Contents

Introduction .................................................... 1
Identify the threat .............................................. 2
Identify the compromised computers .......... 3
Isolate the compromised computers .......... 3
Clean the compromised computers .......... 4
Post-op: Prevent reoccurrence .............. 6
Conclusion ..................................................... 9
Further reading .............................................. 9

Introduction

“The network is infected.”

It’s not the sort of statement you want to hear in regards to your network. Whether you’re a network admin planning a containment strategy or an executive assessing the damage done, you know that such situations cost time and money to resolve. Determining where to start can be equally as frustrating, especially when eradicating a threat can sometimes feel like a carnival game of Whack-A-Mole. Not all threats behave the same and some even update themselves, changing their behavior partway through a disinfection procedure. To make matters more complicated, you may hear references to “viruses” or “worms” and these will be used interchangeably with “threats”.¹

Fortunately there is an easier way to approach threat removal in large networks. Within Symantec we help people through these situations on a daily basis. With millions of hours of threat removal experience, we have been able to distil threat removal into a set of best practices that can be followed to simplify the removal process and help to prevent future infections.

The purpose of this guide is to describe the principles behind these best practices with as little technical and Internet Security industry terminology as possible. Since we understand that it may not be part of your daily responsibilities to carry out the actual removal procedures, this will hopefully make it easier for you to understand what needs to be

¹ For the sake of simplicity, we will use the term “threat”. This document explains the differences between these terms.
done by those in your organization whose job it is. This has therefore been compiled as a starting point for an understanding of what tackling an outbreak on your network and then shoring it up against future attacks would entail.

It is important to involve your IT Security, Incident Response or Operations Security team for the implementation details and specifics of the individual tasks that need to be performed. We will refer to this group as the “Security Team” in the rest of this document. It is for this group that certain specific technical details are included.

We will discuss a number of basic measures that have to be taken to clean up your network and to prevent or limit possible reoccurrence. The steps involved are:

1. Identify the threat
2. Identify the computers the threat has compromised
3. Isolate the compromised computers
4. Clean the compromised computers
5. Prevent reoccurrence

Since the purpose of this document is to give you a general overview, we have also included a references section at the end for more up to date and additional information.

**Identify the threat**

You may already have been made aware of a threat on computers in your network or on local computers. The next step is to identify it, what it could do, and assess the damage already caused by the threat. But amidst all the legitimate traffic on the network and myriad of corporate applications, how do you separate the good from the bad?

If you suspect that a computer has been compromised, the first thing to do is run an antivirus scan with the latest virus definitions (or signatures as they are sometimes called, because they contain the “fingerprints” of known threats). The vast majority of threats will be uncovered by doing so. While the scan results may not return the name of a particular threat, many of our enhanced detections are designed to capture and identify particular behaviors common to many threats.

If the scan results are negative and you still suspect that a threat is present, there are certain techniques available to look for potentially suspicious files on a computer. Checking the load points on the computer is one such technique. A load point is a location within an operating system where software is loaded when the computer starts up or when a particular program is run. For example, this is how your favorite Instant Messaging program always starts when you log on to your computer. Threats often use load points just as legitimate programs do, loading themselves into memory to perform their malicious actions, much like an Instant Messaging program would load.

Symantec has a tool available for Enterprise customers that can quickly scan a computer’s load points and generate a report that can be sent to your technical support agent. The agent can then analyze the report and determine for you if there is indeed a threat present. If you would prefer the designated Security Team in your organization to investigate the load points on a computer manually, there are a handful of locations to start out in. The video in figure 1 covers these load points.
Armed with this information, you are already a good way towards solving the issue. Gather any information you can about the threat from the Security Response Web site. Once the threat has been identified, it’s time to determine the breadth of the infection within the network by identifying all compromised computers.

**Identify the compromised computers**

After determining which threat is present on your network, the next step is to pinpoint which computers on the network are compromised. The simplest way to do this is to have your Security Team update the antivirus software on all of the computers in the network with the latest virus definitions and run a complete virus scan. Our current antivirus products allow this to be done from a single management console. When the scan completes, a review of the scan results and any threat logs will provide information to begin a tally of the computers compromised.

It may also be necessary to perform a network audit in order to determine if any computers do not have antivirus installed or if the definitions are not updating successfully. A computer with malfunctioning or missing antivirus software could very well be compromised and an audit should help to determine their location. Add any such computers to your tally in order to determine that they are clean or compromised by the threat.

Your Security Team may also have access to another good source of information, such as firewall logs. Firewalls are control mechanisms that regulate and log your computers’ access to the outside world, such as the Internet, or other internal computer networks in your organization. These logs could reveal any computers that are generating a lot of network traffic when they shouldn’t be. Certain threats attempt to connect to other computers in the network and any such attempts or unexpected connections may be logged in the firewall logs.

