

Describing the Types of Trojans



Dale Meredith

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

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

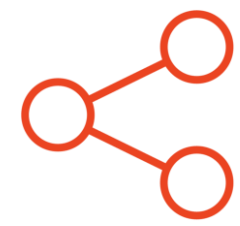
Would you say I have a plethora of piñatas?

El Guapo

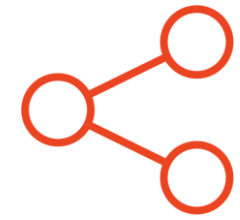


Dale's Top 10

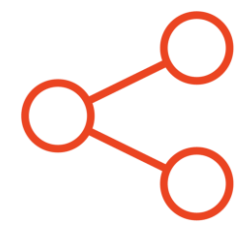
Notification



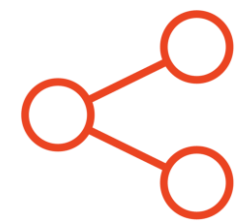
IRC



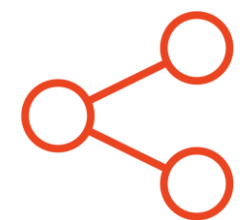
PHP



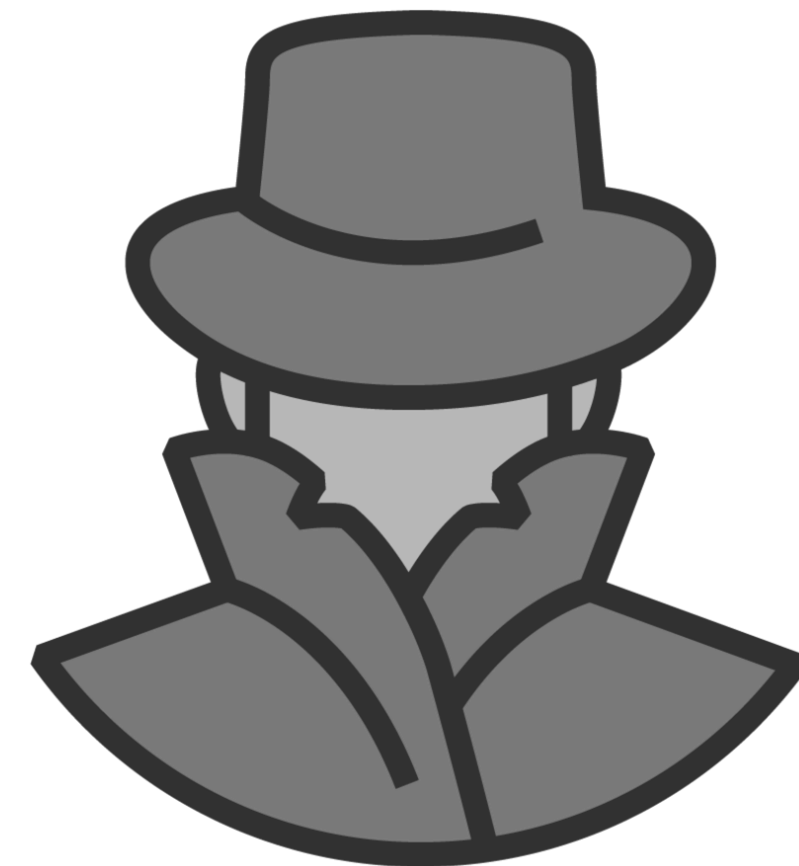
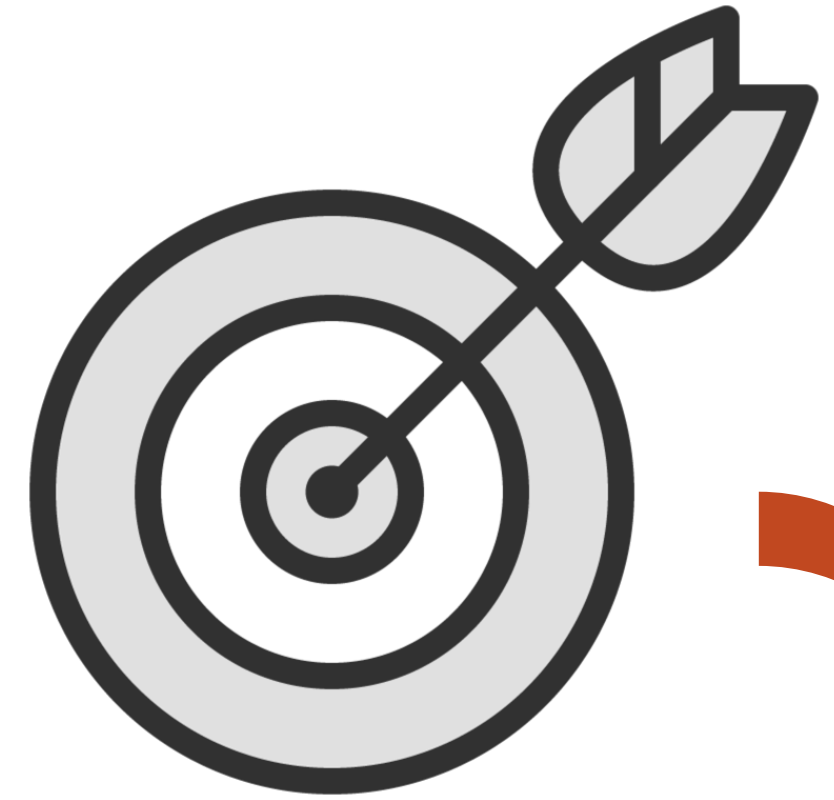
Net Send



