Splinter the RAT Attack:

Create Your Own Botnet to Exploit the Network

Solomon Sonya

@Carpenter1010

"Sometimes, the problem becomes more tractable when presented with the solution"

DISCLAIMER!!!

This project is meant for educational purposes only. Views, concepts, techniques, knowledge, etc are that of the authors and do not represent our employers. This briefing is intended to strengthen network defense by highlighting the relative ease attack tools can be built such that network security professionals gain greater awareness to audit networks and secure computer systems. Only execute concepts presented here on isolated networks of which YOU have express permission to conduct these assessments. We are not liable for damages resulting from concepts or tools discussed in this presentation. Use at your own risk!

What to Expect

- Background, Intent, and Motivation
- Botnet Overview (Characteristics and Features)
- System Exploitation Overview

Live Demo Gremlin…

http://logout.hu/dl/upc/2011-06/230806_gremlin_in_my_computer-lyvind_berget.jpg, Retrieved 17 Sep 13

- How to Create your Botnet!
  - Remote Code Execution
  - Bypassing Infrastructure Security
  - Establishing a Beacon Bot
  - Payload Migration for Advanced Exploitation
- Advancing the Attack
- Live Demos
- Conclusion and Questions

Research Motivation

Network Defense is Behind

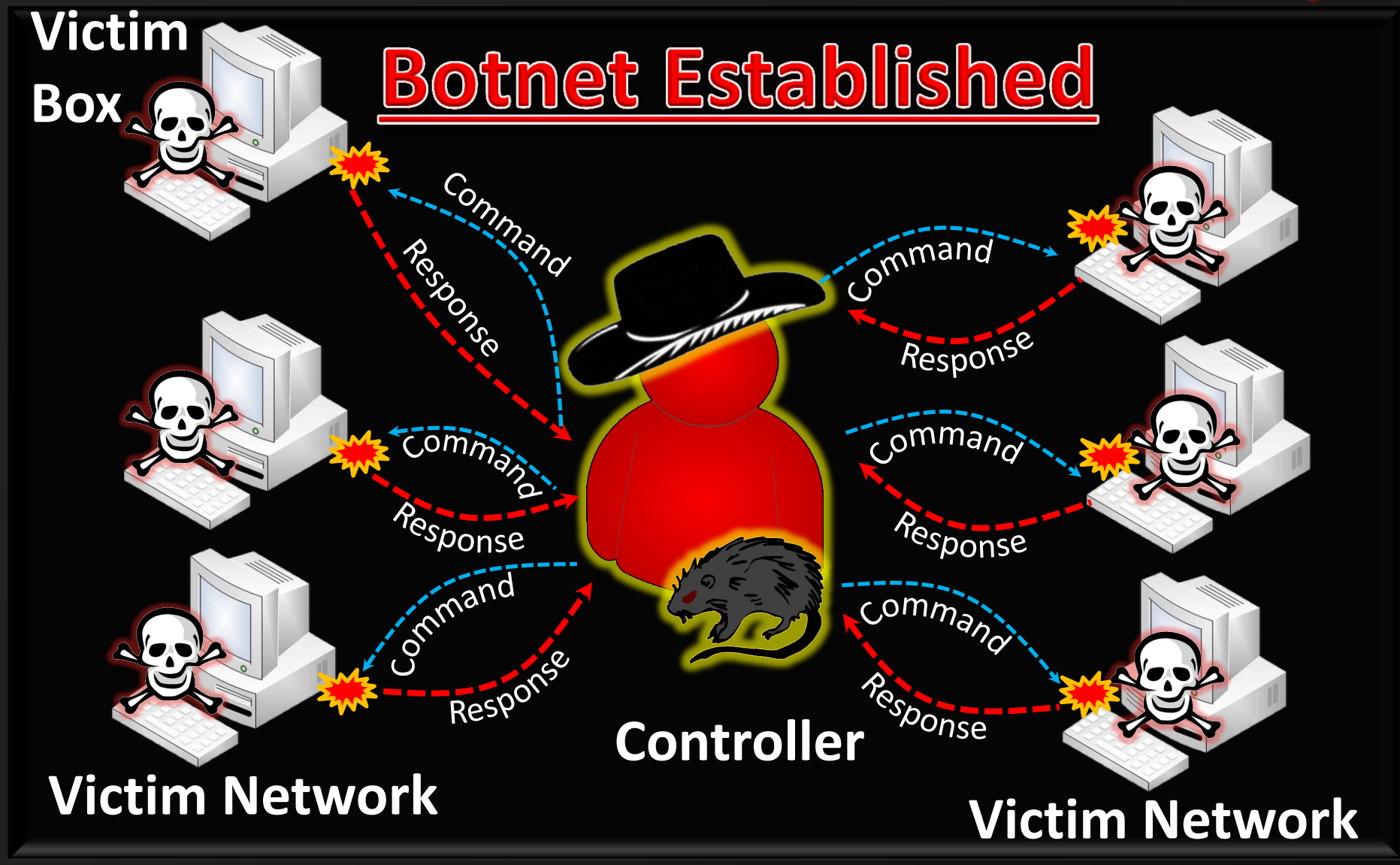
- **Network defense is failing to keep up with emerging threats**
- **Intent:**
  - Bridge gap between Botnet creation and exploitation
  - Understanding how this malware is created and communicates gives you the knowledge of what to look for on your network and helps you identify ways to prevent future intrusions
- **Truly knowing how to attack allows us to develop better ways to defend our critical assets**

What is this Botnet You Speak of?

