

# Managing Malware

## How to Limit the Impact of Malware

- Malware is a major threat to data security for many campuses. While the impact of malware is not limited to data compromise, this document will primarily focus on steps you can take to protect your data from malware.
- There are at least two schools of thought on how to do this. If you have the ability to dictate clear rules regarding what your end user community can do you can implement items from [List 1](#).
- If you have a more open environment where centralized IT management is not the norm, implement items from [List 2](#).
- If you only have very limited resources, implement items from [List 3](#) as a starting point. Some of these items do overlap.
- Please note that while individual list entries are numbered, these are not necessarily numbered in priority order. Numbering is provided for ease of reference.
- Finally, consider that depending on your environment, established change windows, organizational culture, and/or other circumstances, "as soon as practicable" will vary.

List 1: For environments managed by an IT Professional (e.g., staff with IT support as a primary or sole duty for an entire campus, college, department or business unit)

1. Where practicable, do not grant administrative or root/superuser privileges to end-users.
  - a. Commonly called [LUA](#) (least user access)
2. Know where your data are.
  - a. The tools listed below can help you locate sensitive data on your systems:
    - i. [Identity Finder](#), [Spider](#), [SENF](#), [Find\\_SSNS](#)
  - b. Securely erase data if it is no longer needed.
    - i. [Information from the Electronic Frontier Foundation](#), [DBAN](#)
  - c. Concentrate security resources on systems containing sensitive data.
3. Microsoft Windows continues to be a major target - focus your efforts here first. Having said that, ensure the rest of your technology environment is also well managed.
  - a. Install important security updates on all affected systems (Microsoft Windows, Apple Mac OS, Linux, Unix, etc.) as soon as practicable.
    - i. The following tools can help you deploy updates: [Secunia\( .edu specific information\)](#), [Bigfix](#), [WSUS](#), [Shavlik](#), [VT WSUS](#)
  - b. Harden passwords to prevent password guessing worms from infecting your system via File Sharing, RDP, etc
    - i. [ADpasswordfilter](#)
  - c. Watch systems for new unexplained listening network ports
    - i. [Portinator](#)
  - d. Follow established best-practices for securing mission-critical systems or systems that store, process or transmit sensitive information.
    - i. [Information Security Guide](#)
4. Regularly participate in security training and awareness events.
  - a. For IT staff:
    - i. [SANS Institute](#)
    - ii. [SANS Partnership Series](#) (discounts for higher-ed)
    - iii. [Security Professionals Conference](#)
  - b. For everyone else:
    - i. [EDUCAUSE Cybersecurity Awareness Resource Library](#)
5. Install and appropriately maintain end-point defenses.
  - a. Use centrally managed anti-virus and anti-spyware software where appropriate.
    - i. [Microsoft System Center 2012 Endpoint Protection](#)
  - b. Enable and appropriately configure host-based firewalls where practicable. This is particularly important for out-bound traffic.
    - i. Enable Windows advanced firewall and push In/Out rules via group policy (if possible) for consistent application: [link](#)
  - c. Install host-based intrusion prevention software where practicable.
    - i. [eEye Blink](#), [Mcafee Host Intrusion Prevention for Desktop](#), [Symantec Critical System Protection](#), [Checkpoint Endpoint Security](#), [Cisco Security Agent](#)
  - d. Where feasible, make available protection software licensed for home use.
6. Use an intrusion detection/prevention system where practicable.
  - a. [Snort](#), [Bro](#), [Fireeye](#), [eEye](#), [Tippingpoint](#)
7. Use DNS based protection where practicable.
  - a. [Sink-holes](#), [OpenDNS](#), guidance from the [MAAWG](#), [host file](#)
8. Use web filtering software, services or appliances where practicable.
  - a. [Websense](#), [Squid](#), [Microsoft Forefront Threat Management Gateway](#)
9. Implement application white-listing where practicable.
  - a. [Bit9](#), [CoreTrace](#), [Savant](#), [Windows 7 built-in AppLocker](#)
10. Know where you are vulnerable.
  - a. [Nessus](#), [Nmap](#), [Metasploit](#), [Core](#), [Canvas](#), [Rapid7](#), [SafetyNet](#)
  - b. Review status reports from available patch-management systems.
11. Gather vulnerability and threat information from online sources.
  - a. For vulnerabilities in software
    - i. [Secunia](#), [National Vulnerability Database](#), [SANS Top Cyber Security Risks](#)
  - b. For current threats
    - i. [SANS Internet Storm Center](#), [F-Secure](#), [Web Sense Security Labs](#), [FireEye](#), [M86 Security Labs](#), [Malware Intelligence](#), [Arbor Networks](#), [Microsoft Security Response Center](#)
12. Monitor available logs and network activity for indicators of malicious software.
  - a. Regularly check anti-virus logs.
  - b. Regularly check DNS traffic for queries to known malware hosting domains.
  - c. Subscribe to [Shadowserver notifications](#) for networks you manage.
  - d. Centralize event log management and apply appropriate logic to identify out-of-spec results
    - i. [Microsoft System Center Operations Manager](#)

