



Introducing Microsoft Antimalware Technologies

June 2011

Microsoft®

Introducing Microsoft Antimalware Technologies

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Copyright © 2011 Microsoft Corporation. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Executive Summary	3
Malware Overview	4
Challenges to Detecting Malware	5
Association of Malware to Botnets	6
Antimalware Engine.....	9
Scanning	10
Detection	11
Classification.....	12
Removal.....	13
Update Deployment.....	14
Preventing Exploitation of Software Vulnerabilities	15
Final Thought: Battling Botnets	16
Appendix: Additional Resources.....	18

Executive Summary

Malware (malicious software) is software that has been designed to damage a user's computer, a server, or a network; or to cause harm to computer users by stealing personal or otherwise sensitive information, defrauding the user through various scams, and other nefarious business. Malware is a global problem that affects different parts of the world in different ways.

This paper describes the technologies that Microsoft uses to combat malware. A core technology is the *antimalware engine*, a component that works with many Microsoft products and services. The antimalware engine scans client computers for signs of malware at every possible level of infection, from the browser or application level down to system files. These technologies form part of a larger Microsoft antimalware effort that includes uniform deployment of updates and innovative technology that helps prevent exploitation of software vulnerabilities.

These technologies are supported by the efforts of the Microsoft Malware Protection Center (MMPC), which constantly accrues and analyzes global data to help protect Microsoft customers. The MMPC publishes an analysis of the evolving threat landscape in the [Microsoft Security Intelligence Report](http://www.microsoft.com/sir)¹ (SIR), including detailed content for several countries and regions around the world. For more information about the MMPC, see [Malware Research and Response at Microsoft](http://go.microsoft.com/?linkid=9768948)².

¹ <http://www.microsoft.com/sir>

² <http://go.microsoft.com/?linkid=9768948>

Malware Overview

Malware has become a standard weapon in organized crime's arsenal against legitimate enterprises. Often, individual types of malware are deployed together as part of a large, sophisticated assault designed to unleash waves of malware over time and to recruit vulnerable computers into *botnets*, or networks of compromised computers that are controlled remotely and surreptitiously by cybercriminals.

To install malware on computers, criminals exploit any vulnerabilities that they can find—human vulnerabilities as well as technical ones like weak security policies. Increasingly, the easiest route into a system is *social engineering*: luring users (through websites, downloads, and online advertising) to navigate to sites that install malware on their computers.

Malware can be spread through such vectors as downloaded email and IM attachments, applications shared on social networking sites, files shared peer-to-peer or on network shares, removable flash drives, and hard disks. It can also be spread through exploiting vulnerabilities in the security of legitimate software.

Common types of malware include:

- **Rogue security software.** Rogue security software masquerades as legitimate security software. Sometimes it even imitates the Microsoft Update user interface. It might create fake alerts to scare a user into thinking that his or her computer has been compromised and then clicking a link in order to fix the problem. Clicking such a link downloads malware to the computer. The malware might pretend to detect viruses and then entice the user into paying for a subscription to have the viruses removed. Or, it might download other malware.
- **Password stealers.** A password stealer transmits personal information, such as user names and passwords.
- **Keyloggers.** A keylogger sends keystrokes or screenshots to an attacker. Attackers can use keyloggers to collect passwords, bank account numbers, or any sensitive information that a user types. Keyloggers often work in conjunction with password stealers.

- **Rootkits.** A rootkit performs functions that a system administrator cannot easily detect or undo. A rootkit is often installed as part of a bundle of malware, where it hides itself and other malware that performs a more dangerous activity. When a rootkit runs at the kernel of the computer, it can be especially difficult to detect, because antimalware file scanners cannot trust the data received from the operating system. Successfully removing rootkits has become a special focus area for Microsoft antimalware technologies.
- **Viruses.** Viruses are malware that replicates by infecting other files on the computer, thus allowing the execution of the malware code and its propagation when those files are activated.
- **Worms.** A worm is a self-propagating program that can automatically distribute itself from one computer to another.
- **Trojan horses.** A trojan horse is an application that appears legitimate and useful, but performs malicious and illicit activity on an affected computer. A *trojan clicker* generates revenue by forcing users to access pay-per-click sites or by increasing web traffic to certain sites. A *trojan downloader/dropper* installs other malicious files to the infected computer either by downloading them from a remote computer or by dropping them directly from a copy contained in its own code.
- **Spyware.** Spyware collects information, such as the websites that a user visits, without obtaining the user's consent and often without the user's knowledge.

