Categories

All
ActiveBreach (15)
Adversary Simulation (14)
Exploitation (14)
Hardware (5)

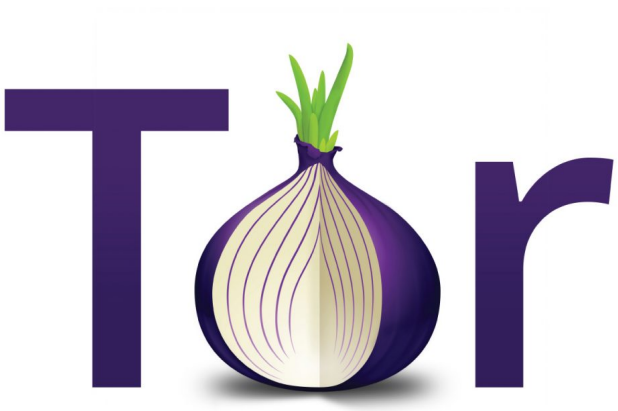
TOR Fronting – Utilising Hidden Services for Privacy

13/02/2017 | Author: Admin

What we do

Adversary Simulation

Our ActiveBreach team



Tor, also known as The Onion Router as well as the Dark Web is a network that is aimed to conceal its users' identity and their online activity from surveillance and traffic analysis. Tor makes it possible for users to hide their locations while offering various kinds of services, such as web publishing. Tor hidden services are also known as .onion sites and often contain a variety of interesting content. In this post we are not interested in the Tor network and what resides on it but instead we want to make use of this infrastructure and freely available technology to hide the origin of our C2 infrastructure.

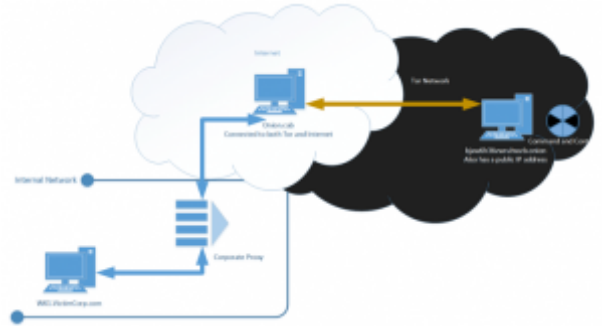
Prior work in this space includes Josh Pitt's guide to using Empire over the Tor network This post details the

necessary requirements for developing a Malleable profile for Cobalt Strike that uses the Tor network as a C2 channel.

The onion.cab website provides a Tor2Web gateway which can be used to access the Tor network:

Upon clicking on the “I know what I’m doing” button, a cookie is set named *onion_cab_iKnowShit* with a value of *0130b15fefbb6eb4e5d3764a8ff4d74f*. This hash value changes periodically and is used to re-verify the user. MDSec were unable to test whether or not this cookie expires while a session is active.

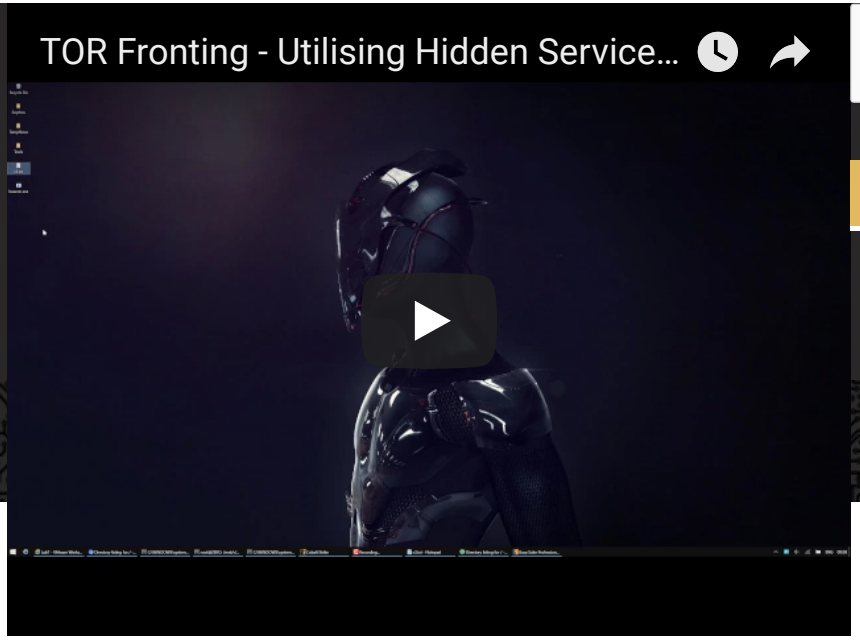
During the investigation, it was found that the onion.cab domain could be used as a front – hiding the hidden service address (onion URL) from DNS queries. For more information on domain fronting, refer to the original post here. Such a deployment can be logically represented as follows:



The thick blue arrows indicate that the data is being transferred over TLS and the yellow arrow indicates that the traffic is over cleartext HTTP. Therefore, we can see that the victim machine must initiate a HTTPS call out to the onion.cab proxy and the proxy then initiates a HTTP call out to our attacker infrastructure.
The onion.cab machine could be logging traffic and would be able to advise the victim organisation as to what hidden service it is connecting to. However, the organisation under attack can also perform SSL inspection to identify the Host header that points to the hidden service address. In a perfect world where Tor is untraceable, the C2 infrastructure's Internet origin would be difficult to uncover and would require attacks on the C2 communication protocol. The Malleable profile that was used is released on the MDSec Github.

An introduction and proof of concept explanation video can be found below:

While a full walkthrough of the analysis, debugging and development of the profile can be found below:



It is also worth noting that during our research several proxies, including the Sophos Web Security gateway that is used in the above demonstrations, did not block the “onion.cab” website using categorisation even on their strictest configurations.

While we would not recommend using Tor on an adversary simulation engagement, this post demonstrates how an adversary may be able to maintain anonymity for their C2 infrastructure using Tor fronting and provides indicators that the blue team can use to detect such behaviour.

This post was written by @vysecurity