Botnet Terminology

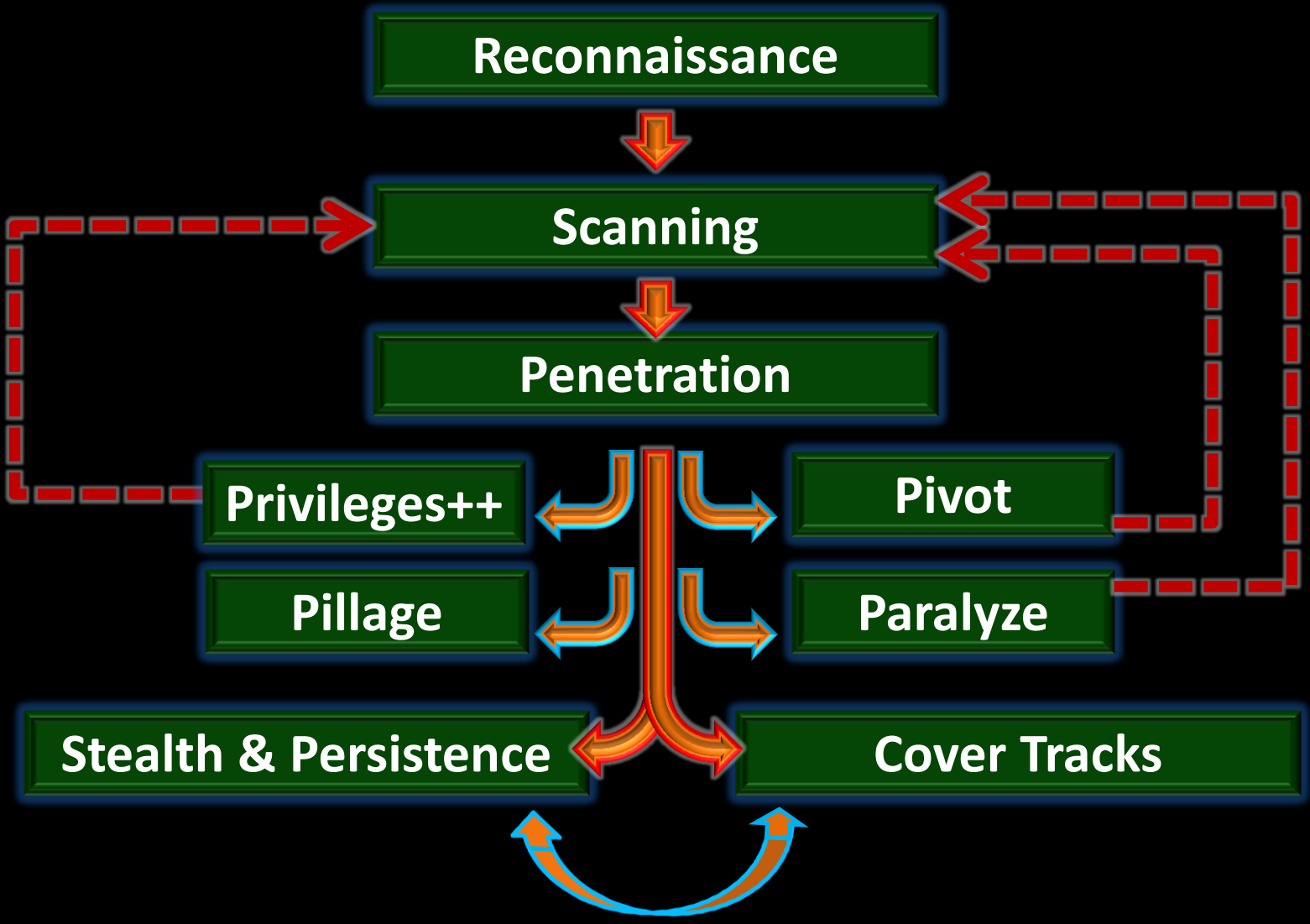
- Network of autonomous agents that synchronize with the Command and Control (C2) Server to exe commands and automate remote exploitation
- **Controller**
  - Robust UI; only run by BotMaster/BotHerder to control 1++ agents simultaneously
- **Dropper**
  - Exploits victim, configures environment, downloads and executes implant
- **Implant**
  - Listener agent on each infected machine, syncs with to Controller, exe's commands
- Very light-weight
  1. Exploit a system, establish shell and maintain persistent connection to Controller
  2. Listen for Commands and Executes received statements
  3. Pipe response and status back to Controller
  4. Evade detection and persist on host as long as possible