Challenges to Detecting Malware

Malware writers use constantly evolving techniques to make detecting and removing their software difficult. These techniques include the use of:

- **Packers.** A packer is a program that a malware writer can use to package or bundle a file. Initially, the goal of packers was to reduce file size. Over time, attackers began to use them to hide the structure of a malware file, as packing a single file by using different packers results in different packages. The output of packers also is randomly seeded to produce many files with the same malware inside.
- **Cryptors.** Cryptors encrypt malware code to transform readable data into unreadable data for the purpose of secrecy. After data has been encrypted, it cannot be interpreted (by humans or machines) until it is decrypted. Many encrypted malware files contain the decryption code in the binary itself, allowing the encrypted binary to run without decryption. A common and simple encryption technique used by malware is *XORing*, in which the Exclusive Or (XOR) computational operation is applied to each

bit according to a key. Encryption used by malware is rarely strong; it tries to evade antimalware detection by generating multiple versions of the malware that are functionally equivalent yet appear different to the antimalware program.

Custom-designed packer tools that add layers of obfuscation and encryption to foil analysts and antimalware products are available on the black market, along with license agreements and technical support. Criminals can use them to scramble existing malware, or to create thousands of variants on an existing malware family and release them simultaneously.

Association of Malware to Botnets

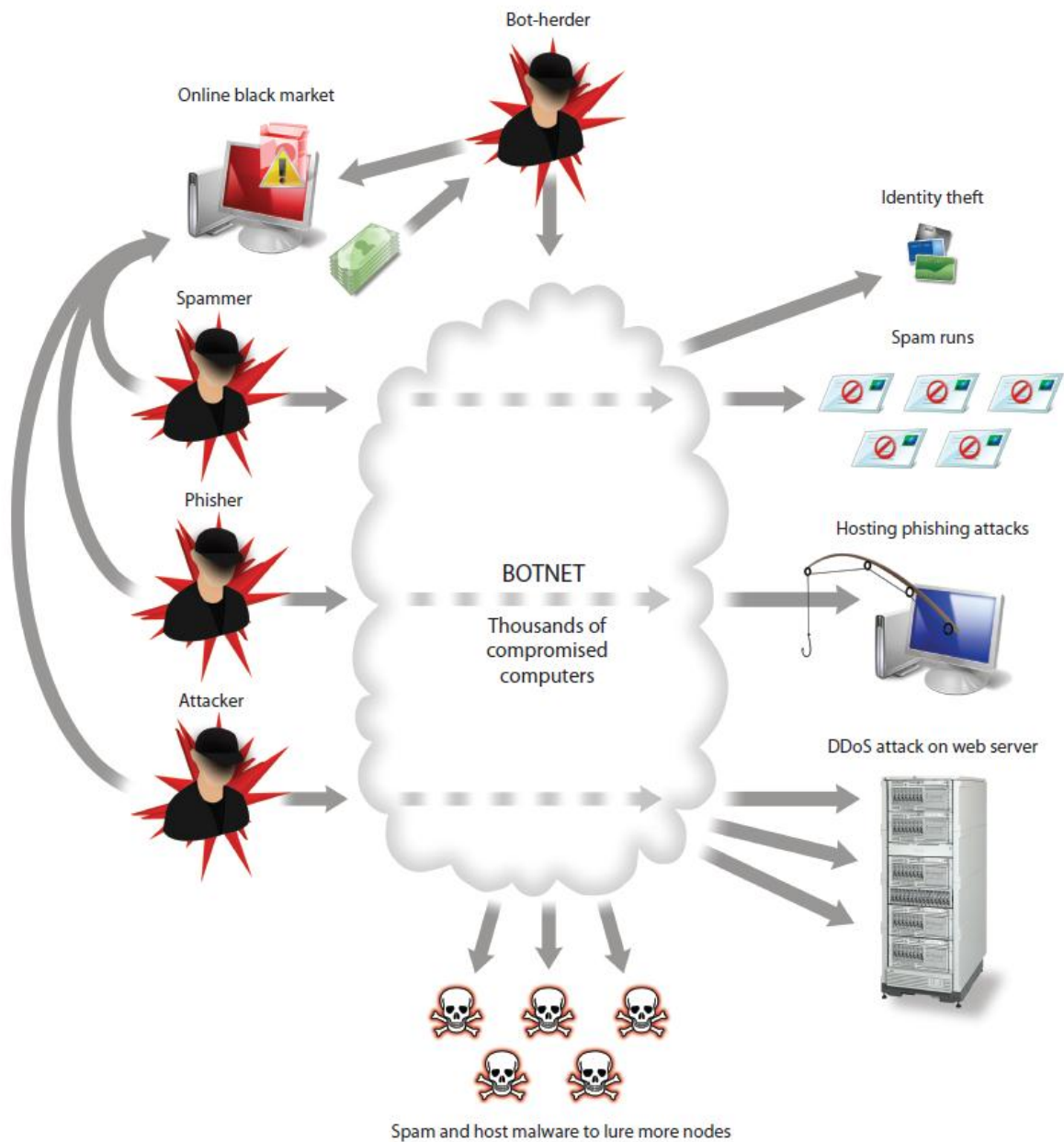
Computers are recruited into botnets when malware is installed on them. Botnets are attractive to criminals because they are easy to hide behind and can be lucrative for the botnet controller, and their use is on the rise.

