Can You Stay Anonymous While Participating in a DDoS Attack?

**Key Findings**
Taking part in a Hacktivist group is completely different than being part of a Botnet. In the Botnet, case participants are recruited to an attack without their knowledge, and in the Hacktivist group, case members knowingly take part in attack activities.

Consequences for voluntary participation in DDoS (Distributed Denial of Service) attacks can be severe. DDoS is illegal in the United States, the United Kingdom, Sweden and other countries. Just recently, in January 2013, Anonymous hackers in London were jailed for a series of DDoS attacks on PayPal and other payment services like Visa and MasterCard.

In this paper we researched the various options to launch a DDoS attack while keeping the attacker anonymous. The key findings in this paper reveal that:

- Attackers need to choose between launching effective DDoS attacks or remaining anonymous
- Only the top hackers can truly hide themselves during attacks
- The crowd that follows Anonymous guides for anonymity believes that they hide themselves, but in reality they cannot hide completely and they find themselves prosecuted.

**Introduction**
While few DDoS participants are caught and arrested, others manage to keep their anonymity. Typically, it is the attack leaders who are more knowledgeable about Internet security and anonymity compared to their followers who tend to be the ones getting caught. This paper explores the different means and methods leveraged by attackers to keep their anonymity.

In this paper we will:

- Learn how anonymity guides for Hacktivists are published.
- Understand the advantages and disadvantages of various solutions like TOR and VPN, on their own and combined.
- See whether Hacktivists are adopting these anonymity guidelines by showing our research on TOR usage with DDoS attacks.
- See the downsides of using anonymity services while launching DDoS attacks and how to use these vulnerabilities to mitigate attacks.

**Anonymous Guides**
DDoS attack leaders often publish anonymous guides on the Internet providing instructions to their followers on how to maintain anonymity. For example, this ‘How to Stay Anonymous’ YouTube guide instructs users on how to launch a DDoS attack behind TOR. During one of the recent large DDoS attacks, attackers referred to a guide published on pastebin.com with a detailed explanation on how to set an attack using both TOR and VPN services.
In this guide, the instructor shares the tools and several detailed explanations on how to setup and check that the attacker’s real IP is not visible to the target or to the man-in-the-middle.

The tweet below is another example of the methods used by attackers to distribute instructions and recommendations for keeping anonymity.

TOR
TOR, short for The Onion Router, is a free network intended to provide online anonymity. The TOR client software directs Internet traffic through a volunteer network of servers to conceal a user’s location or usage. The term Onion Routing refers to the layered nature of the encryption service: the original data is encrypted multiple times, then sent through successive TOR relays, each one decrypting a “layer” of encryption before passing the data on to the next relay and ultimately to its destination. This process reduces the possibility of the original data being unscrambled or understood in transit.

The diagram, from the TOR project website illustrates how the TOR network works.

As an example, a user named Alice wants to connect to Bob (a Web server). Alice first obtains a TOR nodes list from Dave and then picks a random path to Bob. Alice uses the public key of each node in the route, in reverse order, to encrypt the message. This route will change every ten minutes, using different
entry and exit nodes which make tracking even more difficult. On the way back, the nodes will encrypt the response with their private key and Alice’ will peel it all off using the public keys.

The fact that each routing node (router) in the path knows only the node before and after, makes it almost impossible for one node to identify both the source and the target. Like someone peeling an onion, each node in the path removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated.

One weakness of TOR is that the exit node (the last node in the path) needs to decrypt the last layer of encrypted data before sending it to the destination server. Unless the application encrypts data using SSL, whoever controls the exit node can sniff the data.

While TOR provides an excellent platform for keeping anonymity, it also depends on how it is being used. Several techniques were used in the past to break TOR’s anonymity, such as using JavaScript and Flash together with HoneyPots to trap users into sending their real IP.

Using TOR for flood-based attacks can be a double edged sword as it can eventually end up hitting the TOR network itself, making it difficult for attackers to remain anonymous on IRC channels, Twitter and other IM services.

**TOR Usage Along the Years in DDoS Attacks**
Attackers use different anonymity techniques during DDoS attacks to avoid detection. The Radware ERT (Emergency Response Team) compared attacker IPs with known TOR exit nodes at the attack time in order to analyze the usage of TOR networks in DDoS attacks.

The IPs that were not identified as TOR exit nodes were hard to determine whether they were the attackers real IPs or Web Proxy IP addresses, so we assumed false negative identification of attacker IPs which were originally Proxy/VPN IP addresses.

The goal was to show that anonymity is being taken into account and that users are putting much more effort into hiding their true identity. Since TOR is most often mentioned as a good anonymity service, it should provide a good indication for the ‘attacking and staying anonymous’ research in general.

