McAfee Platinum Technical Support Handbook

Version 8.1

COPYRIGHT

TRADEMARK ATTRIBUTIONS

Dear Platinum Support Customer:

The profound expertise embedded in our comprehensive solutions and services delivers a proven ability to block attacks and prevent disruptions, allowing you to secure your business advantage.

Balancing business priorities with security needs is a constant challenge in today's ever-changing business environment. McAfee helps you meet this challenge, head on, with practical, proven solutions, combined with unmatched security expertise. Working with us, you can plan, execute, and continuously improve your security posture, with the most effective use of available resources. When you choose McAfee you can be confident that your systems and networks are protected from attacks, and costly business disruptions are prevented.

We would like to welcome you as a customer of McAfee Platinum Support. Our goal is to provide you with the highest level of service available in the industry. In this handbook, we will explain the services to which you are entitled; as well as some of the processes and procedures that we have in place. You will find details on how you can contact your assigned Technical Account Manager (TAM) during office hours and in emergency out of hour's situations.

Thank you for giving us the opportunity to serve you.

The McAfee Inc. Platinum Support Team

Be sure to print this guide and forward it to all contacts that are authorized to contact your assigned TAM on behalf of your organization. Individual pages with the phone symbol should be printed for future quick reference.

Accessing Platinum Support

Technical Account Manager (TAM) Information:

Name:	{TAM Name}
E-mail Address:	{TAM E-Mail Address}
Direct Phone:	{TAM Phone}
Mobile Phone:	{TAM Mobile} – **for severity 1 and 2 issues only**

Telephone Access:
This is 24 x 7 Support * Local Office hours are 0800 to 1800 Local Time
(Subject to local holidays and weekends)

Your TAM's working hours are: 8:00 a.m. to 5:00 p.m. Central Time

OneCall: 800-977-2237 (OneCall is available in North America Only)

OneCall is a method to alert Platinum Support Management if you have not received a return call within 30 minutes after paging your TAM on an urgent situation. Please dial the One Call toll-free number. Provide the operator with your name, contact number, company name and the assigned TAM's name. The operator will then notify a member of the Platinum Support Management Team to contact you and promptly engage your TAM with regards to your issue.

Platinum Support Management Escalation Contacts

Manager, Platinum Support

Name:	
E-mail Address:	
Direct Phone:	
Mobile Phone:	

Director, Platinum Support

Name:	James Pleasant
E-mail Address:	james_pleasant@mcafee.com
Direct Phone:	972-963-7403
Mobile Phone:	469-853-6935

Vice President of Global Customer Service and Technical Support

Barry McPherson	North America
Direct Voice:	972-987-2826
Email Address:	barry_mcpherson@mcafee.com
Mobile Phone	214-578-1081

Platinum Support Features

What is included?	Description	Availability
Certified Technical Account Manager	An assigned Technical Account Manager (TAM) is your direct line to McAfee: • Security Certified Technician to utilize as an extension of your staff • Direct access to Tier 3 and Product Engineering to provide quick resolution to issues • No waiting in a telephone queue	Included
Proactive support	TAM contacts customers at customer defined frequency to review current issues and new information from McAfee. • Frequency and contact method determined by the customer	Included
Response Charter	• Direct Access to TAM	Included
Customer care ServicePortal	• Open and track technical support service requests and service request history • Search Knowledgebase and FAQs for technical solutions • Receive alerts on product patches, product upgrades, and more • Receive proactive e-mail notification on your open service requests • Ability to customize user profile and update account information • Online tools to aid in quicker issue resolution	Included
McAfee Security Alert Service (MSAS)	Delivers fast alert notification with your choice of communication methods • Communication options: voice, e-mail, SMS, fax • Alerting type options vulnerabilities, product upgrades, and product patches • Threat severity notification: option to configure by time and method of communication, and by level of threat assessment	Included Configurable Online 24/7
Newsletter	The Platinum Newsletter is available to our customers • Contains information on security threats & vulnerabilities, current products, & updates • New developments in the product line • Suggestions, tips, and tricks	Included
Activity reports	Comprehensive report detailing all support activities undertaken on behalf of the customer, delivered on a schedule agreed to by the customer and TAM (weekly, monthly, etc.)	Included
Security planning assistance	Assist in planning of the rollout and upgrade of McAfee security products and solutions. Where applicable, use McAfee Global Support Lab as a tool in preparing upgrades, product rollouts and demonstrations before the actual implementation.	Included
Onsite visits	Onsite visits are designed to provide additional support. Examples of onsite activities include: • Account Business review • Protection Analysis review • Future upgrade discussions	Included
Joint Development Program (JDP)	Opportunity to participate in the Joint Development Program (JDP) • Direct engineering contact • Code development stage • Implementation/usability planning	Included
Regional TAM Availability	In addition to the primary Platinum TAM, customers have the ability to leverage a regional TAM in the following geographies. Japan—Asia Pacific (APAC) —Europe, Middle East, and Africa (EMEA)—Latin America (LATAM)—North America (NA)	Optional
Malware submissions (anti-virus only)	McAfee Avert® WebImmune is the world's first Internet virus security scanner that resides on the web. It is constantly available (24x7/365). You can submit potentially infected files to WebImmune for analysis. You will receive information about your files, including solutions and real-time fixes, if required.	Included
Customer visit and/or VPN access to Global Support Lab	Scheduled access to our Global Support Lab to plan product roll out or testing with TAM. McAfee's Global Support Lab offers remote or onsite (in the Plano, Texas, Support Center) connectivity to multiple changeable configurations of McAfee security products for testing, training, and development.	Prioritized for Platinum Technical Support customers
Dedicated TAM	If needed, a security certified TAM dedicated to your account and your account alone for individual attention, planning, and advice.	Optional

TAM Out of Office Procedures

The idea of Platinum support is to provide a single point of contact for all our customers support needs. At times this is not always possible due to illness, holidays, meetings etc. When this situation occurs we have the following procedures in place.