Botnet Concept

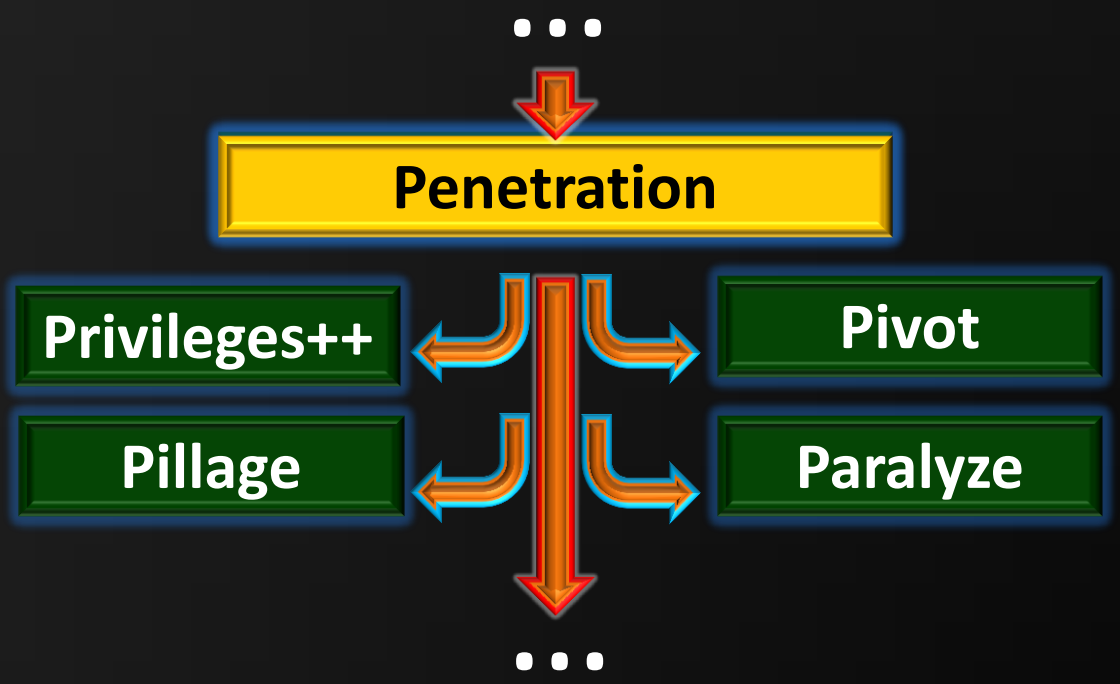


So Where Do We Begin?