![TOR usage](chart)
While most users still choose other methods (VPN/Proxies) or no anonymity at all, we can definitely see a rise in the TOR usage in the past three years.

**VPN**

A Virtual Private Network (VPN) extends a private network across the Internet to connect nodes. Using encryption and other security mechanisms, a VPN ensures that only authorized users can access the network and that the data cannot be intercepted.

When using a VPN, the home computer of the private user becomes part of a private network. The tunnel created over the Internet between the home computer and the VPN server is encrypted and safe. From the VPN server, the IP changes to a new public IP, so that it becomes difficult to track the originator of the data.

**VPN Providers and Anonymity**

Some providers offer free VPN services. However, the drawback is that such entities sell information about clients to 3rd parties (i.e. ad companies). Usually, Hacktivist leaders strongly advise their followers to pay for VPN services in order to avoid compromising their identity.

Paid VPN services also do not always ensure anonymity. A member of the Lulzsec hacker group was tracked down even though he used the HideMyAss paid VPN service. For instance, if a VPN provider keeps logs and hands those over to the authorities under circumstances such as criminal activity, then anonymity cannot be ensured.
DNS Leakage
DNS leakage occurs when web traffic goes through the VPN or list of proxies, but address resolution is done locally by the ISP provider. Obviously, such address resolution outside the VPN can reveal attackers identify. Attacker guides (see earlier section) specifically mention this with guidelines to make sure that DNS resolving is done through the VPN service.

A DNS leakage often happens when there is a slight delay in the answer from the VPN DNS server or when the VPN fails to resolve the address.

Proxy Chains
A proxy chaining solution is similar to TOR but instead of relying on volunteers as nodes in the path, a proxy chain is based on public servers. Also, proxy chains do not have onion routing and therefore offers no built-in encryption.

A proxy server is basically a server placed between the client and an Internet server endpoint. The client IP is unknown to the Web Server, since all requests and responses go through the Proxy Server.

As for web Proxy anonymity, within web sessions the browser (or the Proxy) usually transmits information about the client, such as: Browser name/version, OS name/version, browser plugins and configuration, and IP of the client.
The most important piece of information is obviously the IP address which can reveal the identity of the originator of the data.

Information is sent to the web server as variables within the HTTP request with the most important variables being:

- **REMOTE_ADDR** – the client’s IP address
- **HTTP_VIA** – the address(es) of a proxy server(s) (added by the proxy server itself)
- **HTTP_X_FORWARDED_FOR** – the real IP address of a client (added by the proxy server)

If no proxy server is being used, the REMOTE_ADDR variable lists the IP address of the client. When a proxy server is used, then these variables may have different values depending on the type of proxy being used.

**Transparent Proxy**
A transparent proxy does not really hide the originator IP on the Internet and is mostly used for caching purposes. When using a transparent proxy, the environment variables will appear like this:

- **REMOTE_ADDR** = proxy IP
- **HTTP_VIA** = proxy IP
- **HTTP_X_FORWARDED_FOR** = your IP «

**Anonymous Proxy**
An anonymous proxy does not hide its usage, but simply changes all the IPs in the variables to the Proxy IP.

- **REMOTE_ADDR** = proxy IP
- **HTTP_VIA** = proxy IP
- **HTTP_X_FORWARDED_FOR** = proxy IP

There are some anonymous proxies called ‘distorting proxies’ which put a random IP address in the **HTTP_X_FORWARDED_FOR** variable.

**High Anonymity Proxy**
These proxies are also called ‘High Anonymity or Elite’ because they hide the fact that they are being used. The variables appear as if no proxy is being used, with the variable values of the Proxy IP address.

- **REMOTE_ADDR** = proxy IP
- **HTTP_VIA** = not determined
- **HTTP_X_FORWARDED_FOR** = not determined

**Proxy Chaining and Anonymity**
In proxy chaining, more than one Proxy is used. The more proxies that are chained, the harder it is to trace back the traffic to the originator.

Chaining through multiple proxies based in different countries (preferably hostile to you own country) is yet another way to strengthen anonymity and make it difficult to discover the originator.
Like TOR, public proxy servers, particularly the ones published for free on the Internet, usually suffer from performance issues. Performance further degrades as more public proxies are chained.

**TOR->VPN vs. VPN->TOR**
In order to increase anonymity and privacy, some guides suggest using both TOR and VPN simultaneously. In some cases, attackers may go even further to protect their anonymity by chaining proxies and using SSH tunnels on top.