Because botnets harness the processing power, storage, and bandwidth of personal and business computers, they can be used to generate vast amounts of spam, launch attacks against large websites, commit online advertising fraud, and more. Tracing the origin of an attack only leads back to the hijacked computer of an innocent user.


Botnets are an international problem. The SIR provides the following statistics for the second quarter of 2010:

- The United States had the most botnet infections (2.1 million), far ahead of Brazil, which had the second greatest number of infections (550,000). Spain had the most infections in Europe (382,000), followed by France, the United Kingdom, and Germany.
- Korea had the highest rate of botnet infections (14.6 bot computers cleaned per thousand), followed by Spain (12.4 bot computers cleaned per thousand) and Mexico (11.4 bot computers cleaned per thousand).

The following figure shows an example of a botnet in action.



Botnet creators might attempt malicious activities individually, or they might return to a black market forum and advertise the services of their new network. Sellers may offer malware kits that enable prospective botnet creators to build



their own botnets. Existing botnet owners may rent their networks to spammers and attackers, or sell collections of bots to new owners.

Other sellers offer lists of vulnerable IP addresses or hosting for command and control servers that are supposedly less likely to be taken down by law enforcement. Or they might sell tools such as packers and cryptors.

Antimalware Engine

At Microsoft, the antimalware engine is the core of malware protection. The antimalware engine scans files on more than 600 million computers every month. It runs inside all Microsoft products that include antimalware capabilities, such as:

- Microsoft® Security Essentials
- Microsoft Forefront® Protection Manager
- Microsoft Forefront Endpoint Protection
- Microsoft Forefront Online Protection for Exchange
- Microsoft Forefront Threat Management Gateway (TMG)
- Malicious Software Removal Tool
- Microsoft Safety Scanner

In addition, the technology and reporting in the antimalware engine are used in Windows® 7 security features and Windows Defender scanning and removal features. The antimalware engine also underlies the filters that help protect Windows Live™ Hotmail® and Windows Live SkyDrive™ from malware.

Other technologies work in tandem with the antimalware engine. For example, the Dynamic Signature Service feature helps Microsoft Security Essentials and Forefront Endpoint Protection improve their ability to identify potential threats and prevent false positives.

