

MALWARE

Introduction to Malware

It's your first day on the job at Cybercademy — a new cybersecurity organization that helps companies improve their security practices.

Your Task

Identify various types of [malware](#) on an infected device and provide suggestions to the client on how they can prevent this from happening in the future.

But first, what is malware? *Malware* is malicious hardware, firmware, or software inserted into a system to cause damage or gain unauthorized access to a network. Any type of malware can greatly compromise the security principles of Confidentiality, Integrity, or Availability.

Throughout this lesson, you will learn how each type of malware gets into a system, what it does, and a short suggestion for how to be cautious against this form of malware.



Adware

First, you open the web browser. The first page it opens to is a strange page about a computer cleaner that's "guaranteed to make your computer run 10X faster!!". What an odd choice for a homepage.

As you navigate the web, you notice lots of ads popping up all over the place. There are so many popping up on your screen that it's actually slowing down the webpage and increasing page load times.

It's clear this computer has [adware](#). *Adware* is unwanted software designed to throw advertisements on your screen. While not overly malicious on the surface, sometimes adware can come bundled with other, more harmful [malware](#).

With enough adware on your machine, this could become a real performance issue.

Your Suggestion

- You tell your client to make sure to not click on any strange links or download any untrustworthy files.
- A trustworthy antivirus software could also help with this issue.

Instructions

Let's play around with an example of how adware might work.

1. Click the "Click HERE to Download!" button on the sample webpage to the right.
2. Wow, that's a lot of ads! Now, try clicking on the link on one of the ads and see what happens.

Potential adware won't always be so obvious (and look so badly made) so don't click on anything you're not 100% sure of!

EPIC Disk Cleaner

guaranteed to make your computer run 10X faster!!

"You'll never need another cleaner!"

~ Barbara



"1 of a Kind!"

~ Best Computer Cleaner Mag

Click [HERE](#) to Download!

Virus

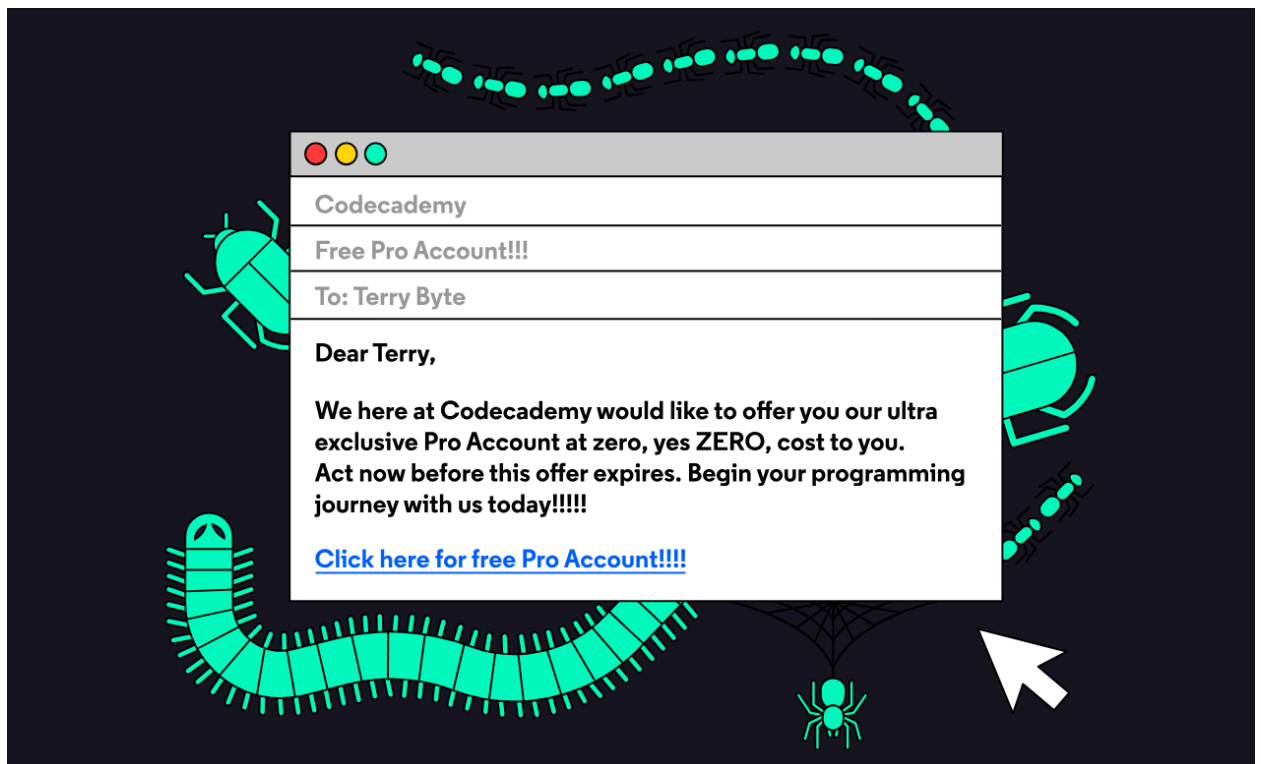
You navigate to your client's email. Immediately, you see that your client opened some emails sent from an odd email address. You open the emails and see that the client clicked on links and likely downloaded files from these suspicious emails. Uh oh. Did your client download a virus?