While some guides place no importance on how these two solutions are implemented together, there is a big difference. While TOR->VPN increases privacy and anonymity, the other direction of VPN->TOR exposes the originator identity as explained below.

**TOR to VPN**
As described earlier, the data on TOR exit node is not encrypted and can be sniffed easily.

When wrapping it with another encryption layer of the VPN tunnel, no one can sniff the data on the exit node. Additionally, even if the VPN provider keeps logs, the IP of the attacker is still safe since he is hiding behind TOR and the VPN server will log the TOR exit node IP.

Additionally, some websites block TOR traffic. Using this setup, the website sees the VPN IP address rather than that of the TOR.

**VPN to TOR**
In a VPN->TOR setup, the attacker first establishes a VPN connection and then uses TOR as a proxy service for anonymity. In this implementation, both solutions are serialized (no double encryption). Therefore, the identity of the attacker can be easily compromised, similar to when user data is sniffed on the TOR exit nodes or when there is access to the VPN server.

This setup is often used when the ISP/GW does not allow using TOR but allows VPN connections.
Bandwidth, Exit Nodes and Black Listing

TOR networks suffer from both latency and limited bandwidth, which can sometimes seriously weaken high-bandwidth DDoS attacks, making them a total failure. Also, using TOR for DDoS attacks can impact the TOR network itself.

The following TOR status snapshot indicates that the average throughput at the time the snapshot was taken did not exceed 645 MByte/s. (This is a rough estimation, assuming the bandwidth is equally distributed among regular nodes and exit nodes, and the entire TOR network is free for the attackers to use). This does not seem even close to the volumes of the recent attacks carried on U.S. financial institutions.

<table>
<thead>
<tr>
<th>Aggregate Network Statistic Summary</th>
<th>Graphs/Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total bandwidth of displayed Routers [KBytes/s]</td>
<td>2204212</td>
</tr>
<tr>
<td>Total Number of Routers</td>
<td>3082</td>
</tr>
<tr>
<td>Routers in Current Query Result Set</td>
<td>3077</td>
</tr>
<tr>
<td>Total Number of “Authority” Routers</td>
<td>10</td>
</tr>
<tr>
<td>Total Number of “Bad Directory” Routers</td>
<td>0</td>
</tr>
<tr>
<td>Total Number of “Bad Exit” Routers</td>
<td>13</td>
</tr>
<tr>
<td>Total Number of “Exit” Routers</td>
<td>909</td>
</tr>
<tr>
<td>Total Number of “Fast” Routers</td>
<td>2697</td>
</tr>
<tr>
<td>Total Number of “Guard” Routers</td>
<td>930</td>
</tr>
<tr>
<td>Total Number of “Hibernating” Routers</td>
<td>0</td>
</tr>
<tr>
<td>Total Number of “Named” Routers</td>
<td>1997</td>
</tr>
<tr>
<td>Total Number of “Stable” Routers</td>
<td>1784</td>
</tr>
<tr>
<td>Total Number of “Running” Routers</td>
<td>3082</td>
</tr>
<tr>
<td>Total Number of “Valid” Routers</td>
<td>3082</td>
</tr>
<tr>
<td>Total Number of “V2Dir” Routers</td>
<td>1803</td>
</tr>
<tr>
<td>Total Number of “Directory Mirror” Routers</td>
<td>1803</td>
</tr>
</tbody>
</table>
Nevertheless, for ‘low and slow’ attacks using tools like Slowloris and Pyloris, which attack the application protocol layer and do not require volume, a TOR network provides a reasonable anonymity venue.

Another drawback of TOR networks is the fact that TOR exist nodes are constantly tracked with lists published on the Internet. Some services even publish TOR exit nodes in real time - making it quite easy to blacklist these IPs. The same is true for some of the VPN services and for some public Proxy servers. Such IP-reputation solutions are already being integrated in IPS and Anti-DDoS solutions.

Summary

Hacktivist group leaders publish guides, providing their recruits with instructions on how to maintain their anonymity during DDoS attacks. Such guides, which explain how to properly use TOR and VPN services, lower the bar for many less technical attackers.

Nevertheless, anonymity has its price. TOR, VPN solutions and public proxy services have many drawbacks:

- With TOR networks, performance is significantly reduced, decreasing the effectiveness of volumetric attacks.
- TOR exit nodes, public Proxy lists and VPN services are constantly monitored and published, making it quite easy to blacklist IPs and defend against DDoS attacks arriving from blacklisted sources.
- TOR and VPN solutions do not provide a bulletproof solution for anonymity. Without deep networking and security knowledge, users can still be traced and caught.

References

http://en.wikipedia.org/wiki/Tor_(anonymity_network)
http://torstatus.blutmagie.de