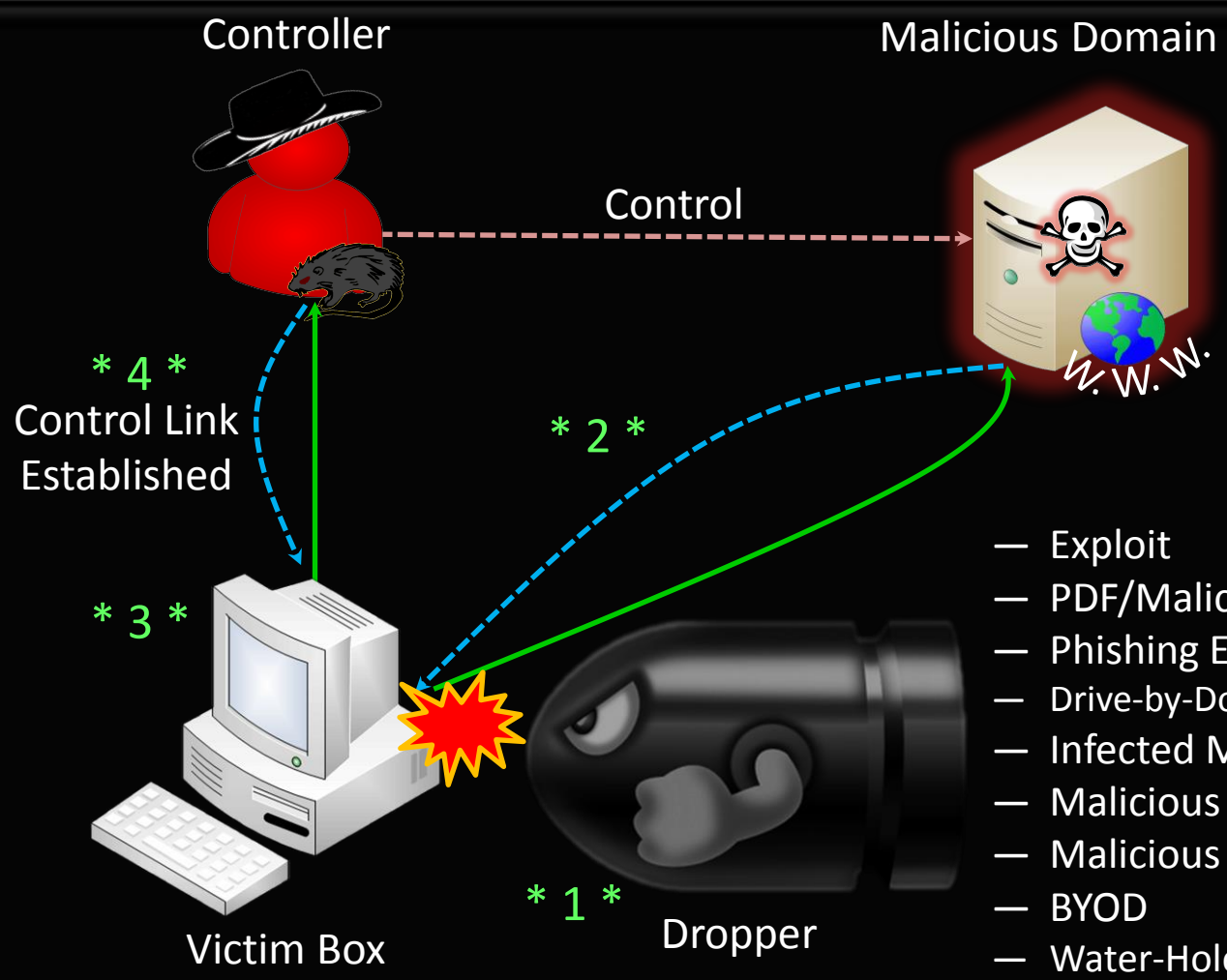
Anatomy of an Attack



PENETRATION: Using a Dropper Script



Dropper Concept: Pictogram



Stage 1: Infect Victim

Stage 2: Establish C2

Stage 3: Persistence

Stage 4: Pivot

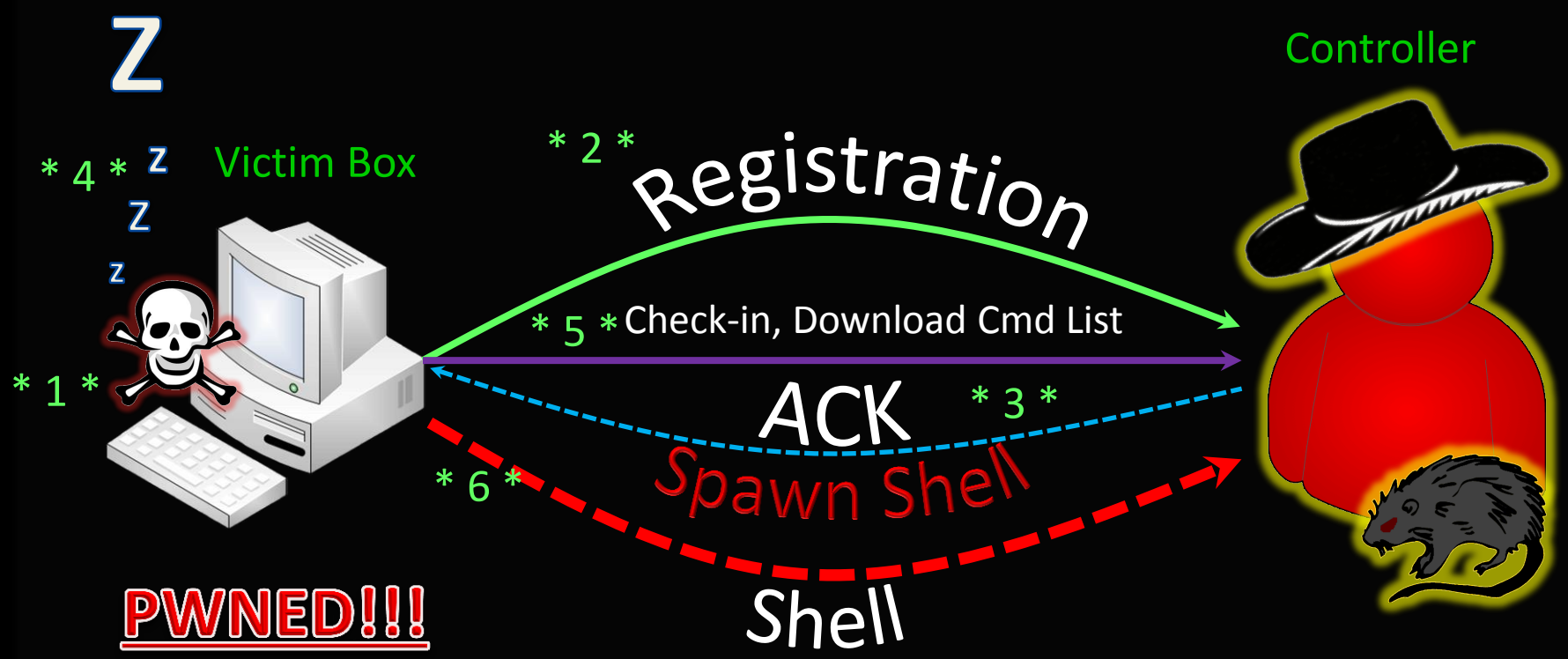
PWNED!!!