A [virus](#) is a malicious self-replacing application that attaches itself to other programs and executables without the permission of the user. It's possible a downloaded virus could alter or delete data on the computer.

If the virus was able to access or alter data, the confidentiality and integrity of that data is now in question.

Your Suggestion

- Just like with [adware](#), avoid suspicious links and install trustworthy antivirus software.
- Immediately report suspicious emails to your IT department and never open them.



Worms

What type of [virus](#) is this? You check your client's "Sent Emails" folder and notice your client recently sent the same email to everyone on their contacts list. The emails have the same subject line as the malicious email they received. It almost seems like the email replicated itself...

Aha! Rather than a virus, which needs to be attached to a file or application to spread, you may have found a worm.

A *worm* is self-replicating code that copies itself from computer to computer without user intervention. This worm could be just as dangerous as a virus.

The worm could also replicate so much that it overloads your client's system. By doing this, the worm could bring down the system and violate availability.

Your Suggestion

- Follow the previous suggestions for [adware](#) and viruses.
- Monitor the computer for any unexpected changes! Is it slower than usual? Is there less hard drive space than expected? Have files mysteriously appeared or disappeared? These could all be signs of worms.

Instructions

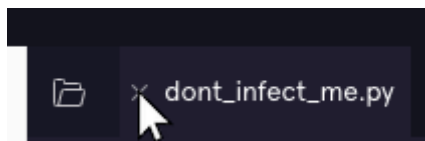
1.

How does a worm work? While worms don't attach themselves to files, we'll use files to simulate their duplicative nature!

First, let's look at some innocent files that our "worm" will infect.

Press "Run" to run **dont_infect_me.py**.

Press the "x" next to the filename to close the file.



Hint

Make sure you ran the correct file! If you did, make sure the file says:

```
print("Don't infect me, please!")
```

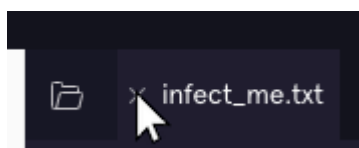
2.

Let's look at another innocent file.

Make sure you've closed the **dont_infect_me.py** file. You should now see the **infect_me.txt** file in the workspace.

Press "Run" to run **infect_me.txt**. (Nothing will happen because it's a text file!)

Press the "x" next to the filename to close the file.



Hint

Make sure you ran the correct file! If you did, make sure the file says:

```
What? Why me? I'm just a text file.
```

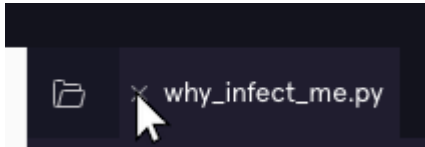
3.

Let's look at our last innocent file.

Make sure you've closed the **infect_me.txt** file. You should now see the **why_infect_me.py** file in the workspace.

Press "Run" to run **why_infect_me.py**.

