

# Ethical Hacking: Malware Threats

---

## The Hard Truth Behind Malware

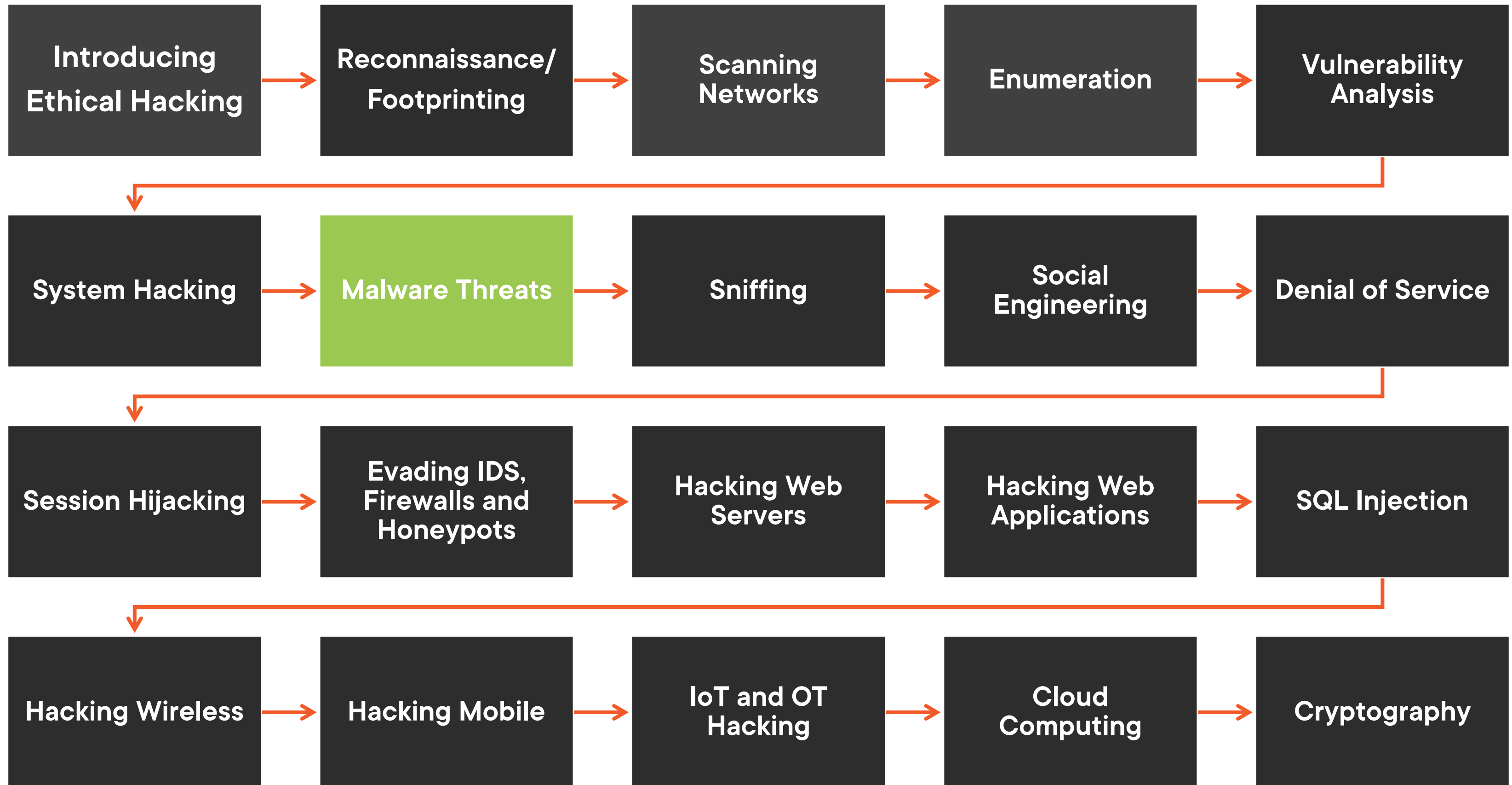


### **Dale Meredith**

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

[dalemeredith.com](http://dalemeredith.com) | [Twitter: @dalemeredith](https://twitter.com/dalemeredith) | [Linkedin: dalemeredith](https://www.linkedin.com/in/dalemeredith)

# Ethical Hacking Series



# The Hard Truth Behind Malware

---

# Complacency Mindset



The first step toward change is awareness. The second step is acceptance.

**Nathaniel Branden**

What are you going to do about it?



