Russian-language actor exploits hype over Telegram ban in Central Asia

securelist.com/octopus-infested-seas-of-central-asia/88200/

By GReAT

For the last two years we have been monitoring a Russian-language cyberespionage actor that focuses on Central Asian users and diplomatic entities. We named the actor DustSquad and have provided private intelligence reports to our customers on four of their campaigns involving custom Android and Windows malware. In this blogpost we cover a malicious program for Windows called Octopus that mostly targets diplomatic entities.

The name was originally coined by ESET in 2017 after the 0ct0pus3.php script used by the actor on their old C2 servers. We also started monitoring the malware and, using Kaspersky Attribution Engine based on similarity algorithms, discovered that Octopus is related to DustSquad, something we reported in April 2018. In our telemetry we tracked this campaign back to 2014 in the former Soviet republics of Central Asia (still mostly Russian-speaking), plus Afghanistan.

In the case of Octopus, DustSquad used Delphi as their programming language of choice, which is unusual for such an actor. Among others exceptions are the Russian-language Zebrocy (Sofacy's Delphi malware), the Hindi-language DroppingElephant and the Turkish-language StrongPity. Although we detected Octopus victims that were also infected with Zebrocy/Sofacy, we didn't find any strong similarities and we don't consider the two actors to be related.

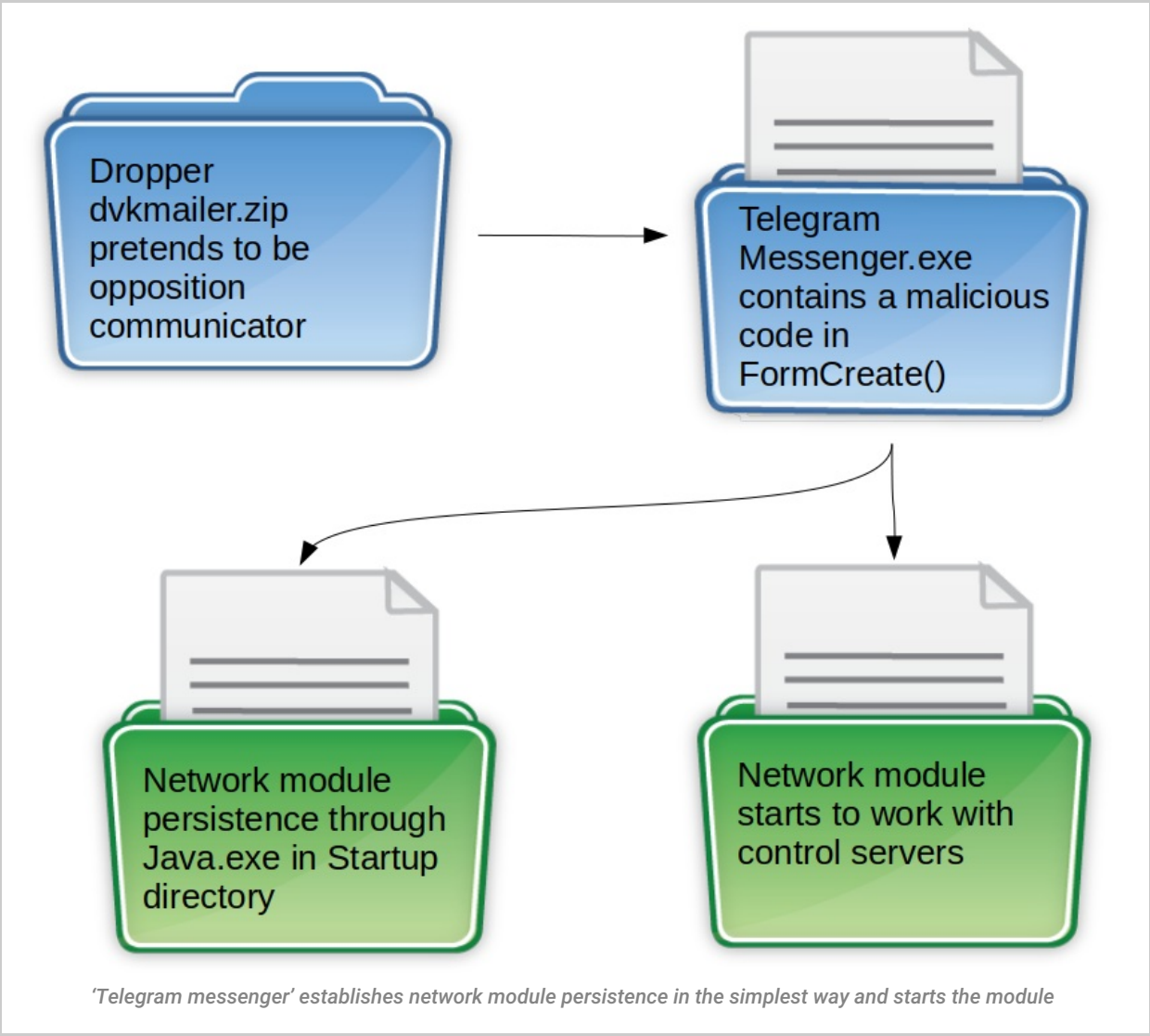
What happened?

