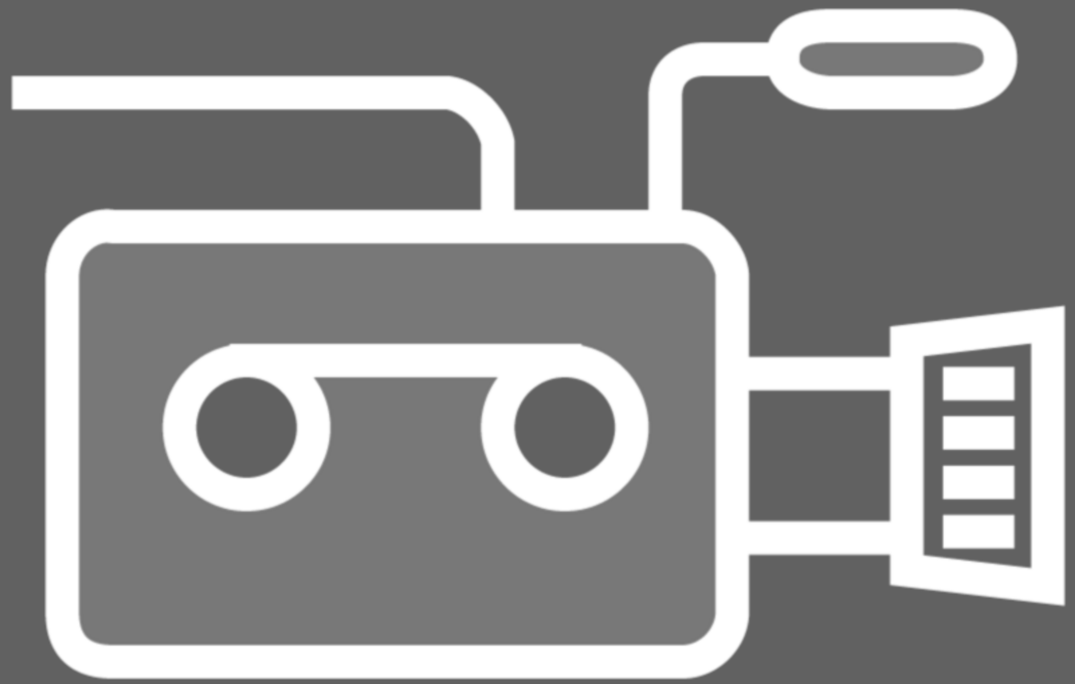
Diving Deeper into Trojans

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|



This is your last chance. After this, there is no turning back. You take the blue pill - the story ends, you wake up in your bed and believe whatever you want to believe. You take the red pill - you stay in Wonderland and I show you how deep the rabbit-hole goes.

Morpheus

How to Infect the Target

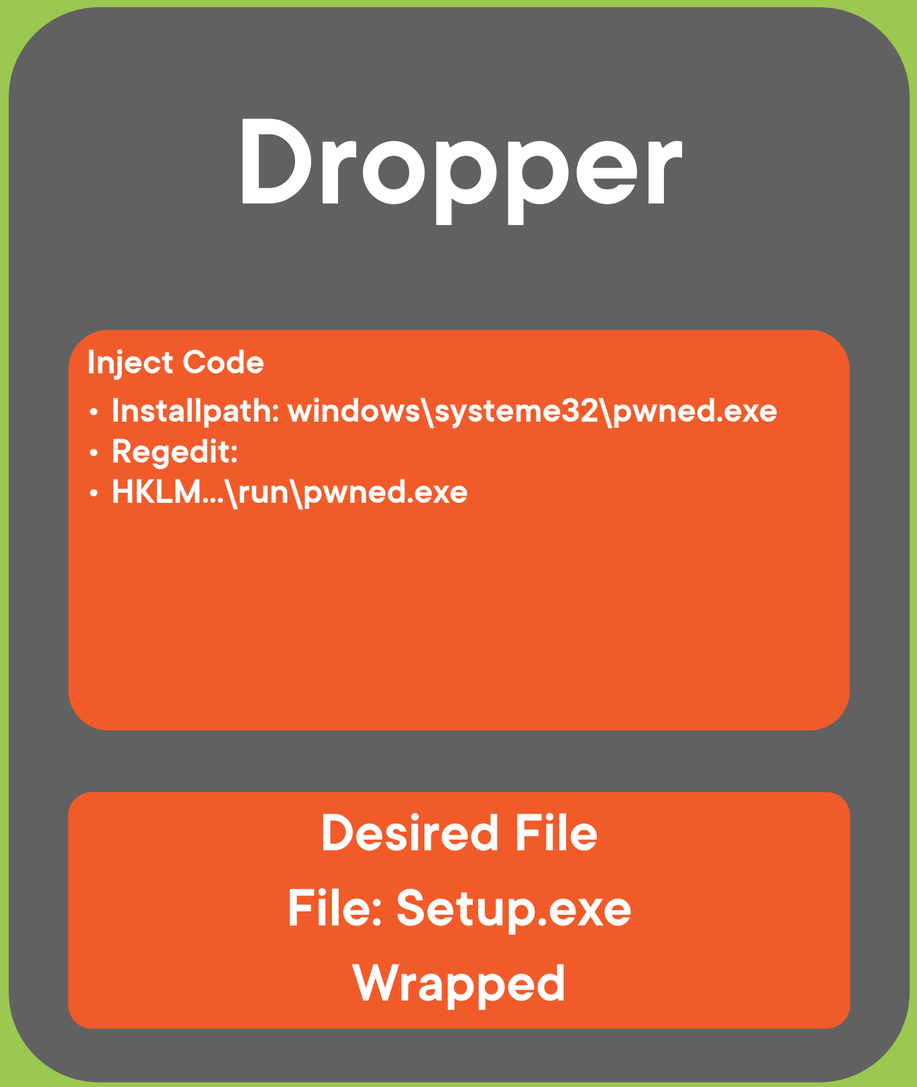
Step One

New Trojans have a higher chance of succeeding in compromising the target system, as the security mechanisms often fail to detect them

Create your monster by using various tools or a script

Step Two

A Dropper appears to users as a legitimate application or a well-known and trusted file.