ICQ

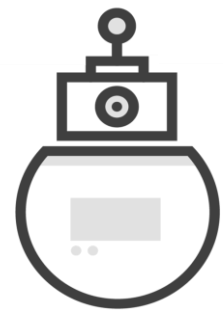


Email



Botnet

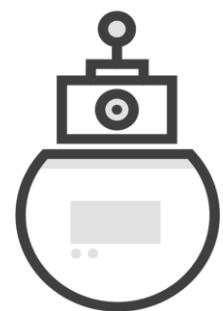
Also known as 'bot herders'



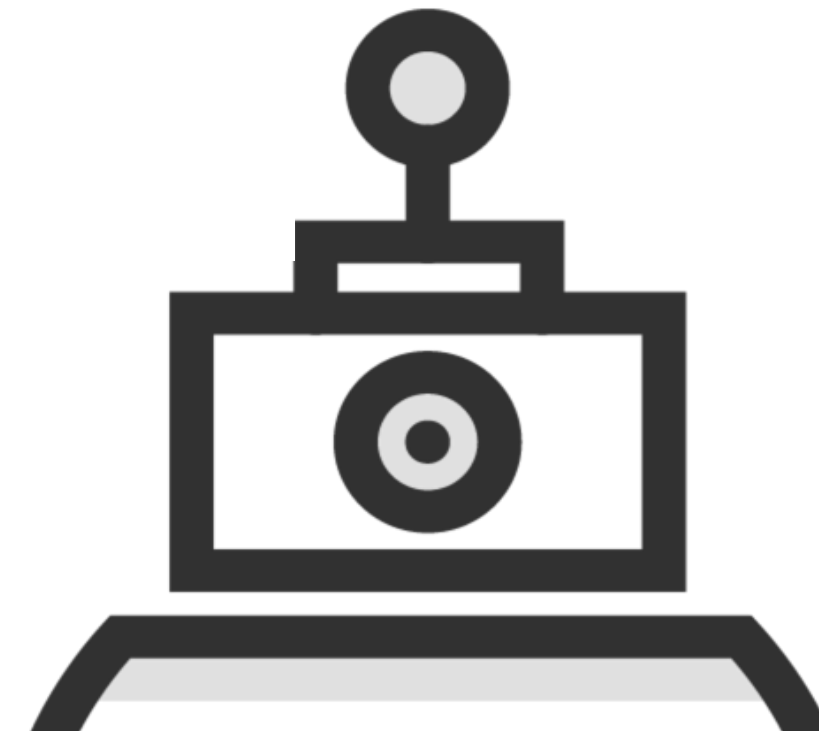
Collection of pwned systems



Education, government, and military



DOS, SMTP, and Click Fraud



Extortion-ware

Proxy Server



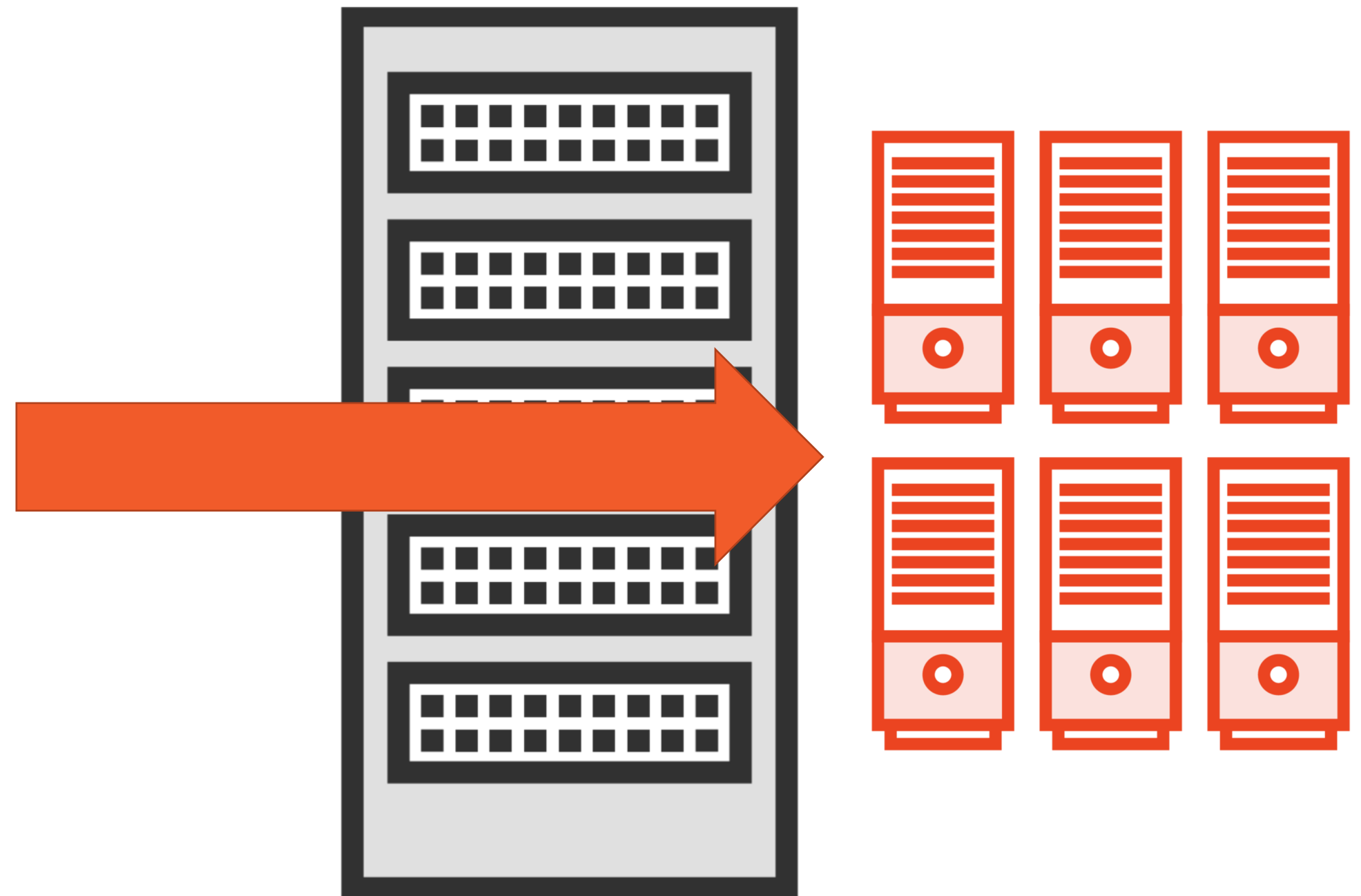
Loaded on the target



Target proxies out



Creates a proxy chain



FTP Server

Installs a FTP Server

**Sends remote
connection info**

Full access



Confidential Information



VNC



Uses a VNC server



VNC is a utility



Create your own VNC

HTTP/HTTPS



Creates a tunnel



Ports 80/443

HTTP/HTTPS

Executed on an internal host and spawns a child program which is a user to the firewall

The child program executes a local shell that appears as a legitimate HTTP request and sends it a ready signal

The programs are typically small; the master and slave programs consist of only 260 lines per file