- Exploit
- PDF/Malicious Document
- Phishing Email
- Drive-by-Download, Browser Exploit
- Infected Media: (USB/CD/DVD)
- Malicious Insider
- Malicious Executable (Game, SW…)
- BYOD
- Water-Hole, Malicious Executable Script
- etc

Stealth & Persistence: Beacon Bot

Beacon Bot: Overview

- Inspiration: Raphael Mudge
- Motivation: Minimize footprint and detection on the network
  - Steps: Wake, check-in, download and exe commands, sleep, RECURSE

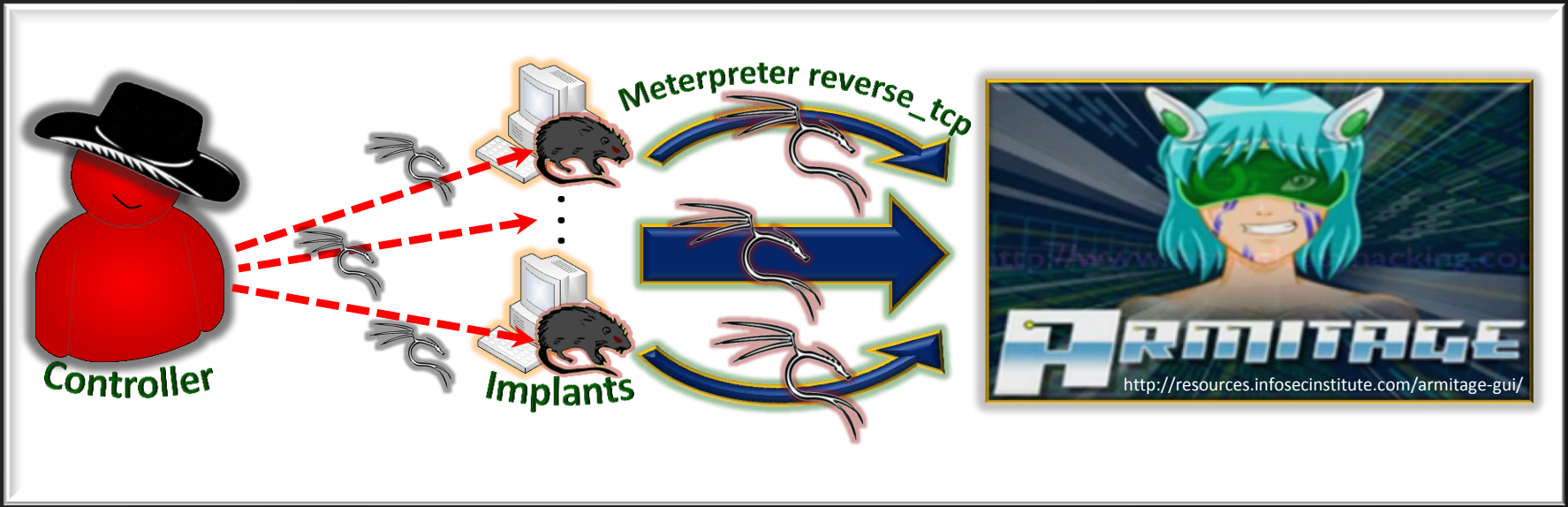


PWN ED!!!

