Explaining Trojans

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

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

Pay no attention to that man behind the curtain!

Oz

Trojans up Close

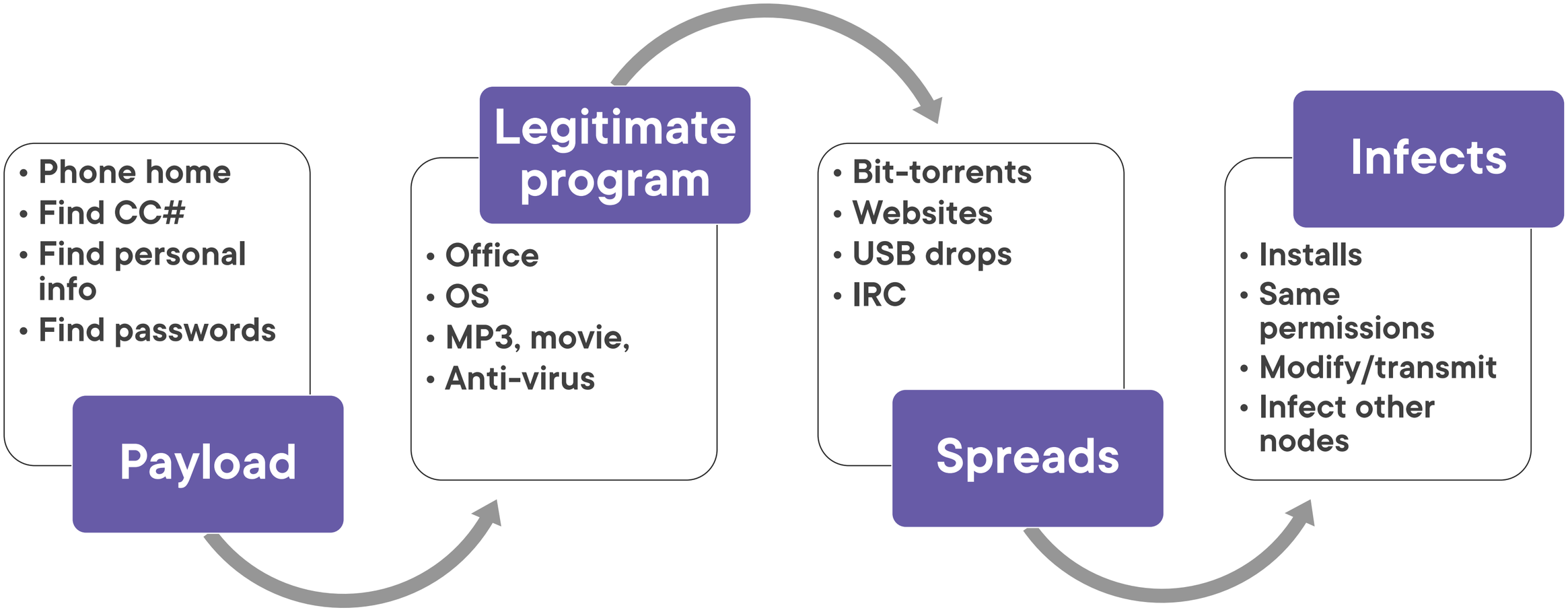
Trojan

A program in which malicious or harmful code (called a payload) is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage.

Typically contains spyware, keyloggers, rootkit, or other executables

Can relay or steal data

Trojan Lifecycle



What's the Goal?

Here's the Endgame

Disable firewalls

Replace or delete OS files

Open a backdoor

Disable Anti-virus

Turn the target into a proxy

Add to a Botnet



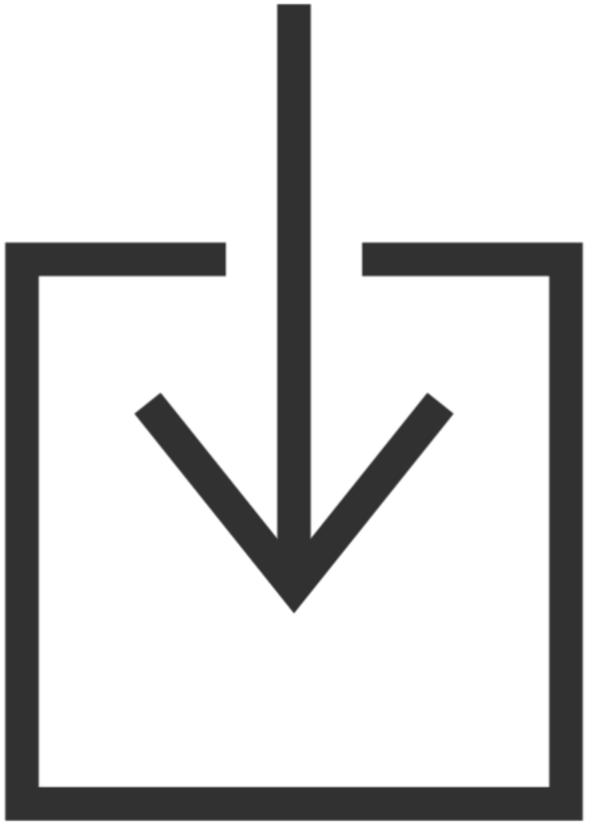




Here's the Endgame

Generate bogus traffic for DoS

Download & install spyware, adware, and malware



Here's the Endgame

Generate bogus traffic for DOS

Download & install spyware, adware, and malware

Grab screenshots

Record video from camera

Steal passwords, codes, financial, and personal data

Use target for spamming

How Trojans Communicate and Hide

Now You See Me - Now You Don't

Overt Channel
The file everybody wants
The latest and greatest

Covert Channel
Hidden path

So Many Ports, So Little Time

Port	Trojan	Port	Trojan	Port	Trojan
20/22/80/443	Emotet	1807	SpySender	8080	Zeus, Shamoon
21	Blade Runner, DarkFTP	1863	XtremeRAT	8787/54321	Backoffice 2000
22	SSH RAT, Linux Rabbit	2140/3150/6670-71	Deep Throat	10048	Delf
23 EliteWrap	EliteWrap	5000	SpyGate RAT, Punisher RAT	10100	Gift
68	Mspy	5400-02	Blade Runner	11000	Senna Spy
80	Ismdoor, Poison Ivy, Executioner	6666	KillerRat, Houdini RAT	11223	Progenic Trojan
443	Cardinal RAT gh0st RAT, Trick Bot	6667/12349	Bionet, Magic Hound	12223	Hack'99 KeyLogger

Demo

What ports are listening?

Indicators You Have a Trojan

Indications of a Trojan Attack

- **Updates denied**
- **Restarts/Shutdowns**
- **Task Manager won’t launch**
- **Screensavers**
- **CTR-ALT-DEL not working**
- **Taskbar disappear**

Indications of a Trojan Attack

- **Display altered**
- **DVD drive**
- **Windows Start button disappears**
- **Printer starts printing documents**
- **Redirections**
- **Hard drive activity**

Indications of a Trojan Attack

- Web pages open
- Data is corrupted
- Contacts are spammed by an unknown user
- Backgrounds change
- Date/time changes
- Amazon orders going to Dale Meredith ;-)

Learning Check

Learning Check

- **Overt channel**
- **Covert channel**
- **Overt**

Up Next:
Diving Deeper into Trojans