When your TAM is away from the office due to illness, holidays, and meetings or as other circumstances arise, he or she will proactively notify you of the length of time they will be away. They will provide you with the name and phone number of the temporary TAM that will be covering your account until their return. They will also activate their "out of office" message on their voicemail system and provide the name and phone number of the temporary TAM that will be covering your account until their return.

TAM Onsite Business Review Procedures

Platinum Support customers are entitled to Onsite Business Reviews with their TAM. Onsite Site Business Reviews activities include:

- ✓ General "Meet and Greet" – team introductions
- ✓ Account Business Review – A review of all account interactions within a specified period of time
- ✓ Security Upgrade Planning – Opportunity to discuss upgrade or migration strategies
- ✓ Protection Analysis – Product review, account review, product upgrade planning session
- ✓ Product Roadmap discussions – Non Disclosure Agreement (NDA) must be in effect; advanced notice is required

At the conclusion of the Onsite Business Review, the TAM will document the visit and record any actionable items and ownership of these items. A copy of this document will be forwarded to the account Primary contact and the McAfee Sales Account Manager.

TAM Response Charter

Direct access via cell phone
Emergency Cell Phone Messages: 30 minutes
Office Voicemail: 1 hour
Email: 2 hours

Severity Codes and Service Level Agreements

A severity code is associated with all service requests, failures and enhancement requests. The severity code indicates the impact to the customers business and, along with priority level, the urgency required.

Severity	Ack/Resp	Escalation to Tier III	Escalation to Development	Status Updates
1 - Business Stopped	Immediate	30 Minutes	4 Hours	Continuous Phone Bridge
2 - Business severely impeded	Immediate	1 Hour	6 Hours	Hourly
3 - Business impeded but functioning	Immediate	5 Days	5 Days	Daily
4 - Business not affected but symptoms exist	Immediate	25 Days	25 Days	Weekly
5 - Request for Information	Immediate	30 Days	30 Days	Every 2 Weeks

(NOTE: McAfee Inc. does not guarantee defects will be fixed in any specific time duration due to the nature of software operating in a multi vendor environment. It is the goal of McAfee Inc. to deliver our best effort to satisfactorily resolve each incident using the guidelines in the table.)

Severity Defined

Severity is the definition of the issue based on the actual technical problem and the impact on the customer's business.

Severity 1 – Customer's business has stopped.

Our product is not functioning; Internet connectivity or mail flow has stopped. There is no viable workaround for this customer either in the system or via manual processes. Customer is unable to provide available virus protection to his network.

Severity 2 - Customer's business is severely impacted.

Symptoms are present across the environment, includes installation failures, conflicts with major brand software, or a specific mail flow issue. Customer is generally able to provide available virus protection to his network but specific resources cannot update.

Severity 3 - Customer's business is impeded but functioning.

The symptom affects a single machine or isolated parts of the environment. The problem restricts the use of one or more features of the product to perform necessary business functions but does not completely restrict use of the product.

Severity 4 - Customer's business is not affected - symptoms exist.

The symptom affects few machines or is easily circumvented. The error can cause some functional restrictions but it does not have a critical or severe impact on operations.

Severity 5 - Request for Information

This includes general requests for product information and Feature Modification Requests. Severity 5 service requests would not involve any shortcomings in virus protection.

Submitting a Service request

Service requests should be submitted directly to your TAM in the region where the software problem or error has occurred. Prior to contacting McAfee Technical Support, ensure that the following information is available:

- ✓ Detailed description of the problems or errors
- ✓ Description of the hardware (must meet published McAfee specifications) that the software is installed on, including the serial number or service tag where applicable
- ✓ Name and versions of any operating system, network, and software running with
- ✓ the McAfee software, including patches and fixes

Minimum Escalation Requirements Tool (MER Tool)

If your call needs to be escalated to Tier III support, Platinum support will require some files from the machine or machines that are experiencing your issue. These additional files are needed by Tier III to further investigate the issue. When run, this tool will obtain necessary files from your system. These files will vary depending on the O/S and the McAfee software that has the issue. The type of information that will be obtained will be an MSD report (or other O/S equivalent), event logs, McAfee (or Network Associates) registry keys, McAfee log files and current McAfee EXE files. This is just a basic range of the types of files that will be obtained. Once obtained the tool will create a .TGZ file (compressed) and this can then be sent to your TAM to analyze or escalate the service request. Please note that on certain issues a screen shot of the error will also be requested in addition to the MER tool being run.

For full details of a particular MER tool, please contact your TAM as the MER tools change regularly.