In April 2018 we discovered a new Octopus sample pretending to be communication software for a Kazakh opposition political group. The malware is packed into a ZIP file named dvkmailer.zip with a timestamp from February-March 2018. DVK stands for Kazakhstan Democratic Choice, an opposition political party that is prohibited in the country. The image below shows the acronym 'ДВК' in Russian (Демократический Выбор Казахстана). DVK enjoys a healthy Telegram presence, making Telegram´s potential ban a hot topic in Kazakhstan. The dropper pretends to be Telegram Messenger with a Russian interface.

We couldn´t find any legitimate software that this malware appears to be impersonating; in fact, we don´t believe it exists. The Trojan uses third-party Delphi libraries like The Indy Project for JSON-based C2 communications and TurboPower Abbrevia (sourceforge.net/projects/tpabbrevia) for compression. Malware persistence is basic and achieved via the system registry. The server side uses commercial hosting in different countries with .php scripts deployed. Kaspersky Lab products detect the Octopus Trojan as Trojan.Win32.Octopus.gen. For more information, please contact: intelreports@kaspersky.com.

Technical details

The attackers used the potential Telegram ban in Kazakhstan to push its dropper as an alternative communication software for the political opposition.



'Telegram messenger' establishes network module persistence in the simplest way and starts the module

We can't confirm how this malware is being distributed, although it clearly uses some form of social engineering. This actor previously used spear phishing to spread malware.

Dropper

MD5 hash	979eff03faeaeea5310df53ee1a2fc8e
Name	dvkmailer.zip

Archive contents

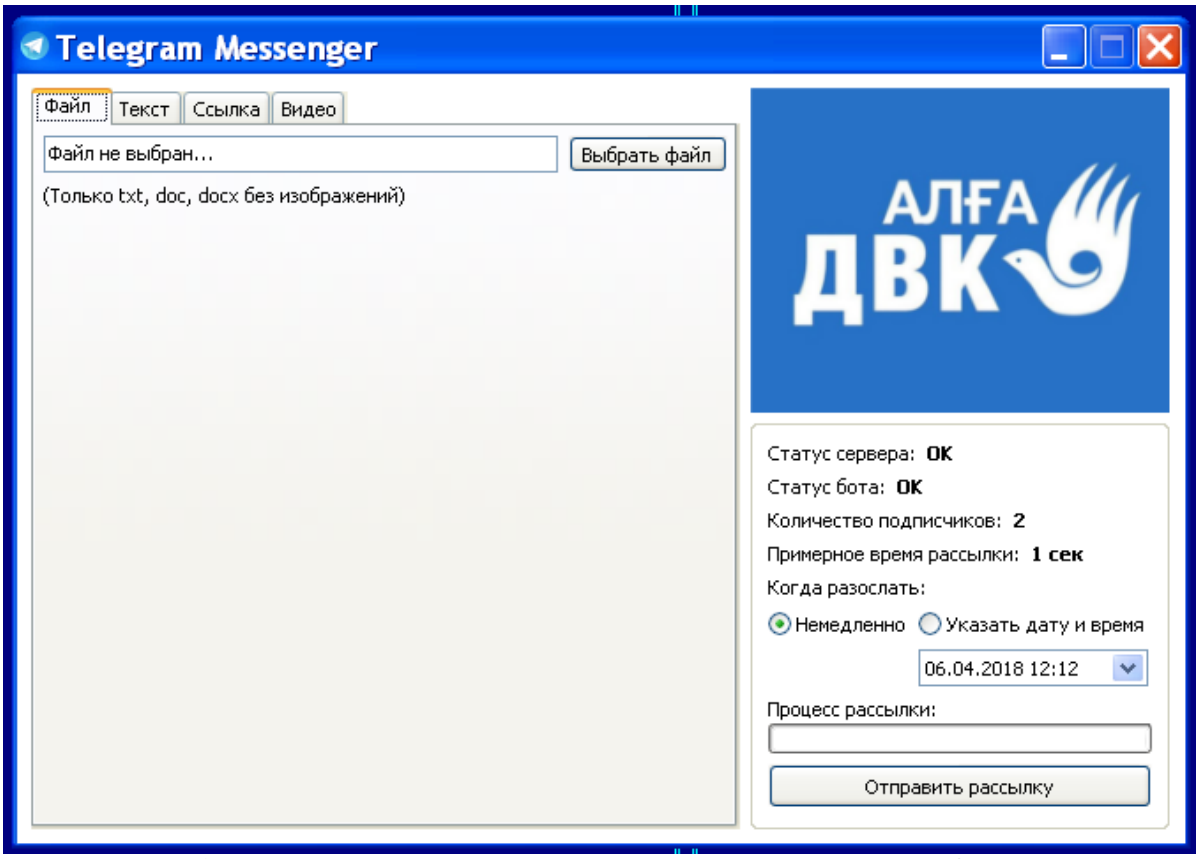
d6e813a393f40c7375052a15e940bc67	CsvHelper.dll	Legit .NET CSV files parser
664a15bdc747c560c11aa0cf1a7bf06e	Telegram Messenger.exe	Persistence and launcher