Press the "x" next to the filename to close the file.



Hint

Make sure you ran the correct file! If you did, make sure the file says:

```
print("What's going on?")
print("What are you doing?")
print("I'm super important!")
```

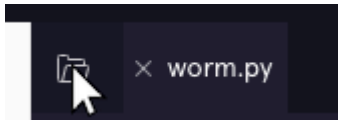
4.

Finally! We've reached the worm file.

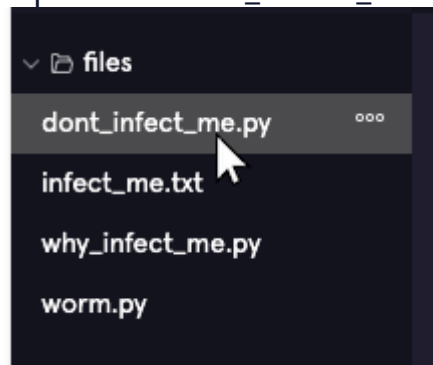
What this file will do is search for any python file with "infect_me" in its name. You don't need to understand this code, all you need to do is run it!

Press the "Run" button.

Now, click the folder button in the workspace to look at the files.



Open the **dont_infect_me.py**, **infect_me.txt**, and **why_infect_me.py** files.



The "worm" should have copied itself into the files with the `.py` extension.

If you didn't close those files, you will need to close and reopen them to see your worm in action!

Hint

If the files look exactly the same, try running **worm.py** again, closing each of the files, and reopening them again.

You should see that the worm copied itself into all of the files with the `.py` file extension!

Spyware

Wow, what a disaster computer. Hm, when you type, there seems to be a slight delay before some of the characters show up. What's going on?

Oh no! It looks like your client may be in deeper trouble — they may have downloaded [spyware](#) as well. *Spyware* is malicious code downloaded without a user's authorization which is used to steal sensitive information and relay it to an outside party in a way that harms the original user. If the spyware contained a [keylogger](#), a program that can record what a victim types into their computer, a threat actor could potentially gain access to sensitive information.

This means any sensitive data, like passwords, will soon be in the hands of a malicious third-party. While spyware usually isn't used to alter data, it definitely violates the principle of confidentiality. A malicious actor may have been spying on sensitive data your client was typing.

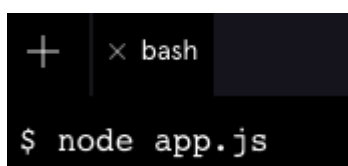
Your Suggestion

- Noticing a trend? Be careful what you click on and install that trustworthy antivirus already!

Instructions

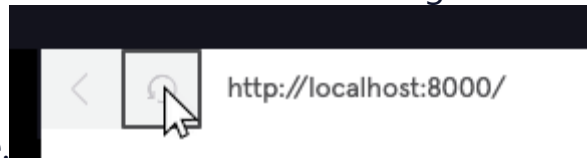
Let's run the app and test out your spyware!

1. Type `node app.js` into the terminal and press the `Enter` or `return` key on your keyboard to start your keylogger app.



```
+ | × bash
$ node app.js
```

1. Press the circular arrow button on the right side of the screen to load



the webpage.

2. Now, try typing in a fake username and password. What prints to the terminal when you type in the password field?

Hint: Not working? Make sure you don't have this exercise open in any other tabs! Then, refresh this page and try again.

Trojan Horses

While the presence of [spyware](#) makes it obvious something nefarious was installed on the computer, was anything else installed?

