

Virus infection (or other malware)

I have a problem with virus infection (or other malware); what should I do?

Introduction

Viruses and other malicious software (“malware”) are an ever-present threat to any organisation with computers. In the past viruses were a significant nuisance, but not much more. Today they are a threat to the security and even the survival of the organisations they affect.

Ideally any organisation should have some kind of incident response plan to deal with large scale malware infection but most, we find, do not. We have prepared the following brief document for IT personnel or other managers who are faced with a malware problem or are thinking of preparing a plan for dealing with malware infections. This document is not a complete incident response plan. We hope, however, that it will provide a useful guide to the key issues in dealing with a large scale malware infection, and may help anyone faced suddenly with dealing with such an event. We think it deals with most of the main issues facing organisation experiencing malware problems.

Grant Thornton has extensive experience helping organisations deal with crises such as these. We have helped many others prepare detailed incident response plans to allow them to quickly react to, control and end incidents that threaten to disrupt or damage their organisations. If you need more advice, or would like to talk to us about our services we would be delighted for you to contact us.

What is “malware”?

“Malware”, is maliciously developed software, designed to alter the operation of a computer, usually to the user’s disadvantage. It is usually transmitted and installed without the user’s knowledge or consent. It comes in a number of forms, the best known and longest standing being “Virus” or “Worm” programs.

The more common varieties of malware include:

Adware: Adware is software that causes advertising to pop-up on the users screen. Typically the presence of adware on a computer constitutes little more than a nuisance, only becoming a problem when multiple instances of the software, running simultaneously, slow it down.

Spyware: Spyware is malicious software that collects information about the computer's user without their informed consent. Although much is relatively harmless, the most damaging spyware software can collect personal information stored on a user's computer, monitor and record users typing and pass this information to third parties. Spyware software can be installed with software or when users visit certain websites. Typically the software is installed either without the user's knowledge or through deception.

Viruses and Worms: These two terms are often used interchangeably, although in strict terms they differ. By definition, viruses are spread unintentionally by user action, while worms spread without user intervention. Most computers now have anti-virus software installed. It should be considered, however, that such software is not infallible. It is only as good as the last update, and even then the best packages can only be expected to detect a third of known viruses. Virus infection remains, therefore, an occupational hazard for any organisation with a computer network.

Effects

Some viruses continuously download new versions of themselves to keep ahead of anti-virus software. Others are "polymorphic" and change their internal structures to evade detection and deletion. Other functionality can include:

Typical malware functions

- antivirus software deactivation;
- search routines for passwords, certificates, financial details or other sensitive information for the purposes of fraud;
- installation of keypress-logging software or other eavesdropping software;
- installation of "backdoor" or "trojan horse" software (which may allow the virus writer to gain complete control to the infected computer);
- software allowing distribution and/or warehousing of illegal material;
- remote control (or "bot") software which can allow the virus writer to use the computer for distributing spam or carrying out denial of service attacks; and
- "dialler" payloads which can repeatedly make the computer's modem dial premium-rate telephone services).

Malware telltales

Not every antivirus package will identify every virus, so how do you know if you have been infected? The following are often clues.

Malware indicators

- anti-virus/anti malware alerts on multiple computers (obviously);
- unexplained system crashes;
- unexplained, poor system performance;
- antivirus software disabled on multiple hosts;
- changes in file characteristics or dates;
- a sudden increase in the amount of data passing through the network;
- new files in system directories;
- large numbers of "bounced" e-mails arriving at a mail gateway; and
- inexplicable system behaviour that cannot be diagnosed.

Basic incident response

Priorities

Your priorities in dealing with viruses and other malware infections should be

- to prevent the virus spreading to other computers or subnets;
- to prevent the theft or destruction of data;
- to remove the malware from all systems; and
- to identify the origin of the malicious software.

It is not always necessary to carry out a full incident response for every virus infection. Minor virus infections affecting a handful of computers are relatively commonplace and can probably be treated as a routine maintenance issue.

Other issues you need to consider

Documentation: As with any incident, the first responder should document all significant events, observations and actions taken from when the incident is first detected. If these are not recorded immediately it is very likely that key details will be missed which may delay or reduce the effectiveness of later remedial actions.

Reporting: Managers and key affected stakeholders should be advised of the event:

Considering advising?

- General Management;
- IT Management;
- Business/Operation Unit Management;
- Legal;
- HR/Industrial Relations;
- Public Relations; and
- Internal Audit/Fraud Control.

