Worm-AAEH with the robust behavioral and signature analysis capabilities of McAfee HIPS.
- **Dynamic stateful firewall:** McAfee Host Intrusion Prevention System is integrated with McAfee GTI to protect endpoints against advanced threats such as botnets, DDOS, and emerging malicious traffic before attacks can occur.
- **Enforced geolocation policies:** Denies inbound and outbound connections with countries that your company does not do business with, and reduces the chance of exposure of your endpoints.
- **Start-up protection:** Allows only outbound traffic and prevents Intel Security services from being disabled during start-up until the complete firewall and IPS policies have been enforced.

McAfee Network Security Platform

McAfee Network Security Platform, based on next-generation architecture, is designed to perform deep analysis of network traffic. Combines advanced inspection techniques—including full protocol analysis, threat reputation, behavior analysis, and advanced malware analysis—to detect and prevent both known and zero-day attacks on the network.

- **Comprehensive malware defense:** Combines file reputation from McAfee GTI, deep file analysis with JavaScript inspection, and signatureless, advanced malware analysis to detect and defeat zero-day threats, custom malware, and other stealthy attacks.
- **Leverages advanced inspection techniques:** Includes full protocol analysis, threat reputation, and behavior analysis to detect and prevent both known and zero-day attacks on the network.
- **Integration with McAfee GTI:** Combines real-time feeds of file reputation, IP reputation, and geolocation with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks. Detecting W32/Worm-AAEH calling its control server is even easier thanks to this integration.
- **Security Connected:** Actionable integration with McAfee Advanced Threat Defense enables McAfee Network Security Platform to submit suspect files found in monitored traffic to McAfee Advanced Threat Defense, and deny or allow their passage based on its findings.

McAfee Threat Intelligence Exchange

An intelligence platform that can adapt to suit your environment's needs is essential. **McAfee Threat Intelligence Exchange** significantly reduces exposure to these types of attacks thanks to its visibility into immediate threats such as unknown file or applications being executed in the environment.

- **Comprehensive threat intelligence:** Easily tailor comprehensive threat intelligence from global intelligence data sources. These can be McAfee GTI or third-party feeds, with local threat intelligence sourced from real-time and historical event data delivered via endpoints, gateways, and other security components.
- **Execution prevention and remediation:** McAfee Threat Intelligence Exchange can intervene and prevent unknown applications from being executed in the environment. If an application that was allowed to run is later found to be malicious, McAfee Threat Intelligence Exchange can disable the running processes associated with the application throughout the environment due to its powerful central management and policy enforcement capabilities.
- **Visibility:** McAfee Threat Intelligence Exchange can track all packed executables files and their initial execution in the environment, as well as all changes that occurred afterward. This visibility into an application or process action from installation to the present enables faster response and remediation.
- **Indicators of compromise:** Import hashes of known bad files and McAfee Threat Intelligence Exchange can immunize your environment against these known threats through policy enforcement. If any of the indicators trigger in the environment, McAfee Threat Intelligence Exchange can kill all processes and applications associated with the indicator.

McAfee VirusScan Enterprise

Detecting and cleaning worms such as W32/Worm-AAEH is simple with **McAfee VirusScan® Enterprise**. VirusScan Enterprise uses the award-winning McAfee scanning engine to protect your files from viruses, worms, rootkits, Trojans, and other advanced threats. Further protect your company with VirusScan Enterprise's ability to block ports, filename blocking, folder/directory lockdown, file-share lockdown, and infection tracing and blocking.

- **Proactive protection from attacks:** Integrates antimalware technology with intrusion prevention to protect against exploits that leverage buffer overflow exploits targeted at vulnerabilities in Microsoft applications.
- **Unbeatable malware detection and cleaning:** Protects against threats such as rootkits and Trojans with advanced behavioral analysis. Stops malware in its tracks through techniques such as port blocking, filename blocking, folder/directory lockdown, file-share lockdown, and infection tracing and blocking.
- **Real-time security with McAfee GTI integration:** Protects against known and emerging threats across all threat vectors—file, web, email, and network—with the support of the most comprehensive threat intelligence platform in the market.

Although detecting and defeating worms like W32/Worm-AAEH can be a daunting task, Intel Security technology can help your company proactively protect itself against advanced malware both on the endpoint and the network.

