Skillmine
Technology • Consulting • Services

infosec
Miners

# MALWARE

Malware, short for malicious software, is a blanket term for viruses, worms, trojans and other harmful computer programs hackers use to wreak destruction and gain access to personal information. “Malware is a software designed to cause damage to a computer, server, or computer network."

## Types Of Malware:

There are different types of malwares:

- A Worm is a standalone piece of malicious software that reproduces itself and spreads from computer to computer without human interference.
- A Virus is a piece of computer code aimed to disrupt systems, cause major operational issues, and result in data loss and leakage. It needs human interaction to spread.
- A Trojan is a program that cannot reproduce itself but masquerades as something the user wants and tricks them into activating it. Trojan does its damage and spreads through the system's back door.
- Adware or advertising-supported software displays unwanted advertisements on our computer devices.
- A Botnet is a collection of bots. The term also refers to the malware run on a connected device to turn it into a bot.
- Hijacker modifies a web browser’s settings without users’ permission, usually to inject unwanted ads into the browser or redirect to scam sites.
- Keylogger is a trojan spyware that can steal or record user keystrokes.
- Spyware is a "malware used to gather data on an unsuspecting user secretly." In essence, it spies on your behaviour as you use your computer and the data you send and receive, usually to send that information to a third party.
- Ransomware is a form of malware that locks you out of your device and encrypts your files, then forces you to pay a ransom to get them back.

## How To Detect Malware?

Users may be able to detect malware if they observe an unusual activity, such as

Sudden loss of disk space.

Prolonged speeds.

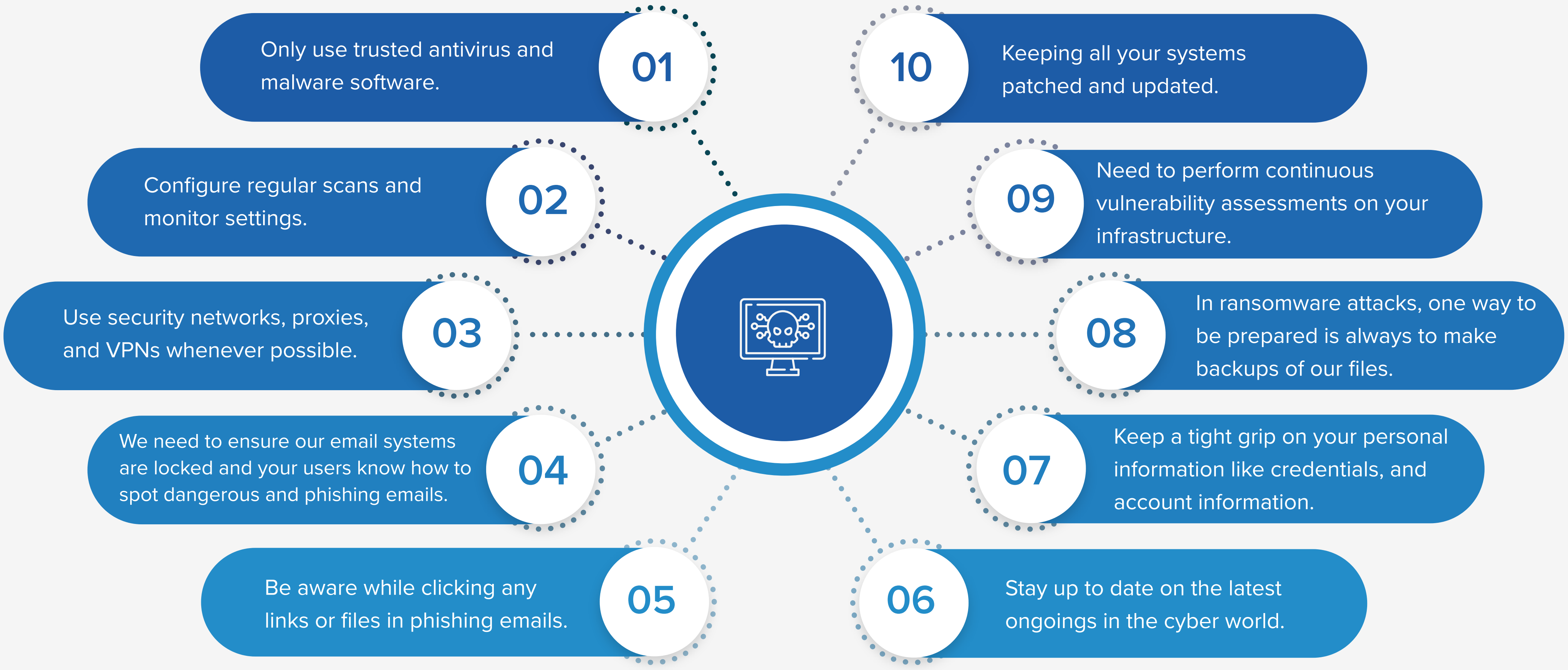
High unwanted internet activity and pop-up advertisements.

Repeated crashes or freezes.

Automatic shutting down/rebooting of the computer device.

High bandwidth utilization.

## How To Prevent Malware?



01 Only use trusted antivirus and malware software.

02 Configure regular scans and monitor settings.

03 Use security networks, proxies, and VPNs whenever possible.

04 We need to ensure our email systems are locked and your users know how to spot dangerous and phishing emails.

05 Be aware while clicking any links or files in phishing emails.

06 Stay up to date on the latest ongoings in the cyber world.

07 Keep a tight grip on your personal information like credentials, and account information.

08 In ransomware attacks, one way to be prepared is always to make backups of our files.

09 Need to perform continuous vulnerability assessments on your infrastructure.

10 Keeping all your systems patched and updated.

## Famous Malware Threats:

### Clop Ransomware:

“Clop” (CryptoMix ) is one of the latest ransomware threats, which frequently targets Windows users. It blocks 600 Windows processes and disables multiple Windows 10 applications, Windows Defender and Microsoft Security Essentials — leaving you with zero chance of protecting your data.

### Zeus Gameover:

Zeus Gameover is part of  “Zeus”( a late '00s keylogger Trojan that targeted banks) family of malware and viruses. This malware is a Trojan disguised as something legitimate that accesses your sensitive bank account information.

### ILOVEYOU:

It’s a worm that spread like wildfire in the early 2000s and gave way to more than $15 billion in damage. It infected over ten million Windows personal computers on and after 5th May 2000. The modus operandi is dropping an email with the " ILOVEYOU " subject line and the attachment "LOVE-LETTER-FOR-YOU.TXT.vbs.

### Conficker:

It’s a worm that exploits unpatched flaws in Windows and leverages a variety of attack vectors – from injecting malicious code to phishing emails – to ultimately cracking passwords and hijacking Windows devices into a botnet.

### Stuxnet:

Stuxnet is an intelligent worm that infected computers worldwide; however, catastrophic damage occurred in the Iranian nuclear facility at Natanz. The worm destroyed uranium-enriching centrifuges, the mission the U.S. and Israeli intelligence agencies built for it.

## SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

India | KSA | UK | USA

Stay connected