87126c8489baa8096c6f30456f5bef5e	TelegramApi.dll	Network module
d41d8cd98f00b204e9800998ecf8427e	Settings.json	Empty

Launcher

MD5 hash	664a15bdc747c560c11aa0cf1a7bf06e
File name	Telegram Messenger.exe
PE timestamp	2018.03.18 21:34:12 (GMT)
Linker version	2.25 (Embarcadero Delphi)

Before any user interaction, inside the FormCreate() function the launcher checks for a file named TelegramApi.dll in the same directory. If it exists, the launcher copies the network module to the startup directory as Java.exe and runs it.



The 'Send mailing' button in the bottom right corner doesn't even have a handler function

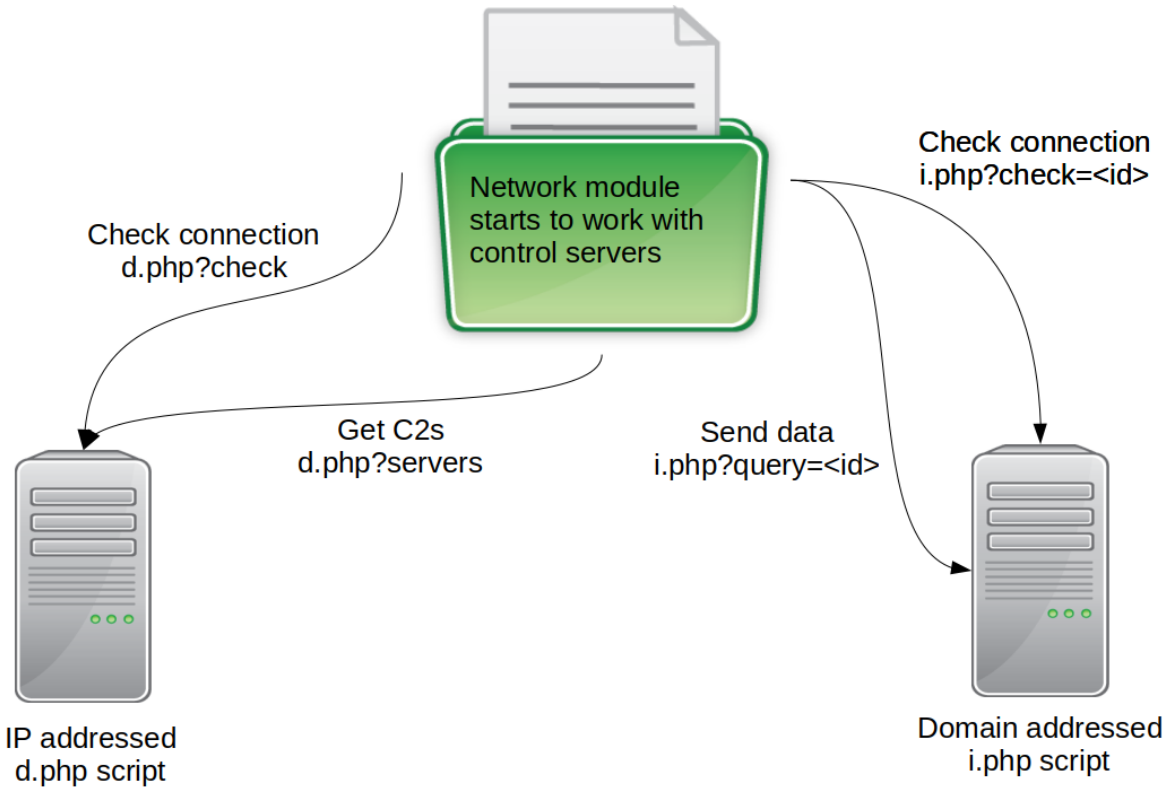
Delphi Visual Component Library (VCL) programs are based on event handlers for form elements. Such programs are extremely large (about 2.6 MB and 12,000 functions), but all this code is mostly used to handle the visual components and run-time libraries. There are only three programmer-defined handlers for controlling elements inside the Octopus launcher.