13. Have a back-up strategy for your endpoints.
  - a. Ensure backup stream is encrypted over the wire.
14. Make sure people can report problems to you.
  - a. Are all your points of contact in [whois](#) current (e.g., for your domain, and for your IP blocks, and for your [ASN](#))?
  - b. Do you have [RFC2142](#) standard abuse reporting addresses?
  - c. If someone checks for your domain at [www.abuse.net](#), will they find reasonable abuse reporting contacts listed?
15. Know where to get help.
  - a. Online malicious software analysis tools
    - i. [ThreatExpert](#), [Anubis](#), [CWSandbox](#), [JoeBox](#)
  - b. Your local network team.
  - c. Your local desktop support and/or server support team.
  - d. [Report](#) domain names with bad whois information.
  - e. Sign up for Google's hostmaster tools to scan your sites and report malware infections: [link](#)
  - f. [REN-ISAC](#)
  - g. [US-CERT](#)
  - h. [EDUCAUSE](#)
16. Share your knowledge.
  - a. Submit new malware samples to your anti-virus vendor. Doing so may result in early/beta signature files to help with current problems.
    - i. Learn what the submission process is for your vendor as soon as possible so you don't waste precious time during a crisis figuring out who to talk to and how to submit your sample.
  - b. Submit new malware samples to [VirusTotal](#).
  - c. Participate in the [REN-ISAC](#).
  - d. Participate in [EDUCAUSE](#).
  - e. Participate in [DSHIELD](#)
17. Ensure your incident management/response process is current.
  - a. The following guidance is available from the Internet2 Computer Security Incidents working group: [Security Incident Management Essentials](#)

#Top of page

List 2: For personally managed environments (e.g., IT support is a secondary duty or not specifically assigned to anyone in particular)

1. Do not use an account with administrator or root/superuser privileges for day-to-day activities such as surfing the web or checking e-mail. Only use a privileged account when necessary.
2. Know where your data are.
  - a. If you are not storing sensitive university data on your computer, such as personally identifiable information other than your own, you greatly reduce the scope and potential of harm in the event of malware compromise. The tools listed below can help you locate sensitive data on your computer:
    - i. [Identity Finder](#), [Spider](#), [SENF](#), [Find\\_SSNs](#)
  - b. Securely erase data if it is no longer needed.
    - i. [Information from the Electronic Frontier Foundation](#)
3. Windows:
  - a. Make sure Windows Update is enabled and set to at least notify you whenever updates are available. Additionally, tools like [FileHippo.com Update Checker](#) and [Secunia OSI](#) can help you stay up to date on individual Windows computers.
4. Mac OS X:
  - a. Use the built-in [Software Update](#) feature. Additionally, you might also be interested in tools like [Appfresh](#), [MacUpdate Desktop](#) and [Versio ntracker](#) to help with third-party application updates.
5. Install and appropriately maintain end-point defenses.
  - a. Use anti-virus and anti-spyware software where appropriate.
  - b. Enable and appropriately configure host-based firewalls where practicable. This is particularly important for out-bound traffic.
  - c. Use a security-focused DNS [host file](#).
6. Deploy network-based defenses.
  - a. Use DNS based protection where practicable.
    - i. [OpenDNS](#)
7. Know where you are vulnerable.
  - a. [Nessus](#), [Nmap](#), [Metasploit](#)
8. Gather vulnerability and threat information from online sources.
  - a. For vulnerabilities in software
    - i. [Secunia](#), [National Vulnerability Database](#), [SANS Top Cyber Security Risks](#)
  - b. For current threats
    - i. [SANS Internet Storm Center](#), [F-Secure](#), [Web Sense Security Labs](#), [FireEye](#), [M86 Security Labs](#), [Malware Intelligence](#), [Arbor Networks](#), [Microsoft Security Response Center](#)
9. Have a back-up strategy for your endpoints.
  - a. If centralized backups are not available, potential options include:
    - i. Off-site/"In the cloud": [Mozy](#), [Jungledisk](#), [Carbonite](#), [Windows Live Skydrive](#), [Dropbox](#), [Syncplicity](#), [Sugarsync](#), [Apple MobileMe](#)
    - ii. Local: [Apple Time Machine](#), [Microsoft Windows 7 Backup and Restore](#)
10. Know where to get help.
  - a. Online malicious software analysis tools
    - i. [ThreatExpert](#), [Anubis](#), [CWSandbox](#), [JoeBox](#)
  - b. Other local IT support professionals.
  - c. Your central IT support staff.
  - d. Your central IT Security team.
  - e. [Report](#) domain names with bad whois information.
  - f. [REN-ISAC](#)
  - g. [US-CERT](#)
  - h. [EDUCAUSE](#)

[#Top of page](#)

List 3: Operating on very limited resources (e.g., smaller schools where dedicated IT professionals are relatively rare or environments with only one or two dedicated security staff)

1. As best as you can, determine which computers contain the largest repositories of sensitive data on your campus. Doing so will help you focus your limited security resources on protecting IT assets with the biggest potential for data compromise.
  - a. The tools listed below can help you locate sensitive data on your systems:
    - i. [Identity Finder](#), [Spider](#), [SENF](#), [Find\\_SSNs](#)
  - b. Securely erase data if it is no longer needed.
    - i. [Information from the Electronic Frontier Foundation](#)
2. Implement network based protection that will cover as many users and IT assets as possible.
  - a. Use DNS based protection where practicable.
    - i. [Sink-holes](#), [OpenDNS](#), guidance from the [Messaging Anti-Abuse Working Group](#)
  - b. Use web filtering software, services or appliances where practicable.
    - i. [Websense](#), [Squid](#)
3. If you have not already done so, develop your incident management/response process.
  - a. The following guidance is available from the Internet2 Computer Security Incidents working group: [Security Incident Management Essentials](#)

[#Top of page](#)

---

[?](#) Questions or comments? [i](#) [Contact us](#).

 Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License ([CC BY-NC-SA 4.0](#)).