
Detecting BitTorrent Using Snort

Richard Wanner
December 2009
GIAC GSEC GCIH GCIA GCPM GSNA GREM GHTQ

SANS Technology Institute - Candidate for Master of Science Degree

1

Objective

- Understand the mechanisms involved in BitTorrent transfers.
- Identify ways to detect BitTorrent transfers.
- Devise Snort Signatures to detect BitTorrent traffic.
- Discuss encryption which provides a way to circumvent detection.

SANS Technology Institute - Candidate for Master of Science Degree

2

BitTorrent

- Peer-to-peer protocol invented by Bram Cohen.
- Very efficient way to distribute large files.
- Estimated that up to 60% of all Internet traffic is BitTorrent related.

BitTorrent Clients

- BitTorrent 6
- BitComet
- LimeWire
- Shareaza
- Vuze (formerly Azureus)
- μ torrent

Detecting BitTorrent

- Torrent tracker website
- Torrent metafile
 - .torrent extension
 - Metafile contents
- BitTorrent Protocol
- Distributed Hash Table (DHT)

Torrent Tracker Websites

- Tracker websites allow peers to find content.
- There are over 150 known tracker websites.
 - Mininova
 - ThePirateBay
 - Torrentreactor
 - Demonoid
 - Isohunt
 - TVtorrents

Anatomy of a Snort Rule

- Rule Header – describes high-level rule trigger and action
- Rule Options – detailed matching criteria and output

```
alert tcp any any -> 10.10.10.0/24 80
(content:"GET"; msg:"www GET detected";
sid:1000001; rev:1;)
```

Detecting BitTorrent Tracker Website Access

- http GET request
- One signature required for each tracker website

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any
(msg: "P2P mininova"; content:"GET";
content:"mininova"; threshold: type limit, track
by_src, count 1 , seconds 60; sid:1100021;
rev:1;)
```

Torrent Metafile Download

- Metafile has .torrent extension
- Downloaded as HTTP GET

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any
(msg: "P2P .torrent metafile"; content:"HTTP/";
content:".torrent"; flow:established,to_server;
classtype:policy-violation; sid:1100010; rev:1;)
```

Torrent Metafile Content

- Contents are a bencoded dictionary containing "keys".
- Announce is required key which identifies the URL of the tracker.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg: "P2P torrent metafile Download";
content:"d8\:announce"; flow:established;
classtype:policy-violation; sid:1100000; rev:1;)
```

BitTorrent Handshake

- The handshake is required.
- Must be the first message sent when client is contacting the peer.
- Contains the string "BitTorrent protocol".

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any
(msg:"P2P BitTorrent handshake";
 flow:to_server,established; content:"BitTorrent
 protocol"; classtype:policy-violation;
 sid:1100012; rev:1;)
```

Trackerless Torrents

- Decentralized method of finding peers
- Enabled peers keep distributed hash table (DHT) of available content.
- Formatted as bencoded dictionary.
- Most common command is DHT Ping

```
d1:ad2:id20:abcdefghij0123456789e1:q4:ping1:t2:aa1:y1:qe
```

```
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg: "P2P torrent
DHT ping"; content:"d1\:ad2\:id20\:"; content:"ping"; threshold: type
limit, track_by_src, count 1 , seconds 60; classtype:policy-violation;
sid:1100021; rev:1;)
```

Traffic Shaping

- Some ISPs use Traffic Shaping to detect and limit peer-to-peer traffic.
- Most common methods identify and rate limit based on protocol.
- Seriously limits speed of BitTorrent transfers.

BitTorrent Encryption

- Message Stream Encryption (MSE)/Protocol Encryption (PE) - BitTorrent protocol encryption specification.
- Employs obfuscation and randomized packet sizes.
- Defeats most types of traffic shaping.
- Encryption masks the contents of all aspects of the BitTorrent protocol.
- Still possible to detect tracker website requests and metafile downloads.

Summary

- There are a number of different approaches that can be used to detect BitTorrent usage.
- BitTorrent encryption will defeat detection of the BitTorrent Handshake and DHT.