Step Three

Multiple files can be combined together as well

Use a Wrapper to connect the Trojan to a legitimate file

Step Four

Employ a crypter

Step Five

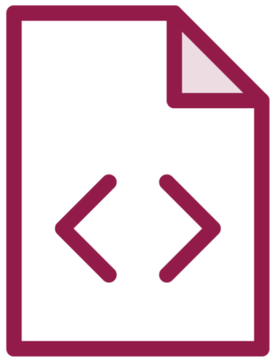
Propagate the Trojan

Step Six

Execute the damage routine

Infection

Why just telling people not to click on a link won't work?



Click on a File

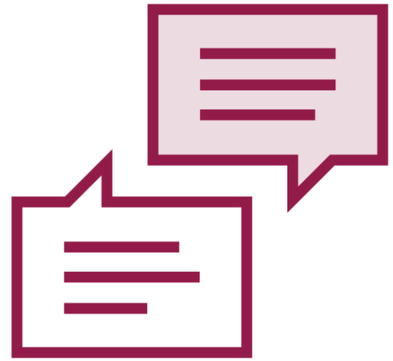
Adult materials

Screen saver

Email Attachment

Actual files

Links to files



Socially Engineered

Pop-up ads

Yes/no

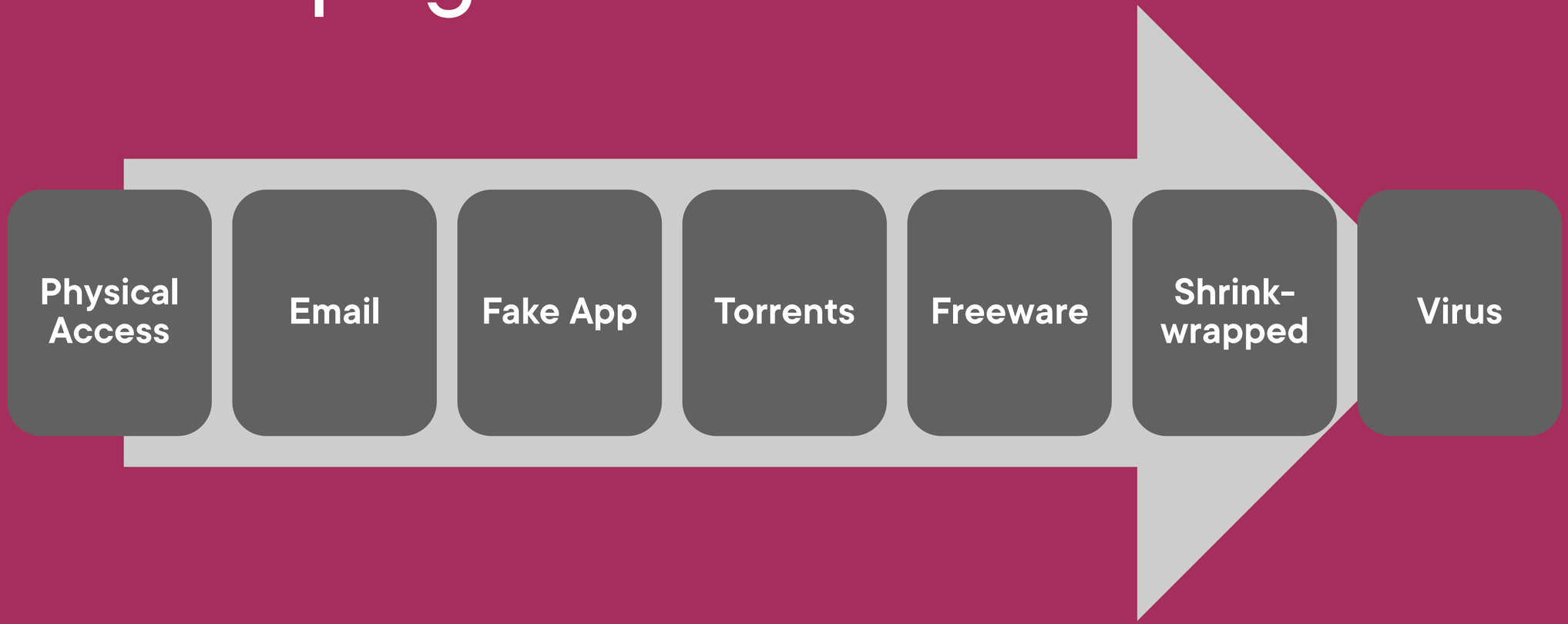
Demo

Using SET to create a trojan

Transmitting a Trojan Package

Step Five

Propagation



Evading Anti-virus

Important to Know

- Change checksum
- Write your own
- Use a hex editor
- Break the Trojan into multiple files
- Modify the syntax
- Avoid ID's Trojans

Demo

Create a Trojan

Learning Check

Learning Check

- Wrapper
- Dropper
- Crypter
- Shrink-wrapped
- Break up into multiple files

Up Next:
Describing the Types of Trojans