Trojans – The Forgotten Enemy

Dave Chronister, CISSP, C|EH, MCSE, C|HFI

Managing Technical Partner

PARAMETER SECURITY

The Tao of Hackers

“It has the same basic rules, rules like gravity. What you must learn is that these rules are no different from the computer system. Some of them can be bent and others can be broken.” – Morpheus, The Matrix

Trojans:

The Forgotten Enemy

Parameter™

- History, Features, and Workings
- Demo - Creation and In Action
- Evasion and Spreading Methods
- Case Study

Trojans:

The Forgotten Enemy

History, Features, and Workings

Trojans:

What are They?

- A Client Server application which will bypass all security mechanisms
- Give a Malicious Attacker access to ALL aspects of the victim system
- The ultimate Spy-Ware
- R.A.T. – Remote Administration Tool

Trojans: What can they do?

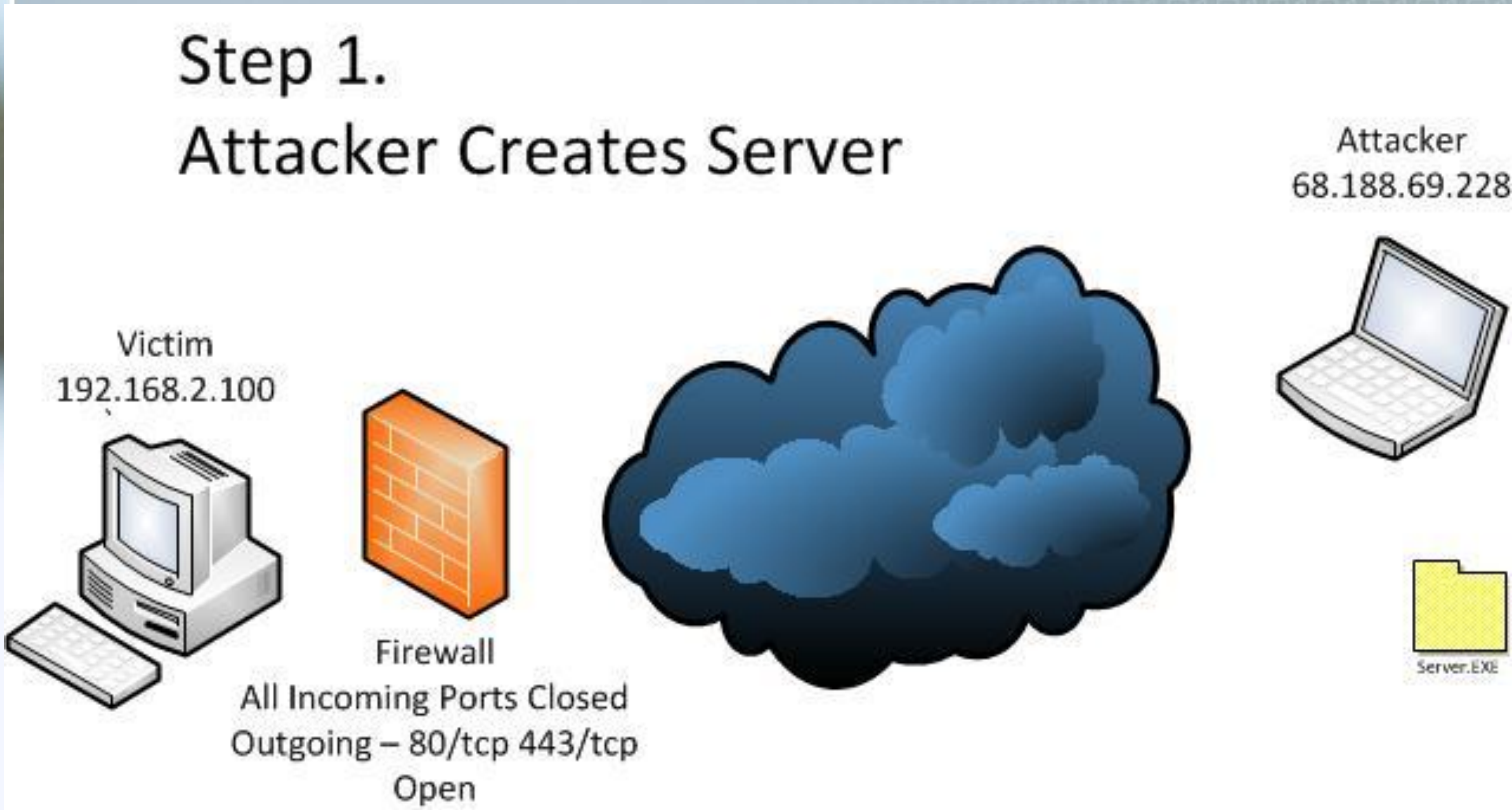
- Key logging
- File Explorer
- Web Cam Viewer
- Desktop Control
- Program Manager
- Geo Location
- “Freak”-ware
- Audio Recording
- “Bot” Features
- Much, Much More

Trojans:

What they are not….

