UKaid
from the British people

DigiGirls

Protecting Against Viruses and Other Malwares

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Malware

CONTENT

- What is Malware?
- Types of Malwares
- Case Studies
- Signs of a Malware Attack
- Preventive Measures

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Malware Case Study

An initiative of
cybersafe.
FOUNDATION

What is a Malware?

Malware is shorthand for malicious software. Malware is a collective name for a number of malicious software variants, including viruses, ransomware and spyware. This software is intentionally designed to cause damages to a computer, server, client or computer network.

UKaid
from the British people

DigiGirls

Types of Malware

Viruses

Trojan

Worms

Rootkit

Key loggers

Ransomeware

Adware

Spyware

An initiative of
cybersafe.
FOUNDATION

Case Study 1

https://thehackernews.com/2023/03/nexus-new-rising-android-banking-trojan.html

Case Study 2

https://vpnoverview.com/news/nigerian-hacker-solicits-disgruntled-employees-and-accidently-reveals-his-identity/

Case Study 3

https://www.kaspersky.com/about/press-releases/2023_industrial-sector-attacks-on-the-rise-an-annual-overview-by-kaspersky

Case Study 4

https://www.bleepingcomputer.com/news/security/new-hook-android-malware-lets-hackers-remotely-control-your-phone/#:~:text=A%20new%20Android%20malware%20named,VNC%20(virtual%20network%20computing).

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Malware Types
Part 1

An initiative of
cybersafe.
FOUNDATION

Business Email Compromise

This a social engineering method that targets companies who conduct wire transfers and have suppliers abroad. Corporate or publicly available email accounts of executives or high-level employees related to finance or involved with wire transfer payments are either spoofed or compromised through keyloggers or phishing attacks to do fraudulent transfers, resulting in massive losses.

Viruses

A computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.

A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code.

Worms

Worms are basically harmful software which uses network/system vulnerabilities to spread themselves from system to system. They are typically part of other software such as rootkits and are normally the entry point into the system. They basically compromise the system (locally or remotely) and provide access to other malware.

Rootkit

A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. Originally, a rootkit was a collection of tools that enabled administrator-level access to a computer or network.

Root refers to the Admin account on Unix and Linux systems, and kit refers to the software components that implement the tool.

Ransomware

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

UKaid
from the British people

DigiGirls

Trojans

Trojan is a type of malware that invade your computer disguised as a real, operational programs. Once a trojan is inside your system, it can perform destructive actions before you even know it's there. Once inside, some trojans sit idly on your computer and wait for further instructions from its host hacker, but others begin their malicious activity right from the start.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Malware Types
Part 2

An initiative of
cybersafe.
FOUNDATION

Spyware

Spyware is loosely defined as malicious software designed to enter your computer device, gather data about you, and forward it to a third-party without your consent. Spyware can also refer to legitimate software that monitors your data for commercial purposes like advertising. However, malicious spyware is explicitly used to profit from stolen data.

UKaid
from the British people

DigiGirls

Keyloggers

A keylogger is an insidious form of spyware. You enter sensitive data onto your keyboard, believing nobody is watching. In fact, keylogging software is hard at work logging everything that you type.

Adware

Adware, also known as advertisement-supported software, is software that displays unwanted (and sometimes irritating) pop-up adverts which can appear on your computer or mobile device. It generates revenue for its developers by automatically generating adverts on your screen, usually within a web browser.

UKaid
from the British people

DigiGirls

Scareware

Scareware is a social engineering tactic that manipulates users into believing they need to download or buy malicious, sometimes useless, software. Most often initiated using a pop-up ad. Scareware uses social engineering to take advantage of a user's fear, coaxing them into installing fake anti-virus software.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Signs of a Malware Attack

An initiative of
cybersafe.
FOUNDATION

Signs of a Malware Attack

- Frequent pop-up windows.
- Your usual homepage may change to another website, for instance. Plus, you may be unable to reset it.
- Mass emails being sent from your email account.
- Frequent system crashes.
- Unusually slow computer performance.
- Unknown programs that start up when you turn on your computer.

Signs of a Malware Attack

- Unusual activities like password changes. This could prevent you from logging into your computer.
- Unusually slow or frozen system functionality
- Spam and pop-up ads
- Unknown icons on the desktop
- Redirection from a popular website to an unknown one
- New files or folders created without your permission

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

How Malware Spreads

An initiative of
cybersafe.
FOUNDATION

How Malware Spreads

Malware is typically distributed via:

1. Email attachments
2. Infected external storage devices
3. Fake internet ads
4. Social engineering tactics
5. Infected applications or websites

How Malware Spreads

Often, users are tricked into downloading malware with links or pop-ups that seem legitimate such as:

- Flashing messages like, “Your computer has been infected! Click here to run a scan!”
- Unknown applications that purport to convert files, unzip files or find discounts
- “Gifts” or “prizes” offered for clicking a button
- Clicking the link or button directs the user to a website that automatically installs malware onto their computer.

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION

UKaid
from the British people

DigiGirls

Malware Preventive Measures

An initiative of
cybersafe.
FOUNDATION

Preventive Measures

- Keep your computer and software updated
- Think twice before clicking links or downloading anything
- Be careful about opening email attachments or images
- Don’t trust pop-up windows that ask you to download software
- Limit your file sharing
- Use an antivirus software

Preventive Measures

- Only buy Apps from trusted sources
- Install a firewall
- Back up your data regularly
- Get a password manager
- Only access secured sites
- Read emails with an eagle eye.

Topic Activity

- Scan malicious links or attachments using VirusTotal
- Find a case study of a cyber attack and identify what malware variants were used

UKaid
from the British people

DigiGirls

THANK YOU

An initiative of
cybersafe.
FOUNDATION