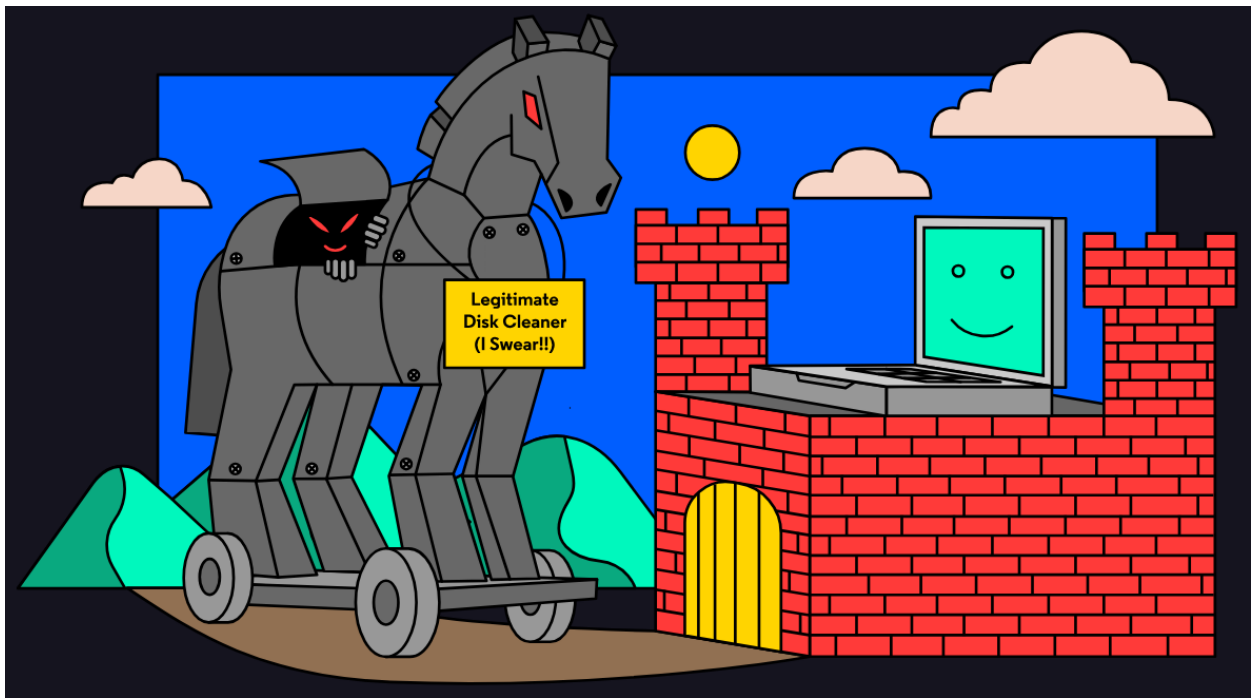
Ugh, of course. After more digging, you find a [Trojan](#) Horse. Wow, is there any download link your client didn't click on?

While similar to Spyware, the *Trojan Horse*, sometimes just called a "Trojan", does more than just monitor what's happening on a system. Trojans are a type of contained, non-replicating malware that disguises itself as legitimate software in order to allow scammers and hackers access to a user's system.

Just like the Greeks hid inside a giant wooden horse to sneak into the city of Troy, this malware snuck right onto your client's computer while pretending to be a legitimate antivirus software!

Your Suggestion

- Be wary of disk or computer cleaners as well as unknown antivirus software. Trojan horses often pretend to be trustworthy software in order to convince you to download them onto your machine.



Rootkits

What exactly is the [Trojan](#) Horse up to? What was it trying to do? You have to find the answer.