Witness Program

McAfee Technical support strives to provide the best possible service to its customers and has invested in a comprehensive call management tool that allows its management and business excellence team to recover all details regarding a specific service request.

The Witness tool stores a recording of the data entry as it is entered into our system including keystrokes and mouse positions, and synchronizes this with the recorded voice or chat call. This information is used to provide feedback to our engineers on best practices and examples of best of practice. Customers with a grievance to the way their call has been handled can also request a manager to review their service request.

Customer Satisfaction Survey's

Every time a service request is submitted to McAfee we will track this issue and upon the resolution of the service request to your satisfaction McAfee will request an independent 3rd Party research company (Walker Information, Inc.) to send you a survey to complete. Surveys are available in all languages that McAfee Supports.

The information in this survey is totally confidential and will not be passed on to any company outside of McAfee. This information will allow us to improve the service we offer while at the same time act as a safeguard to ensure that you are happy with the service that you receive. This is monitored through a closed-loop process tool that is used to ensure we are communicating with those customers who have asked for further communication from our management team.

Metrics and responses from these surveys are analyzed weekly and feedback provided to Support Management, Product Management, Engineering, and Sales on results. We implement measurable actions based off of key drivers.

Proactive Information

In order to help you be prepared and manage your anti-virus environment with the maximum information possible, you will receive the following reports from your TAM on a regular basis:

Bi-Weekly Newsletter (NDA required)

On a bi-weekly basis, you will receive a newsletter. This newsletter may consist of the following information and any new developments from McAfee:

- News releases
- Beta Releases
- Product Updates
- Product Releases
- Latest Advisories (Viral or Vulnerabilities)
- Top 10 KB articles
- Latest KB Articles created
- New Hot fixes
- Technical documentation
- Product End of Life (EOL) Information
- And an assortment of other useful information

Executive Summary Report

This report will be sent out to Platinum Primary contacts on a quarterly basis and provided during Onsite Visits with your TAM. It will contain historical information on your issues during a specified review period including:

- ✓ The number of service request submissions by product
- ✓ The service request Average Resolution Time (ART) by product
- ✓ The service request closure rates, by product
- ✓ The number of Proactives sent to you, by month
- ✓ Percentage of service requests, by product and by severity level
- ✓ And a brief recap of each service request submitted during the specified review period

Product Upgrades (http://www.mcafee.com/us/enterprise/downloads/index.html)

As a Platinum Support customer you are entitled to download the latest versions of your software any time, providing that you have a valid support contract. This service is provided free of charge and allows you to maximize the security of your systems by providing protection from the very latest threats.

Entering your valid Grant number at the following site will display the software you are entitled to, which can then be downloaded ready for installation. The following location can be used to check for available software.

Deployment of product upgrades across multiple nodes can be carried out simply using the ePolicy Orchestrator (ePO) application. Instructions on upgrading software using ePO can be found in the KnowledgeBase. Additionally, flash-based demos are now available on the McAfee ServicePortal.

McAfee Security Alerting Service (MSAS)

MSAS is a proactive alerting tool to notify you of threats as they arise, as well as product patches or upgrades as they become available. As a new threat assessment rises, or as a new improvement is made to an existing McAfee solution, MSAS sends timely and actionable intelligence to the right person or people - on the communications device(s) of their choice.

MSAS alerts are customizable by the user in a number of ways, allowing you to determine both by product and by threat assessment when and where your alerts should be delivered.

McAfee's emergency threat response teams, including McAfee Avert®, our industry leading virus research center, and McAfee Research, the technology research division of McAfee, perform round-the-clock analysis on potential vulnerability and virus threats. McAfee monitors and assesses threats of all sorts, and categorizes them by risk and severity. When a threat is determined, McAfee generates a notification message that can be distributed to every subscriber of MSAS in as little as 30 minutes, including all the communication methods selected by the subscriber.

Access to MSAS is available through the McAfee ServicePortal . Once set up, simply click on the 'MSAS' link to set up your preferred alerting profiles as well as the level of risk assessment to be alerted on for each contact method.

Standard Alerts

Customers using McAfee Security Technical Support can review all current alerts using the McAfee ServicePortal, and are given multiple options to configure the alert notifications that best meet their needs. Upon logging in to the ServicePortal, all of the customers' recent and current alerts are made available in each of the following areas of interest:

- ✓ Announcements
- ✓ Product Alerts
- ✓ Grant Expirations – Upcoming expirations, and already expired
- ✓ Service request Updates
- ✓ Hotfixes
- ✓ Available Downloads
- ✓ New documentation (White papers, technical bulletins, release notes, etc.)
- ✓ New/Updated solutions

Deployment Assistance Program

To aid customers in the limited installation and evaluation of new appliances McAfee offers the Deployment Assistance Program (DAP).

A McAfee Platinum Support TAM is assigned to remotely support you and your organization. The assigned Platinum Support TAM is selected from our highly skilled and certified Platinum Support team based on their product expertise. You can rest assured you are dealing with a product Expert.

The Platinum Support TAM will work with you to schedule the deployment at your convenience. The TAM will remotely connect to your site and:

- Assist with the installation
- Deliver configuration training
- Share best practices
- Advise on system tuning tips
- Much more!

Your Platinum Support TAM is your trusted security advisor during and after the deployment process.