The antimalware engine needs to be extremely robust, perform quickly, and be agile to react to emerging malware threats. It is updated regularly to add new features and capabilities to detect malware. It looks for malware based on *signatures* (characteristics that help identify malware) and *definitions* (sets of signatures). Other organizations may refer to definitions as DAT files, pattern files, identity files, or antivirus databases.

The engine can block malware at multiple entry points. For example, the engine may catch a dangerous email attachment before a user can download it, or identify changes to registry settings that might indicate the presence of a rootkit.

Having a broad view of the malware ecosystem enables Microsoft to better understand, react to, and interdict malware threats. Through the antimalware

engine, the various Microsoft products gather anonymized *telemetry* (data that can be used for research) about malware and potential malware from client computers and from web crawlers. The ability of malware researchers to automatically filter telemetry data—through technology that works like AppLocker in Windows 7—helps further prevent false positives in identifying malware. In addition, Microsoft partners with external industry organizations to share information and trends, and anyone can submit suspected malware files through the [MMPC sample submission page](#).

By using sources like these, the MMPC has established an extensive, highly detailed, and searchable [malware encyclopedia](#) that is constantly updated and expanded. The encyclopedia contains descriptions of malware behavior, triggers, infection techniques, and removal steps.

Scanning is the first general task that the antimalware engine performs. The engine then detects, classifies, and removes any threats that it finds. The following sections describe these tasks.

Scanning

To minimize performance impacts on clients, the antimalware engine scans only essential files and essential parts of files to check for malware. The engine monitors and examines various locations throughout the computer, such as the hard disk, the registry, and the computer's memory. It quickly checks file attributes and submissions metadata to determine whether the code has any obviously suspicious properties. It then refers to a list that contains the signatures of known malware, and that is updated multiple times a day. If the engine identifies that a change has been made to a critical component such as the file system or registry (known as *behavior monitoring*), or if a file contains the signatures of known malware or traits that are similar to known malware, the engine moves to detection mode.

Microsoft antimalware solutions provide the following scanning options:

- **On-demand scanning.** In on-demand scanning, a system can be scanned at the user's or administrator's request. This option is useful when the user or administrator is troubleshooting a possible infection and needs the latest results of a system checkup immediately. During this process, the antimalware engine also performs deep exploration of archive files on the system.

- **Scheduled scanning.** In a scheduled scan, a quick or in-depth scan of the entire system can run at a time that is convenient for the user (such as in the evening or early morning). Such scans enable administrators to collect system information over time, notice trends, and help ensure that computers are examined on a regular schedule and at an off-peak time. As with on-demand scanning, the antimalware engine also performs deep exploration of archive files on the system during this process.
- **On-access (real-time) protection.** A more powerful method of scanning is on-access protection, where files are scanned before they are opened. If malware is detected, access to the file is blocked to prevent infection. Some Microsoft antimalware products use a minifilter driver to intercept file changes in the Windows kernel and to allow the antimalware engine to scan for malware. Threats at the alert levels of high and severe are blocked from all access, except deletion or remediation by the product that incorporates the antimalware engine.

Detection

After the antimalware engine has identified an item that requires further examination, it must determine whether malware is present. The engine uses various techniques to detect malware:

- **Heuristics.** Heuristics are sets of rules used to classify a program based on its behavior and its static features. These rules are based on existing malware; if a program acts similarly to known malicious software, it is likely to be some type of threat. A challenge with heuristics is authoring them to be specific to malware and not catch programs that are making legitimate changes. Microsoft analysts balance the performance, coverage, and accuracy of detection when creating definitions.
- **Static analysis.** The antimalware engine can analyze heuristics by examining the properties of a suspected program. For example, one heuristic might be to look for instructions that indicate that the program is attempting to modify other executable programs. The engine can perform static analysis quickly by looking at certain patterns of commands.
- **Dynamic translation.** Some viruses are *polymorphic*—they can mutate their structure to avoid detection by antivirus programs, usually by changing one or more variables in their code without changing their overall functionality. Static analysis is not a scalable way to detect polymorphic viruses. In these cases, the antimalware engine can use dynamic translation: It can execute the malware's instructions, step by step, in an isolated virtual environment. If the program attempts to make

- critical changes, such as attaching itself to other files, heuristic detection might notice this suspicious action and identify the program as malware.
- **Behavior monitoring.** Monitoring a program during run time to detect any unexpected behavior, such as changes to critical Windows files or components, or behavior patterns similar to known malware, is more complete than static analysis. However, this approach can take more processing power because the analysis occurs inside a virtual machine. Some malware attempt to evade this detection by looking for signs that it is being run inside a virtual machine and then taking evasive action. The Microsoft antimalware engine can detect these tactics and react accordingly.