# A Course Everyone Should Watch

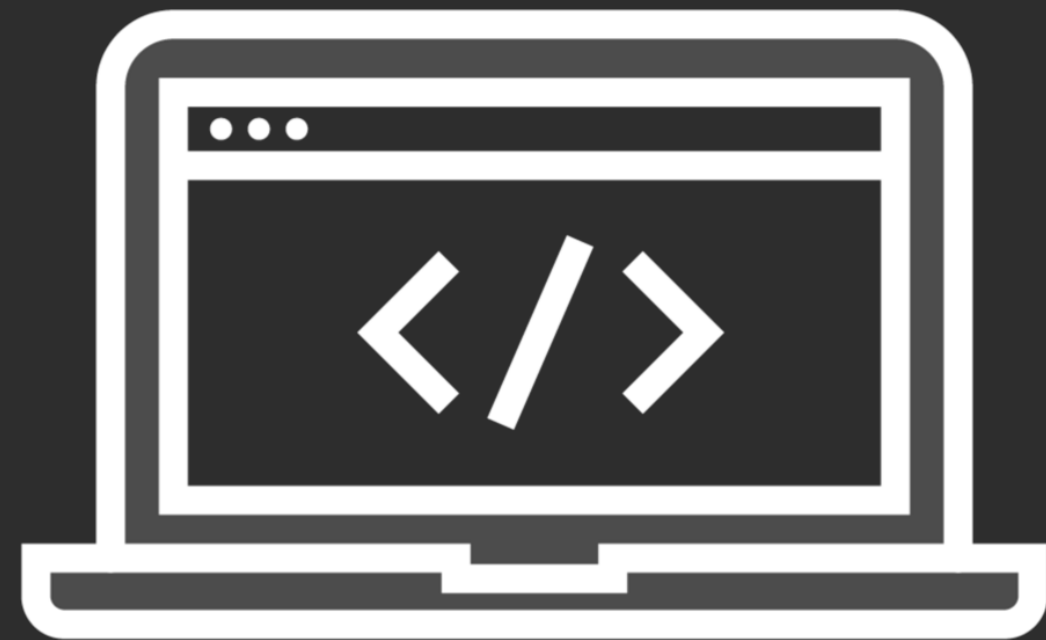




# What Is Malware?

---

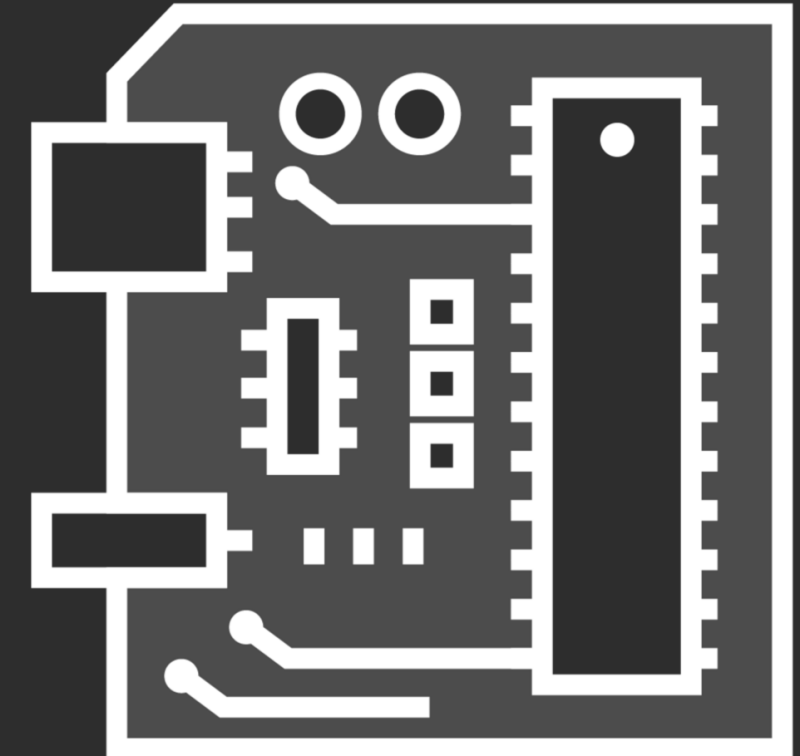
# Let's Break It Down



**Software or program  
that performs  
malicious actions**



**Malicious + software  
=malware**



