Resilient Botnet Command and Control with Tor

Dennis Brown
July 2010

Introduction

- Who am I?
  - Work for Tenable Network Solutions
  - Spoken previously at Toorcon, PaulDotCom Podcast
  - Run Rhode Island's Defcon Group DC401

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

- Lots of time lost
  - Setting up servers
  - Building the bot
  - Crypting
  - Spreading
    - Seeding bad Torrents takes time
    - Setting up drive-by downloads takes more time
- Lots of money lost
  - Could be spending that time reselling, DDoSing, etc.

How do botnets get taken down?

- Common methods include
  - Hosting provider de-peered
    - Example: McColo, Troyak
  - Server hosting botnet cleans up/kicks off
    - Public IRC servers, free web hosting
  - Compromised host cleaned up/rebuilt
  - DNS Revoked
  - IP of C&C server banned
    - Because Metus pwnz and I open a port on my router at home just like the tutorial told me!

Wouldn't it be great if we had a way to host these things with less risk of take down?

We do. Its called Tor.

I Really Like Tor

- Tor isn't “bad”, but people who use it can be
  - Most people that use it aren't (I hope!)
- The capacity for devastating abuse with Tor is huge
  - Anonymity is King
- How anonymous is Tor?
  - Recap research about beating Tor's anonymity
  - Hey, it's good enough for WikiLeaks, right?

How does Tor help us hide our botnets?

- Hidden Services
  - Every bot master's dream!
- Authenticated Hidden Services!
- Private Tor Networks
- Exit Node Flooding

- Come at a price
  - Speed
  - Ease of Control

HTTP Hidden Service

HTTP Hidden Service

- Very basic, very effective
- What is a Hidden Service?
  - Standard feature of Tor
    - Insert Diagrams, etc
  - Works behind NAT, Firewalls, etc.
    - No need to expose services to the network
    - We can use this to our advantage to stay hidden
      - Hence the name

So I have a Zeus botnet...

- Easy to get running
  - LAMP server running pretty much anywhere
    - Watch out for data leakage revealing your IP!
  - Zeus Control Panel running on this server
    - Watch out for poorly written control panels!
  - Configure a Hidden Service for the web server
    - Will receive an Onion address
- Problem
  - Where do we point the bot to?

Tor2Web

- Tor2Web is a proxy to redirect .onion web traffic
- Not a part of Tor; 3rd party tool
  - Web redirection service
  - Scripts to run your own
- Command and Control happens via Tor2Web
  - Configure bot to connect to http://tor2web.org/fiewfh9sfh2fj
  - Bot connects to Tor2Web, and is then redirected to Hidden Service via .onion address

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
    - Provides a single point of failure

Proxy-aware Malware over Tor network

Proxy-aware Malware over Tor network

- Hiding in "plain" sigh
- Will require proxy-aware malware
  - Most malware (RATs, DoSers, etc) are not proxy aware
  - Connect direct to a port on a host directly
- Will need to run Tor on infected hosts
  - Not a major problem!
    - Virustotal report

Setup

- This will work for virtually any kind of botnet
  - HTTP, IRC, Custom client/servers, etc
- Set up hidden service for C&C port
- Bots will need to have SOCKS5 support
  - Connect through Tor to .onion addresses
- Bots will need to load Tor onto infected hosts
  - No different than loading something like FakeAV
- Connect through Tor, get commands, send data, win!

Strengths

- Strengths
  - Keeps servers hidden, behind NAT, etc
  - Doesn't rely on 3rd party
    - Takes place via Tor network
    - Direct to your server
  - Uses existing, stable Tor network
    - Should blend in with all other Tor traffic
  - No exit nodes used!
    - Contained entirely within Tor network

Weaknesses

- More complicated to get working
  - Add SOCKS5 support to bot
    - Not that complicated, but not always straightforward
  - Requires Tor to be present on all servers
    - Not complicated, malware does this all the time
  - Tor needs to function properly
    - Have bot sync time for the system?
    - Fortunately, no real configuration hurdles
  - Emergence of new Tor traffic on a network may be detected
    - Network anomaly detection may be effective

Other Alternatives

- Private Tor network
  - 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
- Effectively the same idea
  - Potentially stealthier – less traffic
  - Easier to block?
    - Potentially less relays, easier to enumerate
      - Probably not

P2P C&C

P2P C&C

- The most dangerous option
  - Also the most complex
- Recap popular P2P botnets
  - Sality
  - Conficker
  - Weaknesses
    - Sality UDP-based protocol
    - Conficker Domain Generation

How weaknesses are overcome?

- Tor Hidden Services work around weaknesses
  - No longer blocked by firewalls
- Can provide even greater C&C capabilities
  - Each infected host can be HTTP server
    - With unique .onion addresses
    - Can use them at any time, won't be known prior
  - Distribution through all peers on network
  - Distribute lists of infected hosts

Weaknesses

- Managing all hosts becomes very complicated
- Ensuring new updates apply is critical
- Network fragmentation would result in multiple, unsynched networks

Strengths

- Virtually impossible to take down if working properly
- More effective than whats been seen by Sality, Conficker, etc.
- Just as easy to sell sub-nets to 3rd parties
- Examine research done against Storm, Conficker, etc.
  - Many of the defenses against these worms will be beaten by bypassing firewalls, routing through Tor, using .onion addresses, etc.

Conclusion

- Strength & Weakness Recap
- Turning weaknesses into countermeasures
- Where to go from here?

Q&A