Classification

Expert MMPC researchers provide the definitions that the Microsoft antimalware engine uses. These researchers examine new malware samples and read the code to determine exactly what the malware is programmed to do. If the antimalware engine matches a file to a definition, it classifies the file as the appropriate type of malware, such as virus, trojan horse, or spyware.

Classifying potential malware is challenging. Malicious programs have a wide variety of behaviors, appear in a variety of contexts, and involve nearly every technology available on computers (C++, Java, HTML, etc.). Some programs are obviously malicious and offer no benefit to the user, such as viruses, worms, and trojan horses. Most security policies would remove such programs as soon as they are detected.

Other programs present a challenge because they're useful to certain users, but they might have unwanted side effects. For example, some programs display advertisements in exchange for a free service. If the user is informed and consents to the installation, it's not really malware. If the program was installed without the user's consent and control, it may be malicious.

Similarly, IT pros might use tools that enable them to share files over File Transfer Protocol (FTP) or to access computers remotely. These programs are not inherently malicious, but they have the potential to be abused. For example, remote-access software might be installed by a system administrator, or it might be installed by malware or a hacker. Microsoft products enable administrators to assess this risk and decide which programs to allow in their environment.

Removal

The final step is for the antimalware engine to take action against the files that are identified as a type of malware. Any legitimate software that might have been infected is quarantined for closer inspection according to the preferences that the IT administrator has selected for the computer, or the engine removes it automatically.

Because simply disabling executable portions of malware and leaving its auxiliary files on the computer may cause unwanted side effects, the antimalware engine allows for holistic removal of malware. It scans for all components of a single threat—from subcomponents and registry entries to icons and shortcuts—and removes them as a group.

The antimalware engine includes advanced technology that allows for custom remediation for various threats. These steps can include re-creating registry entries and restoring modified settings to safety defaults, which do not happen if a threat is simply removed.

Update Deployment

Keeping computers up to date is an important part of combating malware. Microsoft antimalware products can be configured to automatically download and new definition files as they are released by the MMPC. These automatic channels use binary differencing technology to minimize the resources needed to keep protection update to date.

Mechanisms for distributing these updates include the following:

- **Windows Update.** Automatic update mechanism for Windows components.
- **Microsoft Update.** Automatic update mechanism for Windows plus additional Microsoft software.
- **Windows Server® Update Services (WSUS).** Configurable technology that enables IT administrators to centrally gather, approve, and distribute updates to clients in accordance with change control policies.
- **Alternate Download Location.** Mechanism for downloading specific definition files directly from the MMPC website.

Preventing Exploitation of Software Vulnerabilities

The Forefront TMG Intrusion Prevention System includes Network Inspection System (NIS) technology, which helps prevent exploitation of known software vulnerabilities in Microsoft products and services. If a software vulnerability has been disclosed but Microsoft has not released a security update—or the update cannot be immediately deployed—NIS uses signatures of known vulnerabilities to help detect and block malicious traffic. These signatures are produced by the MMPC and released through the Microsoft Update service.

NIS uses the following types of signatures:

- **Vulnerability-based.** These signatures detect most variants of exploits against a particular vulnerability.
- **Exploit-based.** These signatures detect a specific exploit of a particular vulnerability.
- **Policy-based.** These signatures are generally used for auditing purposes and are developed when neither vulnerability-based nor exploit-based signatures can be written.