**Infects any device**

# Let's Break It Down



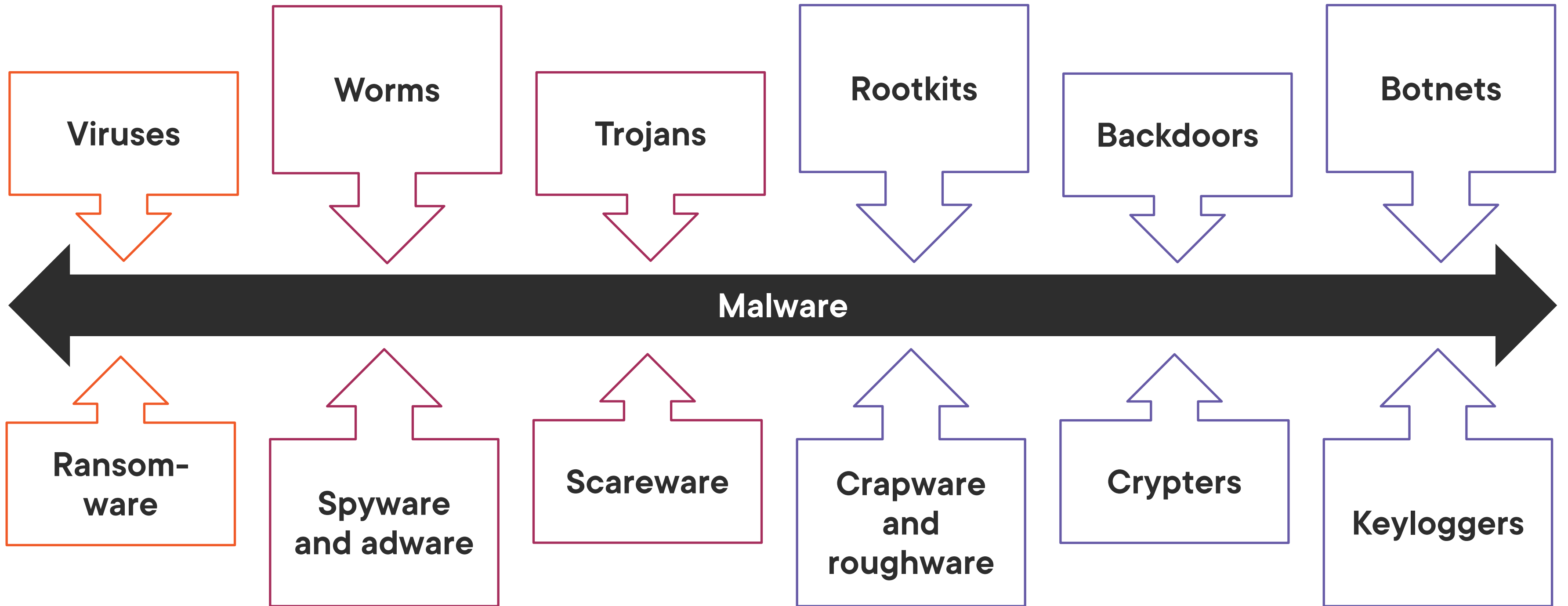
**Everyone's a target**



**Motivated by money**



**Comes in various forms**



# Goals of Malware



**Steal data**

**Harvest usernames and passwords**

**Use your resources**

# Other Malware Uses

**Attack browsers and  
websites visited**

