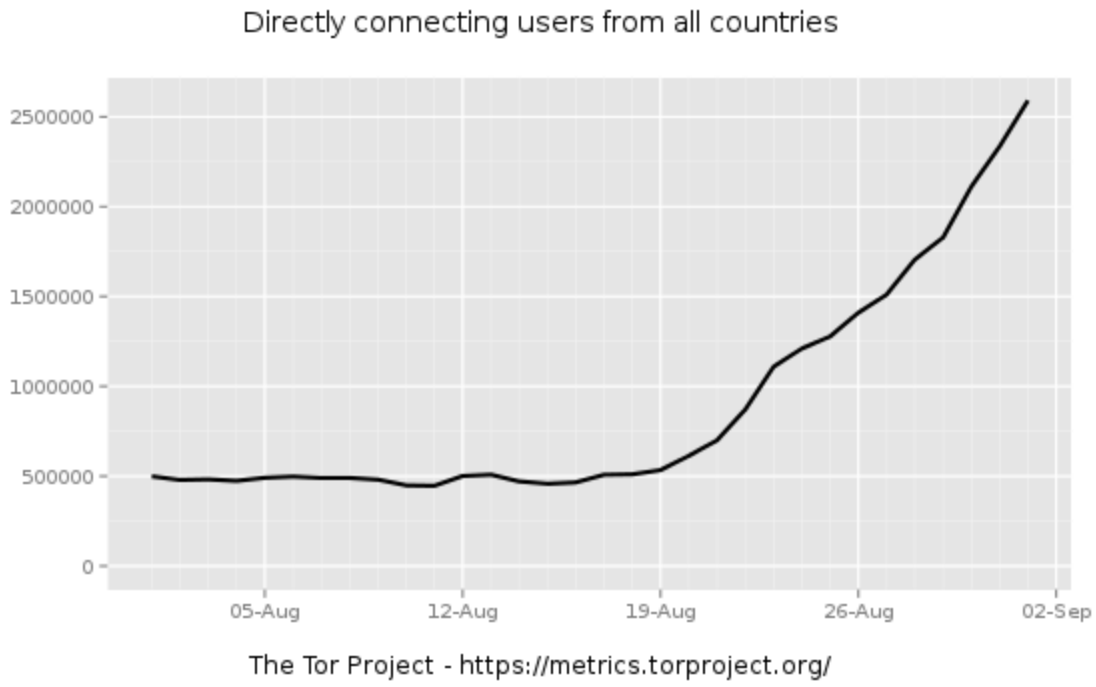
Large botnet cause of recent Tor network overload

blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/

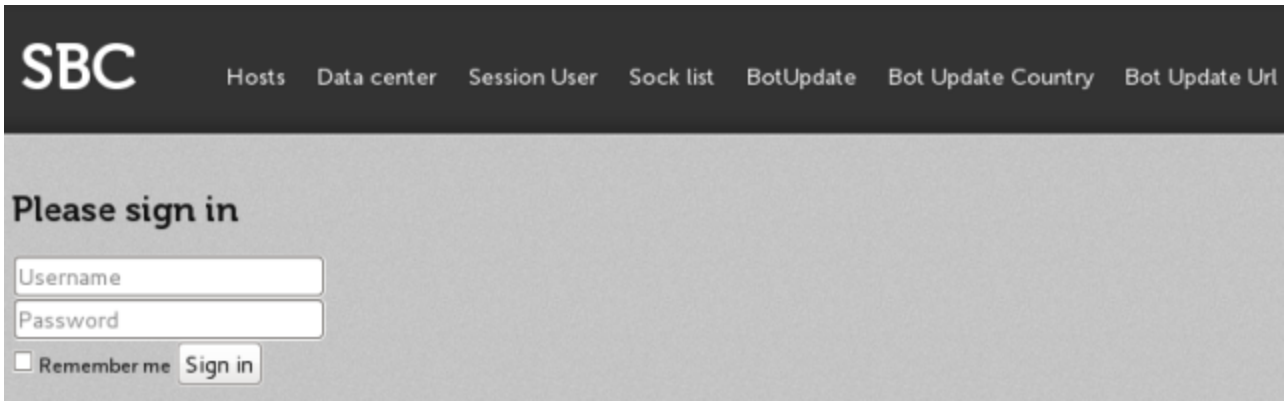
September 5, 2013

Recently, Roger Dingledine described a sudden increase in Tor users on the Tor Talk mailinglist. To date there has been a large amount of speculation as to why this may have happened. A large number of articles seem to suggest this to be the result of the recent global espionage events, the evasion of the Pirate Bay blockades using the PirateBrowser or the Syrian civil war.

At the time of writing, the amount of Tor clients actually appears to have more than quintupled already. The graph shows no signs of a decline in growth, as seen below:



An alternative recurring explanation is the increased usage of botnets using Tor, based on the assertion that the increase appears to consist of mostly new users to Tor that apparently are not doing much given the limited impact on Tor exit performance. In recent days, we have indeed found evidence which suggests that a specific and rather unknown botnet is responsible for the majority of the sudden uptick in Tor users. A recent detection name that has been used in relation to this botnet is “Mevade.A”, but older references suggest the name “Sefnit”, which dates back to at least 2009 and also included Tor connectivity. We have found various references that the malware is internally known as SBC to its operators.



Previously, the botnet communicated mainly using HTTP as well as alternative communication methods. More recently and coinciding with the uptick in Tor users, the botnet switched to Tor as its method of communication for its command and control channel. The botnet appears to be massive in size as well as very widespread. Even prior to the switch to Tor, it consisted of tens of thousands of confirmed infections within a limited amount of networks. When these numbers are extrapolated on a per country and global scale, these are definitely in the same ballpark as the Tor user increase.

Thus one important thing to note is that this was an already existing botnet of massive scale, even prior to the conversion to using Tor and .onion as command and control channel.

As pointed out in the Tor weekly news, the version of Tor that is used by the new Tor clients must be 0.2.3.x, due to the fact that they do not use the new Tor handshake method. Based on the code we can confirm that the version of Tor that is used is 0.2.3.25.

The malware uses command and control connectivity via Tor .onion links using HTTP. While some bots continue to operate using the standard HTTP connectivity, some versions of the malware use a peer-to-peer network to communicate (KAD based).

Typically, it is fairly clear what the purpose of malware is, such as banking, clickfraud, ransomware or fake anti-virus malware. In this case however it is a bit more difficult. It is possible that the purpose of this malware network is to load additional malware onto the system and that the infected systems are for sale. We have however no compelling evidence that this is true, so this assumption is merely based on a combination of small hints. It does however originate from a Russian spoken region, and is likely motivated by direct or indirect financial related crime.

This specific version of the malware, which includes the Tor functionality, will install itself in:

```
%SYSTEM%\config\systemprofile\Local Settings\Application Data\Windows Internet Name System\wins.exe
```

Additionally, it will install a Tor component in:

```
%PROGRAMFILES%\Tor\Tor.exe
```

A live copy for researchers of the malware can be found at:

```
hxxp://olivasonny .no-ip .biz /attachments/tc.c1
```

This location is regularly updated with new versions.

Related md5 hashes:

```
2eee286587f76a09f34f345fd4e00113 (August 2013)
c11c83a7d9e7fa0efaf90cebd49fbd0b (September 2013)
```

Related md5 hashes from non-Tor version:

```
4841b5508e43d1797f31b6cdb83956a3 (December 2012)
4773a00879134a9365e127e2989f4844 (January 2013)
9fcddc45ae35d5cdc06e8666d249d250 (February 2013)
b939f6ef3bd292996f97aa5786757870 (March 2013)
47c8b85a4c82ed71487deab68de196ba (March 2013)
3e6eb9f8d81161db44b4c4b17763c46a (April 2013)
a0343241bf53576d18e9c1329e6a5e7e (April 2013)
```

Thank you to our partners for the help in investigating this threat.

ProtACT Team & InTELL Team