Function name	Functionality

FormCreate()	Runs as constructor before any user activity. Makes the network module persistent via Startup directory and runs it
Button1Click()	Shows the explorer dialog window to choose the “mailing file”
DateTimePicker1Click()	Shows calendar to select the “mailing date”

There is no handler for the ‘Send mailing’ button, so the launcher pretends to be an alternative communicator that in reality does nothing. This may be because the malware is still unfinished – after all, messages sent through it could be of value to the attackers. However, we believe it is more likely that the malware was created in a hurry and the attackers decided to skip any communication features.

Network module



C2 communication scheme

MD5 hash	87126c8489baa8096c6f30456f5bef5e
File name	TelegramApi.dll
PE timestamp	2018.02.06 11:09:28 (GMT)
Linker version	2.25 (Embarcadero Delphi)

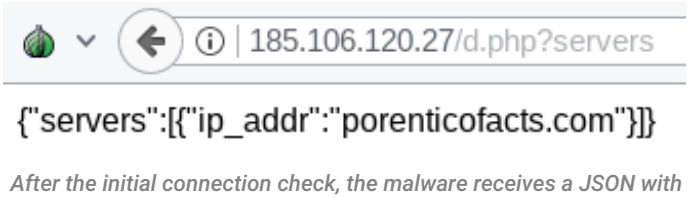
Despite the file extension, this network module is a self-sufficient portable executable file and not a dynamic-link library. The first sample checks for files with names like 1?????????.* in the user’s temporary folder and deletes any files it finds. Then it creates .profiles.ini in the Application Data directory where the malware stores its log.

HTTP request	Response
GET /d.php?check	JSON “ok”
GET /d.php?servers	JSON domain name
GET /i.php?check=	JSON “ok”
POST /i.php?query=	JSON response code or command depends on POST data

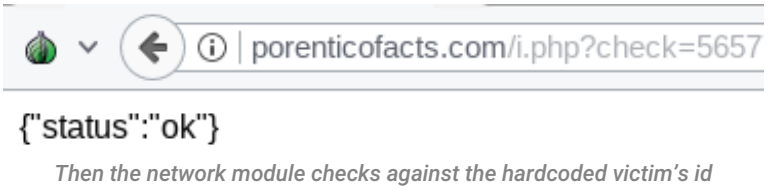
```php
<?php
if(isset($_GET['check'])){echo(json_encode(array('status'=>'ok')));}
if(isset($_GET['servers'])){
    $arr_servers = array();
    array_push($arr_servers,array('ip_addr'=>'latecafe.in'));
    echo(json_encode(array('servers'=>$arr_servers)));
}
?>
```

First stage .php script to check connection and get C2 domain name

All network modules consist of hardcoded IP addresses belonging to commercial web-hosting services based in different countries. The operators simply deploy their first-stage .php script in them, which will check the connection and get the actual C2 server domain name using an HTTP GET request.