**Degrades system  
performance**

**Cause hardware  
failure**

**Erase valuable data**

**Attack other  
systems from the  
compromised  
system**

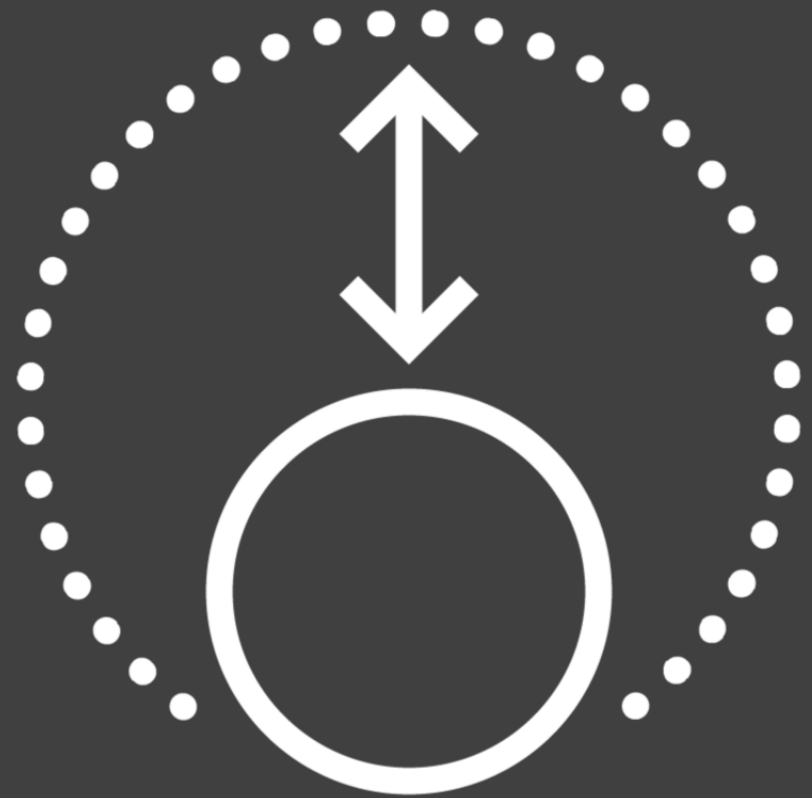
**Spam inboxes**

# Key Targets

**Individuals**

**Organized crime**

**Governments**