HTTP/HTTPS



Creates a tunnel

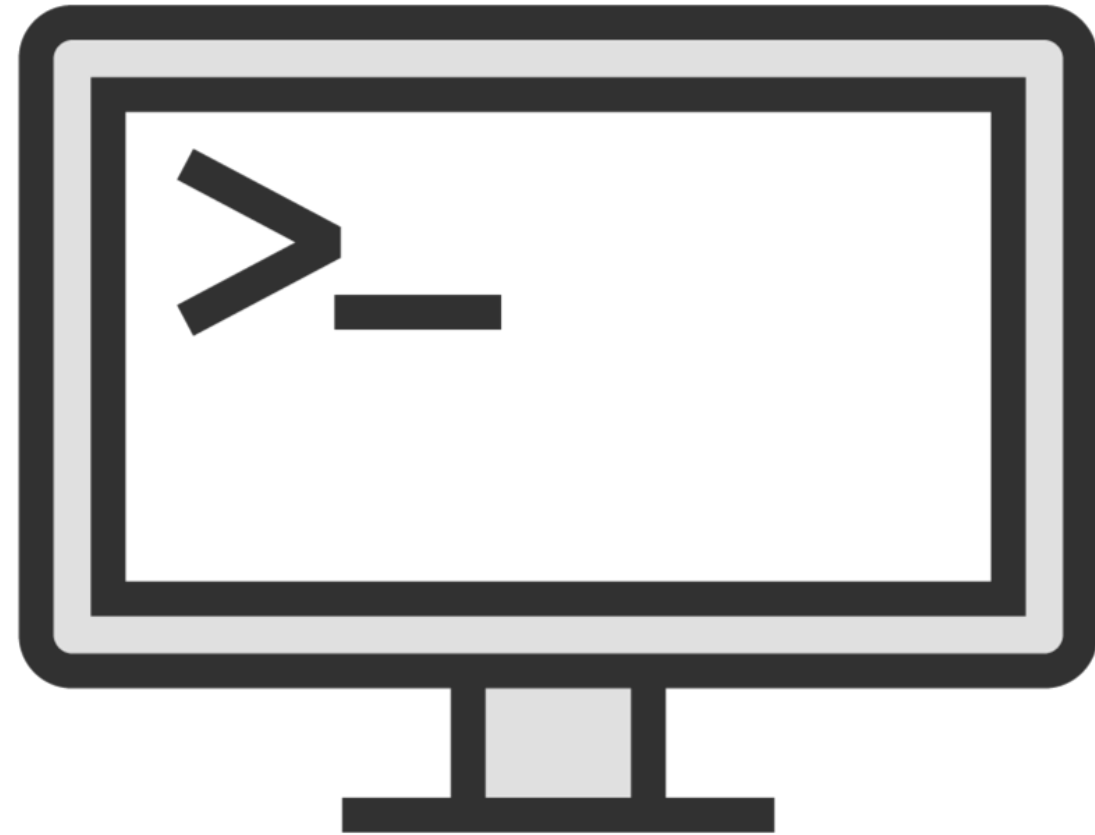


Ports 80/443



Traffic is converted Base64

Command Shell



DNS Messenger and GCat are some of the latest commands shell Trojans

Document

Embeds inside a document



Transmitted via email

Commonly found in PDF Documents

Email



Opening executes



**Command is sent via
the email**



**Executes apps, and
open files**

RAT

Remote Access Trojan

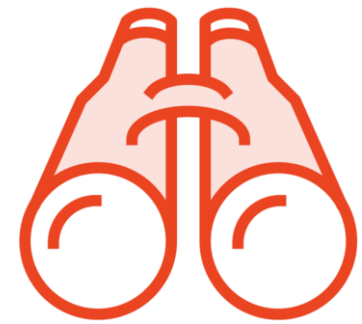
Back Orifice / NetBus

Loads smaller apps (server side)

njRAT and FatalRAT



RAT



Screen and camera capture



Password sniffing



Code execution



Download and execute malware



Keylogging and file access



Execute shell commands

That completes Dale's
top 10

More to come..

