CERIAS

The Center for Education and Research in Information Assurance and Security

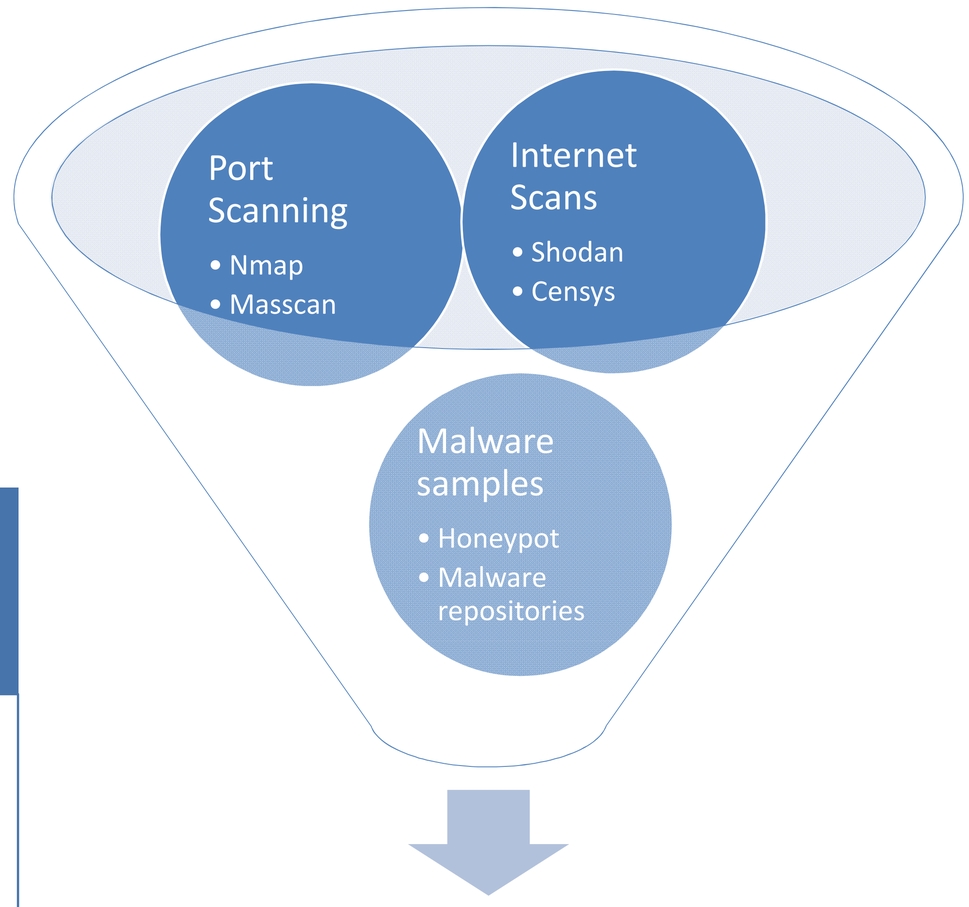
Botnet Attacks: A Case Study of Qbot Botnet Monitoring and Victims

Rushabh Vyas, Nichole McFarland, Connie Justice
Living Lab, Department of Information and Technology
Purdue School of Engineering and Technology, IUPUI

Abstract

In this case study, a Linux DDoS botnet malware, qbot, is researched and botnets are observed to find who the victims of DDoS attacks. Data gathered from honeypots, Shodan, and Censys was used to find C2 servers. To conduct monitoring of the C2 servers, a script was used to emulate a bot and connect to C2 servers. After a month of monitoring qbot C2 servers, it was discovered that DDoS attacks were conducted against video streaming sites, video game related sites and gaming servers, and rival DDoS services. Attackers were also observed communicating on C2 servers. C2 servers were seen mainly running on popular VPS provider networks.

C2 Discovery Techniques



Possible Monitoring Methods

Packet Capture and Analysis – Extracting C2 communication from network traffic	Binary Instrumentation or Modification – Using LD_Preload trick or tools such as Frida	Bot emulation – Writing a script to emulate the interaction with C2, while not launching attacks ✓

Victims and Attacks

Victims of DDoS attacks were fit into the following categories:

- Video Piracy/Streaming sites
- Gaming Servers or Gaming related services, such as forums
- VPS Providers
- Rival DDoS service providers
- Email spammers
- Services used for providing Facebook Likes and views

Interesting victims include:

- Paypal
- Pastebin
- Instagram
- Tor Project
- Phishing site which appeared to look like blockchain.info

Most of the DDoS attacks utilized UDP. TCP, and HTTP based attacks were also observed.

Limitations

-Missing attacks and C2 servers

- Not all the attacks can be monitored, depending on when the server was discovered
- C2 servers can be missed if the malware is not seen on the honeypot or based on when Shodan and Censys perform scans

-Botnet size cannot be determined

Future Research

Implement automation

- Create a custom honeypot or modify existing honeypots
  - Automatically download malicious binaries
  - Extract C2 information from the binary using regex
  - Connect to C2 using the monitoring script
  - Log data to Elasticsearch
- Use Shodan and Censys API
  - Query scan results for C2 banner information
  - Connect to C2 using the monitoring script
  - Log data to Elasticsearch

PURDUE UNIVERSITY

CERIAS

Discovery Park