Everest engineering

Anti-malware policy

ISM.06

Version 0.2.3

July 1 2025

Contents

1 Introduction

Malware is any form of software that can compromise security. Malware can damage our organisation's reputation, cause financial loss and hinder operational activities. The prevalence of malware requires us to take precautions to protect ourselves and our customers.

1.1 Scope

This policy applies to all Everest Engineering permanent employees, contractors, advisors and contracted partners using, or granted access to, information assets and information processing facilities owned by Everest Engineering, our customers (whether contracted or not) and third party partners.

2 Understanding malware

Malware is any code or software that may be harmful or destructive to the information processing capabilities of the organisation. The term is derived from the phrase *malicious software* and may also be called malicious code.

2.1 Types of malware

Malware is constantly changing as previous attack vectors are closed and new ones are discovered. The most common types of malware found are:

- **Viruses** perform unwanted functions on the infected computer. This could involve destructive actions or the collection of information that can be used by the attacker;
- **Trojans** pretend to be legitimate but conceal other unwanted functions;
- **Worms** copy themselves onto other computers or devices without user interaction;
- **Logic bombs** are malicious software that have been set to run at a specified date and time or when certain conditions are met;
- **Rootkits** disguise malicious activities on a computer by hiding the processes and files from the user;
- **Keyloggers** record keystrokes entered by the user;
- **Backdoors** allow unauthorised access to an attacker;
- **Adware** automatically delivers advertisements. Common examples include pop-up ads on websites and ads displayed by applications;
- **Bots** are autonomous programs which can interact with systems and users for malicious intent;
- **Spyware** enables malicious actors to obtain information about another computer's activity; and
- **Cryptolocker/ransomware** is a form of malware that holds a computer system captive while demanding payment. Ransomware restricts user access by encrypting files on the hard drive or locking down the system. It also displays messages intended to force the user to pay the ransomware creator to remove the restrictions and regain access to their computer.

Often these types of malware will be used in combination with each other. For example, an attacker will encourage an unwitting user to infect a computer with a virus which will allow unauthorised access. This initial access will then be used to install a rootkit to disguise further activities, a keylogger to capture keystrokes and a backdoor to allow future access without detection.

2.2 How malware spreads

Malware needs to be installed on the target device or computer in order for it to carry out its mission. This section describes the most common infection techniques.

2.2.1 Phishing

This method involves tricking the user into taking actions that allows a malicious program to run and infect a device. It is usually achieved via the blanket sending of unsolicited emails with file attachments or web links. A malicious action is triggered when the user opens the file or clicks the link.

Phishing attacks have become more sophisticated and can be very believable and enticing. More targeted versions of phishing have appeared such as targeting a particular organisation (spear phishing) and individuals (whaling).

2.2.2 Websites and mobile code

Widespread use of mobile code such as JavaScript on websites provides attackers with another mechanism to infect devices. Websites will be created to host malware that is activated either by clicking on a link or, in some cases, by visiting a website.

Legitimate websites may also be compromised and used to host malware without the owner's knowledge.

2.2.3 Removable media

USB memory sticks, CDs, DVDs and other removable media devices provide an effective way of spreading malware. Insertion of such media may be enough to trigger an infection.

2.2.4 Cracking

Cracking is a targeted and, therefore, less common method of introducing malware onto a computer or network by exploiting vulnerabilities in software and networked devices. Once access has been gained, malware will be installed onto the compromised machine.

3 Anti-malware controls

The following controls comprise a *defence in depth* approach that avoids reliance on a single protection. All the following controls should be implemented where relevant in order to protect against single failures.

3.1 Firewalls

A firewall will be installed at all points at which an internal network is connected to the Internet. Mobile devices such as laptops constitute part of the internal Everest Engineering network.

Where possible, individual firewalls will be enabled on endpoint computers. Endpoint monitoring software must warn if the firewall is disabled by the user.

Note that references to internal networks is not limited to Everest Engineering processing facilities. They include networks set up by us as part of delivering customer projects.

3.2 Antivirus

Tools used to detect and isolate malware and viruses deployed to critical infrastructure and endpoints used by the organisation must receive updates on current and emerging signatures:

- firewalls and network flow control systems such as web proxies and web application firewalls;
- communication services such as email servers;
- all systems containing classified or sensitive information;
- all other servers/systems unless exemption exists with a vulnerability management plan in place; and
- user computers and devices including BYOD computers.

Antivirus clients must obtain signature updates on a regular basis, either directly from the vendor or from a central server within the organisation.

On-access scanning must be enabled by default to provide real-time protection. Regular full scans must also be carried out at least once a week.

Antivirus programs must be configured from a central management console to ensure that the software cannot be disabled or altered by users. This will be routinely verified by Everest Engineering's security function.

Antivirus programs must also be configured to stay up to date and to generate audit logs of their actions.

3.3 Systems not requiring antivirus

Some may not be affected by malware and therefore will not have antivirus software installed. These systems must be periodically reviewed to ensure this situation hasn't changed.

3.4 Spam filtering

Email systems must be configured to filter out unsolicited and potentially harmful emails before they are delivered to users.

3.5 Software installation and scanning

Users may install any legally obtained software on their Everest Engineering devices unless that software has been explicitly banned.

Regular scanning of user computers must be carried out to detect unauthorised software.

3.6 Vulnerability management

Information on software vulnerabilities will be collected from vendors and third-party sources and updates applied where available. If possible and if permitted by the organisational change management policy, updates will be applied automatically as soon as they are released.

Vulnerability scanning must be carried out regularly, particularly on business-critical servers and networks.

New vulnerabilities identified by Everest Engineering employees may only be communicated following coordinated disclosure practices.

3.7 User awareness training

Users must be made aware of the information security policy when starting with the organisation. They must be trained in ways to avoid falling victim to attacks such as phishing.

This security awareness training must be completed on a regular basis by all employees who have an Everest Engineering email address.

3.8 Threat monitoring and alerts

Information about emerging threats will be obtained from appropriate sources and users alerted proactively of potential attacks, giving as much detail as possible to maximise the chance of recognition.

3.9 Technical reviews

Regular reviews will be carried out of business-critical servers and networks to identify any malware that has been installed since the last review.

3.10 Malware incident management

Detection of malware on any Everest Engineering device must trigger a security incident which must be managed according to incident management procedures.