

Malware breakout penetration testing

No one is safe when it comes to malware.

Malware can gain access to your network from a huge range of unlimited attack vectors and can infiltrate in the most devious ways.

Malware is short for "malicious software" – programs designed to infiltrate and damage networks or computers without the user's consent. **Malware** is the general term covering all the different types of threats to your computer safety such as viruses, AdWords, trojans, Ransomware and so on.

- **Virus** – Malware that piggybacks another program to gain access. Once in, starts replicating itself through modifying existing programs and infecting them.
- **Adware** – Software that generates pop-up ads on your screen, mostly via a web browser.
- **Trojan horse** – The most dangerous type. It manifests itself into something useful to gain access. Once in, trojans can be used to steal financial information or install viruses and ransomware.
- **Ransomware** – Software that locks you out of your device while it encrypts your system and

data and then requests you to pay a ransom to retrieve it back.

- **Rootkits** are a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that is not otherwise allowed
- **Browser Hijacking** is a form of unwanted software that modifies a web browser's settings without a user's permission, to inject malicious content into the user's browser

The most basic, common and most successful method is via opening of a malicious email attachment or password theft.

How do attackers use it and what are the implications?

Typically, malware is delivered from external sources. It's often made to look like it has originated from a known

trusted source. An unsuspecting internal user that clicks on a link or executes malicious code delivered via a phishing attack can be easily compromised and used as a pivot point to attack other systems, users or data in the internal network.

Anybody can be fooled into clicking on a malicious link they think came from a Facebook friend, LinkedIn connection, or what looks like an internal email.



A successful external attack can quickly become a broader internal attack, compromising many systems without any warning.

Stealing, encrypting, deleting data, altering or capturing core computer functions, spying on your computer activity without your knowledge or permission can be far more damaging.

Malware intrusion by organised crime is more prevalent and their ways to gain access to a system are becoming increasingly sophisticated. A successful Malware attack can result in heavy financial and reputation losses.

Common signs of attack

The most common warning signs to be aware of include:

- Receiving an email asking you to download software or click on a link for more information;
- Receiving an email asking you to follow a link and enter your credentials;
- Pop up boxes start appearing on your screen that are requesting you to answer a simple question or a close button;

- New icons appear on your computer screen; or
- Your computer becomes slower than usual.

Becoming aware of the signs that you have been attacked by malware is step one, step two is realising that you have been compromised. The signs include:

- Your system crashes, freezes or displays what we call 'the blue screen of death.';
- Disk space decreases;
- Internet activity has increased in an unexplainable way;
- Your home page changes without authorisation or new toolbars appear;
- Extensions or plugins start appearing on your browser; or
- The anti-virus ceases working.

How can I protect myself from malware?

As an organisation, simple procedures to keep in mind to protect yourself from malware include:

- Avoid clicking on pop-up ads, opening unsolicited email attachments or downloading software from unknown sites;
- Make sure your anti-virus and anti-spyware is up to date, as well as your operating systems, browsers and plugins;
- Most importantly, change passwords regularly, or better still, introduce a centralised password management solution; and
- Back up your data and always backup offline and preferably offsite.

Malware breakout penetration test

The ideal preparation for an attack is conducting a **malware breakout penetration test**.


This test will identify:

- The likely path malicious code will travel through your systems both internally and externally;
- Show the outcome and likelihood of a successful phishing campaign;
- Find the vulnerabilities in your desktop deployment;
- See how easily ransomware could spread in the network and what can it see;
- Identify advanced persistent threats;
- Review the security of your Active Directory deployment;
- Review the effectiveness of your mail filtering and endpoint protection solutions; and
- Ensure your logging and event management solutions are alerting you on suspicious activities.

In parallel with the test, we strongly recommend bolstering internal security controls by implementing actionable recommendations.



Contact us to discuss how our security solutions can help protect your most vital assets

 1300 922 923
+61 (2) 9290 4444

 info@senseofsecurity.com.au

 senseofsecurity.com.au