**Has a snowball effect**



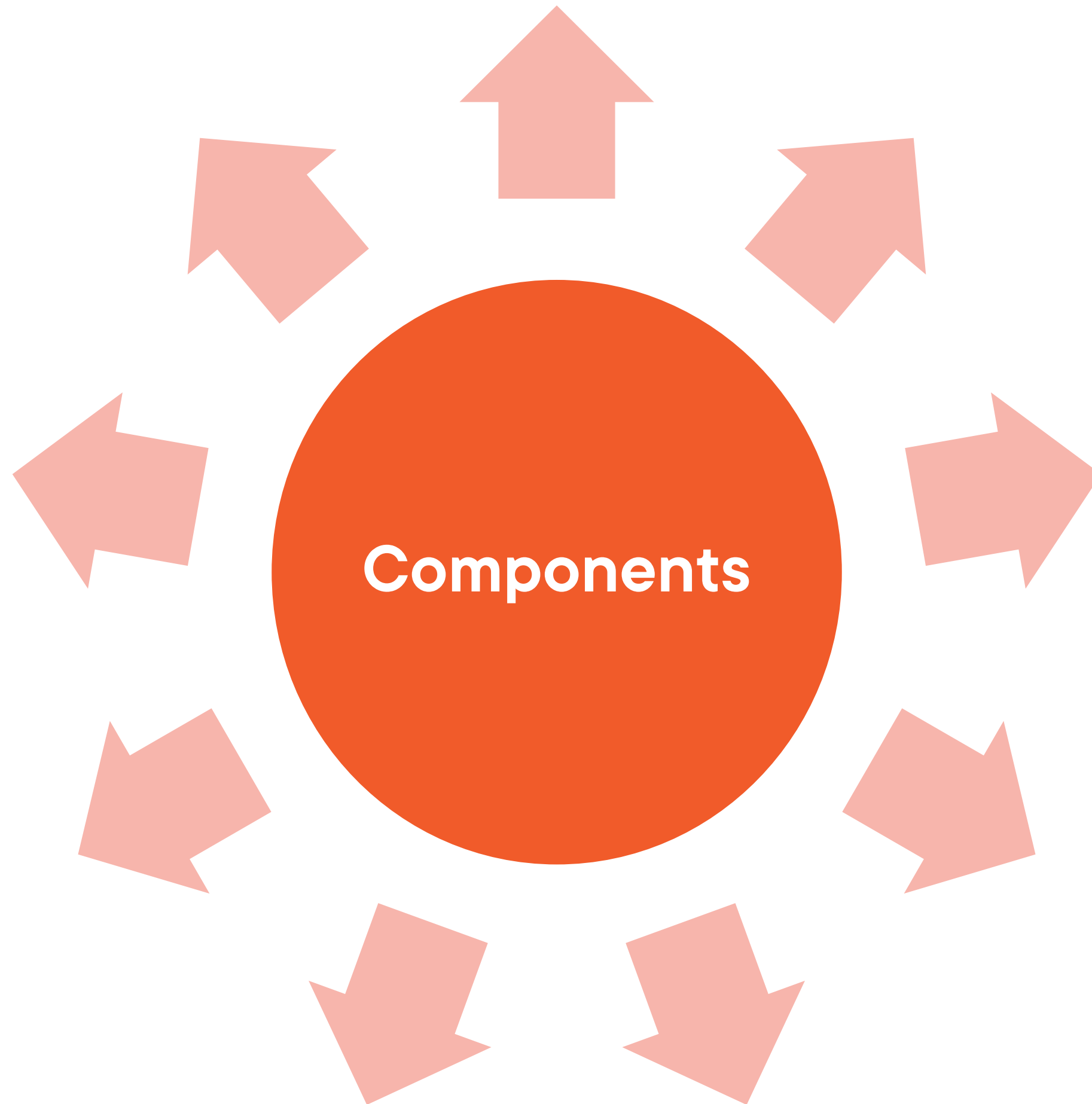
**Creates full-time jobs**

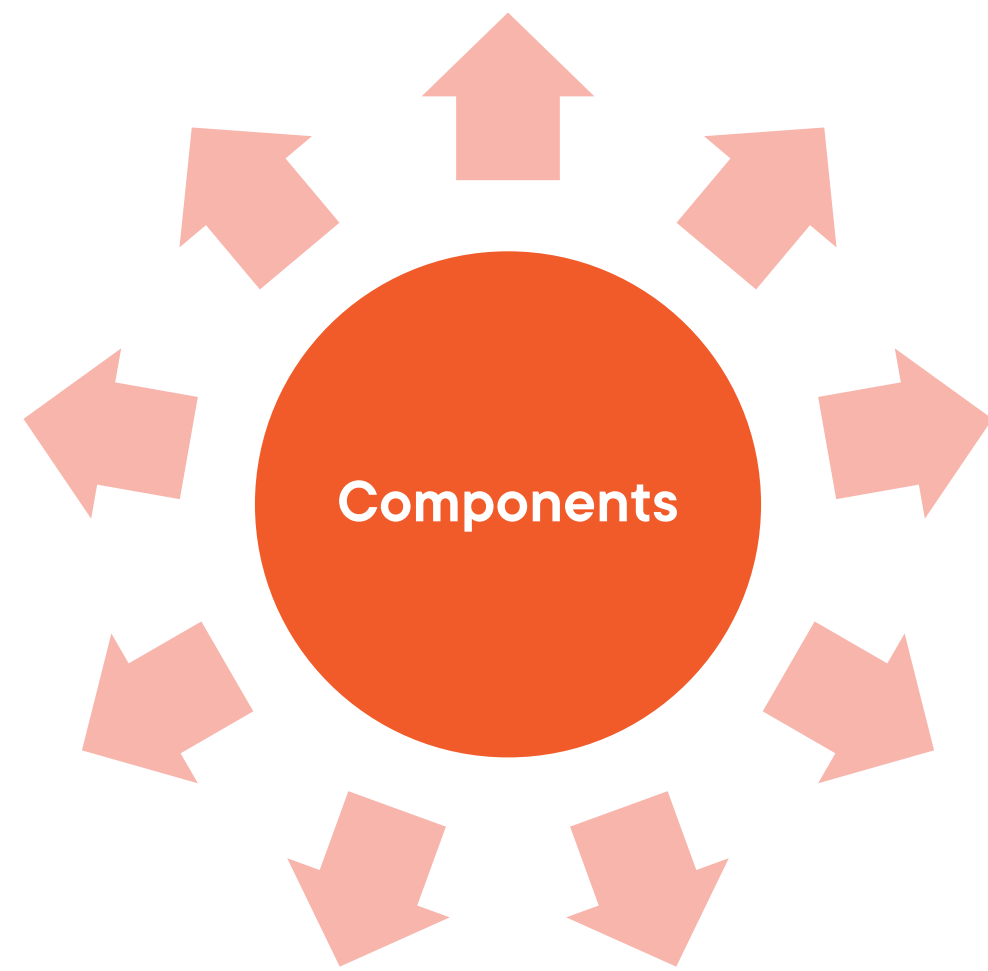


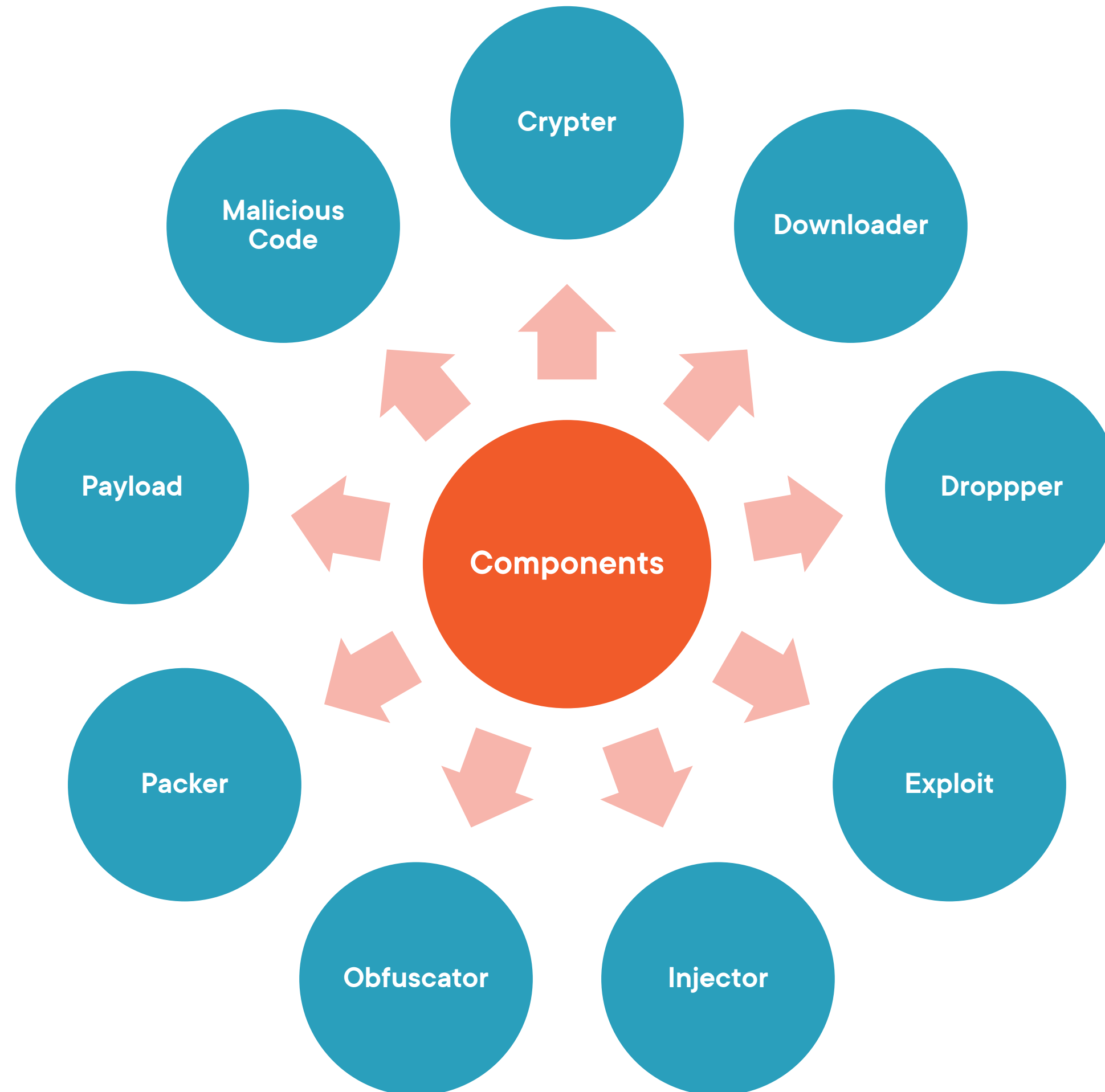


# Malware Components

---







# How Malware Gets in a System

---

How does malware get in  
a system?