Deployment Assistance is available for the following McAfee products:
- SCM
- Foundstone FS1000
- IntruShield
- MHIPs

For additional information on DAP, please contact your TAM or your McAfee Sales Account Manager or Channel Partner.

McAfee ServicePortal

Our ServicePortal offers 24-hour access to solutions to the most common support requests; you are also able to use the ServicePortal to view your open service requests, log new calls, request alerts for hot fixes or product upgrades, plus much more. Using the ServicePortal, you can find the following information:

- ✓ Log, update, search and review service requests
- ✓ Over 10,000 Knowledgebase Articles
- ✓ Video Tutorials and Guides
- ✓ McAfee Security Alerting Service (MSAS)
- ✓ Chat Support
- ✓ Manuals
- ✓ FAQs
- ✓ Attack Encyclopedia
- ✓ Alerts on hot fixes, upgrades, documentation and Grant Expiration

Global Support Lab

The Global Support Lab provides customers with hands-on access to McAfee's products from almost anywhere in the world. Secure internet connectivity allows users gain access to their own secure Lab environment without having to purchase or transport products to their own facilities.

The Global Support Lab infrastructure is located in several locations around the world and includes McAfee's server and appliance based products. Multi-lingual support can be provided for most major languages and includes "Double Byte" compatibility from our Japan location. The Global Support Lab offers a variety of different options and benefits, based on the scenarios selected by the user.

- ✓ Test out a new configuration before deploying in your environment
- ✓ Pre-deployment testing of new functionality
- ✓ Check out a product upgrade process
- ✓ Evaluate new products

The Global Support Lab provides quick and easy access to McAfee products at the click of a mouse. This automated solution allows full control of dynamically configured servers and clients. Users can configure and install products in a safe and controlled environment, with control of McAfee hardware appliances as well as software products.

Demonstration

The Global Support Lab provides an excellent tool for you to receive demonstrations of the latest products from your reseller or McAfee salesperson. With the ability for several users to view the same session, demonstrations can even be given remotely, without the need to be in the same location. New product features can be demonstrated as soon as the products are released to ensure that you are aware of the latest technologies and you can ensure your infrastructure remains as secure as possible. These scenarios provide the user with the product in a default configuration and can also be used for Evaluations if installation is not required.

Evaluation

These scenarios enable users to gain hands on experience with products in a safe environment. The latest products can easily be accessed and enable users to be confident in deploying the product. Customers in the McAfee Beta program for a specific product have the ability to evaluate that product using McAfee hardware from their office, without having to find their own dedicated machine. For server based scenarios the user is provided with the base operating system and the install files for a total product experience.

Training

A significant number of training scenarios are available covering some of the common issues that the McAfee Technical Support organization has identified. McAfee is constantly developing new scenarios on a daily basis to aid in the familiarization of its products and help fault finding on its products.

Custom Configurations

The Global Support Lab also provides facilities for custom configurations to be created for a specific customer. These scenarios could be replication of configuration issues or pre-deployment testing of a specific configuration. Customers can work with a reseller or McAfee Sales Engineer to understand their specific needs and requirements. (McAfee may charge for custom configurations).

McAfee Professional Services (Training and Consulting Services)

In addition to our Technical Support Services, McAfee offer comprehensive Professional Services around the globe. The goal of McAfee's Professional Services organization is to ensure, via delivery of consulting and education services, that our customers derive maximum benefits and ROI from the successful and efficient deployment of our technology.

Our Education Services provide training in product installation, configuration and administration, analysis and troubleshooting. Through the provision of class-room training, custom on-site training and consultancy, our aim is to facilitate customers' self-sufficiency with the installation, administration and upgrade of our products as efficiently and cost-effectively as possible.

For further information please see: http://www.mcafeesecurity.com/us/services/home.htm

Beta Participation

We highly value Customer participation in our Beta programs. Your participation ensures we release very high quality products that have been tested in real-world environments. The benefits of participating is having early access to the software and influencing the feature set for next versions.

Beta Objectives

- ✓ To test the product in a real world environment for the purpose of identifying major defects prior to the release.
- ✓ To ensure that new product features meet customers' needs.
- ✓ To gather feedback on the usability of our products.

Public

Most of our Betas are open to the public for testing. Anyone wishing to participate in the public beta test is welcome to do so. Beta Participants receive technical support and communication updates via the beta forum.

For more information please see: http://www.mcafee.com/us/enterprise/downloads/beta/index.html

Joint Development Program

Purpose
The Joint Development Program is an integral part of our Customer-centric product development process. Customers work closely with the development team at the beginning of the project to validate requirements, design, features and quality.

Recruitment
JDP Partners are enrolled on a per project basis, based upon needs identified by the project team and by customer interest in participating. Not every project or release requires a JDP, some items considered when identifying appropriate projects are; the introduction of significant new functionality, the amount of changed code, whether not the use model of a given product is altered. To ensure an effective program, the number of JDP Partners associated with a product release is strictly limited. Typically there will be 4 to 6 JDP Partners assigned to a product release.

Requirements for the Joint Development Program:

- ✓ Participants must be available to test and provide feedback during the project cycle.
- ✓ Participants must be available for weekly calls.