So let's piece it all together…

Demo

PENETRATION: Payload Migration

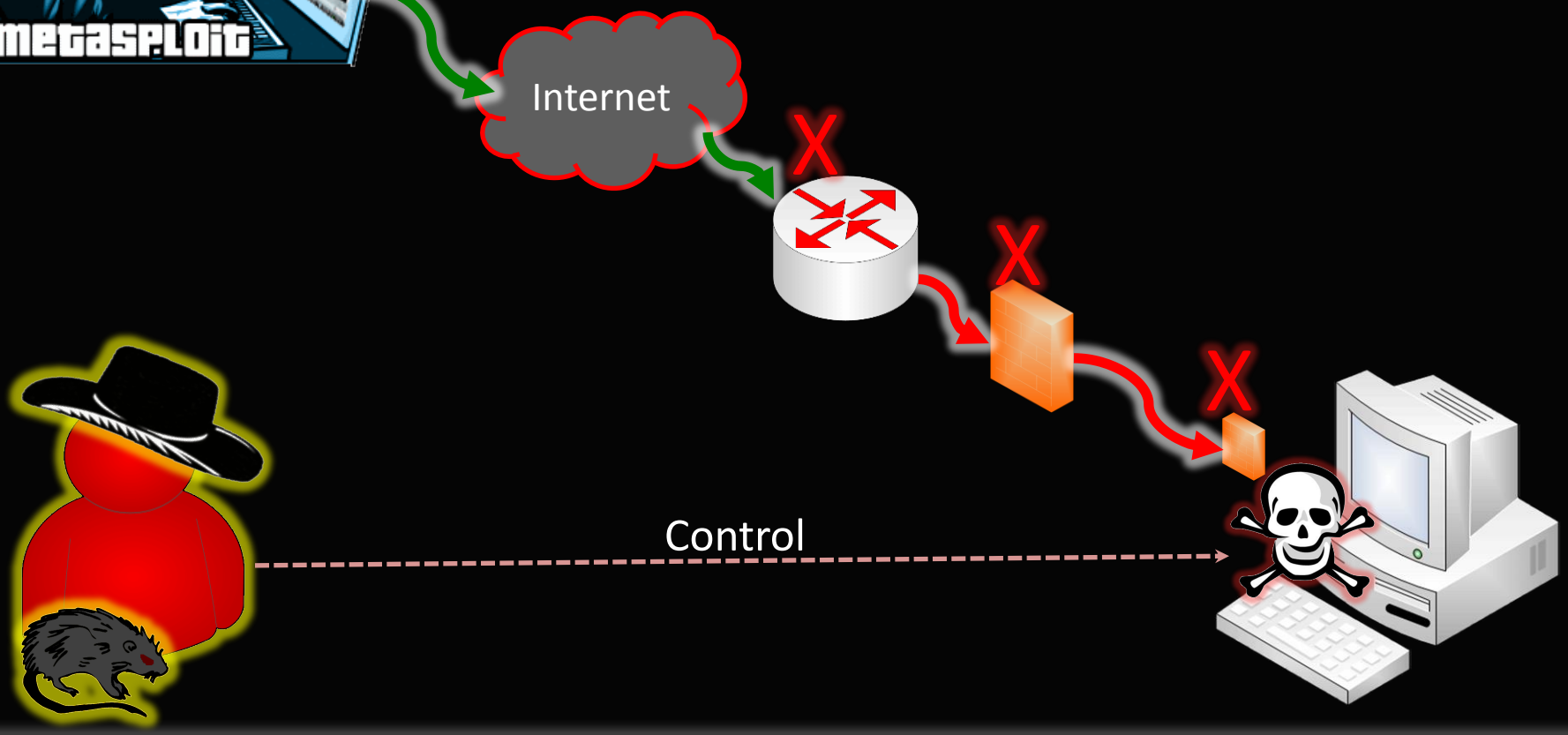


Special thanks to Raphael Mudge (@armitagehacker)

Splinter RAT – Botnet * Solomon Sonya * 2014

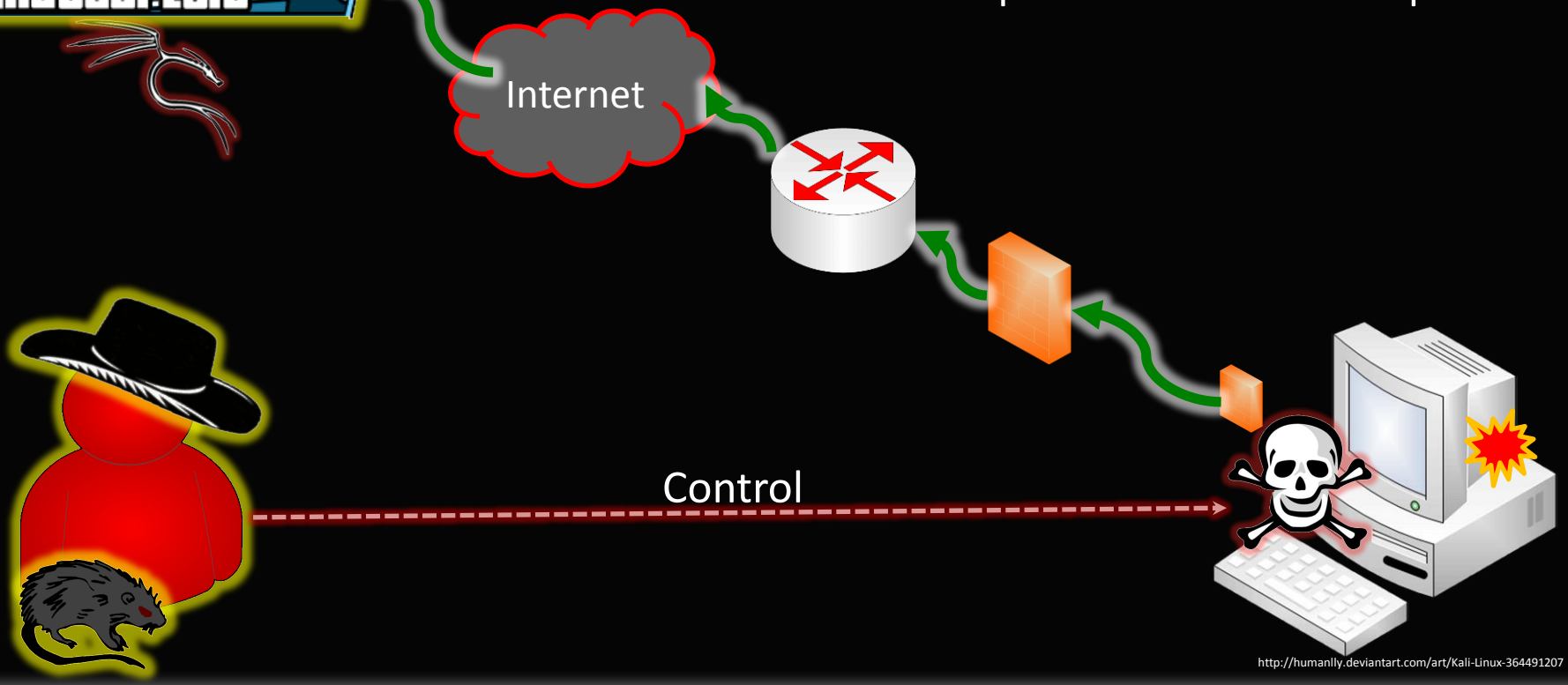
How Can We Migrate Additional Payloads?

Sometimes, initial Metasploit connection is blocked



Solution: Payload Migration!!!