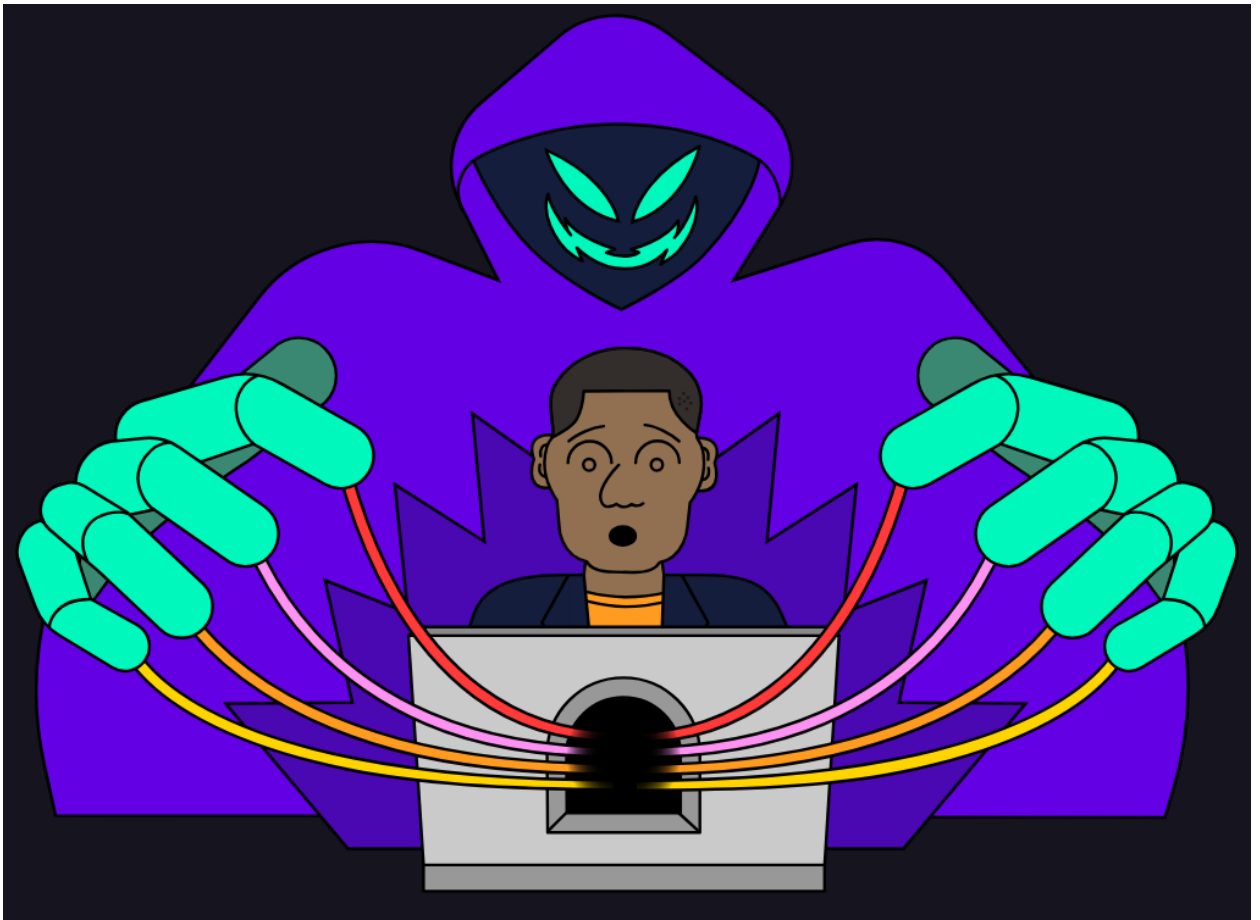
Scanning the device, you find that this horrible device just keeps getting worse; the Trojan horse was used to sneak a [rootkit](#) onto the system.

Rootkits are a collection of malicious programs that secretly provide continued, privileged access to a system for an unauthorized user. A rootkit can create a *backdoor* on a computer to let a hacker in. This rootkit was able to gain admin access to this computer, and it will be incredibly hard to remove.

In this case, the Trojan Horse pretended to be a trustworthy antivirus software in order to install a rootkit. This means that a malicious, third-party somewhere has admin access to this computer and its data. This is a nightmare scenario for the confidentiality and integrity of your client's system. While some specialized tools can remove a rootkit, it isn't easy.

Your Suggestion

- Back up any important data on this system and reimage it.



Ransomware

The [rootkit](#) allowed someone access to this computer. What did they do with that access? You realize that the rootkit was used to deny the user access to files on their system that contain lots of important company data.