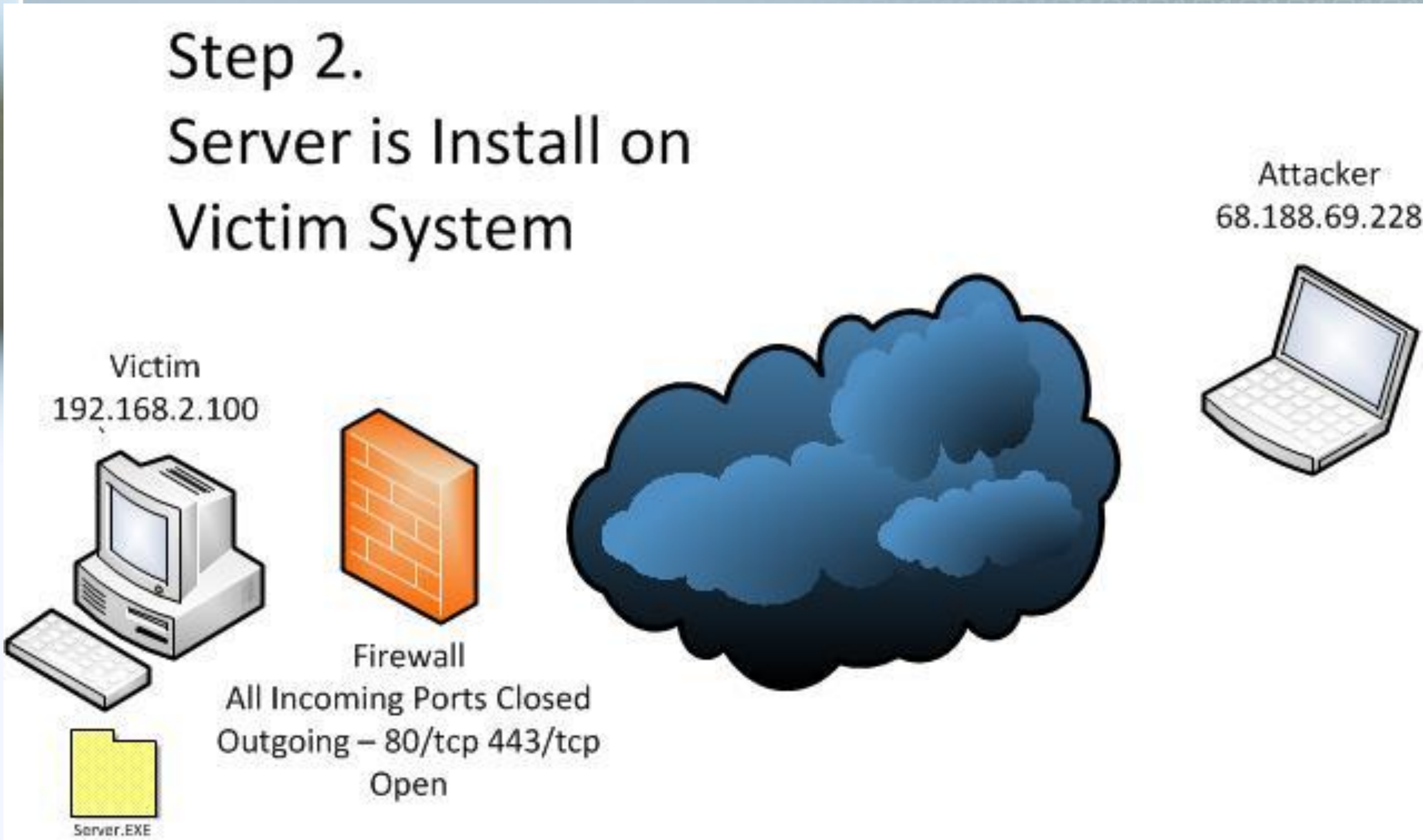
- Able to infect other files … Trojans are complete applications
- Spread via Self Propagation – Must be manually installed, spread via SE
- Noticeable when installed – Well programmed Trojans are small and undetectable