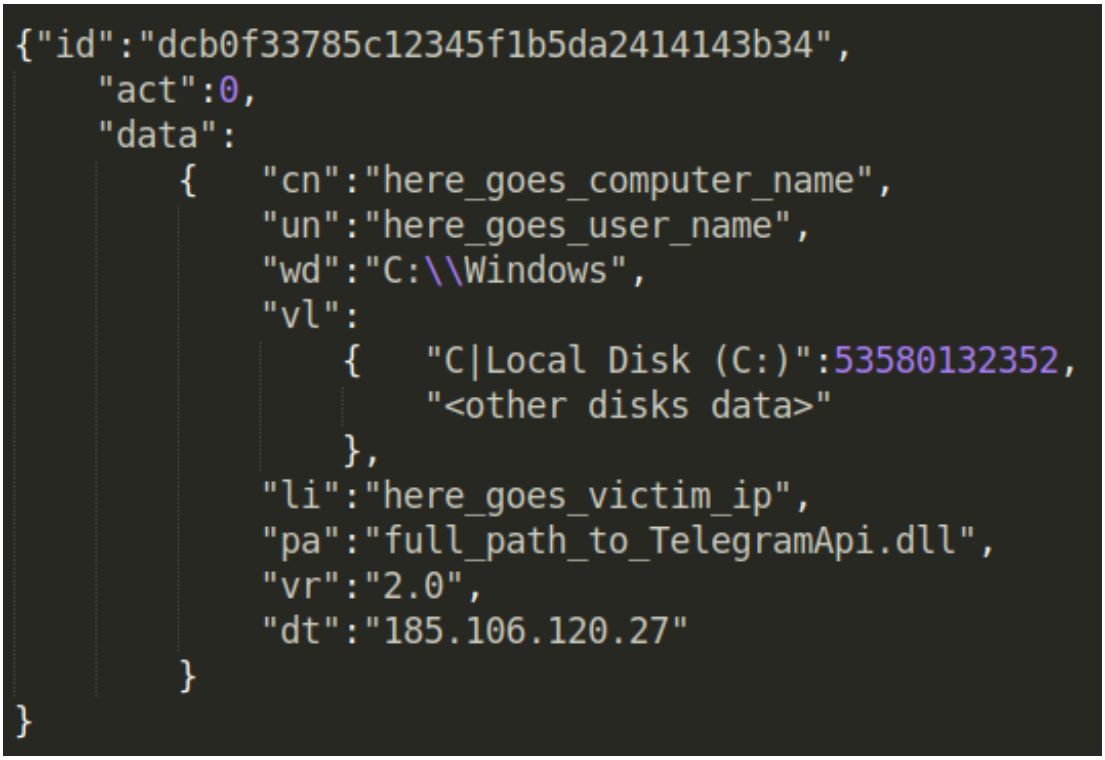


After the initial connection check, the malware receives a JSON with the actual C2 domain name



Then the network module checks against the hardcoded victim’s id

The network module checks against a 32-digit hardcoded victim id and sends the gathered data to the C2 using a HTTP POST request. In terms of programming, this id is strange, because the malware simultaneously ‘fingerprints’ its victim with an MD5 hash of its system data.



JSON-based gathered data sent in a HTTP POST base64-encoded request

All communication with the C2s is based on JSON-formatted data and the HTTP protocol. For that, the developers used The Indy Project (indyproject.org) publicly available library as well as the third-party TurboPower Abbrevia (sourceforge.net/projects/tpabbrevia) for compression.

After all the initial HTTP GET requests, the malware starts to gather JSON-formatted system data. For all the fixed drives in the system, the network module stores the disk name and size, as well as computer and user name, Windows directory, host IP, etc. One interesting field is “vr”:”2.0" which appears to be the malware version encoded in the communication protocol.

The ‘id’ field is the victim’s fingerprint for which the malware actively uses the Windows Management Instrumentation mechanism. The Trojan runs WMIC.exe with the following arguments:

C:\WINDOWS\system32\wbem\WMIC.exe computersystem get Name /format:list
C:\WINDOWS\system32\wbem\WMIC.exe os get installdate /format:list
C:\WINDOWS\system32\wbem\WMIC.exe path CIM_LogicalDiskBasedOnPartition get Antecedent,Dependent

Then the module concatenates the gathered ids and computes an MD5 hash, which will be the victim’s final id. The “act” field numbers the communication stage (0 for initial fingerprinting). After this, the HTTP POST control server returns a JSON {“rt”:”30"} and the client continues with the next “act” in the HTTP POST:

```
{"id":"dcb0f33785c12345f1b5da2414143b34",
    "act":1
}
```

At this point the C2 sends a JSON with commands to execute, including uploading/downloading files, taking a screenshot and finding *.rar archives on the host.