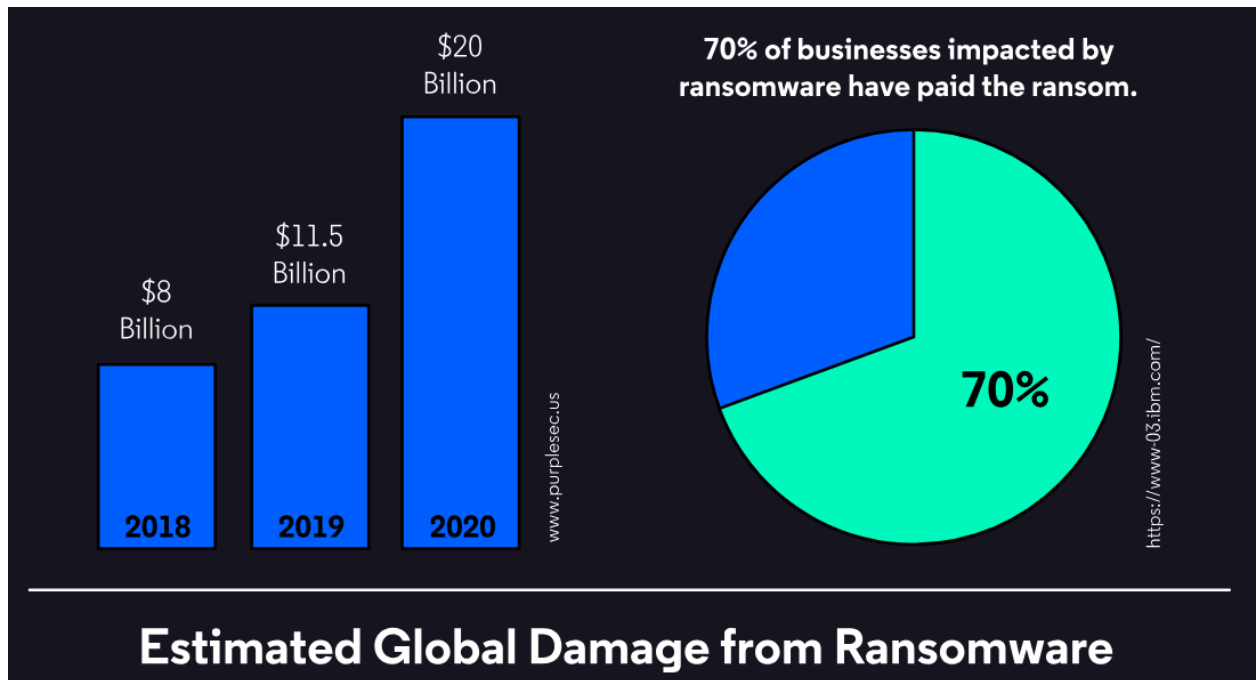
If the malicious actors block access to data or threaten to publish the sensitive data unless the client pays them money, that could be a case [ransomware](#). The use of *ransomware* has been skyrocketing as threat actors have realized it's safer and easier to rob a virtual location rather than a physical one! Ransomware is one of the largest cybersecurity threats facing industries today.

Blocking a user's access to data greatly threatens availability. While availability might not seem important, it can be devastating to some organizations. Imagine if a hospital or flight system lost access to their system or data!

Your Suggestion

- Regularly back up important files.

- Have a procedure in place for ransom requests. They should include a step in which the authorities are alerted.



Fileless Malware

It seems like nothing else could go wrong with this computer. If this was a game of [malware](#) bingo, you would be one step away from winning the jackpot. For fun, you investigate some command-line programs to see if they've been altered. Aaaand, did someone say bingo?