Now that you’ve identified the compromised computers, it’s time to isolate and clean them.

**Isolate the compromised computers**

Once the compromised computers have been identified, it is important that, whenever possible, they are taken off the network while being cleaned. One of the main classes of threats—worms—spread by using various techniques to “hop” from one computer to another through the network. In this sense, an often-used term for threats—viruses—can be more illustrative. 2 As a biological virus spreads from one host to another using a variety of vectors of infection, such as sneezing or mosquito bites, so too does a computer worm spread from one computer to another over the network. This is why it is so critical to remove a computer from the network once you discover it has been compromised—it is highly likely that the threat in question could infect another computer as you attempt to remove the threat from the computer.

---

2 It is worth noting that, while often used colloquially to describe malicious code, a “virus” is not the same thing as a “threat”. A threat is an industry-wide term used to describe all malicious code. In contrast a virus is a subclass of threats that spread by attaching themselves to files, in much the same way a biological virus attaches itself to the cells of its host.
Sometimes a compromised computer is mission-critical and cannot be isolated from the network. In some cases, depending on the infection, these can be isolated in so-called quarantine networks with some heavily restricted network access. Naturally this only works for cases where the threat’s activity doesn’t coincide with the necessary functions needed by the compromised computer.

It would be up to your Security Team to verify if the necessary preparations and infrastructure are in place to facilitate this. It should also only be done once all of the ways the threat spreads are known, documented, and steps needed to prevent further spreading are put into place. Still, this method provides some limited productivity during the cleaning up or disinfection process.

It is also a good idea to perform another network scan once all compromised computers have been removed from the network. This eliminates the possibility that the threat could have compromised another computer while identified computers were being taken off the network. If the scan comes back without any results, it is time to move to the next step—cleaning the computers.

Clean the compromised computers

We are now at the point where the threat will be eradicated from the compromised computers. With the threat isolated to individual computers the threat can be removed and the changes it made can be restored.

The following steps contain detailed information that should be taken by your Security Team to:

- Assess if it would be more cost-effective to “start from scratch”— i.e. to freshly rebuild or reinstall a compromised computer.
- Assess if any threats found can be easily removed from a computer by running an antivirus scan, or if some additional tasks have to be performed before or afterwards.
- Assess if any system changes were made on infected computers and how to revert those changes.
- Assess when it is safe to add the computers back to the network.

Back doors or rootkits

Before proceeding with a disinfection of a compromised computer, it is important to consider your options if a back door or a rootkit is present. These malicious code subclasses allow threat writers to gain undetected access and hide their malicious files, respectively. In both these cases determining the extent of the damage done to a computer is harder, and they increase the difficulty of removing all malicious functions from the computer. Under such circumstances it is often less time consuming to start from scratch by reimaging the operating system and restoring needed data from clean backups.

Stop the viral process

In order to remove the malicious files from the computer, any processes used by the threat must be stopped beforehand. There are three primary options for doing this.

Antivirus scan

This is perhaps the easiest option. If you have Symantec AntiVirus 10 or Symantec Endpoint Protection installed on the computer, it should be able to stop any malicious processes while it scans the computer.

End the task

In some cases you can open the Task Manager and end the malicious process. Note that some threats may prevent you from doing this, in which case you will need to try one of the other options.

Safe Mode

Restarting the computer in Safe Mode will prevent the vast majority of threats from loading as the operating system loads. You can then proceed with manually removing the malicious files or running an antivirus scan. When you are finished removing the threat, ensure that you restart the computer back into Normal mode.
Remove the malicious files

The simplest way to remove the threat from the computer is to run a full system scan of the compromised computer. With the latest definitions installed the scan should be able to remove the threat in most cases without incident.

In some cases there may also be the option to use a Symantec removal tool, if one is available for the threat in question. Check here for a current list of removal tools.

Finally, you can attempt to remove the files manually. Navigate to the location the threat dropped them and delete the files in question. This can be time consuming, though it can work if you know the names and locations of all the files created by the threat. However, we don’t necessarily recommend it. The complexity of many of today’s threats leaves many chances for something to be overlooked when attempting a manual removal.

Restore changes made by the threat

There are often a number of changes that a threat makes to a computer beyond just dropping files. Quite often security settings are lowered by the threat and system functionality reduced based on changes to the computer’s configuration. In many cases your Symantec antivirus program can restore these items to a predetermined, secure setting. You can then adjust these settings further to suit the needs of your network. There are cases where you may need to manually confirm or restore various system settings after removing a threat.

Registry changes

More often than not, threats create or modify registry subkeys or entries on a computer, which provide functionality ranging from starting up when Windows starts to granting themselves Internet access through the Windows Firewall.

Leaving these items unchanged after the threat has been removed can cause error messages to appear while starting or using the computer. In some cases, it may prevent the user from logging in when the computer is restarted.

