Information security procedure

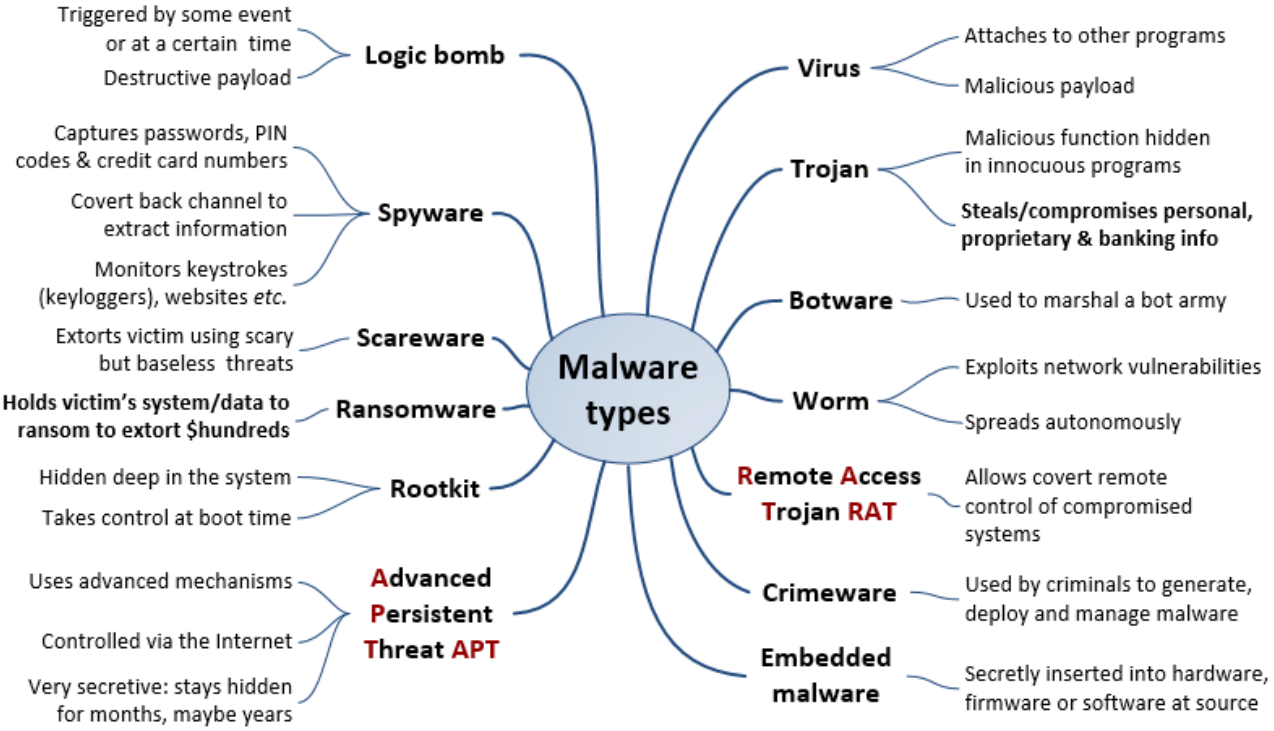
Reporting malware

Introduction

Corporate policy requires us to report information security incidents such as malware infections promptly. This procedure describes the typical symptoms of infection, explaining how to report them and seek help.

What *is* malware?

Malware is **mal**icious soft**ware**, commonly known as "viruses". Aside from true computer viruses, malware includes other types of mean and nasty software:



Modern remotely-controlled multifunctional malware can take on the characteristics of any of these, and actively evades antivirus software. Networked or standalone computers (desktops and servers), laptops, tablet PCs, smartphones and other IT devices (including *things* and industrial controllers) can be infected.

While Windows systems are usually hit, malware is also a problem on Linux and MacOS, mobile operating systems such as iOS, Android and Java, and others.

Your device *might* be infected with malware if …

- *Someone* using the computer/device (not necessarily you) has visited an infectious website, downloaded and installed an infected program, opened an infected email attachment, plugged in an infected USB memory stick/thumb drive, loaded an infected CD/DVD …;
- The antivirus software reports finding malware, or stops working (locks up or shuts down);

- Friends say they have received infected messages from you, even if you didn't send them;
- Your computer takes longer than normal to boot or runs unusually slowly (malware is just one possible reason!);
- New files or folders appear or old ones disappear, or free disk space unexpectedly shrinks;
- Corporate or personal secrets are compromised, business information is deleted, corrupted or disclosed, systems become unusable, a ransom is demanded, your identity is stolen, your bank account or the corporate bank accounts are drained, the police turn up with bad news …

What to do

It almost goes without saying that you should avoid malware infections like the plague.

The following cut-out-and-keep reminder tells you what to do if, despite your best efforts, you think your computer, tablet, smartphone, *thing etc*. might have been infected with a virus:

Reporting malware

Call the Help Desk as soon as you notice possible symptoms of a computer virus infection. Help Desk will log the incident, gather basic information, give you first-responder advice on what to do and if necessary initiate a full emergency response from the IT support professionals. When you call, Help Desk will ask you for:

- Your name and contact details;
- Details about the issue *e.g*. the symptoms;
- Further information needed to diagnose and deal with the incident.

Please don't mention malware to anyone outside of the organization. Incidents and rumors spread alarm and can seriously harm the business.

It is important to report actual and suspected malware incidents promptly because infections can spread very quickly. It is better to report something that turns out to be a false alarm than to hesitate or ignore something that turns out to be very serious. We must also watch out for little clues that the IT systems have been compromised. If we keep our eyes and ears open and share our concerns, we stand a much better chance of identifying and stopping malware before all is lost.

If something strikes you as odd, don't keep it to yourself.
Tell someone about it – preferably your colleagues, your manager or the Help Desk. **You might even earn a reward for being the first to spot a serious malware infection!**

Further information

Browse the intranet *Security Zone*, speak to your manager or contact the Help Desk for more about malware, or to report your concerns.