# Types of Malware

**1**

**Propagation**

**2**

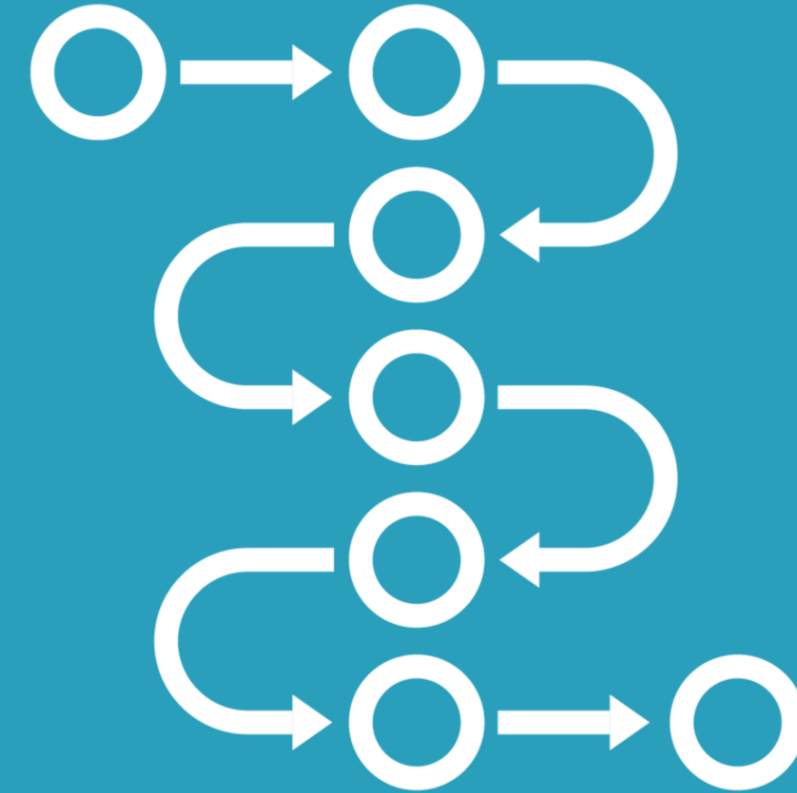
**Concealment**

# Examples of Propagation Malware



## **Virus**

Human assisted



## **Worms**

Automatic: No human needed

# Examples of Concealment Malware



## **Rootkit**

Modifies the OS to hide



## **Trojan**

Code hidden inside a file

# How Malware is Deployed

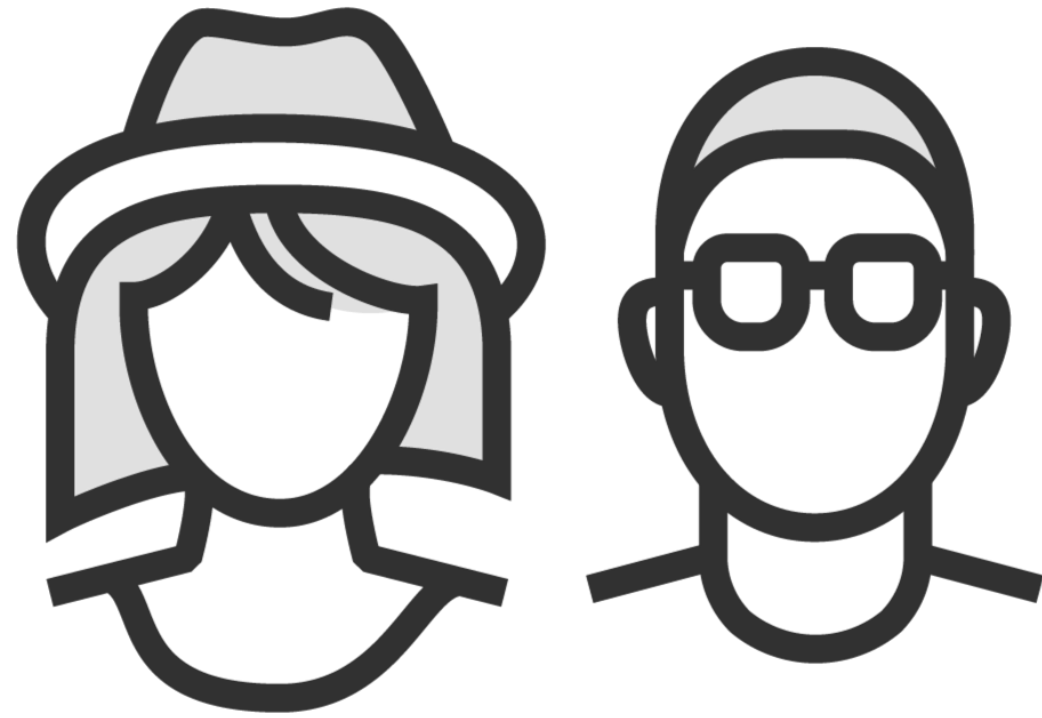