The McAfee Avert® Labs Threat Risk Assessment Program

Goals and Benefits

The McAfee Risk Assessment Program evaluates the level of risk posed by threats encountered in the field or at customer sites. The team of global threat experts at McAfee® Avert® Labs strives to inform customers and PC users about current infection risks and their possible consequences, so that they can take appropriate security measures to protect themselves against infection. Risk assessments are included in the threat descriptions posted to the Threat Library. The information is also available at our online Threat Center. Note that risk assessments are supplied only for malicious threats, such as viruses, worms and Trojan horses, at this time. Potentially unwanted programs (PUPs) are not rated currently.

Executive Summary

Today, there are more than 150,000 viruses, virus variants, Trojans, and other types of malicious code in circulation. Every month, this figure increases by approximately 2,500 to 4,000. In order to help network administrators and home users protect their networks and systems when new threats strike, McAfee Avert® Labs rates each threat based on criteria described below.

When assessing the level of a particular threat, McAfee Avert® Labs determines risk to corporate users and home users separately. This information is included in the threat definition posted by our researchers.

Criteria for Assessing the Risk

Risk of a threat to any individual or corporation can be determined by answering the following questions:

1. How likely is it that I will be attacked successfully (exposure)?
2. What is the impact if I am attacked successfully (impact)?

Note that this is a statement of probability. While it may be true for a hypothetical user and a hypothetical threat, for any individual user or corporation with a real threat, the answer is that you either will or will not be infected. Whether that occurs depends on your particularly security posture, countermeasures you have in place, response speed, effectiveness of your countermeasures, and even pure luck. When determining the risk of a threat, McAfee Avert® Labs attempts to gauge the **average** probability for our customers globally. This does **not** mean that some customers will not be affected by low-risk threats, or that many users will be unscathed by high-risk threats.

Exposure*: How likely is a successful attack?*

In theory, measuring exposure should be fairly straightforward. If a threat is e-mail-borne, and one in 10 e-mails contains the threat, then the risk of exposure is 10 percent. In practice, the situation is seldom this straightforward. Some factors that may alter true exposure levels include:

- The number and popularity of possible targets (Microsoft® Windows® threats are likely to spread more effectively than Macintosh® or Unix threats)
- The number of propagation or infection vectors the threat is capable of exploiting.
- · The popularity of those vectors. (For example, significantly more people use e-mail than peer-to-peer file-sharing programs.)
- · Whether the threat requires user interaction to mount a successful attack.

- If the threat requires user interaction, the effectiveness of the social engineering employed to trick the user into running the threat.
- If the threat exploits a vulnerability in a piece of software, the availability of a patch and the length of time that the patch has been available.
- The existence and effectiveness of existing countermeasures capable of thwarting an attack. (Do some or most anti-virus vendors detect the threat proactively?)
- The degree to which previous threats exploiting the same vectors or media interest have alerted users to the dangers posed by the social engineering or an unpatched vulnerability.
- The degree to which customers have become desensitized to security industry warnings as a result of frequent or exaggerated warnings about other threats.
- The number and types of limitation or bugs in the threat's coding.
- Whether the threat was actually ever released and how it was released. (Was the threat seeded slowly or mass-spammed? Were the initial seeding attempts thwarted?)
- The speed and effectiveness at which the security community-including security vendors, Internet service providers, and law enforcement agencies--responds to the threat.

The single most reliable measure of exposure is prevalence to date. Prevalence can be thought of as actual, verified customer reports of successful attacks over time. However, measuring this can be complicated as well for these reasons:

- Customers may fail to notify us of infections.
- Customers may report blocked threats as if they were infections or vice versa.
- Attempts to extrapolate infection rates from volume of infected e-mails are notoriously flimsy. Threats can vary by many orders of magnitude in terms of number of infected e-mails per infected machine.
- Occasional traces such as the counter supplied by the MyWife.d author may be misinterpreted or abused.

As a result, it is difficult to determine a numeric or absolute standard for different prevalence levels. The following guidelines work with some threats, but Avert® may revise them on a case-by-case basis based on our decade of experience fighting malware. In some cases, higher exposure risks may be assigned:

- **High Exposure Potential** - The threat has been identified in the field, and more than 20 instances have been reported in less than four hours. Threats exploiting unpatched vulnerabilities in popular operating systems or applications with significant secondary indications of infection may also be placed in this category.
- **Significant Exposure Potential** - The threat has been identified in the field, and more than 20 instances have been reported during one business day (eight hours). The reported cases can originate in a single country or region or from numerous countries and regions. Threats exploiting patched vulnerabilities in popular operating systems or applications; unpatched vulnerabilities in less common applications or operating systems.
- **Moderate Exposure Potential** - The threat has been identified in the field, but fewer than 20 instances have been reported over 24 hours. This classification applies to threats exploiting vulnerabilities where a patch has been available for more than a certain number of days.
- **Low Exposure Potential** - The virus is known to our researchers, but few or no infections have been reported over a period of several days.

Payload*: What kind of damage results from infection?*

Like exposure, damage can be difficult to measure in an absolute fashion. Generally, damage that is visible and obvious is considered less severe than damage that is difficult to see or quantify. Examples of more complex damage include:

- Data or potentially confidential files being sent to third-parties.
- Loss of reputation or legal liability as a result of data breaches.
- Installation of components that allow arbitrary code execution at a future point in time (backdoors and bots).
- Subtle manipulation of data files (See see XM/Compat.A)
- Allows attacks on other parties (DDoS clients).
- Causes issues with printers or other network-attached devices. (See W32/Bugbear@MM)
- Terminates or otherwise interferes with security products, leading to exposure to unknown future attacks.

