NAWA Media

Ways in which Malware can Infect your Device/Network

Section: 3.2

Malware Attacks

Your device can be affected by malware in many ways.

For instance, clicking on random links, installing software online, clicking on a link or even just by visiting any website sent by your friend.

As journalists, your data is extremely valuable and under increased likelihood of attack.

Next are the different ways you could get infected by any malicious software:

Malware Attacks on your Device

Type of Malware Attack Mitigation	Mitigation
Email attachments/Phishing attacks	Before you open any file or link attached to the email, ask yourself “is this from someone I know?” Only open links from email addresses you trust. If you receive any of the suspicious file extensions (.bat, exe, .dmg, vbs etc) within your email do not open it. Rule of thumb, do not fill out forms unless you completely trust the source or until you absolutely HAVE to. If you receive any suspicious or unexpected attachment on email, get it scanned through **virustotal.com**.
Monitoring Online Activities	Switch to “private mode” or “incognito mode” within your browser. Use any adblocker service to prevent accessing malware while browsing. Browser extensions like Ghostery or Disconnect show the name of trackers, and you can then block them. Always use the updated version of the browser that you’re using.

Email attachment

Spreading malware through email is the most common and effective way to target any journalist, activist and any other internet user.

In the last few decades, email has become one of the effective methods for communication and hackers are utilizing this platform to spread malicious links, documents and other malicious content which, if clicked on or downloaded by a user unknowingly, can compromise the whole device or parts of it.

There have been many incidents where malware campaigns are initiated at the global level and have targeted multiple companies, communities and even individuals. Once the device is infected with malware, it can lead to substantial financial loss, breaching of data or even do nothing and silently spying on your online activities.

Email Attachment: Mitigation

Before you open any file or link attached to the email, the first step is to make sure you ask yourself “is this from someone I know?” Only open links from email addresses you trust, be suspicious of social engineering attacks that might be directed towards you.

Social engineering techniques include sending emails on behalf of friends or someone you know, either by taking over their account or spoofing their emails through similar sounding email addresses. For the untrained eye, these social engineering attacks can be quite deceptive.

There are few file extensions which are already blocked by most of the mail providers. Few of them are .bat, exe, .dmg, vbs etc . So, if you receive any of the mentioned file extensions within your email then do not open it as it might hold a malicious script which will be executed if you clicked.

Phishing attacks can also be done via email, where the attacker seeks to steal the sensitive information like login credentials, passwords or financial data by tricking the user to fill up an HTML form or redirecting them to the suspicious website. Rule of thumb, do not fill out forms unless you completely trust the source or until you absolutely HAVE to.

If you receive any suspicious or unexpected attachment on email, get it scanned through virustotal.com. It might not hundred percent detect the malware but still is a good practice to follow.

Having an updated version of the browser and antivirus software also prevents you from downloading and installing any malicious script.

Online Activities

Scrolling on our newsfeeds, browsing the internet and using search engines is part of our daily routines, it happens almost every time we pick up our devices.

We see hundreds of websites which can be used to spread malware by injecting malicious code into the device or by maladvertising.

Online Activities: Mitigation

Switching to “private mode” or “incognito mode” within your browser is one of the easiest and most basic approaches a user can use to protect information.

Private mode does not store your browsing history and somewhat protects you from trackers used for collecting information for advertisements (depends on the browser).

Ads are the most significant cause of malware spreading, and can annoy users if a website is full of ads. It’s better to use any adblocker service to prevent such behaviour while browsing online.

Web trackers reveal a significant amount of useful information to the third-party companies, and it’s a bit hard to find who is tracking us, and from where they are doing it.

Any browser extension like Ghostery or Disconnect shows the name of trackers, and you can then block them.

Always use the updated version of the browser that you’re using. There are a number of vulnerabilities an attacker can use to infiltrate the whole device, every update brings us more security features and a better GUI.

NAWA Media

In the **next** section, a case study will be used to illustrate the nature of threats journalists face in online spaces.

BCMCR | Birmingham Centre for Media and Cultural Research

BIRMINGHAM CITY University

MEEDAN

Check

Sida