Any items added to the registry should be removed. Any changes made to existing registry items should be fixed as well, either by setting them back to their previous settings or to more secure settings.

System files

There are a number of system files used by the operating system that threats like to take advantage of. The following items should be checked for signs of modification when a computer is cleaned.

hosts file

This file is used to store certain Internet locations locally, as opposed to querying a DNS server. Threats sometimes modify this file in order to redirect a user to a malicious Web page or away from security sites, such as www.symantec.com. If you find that there are entries in the hosts file that may have been added by the threat, comment them out. If network functionality is not impacted, these items are likely unnecessary, and you may be able to remove them entirely, if you so wish.

win.ini file

This file, while still functional in the latest versions of Windows, is really a throw-back to the Windows 3.11 days. Its purpose is to store basic system settings during startup. Over time its use has been phased out in favor of the registry, but it is still available, maintaining backwards-compatibility with old programs, even in Vista.

Threats sometimes find the startup functionality of the win.ini file to be useful for their malicious processes. Check the win.ini file for suspicious entries, and investigate any found. If you believe they are related to the threat, comment out, test, and then remove the entries.
System File Checker
There is a utility within Windows called the System File Checker that protects critical system files. Some threats attempt to modify portions of this utility, particularly the sfc.dll file, in order to grant their malicious files wider access and functionality on the compromised computer. If the sfc.dll file, or any other system file, is compromised it should be restored. The most reliable way to do this is to use the original installation media, boot to Recovery Mode, and replace the file.

Antivirus software
Some threats specifically target the antivirus software installed on the computer. If successful, this can lead to the antivirus software not alerting on the threat or not being able to update its definitions. If this has happened to a compromised computer, you will want to check if the software needs to be reinstalled.

Reintroducing computers to the network
Once a computer has been successfully cleaned, one last safety check is recommended—run a final antivirus scan with the latest definitions. If the scan comes back clean, you should be able to reintroduce the computer to the network without fear of it further compromising other computers.

Post-op: Prevent reoccurrence
Even though the threat is removed from your network at this stage, the most important step is yet to come. The Security Team should take a network audit to determine how the threat got into the network and then put security measures in place to prevent it from happening again.

The following are common weak-points in networks that often lead to threats appearing within them. Not all of these will apply in a given situation, but addressing all of them is very important in order to protect your network.

It is also important to realize that some of the weak-points are actually technologies that make working with computers so much easier these days. The sad fact is that security and ease-of-use are, in many ways, inversely proportional. An increase in security can increase steps needed to perform a task. However, ease-of-use, while more efficient, often opens security holes that make it very easy for threats to spread.

The following sections contain detailed information on security weak-points—common ways through which threats spread—and provides suggestions on how to shore up these weak-points.

Patching
Vulnerabilities are computer software flaws that can be exploited by malicious code. These vulnerabilities can be repaired by applying “patches” provided by the software developer. In today’s network environment, regular patching is a must. Every network should have a Patch and Configuration Management Policy for testing new patches and then rolling them out to client computers. But patching plans should apply to much more than just client operating systems, such as Windows. Any software installed on a computer should be regularly checked for updates—from office utilities to databases to Web-server applications—all software should be cataloged and regularly checked for updates. Internally developed code should be regularly audited for security holes and fixed as soon as possible. Appliances, such as routers and printers, should also be checked for software updates and patched quickly. This can be a lot to manage, but vitally important in preventing outbreaks.

AutoPlay
Since being introduced near the turn of the century, USB flash drives have become a preferred method for transferring large files between end users. USB and IEEE1394 (a.k.a. Firewire) hard drives have also grown in popularity, given their ease of scalability, as opposed to installing a new internal hard drive. These removable drives have become such useful tools that it is hard to imagine performing some tasks without them.
However, with the added convenience come added security concerns. A feature in Windows called AutoPlay allows for the easy execution of files on removable drives when they are plugged into a computer. This is done when an .inf file that contains execution instructions resides on a removable device. AutoPlay carries out the instructions in the file when loading the drive. Unfortunately, many threats also take advantage of this functionality as well. The video in figure 3 describes this situation in detail.

In order to protect your network, disabling AutoPlay is the recommended course of action. This can be done on individual computers, pushed out to client computers using the Group Policy editor, or if you would like to prevent the use of removable drives entirely, you can disable the external media ports on the computer entirely from within the BIOS.

AutoPlay also works with mapped network drives. In order to protect against threats that use AutoPlay functionality to spread, it should be disabled on these types of drives as well.

**Network shares**

As is the case with removable drives, network shares also facilitate easy transfer of files. Yet they also allow threats to spread, if not well protected. First and foremost, access to all network shares should require a strong password, not easily guessed or “cracked”\(^3\). Not only does this limit the access by potential threats, it also safeguards against sensitive information being viewed by unintended users.