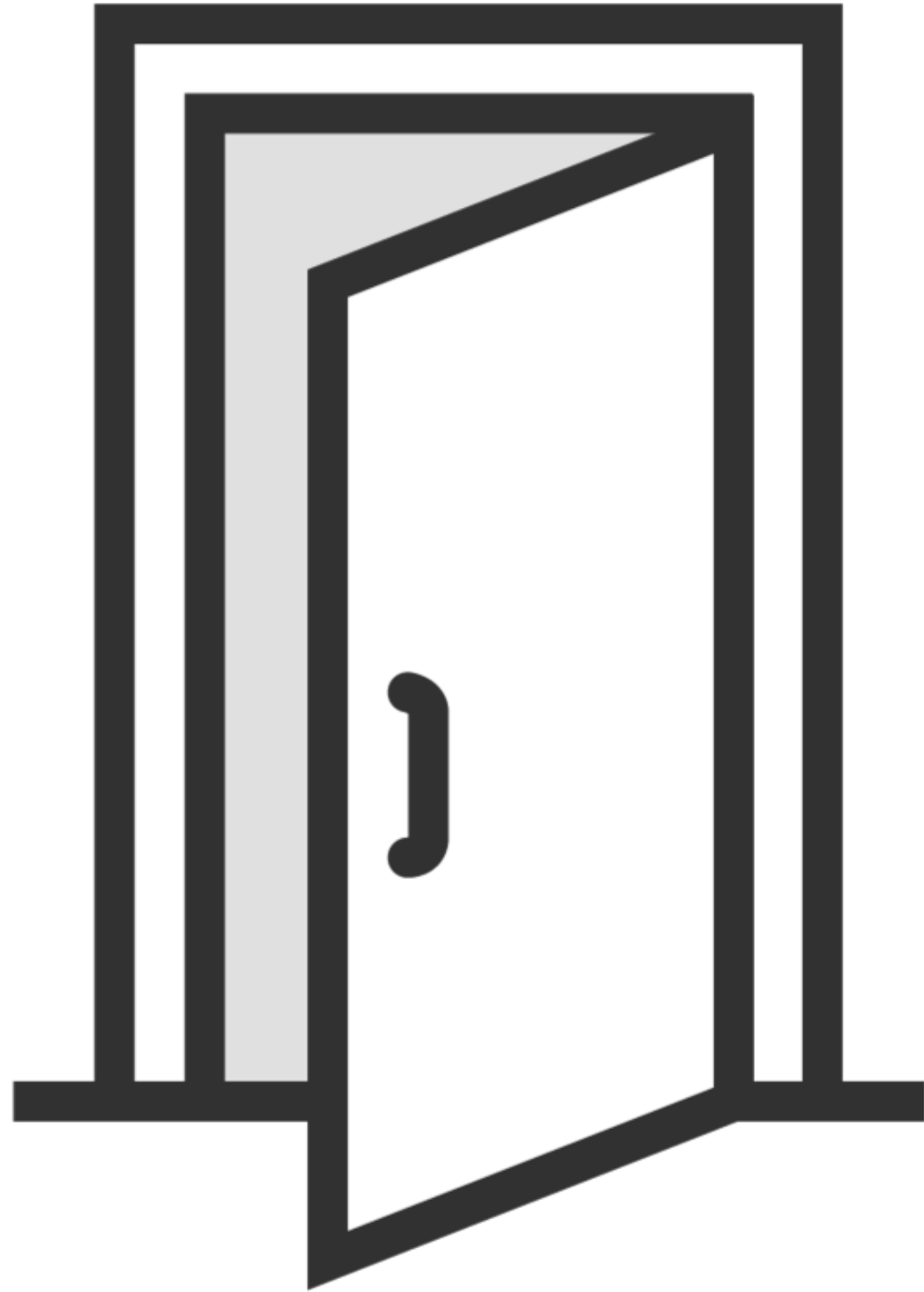
More Trojans



Backdoor Trojans

A program that can bypass the
standard system
authentication or conventional
system mechanisms, without
being detected.

What's The Difference?



PoisonIvy

Consists of a graphical user interface, and the backdoors are small

Once executed it copies itself to the Windows folder or the
Windows/system 32 folder

Some variations copy themselves into alternate datastreams (ADS)

Did you hear what I just said?

Other Backdoor Trojans

Kovter

POWERSTATS v3

ExtraPulsar

RogueRobin

ServHelper

**SpeakUp linux
backdoor**

Winnti backdoor



RANSOMWARE

RANSOMWARE

Ransomware

Ransomware spreads as a Trojan and enters a system through:



Email attachments



Hacked websites



Infected programs and app downloads



Vulnerabilities in network services

Ransomware

Locky

WannaCry

Petya

NotPetya



Cerber

CryptXXX

CTB-Locker

CryptorBit

Sodinokibi

CryptoLocker

BitPaymer

Police-themed



E-banking Trojans



Extremely dangerous and are a significant threat to online banking



Installed through malicious email attachments or advertisements



Programmed to steal minimum and maximum amounts to avoid suspicion



E-banking Trojans

How they work

TAN Gabber

HTML Injection

Form Grabber

Covert Credential Grabber

E-banking Trojan Methods

Keylogging

**Form data
capture**

**Fraudulent form
fields**

**Screen capture
and recording**