How they Function



Step 1.
Attacker Creates Server

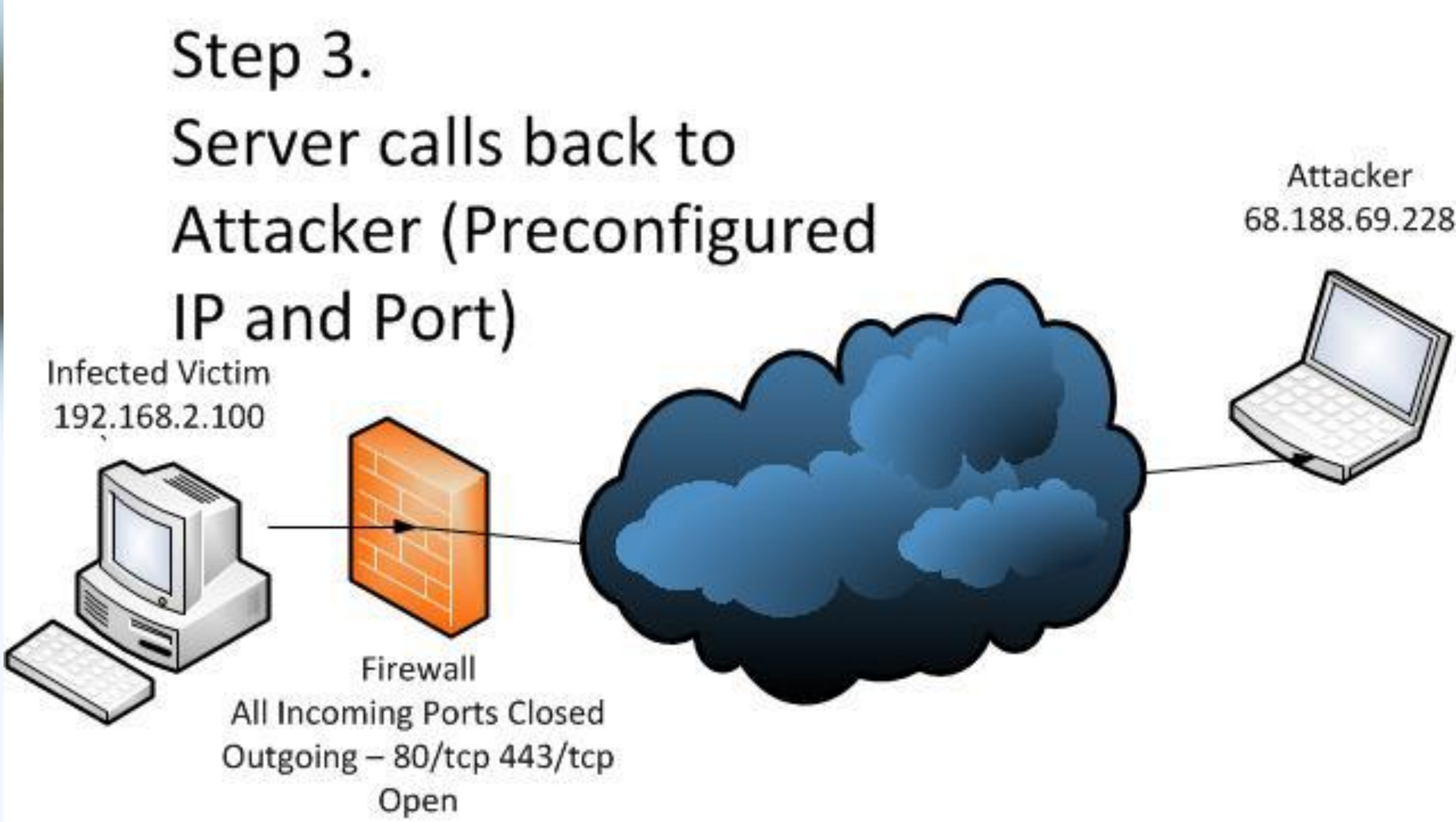
How they Function



Step 2.