Write and execute privileges on network shares should also be restricted. If a user only needs to obtain files from a source, they should only be granted read access. For added security, write access for users needing file-transfer capabilities can be limited to a “temporary” storage folder on a file server, which is cleared semi-regularly. In terms of execution permissions, limit this access to administrators or power users who have such need.

Disabling or limiting access to two other share-types is also recommended. Admin$ shares allow complete root access on a computer to any user that can authenticate as a member of the administrator group. Inter-Process Communication (IPC) shares, or IPC$, are intended to help communication between network-available processes and other computers on the network.

The problem with those two shares is that regardless of whether or not strong passwords are in place, the fact that once a user is logged on to a system with elevated rights any threat present could use those credentials to access Admin$ or IPC$ shares available on the network. The principle here is once you’re logged on, your rights and permissions are implicit. So no matter how strong your password policy is, once you are logged on you have unlocked the door so to speak. Anything you have access to will be accessible to anything that impersonates you.

\(^3\) Please refer to the Further reading section for further information on creating strong passwords.
So, the best practices in this regard are three-fold:

- Do not log on using an account with elevated privileges (such as the domain or local Admin) unless absolutely necessary to perform a certain task.
- Be sure to log off once the task is completed.
- For most day to day duties, use a more restrictive account.

It should be noted that the above does not negate the necessity for strong passwords, because many threats will try to gain access by guessing the password from an extensive list of commonly used passwords.

**Email**

Email attachments, while perhaps not as prevalent as in years past, are still used to spread malicious code today. Most email servers currently on the market provide the ability to strip certain attachment types from emails. Limiting the types of files that are valid as attachments handicaps many threat’s ability to spread.

Investing in antispam software is another way of reducing exposure to threats. Doing so reduces the number of phishing scams and spam that reach end users, and thus the network as a whole.

**Limit permissions**

Today, when users in a large network are given full administration rights on their client computers, it’s rarely a question of if an outbreak occurs—rather it’s when. On the other side, the default Limited user available in Windows often doesn’t meet the needs of users.

But it doesn’t have to be an all or nothing situation—there are plenty of options available for providing varying degrees of access. The Local Users and Groups snap-in, available in the Microsoft Computer Management console, offers many more options. The Group Policy editor also offers a variety of controls for programs built into the operating system. With these options, it is entirely possible to provide adequate functionality, while still protecting the computer and network from accidental infection.

**Education**

An educated end user is a safer end user. Ensure that your users understand the basics of safe computing, such as the following:

- Do not give your password to anyone or store it in an easily accessible location, physical or electronic.
- Do not open unexpected email attachments from known or unknown sources.
- Do not click on unknown URLs.
- Scan software downloaded from the Internet before installing it.

Having documentation, internal training, or periodic seminars on computer security available gives your users options for learning more about the topic.

**Firewalls and other tools**

Perimeter firewalls are critical to protect the network as a whole, but cannot cover all points of entry. Client firewalls add an extra layer of security by protecting individual computers from malicious behavior, such as Denial of Service attacks.

Beyond basic firewalls, network and host-based Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS) can help monitor unwanted activity on the network, and in many cases allow you to stop the offending traffic in real-time. Many client-side firewalls today provide these features.

A semi-regular penetration test is also recommended in order to evaluate the security of your network. Running such tests can give you a good idea of the weak points in your network and allow you to plan out steps to close these holes.
**Emergency response plan**

Even after all these tasks are complete, it is still a good idea to be prepared in case of the worst. Draft a plan for how you will respond to a potential outbreak. How quickly will you know if there's something on the network? Will there be administrators available to deal with it? How easy is it to reroute traffic and services on your network? Can you quickly isolate compromised computers before they affect other computers? Having plans in place for these things makes dealing with unpleasant situations much easier.

**Conclusion**

While removing a threat and locking down a network is time consuming and often costly, there is good news in all of this. These days we rarely see new methods of propagation or infection with breaking threats. The vast majority of threats out there in the real world today use time-tested methods for spreading their malicious code. They work solely because many organizations leave such security holes in their network. Following sound security policies and practices drastically reduces the chances of an outbreak within a network. While it’s hard work at the beginning, it is worth it in the long run. Due diligence and sound monitoring from a security standpoint will likely free up IT resources and budget spent on cleanup for other, more enjoyable projects.

**Further reading**

- Security Response Web site
- Symantec Support Services
- Introductory information on viruses, worms, and other threats
- Security Response glossary
- Tips for creating strong passwords
- Internet Security Threat Report
- Other research papers written by Security Response
About Symantec
Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

About the authors
Ben Nahorney is a Senior Information Developer in Symantec Security Response. Eric Maengkom is a Senior Principal Product Support Engineer within Symantec’s Support organization.

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.