Based on these considerations, Avert® uses the following guidelines for determining potential damage caused by threats.

- **Unforeseeable Damage** - The threat redistributes confidential data to third parties, creates additional unbounded security holes, or brings down an entire network.
- **Extremely Serious Damage** - The threat manipulates data silently or contributes to the harm of others.
- **Serious Damage** - The threat deletes a number of files, formats hard drives, or deletes the Flash BIOS.
- **Medium Damage** - The threat deletes individual files or renders the computer temporarily unavailable.
- **Minimal Damage** -The threat generates bogus text or generates sounds.

Risk Levels

McAfee Avert® Labs report risk levels for threats in order of severity: The risk level assigned to a threat changes as its prevalence changes. Each level is defined below. Recommended actions for customers and actions taken by Avert® with each risk level are listed in a table following the risk level descriptions. The recommended action should be modified to meet your specific needs.

High/Outbreak

These viruses are detected by our threat researchers on most continents within a very short period of time. They are almost always spread via mass mailings or via remote vulnerability exploitation, so they often have a global impact in a matter of hours.

Examples:

- W97M/Melissa
- VBS/Loveletter
- VBS/VBSWG (Anna)
- W32/Nimda
- W32/Mydoom

High

Viruses in this category are discovered in the field and have a payload that can cause serious damage. They usually spread rapidly on common platforms with widely used operating systems. If a virus causes serious damage or catastrophic damage, it may be classified as high risk even if its prevalence is low.

Examples:

- Win95/CIH

- VBS/Newlove
- W32/SQLSlammer.worm
- W32/Sobig.f
- W32/IRCbot.worm!MS05-039

Medium/On Watch

These viruses gain prevalence quickly, have a payload, and usually infect common systems or spread via popular applications. This risk level serves as an early warning signal. The experts at McAfee Avert® Labs closely monitor the prevalence of these viruses as they spread to determine whether the risk level needs to be elevated.

Examples:

- W97M/Resume
- W32/Badtrans.b
- W32/Fizzer.gen
- W32/Blaster.worm
- W32/Bagle.aa

Medium

This level of risk applies to viruses that have been reported by several McAfee customers or McAfee Avert® Labs researchers. They may have a destructive payload and may infect common platforms and widely used applications.

Examples:

- W32/Sober.c
- W32/Bagle
- W32/Netsky.b
- W32/Sasser.worm
- W32/Zafi.d

Low/Profiled

This rating applies to viruses that appear to be low risk but warrant additional monitoring because they have attracted media interest. These viruses may not yet have been discovered in the field and may not have a dangerous payload. We may also classify a virus as a Low/Profiled if it is a variant of a family of viruses that has high prevalence and has the potential to spread.

Examples:

- W32/Bugbros@MM
- W32/Bizex.worm
- W32/Evaman@MM
- W64/Shruggle

Low

This classification is for viruses that may not yet have been reported in the field and may not have a dangerous payload. These viruses typically target obscure or rarely used applications, though at times, they may run on common platforms. The risk assessment for such viruses is Low if the payload is classified as Extremely Serious or Unforeseeable.

Examples:

- W32/Cycle.worm.a
- W32/Reatle.gen
- W32/Vulgar

Not Applicable (N/A)

The Not Applicable (N/A) risk assessment is used on descriptions for threats or apparent threats that do not warrant an assessment. E-mail hoax descriptions have a risk assessment of N/A as they are not Trojans or infectious like viruses. Trojan and virus family descriptions and heuristic detection descriptions have a risk assessment of N/A because they are general descriptions and do not describe specific threats.

Updated Risk Assessments

The risk level for a virus can move from lower to higher over a period of time. For example, a virus may start out with a Low risk assessment, but is later elevated to a Medium or Medium/On Watch level as its prevalence increases. In most instances where a virus is classified as Medium/On Watch, we frequently raise the risk assessment to High. A risk assessment is lowered when the prevalence of a virus decreases. When a virus is no longer classified as a High risk, it often stays in the Medium risk category for a period of time.

Examples of viruses that have had their risk assessments raised:

- IRC/Stages
- W32/SirCam
- W32/APost

Notes:

ASAP—Deploy patches (if necessary to prevent exploitation of a vulnerability by a threat with this rating), EXTRA.DATs, or full DATs as soon as available.

Recommended —Avert® Recommends that you also perform these steps as soon as possible (if you cannot perform a step because of lack of resources or lack of appropriate technology deployment).

Where Applicable —Entercept® and IntruShield® signatures will be released on Medium and above threats when those technologies are capable of protection.

If Necessary—EXTRA.DAT files will only be created if the latest full DAT release does not contain detection for the threat.

Next Regular Update—Low/Profiled and below threats will be included in the next regular DAT release unless they increase in risk.

The McAfee Avert® Labs Vulnerability Risk Assessment Program

Goals and Benefits

The McAfee Vulnerability Risk Assessment Program evaluates the level of risk posed by vulnerabilities and associated exploit code. Our team of global threat experts at McAfee Avert® Labs strives to inform customers about vulnerabilities and their possible consequences, so that they can take appropriate security measures to protect themselves against exploitation. Risk assessments are included in the vulnerability descriptions posted to the Vulnerability Library. The information is also available at our online ThreatCenter.