**Insider Attack**

**Backdoor**

**Logic Bomb**

**Omega Bomb**

# Insider Attack



**Employee(s)**

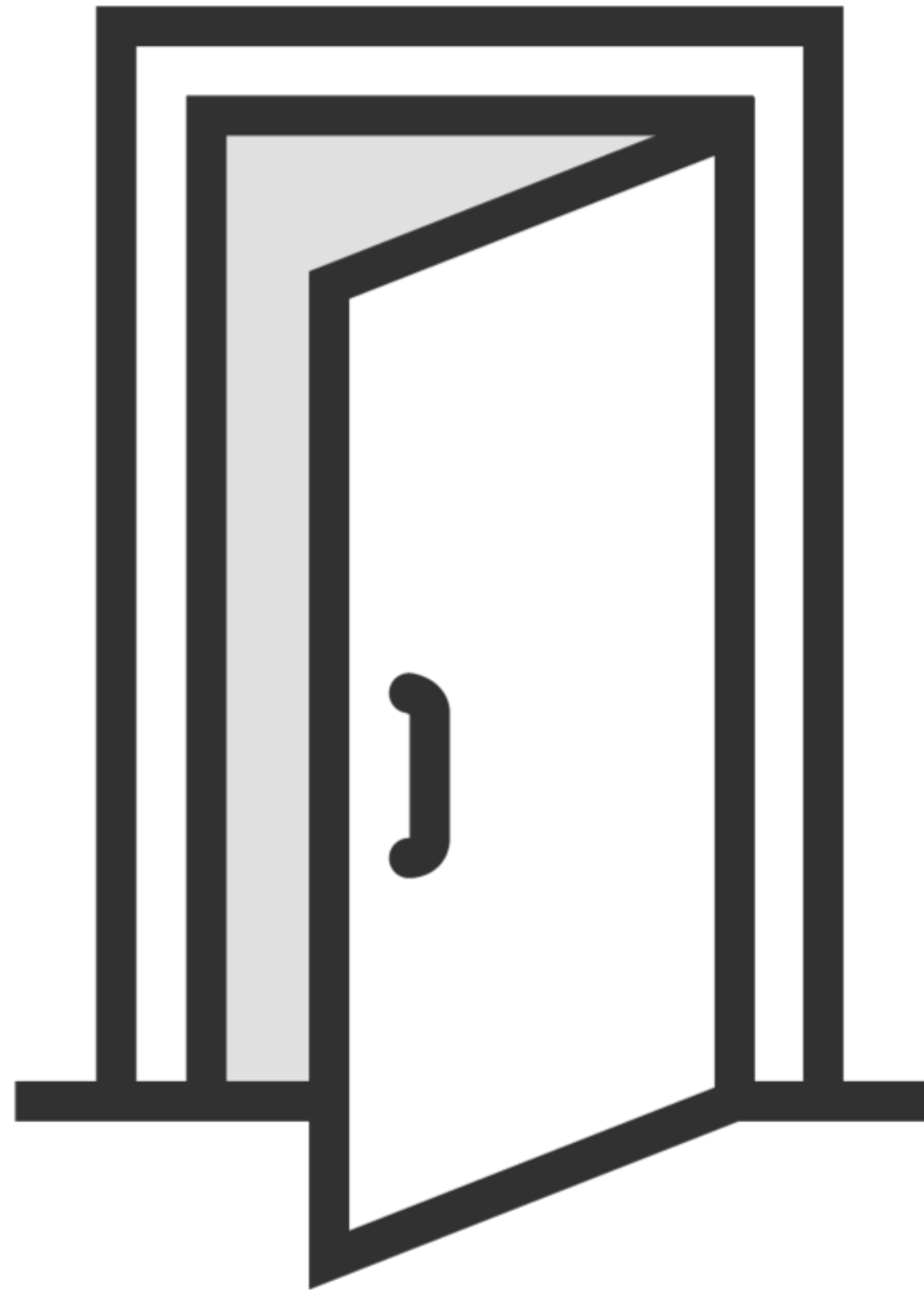


**Contractor or Vendor**



**IT Personnel**

# Backdoor



**Trapdoor**

**Hidden feature**

**Program runs as expected until the backdoor  
is activated**



# Logic Bomb



**A set of instructions is secretly incorporated into a program so that if a particular condition is satisfied, it will be carried out**