Specific considerations with malware infections

Malware infections raise a number of unique issues which must be considered and dealt with during any effective incident response process. We think it is worth paying attention to the following:

Identification

- containment of the virus is usually more important than identifying its source. Any affected computers and subnets should be isolated from the main network.
- you start this by identifying the infected machines by means of malware databases, anti-virus software or forensic analysis. This should allow you to identify the type of malware, and its likely functionality.
- not every antivirus package picks up every virus. You might consider buying another brand of anti-virus software to see if it finds an infection your normal package may have missed.
- if you have been specifically targeted by "custom" virus software (it happens - particularly to larger organisations), you may need help from a forensics investigator. Grant Thornton have the most experienced IT forensics investigators of any professional service firm in the country.

Eradication

- the network should be swept for presence of malware programs. You should carefully record each computer infected.
- it is also useful if, before removing the virus, you can identify the creation date and time of the virus program. Your anti-virus provider will usually have an on-line database that will tell you the name and likely storage locations of any such program. The computer containing the virus program with the earliest creation date is likely to be the first infected.
- eradication should ideally be carried out by wiping and reinstalling all infected computers (some malware can embed in operating systems so completely that they cannot be removed).
- where wiping computers is not an option, viruses can be removed using anti-virus software where possible. If the malware is of a previously unknown type, investigation by IT forensics specialists will reveal the majority of executables and registry changes. These can be removed using scripts.
- any computer which has been cleaned in this manner should be monitored to ensure no further reoccurrence.

Damage assessment

- you need to assess the likely extent of any damage or data compromise caused by the virus. You can base the assessment on the known characteristics of the virus and the contents of any affected computers.
- remediation should be carried out by updating the antivirus software on all computers.

Identification of origin

- forensic analysis may be carried out on the first infected computer to determine if infection was accidental, culpable or deliberate.

Remediation and reporting

Remediation

Remediation involves putting measures in place to ensure, as far as possible, similar incidents do not reoccur. In the case of virus and other malware infections we suggest the following precautions, if they are not already in place:

Remediation actions

- develop a full incident response plan for future malware infections, based on lessons learned from the incident just finished. Grant Thornton can help you develop an effective plan;
- anti-virus software should be updated daily;
- memory-resident malware-detecting software must be loaded at all times on every computer and a full virus scan must be performed at regular intervals on all machines. Note that memory resident scanners can sometimes identify viruses "on the move" after disk scanners have missed them;
- the antivirus software should be set up so that users cannot turn it off;
- prohibit the use unauthorised software on your computer systems;
- keep your computers and other systems up to date with application and operating system patches.
- introduce a policy of "least-privilege" across your network. If possible, applications should be set-up to run without high level privileges. These precautions will lessen most viruses' ability to cause damage or spread;
- any files or software obtained from outside your organisation must be swept for malware before being used on any of your computers;
- some files, particularly program files, should be blocked at the mail gateways;
- some modern viruses transmit themselves over USB devices, so these need to be tightly controlled. Only devices owned by your company should be allowed to be connected to your computer systems; and
- access to other networks (including the Internet) should only be allowed through computers or gateways you control. The use of tunnelling or anonymous proxies should be strictly prohibited.

Reporting

It is often necessary to prepare a formal report on any incident for senior managers, regulators or other stakeholders. In writing the report on the incident it is probably worthwhile considering the following issues:

Possible report content

- the source of the infection (if determined);
- contributory factors to the incident;
- timeline of incident response activities;
- actions taken to recover from the incident;
- assessment of any damages incurred, data lost;
- further remedial actions required; and
- other relevant information.

If you need more advice

Our incident response and computer forensics specialists have helped hundreds of organisations deal with incidents quickly and effectively, helping them resolve their problems with the minimum of loss, disruption or distress.

If you would like to talk to us about computer forensics, incident response planning or any other issue, please feel free to give us a call at the numbers below.

Contact

Paul Jacobs
Partner, Forensic & Investigation Services
D +353 (0)1 6805 835
E paul.jacobs@grantthornton.ie

Andrew Harbison
Director, IT Forensics & Investigation Services
D +353 (0)1 6805 766
M +353 (0)86 040 7211
E andrew.harbison@grantthornton.ie

24-26 City Quay, Dublin 2

Offices also in Limerick and Kildare

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialist advice should always be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing. Grant Thornton is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.