Other software

Besides the Trojan itself, the Octopus developers used the password dumping utility fgdump.

Infrastructure

MD5 hash	IPs	C2 domain
87126c8489baa8096c6f30456f5bef5e	185.106.120.27 204.145.94.10	porenticofacts.com
ee3c829e7c773b4f94b700902ea3223c		
38f30749a87dcbf156689300737a094e	185.106.120.240 204.145.94.101	certificatesshop.com
6e85996c021d55328322ce8e93b31088	5.188.231.101 103.208.86.238	blondehairman.com
7c0050a3e7aa3172392dcbab3bb92566	5.8.88.87 103.208.86.237	latecafe.in
2bf2f63c927616527a693edf31ecebea	85.93.31.141 104.223.20.136	hovnanflovers.com
d9ad277eb23b6268465edb3f68b12cb2	5.188.231.101 103.208.86.238	blondehairman.com

The most recent samples (2017-2018) of hardcoded IPs and web domains obtained from the .php script

Conclusions

Political entities in Central Asia have been targeted throughout 2018 by different actors, including IndigoZebra, Sofacy (with Zebrocy malware) and most recently by DustSquad (with Octopus malware). Interestingly, we observed some victims who are 'threat magnets' targeted by all of them. From our experience we can say that the interest shown by threat actors in this region is now high, and the traditional 'players' have been joined by relative newcomers like DustSquad that have sprung up locally.

Indicators of compromise

File hashes

87126c8489baa8096c6f30456f5bef5e
ee3c829e7c773b4f94b700902ea3223c
38f30749a87dcbf156689300737a094e
6e85996c021d55328322ce8e93b31088
7c0050a3e7aa3172392dcbab3bb92566
2bf2f63c927616527a693edf31ecebea
d9ad277eb23b6268465edb3f68b12cb2

Domains and IPs

85.93.31.141
104.223.20.136
5.8.88.87
103.208.86.237
185.106.120.240
204.145.94.101
5.188.231.101
103.208.86.238
185.106.120.27
204.145.94.10
hovnanflovers.com
latecafe.in
certificatesshop.com
blondehairman.com
porenticofacts.com

Auxiliary URLs to upload/download files:

www.fayloobmennik.net/files/save_new.html
http://uploadsforyou.com/download/
http://uploadsforyou.com/remove/

The following are old indicators of compromise no longer used by this actor, but which can be used for forensic purposes:

031e4900715564a21d0217c22609d73f
1610cddb80d1be5d711feb46610f8a77
1ce9548eae045433a0c943a07bb0570a
3a54b3f9e9bd54b4098fe592d805bf72
546ab9cdac9a812aab3e785b749c89b2
5cbbdce774a737618b8aa852ae754251
688854008f567e65138c3c34fb2562d0
6fda541befa1ca675d9a0cc310c49061
73d5d104b34fc14d32c04b30ce4de4ae
88ad67294cf53d521f8295aa1a7b5c46
a90caeb6645b6c866ef60eb2d5f2d0c5
ae4e901509b05022bbe7ef340f4ad96c
ca743d10d27277584834e72afefd6be8

ce45e69eac5c55419f2c30d9a8c9104b
df392cd03909ad5cd7dcea83ee6d66a0
e149c1da1e05774e6b168b6b00272eb4
f625ba7f9d7577db561d4a39a6bb134a
fc8b5b2f0b1132527a2bcb5985c2fe6b
f7b1503a48a46e3269e6c6b537b033f8
4f4a8898b0aa4507dbb568dca1dedd38

First stage .php script placed at:

148.251.185.168
185.106.120.46
185.106.120.47
46.249.52.244
5.255.71.84
5.255.71.85
88.198.204.196
92.63.88.142

Domains returned by .php script:

giftfromspace.com
mikohanzer.website
humorpics.download
desperados20.es
prom3.biz.ua