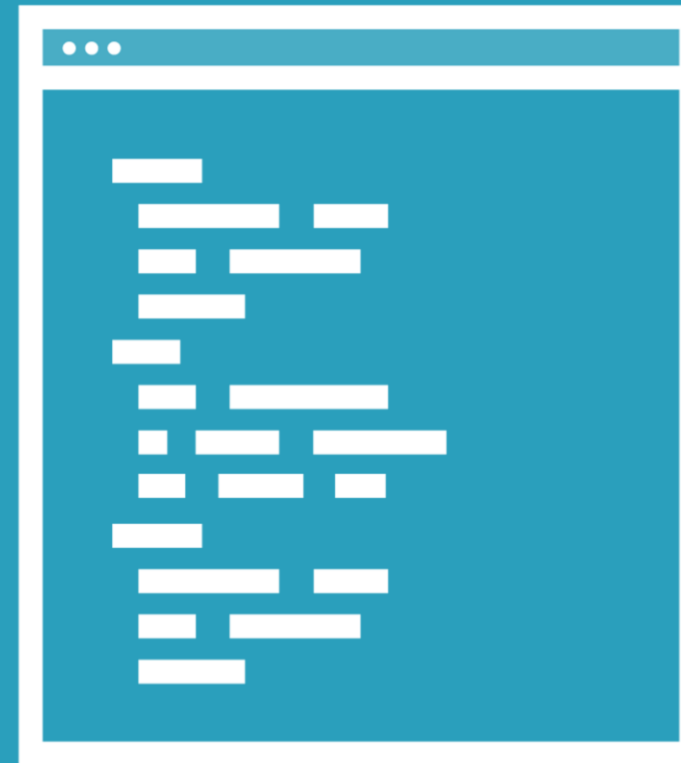


# Omega Bomb

# Hacking Time Bomb

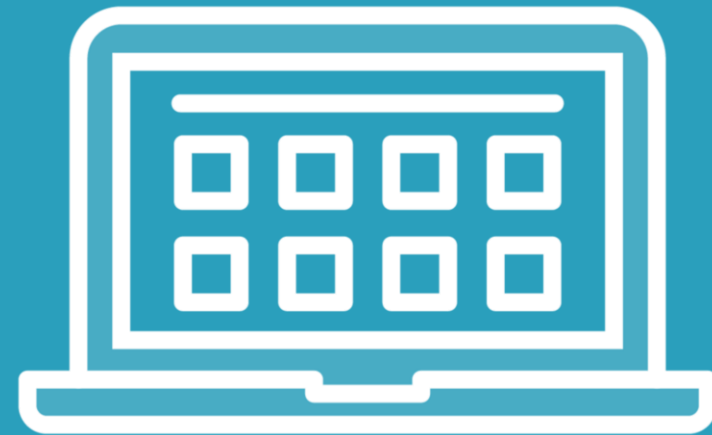


# Hacking Time Bomb



Delete  
everything

# Hacking Time Bomb



# Deployment Techniques

---

# How Malware Enters a System



**Untrusted sources, sites and free software**



**During Installation**



**Propagation**

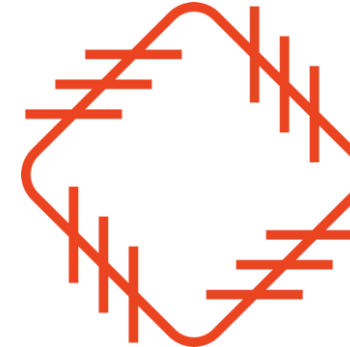


**Not updating anti-software tools**

# How Malware Enters a System



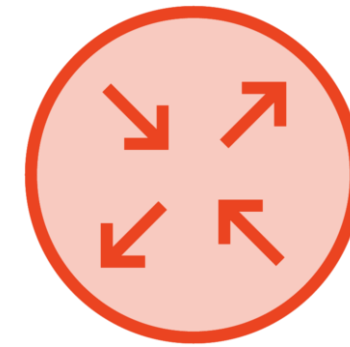
**Instant messenger applications**



**Insecure patch management**



**Removable devices and portable media**



**Decoy applications**



**Browser and email software bugs**



**Downloading files**

# How Malware Enters a System



**Installed by other  
malware**



**File sharing**



**Email attachments**



**Bluetooth and wireless  
networks**

# Common Techniques to Distribute Malware



# Give Me a Sign



**Look at your processes**

**Does it have a icon**

**Is it a reputable description**

**Does the process running live in the right place**

**Unique URL's**

**Are there any open TCP/IP endpoints**

Let Me Show You What I Mean

Demo



**Task Manager**

**Process Explorer**

# The Numbers Behind Malware

---

Why is Malware so popular?



**Average number of malware alerts: 20,000 wk**

Just 4% of alerts are investigated

**Average total cost of ransomware breach: \$4.62m**

Payments average around \$150,000

Businesses of all sizes are being attacked

**71% of companies have been hit**

**61% disrupted business**

**60% understaffed**

**Mobile is a key target**

**28% of malware products are VM aware**

# IT Admins Report

**75%**

**Installed by end-users**

**71%**

**Have protection in place**

**39%**

**Audit less than once a year**



# End-users

**60%**

**Afraid of losing their data**

**51%**

**Concerned about online fraud**

**43%**

**Aren't current on security updates**



**Pirated  
Software**

# Learning Check

---

# Learning Check



**Logic bomb**



**Cypter**



**Downloader**



**Dropper**



**Exploit**



# Learning Check



**Packer**



**Payload**



**Insider attack**



**Drive-by downloads**



**Black hat SEO**



Up Next:

Discussing Advanced Persistent Threats  
(APT)

---