**Mimicking
financial sites**

**Redirecting to
banking sites**

**Man-in-the-
middle attack**

Mobile and IoT Trojans

Mobile Trojans



Mobile Trojans



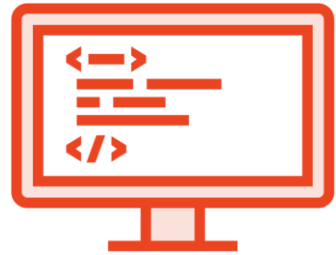
Attacks banking credentials, social networking credential stealing, data encryption and device locking

BasBanke

IoT Trojans



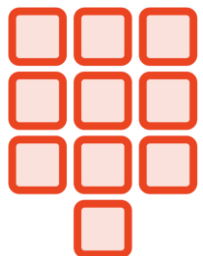
IoT Trojans



Malicious programs that attack IoT networks



Leverage a botnet to attack other machines outside the IoT network



Using anti-Trojan software and updating usernames and passwords can help to prevent IoT Trojan attacks

Silex BrickerBot

Satori

Torii botnet

Miori IoT Botnet

Bashlite IoT Malware

Gafgy Botnet



Time to Review

Types of Trojans



Remote Access Trojans



Rootkit Trojans



Backdoor Trojans



E-Banking Trojans



Botnet Trojans



Point-of-Sale Trojans

Types of Trojans



Defacement Trojans



IoT Trojans



Service Protocol Trojans



**Security Software
Disabler Trojans**



Mobile Trojans



Destructive Trojans

Types of Trojans



DDoS Attack Trojans



Command Shell Trojans

Unlike viruses or worms, a Trojan does not self-replicate, so it needs to be installed by a valid user

Demo



Creating our own trojan using TheFatRAT

Learning Check

Learning Check



Botnet



Document trojan



No interface on backdoors



HTTP/s trojans



Doesn't self-replicate



Up Next:

Explaining Worms and Viruses