Executive Summary

The McAfee Vulnerability Risk Assessment Program evaluates the severity of weaknesses in your system or infrastructure that may open the door to potential attacks. Vulnerabilities can pose great risks for businesses and users' systems. Such attacks may violate the access, availability, or confidentiality of your systems, data, and applications. We have categorized Vulnerability Risk Assessment levels as Low, Medium, High, and Critical. These assessments are primarily based on how easy it is to exploit the vulnerability and the impact of the exploitation. The classifications are also based on the availability of exploit code and other parameters. These risk assessments are not subject to rigorous algorithmic measurement, so judgment calls are often made when assigning a risk level.

Criteria for Assessing the Vulnerability Risk

McAfee Avert® Labs considers the following criteria when evaluating vulnerability risk:

Origins of potential attacks

Vulnerabilities can be exploitable from outside your network (“remotely exploitable”), or they can only be exploitable from a local network or on a particular user's system (“locally exploitable”). A locally exploitable vulnerability can only be targeted by attackers within the network, while a remotely exploitable vulnerability can be targeted by insiders as well as by attackers outside the network.

Self-execution capabilities of attacks

Vulnerabilities can be exploited without any involvement by the victim, or they can only be exploited with the unwitting cooperation of the victim. In the latter, the victim is tricked into engaging in a certain activity, such as visiting a malicious website or opening a malicious media file.

Results of successful attacks

Vulnerabilities are exploited in order to execute code, elevate access privileges, obtain sensitive information, cause a denial of service of an application, service, or system, enable extortion, etc. In general, vulnerabilities that lead to code execution are the most dangerous, while vulnerabilities that result in a denial-of-service are far less dangerous. Denial-of-service attacks usually do not result in permanent damage.

In addition to the above criteria, we also take into account the availability of exploit code, the number of vulnerable systems or applications, and the configuration of the vulnerable software. The risk assessment will change over time, depending on the vulnerability life-cycle.

Vulnerability Risk Levels

Critical

- Applies to vulnerabilities that were originally rated "High" but are elevated when exploit code is published.

High

- Applies to remotely exploitable vulnerabilities that require no user interaction. When these vulnerabilities are successfully leveraged, the result is permanent compromise of the attacked systems.
- Applies to vulnerabilities that were originally rated "Medium" but are elevated when exploit code is published.

Medium

- Applies to remotely exploitable vulnerabilities that require no user interaction and that, when successfully leveraged, do not result in a permanent compromise of the attacked systems
- Applies to remotely exploitable vulnerabilities that require user interaction
- Applies to a locally exploitable vulnerabilities that, when successfully leveraged, result in a permanent compromise of the attacked systems.

Low

- Applies to locally exploitable vulnerabilities that, when successfully leveraged, do not result in a permanent compromise of the attacked systems
- Applies to vulnerabilities that were originally rated "Medium" and are present only in a non-default configuration or in a application with a limited distribution

Avert® Labs Malware Sample Submission Procedure

Methods of Submitting Samples to McAfee AVERT®

Please DO NOT submit samples to your TAM.

There are three (3) delivery methods approved to submit viral sample to AVERT® WebImmune:

1. Email: virus_research_platinum@avertlabs.com
2. The WebImmune Site: https://www.webimmune.net/faqs.asp
3. Standard mail: Address list below

Platinum E-mail Queue– This method is for Platinum customers only

When our automation systems receive a sample directed to this mailbox it will move the sample into the Platinum submission queue, which is a queue with higher priority than submissions from other areas. The Platinum queue is handled on a FCFS (first-come, first-served) basis so new submissions will be at the end of the Platinum queue, but ahead of all other customers. Once processed by automation, if the sample needs further review by a researcher it will again go in to a Platinum queue that is manually processed ahead of other customers.

Submitting samples to this system still requires that the samples be added to a password protected zip file using **"infected"** (no quotes) as the password. Failure to do this will lead to the samples not being processed.

You can send e-mails directly to the Avert® automated systems for review. If the automated system is unable to determine a threat exists then the issue will be escalated to an Avert® Research Analysts.

WebImmune Site – This is the preferred method to submit samples to Avert® as it provides the fastest turnaround time on sample reviews, and provides historical information of all samples that you have submitted. By accessing https://www.webimmune.net and creating a free account you will be able to upload files directly to the Avert® automated systems for analysis. If the automated system is unable to determine a threat exists, then the issue will be escalated to Avert® Research Analyst for analysis.

More information about WebImmune can be found at https://www.webimmune.net/faqs.asp.

Standard Mail – This is the least preferred method as submitting samples in this way will cause the longest turnaround time for review of your sample.

When submitting a sample through Webimmune, there are several questions that you are asked to fill out regarding your operating system, the Anti-Virus product you are using, and information about the file/s that you are submitting. Filling this information out as completely as possible will assist Avert® in processing your sample quickly.
With any sample that is submitted to Avert® via e-mail, it is best that you provide additional information on what symptoms you are seeing and basic information on your operating system. Providing the below information along with your sample will also help speed the sample review process:

- A list of all files contained in the sample submission, including a brief description of where or how the files were found
- What symptoms cause you to suspect that your machine is infected
- Whether any products find a virus (version number, company, virus name given)
- Your McAfee Antivirus Product information (Product, Engine and DAT versions)
- System details that may be relevant (Operating System, Service Packs)

- Your name, company name, phone number and email address if possible

You are strongly encouraged to notify your TAM of any virus samples submitted to Avert® Webimmune or the Virus Research Lab. Please have the submission analysis ID that Avert® provides ready.