1. Exploit Established Connection in Splinter
2. Migrate Meterpreter through Splinter
3. Execute Meterpreter on Victim Box
4. Connect Outbound to Metasploit
5. Advance Exploitation with Metasploit



PWN ED!!!

So let's piece it all together…

Demo

Social Engineering
(Surgical Approach)

- DNS Host File Poisoning
- Credential Harvesting
- Spoofing UAC

DNS Cache Poisoning

At least 3 ways exist to poison DNS entries:

- Cache Poison DNS servers with incorrect response (much harder now) ← very noisy, and detectable now
- MiTM, constantly poison host with gratuitous ARP (fastest one wins!) ← very noise, highly detectable
- Spoof host file by adding new entry (only once) ← extremely efficient… wait, what is a host file???

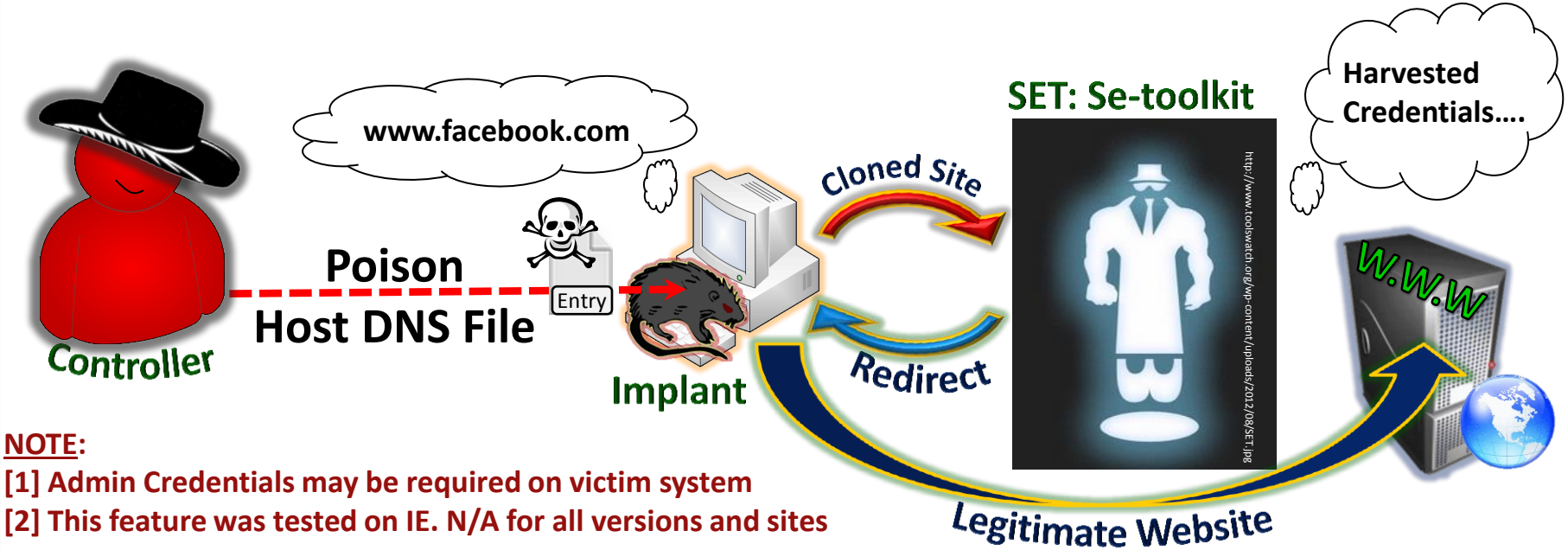
Windows Host DNS File

- Location: %systemroot%\system32\drivers\etc\hosts
- Important flat file (no extension) used to map or override IP addresses before accessing a DNS server
- (Before resolving an IP of a domain name, the host file is checked if an entry exists)
- Sometimes used for redirects, ad, and spyware blocking

So how does it work?

- Say you wish to go to facebook.com
- If an entry for www.facebook.com exists in the host file, browser will go to this address, otherwise, the domain name server is used to resolve the IP
- IT IS VERY IMPORTANT TO CHECK ENTRIES IN YOUR HOST FILE

And now for the Attack!!!



NOTE:
[1] Admin Credentials may be required on victim system
[2] This feature was tested on IE. N/A for all versions and sites

Special thanks to Dave Kennedy (ReL1K) (@HackingDave) and setoolkit

PWN ED!!!