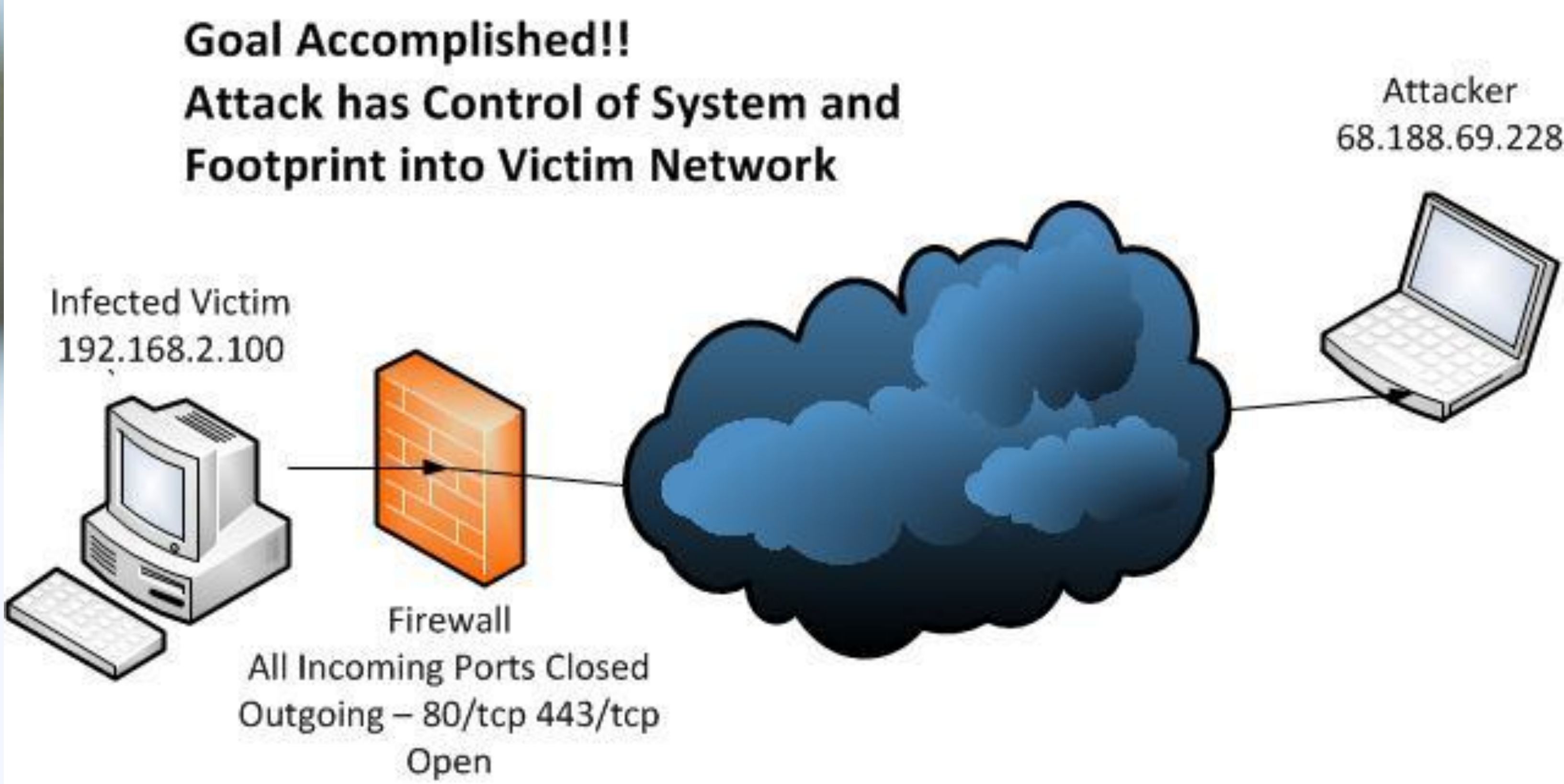
Server is Install on Victim System

How they Function



Step 3.
Server calls back to Attacker (Preconfigured IP and Port)

How they Function



Goal Accomplished!!
Attack has Control of System and
Footprint into Victim Network

Infected Victim
192.168.2.100

Firewall
All Incoming Ports Closed
Outgoing – 80/tcp 443/tcp
Open

Attacker
68.188.69.228

Code Injection

Installing is so 2000s

- Trojan is injected into Executables, DLLs, and even Kernels
- Methods include: API Hooking, Kernel Hooking, PE Loader Injection
- Helps bypass outbound firewalls

Demo:
Trojan Creation / Function

A/V Evasion Techniques

- Compile Modified Source Code
- Edit Server with HEX Editor
- Crypters – Commercially Available
- Packers – Executable Archive
- Purchase Undetectable Copy

Anti-Detection Techniques

- Virtual Machine Detection
- Sandbox Detection
- Anti-Sniffing
- Anti-Traffic Analysis

Trojans in the Wild

- P2P Networks
- 1px I-Frame in Advertisements
- Facebook Applications
- Smartphone App Stores

Trojan Case Study

- Company Infected – Hacker successfully logged in to bank accounts
- Company wiped systems and changed passwords for accounts
- Hacker logged in with new passwords less than a week later

Trojan Case Study

- Attacker Spread Trojan due to bad permissions for Domain User
- Detected Trojan “Signature” using Wire Shark and a Hub
- Filter Traffic at firewall and Wiped all machines infected
- Followed up for any possible covert channels.

Best to Prevent Infection

- Defense in Depth
- Wipe machines when suspected of being infected
- A/V installed and up to date (will stop Script Kiddies)
- END USER TRAINING!!!!!!!!!

Contact Info:

Parameter Security

dave.chronister@parametersecurity.com

314.442.0472

223 Salt Lick Road | Suite 220 | St. Peters, MO | 63376