*Please note, if you are sending a file/macro virus, compress your samples into a single file with a .ZIP extension and password-protect it with the password **"infected"**. If a sample is not protected in this way, AV Scanners may detect and clean samples before they reach us.*

Before submitting any samples to Avert®, it is important that you continue reading this page in order to understand everything that is needed when submitting a sample to Avert®.

Please DO NOT submit viral samples to your TAM

Maximizing The Chance Of Capturing The Possible Virus

When capturing a sample for Avert®, it is best that your machine is running in the apparently infected state. This means ensuring that the machine is started up as normal; not started up from a boot disk, in safe mode, or booted to a command prompt.

Capturing the Samples

Usually there is a file that you feel is suspicious and that is what you will want to submit to Avert®. However, there can be additional files associated with threats and you will want to try and capture as many of those as possible.

Before starting to capture files for submission, create a temporary folder on your system in which to store any files that you will be submitting to Avert®. Creating C:\avertsamples would be a good folder as the name explains what is in the folder, as well as making it easy to browse to when ready to package and submit the samples.

On Windows XP systems, click START – RUN, type MSCONFIG and hit ENTER
Click the Startup tab . If any files in the COMMAND field do not look familiar, copy those files to the temporary folder you created.
Non-Windows XP users:

- Run Regedit and go to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run and review the files associated with this key. If any files do not look familiar, copy them to the temporary folder you created.
- Run Regedit and go to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunServices and review the files associated with this key. If any files do not look familiar, copy them to the temporary folder you created.
- Run Regedit and go to HKEY_Current_User\Software\Microsoft\Windows\CurrentVersion\ Run and review the files associated with this key. If any files do not look familiar, copy them to the temporary folder you created.
- Open your Win.ini and system.ini files and review the Load= and Run= lines and copy any files associated with those lines to the temporary folder you created.

If you believe that you have a Macro virus:

Microsoft Word - Copy normal. dot and every file from the Microsoft Office Startup folder, normally located in Program Files\Microsoft Office\Office\Startup to the temporary folder you created.
Microsoft Excel - Copy all the files from the \XLSTART folder to the temporary folder you created.

Microsoft PowerPoint - Copy Blank Presentation.pot to the temporary folder you created.

Packaging the Samples for Delivery

Depending on the submission method that you are going to use, there are different ways to package the files:

Webimmune Submissions – With Webimmune, you have the ability to directly upload individual files to Avert®'s automated systems. When you logon to Webimmune you will see the Scan A File option on the right hand side of the screen. Clicking that link will take you to a page from which you can browse your system to upload the file.

If you have multiple files to submit to Webimmune you can add the files into a .ZIP file and submit that. When creating this .ZIP file, it is important to understand that the .ZIP can be no more than 3 megabytes in size and can contain no more than 30 files. Additionally, any .ZIP file created must be password-protected using the password "**infected**".

Failure to follow these guidelines will cause your submission to be rejected by the Avert® systems.

E-Mail Submission – when submitting samples via E-mail all samples must be packaged in a .ZIP file. When creating this .ZIP file, it is important to understand that the .ZIP can be no more than 3 megabytes in size and can contain no more than 30 files. Additionally, any .ZIP file created must be password-protected using the password infected. Failure to follow these guidelines will cause your submission to be rejected by the Avert® systems.

When submitting the sample via E-mail, send it to the global virus_research@avertlabs.com e-mail address. If you are submitting possible Adware or Spyware, submit the sample to spyware_research@avertlabs.com with the subject line "MAS Content".

Standard Mail Submission – Copy all the files from the temporary folder that you created onto a floppy diskette, or several if you have too many files to fit on a single floppy diskette. Additionally, if you have a Writeable CD, you can copy the samples to there as well. Diskettes or CD's sent to Avert® will not be returned.

What NOT to Send –

When using standard mail to send samples to Avert® only use floppy diskettes or CD's. Any other media (such as ZIP Drives, Hard Drives, and Full Computer Systems) will not be reviewed and will not be returned. Below are the mail addresses for the various Avert® sites that are authorized to receive standard mail submissions:

In the **US**: **McAfee Inc.** Virus Research 20460 NW Von Neumann Drive Suite 100 Beaverton, OR 97006	In **The Netherlands** : **McAfee Inc.** Virus Research Gatwickstraat 25 1043 GL Amsterdam Netherlands	In **Australia**: **McAfee Inc.** Virus Research Level 3, 40 Miller St North Sydney, NSW Australia 2060
In the **UK**: **McAfee Inc.** Virus Research Gatehouse Way Aylesbury, Bucks HP19 3XU UK	In **Germany**: **McAfee Inc.** Virus Research Sachsenfeld 2 20097 Hamburg Germany	In **Japan**: **McAfee Inc.** Virus Research Shibuya Mark City West 20F 1-12-1 Dougenzaka, Shibuya-ku Tokyo Japan 150-004 Japan 150-004