UNIVERSITY OF PORTSMOUTH

IS ADVISORY ON MALICIOUS SOFTWARE

March 2016

Contents

Document title		
Normal text		
Document author and department		
Normal text		
Approving body		
Normal text		
Date of approval		
Normal text		
Review date		
Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? Tick as appropriate		**YES**
For public access on request copy to be mailed Tick as appropriate	**NO**	**YES**
OR For staff access only (intranet)? Tick as appropriate		**YES**
Password protected Tick as appropriate	**NO**	**YES**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk		

If you need this document in an alternative format, please email corporate.communications@port.ac.uk

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents/qA43279

Summary

What is this document about?

This advisory provides information about the main types of malicious software affecting IT systems, how they can be recognised and what should be done to defend against them. Malware is a broad term that refers to a variety of malicious software programs. As well as gathering personal information about you, your browsing habits, your financial details etc., and sending that information elsewhere, malware can also slow your system down by hogging system resources and network bandwidth. Some spyware and adware can even open up your system to cyber-attack.

The University network is protected by Sophos EndPoint Security. This offers on-demand scanning of suspicious files and on-access scanning when malicious threats activate.

Who is this for?

This IS Advisory is aimed at all staff and students of the University of Portsmouth

How does the University check this is followed?

Annual review of this IS Advisory will be performed to keep it up to date with new information on threats and how to handle them.

Who can you contact if you have any queries about this document?

Any questions about this advisory should be directed to servicedesk@port.ac.uk

1. How do I know if I'm infected?

Malicious software will tend hide in the background while your computer is switched on. Spyware - by definition - will not want to advertise its presence. On the on the hand, adware may create pop-up ads and banners or it may install a 'toolbar 'on your browser which hijacks your internet browsing.

1.1 Typical symptoms of a malware infection

While these types of malware differ greatly in how they spread and infect computers, they all can produce similar symptoms. Computers that are infected with malware can exhibit any of the following symptoms:

A. Unexplained increased CPU usage
B. Slow web browser speeds
C. Problems connecting to networks
D. Freezing or crashing
E. Modified or deleted files
F. Appearance of strange files, programs, or desktop icons
G. Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs)
H. Emails/messages being sent automatically and without user's knowledge (a friend receives a strange email from you that you did not send)

1.2 How did I get 'infected'?

There are many ways to get infected. Computer users can accidentally download spyware or adware when downloading other programs - even simply visiting an infected website can result in infection. Many popular peer to peer applications and browser plug-ins also include hidden adware or spyware packages.

2.0 What can be done about it?

If you believe that you may have malware then call the Service Desk (ext 7777). The University's anti-malware defence - Sophos - will alert Information Services if you have been infected - so the first thing that might happen is that you get a call from the Service Desk. Don't worry, service desk staff can remotely access your computer (with your permission) and run removal tools which should eliminate the problem. Never pass on emails about supposed security issues to other colleagues - only to IS who can deal with the problem safely.

2.1 Malware Prevention and Removal

Install and run anti-malware and firewall software. When selecting software, choose a program that offers tools for detecting, quarantining, and removing multiple types of malware. At the minimum, anti-malware software should protect against viruses, spyware, adware, trojans, and worms. The combination of anti-malware software and a firewall will ensure that all incoming and existing data gets scanned for malware and that malware can be safely removed once detected.

2.2 Patches

Keep software and operating systems up to date with current vulnerability patches. These patches are often released to patch bugs or other security flaws that could be exploited by attackers.

2.3 Vigilance

Be vigilant when downloading files, programs, attachments, etc. Downloads that seem strange or are from an unfamiliar source often contain malware.

3.0 Malware Types

3.1 Spyware

is a type of malicious programme that is specifically designed to steal information about your activities on your computer. Spyware can perform a number of illicit functions, from creating pop up advertisements to stealing your bank login details, recording the sites you visit and even logging the keystrokes you type.

3.2 Adware

is software that displays advertising banners, re-directs you to websites, and otherwise generates advertising on your computer (not to be confused with popup ads, which come from the websites that you visit).

3.3 Ransomware

Ransomware is a form of malware that holds a computer system captive (by encrypting files on the hard drive or locking down the system) while demanding a ransom from the user to pay to remove the restrictions and regain access to their computer.

3.4 Rootkit

A “Rootkit” is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, a downloaded file or through some other vulnerability in a network service.

3.5 Trojan

A “Trojan,” is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware. When installed, a Trojan can allow a hacker to gain remote access to the infected computer.

3.6 Virus

“Virus” is a general term for malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs.

3.7 Worm

Computer worms are among the most common types of malware. They spread over computer networks by exploiting operating system vulnerabilities. Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers. Computer worms can also contain malicious “payloads” that damage host computers or steal data.

3.8 Potentially Unwanted Software (PUS)

Spyware and adware are sometimes called ‘Potentially Unwanted Software ’because they may or may not be malicious and may or may not have been downloaded intentionally. At best, PUS is a nuisance and it is safe to assume that if any software has installed itself on your computer without you full knowledge and consent, then it is up to no good.

References:

http://nakedsecurity.sophos.com/

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3141
F: +44 (0)23 9284 3122
E: university.secretary@port.ac.uk
W: www.port.ac.uk