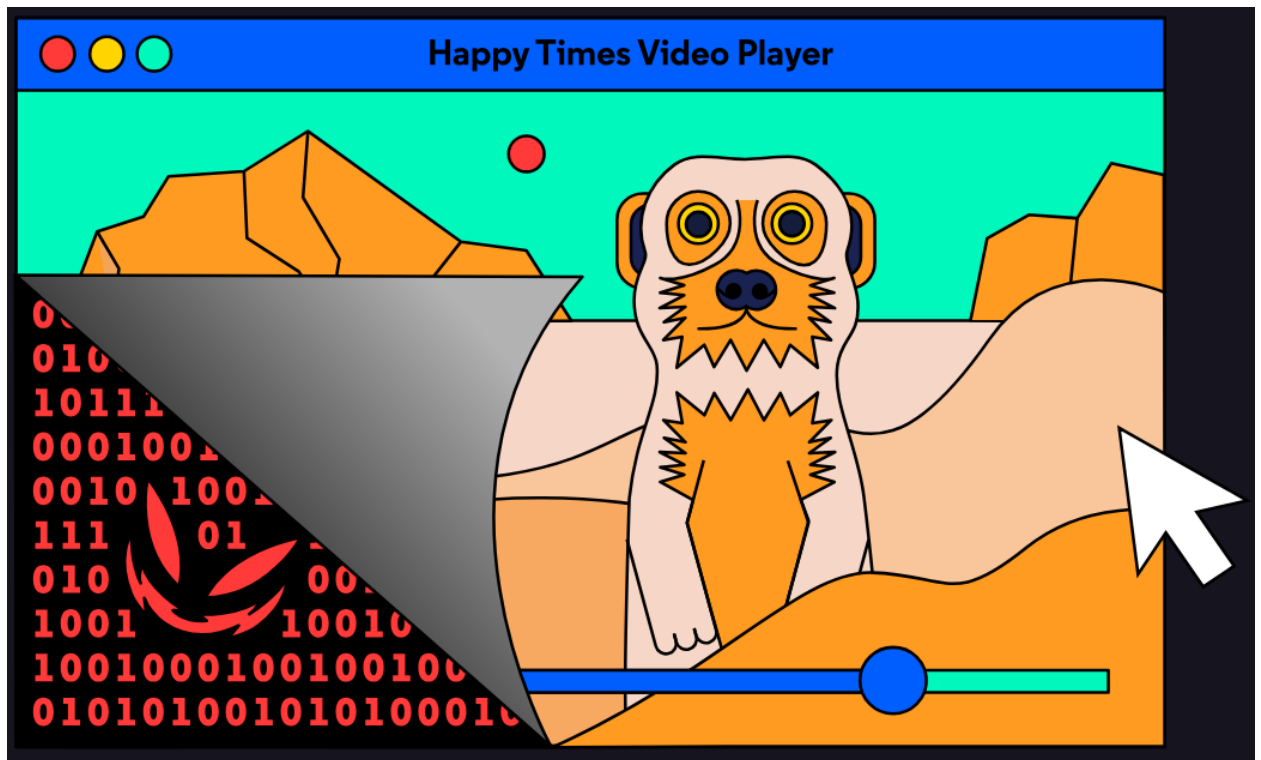
Fileless malware is a type of malware that 'lives off the land' and uses legitimate tools and the user's operating system to perform malicious activities like privilege escalation, data collection, and more. It's incredibly hard to detect and almost always missed by antivirus software.

Unlike a [Trojan](#) Horse, fileless malware is not pretending to be legitimate software, it actually is a part of legitimate software. Fileless malware hides itself within the code of legitimate software, often altering existing code to make it malicious.

Certain programs, like Microsoft PowerShell, are particularly vulnerable to these attacks. Someone could use this attack vector to gather data, use your device resources to mine cryptocurrency, or even install other malware.

Your Suggestion

- Did you download that antivirus yet? Still avoiding those suspicious links?
- Disable command-line applications and macros not in use on the device.
- Keep your applications and system up to date for the latest security updates.
- Reboot the computer.



Fileless Malware

It seems like nothing else could go wrong with this computer. If this was a game of [malware](#) bingo, you would be one step away from winning the jackpot. For fun, you investigate some command-line programs to see if they've been altered. Aaaand, did someone say bingo?

Fileless malware is a type of malware that 'lives off the land' and uses legitimate tools and the user's operating system to perform malicious activities like privilege escalation, data collection, and more. It's incredibly hard to detect and almost always missed by antivirus software.

Unlike a [Trojan](#) Horse, fileless malware is not pretending to be legitimate software, it actually is a part of legitimate software. Fileless malware hides

itself within the code of legitimate software, often altering existing code to make it malicious.

Certain programs, like Microsoft PowerShell, are particularly vulnerable to these attacks. Someone could use this attack vector to gather data, use your device resources to mine cryptocurrency, or even install other malware.

Your Suggestion

- Did you download that antivirus yet? Still avoiding those suspicious links?
- Disable command-line applications and macros not in use on the device.
- Keep your applications and system up to date for the latest security updates.
- Reboot the computer.