For information about configuring, monitoring, and troubleshooting NIS, see the [NIS in TMG white paper](http://download.microsoft.com/download/F/4/0/F40887FD-648B-40E1-B79B-AAE43CEDCA4C/NIS%20in%20TMG%20Whitepaper.docx)³.

³ <http://download.microsoft.com/download/F/4/0/F40887FD-648B-40E1-B79B-AAE43CEDCA4C/NIS%20in%20TMG%20Whitepaper.docx>

Final Thought: Battling Botnets

Although this paper has focused on antimalware technologies from Microsoft, the company is moving against the associated threat of botnets as well.

On September 8, 2010, Microsoft announced that its legal action—in cooperation with industry and academic experts around the world—to [shut down a major botnet known as Waledac](#) was successful. Before the shutdown, Microsoft estimated that Waledac infected hundreds of thousands of computers around the world and had the capacity to send more than 1.5 billion spam email messages a day. Microsoft also found that from December 3 through December 21 of 2009, Waledac was responsible for approximately 651 million spam email messages directed to Hotmail accounts alone, including offers and scams related to online pharmacies, imitation goods, jobs, penny stocks, and more.

This successful operation against Waledac has paved the way for future shutdowns in cases where criminals are abusing anonymity to victimize computer users around the world. Microsoft gained a deep insight into the workings and footprint of the Waledac botnet, and it began working with the Computer Emergency Readiness Team (CERT) and Internet service providers (ISPs) to help customers remove the Waledac malware from their computers.

The Waledac shutdown was the first undertaking in a larger initiative called Project Microsoft Active Response for Security (MARS), which is a joint effort between the Microsoft Digital Crimes Unit, the MMPC, Microsoft Support, and the Microsoft Trustworthy Computing team to annihilate botnets. In March 2011, Microsoft announced another success under the MARS initiative when it collaborated with industry and academic partners and law enforcement agencies to [act against the Rustock botnet](#). This botnet was estimated to have approximately 1 million infected computers operating under its control and was capable of sending billions of spam messages every day, including fake Microsoft lottery scams and offers for fake—and potentially dangerous—prescription drugs.

Microsoft created the [Virus and Security Solution Center](#) to help people understand botnets and remove malware from their computers. This site, the efforts of Project MARS, and the Microsoft teams and technologies that continuously work to combat malware help make computing safer for everyone.



Appendix: Additional Resources

For more information related to the concepts in this paper, see the following resources:

- [Microsoft Malware Protection Center \(MMPC\) website](#). Contains details of top threats, an in-depth malware encyclopedia, malware tools and resources, and a malware sample submission mechanism.
- [MMPC blog](#). Provides a real-time method for MMPC subject-matter experts to communicate with customers. Topics include “behind the scenes” information about new, emerging, and notable malware threats, in addition to other research topics in the field of computer security.
- [MMPC Twitter feed](#). Provides timely information from the MMPC.
- [MMPC Facebook page](#). Provides a way to keep up to date with MMPC activities.
- [Malicious Software Removal Tool \(MSRT\)](#). Helps identify and remove specific, prevalent malware families from customer computers running the Windows 7, Windows Vista®, Windows XP, Windows Server 2008, Windows Server 2003, and Windows 2000 operating systems. This free tool is released as an Important update through Windows Update, Microsoft Update, and Automatic Updates. A version of it is also available from the Microsoft Download Center. As of April 2011, the tool detects and removes 155 malware families. When the detection and removal process is complete, the tool displays a report that describes the outcome. **Note:** The MSRT is not a replacement for an up-to-date antivirus solution because it lacks real-time protection and uses only the portion of the Microsoft antivirus signature database that enables it to target specifically selected, prevalent malware.
- [Microsoft Security Response Center \(MSRC\) website](#). Provides information about the MSRC and the programs that it operates.
- [MSRC Twitter feed](#). Provides timely information from the MSRC.
- [Trustworthy Computing security and privacy blog aggregator](#). Features blogs from the Microsoft Trustworthy Computing group, which works to deliver more secure, private, and reliable computing experiences. Also provides information about the Microsoft long-term vision and strategy for computing privacy and security.





Microsoft®

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security