So let's piece it all together…

Demo

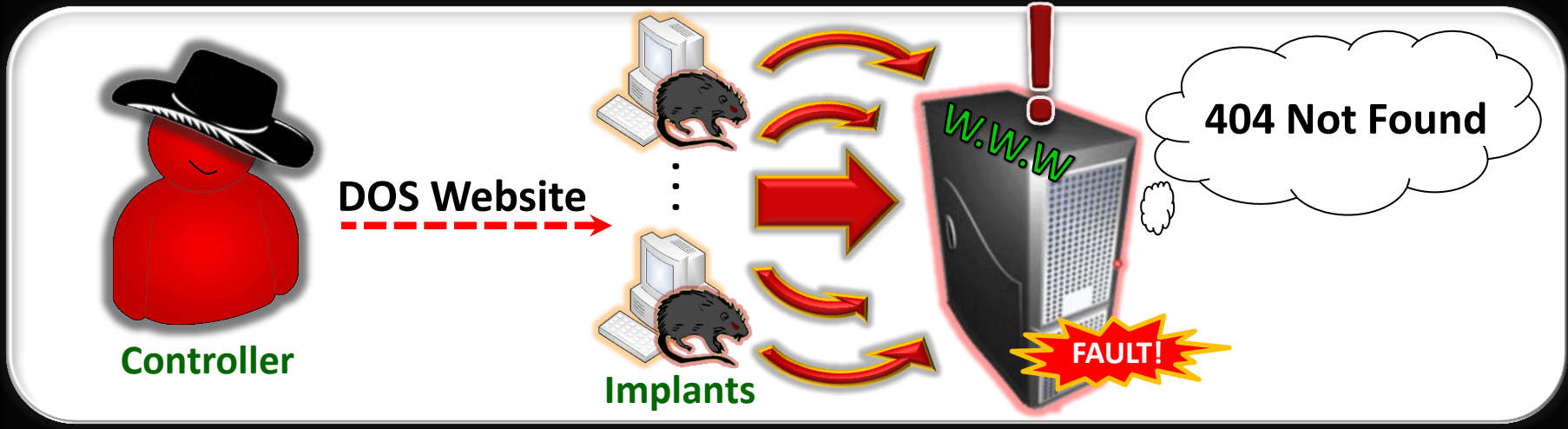
Scorched Earth…

And now for the DDOS

http://www.artsjournal.com/dewey21c/2010/03/proposal_to_scorch_the_earth_i.html

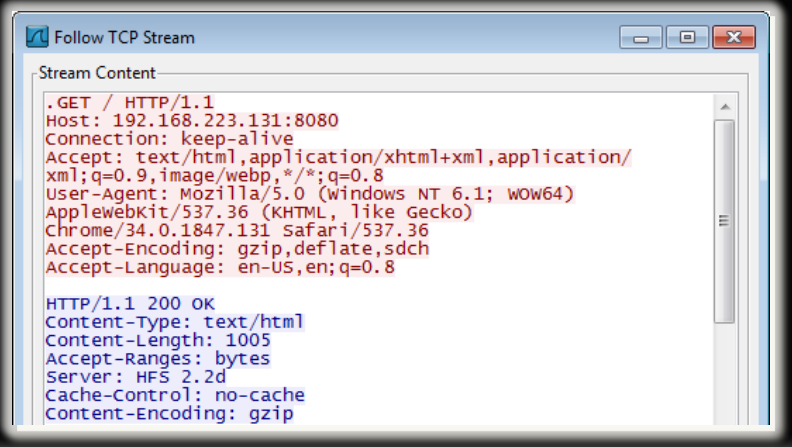
DOS (Denial of Service) Attacks

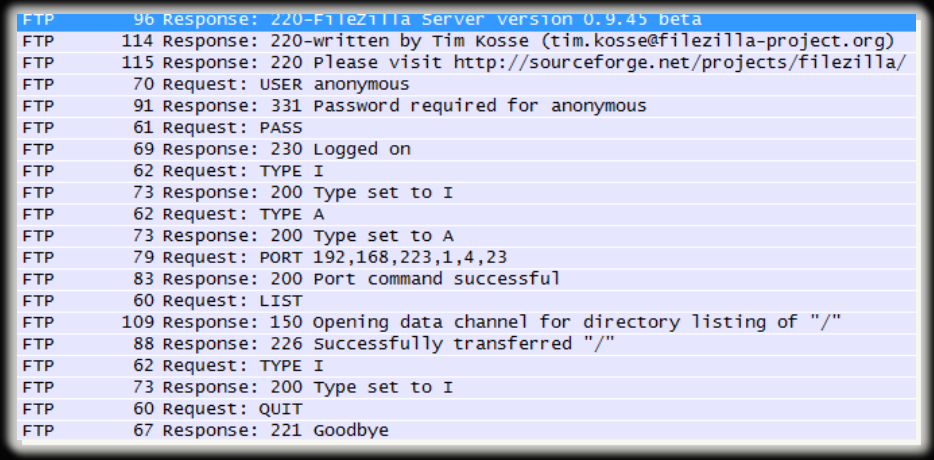
- Most Define: “Denial of service… send too much information than server can handle…”
- What about: “Resource Starvation” such that access to a system at a minimum is degraded, maximum is disrupted



Website DOS Attack Procedure

- Many Techniques exist!!!
- Abbreviated Version:
  - Analyze the legitimate traffic
  - Learn the protocol and structure
  - Mimic the behavior
  - HAPPY DANCE!





PWN ED!!!

So let's piece it all together…

Demo

Additional Features

- Orbiter Payload
- Clipboard Injection
- Spoof UAC
- Relay bot
- Screen Scrape
- Logging Agent
- Enumeration
- File Browser and Transfer
- Want more? Send me an email!

Questions?

- Github Code Repository: github.com/splinterbotnet
- Email: splinterbotnet@gmail.com
- Solomon Sonya: @Carpenter1010